Informatica®
10.5.4

Command Reference

Informatica Command Reference
10.5.4
May 2023

Publication Date: 2023-05-11

Table of Contents

Preface

Refer to the *Informatica® Command Reference* for information about the command line programs and utilities, such as infacmd, infasetup, pmcmd, pmpasswd, and pmrep to manage the Informatica domain, application services, and objects. Learn command descriptions, options, and arguments. You can perform much of the command line functionality through the Administrator tool and other client tools.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Command Line Programs and Utilities

This chapter includes the following topic:

Command Line Programs and Utilities Overview

The Informatica installation includes customer support tools and command line programs and utilities. Use the command line programs and utilities to manage the Informatica domain, application services, and objects. You can run the command line programs and utilities on any machine that can access the Informatica domain.

When you install the Informatica services or the Informatica clients, the command line programs and utilities are installed by default. You can also install and run the programs and utilities on other machines by installing the Informatica utilities.

The following table describes the Informatica utilities:

Command Line Program	Description
infacmd	Administer the Informatica domain and application services and processes, including the repository and integration services. You can also use infacmd to access and administer licenses and log events and export and import objects and user accounts.
infasetup	Administer domains and nodes.
filemanager	Administer the preprocessing and file-watching capabilities for a cloud ecosystem.

The following table describes the PowerCenter® utilities:

Command Line Program	Description
pmcmd	Manage workflows. Use pmcmd to start, stop, schedule, and monitor workflows.
pmpasswd	Encrypt passwords to use with pmcmd and pmrep environment variables.
pmrep	Performs repository administration tasks. Use pmrep to list repository objects, create and edit groups, and restore and delete repositories.

CHAPTER 2

Installing and Configuring Command Line Utilities

This chapter includes the following topics:

Installing and Configuring Command Line Utilities Overview

When you install the Informatica services or the Informatica clients, the command line utilities are installed by default. You can also install and run the command line utilities on any machine without installing the Informatica products.

To install and configure the command line utilities on a machine that does not have the Informatica products installed, complete the following tasks:

- Install the command line utilities.
- Configure the command line utilities.

  Before you run the command line programs, you must configure the environment variables for the command line programs. You must also grant run permission on the utility files to user accounts that run the commands.
- Configure security for the command line utitilities.

  If secure communication is enabled for the domain or if the domain uses Kerberos authentication, perform security configuration on the machines where you installed the command line utilities.

Installing the Command Line Utilities

Informatica provides a separate zip file to install the command line utilities on a machine that does not have the Informatica products installed.

1. Contact Informatica Global Customer Support to get the command line utilities zip file.
2. Extract the files to the machine where you want to run the command line utilities.
3. Make sure that the shell files of the command line utilities have 755 permissions.
4. On Windows, install the Microsoft Visual Studio 2013 redistributable package included in the extracted files. Run the 32-bit or 64-bit file located in the following directory:

   ```
   <Utilities installation directory>/PowerCenter/server/VS2013
   ```

   Informatica products on Windows require the Microsoft Visual Studio 2013 redistributable package. When you install the Informatica services or the Informatica clients, the installer installs the redistributable package for you. When you install the standalone command line utilities, the redistributable package is included in the extracted files, and you must manually install the package.

Installation Directories

The installation directories of the command line utilities vary based on whether the utilities are installed with Informatica services installation, Informatica client installation, or standalone command line utilities installation.

Informatica Services Installation

The Informatica utilities are installed in the following directory:

```
<Informatica installation directory>/isp/bin
```

The PowerCenter utilities are installed in the following directory:

```
<Informatica installation directory>/server/bin
```

The Metadata Manager utilities are installed in the following directory:

```
<Informatica installation directory>/services/MetadataManagerService/utilities
```

Informatica Client Installation

When you install the Developer tool, the Informatica utilities are installed in the following directory:

```
<Informatica installation directory>/clients/DeveloperClient/infacmd
```

When you install the PowerCenter client, the PowerCenter utilities are installed in the following directory:

```
<Informatica installation directory>/clients/PowerCenterClient/CommandLineUtilities/PC/
server/bin
```

When you install the PowerCenter client, the Metadata Manager utilities are installed in the following directory:

```
<Informatica installation directory>/clients/PowerCenterClient/CommandLineUtilities/MM
```

Command Line Utilities Installation

The Informatica utilities are installed in the following directory:

```
<Utilities installation directory>/PowerCenter/isp/bin
```

The PowerCenter utilities are installed in the following directory:

```
<Utilities installation directory>/PowerCenter/server/bin
```

The Metadata Manager utilities are installed in the following directory:

```
<Utilities installation directory>/MetadataManager/utilities
```

Configuring the Command Line Utilities

Configure the path and environment variables as required by the command line utilities. Grant execute permission on the utility files to user accounts that run the commands.

Configure the Informatica Utilities

Configure the environment variables required for the infacmd and infasetup command line programs.

To run infacmd, set the ICMD_JAVA_OPTS environment variable.

To run infasetup, set the INFA_JAVA_CMD_OPTS environment variable.

Configure the PowerCenter Utilities

Before you run the PowerCenter utilities, use the following guidelines to configure the program files and variables:

- To run pmrep, pmcmd, and pmpasswd, copy the domains.infa file for the Informatica domain to the utilities directory.
- To run pmrep, pmcmd, and pmpasswd on UNIX, set the INFA_HOME, PATH, and library path environment variables to the location of the utilities.

For example, if the command line utilities are installed in the `/data/Informatica_cmd_utilities/` folder, then the PowerCenter utilities are located in the `/data/Informatica_cmd_utilities/PowerCenter/server/bin` folder. On Linux, you can set the environment variables at the command prompt as follows:

```
setenv INFA_HOME /data/Informatica_cmd_utilities/PowerCenter/
setenv PATH .:/data/Informatica_cmd_utilities/PowerCenter/server/bin:$PATH
setenv LD_LIBRARY_PATH .:/data/Informatica_cmd_utilities/PowerCenter/server/
bin:$LD_LIBRARY_PATH
```

Note: Restart the machine after you configure the INFA_HOME or library path environment variable.

Configure the Metadata Manager Utilities

To configure the Metadata Manager utilities, configure environment variables that specify the location of the Java Virtual Machine and the Informatica root directory.

If the domain uses Kerberos authentication, create the domains.infa file. Metadata Manager command line programs use the domains.infa file to get gateway connectivity information for the domain.

Configure the following environment variables:

JAVA_HOME

Specifies the location of the Java Virtual Machine. Set JAVA_HOME to the PowerCenter Java directory in the command line utilities installation. For example:

```
<Utilities installation directory>\PowerCenter\java
```

Set this environment variable in each Metadata Manager command line program as follows:

1. Open the batch file or shell script with a text editor.
2. Find the line that sets JAVA_HOME to `@INFA_JDK_HOME@`.
3. Replace the string `@INFA_JDK_HOME@` with the PowerCenter Java directory. For example:

   ```
   set JAVA_HOME=C:\InfaUtilities\PowerCenter\java
   ```
4. Save and close the batch file or shell script.

INFA_HOME

Specifies the Informatica root directory so that any Informatica application or service can find the other Informatica components that it needs to run. Set INFA_HOME to the PowerCenter directory in the command line utilities installation. For example:

```
<Utilities installation directory>\PowerCenter
```

Set this environment variable on each machine where you installed the Informatica utilities.

Note: Restart the machine after you configure the INFA_HOME .

Create the domains.infa File

The domains.infa file contains the gateway connectivity information for the domain. When the domain uses Kerberos authentication, create the domains.infa file so that the command line programs can get the gateway connectivity information for the domain.

If the domain uses Kerberos authentication, you must enter domain connectivity information when you run the command line program commands. You enter domain connectivity information through the --domainName option or the --gateway option. To use the --domainName option, the domains.infa file must contain the domain gateway connectivity information. If the domains.infa file does not exist or the information in the file is out of date, you must use the --gateway option when you run any command that connects to the domain.

When you install Informatica services, the domains.infa file is available in the INFA_HOME directory. For any other installation, create the file and verify that it is available on the machine from which you want to run the commands.

To create the domains.infa file, run the infacmd isp UpdateGatewayInfo command. The command creates or updates the domains.infa file in the PowerCenter directory in the command line utilities installation, for example, `<Utilities installation directory>\PowerCenter`.

Security Configuration for Informatica Utilities

When you install Informatica utilities, you might need to configure the machines based on the domain security configuration. If you do not configure the machines correctly, the command line programs might not be able to authenticate users with the domain.

Configure the machines where you installed the Informatica utilities when the domain uses the following security configurations:

Secure communication

If secure communication is enabled for the domain, you might need to configure the machines to use the truststore file. If you use a custom truststore file, you must configure environment variables that specify the truststore file directory and the truststore password.

Kerberos authentication

If the domain uses Kerberos authentication, you must copy the Kerberos configuration file to the machines where you installed the Informatica utilities. You must also configure the machines to locate the Kerberos configuration file for the domain.

Related Topics:

- " Running Commands in a Secure Domain" on page 39
- "Running Commands on UNIX with Kerberos Authentication" on page 39
- "Running Commands on Windows with Kerberos Authentication" on page 41

CHAPTER 3

Using the Command Line Programs

This chapter includes the following topics:

Using the Command Line Programs Overview

Informatica includes command line programs that you use to complete tasks from any machine in the Informatica environment. The command line programs allow you to run a subset of tasks that you can complete in Informatica Administrator.

For example, you can enable or disable a Repository Service from the Administrator tool or the infacmd command line program.

Informatica includes the following command line programs:

- **infacmd**. Use infacmd to access the Informatica application services.
- **infasetup**. Use infasetup to complete installation tasks such as defining a node or a domain.
- **pmcmd**. Use pmcmd to manage workflows. You can start, stop, schedule, and monitor workflows using pmcmd.
- **pmrep**. Use pmrep to complete repository administration tasks such as listing repository objects, creating and editing groups, and restoring and deleting repositories.
- **mmcmd**. Use mmcmd to load and manage resources and to import and export models and custom resources.
- **mmLineageMigrator**. Use mmLineageMigrator to migrate data lineage linking information after you upgrade from Metadata Manager 9.6.x to the current version.

  Note: Because this program runs automatically, do not run this program unless the migration fails and you fix the error or unless you are directed to run this program by Informatica Global Customer Support.

- **mmRepoCmd**. Use mmRepoCmd to create, delete, back up, and restore Metadata Manager repository contents. You can also restore a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database.
- **mmXConPluginUtil**. Use mmXConPluginUtil to generate the image mapping information or the plug-in for a universal XConnect.
- **rcfmu**. Use rcfmu to migrate a resource configuration file from a previous version of Metadata Manager to the current version.
- **rmu**. Use rmu to migrate resources from a previous version of Metadata Manager to the current version.

To run command line programs on UNIX, you may need to set the library path environment variable to the location of the Informatica utilities.

For ease of use, you can configure environment variables that apply each time you run the command line programs.

For example, you can set an environment variable for the default domain name, user, and password to avoid typing the options at the command line.

Entering Options and Arguments

Each command line program requires a set of options and arguments. These include user name, password, domain name, and connection information.

Use the following rules when you enter command options and arguments:

- To enter options, type a hyphen followed by one letter, two letters, or a word, depending on the program syntax for the command.
  For example, the pmrep Connect command uses a single letter option for the repository name:

  ```
  Connect -r <repository_name>
  ```

- Enter options in any order.
- If any option that you specify from the command line contains spaces, enclose the option in double quotes.
- The first word after the option is the argument.
- Most options require arguments.
  You must separate options from arguments with a single space when using pmcmd or infacmd. You do not have to separate options from arguments when using pmrep.
- If any argument contains more than one word, enclose the argument in double quotes.
  For pmrep and pmcmd, you can also use single quotes.

  Unmatched quotes result in an error.

  For infacmd or pmcmd, the command line programs ignore quotes that do not enclose an argument.
- If an argument is in the format `option_name=value`, and the value contains both a space and an equal sign (=), then you must precede the equal sign with a backslash.
  For example, an argument contains the option `DatabaseUser`, and the database user name is `a#v%5^=! !`.
  Use the following format when you enter the argument: `DBUser=a#v%5^\=! !`
- To update connection options values with existing environment variables, use an escape character before any dollar sign ($) with any shell other than CSH.

- For pmrep, you can use space characters in an argument. To specify an argument containing space characters, enclose the argument with either single or double quote characters. When you use either single or double quotation marks in the argument, you must precede the required quotation marks with a backslash.

Syntax Notation

The following table describes the notation used in this book to show the syntax for all Informatica command line programs:

Convention	Description
-x	Option placed before a argument. This designates the parameter you enter. For example, to enter the user name for pmcmd, type -u or -user followed by the user name.
< x >	Required option. If you omit a required option, the command line program returns an error message.

<x | y >
 	
{x | y}
	Select between required options. For the command to run, you must select from the listed options. If you omit a required option, the command line program returns an error message.
	In pmrep, curly brackets denote groupings of required options, as in the following example:
	`KillUserConnection`
	`  {-i <connection_id> |`
	`  -n <user_name> |`
	`  -a (kill all)}`
	If a pipe symbol (|) separates options, you must specify exactly one option. If options are not separated by pipe symbols, you must specify all the options.

[x]	Optional parameter. The command runs whether or not you enter optional parameters. For example, the Help command has the following syntax: `Help [Command]` If you enter a command, the command line program returns information on that command only. If you omit the command name, the command line program returns a list of all commands.
[x | y]	Select between optional parameters. For example, many commands in pmcmd run in either the wait or nowait mode. `[-wait|-nowait]` If you specify a mode, the command runs in the specified mode. The command runs whether or not you enter the optional parameter. If you do not specify a mode, pmcmd runs the command in the default nowait mode.

Convention	Description
< < x | y> | <a | b> >	When a set contains subsets, the superset is indicated with bold brackets **< >** . A bold pipe symbol (**|**) separates the subsets.
(text)	In pmrep, parentheses surround descriptive text, such as the list of the possible values for an argument or an explanation for an option that does not take an argument.

Running Commands in a Secure Domain

If the Informatica domain has secure communication enabled, you must set environment variables on the machine that hosts the command line programs to run the commands securely. You must set the environment variables before you run the infacmd, pmrep, mmcmd, mmRepoCmd, and pmcmd commands.

Set the following environment variables before you run the commands:

INFA_TRUSTSTORE

Set the INFA_TRUSTSTORE environment variable with the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named infa_truststore.jks and infa_truststore.pem. You must set the INFA_TRUSTSTORE variable whether you use the default SSL certificate from Informatica or you specify a SSL certificate.

INFA_TRUSTSTORE_PASSWORD

If you specify the SSL certificate to enable secure communication in the domain, set the INFA_TRUSTSTORE_PASSWORD environment variable with the password for the infa_truststore.jks that contains the SSL certificate. You do not need to set this variable if you use the default SSL certificate from Informatica.

Note: The password must be encrypted. Use the command line program pmpasswd to encrypt the password with encryption type CRYPT_SYSTEM. For more information, see "Encrypting Passwords" on page 58.

Running Commands on UNIX with Kerberos Authentication

If the Informatica domain uses Kerberos authentication, set the Kerberos configuration environment variable before you run the command line programs. If you run the command line programs with single sign-on, you must generate a credential cache file and specify the path and file name in an environment variable.

You must set the environment variables before you run the infacmd, pmrep, mmcmd, mmRepoCmd, and pmcmd commands on UNIX.

Running Commands on UNIX with Single Sign-On

If you run the command line programs with single sign-on, you must generate a credentials cache file to authenticate the user account running the commands on the Kerberos network. Use the *kinit* utility to generate the credentials cache file.

If you have a credentials cache file, you can run the commands without the user name and password options.

To run commands on UNIX with single sign-on, perform the following tasks:

1. Set the Kerberos environment variables.
2. Download the *kinit* utility and generate a credentials cache file.

Setting the Kerberos Environment Variables

On the machine that hosts the command line programs, specify the location of the credential cache and configuration file in the Kerberos environment variables.

Set the following environment variables:

KRB5CCNAME

Stores the default path and filename for the Kerberos credentials cache. When you run the *kinit* utility to generate the user credential cache, *kinit* stores the credential cache in the default file that you set in the KRB5CCNAME environment variable.

KRB5_CONFIG

Stores the path and file name of the Kerberos configuration file. The name of the Kerberos configuration file is krb5.conf. For information about the contents of the krb5.conf file, see the *Informatica Security Guide*.

Generating the Credentials Cache File

Use the Kerberos *kinit* utility to generate the credentials cache file for the user account that runs the command line programs. The utility is available with the MIT Kerberos V5 download package.

To generate the credentials cache file, perform the following tasks:

1. Download and install MIT Kerberos V5.

   You can download MIT Kerberos V5 from the following website:
   http://web.mit.edu/Kerberos/dist/#krb5-1.12
2. Run the *kinit* utility and specify the user principal name.

   When you create the user credentials cache, you must use the forwardable (-f) option. You can use the following command syntax:

   ```
   kinit -f <principal name>
   ```

   The format for the principal name is <username>@<realmname.com>. Enter the realm name in uppercase letters.

   Note: If you set the *KRB5CCNAME* environment variable before you run the *kinit* utility, *kinit* stores the credentials cache in the location specified in the environment variable.
3. Enter the password for the user account.

Running Commands on UNIX Without Single Sign-On

To run commands on UNIX without single sign-on, set the *KRB5_CONFIG* environment variable to the path and file name of the Kerberos configuration file. Include the user name and password when you run the command or set the user name and password in environment variables.

The commands determine the user credentials based on how you specify the user name and password. The commands check the credentials in the following order:

1. Command options. If you include the user name option (-un) and the password option (-pd) in the command, the command uses the user name and password specified for the options.

   If the domain uses a single Kerberos realm for authentication, specify the samAccountName for the user as the value for the user name option. If the domain uses Kerberos cross realm authentication, specify the user principal name for the user as the value for the user name option.
2. Environment variables. If you do not include the user name and password options in the command, the command uses the user name and password specified in the environment variables INFA_DEFAULT_DOMAIN_USER and INFA_DEFAULT_DOMAIN_PASSWORD.

Note: If you do not set the credentials in the command options or environment variables, the command checks for a credential cache file. If a credential cache is available, the command runs with single sign-on.

Running Commands on Windows with Kerberos Authentication

On Windows, the infacmd, pmrep, mmcmd, mmRepoCmd, and pmcmd commands use the logged in credentials for single sign-on. You do not have to generate a credential cache file.

If you do not use single sign-on on Windows, set the *KRB5_CONFIG* environment variable to the path and file name of the Kerberos configuration file. The name of the configuration file is krb5.conf.
The commands determine the user credentials based on how you specify the user name and password. The commands check the credentials in the following order:

1. Command options. If you include the user name option (-un) and the password option (-pd) in the command, the command uses the user name and password specified for the options.

   If the domain uses a single Kerberos realm for authentication, specify the samAccountName for the user as the value for the user name option. If the domain uses Kerberos cross realm authentication, specify the user principal name for the user as the value for the user name option.
2. Environment variables. If you do not include the user name and password options in the command, the command uses the user name and password specified in the environment variables INFA_DEFAULT_DOMAIN_USER and INFA_DEFAULT_DOMAIN_PASSWORD.

Note: If you do not set the credentials in the command options or environment variables, the command uses the logged-in credentials and runs the command with single sign-on.

CHAPTER 4

Environment Variables for Command Line Programs

This chapter includes the following topics:

Environment Variables for Command Line Programs Overview

You can configure optional environment variables for the command line programs. For example, you can set environment variables to encrypt passwords, configure time and date display options, or store the default login information for a domain.

If you are run pmcmd or pmrep in interactive mode, you must exit the command line program and then reconnect to use changed environment variables.

On Windows, you can configure these environment variables as either user or system variables. For information about setting environment variables on Windows, see the Windows documentation.

Note: The environment variables that you configure apply to command line programs that run on the node. To apply changes, restart the node.

The following table describes environment variables you can configure to use with the command line programs:

Environment Variable	Command Line Programs	Description
ICMD_JAVA_OPTS	infacmd	Sets Java options.
INFA_CLIENT_RESILIENCE_TIMEOUT	infacmd pmcmd pmrep	Limits the number of seconds you want the command line programs to spend establishing a connection to the domain or service.
INFA_CODEPAGENAME	pmcmd pmrep	Configures the character set *pmcmd* and *pmrep* use.
INFA_DEFAULT_CONNECTION_PASSWORD	infacmd	Stores the database truststore file password for the secure database.
INFA_DEFAULT_DATABASE_PASSWORD	infasetup	Stores the default user name password for the domain configuration database.
INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD	infasetup	Stores the database truststore password.
INFA_DEFAULT_DOMAIN	infacmd pmcmd pmrep	Stores the default domain name.
INFA_DEFAULT_DOMAIN_PASSWORD	infacmd	Stores the default user name password for the domain.
INFA_DEFAULT_DOMAIN_USER	infacmd	Stores the default user name for the domain.
INFA_DEFAULT_PWX_OSEPASSWORD	infacmd pwx	Stores an encrypted password for the operating system.
INFA_DEFAULT_PWX_OSPASSWORD	infacmd pwx	Stores a plain text password for the operating system.

Environment Variable	Command Line Programs	Description
INFA_DEFAULT_SECURITY_DOMAIN	infacmd	Stores the security domain for LDAP authentication.
INFA_DOMAINS_FILE	infacmd infasetup pmcmd pmrep	Stores the path and name of the domains.infa file.
INFA_JAVA_CMD_OPTS	infasetup	Sets Java options.
INFA_NODE_KEYSTORE_PASSWORD	infasetup	Stores the password for the infa_keystore.jks file.
INFA_NODE_TRUSTSTORE_PASSWORD	infasetup	Stores the password for the infa_truststore.jks file.
INFA_PASSWORD	infacmd	Stores the default password for the user.
INFA_REPCNX_INFO	pmrep	Stores the name of the repository connection file.
INFA_REPOSITORY_PASSWORD	infacmd	Stores the default PowerCenter Repository password for the user.
INFATOOL_DATEFORMAT	pmcmd	Configures the way pmcmd displays the date and time.
<Password_Environment_Variable>	pmcmd pmrep	Encrypts and stores the password.
<User_Name_Environment_Variable>	pmcmd pmrep	Stores the user name.

Related Topics:

- "Encrypting Passwords" on page 58
- "Setting the User Name" on page 60

ICMD_JAVA_OPTS

ICMD_JAVA_OPTS environment variable applies to the infacmd command line program.

You can configure the environment variable ICMD_JAVA_OPTS to set the Java options such as -Xmx values and system properties. To set a system property, pass the value in the following format:

```
-Dproperty.name=property.value
```

For example, you might want to increase the system memory used by infacmd. The default system memory for infacmd is 512 MB. To configure 1024 MB of system memory in a UNIX C shell environment, type:

```
setenv ICMD_JAVA_OPTS "-Xmx1024m"
```

Configuring ICMD_JAVA_OPTS on UNIX

To configure ICMD_JAVA_OPTS on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv ICMD_JAVA_OPTS <Java_Options>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  ICMD_JAVA_OPTS = <Java_Options>
  export ICMD_JAVA_OPTS
  ```

Configuring ICMD_JAVA_OPTS on Windows

To configure ICMD_JAVA_OPTS on Windows:

- Enter the environment variable ICMD_JAVA_OPTS, and set the Java options such as the -Xmx values and system properties.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_CLIENT_RESILIENCE_TIMEOUT

INFA_CLIENT_RESILIENCE_TIMEOUT environment variable applies to the infacmd, pmcmd, and pmrep command line programs.

You can set the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT to limit the number of seconds the command line programs spend establishing connections to the domain or service. The default time is 180 seconds if you do not set this environment variable.

Configuring INFA_CLIENT_RESILIENCE_TIMEOUT on UNIX

To configure INFA_CLIENT_RESILIENCE_TIMEOUT on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_CLIENT_RESILIENCE_TIMEOUT <number of seconds>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_CLIENT_RESILIENCE_TIMEOUT = <number of seconds>
  export INFA_CLIENT_RESILIENCE_TIMEOUT
  ```

Configuring INFA_CLIENT_RESILIENCE_TIMEOUT on Windows

To configure INFA_CLIENT_RESILIENCE_TIMEOUT on Windows:

- Enter the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT, and set the value to the number of seconds you want the command line programs to spend establishing a connection to the domain or service.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_CODEPAGENAME

INFA_CODEPAGENAME environment variable applies to the pmcmd and pmrep command line programs.

pmcmd and *pmrep* send commands in Unicode and use the code page of the host machine unless you set the code page environment variable, INFA_CODEPAGENAME, to override it. If you set INFA_CODEPAGENAME for *pmcmd,* the code page must be compatible with the Integration Service code page. If you set INFA_CODEPAGENAME for *pmrep*, the code page name must be compatible with the repository code page. If you set INFA_CODEPAGENAME on the machine where you run *pmcmd* and *pmrep*, the code page must be compatible with the Integration Service and the repository code pages.

If the code pages are not compatible, the command might fail.

Configuring INFA_CODEPAGENAME on UNIX

To configure INFA_CODEPAGENAME on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_CODEPAGENAME <code page name>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_CODEPAGENAME = <code page name>
  export INFA_CODEPAGENAME
  ```

Configuring INFA_CODEPAGENAME on Windows

To configure INFA_CODEPAGENAME on Windows:

- Enter the environment variable INFA_CODEPAGENAME, and set the value to the code page name.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_DATABASE_PASSWORD

INFA_DEFAULT_DATABASE_PASSWORD environment variable applies to the infasetup command line program.

Some *infasetup* commands require a domain configuration database password. You can provide this password as an option with *infasetup*, or you can store it as the environment variable INFA_DEFAULT_DATABASE_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the database user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password “monday,” it encrypts to f/wRb5PZsZnqESTDPeos7Q==.
2. Configure the password environment variable to set the encrypted value.

Related Topics:

- "Encrypting Passwords" on page 58

Configuring INFA_DEFAULT_DATABASE_PASSWORD on UNIX

To configure INFA_DEFAULT_DATABASE_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_DEFAULT_DATABASE_PASSWORD <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_DEFAULT_DATABASE_PASSWORD = <encrypted password>
   export INFA_DEFAULT_DATABASE_PASSWORD
   ```

Configuring INFA_DEFAULT_DATABASE_PASSWORD on Windows

To configure INFA_DEFAULT_DATABASE_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the environment variable INFA_DEFAULT_DATABASE_PASSWORD, and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD

INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD environment variable applies to the infasetup command line program.

Some *infasetup* commands configure secure communication for the domain. You can provide the password for the database truststore file for the secure database as an option with *infasetup*, or you can store it as the environment variable INFA_DEFAULT_DB_TRUSTSTORE_DATABASE_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the database user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.

2. Configure the password environment variable to set the encrypted value.

Configuring INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD on UNIX

To configure INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD = <encrypted password>
   export INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD
   ```

Configuring INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD on Windows

To configure INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the environment variable INFA_DEFAULT_DB_TRUSTSTORE_PASSWORD, and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_DOMAIN

INFA_DEFAULT_DOMAIN environment variable applies to the infacmd, pmcmd, and pmrep command line programs.

The command line programs require a domain name. You can provide the domain name as an option with the command line programs, or you can store it as the environment variable INFA_DEFAULT_DOMAIN. If you have more than one domain, choose a default domain.

Configuring INFA_DEFAULT_DOMAIN on UNIX

To configure INFA_DEFAULT_DOMAIN on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_DEFAULT_DOMAIN <domain name>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_DEFAULT_DOMAIN = <domain name>
  export INFA_DEFAULT_DOMAIN
  ```

Configuring INFA_DEFAULT_DOMAIN on Windows

To configure INFA_DEFAULT_DOMAIN on Windows:

- Enter the environment variable INFA_DEFAULT_DOMAIN, and set the value to the domain name.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_DOMAIN_PASSWORD

INFA_DEFAULT_DOMAIN_PASSWORD environment variable applies to the infacmd command line program.

Most *infacmd* commands require a user password. You can provide a user password as an option with *infacmd*, or you can store it as the environment variable INFA_DEFAULT_DOMAIN_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.
2. Configure the password environment variable to set the encrypted value.

Related Topics:

- "Encrypting Passwords" on page 58

Configuring INFA_DEFAULT_DOMAIN_PASSWORD on UNIX

To configure INFA_DEFAULT_DOMAIN_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.
2. In a UNIX C shell environment, type:

   ```
   setenv INFA_DEFAULT_DOMAIN_PASSWORD <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_DEFAULT_DOMAIN_PASSWORD = <encrypted password>
   export INFA_DEFAULT_DOMAIN_PASSWORD
   ```

Configuring INFA_DEFAULT_DOMAIN_PASSWORD on Windows

To configure INFA_DEFAULT_DOMAIN_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.
2. Enter the environment variable INFA_DEFAULT_DOMAIN_PASSWORD, and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_DOMAIN_USER

INFA_DEFAULT_DOMAIN_USER environment variable applies to the infacmd command line program.

Most *infacmd* commands require a user name. You can provide a user name as an option with *infacmd*, or you can store it as the environment variable INFA_DEFAULT_DOMAIN_USER.

Configuring INFA_DEFAULT_DOMAIN_USER on UNIX

To configure INFA_DEFAULT_DOMAIN_USER on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_DEFAULT_DOMAIN_USER <user name>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_DEFAULT_DOMAIN_USER = <user name>
  export INFA_DEFAULT_DOMAIN_USER
  ```

Configuring INFA_DEFAULT_DOMAIN_USER on Windows

To configure INFA_DEFAULT_DOMAIN_USER on Windows:

- Enter the environment variable INFA_DEFAULT_DOMAIN_USER, and set the value to the default user name.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DEFAULT_PWX_OSEPASSWORD

INFA_DEFAULT_PWX_OSEPASSWORD environment variable applies to the infacmd pwx command line program.

Some infacmd pwx commands require an operating system password. You can provide an encrypted password as an option with infacmd pwx, or you can store it as the environment variable INFA_DEFAULT_PWX_OSEPASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. To encrypt the password, use the pmpasswd command line program.

   The pmpasswd program generates and displays the encrypted password. For example, if you enter the password “monday,” it encrypts to f/wRb5PZsZnqESTDPeos7Q==.
2. Configure the password environment variable to set the encrypted value.

Related Topics:

- "Encrypting Passwords" on page 58

Configuring INFA_DEFAULT_PWX_OSEPASSWORD on UNIX

To configure INFA_DEFAULT_PWX_OSEPASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd password
   ```

   The pmpasswd program returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_DEFAULT_PWX_OSEPASSWORD encrypted_password
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_DEFAULT_PWX_OSEPASSWORD = encrypted_password
   export INFA_DEFAULT_PWX_OSEPASSWORD
   ```

Configuring INFA_DEFAULT_PWX_OSEPASSWORD on Windows

To configure INFA_DEFAULT_PWX_OSEPASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd password
   ```

   The pmpasswd program returns the encrypted password.

2. Enter the environment variable INFA_DEFAULT_PWX_OSEPASSWORD, and set the value to the encrypted password.

   For information about setting environment variables on Windows, see the Windows documentation.

INFA_DEFAULT_PWX_OSPASSWORD

INFA_DEFAULT_PWX_OSPASSWORD environment variable applies to the infacmd pwx command line program.

Some infacmd pwx commands require an operating system password. You can provide a plain text password as an option with infacmd pwx, or you can store it as the environment variable INFA_DEFAULT_PWX_OSPASSWORD.

Configuring INFA_DEFAULT_PWX_OSPASSWORD on UNIX

To configure INFA_DEFAULT_PWX_OSPASSWORD on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_DEFAULT_PWX_OSPASSWORD password
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_DEFAULT_PWX_OSPASSWORD = password
  export INFA_DEFAULT_PWX_OSPASSWORD
  ```

Configuring INFA_DEFAULT_PWX_OSPASSWORD on Windows

To configure INFA_DEFAULT_PWX_OSPASSWORD on Windows, set the value to the plain text password.

For information about setting environment variables on Windows, see the Windows documentation.

INFA_DEFAULT_SECURITY_DOMAIN

INFA_DEFAULT_SECURITY_DOMAIN environment variable applies to the infacmd command line program.

The infacmd commands require a security domain if you use LDAP authentication and you specify an Informatica user. You can set the environment variable INFA_DEFAULT_SECURITY_DOMAIN to the native security domain or to an LDAP security domain name.

Configuring INFA_DEFAULT_SECURITY_DOMAIN on UNIX

To configure INFA_DEFAULT_SECURITY_DOMAIN on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_DEFAULT_SECURITY_DOMAIN <security domain name>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_DEFAULT_SECURITY_DOMAIN = <security domain name>
  export INFA_DEFAULT_SECURITY_DOMAIN
  ```

Configuring INFA_DEFAULT_SECURITY_DOMAIN on Windows

To configure INFA_DEFAULT_SECURITY_DOMAIN on Windows:

- Enter the environment variable INFA_DEFAULT_SECURITY_DOMAIN and set the value to the name of the security domain.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_DOMAINS_FILE

INFA_DOMAINS_FILE environment variable applies to the infacmd, infasetup, pmcmd, and pmrep command line programs.

When you install the Informatica services using the Informatica installer, the installer creates a domains.infa file in the Informatica installation directory. The domains.infa file contains the connectivity information for the gateway nodes in a domain, including the domain names, domain host names, and domain host port numbers. The command line programs require the connectivity information present in the domains.infa file to connect to the gateway nodes in a domain. You can set the environment variable INFA_DOMAINS_FILE to the path and name of the domains.infa file. Ensure that you configure the INFA_DOMAINS_FILE variable on the machine where the Informatica services are installed.

Configuring INFA_DOMAINS_FILE on UNIX

To configure INFA_DOMAINS_FILE on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_DOMAINS_FILE <file path><file name>
  ```

In a UNIX Bourne shell environment, type:

```
INFA_DOMAINS_FILE = <file path><file name>
export INFA_DOMAINS_FILE
```

Configuring INFA_DOMAINS_FILE on Windows

To configure INFA_DOMAINS_FILE on Windows:

- Enter the environment variable INFA_DOMAINS_FILE and set the value to the path and name of the domains.infa file.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_JAVA_CMD_OPTS

INFA_JAVA_CMD_OPTS environment variable applies to the infasetup command line program.

You can configure the environment variable INFA_JAVA_CMD_OPTS to set the Java options such as -Xmx values and system properties. To set a system property, pass the value in the following format:

```
-Dproperty.name=property.value
```

For example, you might want to increase the system memory used by infasetup. The default system memory for infasetup is 512 MB. To configure 1024 MB of system memory in a UNIX C shell environment, type:

```
setenv INFA_JAVA_CMD_OPTS "-Xmx1024m"
```

Configuring INFA_JAVA_CMD_OPTS on UNIX

To configure INFA_JAVA_CMD_OPTS on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_JAVA_CMD_OPTS <Java_Options>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFA_JAVA_CMD_OPTS = <Java_Options>
  export INFA_JAVA_CMD_OPTS
  ```

Configuring INFA_JAVA_CMD_OPTS on Windows

To configure INFA_JAVA_CMD_OPTS on Windows:

- Enter the environment variable INFA_JAVA_CMD_OPTS, and set the Java options such as the -Xmx values and system properties.

  For information about setting environment variables on Windows, consult the Windows documentation.

INFA_PASSWORD

INFA_PASSWORD environment variable applies to the infacmd and infasetup command line programs.

Some infacmd and infasetup commands require a user password. You can provide a user password as an option with these commands, or you can store it as the environment variable INFA_PASSWORD.

You can use the INFA_PASSWORD environment variable to store different types of passwords. For example in the infasetup DefineDomain command, you can use the variable to set the keystore password. In the infacmd isp SetLDAPConnectivity command, you can use the variable to set the LDAP credential password. You may need to change the value of this variable based on the commands that you run.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program pmpasswd to encrypt the user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.
2. Configure the password environment variable to set the encrypted value.

Related Topics:

- "Encrypting Passwords" on page 58

Configuring INFA_PASSWORD on UNIX

To configure INFA_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.
2. In a UNIX C shell environment, type:

   ```
   setenv INFA_PASSWORD <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_PASSWORD = <encrypted password>
   export INFA_PASSWORD
   ```

Configuring INFA_PASSWORD on Windows

To configure INFA_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.
2. Enter the environment variable INFA_PASSWORD, and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_NODE_KEYSTORE_PASSWORD

The INFA_NODE_KEYSTORE_PASSWORD environment variable applies to the infasetup command line program.

Some *infasetup* commands configure secure communication for the domain. You can provide the password for the informatica Java Keystore (JKS) file as an option with *infasetup*, or you can store it as the environment variable INFA_NODE_KEYSTORE_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the database user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.

2. Configure the password environment variable to set the encrypted value.

Configuring INFA_NODE_KEYSTORE_PASSWORD on UNIX

To configure INFA_NODE_KEYSTORE_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_NODE_KEYSTORE_PASSWORD  <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_NODE_KEYSTORE_PASSWORD  = <encrypted password>
   export INFA_NODE_KEYSTORE_PASSWORD
   ```

Configuring INFA_NODE_KEYSTORE_PASSWORD on Windows

To configure INFA_NODE_KEYSTORE_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the environment variable INFA_NODE_KEYSTORE_PASSWORD , and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_NODE_TRUSTSTORE_PASSWORD

The INFA_NODE_TRUSTSTORE_PASSWORD environment variable applies to the infasetup command line program.

Some *infasetup* commands configure secure communication for the domain. You can provide the password for the infa_truststore.jks file as an option with *infasetup*, or you can store it as the environment variable INFA_NODE_TRUSTSTORE_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the database user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.

2. Configure the password environment variable to set the encrypted value.

Configuring INFA_NODE_TRUSTSTORE_PASSWORD on UNIX

To configure INFA_NODE_TRUSTSTORE_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_NODE_TRUSTSTORE_PASSWORD  <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_NODE_TRUSTSTORE_PASSWORD  = <encrypted password>
   export INFA_NODE_TRUSTSTORE_PASSWORD
   ```

Configuring INFA_NODE_TRUSTSTORE_PASSWORD on Windows

To configure INFA_NODE_TRUSTSTORE_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <database password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the environment variable INFA_NODE_TRUSTSTORE_PASSWORD , and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFA_REPCNX_INFO

The INFA_REPCNX_INFO environment variable applies to the pmrep command line program.

When you run *pmrep* in command line mode or from a script, it stores repository connection information in a file, pmrep.cnx. *pmrep* uses the information in this file to reconnect to the repository. The INFA_REPCNX_INFO environment variable stores the file name and file path for the repository connection file. Each time you run *pmrep connect*, the command deletes the pmrep.cnx file. If the pmrep connect command succeeds, the command replaces the pmrep.cnx file with the repository connection information.

Use this variable when scripts that issue *pmrep* commands run simultaneously, and the scripts connect to different repositories. In each shell, specify a different repository connection file. This prevents a script from overwriting the connection information used by another script.

If you do not set this environment variable, *pmrep* stores connection information in pmrep.cnx in the home directory. If you want to set the pmrep.cnx file in another location, specify the file path using the INFA_REPCNX_INFO environment variable.

Configuring INFA_REPCNX_INFO on UNIX

To configure INFA_REPCNX_INFO on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFA_REPCNX_INFO <file name>
  ```

In a UNIX Bourne shell environment, type:

```
INFA_REPCNX_INFO = <file name>
export INFA_REPCNX_INFO
```

Configuring INFA_REPCNX_INFO on Windows

To configure INFA_REPCNX_INFO on Windows:

- In a DOS shell, type:

  ```
  set INFA_REPCNX_INFO = <file name>
  ```

  Note: If you run multiple *pmrep* scripts, set this environment variable for the DOS shell, not for the machine.

INFA_REPOSITORY_PASSWORD

INFA_REPOSITORY_PASSWORD environment variable applies to the infacmd command line program.

Some *infacmd* commands require a PowerCenter repository password. You can provide a user password as an option with *infacmd*, or you can store it as the environment variable INFA_REPOSITORY_PASSWORD.

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the user password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password "monday," it encrypts to f/wRb5PZsZnqESTDPeos7Q==.

2. Configure the password environment variable to set the encrypted value.

Related Topics:

- "Encrypting Passwords" on page 58

Configuring INFA_REPOSITORY_PASSWORD on UNIX

To configure INFA_REPOSITORY_PASSWORD on UNIX:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv INFA_REPOSITORY_PASSWORD <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   INFA_REPOSITORY_PASSWORD = <encrypted password>
   export INFA_REPOSITORY_PASSWORD
   ```

Configuring INFA_REPOSITORY_PASSWORD on Windows

To configure INFA_REPOSITORY_PASSWORD on Windows:

1. At the command line, type:

   ```
   pmpasswd <repository password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the environment variable INFA_REPOSITORY_PASSWORD, and set the value to the *encrypted* password.

   For information about setting environment variables on Windows, consult the Windows documentation.

INFATOOL_DATEFORMAT

INFATOOL_DATEFORMAT environment variable applies to the pmcmd command line program.

Use this environment variable to customize the way *pmcmd* displays the date and time. Enter the date format string in DY MON DD HH24:MI:SS YYYY format. *pmcmd* verifies that the string is a valid format. If the format string is not valid, the Integration Service generates a warning message and displays the date in the format DY MON DD HH24:MI:SS YYYY.

Configuring INFATOOL_DATEFORMAT on UNIX

To configure INFATOOL_DATEFORMAT on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv INFATOOL_DATEFORMAT <date/time format string>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  INFATOOL_DATEFORMAT = <date/time format string>
  export INFATOOL_DATEFORMAT
  ```

Configuring INFATOOL_DATEFORMAT on Windows

To configure INFATOOL_DATEFORMAT on Windows:

- Enter the environment variable INFATOOL_DATEFORMAT, and set the value to the display format string.

  For information about setting environment variables on Windows, consult the Windows documentation.

Encrypting Passwords

You can encrypt passwords to create an environment variable to use with infacmd, infasetup, pmcmd, and pmrep or to define a password in a parameter file.

For example, you can encrypt the repository and database passwords for pmrep to maintain security when using pmrep in scripts. Then you can create an environment variable to store the encrypted password. Or, you can define a password for a relational database connection object in a parameter file.

Use the command line program pmpasswd to encrypt passwords.

The pmpasswd utility uses a AES/CBC/PKCS5 padding cipher and generates a base64 encoded and AES 128-bit or AES 256-bit encrypted password.

The pmpasswd utility installs in the following directory:

```
<InformaticaInstallationDir>/server/bin
```

The pmpasswd utility uses the following syntax:

```
pmpasswd <password> [-e (CRYPT_DATA | CRYPT_SYSTEM)]
```

The following table describes pmpasswd options and arguments:

Option	Argument	Description
-	password	Required. The password to encrypt.
-e	CRYPT_DATA, CRYPT_SYSTEM	Optional. Encryption type: - CRYPT_DATA. Use to encrypt connection object passwords that you define in a parameter file. - CRYPT_SYSTEM. Use for all other passwords. Default is CRYPT_SYSTEM.

By default, the pmpasswd utility generates AES 128-bit encrypted password. You can set the environment variable INFA_USE_AES_256_CRYPTOGRAPHER to *true* to enable AES 256-bit encryption for enhanced password security. In single node domain or multinode domain, ensure to shutdown the domain before setting or removing the environment variable.

When you enable the AES 256-bit encryption, the previously stored sensitive data in the environment variables does not work. You must encrypt such previously stored sensitive data again and reset the data in the environment variables after enabling AES 256-bit encryption. However, the license keys remain encrypted with AES 128-bit even if you enable AES 256-bit.

After you choose either AES 128-bit or AES 256-bit encryption, you must use the same encryption mechanism while performing a backup and restore or export and import operation. For example, if you back up a domain or repository using the AES 128-bit mechanism, you must restore the domain or repository using the same 128-bit encryption mechanism. Domain restore fails if AES 256-bit encryption is enabled for domain backup and not enabled during domain restore. In such a case, clean up the database, enable 256-bit encryption and restore the domain again.

Similarly, if you export a domain or repository using the AES 128-bit mechanism, you must import the domain or repository using the same 128-bit encryption mechanism.

Using a Password as an Environment Variable

Use the following steps as a guideline to use an encrypted password as an environment variable:

1. Use the command line program *pmpasswd* to encrypt the password.

   pmpasswd generates and displays the encrypted password. For example, if you enter the password “monday,” the password encrypts to f/wRb5PZsZnqESTDPeos7Q==.

2. Configure the password environment variable to set the encrypted value.

Configuring a Password as an Environment Variable on UNIX

To configure a password as an environment variable on UNIX:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.

2. In a UNIX C shell environment, type:

   ```
   setenv <Password_Environment_Variable> <encrypted password>
   ```

   In a UNIX Bourne shell environment, type:

   ```
   <Password_Environment_Variable> = <encrypted password>
   export <Password_Environment_Variable>
   ```

   You can assign the environment variable any valid UNIX name.

Configuring a Password as an Environment Variable on Windows

To configure a password as an environment variable on Windows:

1. At the command line, type:

   ```
   pmpasswd <password>
   ```

   pmpasswd returns the encrypted password.

2. Enter the password environment variable in the Variable field. Enter the *encrypted* password in the Value field.

   For information about setting environment variables on Windows, consult the Windows documentation.

Setting the User Name

For *pmcmd* and *pmrep*, you can create an environment variable to store the user name.

Configuring a User Name as an Environment Variable on UNIX

To configure a user name as an environment variable on UNIX:

- In a UNIX C shell environment, type:

  ```
  setenv <User_Name_Environment_Variable> <user name>
  ```

  In a UNIX Bourne shell environment, type:

  ```
  <User_Name_Environment_Variable> = <user name>
  export <User_Name_Environment_Variable>
  ```

  You can assign the environment variable any valid UNIX name.

Configuring a User Name as an Environment Variable on Windows

To configure a user name as an environment variable on Windows:

- Enter the user name environment variable in the Variable field. Enter the user name in the Value field.

  For information about setting environment variables on Windows, consult the Windows documentation.

CHAPTER 5

Using infacmd

This chapter includes the following topics:

Using infacmd Overview

infacmd is a command line program that allows you to administer domains, users, and services. Use *infacmd* to administer the following objects and services:

- **Application services and processes.** Create, enable, disable, remove, and get the status of application services and the associated service processes. Ping services. List services and the nodes that run them. Update service processes and service process options. You cannot use *infacmd* to create services of a previous version.
- **Domain gateway.** Update the gateway node connectivity information.
- **Domains.** Link domains and remove domain links. Change the domain administrator password. Update domain options. Add and remove service levels.
- **Folders.** Create, move, list, update, and remove folders. Move objects between folders.
- **Grids.** Create and remove grids. List nodes in a grid.
- **Licenses.** Add, remove, assign, unassign, and list licenses. Show license information.
- **Log events.** Get and purge log events. Get session and workflow logs. Convert log files from binary to text format.
- **Nodes.** Update, ping, shut down, and remove nodes. List node names and options. Update the node role. Add, enable, list, disable, and remove node resources. Change a node from a gateway node to a worker node or from a worker node to a gateway node. Calculate the CPU profile for a node.
- **Users.** Create and remove users. Reset user passwords. Subscribe to and unsubscribe users from alerts. Assign users permission on objects. Enable user account lockout and unlock user accounts.

infacmd ListPlugins

Each infacmd program has a plugin identifier. When you run the program, you include the plugin ID as part of the program name.

For example, dis is the plugin ID for the Data Integration Services infacmd program.

For example, to run a command that lists deployed applications, run the infacmd dis ListApplications command:

```
infacmd dis ListApplications -dn domain_name -un user_name -d password -sn
Data_Integration_Service_Name
```

To list the plugin IDs, enter the following command:

```
infacmd (.sh) ListPlugins
```

To list the valid commands for a plugin, enter the following command:

```
infacmd(.sh) plugin_ID Help
```

To display help for one command, enter the following command:

```
infacmd(.sh) plugin_ID CommandName Help
```

Running Commands

Invoke infacmd from the command line. You can issue commands directly or from a script, batch file, or other program.

To run infacmd commands:

1. At the command prompt, switch to the directory where the infacmd executable is located.

   By default, infacmd installs in the following directory of the Informatica services installation:
   `<Informatica installation directory>/isp/bin`

2. Enter `infacmd` on Windows or `infacmd.sh` on UNIX followed by the plugin ID, the command name, and the required options and arguments. The command names are not case sensitive.

   For example:

   ```
   infacmd(.sh) plugin_ID CommandName [-option1] argument_1 [-option2]
   argument_2...Command Options
   ```

When you run infacmd, you enter options for each command, followed by the required arguments. For example, most commands require that you enter the domain name, user name, and password using command options. Command options are preceded with a hyphen and are not case sensitive. Arguments follow the option.

To enter an argument that is preceded with a hyphen, enclose the argument in quotation marks using the backslash (\) as an escape character before each quotation mark. For example, the following command writes the log for the mapping run with the job ID "-qnLI7G_TEeW9olHBkc9hoA" to the file "MyLog.log" within the infacmd directory on Windows:

```
infacmd ms GetRequestLog -dn MyDomain -sn MyDIS -un AdminUser -pd password -id \"-
qnLI7G_TEeW9olHBkc9hoA\" -f MyLog.log
```

If you omit or incorrectly enter one of the required options, the command fails and infacmd returns an error message.

You can use environment variables for some command options with infacmd. For example, you can store the default user name and password for a domain as environment variables so that you do not have to enter them using command options. Configure these variables before you use infacmd.

Connecting to the Domain

The infacmd command line program contains options that you use to connect to the domain. These options are common for all commands.

The following table describes the infacmd options that are common to all commands:

Option	Description
-DomainName -dn	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Required if the domain uses Native or LDAP authentication. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on. If the domain uses a single Kerberos realm for authentication, specify the samAccountName for the user. If the domain uses Kerberos cross realm authentication, specify the user principal name for the user.
-Password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. If the domain uses native authentication, the default is native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation. Default is Native.
-ResilienceTimeout -re	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

infacmd Return Codes

The infacmd program indicates the success or failure of a command with the following return codes:

- 0 indicates that the command succeeded.
- -1 indicates that the command failed.

Use the DOS or UNIX echo command immediately after running an infacmd command to see the return code for the command:

- In a DOS shell: `echo %ERRORLEVEL%`
- In a UNIX Bourne or Korn shell: `echo $?`
- In a UNIX C shell: `echo $status`

CHAPTER 6

infacmd as Command Reference

This chapter includes the following topics:

CreateExceptionAuditTables

Creates tables that can contain audit trail data for the work that Analyst tool users perform in exception management tasks.

The infacmd as CreateExceptionAuditTables command uses the following syntax:

```
CreateExceptionAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as CreateExceptionAuditTables options:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Analyst Service name.

Option	Description
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

Rules and Guidelines for Exception Management Audit Tables

Before you create tables to store audit data for exception management tasks, review the following rules and guidelines:

- The Analyst Service writes audit data for the exception management tasks that a Data Integration Service creates when it runs a workflow that contains a Human task. Each exception management task is an instance of a Human task in a workflow.

  The HumanTaskDataIntegrationService option on the infacmd as createService help command identifies the Data Integration Service that creates the exception management tasks.
- Before you create the exception Management audit tables, identify a database and a schema for the tables. To identify the database and schema, run the infacmd as updateServiceOptions command.

  When you run infacmd as updateServiceOptions, set the following options:

  -o HumanTaskDataIntegrationService.exceptionDbName

  -o HumanTaskDataIntegrationService.exceptionSchemaName
- The audit tables contain all audit trail data for the work that users perform in the Analyst tool that the Analyst Service specifies. If you do not create the audit tables, the Analyst Service creates audit tables for each exception management task in the database that contains the task data.

CreateService

Creates an Analyst Service in a domain. Also associates a Model Repository Service, Data Integration Services, and Metadata Manager Service with the Analyst Service.

The infacmd as CreateService command uses the following syntax:

```
CreateService

<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-RepositoryService|-rs> model_repository_service_name]
[<-DataIntegrationService|-ds> data_integration_service_name]
```

```
[<-HumanTaskDataIntegrationService|-htds> human_task_data_integration_service_name]
[<-MetadataManagerService|-mm> metadata_manager_service_name]
[<-FlatFileCacheLocation|-ffl> flat_file_location]
[<-CatalogService|-cs> catalog_service_name]
[<-CatalogServiceUserName|-csau> catalog_service_user_name]
[<-CatalogServiceSecurityDomain|-cssdn> catalog_service_security_domain]
[<-CatalogServicePassword|-csap> catalog_service_password]
[<-RepositoryUsername|-au> model_repository_user_name]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
[<-RepositoryPassword|-ap> model_repository_password]
[<-BusinessGlossaryExportFileDirectory|-bgefd> business_glossary_export_file_directory]
<-HttpPort> http_port
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as CreateService options:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-NodeName -nn	Required. Name of the node where the Analyst Service will run.
-ServiceName -sn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-RepositoryService -rs	Optional. Name of the Model Repository Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
-DataIntegrationService -ds	Optional. Data Integration Service name associated with the Analyst Service.

Option	Description
-HumanTaskDataIntegrationService -htds	Optional. Data Integration Service that runs workflows. When a workflow contains a Human task, users log in to the Analyst Service URL to work on the Human task instances.
-MetadataManagerService -mm	Optional. Metadata Manager Service name associated with the Analyst Service.
-FlatFileCacheLocation -ffl	Optional. Full path, excluding the domain name, to the folder in which you want to cache the flat files. Must be in the following format: /<parent folder>/>child folder>
-CatalogService -cs	Optional. Name of the Catalog Service that you want to associate with the Analyst Service.
-CatalogServiceUserName -csau	Optional. Required if you specify Catalog Service. Administrator user name to connect to the Catalog Service.
-CatalogServiceSecurityDomain -cssdn	Required if you use LDAP authentication. Name of the security domain to which the Administrator user belongs.
-CatalogServicePassword -csap	Required if you specify a Catalog Service. User password for the Catalog Service.
-RepositoryUserName -au	Required if you specify a Model Repository Service. User name to connect to the Model repository. If you enter a user name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositorySecurityDomain -rssdn	Required if you use LDAP authentication. Name of the security domain to which the Administrator user belongs.
-RepositoryPassword -ap	Required if you specify a Model Repository Service. User password for the Model Repository Service.
-BusinessGlossaryExportFileDirectory -bgefd	Optional. Location of the directory to export business glossary files.
-HttpPort	Required. Port number for the Analyst Service.

DeleteExceptionAuditTables

Deletes tables that can contain audit trail data for the work that Analyst tool users perform in exception management tasks.

The infacmd as DeleteExceptionAuditTables command uses the following syntax:

```
DeleteExceptionAuditTables
<-DomainName|-dn> domain_name
```

```
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as DeleteExceptionAuditTables options:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Analyst Service name.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

ListServiceOptions

Lists Analyst Service options. Lists the values for each Analyst Service option.

The infacmd as ListServiceOptions command uses the following syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as ListServiceOptions:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Name of the Analyst Service. The name is not case sensitive.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

ListServiceProcessOptions

Lists the Analyst Service process options.

The infacmd as ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as ListServiceProcessOptions:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Name of the Analyst Service. The name is not case sensitive.

Option	Description
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-NodeName -nn	Required. Node where the Analyst Service process runs.

UpdateServiceOptions

Updates Analyst Service options. To view current option values, run infacmd as ListServiceOptions.

The infacmd as UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options |-o> options]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as UpdateServiceOptions :

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Name of the Analyst Service. The name is not case sensitive.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.

Option	Description
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-Options -o	Optional. List of options to configure. Separate each option with a space. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. For example, `... -o option_name=value option_name="value 2" ...` To view options, run the infacmd as ListServiceOptions command.

UpdateServiceProcessOptions

Updates options for the Analyst Service process. To view options, run the infacmd as ListServiceProcessOptions command.

The infacmd as UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd as UpdateServiceProcessOptions:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-ServiceName -sn	Required. Name of the Analyst Service.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.

Option	Description
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-NodeName -nn	Required. Node where the Analyst Service process runs.
-Options -o	Required. List of options to configure. Separate each option with a space. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. For example, `... -o option_name=value option_name="value 2" ...` To view options, run the infacmd as ListServiceProcessOptions command.

CHAPTER 7

infacmd aud Command Reference

This chapter includes the following topics:

getDomainObjectPermissions

Gets the list of domain objects to which the specified users or groups have permission. You can generate reports for the specified users or groups.

Users with the administrator role can run this command.

The infacmd aud getDomainObjectPermissions command uses the following syntax:

```
getDomainObjectPermissions

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd aud getDomainObjectPermissions options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain that you want to create to which the domain user belongs.
–Gateway –hp	Required if the gateway connectivity information in the domains.infa file is out of date. Specify the host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ExistingUserNames -eu	Required if you do not use -ExistingGroupNames (-eg). Name of the user or a list of users to run the reports. For multiple users, separate each user by a comma at the command line.
-ExistingGroupNames -eg	Required if you do not use -ExistingUserName (-eu). Name of the group or a list of groups to run the reports. For multiple groups, separate each group by a comma at the command line.
-ExistingSecurityDomain -esd	Required if you use LDAP authentication. Security domain to which the user or group belongs. Default is Native.
-Format -fm	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

getPrivilegeAssociation

Gets privileges assigned to the users or groups. You can select the users or groups for which you want to generate report.

Users with the administrator role can run this command.

The infacmd aud getPrivilegeAssociation command uses the following syntax:

```
getPrivilegeAssociation

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd aud getPrivilegeAssociation options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
–Gateway –hp	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ExistingUserNames -eu	Required if you do not use -ExistingGroupNames (-eg). Name of the user or a list of users to run the reports. For multiple users, separate each user by a comma at the command line.
-ExistingGroupNames -eg	Required if you do not use -ExistingUserName (-eu). Name of the group or a list of groups to run the reports. For multiple groups, separate each group by a comma at the command line.
-ExistingSecurityDomain -esd	Required if you use LDAP authentication. Security domain to which the user or group belongs. Default is Native.
-Format -fm	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

getUserGroupAssociation

Gets list of users that belong to the group or a list of groups associated with specified users. You can select the users or groups for which you want to generate report.

Users with the administrator role can run this command.

The infacmd aud getUserGroupAssociation command uses the following syntax:

```
getUserGroupAssociation

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd aud getUserGroupAssociation options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
–Gateway –hp	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ExistingUserNames -eu	Required if you do not use -ExistingGroupNames (-eg). Name of the user or a list of users to run the reports. For multiple users, separate each user by a comma at the command line.
-ExistingGroupNames -eg	Required if you do not use -ExistingUserName (-eu). Name of the group or a list of groups to run the reports. For multiple groups, separate each group by a comma at the command line.
-ExistingSecurityDomain -esd	Required if you use LDAP authentication. Security domain to which the user or group belongs. Default is Native.

Option	Description
-Format -fm	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

getUserGroupAssociationForRoles

Gets list of roles assigned to users and groups. You can select the roles for which you want to generate report.

Users with the administrator role can run this command.

The infacmd aud getUserGroupAssociationForRoles command uses the following syntax:

```
getUserGroupAssociationForRoles

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleNames|-en> role_names
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd aud getUserGroupAssociationForRoles options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.

Option	Description
-Gateway -hp	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-RoleNames -en	Required. Name of the role assigned for users or groups in the domain for which you want to generate the report. For multiple roles, separate each role by a comma at the command line.
-Format -fm	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

getUsersPersonalInfo

Gets user information in the domain. The report displays the full name, security domain, description, contact details, and user status. If you run the report for users, the report displays the user information for the specified users. If you run the report for groups, the report organizes user information for all users in the specified group. The report displays nested groups separately.

Users with the administrator role can run this command.

The infacmd aud getUsersPersonalInfo command uses the following syntax:

```
getUsersPersonalInfo

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<<-ExistingUserNames|-eu> existing_user_names|
<-ExistingGroupNames|-eg> existing_group_names>
[<-ExistingSecurityDomain|-esd> existing_security_domain]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-lo> output_file_name]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd aud getUsersPersonalInfo options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-Gateway -hp	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain
-ExistingUserNames -eu	Required if you do not use -ExistingGroupNames (-eg). Name of the user or a list of users to run the reports. For multiple users, separate each user by a comma at the command line.
-ExistingGroupNames -eg	Required if you do not use -ExistingUserName (-eu). Name of the group or a list of groups to run the reports. For multiple groups, separate each group by a comma at the command line.
-ExistingSecurityDomain -esd	Required if you use LDAP authentication. Security domain to which the user or group belongs. Default is Native.
-Format -fm	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

CHAPTER 8

infacmd autotune Command Reference

This chapter includes the following topic:

Autotune

Configures services and connections with recommended settings based on the deployment type. Changes take effect after you recycle the services.

For each specified service, the changes to the service take effect on all nodes that are currently configured to run the service, and the changes affect all service processes.

The infacmd autotune Autotune command uses the following syntax:

```
Autotune

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Size|-s> tuning_size_name
[<-ServiceNames|-sn> service_names]
[<-BlazeConnectionNames|-bcn> connection_names]
[<-SparkConnectionNames|-scn> connection_names]
[<-All|-a> yes_or_no]
```

The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see more information about connecting to the domain, see the Command Reference.

The following table describes infacmd autotune Autotune options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.

Option	Description
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
-ResilienceTimeout -re	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-Size -s	Required. The deployment type that represents big data processing requirements based on concurrency and volume. You can enter Sandbox, Basic, Standard, or Advanced.
-ServiceNames -sn	Optional. List of services configured in the Informatica domain. Separate each service name with a comma. You can tune the following services: - Analyst Service - Content Management Service - Data Integration Service - Model Repository Service - Resource Manager Service - Search Service Default is none.
-BlazeConnectionNames -bcn	Optional. List of Hadoop connections configured in the Informatica domain. For each Hadoop connection, the command tunes Blaze configuration properties in the Hadoop connection. Separate each Hadoop connection name with a comma. Default is none.
-SparkConnectionNames -scn	Optional. List of Hadoop connections configured in the Informatica domain. For each Hadoop connection, the command tunes Spark configuration properties in the Hadoop connection. Separate each Hadoop connection name with a comma. Default is none.
-All -a	Optional. Enter `yes` to apply recommended settings to all Analyst Services, Content Management Services, Data Integration Services, Model Repository Services, Resource Manager Services, Search Services, and Hadoop connections in the Informatica domain. Enter `no` to apply the recommended settings only to the services and Hadoop connections that you specify. Default is `no`.

CHAPTER 9

Infacmd bg Command Reference

This chapter includes the following topics:

upgradeRepository

Upgrades the business glossary data in the Model repository. Run this command after you upgrade the domain and Model Repository Service.

The infacmd bg upgradeRepository command uses the following syntax:

```
upgradeRepository

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd bg upgradeRepository options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.

Option	Description
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
AtServiceName -atn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

deleteAuditHisotry

Deletes the audit history of a glossary from the Analyst tool.

The infacmd bg deleteAuditHistory command uses the following syntax:

```
deleteAuditHistory
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
<-GlossaryIdentity|-gi> Glossary_Identity
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd bg deleteAuditHistory options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.

Option	Description
AtServiceName -atn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
-GlossaryIdentity -gl	Required. The identity of the glossary for which you want to delete the audit history. You can obtain the glossary identity from the Model Repository Service database using the `select PSB_EXTERNID from PO_BGGLOSSARY where POB_NAME = '<glossary_name>'` option.

listGlossary

Displays a list of the business glossaries available in the Analyst tool as a standard output. Each glossary name is displayed as a separate line.

The infacmd bg listGlossary command uses the following syntax:

```
listGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd bg upgradeRepository options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	Name of the Informatica domain.
-Password -pd	Password for the user name.

Option	Description
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
AtServiceName -atn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

exportGlossary

Exports the business glossaries available in the Analyst tool. The Analyst tool exports business glossary data in the .xlsx or .zip format based on the options that you specify.

The infacmd bg exportGlossary command uses the following syntax:

```
exportGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-AtServiceName|-atn> Analyst_service_name
[<-GlossaryList|-gl> Glossary_list]
[<-Delimiter|-dl> Glossary_name_delimiter]
[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]
[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]
[<-IncludeAttachment|-att> Include_attachments_true_false]
[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
[<-ExportasPlainTextOnly|-ept> Export_richtext_as_plain_text_true_false]
[<-status|-s> Status_of_assets]
[<-phase|-p> Phase_of_assets]
<-ExportFilePath|-ep> Export_path
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd bg exportGlossary options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.

Option	Description
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
AtServiceName -atn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
-GlossaryList -gl	Optional. The names of one or more glossaries that you want to export and that you have access to, as determined by the permissions and privileges defined in the Analyst tool. Separate the names of multiple glossaries by the user defined delimiter character. If you do not specify the names of glossaries, the Analyst tool exports all the glossaries that you have permission to access as determined by the permissions and privileges defined in the Analyst tool.
-Delimiter -dl	Optional. Specify a custom delimiter if you are exporting multiple glossaries and one of them has a standard delimiter character as part of the glossary name. The standard delimiter is a comma. Define a custom delimiter of maximum one special character. Use the custom delimiter to separate the names of multiple glossaries.
-IncludeCrossGlossaryLinks -cgl	Optional. Enter one of the following values: - `True` to include cross glossary links in the export file. - `False` to skip cross glossary links in the export file. Default is true.
-IncludeAuditHistory -ah	Optional. Enter one of the following values: - `True` to include audit trail history in the export file. - `False` to skip the audit trail history in the export file. Default is false. **Note:** If you specify the include audit history (-ah) option as true, the business glossary data is exported in a .zip format.
-IncludeAttachments -att	Optional. Enter one of the following values: - `True` to include attachments in the export file. - Specify `False` to skip attachments in the export file. Default is false. **Note:** If you specify the include attachments (-att) option as true, the business glossary data is exported in a .zip format.
-IncludeOnlyTemplates -tem	Optional. Enter one of the following values: - `True` to include only templates in the export file. - `False` to include both templates and glossary data in the export file. Default is false.
-ExportasPlainTextOnly -ept	Optional. Enter one of the following values: - `True` to export formatted rich text content as plain text. - `False` to export formatted rich text content as rich text. Default is false.

Option	Description
-status -s	Optional. Enter one or all of the following values, separated by a comma: - `Active` to export assets that are active. - `Inactive` to export assets that are inactive. The Analyst tool exports assets that are both active and inactive if you do not specify any value.
-phase -p	Optional. Enter one or all of the following values, separated by a comma: - `Draft` to export assets that are in the draft phase. - `In_Review` to export assets that are in the In Review phase. - `Published` to export assets that are in the Published phase. - `Rejected` to export assets that are in the Rejected phase. - `Pending_publish` to export assets that are in the Pending Publish phase. The Analyst tool exports assets that are in all phases if you do not specify any value.
-ExportFilePath -ep	Required. Specify the path where the command line program must store the exported files.

importGlossary

Imports business glossaries from .xlsx or .zip files that were exported from the Analyst tool.

The infacmd bg importGlossary command uses the following syntax:

```
importGlossary

<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
 <-AtServiceName|-atn> Analyst_service_name
[<-GlossaryList|-gl> Glossary_list]
[<-Delimiter|-dl> Glossary_name_delimiter]
[<-IncludeCrossGlossaryLinks|-cgl> Include_cross_glossary_links_true_false]
[<-IncludeAuditHistory|-ah> Include_audit_history_true_false]
[<-IncludeAttachment|-att> Include_attachments_true_false]
[<-IncludeOnlyTemplate|-tem> Include_templates_only_true_false]
[<-IncludeRichTextContentforConflictingAssets|-irt>
Include_richtextcontent_conflicting_assets_true_false]
<-ImportFilePath|-ip> Import_path
[<-ResolutionOnMatchByName|-rmn> Copy_or_replace_or_skip_assets_by_name]
[<-ResolutionOnMatchById|-rmi> Copy_or_replace_or_skip_assets_by_id]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes infacmd bg importGlossary options and arguments:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain.
-Password -pd	Password for the user name.
-SecurityDomain -sdn	Name of the security domain to which the domain user belongs.
AtServiceName -atn	Required. Name of the Analyst Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
GlossaryList -gl	Optional. The names of one or more glossaries that you want to import, and that you have access to as determined by the permissions and privileges defined in the Analyst tool. The glossaries must be present in the .xlsx file. Separate the names of multiple glossaries by the user defined delimiter character. If you do not specify the names of glossaries, the Analyst tool imports all the glossaries that you have permission to access as determined by the permissions and privileges defined in the Analyst tool.
-Delimiter -dl	Optional. Specify a custom delimiter if you are importing multiple glossaries and one of them has a standard delimiter character as part of the glossary name. The standard delimiter is a comma. Define a custom delimiter of maximum one special character. Use the custom delimiter to separate the names of multiple glossaries.
IncludeCrossGlossaryLinks -cgl	Optional. Enter one of the following values: - `True` to import cross glossary links from the export file. - `False` to skip the import of cross glossary links from the export file. Default is true.
-IncludeAuditHistory -ah	Optional. Enter one of the following values: - `True` to import audit trail history from the export file. - `False` to skip the import of the audit trail history from the export file. Default is false.
-IncludeAttachments -att	Optional. Enter one of the following values: - `True` to include attachments when importing business glossaries. - `False` to include both templates and glossary data when importing business glossaries Default is true.

Option	Description
-IncludeOnlyTemplates -tem	Required. Enter one of the following values: - `True` to include only templates when importing business glossaries. - `False` to include both templates and glossary data when importing business glossaries. Default is false.
-IncludeRichTextContentforConflictingAssets -irt	Optional. Enter one of the following values: - `True` when you want to import rich text content for conflicting assets. - `False` when you do not want to import rich text content for conflicting assets. Default is true.
-ImportFilePath -ip	Required. Specify the path and filename where the import file is available.
-ResolutionOnMatchByName -rmn	Optional. Enter one of the following values: - `Copy` to copy all assets when there is a conflict based on the name. - `Replace` to replace all assets when there is a conflict based on the name. This is the default value. - `Skip` to skip all assets when there is a conflict based on the name.
-ResolutionOnMatchById -rmi	Optional. Enter one of the following values: - `Copy` to copy all assets when there is a conflict based on the asset ID. - `Replace` to replace all assets when there is a conflict based on the asset ID. This is the default value. - `Skip` to skip all assets when there is a conflict based on the asset ID.

CHAPTER 10

infacmd ccps Command Reference

This chapter includes the following topics:

deleteClusters

Deletes clusters created by the cluster workflow from the cloud platform.

The infacmd ccps deleteClusters command uses the following syntax:

```
deleteClusters
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
<-ClusterIDs|-cids> cluster_ids
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: When you use this command to delete clusters on the Azure cloud platform, the process blocks any other command through the command shell until the Azure cloud platform completes the process to release cluster resources. This process could take several minutes. If you try to kill the command using CTRL-C, and then re-run the command, the same time delay and block apply.

The following table describes infacmd ccps deleteClusters options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Required. ID of the cloud provisioning configuration.
-ClusterIDs -cids	cluster_ids	Required. Comma-separated list of clusters to delete. The cluster ID is the same as the cluster ID listed on the cloud platform site.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-DeleteConnections -dc	delete_associated_connection	Optional. Deletes the connections that the cluster configuration created. Use one of the following values: - TRUE - FALSE Default is FALSE.

listClusters

Lists clusters that the cluster workflow creates and that exist on the cloud platform.

The infacmd ccps listClusters command uses the following syntax:

```
listClusters
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ccps listClusters options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Required. ID of the cloud provisioning configuration.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

updateADLSCertificate

Updates the Azure Data Lake Service Principal certificate path in a cloud provisioning configuration.

The infacmd ccps updateADLSCertificate command uses the following syntax:

```
updateADLSCertificate
    <-DomainName|-dn> domain_name
    <-UserName|-un> user_name
    <-Password|-pd> password
    <-CloudProvisioningConfigurationID|-cpcid> cloud_provisioning_configuration_id
    <-CertificateFilePath|-certPath> certificate_file_path
    [<-SecurityDomain|-sdn> security_domain]
    [<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ccps updateADLSCertificate options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-CloudProvisioningConfigurationID -cpcid	cloud_provisioning_configuration_id	Required. ID of the cloud provisioning configuration to update with the certificate file path.
-CertificateFilePath -certPath	certificate_file_path	Required. Path to the ADLS Service Principal certificate on the Data Integration Service machine.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

CHAPTER 11

infacmd cluster Command Reference

This chapter includes the following topics:

createConfiguration

Imports cluster information directly from a cluster or from a cluster archive file.

The cluster configuration is an object in the domain that contains configuration information about the compute cluster.

The infacmd cluster createConfiguration command uses the following syntax:

```
createConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
```

```
[<-DistributionType|-dt> CDH|EMR|HDI|HDP|MAPR|DATAPROC|DATABRICKS]
[<-DistributionVersion|-dv> distribution_version]
[<-ClusterManagerUri|-uri> cluster_manager_uri]
[<-ClusterManagerUser|-cmu> cluster_manager_user]
[<-ClusterManagerPassword|-cmp> cluster_manager_password]
[<-ClusterName|-cln> cluster_name]
[<-FilePath|-path> file_path]
[<-createConnections|-cc> true|false]
```

The following table describes infacmd cluster createConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication or if you import properties directly from the cluster. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConfigurationName -cn	Name of the cluster configuration	Required. The cluster configuration name must meet the following requirements: - Unique within the domain - Cannot exceed 128 characters - Cannot contain white spaces or the following special characters: - ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? / Values are not case sensitive.
-DistributionType -distType	Distribution	Required. One of the following distribution types: - CDH. Cloudera CDH or Cloudera CDP. - EMR. Amazon EMR. - HDI. Azure HDInsight. - HDP. Hortonworks HDP. - MAPR - DATAPROC - DATABRICKS Values are not case sensitive.
-DistributionVersion -dv	Distribution version	Optional. Specify a distribution version other than the default version. Each distribution has a default version. Use the -dv option to specify a different supported version to apply to the cluster configuration. Default is the most recent distribution version that Data Engineering supports.
-ClusterManagerUri -uri	Cluster manager URI	Required to import directly from the cluster. URI of the cluster configuration web interface.
-ClusterManagerUser -cmu	Cluster Manager user	Required to import directly from the cluster. User name of the account to log in to the cluster configuration web interface.
-ClusterManagerPassword -cmp	Cluster Manager password	Required to import directly from the cluster. Password of the account to log in to the cluster configuration web interface.
-ClusterName -cln	Cluster name	Required if the cluster manager manages multiple clusters. If you do not provide a cluster name, the wizard imports information based on the default cluster.
-FilePath -path	Path and filename to the location of the archive file.	Required to import cluster information from a file. Path and file name of the archive file that contains cluster information.
-createConnections -cc	true|false	Optional. Indicates whether to create connections associated with the cluster configuration. Default is false.

createConfigurationWithParams

Creates a cluster configuration through cluster parameters that you specify in the command line.

The cluster configuration is an object in the domain that contains configuration information about the compute cluster.

The infacmd cluster createConfigurationWithParams command uses the following syntax:

```
createConfigurationWithParams
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-DistributionType|-dt> CDH|EMR|HDI|HDP|MAPR|DATAPROC|DATABRICKS
[<-DistributionVersion|-dv> distribution_version]
<-Parameters|-params> parameters, separated by space in the form of name=value.
Use single quote to escape any equal sign or space in the value.
```

The following table describes infacmd cluster createConfigurationWithParams options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication or if you import properties directly from the cluster. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. The cluster configuration name must meet the following requirements: - Unique within the domain - Cannot exceed 128 characters - Cannot contain white spaces or the following special characters: - ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? / Values are not case sensitive.
-DistributionType -distType	Distribution	Required. One of the following distribution types: - CDH. Cloudera CDH or Cloudera CDP. - EMR. Amazon EMR. - HDI. Azure HDInsight. - HDP. Hortonworks HDP. - MAPR - DATAPROC - DATABRICKS Values are not case sensitive.

Option	Argument	Description
-DistributionVersion -dv	Distribution version	Optional. Specify a distribution version other than the default version. Each distribution has a default version. Use the -dv option to specify a different supported version to apply to the cluster configuration. Default is the most recent distribution version that Big Data Management supports.

-Parameters
-params
	Parameters	Separated by space in the form of name=value. Use single quote to escape any equal sign or space in the value.
		You can use the following parameters for each distribution :
		- Databricks:
		  - url
		  - accesstoken
		  - clusterid
		- All other distribution types:
		  - host
		  - port
		  - username
		  - password
		  - clustername

deleteConfiguration

Deletes a cluster configuration from the domain.

You cannot delete a cluster configuration that is used by any connection object.

The infacmd cluster deleteConfiguration command uses the following syntax:

```
deleteConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-DeleteConnections|-dc> delete_associated_connections]
```

The following table describes infacmd cluster deleteConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-DeleteConnections -dc	delete_associated_connection	Optional. Set to TRUE to delete all of the connections that are associated with the cluster configuration. Default is FALSE.

clearConfigurationProperties

Clears overridden property values in the cluster configuration set.

The command clears overridden values of imported properties and restores the value that was imported. The command deletes user-defined properties from a configuration set. To delete an imported property, use the -del option.

Note: When you delete an imported property, the refresh operation restores the property if it exists on the cluster.

For example, the following command deletes the user-defined properties "foo.bar" and "biz.baz" from the core-site.xml set of the CDH1 cluster configuration:

```
infacmd cluster clearConfigurationProperties -cn CDH1 -cs core-site.xml -pn foo.bar
biz.baz
```

The infacmd cluster clearConfigurationProperties command uses the following syntax:

```
clearConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration name
<-ConfigurationSet|-cs> configuration set
<-PropertyNames|-pn> list of property names separated by space
[<-DeleteProperties|-del> delete_properties]
```

The following table describes infacmd cluster clearConfigurationProperties options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-ConfigurationSet -cs	Configuration set	Name of the configuration set. Enter the xml configuration file name. For example, hdfs-site.xml. When you enter an .xml file name, the command returns the properties and values in that configuration set.
-PropertyNames -pn	property_name	Properties to run the command against. When you include an imported property, the command clears an override value. When you include a user-defined property, the command deletes the property. To edit more than one property, separate property names with spaces. When the property is not a user-defined property, use the -del option.
-DeleteProperties -del	delete_properties	Optional. When you set the option to TRUE, deletes an imported property. Default is FALSE.

exportConfiguration

Exports a cluster configuration to an archive file containing .xml files or a combined .xml file.

Export the properties that a cluster configuration object contains to a compressed file in a path that you specify.
When you export the cluster configuration file, you create a .zip archive.

The infacmd cluster exportConfiguration command uses the following syntax:

```
exportConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-FilePath|-path> file_path
[<-IncludeSensitive|-is> include_sensitive_properties]
```

The following table describes infacmd cluster exportConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-FilePath -path	Path and file name to the location of the file to create.	Required. Path and file name of the compressed file to be created as an archive of the cluster configuration. You can specify an absolute path or a relative path to the file name. Include a `.zip` or `.tar` suffix.
-IncludeSensitive -is	include_sensitive_properties	Optional. Set to TRUE to export sensitive properties. You must have write permission on the cluster configuration to include them in the export. Default is FALSE.

listAssociatedConnections

Lists connections by type that are associated with the specified cluster configuration.

The command lists results by connection type.

The infacmd cluster listAssociatedConnections command uses the following syntax:

```
listAssociatedConnections
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
```

The following table describes infacmd cluster listAssociatedConnections options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.

listConfigurationGroupPermissions

Lists the permissions that a group has for a cluster configuration.

Command output includes group permissons and the security domain that the group is a member of.

The infacmd cluster listConfigurationGroupPermissions command uses the following syntax:

```
listConfigurationGroupPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-Direct> direct]
[<-GroupFilter|-groups> group_filter]
```

The following table describes infacmd cluster listConfigurationGroupPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.

Option	Argument	Description
-Direct	Whether to list direct or effective permissons.	Optional. Determines whether you list permissions that the administrator has directly granted to the cluster configuration. Specify one of these values: - Direct. The permissions that the administrator directly granted to the group. - Effective. All of the permissions that the group has, including direct and inherited permissions. Default is effective.
GroupFilter -groups	Group filter	Optional. List the group or groups to show results for. If you do not specify a group, the command displays results for all groups by default. Separate group names with spaces.

listConfigurationSets

Lists the configuration sets that a cluster configuration contains.

The infacmd cluster listConfigurationSets command uses the following syntax:

```
listConfigurationSets
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
```

The following table describes infacmd cluster listConfigurationSets options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.

listConfigurationProperties

Lists properties and active values for a configuration set.

The infacmd cluster listConfigurationProperties command uses the following syntax:

```
listConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-ConfigurationSet|-cs> configuration_set
```

The following table describes infacmd cluster listConfigurationProperties options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.

-ConfigurationSet
-cs
	configuration set	Name of the configuration set.
		Enter one of the following configuration set options:
		- general. When you enter this option, the command returns the property values under the General category of cluster configuration options:
		  - Description
		  - Distribution type
		  - Distribution version
		  - Last refreshed time
		- .xml configuration file name. For example, hdfs-site.xml. When you enter an .xml file name, the command returns the properties and values in that configuration set.

listConfigurations

Lists the cluster configurations in the domain.

The infacmd cluster listConfigurations command uses the following syntax:

```
listConfigurations
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cluster listConfigurations options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

listConfigurationUserPermissions

Lists the permissions that a user has for a cluster configuration.

The infacmd cluster listConfigurationUserPermissions command uses the following syntax:

```
listConfigurationUserPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-Direct> direct]
[<-UserFilter|-users> user_filter]
```

The following table describes infacmd cluster listConfigurationUserPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.

Option	Argument	Description
-Direct	Whether to list direct or effective permissons.	Optional. Determines whether you list permissions that the administrator has directly granted to the cluster configuration. Specify one of these values: - Direct. The permissions that the administrator directly granted to the group. - Effective. All of the permissions that the group has, including direct and inherited permissions. Default is effective.
UserFilter -users	user_filter	Optional. List the user or users to show results for. If you do not specify a user, the command displays results for all users by default. Values are not case sensitive.

refreshConfiguration

Refreshes a cluster configuration from a cluster archive file or from a remote cluster manager. Changes take effect after you restart the Data Integration Service.

Updates the cluster configuration properties from a cluster or from a cluster archive file. The refreshConfiguration command updates the configuration values that you imported. It does not affect the overrides that you configured.

The infacmd cluster refreshConfiguration command uses the following syntax:

```
refreshConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
[<-ClusterManagerUri|-uri> cluster_manager_uri]
[<-ClusterManagerUser|-cmu> cluster_manager_user]
[<-ClusterManagerPassword|-cmp> cluster_manager_password]
[<-ClusterManagerName|-cmn> cluster_name]
[<-FilePath|-path> file_path]
```

The following table describes infacmd cluster refreshConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-ClusterManagerUri -uri	Cluster manager URI	Required to import directly from the cluster. URI of the cluster configuration web interface.
-ClusterManagerUser -cmu	Cluster Manager user	Required to import directly from the cluster. User name of the account to log in to the cluster configuration web interface.

Option	Argument	Description
-ClusterManagerPassword -cmp	Cluster Manager password	Required to import directly from the cluster. Password of the account to log in to the cluster configuration web interface.
-ClusterName -cln	Cluster name	Required if the cluster manager manages multiple clusters. If you do not provide a cluster name, the wizard imports information based on the default cluster.
-FilePath -path	Path and filename to the location of the archive file.	Required to import cluster information from a file. Path and file name of the archive file that contains cluster *-site.xml configuration files.

setConfigurationPermissions

Sets permissions on cluster configuration to a user or a group after removing previous permissions.

Allows you to add, change or delete cluster configuration permissions for a user or a group. Removes previous permissions on the user or group.

Use either the `-RecipientUserName` or the `-RecipientGroupName` option.

You can grant multiple permissions from the following set in a single command: READ, WRITE, EXECUTE, GRANT. You can grant only ALL or NONE separately.

The infacmd cluster setConfigurationPermissions command uses the following syntax:

```
setConfigurationPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<<-RecipientUserName|-run> recipient_user_name | <-RecipientGroupName|-rgn>
recipient_group_name>>
[<-RecipientSecurityDomain|-rsd> recipient_security_domain]
<-Permissions|-p> READ_WRITE_EXECUTE_GRANT|ALL|NONE
```

The following table describes infacmd cluster setConfigurationPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-RecipientUserName -run	recipient_user_name	Required if you do not use the RecipientGroupName option. Name of the user to grant permission to.
-RecipientGroupName -rgn	recipient_group_name	Required if you do not use the RecipientUserName option. Name of the group to grant permission to.

Option	Argument	Description
-RecipientSecurityDomain -rsd	recipient_security_domain	Security domain that the user or group is a member of.
-Permissions -p	READ | WRITE | EXECUTE | GRANT ALL NONE	Permission or permissions to grant. To enter more than one permission, separate permissions with a space.

setConfigurationProperties

Adds user-defined properties or overrides imported property values.

The infacmd cluster setConfigurationProperties command uses the following syntax:

```
setConfigurationProperties
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-ConfigurationSet|-cs> configuration_set
<-UserProperties|-up> user_properties_separated_by_&:
```

The following table describes infacmd cluster setConfigurationProperties options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-ConfigurationSet -cs	configuration set	Name of the configuration set. Enter the xml configuration file name. For example, hdfs-site.xml. When you enter an .xml file name, the command returns the properties and values in that configuration set.
-UserProperties -up	User properties to set	Property name-value pairs. Use the equals (=) character to delimit property-value pairs. Use the characters `&:` to separate each pair.

-UserProperties Examples

The following examples show how to add a single user property, multiple property-value pairs, or how to overwrite a user property:

Add a single user property

To add a single user property, use the equals (=) character to delimit property-value pairs. For example, the following command adds the property foo.bar to the core-site.xml namespace of the cluster configuration, and assigns foo.bar a value of 1:

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up 'foo.bar=1'
```

Add multiple property-value pairs

Use the equals (=) character to delimit property-value pairs, and use `&:` to separate pairs. For example, the following command adds the property foo.bar to the core-site.xml namespace of the cluster configuration and assigns foo.bar a value of 1. It then adds the property start.interval to the same namespace and assigns start.interval a value of 5:

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up
'foo.bar=1&:start.interval=5'
```

Overwrite a user property

To overwrite the value of a user property, specify the property-value pair with another value. For example, the following command edits the existing property fs.trash.interval in the core-site.xml namespace of the cluster configuration. The command overrides the existing value and assigns a value of 2:

```
infacmd cluster setConfigurationProperties -cn cdh -cs core-site.xml -up
'fs.trash.interval=2'
```

updateConfiguration

Updates the Hadoop distribution version of a cluster configuration.

Use the -dv option to change the distribution version of the Hadoop distribution of a cluster configuration.

The infacmd cluster updateConfiguration command uses the following syntax:

```
updateConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConfigurationName|-cn> configuration_name
<-DistributionVersion|-dv> distribution_version
```

The following table describes infacmd cluster updateConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConfigurationName -cn	Name of the cluster configuration	Required. Name of the cluster configuration on the domain. Values are not case sensitive.
-DistributionVersion -dv	Distribution version to change to.	Required. Specify a different distribution version for a cluster configuration. For example, if the default supported version of the Hadoop distribution is 5.13 but the cluster is version 5.12, specify 5.12.

CHAPTER 12

infacmd cms Command Reference

This chapter includes the following topics:

CreateAuditTables

Creates audit tables that contain audit trail log events for reference tables managed by the specified Content Management Service.

The infacmd cms CreateAuditTables command uses the following syntax:

```
CreateAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cms CreateAuditTables options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence..
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CreateService

Creates a Content Management Service in a domain.

The infacmd cms CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-DataServer|-ds> data_service_name
<-RepositoryService|-rs> repository_service_name
<-RepositoryUsername|-rsu> repository_user_name
<-RepositoryPassword|-rsp> repository_password
[<-RepositorySecurityDomain|-rssd> repository_security_domain]
<-ReferenceDataLocation|-rdl> reference_data_location
[<-HttpPort> http_port]
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
```

The following table describes infacmd cms CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 128 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-NodeName -nn	node_name	Required. Name of the node where the Content Management Service will run.
-DataServer -ds	data_service_name	Required. Data Integration Service name associated with the Content Management Service.
-RepositoryService -rs	repository_service_name	Required. Model Repository Service to associate with the Content Management Service.

Option	Argument	Description
-RepositoryUsername -rsu	repository_user_name	Required. User name to connect to the Model Repository Service. To perform reference table management tasks in the Model repository, the user identified in the property must have the Model Repository Service Administrator role. The reference table management tasks include purge operations on orphaned reference tables.
-RepositoryPassword -rsp	repository_password	Required. Password to connect to the Model Repository Service.
-RepositorySecurityDomain -rssd	repository_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Security domain is case sensitive. Default is Native.
-ReferenceDataLocation -rdl	reference_data_location	Required. Connection name for the database that stores data values for the reference tables defined in the Model repository. The specified database stores reference data values. The Model repository stores metadata for the reference tables.
-HttpPort	http_port	Required. Unique HTTP port number for the Content Management Service.
-HttpsPort	https_port	Optional. HTTPS port number that the service runs on when you enable the Transport Layer Security (TLS) protocol.
-KeystoreFile -kf	keystore_file_location	Path and file name of the keystore file that contains the keys and certificates required if you enable TLS and use the HTTPS protocol for the service.
-KeystorePassword> -kp	keystore_password	Required if you enable TLS and use HTTPS connections for the service. A plain-text password for the keystore file.

DeleteAuditTables

Deletes the audit trail tables for the specified Content Management Service.

The infacmd cms DeleteAuditTables command uses the following syntax:

```
DeleteAuditTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cms DeleteAuditTables options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence..
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceOptions

Lists the options for a Content Management Service.

The infacmd cms ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cms ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence..

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists the options for a Content Management Service process.

The infacmd cms ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes cms ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
NodeName -nn	node_name	Required. Name of the node where the service process runs.

Purge

Deletes from the reference data warehouse any reference table that is no longer associated with a reference table object in the Model repository.

When you run infacmd cms Purge, the Content Management Service identifies the tables that store data for reference table objects in the associated Model repository. The Content Management Service deletes all other tables from the warehouse and generates a list of the deleted tables. Run infacmd cms Purge on the master Content Management Service for the Model repository.

Note: To prevent accidental data loss, the purge operation does not delete tables if the Model repository does not contain a reference table object.

Before you run infacmd cms Purge, verify the following prerequisites:

- The user name that you specify in the command has the Manage Service privilege on the domain.
- The Model repository user that the Content Management Service specifies has the Administrator role on the Model Repository Service.
- All Data Integration Services associated with the Model repository are available.
- There are no data operations in progress on the reference data warehouse.
- The reference data warehouse stores data for the reference table objects in a single Model repository.

The infacmd cms Purge command uses the following syntax:

```
Purge
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cms Purge options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 128 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.

RemoveService

Removes the Content Management Service from the domain. Before you remove the service, you must disable it.

The infacmd cms RemoveService command uses the following syntax:

```
RemoveService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd cms RemoveService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to remove. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ResyncData

Synchronizes probabilistic model files or classifier model files between a specified Content Management Service machine and the master Content Management Service machine in the domain. The ResyncData command updates the files on the Content Management Service machine that you specify with the files from the master Content Management Service machine.

The command synchronizes any file saved on the master Content Management Service machine after a time and date that you specify. You run the ResyncData command for a single type of model file. To synchronize probabilistic model files and classifier model files, you must run the command twice.

When you run infacmd cms ResyncData, you must have access permissions on both Content Management Service machines. Informatica Administrator sets the access permissions on the services.

The infacmd cms ResyncData command uses the following syntax:

```
ResyncData

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Type|-t> type

<-StartTime|-st> start_time
```

The following table describes infacmd cms resyncData options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service. The command copies files to the machine that hosts the service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence .
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Type -t	type	Required. Identifies the type of data file to copy from the master Content Management Service machine. Enter one of the following options: - NER. Specifies probabilistic model data files. - Classifier. Specifies classifier model data files.
-StartTime -st	start_time	Required. Identifies the files to copy from the master Content Management Service machine to the Content Management Service machine that you specify in the ServiceName property. The command does not copy any file with a time stamp earlier than the StartTime value. The command uses the system clock on the master Content Management Service machine to determine the time. Enter the date in the default locale format.

UpdateServiceOptions

Updates the Content Management Service with options that are introduced in the current release. To view current options, run the infacmd cms ListServiceOptions command.

The infacmd cms UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

The following table describes infacmd cms UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter each option and value to update. Separate each option by a space. To view application options, run the infacmd cms ListServiceOptions command.

Username and Password Options

You can use the UpdateServiceOptions -o option to update the user name and password that the Content Management Service uses to connect to the Model Repository Service.
Use the DataServiceOptions.RepositoryUsername and DataServiceOptions.RepositoryPassword options to update the user name and password values. You can also set the options in Informatica Administrator.

Reference Data Options

You can use the UpdateServiceOptions -o option to update the following directory and database settings for reference data:

- Use the FileTransferOptions.TempLocation option to identify the reference data staging directory. The Content Management Service uses the directory to stage data that it adds to a reference table.
- Use the DataServiceOptions.ReferenceDataLocation option to identify the connection to the reference data database. The reference data database stores the values for the reference tables that you can select in the Model repository.
- Use the DataServiceOptions.RefDataLocationSchema option to specify the schema that identifies the reference data tables in the reference data database.

  If you do not specify a reference table schema on the Content Management Service, the service uses the schema that the database connection specifies. If you do not specify a schema on the Content Management Service or on the database connection, the service uses the default database schema.

You can also set the options in Informatica Administrator.

Note: Establish the database and the schema that the Content Management Service will use for reference data before you create a managed reference table.

UpdateServiceProcessOptions

Updates options for a Content Management Service process. To view current options, run the infacmd cms ListServiceProcessOptions command.

The infacmd cms UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

The following table describes infacmd cms UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
NodeName -nn	node_name	Required. Name of the node where the service process runs.
-Options -o	options	Required. Enter each option and value to update. Separate each option by a space. To view application options, run the infacmd cms ListServiceProcessOptions command.

Identity Match Analysis Options

You can use the UpdateServiceProcessOptions -o option to update the following properties for identity match analysis:

- IdentityOptions.IdentityReferenceDataLocation. Specifies the location of identity population files.
- IdentityOptions.IdentityCacheDir. Specifies the location of the cache directory used in identity match analysis.
- IdentityOptions.IdentityIndexDir. Specifies the location of the index key directory used in identity match analysis.

You can also set the properties in Informatica Administrator.

Upgrade

Upgrades the Content Management Service configuration. Run infacmd cms Upgrade when you upgrade to the current version of Informatica Data Quality.

The infacmd cms Upgrade command uses the following syntax:

```
Upgrade

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The infacmd cms Upgrade command checks the service configuration on the domain and verifies the following service options:

Master Content Management Service

The Upgrade command verifies that the Model repository in the domain uses a master Content Management Service. If the Model Repository Service does not specify a master Content Management Service, the Upgrade command sets the current service as the master Content Management Service . By default, the first Content Management Service to connect to a Model Repository Service becomes the master Content Management Service.

Model Repository Service

The Upgrade command uses the Data Integration Service associated with the Content Management Service to identify the Model Repository Service in the domain.

The Upgrade command verifies that the Content Management Service has a valid username, password, and security domain to connect to the Model Repository Service. If these options are not set, the Upgrade command uses the username, password, and security domain values on the associated Data Integration Service to connect to the Model Repository Service.

Reference Data Location

The Upgrade command verifies that the Content Management Service specifies a reference data location. If the service does not specify a reference data location, the Upgrade command sets the location to the staging database defined on the Analyst Service.

The following table describes infacmd cms Upgrade options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Content Management Service.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence..
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CHAPTER 13

infacmd dis Command Reference

This chapter includes the following topics:

AddParameterSetEntries

Adds entries to a parameter set. Run this command to add parameters from a mapping or workflow that has been deployed as an application.

The infacmd dis AddParameterSetEntries command uses the following syntax:

```
AddParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
```

```
<-paramNameValues|-pnv> parameter name-value pairs, separated by space
```

The following table describes infacmd dis AddParameterSetEntries options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application that contains the parameter set.
parametersetname - ps	parameterset name	Required. Parameter set name.

Option	Argument	Description
-projectScope -prs	project scope	Required. Path to the mapping or workflow that contains the parameters. For a mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
-paramNames -pnv	parameter names	Required. Parameter name-value pairs separated by space. Enclose name-value pairs in double quotes. Enclose each value in single quotes. Use the following syntax: `"parm1='valueA'" "parm2='valueB'" "parm3='valueC"` . You can include spaces in a parameter value. You can include an apostrophe (') or a colon (:) in the value if you escape the character with a backslash (\). `'C:\directory'`

BackupApplication

Backs up a deployed application from a Data Integration Service to an XML file.

The backup file contains all the properties settings for the application. You can restore the application to another Data Integration Service. You must stop the application before you back it up.

The infacmd dis BackupApplication command uses the following syntax:

```
BackupApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-FileName|-f> file_name
```

The following table describes infacmd dis BackupApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application to back up.
Filename -f	file_name	Required. Name and file path of the application backup file.

CancelDataObjectCacheRefresh

Stops the last request to refresh the logical data object cache. If the cache mapping is running, the command stops the current request to refresh the logical data object cache. Future periodic requests to refresh the logical data object cache are not affected.

The infacmd dis CancelDataObjectCacheRefresh command uses the following syntax:

```
CancelDataObjectCacheRefresh
<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object
```

The following table describes infacmd dis CancelDataObjectCacheRefresh options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
Application -a	application	Required. Name of the application.
-Folder -f	folder	Folder in the application that contains the data object.
-DataObject -do	data_model.data_object	Required. Name of the logical data object. The name must be in the following syntax: `<data_model>.<data_object>`

CreateService

Creates a Data Integration Service. By default, the Data Integration Service is enabled when you create it.

The infacmd dis CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name | <-GridName|-gn> grid_name
[<-BackupNodes|-bn> node_name1,node_name2,...]
<-RepositoryService|-rs> model_repository_service_name
<-RepositoryUserName|-rsun> model_repository_user_name
<-RepositoryPassword|-rspd> model_repository_password
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
[<-HttpPort> http_port]
```

```
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-httpProtocolType|-pt> http_protocol_type]
```

The following table describes infacmd dis CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the Data Integration Service runs. You can run the Data Integration Service on a node or grid.
-GridName -gn	grid_name	Required if you do not specify node name. Grid where the Data Integration Service runs. You can run the Data Integration Service on a node or grid.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-RepositoryService -rs	model_repository_service_name	Model Repository Service that stores run-time metadata required to run the mappings and SQL data services.
-RepositoryUserName -rsun	model_repository_user_name	User name to access the Model Repository Service.
-RepositoryPassword -rspd	model_repository_password	User password to access the Model Repository Service.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Required if you use LDAP authentication. Name of the security domain that the Model repository user belongs to.
-HttpPort	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each Data Integration Service process. Default is 8095.
-HttpsPort	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each Data Integration Service process.
-KeystoreFile -kf	keystore_file_location	Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the Data Integration Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority. If you run the Data Integration Service on a grid, the keystore file on each node in the grid must contain the same keys.

Option	Argument	Description
-KeystorePassword -kp	keystore_password	Password for the keystore file.
-httpProtocolType -pt	http_protocol_type	Security protocol that the Data Integration Service uses. Enter one of the following values: - HTTP. Requests to the service must use an HTTP URL. - HTTPS. Requests to the service must use an HTTPS URL. - Both. Requests to the service can use either an HTTP or an HTTPS URL. When you set the HTTP protocol type to HTTPS or Both, you enable Transport Layer Security (TLS) for the service. You can also enable TLS for each web service deployed to an application. When you enable HTTPS for the Data Integration Service and enable TLS for the web service, the web service uses an HTTPS URL. When you enable HTTPS for the Data Integration Service and do not enable TLS for the web service, the web service can use an HTTP URL or an HTTPS URL. If you enable TLS for a web service and do not enable HTTPS for the Data Integration Service, the web service does not start. Default is HTTP.

compareObject

Compares two queried objects.

Query the objects to compare object properties, transformation properties, and ports within transformations between Data Integration Service and Model Repository Service. You can compare objects in the following ways:

- Design-time to design-time within a domain
- Design-time to run-time within a domain
- Run-time to run-time within a domain
- Design-time to design-time across domains
- Run-time to run-time across domains

To query design-time objects, specify the Model Repository Service. To query run-time objects, specify a Data Integration Service. If you do not specify a service, the API runs the query against the run-time objects on the Data Integration Service that hosts the API.

The `infacmd dis compareObject` command uses the following syntax:

```
compareObject
<-DomainName|-dn> domain_name
<-ServiceName|-sn> DIS_service_name
<-UserName|-un> DIS_user_name
<-Password|-pd> DIS_password
[<-SecurityDomain|-sdn> DIS_security_domain]
```

```
[<-sourceDomainName|-srcdn> source_domain_name]
[<-sourceRepositoryService|-srcrs> source_MRS_name]
[<-sourceDataIntegrationService|-srcdis> source_DIS_name]
[<-sourceRepositoryUserName|-srcrsun> source_MRS_user_name]
[<-sourceRepositoryPassword|-srcrspd> source_MRS_password]
[<-sourceRepositorySecurityDomain|-srcrssdn> source_MRS_security_domain]
<-sourceQuery|-srcq> source_query
[<-targetDomainName|-tgtdn> target_domain_name]
[<-targetRepositoryService|-tgtrs> target_MRS_name]
[<-targetDataIntegrationService|-tgtdis> target_DIS_name]
[<-targetRepositoryUserName|-tgtrsun> target_MRS_user_name]
[<-targetRepositoryPassword|-tgtrspd> target_MRS_password]
[<-targetRepositorySecurityDomain|-tgtrssdn> target_MRS_security_domain]
<-targetQuery|-tgtq> target_query
[<-TimeZone|-tz> time_zone]
```

The following table describes `infacmd dis compareObject` options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the `-dn` option or the environment variable `INFA_DEFAULT_DOMAIN`. If you set a domain name with both methods, the `-dn` option takes precedence.
-ServiceName -sn	DIS_service_name	Required. Name of the Data Integration Service.
-UserName -un	DIS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the `-un` option or the environment variable `INFA_DEFAULT_DOMAIN_USER`. If you set a user name with both methods, the `-un` option takes precedence.
-Password -pd	DIS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the `-pd` option or the environment variable `INFA_DEFAULT_DOMAIN_PASSWORD`. If you set a password with both methods, the password set with the `-pd` option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	DIS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the `-sdn` option or the environment variable `INFA_DEFAULT_SECURITY_DOMAIN`. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-sourceDomainName -srcdn	source_domain_name	Required. Name of the domain for the source object.
-sourceRepositoryService -srcrs	source_MRS_name	Optional. Name of the Model Repository Service for the source object.
-sourceDataIntegrationService -srcdis	source_DIS_name	Optional. Name of the Data Integration Service for the source object.
-sourceRepositoryUserName -srcrsun	source_MRS_user_name	Optional. The user name for the Model Repository Service that is used to access the source object. You can set the user name with the `-srcrsun` option or the environment variable `INFA_SOURCE_REPOSITORY_USER`. If you set a user name with both methods, the `-srcrsun` option takes precedence.
-sourceRepositoryPassword -srcrspd	source_MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the `-srcrspd` option or the environment variable `INFA_SOURCE_REPOSITORY_PASSWORD`. If you set a password with both methods, the password set with the `-srcrspd` option takes precedence.
-sourceRepositorySecurityDomain -srcrssdn	source_MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the `-srcrssdn` option or the environment variable `INFA_DEFAULT_SOURCE_SECURITY_DOMAIN`. If you set a security domain name with both methods, the `-srcrssdn` option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.

Option	Argument	Description
-sourceQuery -srcq	source_query	Required. A string that queries the source object. For more information, see "Queries" on page 257
-targetDomainName -tgtdn	target_domain_name	Required. Name of the domain for the target object.
-targetRepositoryService -tgtrs	target_MRS_name	Optional. Name of the Model Repository Service for the target object.
-targetDataIntegrationService -tgtdis	target_DIS_name	Optional. Name of the Data Integration Service for the target object.
-targetRepositoryUserName -tgtrsun	target_MRS_user_name	Optional. The user name for the Model Repository Service that is used to access the target object. You can set the user name with the `-tgtrsun` option or the environment variable `INFA_TARGET_REPOSITORY_USER`. If you set a user name with both methods, the `-tgtrsun` option takes precedence.
-targetRepositoryPassword -tgtrspd	target_MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the `-tgtrspd` option or the environment variable `INFA_TARGET_REPOSITORY_PASSWORD`. If you set a password with both methods, the password set with the `-tgtrspd` option takes precedence.
-targetRepositorySecurityDomain -tgtrssdn	target_MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the `-tgtrssdn` option or the environment variable `INFA_DEFAULT_TARGET_SECURITY_DOMAIN`. If you set a security domain name with both methods, the `-tgtrssdn` option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.

Option	Argument	Description
-targetQuery -tgtq	target_query	Required. A string that queries the target object. For more information, see "Queries" on page 257
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the `java.time.ZoneID` class.

DeleteParameterSetEntries

Deletes entries from a parameter set. Run this command to delete parameter set entries for a mapping or workflow that has been deployed as an application. You can delete specific parameter set entries or you can delete all of the parameter set entries.

If any parameter that you want to delete does not exist in the parameter set, the infacmd returns a warning message. The message indicates the parameter is not deleted because it is not in the parameter set.

The infacmd dis DeleteParameterSetEntries command uses the following syntax:

```
DeleteParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters

<-paramNames|-pnv> parameter names to delete, separated by spaces. For a mapping, M1, in
project P1 and folder F1, the path is P1/F1/mapping/M1.

<-all|> Delete all the parameters in the project scope.
```

The following table describes infacmd dis DeleteParameterSetEntries options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application that contains the parameter set.
parametersetname - ps	parameterset name	Required. Parameter set name.

Option	Argument	Description
-projectScope -prs	project scope	Required. Path to the mapping or workflow that contains the parameters. For a mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
-paramNames -pnv	parameter names	Required. Parameter set entry names to delete, separated by spaces. To delete all the parameters, use the -all option instead of this option.
-all	all	Delete all of the parameters in the parameter set.

deployObjectsToFile

Deploys design-time objects to an application patch archive file.

Query the objects that you want to package in the application patch archive file. You can use the file to perform the following tasks:

- Deploy an incremental application to a Data Integration Service for the first time by using infacmd dis "DeployApplication" on page 162.
- Update a deployed incremental application by using infacmd tools "patchApplication" on page 1093.
- Redeploy an incremental application by using infacmd dis "UpdateApplication" on page 231.

Note: The infacmd dis deployObjectsToFile command creates an application patch archive file on any node in a grid. You can also view the node details in the query report.

The infacmd dis deployObjectsToFile command uses the following syntax:

```
deployObjectsToFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> DIS_service_name
<-UserName|-un> DIS_user_name
<-Password|-pd> DIS_password
[<-SecurityDomain|-sdn> DIS_security_domain]
<-RepositoryService|-rs> MRS_service_name
<-RepositoryUserName|-rsun> MRS_user_name
<-RepositoryPassword|-rspd> MRS_password
[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
<-Query|-q> Query
[<-TimeZone|-tz> time_zone]
<-PatchName|-ptn> patch_name
[<-PatchDescription|-ptd> patch_description]
<-Application|-a> application_name
```

```
[<-FilePath|-fp> DIS_file_path]

[<-OperatingSystemProfile|-osp> OSProfile_name]

[<-OverwriteDeployedFile|-ow> True | False]

[<-MappingDeploymentProperties|-mdp>
Mapping_Deployment_Property_key=value_pairs_separated_by_semicolon]
```

The following table describes infacmd dis deployObjectsToFile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	DIS_service_name	Required. Name of the Data Integration Service.
-UserName -un	DIS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	DIS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	DIS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-RepositoryService -rs	MRS_service_name	Required. Name of the Model Repository Service.
-RepositoryUserName -rsun	MRS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -rsun option or the environment variable INFA_REPOSITORY_USER. If you set a user name with both methods, the -rsun option takes precedence.
-RepositoryPassword -rspd	MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -rspd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -rspd option takes precedence.

Option	Argument	Description
-RepositorySecurityDomain -rssdn	MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -rssdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -rssdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	query	Required. A string that queries the object. For more information, see "Queries" on page 257.
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the java.time.ZoneID class.
-PatchName -ptn	patch_name	Required. Name of the patch.
-PatchDescription -ptd	patch_description	Description of the patch.
-Application -a	application_name	Required. Name of the incremental application that the patch will be used to update.
-FilePath -fp	DIS_file_path	Optional. Path of the application patch archive file on the Data Integration Service machine. You can specify an absolute or relative path to the file.
-OperatingSystemProfile -osp	OSProfile_name	Optional. Name of the operating system profile. The operating system profile name can be up to 80 characters. It cannot include spaces or the following special characters: % * + \ / ? ; < >

Option	Argument	Description
-OverwriteDeployedFile -ow	True | False	Optional. Set to true to overwrite an existing export file. If an export file exists and this option is set to false, the export fails. Default is false.
-MappingDeploymentProperties -mdp	Mapping_Deployment_Property_key=value_pairs_separated_by_semicolon	Optional. Set the deployment properties for the mapping such as optimizing level, high precision, and sorting order.

DeployApplication

Deploys an application to a Data Integration Service.

The infacmd dis DeployApplication command uses the following syntax:

```
DeployApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FileName|-f> file_name
<-Application|-a> application
```

The following table describes infacmd dis DeployApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
Filename -f	file_name	Required. Name of the application file.
-Application -a	application	Required. Name of the application to deploy. If there is a name conflict, the deploy fails.

disableMappingValidationEnvironment

Disables the selected mapping validation environment for mappings that are deployed to the Data Integration Service.

Use the ValidationEnvironment parameter to disable a validation environment for a mapping. Repeat the command for each environment that you want to remove.

Use filters to specify one or more mappings in an application. If you do not include filters, the command updates all mappings that are deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

Changes take effect after you recycle the Data Integration Service.

The infacmd dis disableMappingValidationEnvironment uses the following syntax:

```
disableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-Application|-a> application_name]
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the disableMappingValidationEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Data Integration Service.
Application -a	application_name	Optional. Name of the application that contains one or more mappings. If you do not specify the application, the command updates all applications that are deployed to the Data Integration Service.
-ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository.
MappingNamesFilter -mnf	mapping names	Optional. The names of mappings that you want to disable the validation environment for. Separate mapping names with commas. Default is all mappings that are deployed to the Data Integration Service.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Specify the execution environment for the validation environment you want to remove. You can enter either Native, Hadoop, or Databricks. By default, the validation environment is changed for all engines based on other filter criteria.

Option	Argument	Description
ValidationEnvironment -ve	validation_environment_name	Required. Name of the validation environment to remove from a mapping. You can enter one of the following values: - native - blaze - spark - spark-databricks Run the command for each validation environment to remove.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Selects only mappings whose parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks`
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Selects only mappings whose default parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks`
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

enableMappingValidationEnvironment

Enables a mapping validation environment for mappings that are deployed to the Data Integration Service. The mapping validation environment properties indicate the engines that the mapping will be validated to run in.

Use the ValidationEnvironment parameter to specify a validation environment. Repeat the command and specify a different validation environment to enable an additional validation environment for the mapping.

Use filters to specify one or more mappings in an application or all applications that are deployed to a Data Integration Service. If you do not include filters, the command updates all mappings that are deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

Changes take effect after you recycle the Data Integration Service.

The infacmd dis enableMappingValidationEnvironment uses the following syntax:

```
enableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-Application|-a> application_name]
[<-ConnectionName|-cn> connection_name]
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the enableMappingValidationEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Data Integration Service.
Application -a	application_name	Optional. Name of the application that contains one or more mappings. If you do not specify the application, the command updates all applications that are deployed to the Data Integration Service.
-ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository.
ConnectionName -cn	connection_name	Name of the connection for the mapping validation environment to use. The connection overwrites an existing connection or connection parameter that was set for the environment. Required to enable the non-native environment if no connection is present in the specified mapping. Optional to enable the native environment or if a connection is already present.

Option	Argument	Description
MappingNamesFilter -mnf	mapping names	Optional. The names of mappings that you want to enable the validation environment for. Separate mapping names with commas. Default is all mappings that are deployed to the Data Integration Service.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Identify the execution environment to filter on. You can enter Native, Hadoop, or Databricks. By default, the validation environment is changed for all engines based on other filter criteria.
ValidationEnvironment -ve	validation_environment_name	Required. Name of the validation environment to enable on a mapping. You can enter one of the following values: - native - blaze - spark - spark-databricks Run the command for each validation environment to enable.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Selects only mappings whose parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks`
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Selects only mappings whose default parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks`
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListApplicationObjectPermissions

Lists the permissions that a user or group has for an application object such as mapping or workflow.

The infacmd dis ListApplicationObjectPermissions command uses the following syntax:

```
ListApplicationObjectPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow
<-ApplicationObject|-ao> application_object_name
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd dis ListApplicationObjectPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application.
-ApplicationObjectType -t	application_object_type	Required. Type of the application object type. Enter one of the following values: - Mapping - Workflow
-ApplicationObject -ao	application_object_name	Required. Name of the application object.
-Direct | -Effective	direct | effective	Required. Level of permissions to list. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

ListApplicationObjects

Lists the objects that an application contains.

When you use the -ListObjectTypes option, the command also lists the type of each object.

The infacmd dis ListApplicationObjects command uses the following syntax:

```
ListApplicationObjects
[<-DomainName|-dn> domain_name]
[<-DomainAddress|-da> domain_address. syntax - host:port]
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
```

```
[<-ObjectType|-t> object_type]
[<-ListObjectType|-lt> list_object_type]
[<-PageSize|-ps> page_size]
[<-PageIndex|-pi> page_index]
```

The following table describes infacmd dis ListApplicationObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Optional. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-DomainAddress -da	domain_address	Optional. Address of the Informatica domain.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application.
-ObjectType -t	object_type	Optional. Type of object that you want to list. You can use this option to filter the results by object type.
-ListObjectType -lt	true | false	Optional. Enter one of the following values: - true - false
-PageSize -ps	page_size	Required when you specify the PageIndex option. The number of results to display in each group. When you specify a page size, you organize command results in groups. For example, if you specify `-PageSize 5`, then the command returns results in groups of five or fewer.
-PageIndex -pi	page_index	Optional. Starting with zero, the number of page results to display. For example, if you specify `-PageSize 5 -PageIndex 0`, then the command returns the first page of five results, results one through five. If you omit this option, the command returns the first PageSize of results. Default is zero.

ListApplicationOptions

Lists the properties for an application.

The infacmd dis ListApplicationOptions command uses the following syntax:

```
ListApplicationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application
```

The following table describes infacmd dis ListApplicationOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application.

ListApplicationPermissions

Lists the permissions that a user or group has for an application.

The infacmd dis ListApplicationPermissions command uses the following syntax:

```
ListApplicationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd dis ListApplicationPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application.
-Direct | -Effective	direct | effective	Required. Level of permissions to list. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

ListApplications

Lists the applications that are deployed to a Data Integration Service.

The infacmd dis ListApplications command uses the following syntax:

```
ListApplications
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd dis ListApplications options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service for which to list applications.

ListComputeOptions

List Data Integration Service properties for a node with the compute role.

The infacmd dis ListComputeOptions command uses the following syntax:

```
ListComputeOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd dis ListComputeOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
NodeName -nn	node_name	Required. Node with the compute role that is assigned to the Data Integration Service or to the Data Integration Service grid.

ListDataObjectOptions

Lists properties of a data object.

The infacmd dis ListDataObjectOptions command uses the following syntax:

```
ListDataObjectOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
```

The following table describes infacmd dis ListDataObjectOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application.

Option	Argument	Description
-Folder -f	folder	Required. Repository folder that contains the data object.
DataObject -do	data_model.data_object	Required. Data object name.

ListMappingEngines

Lists the execution engines of the mappings deployed to a Data Integration Service. You can filter the results based on the application, validation environment, execution environment, and execution environment parameters. If you do not specify any filters, the command lists the execution engines of all deployed mappings.

The infacmd dis listMappingEngines command uses the following syntax:

```
ListMappingEngines
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ProjectName|-pn> project_name]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Application|-a> application_name]
[<-ValidationEnvironmentFilter|-vef> validation_environment_name]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParamNameFilter|-pnf> execution_environment_parameter_name]
```

The following table describes infacmd dis listMappingEngines options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
Application -a	application_name	Optional. Filters the mappings by the deployed application that contains the mappings. Enter the name of the deployed application.
ValidationEnvironmentFilter -vef	validation_environment_name	Optional. Filters the mappings by the validation environment where the mapping definition is validated. You can enter one of the following values: - native - blaze - spark - spark-databricks
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Filters the mappings by the execution environment where the mappings run. You can enter Native, Hadoop, or Databricks.
ExecutionEnvironmentParamNameFilter -pnf	execution_environment_parameter_name	Optional. Filters the mappings by the execution environment parameter. Enter the name of the execution environment parameter.

ListParameterSetEntries

Lists the entries in a parameter set.

The infacmd dis ListParameterSetEntries command uses the following syntax:

```
ListParameterSetEntries
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
```

```
<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
```

The following table describes infacmd dis ListParameterSetEntries options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application that contains the parameter set.

Option	Argument	Description
parametersetname - ps	parameterset name	Required. Parameter set name.
-projectScope -prs	project scope	Required. Path to the mapping or workflow that contains the parameters. For a mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.

ListParameterSetObjects

List the objects in a specific parameter set.

The infacmd dis ListParameterSetObjects command uses the following syntax:

```
ListParameterSetObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Password|-ps> parameter set
<-Application|-a> application that contains the parameter set
```

The following table describes infacmd dis ListParameterSetObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-parameterset -ps	parameter set	Required. The name of the parameter set that you want to view.
-Application -a	application	Required. Name of the application that contains the parameter set.

ListParameterSets

List the parameter sets in an application.

The infacmd dis ListParameterSets command uses the following syntax:

```
ListParameterSets

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-Application|-a> application
```

The following table describes infacmd dis ListParameterSets options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application that contains the parameter sets.

listPatchNames

Lists all patches that have been applied to an incremental application.

The infacmd dis listPatchNames command uses the following syntax:

```
listPatchNames
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilientTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

The following table describes infacmd dis listPatchNames options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -dun option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -dun option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -dpd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -dsdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.

Option	Argument	Description
ResilientTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.
Application -a	application_name	Required. Name of the incremental application.

ListSequenceObjectProperties

Lists the properties for a sequence data object.

The infacmd dis listsequenceobjectproperties command uses the following syntax:

```
ListSequenceObjectProperties
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
```

The following table describes infacmd dis ListSequenceObjectProperties options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Integration Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-Application -a	application	Required. Name of the application.
-SequenceObjectPath -sop	sequence object path	Required. Path to the sequence data object. The path must include the following objects, in order, and where applicable: - Project - Folders - SQL data service or web service - Mapping - Sequence Generator transformation - Sequence data object If the sequence data object is in a mapping, SQL data service, or web service, you must use a prefix before the mapping name, SQL data service name, or web service name. Use the following prefixes with options in the command: - Mapping:<mapping name> - SQLDS:<SQL data service name> - WS:<web service name> Separate the options with a slash (/). For example: `<project name>/<folder>/SQLDS:<SQL Data Service Name>/Mapping:<virtual table mapping>/<Sequence Generator transformation>/<sequence data object name>`

.

ListSequenceObjects

Lists the sequence data objects deployed to an application.

The infacmd dis ListSequenceObjects command uses the following syntax:

```
ListSequenceObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
```

The following table describes infacmd dis ListSequenceObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Integration Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application.

.

ListServiceOptions

Lists the properties for a Data Integration Service.

The infacmd dis ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd dis ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists the properties of a Data Integration Service process.

The infacmd dis ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd dis ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-NodeName -nn	node_name	Required. Name of node where the service process runs.

.

PurgeDataObjectCache

Purges the cache for a logical data object. If caching for logical data objects is enabled, this command deletes all cache for a logical data object except the latest cache run. If the latest cache run is older than the time set in the Cache Refresh Period property, the latest cache run is also deleted. If caching for logical data objects is not enabled, this command deletes all cache for the logical data object.

You must disable the application for a logical data object before you purge the data object cache.

The infacmd dis PurgeDataObjectCache command uses the following syntax:

```
PurgeDataObjectCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
<-Folder|-f> folder
<-DataObject|-do> data_model.data_object
[<-PurgeAll|-pa> true|false]
```

The following table describes infacmd dis PurgeDataObjectCache options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
Application -a	application	Name of the application that contains the data object.
Folder -f	folder	Name of the folder that contains the data object model.

Option	Argument	Description
DataObject -do	data_model.data_object	Name of the data object with the cache you need to purge.
-PurgeAll -pa	true | false	Optional. Deletes all cache for a logical data object.

PurgeResultSetCache

Purges the result set caches for an application. You can purge the cache for an application when you do not need the existing result set caches for the SQL data services and the web services in the application.

The infacmd dis PurgeResultSetCache command uses the following syntax:

```
PurgeResultSetCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
```

The following table describes infacmd dis PurgeResultSetCache options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
Application -a	application	Name of the application that you want to purge the result set cache for.

queryDesignTimeObjects

Queries design-time objects from a Model repository and returns a list of the objects.

The infacmd dis queryDesignTimeObjects command uses the following syntax:

```
queryDesignTimeObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> DIS_service_name
<-UserName|-un> DIS_user_name
<-Password|-pd> DIS_password
[<-SecurityDomain|-sdn> DIS_security_domain]
<-RepositoryService|-rs> MRS_service_name
```

```
<-RepositoryUserName|-rsun> MRS_user_name
<-RepositoryPassword|-rspd> MRS_password
[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
<-Query|-q> Query
[<-TimeZone|-tz> time_zone]
```

The following table describes infacmd dis queryDesignTimeObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -dsdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-RepositoryService -rs	MRS_service_name	Required. Name of the Model Repository Service.

Option	Argument	Description
-RepositoryUserName -rsun	MRS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -rsun option or the environment variable INFA_REPOSITORY_USER. If you set a user name with both methods, the -rsun option takes precedence.
-RepositoryPassword -rspd	MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -rspd option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rspd option takes precedence.
-RepositorySecurityDomain -rssdn	MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -rssdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -rssdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	query	Required. A string that queries the object. For more information, see "Queries" on page 257.
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the java.time.ZoneID class.

queryRunTimeObjects

Queries run-time objects that are deployed to a Data Integration Service and returns a list of the objects.

The infacmd dis queryRunTimeObjects command uses the following syntax:

```
queryRunTimeObjects
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
<-Query|-q> query
```

The following table describes infacmd dis queryRunTimeObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -dun option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -dun option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -dpd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -dsdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	query	Required. A string that queries the object. For more information, see "Queries" on page 257.

RefreshDataObjectCache

Refreshes a data object cache.

The infacmd dis RefreshDataObjectCache command uses the following syntax:

```
RefreshDataObjectCache

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object
```

The following table describes infacmd dis RefreshDataObjectCache options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that you want to list the applications for.
-Application -a	application	Required. Name of the application that contains the data object.
-Folder -f	folder	Required. Name of the folder that contains the data object.
-DataObject -do	data_model.data_object	Required. Name of the data object that has cache to refresh.

RenameApplication

Renames a deployed application. Before you rename an application, run infacmd dis StopApplication to stop it.

The infacmd dis RenameApplication command uses the following syntax:

```
RenameApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
<-NewName|-n> new_name
```

The following table describes infacmd dis RenameApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-Application -a	application	Required. Current application name.
-NewName -n	new_name	Required. New name for the application.

replaceMappingHadoopRuntimeConnections

Replaces the Hadoop connection of all mappings in deployed applications with another Hadoop connection. The Data Integration Service uses the Hadoop connection to connect to the Hadoop cluster to run mappings in the Hadoop environment.

The command does not modify Hadoop connections in the transformations. You can specify the application name to replace the Hadoop connection of an application.

The infacmd dis replaceMappingHadoopRuntimeConnections uses the following syntax:

```
replaceMappingHadoopRuntimeConnections
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ApplicationName|-an> application_name]
<-OldConnectionName|-oc> connection_name_of_old_connection_to_replace
<-NewConnectionName|-nc> connection_name_of_new_connection
```

The following table describes the replaceMappingHadoopRuntimeConnections options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
ServiceName -sn	service_name	Required. Name of the Data Integration Service.
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
ApplicationName -an	application_name	Optional. Name of the application that contains the mapping. If you specify this option, the command replaces the Hadoop connection only for the application.
OldConnectionName -oc	connection_name_of_old_connection_to_replace	Required. Name of the Hadoop connection that you want to replace.
NewConnectionName -nc	connection_name_of_new_connection	Required. Name of the Hadoop connection that the Data Integration Service must use to connect to Hadoop cluster to run mappings in the Hadoop environment.

RestoreApplication

Restores an application from a backup file. When you deploy a restored application, the application state depends on the default deployment mode. The application properties are retained in the restored application.

The infacmd dis RestoreApplication command uses the following syntax:

```
RestoreApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FileName|-f> file_name
[<-Application|-a> application]
```

The following table describes infacmd dis RestoreApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to restore the application to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-FileName -f	file_name	Required. Name of the application backup file.
-Application -a	application	Optional. Name of the application after after you deploy it. If there is a name conflict, the deploy fails.

SetApplicationPermissions

Assigns or denies permissions on an application to a user or a group.

You can allow or deny permissions to users with the -ap or -dp options of the SetApplicationPermissions command. If you do not explicitly allow or deny permissions using one of the options, all permissions on the application are revoked.

The infacmd dis SetApplicationPermissions command uses the following syntax:

```
SetApplicationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

```
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
[<-AllowedPermissions|-ap> allowed_permissions]
[<-DeniedPermissions|-dp> denied_permissions]
```

The following table describes infacmd dis SetApplicationPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-Application -a	application_name	Required. Name of the application.
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-AllowedPermissions -ap	allowed_permissions	Optional. List of permissions to allow. Enter any of the following permissions separated by spaces: - View. Users can view application. - Grant. Users can grant and revoke permissions on the application. - Execute. Users can run application.
-DeniedPermissions -dp	denied_permissions	Optional. List of permissions to deny users. Separate each parameter by a space. Enter any of the following permissions separated by spaces: - View. Users can view application. - Grant. Users cannot grant and revoke permissions on the application. - Execute. Users cannot run application.

SetApplicationObjectPermissions

Assigns or denies permissions on an application object such as mapping or workflow to a user or a group.

You can allow or deny permissions to users with the -ap or -dp options of the SetApplicationObjectPermissions command. If you do not explicitly allow or deny permissions using one of the options, the user inherits the application-level permission on the mapping or the workflow.

The infacmd dis SetApplicationObjectPermissions command uses the following syntax:

```
SetApplicationObjectPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-ApplicationObjectType|-t> application_object_type_Mapping_Workflow
<-ApplicationObject|-ao> application_object_name
```

```
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
[<-AllowedPermissions|-ap> allowed_permissions]
[<-DeniedPermissions|-dp> denied_permissions]
```

The following table describes infacmd dis SetApplicationObjectPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-Application -a	application_name	Required. Name of the application.
-ApplicationObjectType -t	application_object_type	Required. Type of the application object type. Enter one of the following values: - Mapping - Workflow
-ApplicationObject -ao	application_object_name	Required. Name of the application object.
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-AllowedPermissions -ap	allowed_permissions	Optional. List of permissions to allow. Enter any of the following permissions separated by spaces: - View. Users can view application. - Grant. Users can grant and revoke permissions on the application. - Execute. Users can run application.
-DeniedPermissions -dp	denied_permissions	Optional. List of permissions to deny users. Separate each parameter by a space. Enter any of the following permissions separated by spaces: - View. Users can view application. - Grant. Users cannot grant and revoke permissions on the application. - Execute. Users cannot run application.

setMappingExecutionEnvironment

Specifies the mapping execution environment for mappings that are deployed to the Data Integration Service.

Use filters to specify a list of mappings, all mappings in an application, or all applications that are deployed to a Data Integration Service. If you do not include filters, the command updates all mappings that are deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

Changes take effect after you recycle the Data Integration Service.

The infacmd dis setMappingExecutionEnvironment uses the following syntax:

```
setMappingExecutionEnvironment
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ProjectName|-pn> project_name]
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-MappingNamesFilter|-mnf> mapping_names]
<-ExecutionEnvironment|-ee> execution_environment_name
```

The following table describes the setMappingExecutionEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository.

Option	Argument	Description
MappingNamesFilter -mnf	mapping names	Optional. The names of mappings that you want to set the execution environment for. Separate mapping names with commas. Default is all mappings that are deployed to the Data Integration Service.
ExecutionEnvironment -ee	execution_environment_name	Required. Identify the execution environment to set. Choose either Native, Hadoop, or Databricks.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
NewConnectionName -nc	connection_name_of_new_connection	Required. Name of the Hadoop or Databricks connection that the Data Integration Service must use to connect to the compute cluster to run mappings in the non-native environment.

SetSequenceState

Updates the current value of a sequence data object.

The infacmd dis SetSequenceState command uses the following syntax:

```
SetSequenceState
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application
<-SequenceObjectPath|-sop> sequence_object_path
<-SequenceValue|-sv> sequence_value
```

The following table describes infacmd dis SetSequenceState options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Integration Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-Application -a	application	Required. Name of the application.
-SequenceObjectPath -sop	sequence object path	Required. Path to the sequence data object. The path can include the following objects, in order, and where applicable: - Project - Folders - SQL data service or web service - Mapping - Sequence Generator transformation - Sequence data object To update a reusable sequence data object, specify the path using only the project, folders, and sequence data object. To update a non-reusable sequence data object that is in a SQL data service or web service, use a prefix before the SQL data service name or web service name. Use the following prefixes with options in the command: - SQLEP:<SQL data service name> - WSEP:<web service name> Separate the options with a slash (/). For example: `<project name>/<folder name>/WSEP:<web service name>/<operation mapping name>/<Sequence Generator transformation name>/<sequence data object name>`
-SequenceValue -sv	sequence_value	Required. The new value for sequence data object. Enter a value that is greater than or equal to the start value of the sequence data object and less than or equal to the end value.

.

StartApplication

Starts a deployed application. You must enable the application before you can start it. The Data Integration Service must be running.

The infacmd dis StartApplication command uses the following syntax:

```
StartApplication

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-Application|-a> application
```

The following table describes infacmd dis StartApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application to start.

StopApplication

Stops an application from running. You might stop an application if you need to back it up or if you want to prevent users from accessing it.

The infacmd dis StopApplication command uses the following syntax:

```
StopApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
```

The following table describes infacmd dis StopApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-Application -a	application	Required. Name of the application to stop.

stopBlazeService

Stops the components of the Blaze engine from running. You might stop the Blaze engine components from running if you want to perform maintenance on the Hadoop cluster such as cleaning up resources or applying software patches.

The infacmd dis stopBlazeService command uses the following syntax:

```
stopBlazeService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-HadoopConnection|-hc> Hadoop_Cluster_Connection_Name
```

The following table describes infacmd dis stopBlazeService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-HadoopConnection -hc	Hadoop_Cluster_Connection_Name	Required. Name of the Hadoop connection that the Data Integration Service uses to run the mapping on the Blaze engine.

Note: When you run the stopBlazeService command, some component logs might not be written to aggregate log files on HDFS. You can view the logs in the directory configured for the Blaze engine logs based on the following Blaze advanced property in the Hadoop connection: `infagrid.node.local.root.log.dir`

tag

Assigns tags to design-time objects.

Tags are metadata that defines an object in the Model Repository service. Query the objects and specify the tags to group objects according to their business usage. If you reassign a tag to an object, the command will overwrite the existing tag.

The infacmd dis tag command uses the following syntax:

```
tag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

<-RepositoryService|-rs> MRS_service_name

<-RepositoryUserName|-rsun> MRS_user_name

<-RepositoryPassword|-rspd> MRS_password

[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]

<-Query|-q> Query

<-TagName|-tn> tag_name

[<-TagDescription|-td> tag_description]

[<-TimeZone|-tz> time_zone]
```

The following table describes infacmd dis tag options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	DIS_service_name	Required. Name of the Data Integration Service.
-UserName -un	DIS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.

Option	Argument	Description
-Password -pd	DIS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	DIS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
RepositoryService -rs	MRS_service_name	Required. Name of the Model Repository Service.
-RepositoryUserName -rsun	MRS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -rsun option or the environment variable INFA_REPOSITORY_USER. If you set a user name with both methods, the -rsun option takes precedence.
-RepositoryPassword -rspd	MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -rspd option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rspd option takes precedence.
RepositorySecurityDomain -rssdn	MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -rssdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -rssdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	Query	Required. A string that queries the repository for a tag name. For more information, see "Queries" on page 257.

Option	Argument	Description
-TagName -tn	tag_name	Required. Name of the tag that you want to assign to the queried object. The name must not exceed 128 characters and start with a number. The name must consist of alphanumeric characters. You can also the special characters such as @ # _.
-TagDescription -td	tag_description	Optional. The description of the tag.
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the java.time.ZoneID class.

untag

Removes tags from design-time objects.

If business usage has changed, remove tags to ungroup objects. Query the objects and specify the tags to remove.

The infacmd dis untag command uses the following syntax:

```
untag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]

<-RepositoryService|-rs> MRS_service_name

<-RepositoryUserName|-rsun> MRS_user_name

<-RepositoryPassword|-rspd> MRS_password

[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]

<-Query|-q> Query

<-TagName|-tn> tag_name

[<-TimeZone|-tz> time_zone]
```

The following table describes infacmd dis untag options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	DIS_service_name	Required. Name of the Data Integration Service.
-UserName -un	DIS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	DIS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	DIS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-RepositoryService -rs	MRS_service_name	Required. Name of the Model Repository Service.
-RepositoryUserName -rsun	MRS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -rsun option or the environment variable INFA_REPOSITORY_USER. If you set a user name with both methods, the -rsun option takes precedence.

Option	Argument	Description
-RepositoryPassword -rspd	MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -rspd option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rspd option takes precedence.
-RepositorySecurityDomain -rssdn	MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -rssdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -rssdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	Query	Required. A string that queries the repository for a tag name. For more information, see "Queries" on page 257.
-TagName -tn	tag_name	Required. Name of the tag that you want to remove from the queried object.
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the java.time.ZoneID class.

replaceAllTag

Replaces all tags that are assigned to design-time objects.

Query the objects and replace the assigned tags. If the business usage has changed, you can use the command to ungroup objects and assign new tags to regroup objects. All assigned tags are deleted and replaced with the specified tag.

The infacmd dis replaceAllTag command uses the following syntax:

```
replaceAllTag
<-DomainName|-dn> domain_name

<-ServiceName|-sn> DIS_service_name

<-UserName|-un> DIS_user_name

<-Password|-pd> DIS_password

[<-SecurityDomain|-sdn> DIS_security_domain]
```

```
<-RepositoryService|-rs> MRS_service_name
<-RepositoryUserName|-rsun> MRS_user_name
<-RepositoryPassword|-rspd> MRS_password
[<-RepositorySecurityDomain|-rssdn> MRS_security_domain]
<-Query|-q> Query
<-TagName|-tn> tag_name
[<-TagDescription|-td> tag_description]
[<-TimeZone|-tz> time_zone]
```

The following table describes infacmd dis replaceAllTag options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	DIS_service_name	Required. Name of the Data Integration Service.
-UserName -un	DIS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	DIS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	DIS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.

Option	Argument	Description
-RepositoryService -rs	MRS_service_name	Required. Name of the Model Repository Service.
-RepositoryUserName -rsun	MRS_user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -rsun option or the environment variable INFA_REPOSITORY_USER. If you set a user name with both methods, the -rsun option takes precedence.
-RepositoryPassword -rspd	MRS_password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -rspd option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rspd option takes precedence.
-RepositorySecurityDomain -rssdn	MRS_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -rssdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -rssdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native.
-Query -q	query	Required. A string that queries the repository for a tag name. For more information, see "Queries" on page 257.
-TagName -tn	tag_name	Required. The name of the replacement tag that you want to assign to the queried objects. The name must not exceed 128 characters and start with a number. The name must consist of alphanumeric characters. You can also the special characters such as @ # _.
-TagDescription -td	tag_description	Optional. The description of the tag.
-TimeZone -tz	time_zone	Optional. By default, the command uses the time zone on the machine that runs the Data Integration Service process. For a list of valid time zones, refer to the java.time.ZoneID class.

UndeployApplication

Removes an application from a Data Integration Service.

The infacmd dis UndeployApplication command uses the following syntax:

```
UndeployApplication
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application
```

The following table describes infacmd dis UndeployApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -un option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to remove the application from.
-Application -a	application	Required. Name of the application to remove from the Data Integration Service.

UpdateApplication

Updates an application from an application file and maintains the configuration. The application must be deployed to a Data Integration Service. End users can access the latest version of the application.

The infacmd dis UpdateApplication command uses the following syntax:

```
UpdateApplication
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FileName|-f> file_name
[<-Application|-a> application]
```

The following table describes infacmd dis UpdateApplication options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-FileName -f	file_name	Required. Name and path of the application file to update the deployed application with.
-Application -a	application	Optional. Name of the deployed application.

UpdateApplicationOptions

Updates application properties.

Separate each option and value with a space. To view current properties, run infacmd dis ListApplicationOptions.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd dis UpdateApplicationOptions command uses the following syntax:

```
UpdateApplicationOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-Options|-o> options
```

The following table describes infacmd dis UpdateApplicationOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application to update.
-Options -o	options	Required. Enter each option and value to update. Separate each option by a space. To view application options, run the infacmd dis ListApplicationOptions command.

UpdateComputeOptions

Updates Data Integration Service properties for a node with the compute role. Use the command to override Data Integration Service properties for a specific compute node.

Enter options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd dis UpdateComputeOptions command uses the following syntax:

```
UpdateComputeOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

The following table describes infacmd dis UpdateComputeOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
NodeName -nn	node_name	Required. Node with the compute role that is assigned to the Data Integration Service or to the Data Integration Service grid.
-Options -o	options	Required. Enter each option separated by a space. To view the options, run the infacmd dis ListComputeOptions command. You can update the following Data Integration Service options: - ExecutionOptions.TemporaryDirectories - ExecutionOptions.DISHomeDirectory - ExecutionOptions.CacheDirectory - ExecutionOptions.SourceDirectory - ExecutionOptions.TargetDirectory - ExecutionOptions.RejectFilesDirectory

UpdateDataObjectOptions

Updates data object properties. To view the current options, run the infacmd dis ListDataObjectOptions command.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd dis UpdateDataObjectOptions command uses the following syntax:

```
UpdateDataObjectOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-Folder|-f> folder

<-DataObject|-do> data_model.data_object

<-Options|-o> options
```

The following table describes infacmd dis UpdateDataObjectOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Application that contains the data object.
-Folder -f	Folder	Required. Name of the folder that contains the data object model.

Option	Argument	Description
-DataObject -do	data_model.data_object	Required. Name of the data object that you want to update.
-Options -o	options	Required. Enter options and values separated by spaces. To view the current options, run the infacmd dis ListDataObjectOptions command.

Data Object Options

Use the data object options to configure caching for a logical data object. Use the data object options with the infacmd dis UpdateDataObjectOptions command.

Enter data object options in the following format:

```
... -o option_type.option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes data object options:

Option	Description
DataObjectOptions.CachingEnabled	Cache the logical data object in the data object cache database. True or false. Default is true.
DataObjectOptions.CacheRefreshPeriod	Number of minutes between cache refreshes. Default is zero.
DataObjectOptions.CacheTableName	The name of the user-managed table from which the Data Integration Service accesses the logical data object cache. A user-managed cache table is a table in the data object cache database that you create, populate, and manually refresh when needed. If you specify a cache table name, the Data Object Cache Manager does not manage the cache for the object and ignores the cache refresh period. If you do not specify a cache table name, the Data Object Cache Manager manages the cache for the object.

UpdateParameterSetEntries

Updates entries from a parameter set. Run this command to update the values in parameter set entries for a mapping or workflow in an application.

The infacmd dis UpdateParameterSetEntries command uses the following syntax:

```
UpdateParameterSetEntries

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Application|-a> application

<-parameterSetName|-ps> parameter set name

<-projectScope|-prs> path to the mapping or workflow that contains the parameters. For a
mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.

<-paramNames|-pnv> parameter name-value pairs, separated by double quotes
```

The following table describes infacmd dis UpdateParameterSetEntries options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that the application is deployed to.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application	Required. Name of the application that contains the parameter set.
parametersetname - ps	parameterset name	Required. Parameter set name.
-projectScope -prs	project scope	Required. Path to the mapping or workflow that contains the parameters. For a mapping, M1, in project P1 and folder F1, the path is P1/F1/mapping/M1.
-paramNames -pnv	parameter names	Required.Required. Parameter name-value pairs separated by space. Enclose name-value pairs in double quotes. Enclose each value in single quotes. Use the following syntax: `"parm1='valueA'" "parm2='valueB'" "parm3='valueC'"` . You can include spaces in a parameter value. You can include an apostrophe (') or a colon (:) in the value if you escape the character with a backslash (\). `'C:\directory'`

UpdateServiceOptions

Updates Data Integration Service properties. To view current properties run the infacmd dis ListServiceOptions command.

You can change service properties and you can change the service to run on a single node or on a grid. Changes take effect after you recycle the service. You can use the RecycleMode (-rm) option to recycle the service.

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options]

[<-NodeName|-nn> node_name | <-GridName|-gn> grid_name]

[<-RecycleMode|-rm> recycle_mode]
```

```
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

The following table describes infacmd dis UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Optional. Enter each option separated by a space. To view options, run the infacmd dis ListServiceOptions command.

Option	Argument	Description
-NodeName -nn	node_name	If you want to remove the Data Integration Service from a grid and run it on a single node, enter the node name. You can enter the node name or grid name, but you cannot enter both.
-GridName -gn	grid_name	If you want to move the Data Integration Service from a single node to a grid, enter the grid name. You can enter the node name or grid name, but you cannot enter both.
-RecycleMode -rm	recycle_mode	Optional. Recycle mode restarts the service and applies the latest service and service process properties. Select Abort or Complete. - Complete. Stops all applications and cancels all jobs within each application. Waits for all jobs to cancel before disabling the service. - Abort. Stops all applications and tries to cancel all jobs before aborting them and disabling the service. Default is Complete.
-BackupNodes -bn	node_name1,node_name2,..	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Data Integration Service Options

Use the Data Integration Service options with the infacmd dis UpdateServiceOptions command.

Enter Data Integration Service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Data Integration Service options:

Option	Description
AdvancedProfilingServiceOptions.ColumnsPerMapping	Limits the number of columns that can be profiled in a single mapping due to save memory and disk space. Default is 5. If you profile a source with over 100 million rows decrease the value to as low as 1.
AdvancedProfilingServiceOptions.ExecutionPoolSize	Maximum number of threads to run mappings.
AdvancedProfilingServiceOptions.MaxMemPerRequest	Maximum amount of memory, in bytes, that the Data Integration Service can allocate for each mapping run for a single profile request. Default is 536,870,912.
AdvancedProfilingServiceOptions.MaxNumericPrecision	Maximum number of digits for a numeric value.

Option	Description
AdvancedProfilingServiceOptions.MaxParallelColumnBatches	Number of threads that can run mappings at the same time. Default is 1.
AdvancedProfilingServiceOptions.MaxStringLength	Maximum length of a string that the profiling service can process.
AdvancedProfilingServiceOptions.MaxValueFrequencyPairs	Maximum number of value/frequency pairs to store in the profiling warehouse. Default is 16,000.
AdvancedProfilingServiceOptions.MinPatternFrequency	Minimum number of patterns to display for a profile.
AdvancedProfilingServiceOptions.ReservedThreads	Number of threads of the Maximum Execution Pool Size that are for priority requests. Default is 1.
AdvancedProfilingServiceOptions.ValueFrequencyMemSize	Amount of memory to allow for value-frequency pairs. Default is 64 megabytes.
DataObjectCacheOptions.CacheConnection	The database connection name for the database that stores the data object cache. Enter a valid connection object name.
DataObjectCacheOptions.CacheRemovalTime	The number of milliseconds the Data Integration Service waits before cleaning up cache storage after a refresh. Default is 3,600,000.
DeploymentOptions.DefaultDeploymentMode	Determines whether to enable and start each application after you deploy it to a Data Integration Service. Enter one of the following options: - EnableandStart. Enable the application and start the application. - EnableOnly. Enable the application but do not start the application. - Disable. Do not enable the application.
DataObjectCacheOptions.EnableNestedLDOCache	Indicates that the Data Integration Service can use cache data for a logical data object used as a source or a lookup in another logical data object during a cache refresh. If false, the Data Integration Service accesses the source resources even if you enabled caching for the logical data object used as a source or a lookup. For example, logical data object LDO3 joins data from logical data objects LDO1 and LDO2. A developer creates a mapping that uses LDO3 as the input and includes the mapping in an application. You enable caching for LDO1, LDO2, and LDO3. If you enable nested logical data object caching, the Data Integration Service uses cache data for LDO1 and LDO2 when it refreshes the cache table for LDO3. If you do not enable nested logical data object caching, the Data Integration Service accesses the source resources for LDO1 and LDO2 when it refreshes the cache table for LDO3. Default is false.
DataObjectCacheOptions.MaxConcurrentRefreshRequests	Maximum number of cache refreshes that can occur at the same time.

Option	Description
ExecutionContextOptions.Spark.MSPEnableUnassignedData	If true, enables midstream parsing functionality that captures unparsed data in the source string and saves it in an `UnassignedData` array as an `unidentifiedDataItem`. By default, if the parser encounters a data field that it cannot parse, the data is ignored. But the source string complex data schema can change. For example, a software update on the server might change the JSON or XML. This option allows you to capture the data for analysis. Default is false.
ExecutionOptions.BigDataJobRecovery	If true, enables data engineering job recovery and distributed queueing for deployed jobs configured to run on the Spark engine. Default is false.
ExecutionOptions.CacheDirectory	Directory for index and data cache files for transformations. Default is `<home directory>/cache`. Enter a list of directories separated by semicolons to increase performance during cache partitioning for Aggregator, Joiner, or Rank transformations. You cannot use the following characters in the directory path: `* ? < > " | ,`
ExecutionOptions.DisHadoopKeytab	The file path to the Kerberos keytab file on the machine on which the Data Integration Service runs.
ExecutionOptions.DisHadoopPrincipal	Service Principal Name (SPN) of the Data Integration Service to connect to a Hadoop cluster that uses Kerberos authentication.
ExecutionOptions.DISHomeDirectory	Root directory accessible by the node. This is the root directory for other service directories. Default is `<Informatica installation directory>/tomcat/bin`. If you change the default value, verify that the directory exists. You cannot use the following characters in the directory path: `* ? < > " | ,`
ExecutionOptions.EnableOSProfile	Indicates that the Data Integration Service can use operating system profiles for mapping execution. You can enable operating system profiles if the Data Integration Service runs on UNIX or Linux. Default is false.
ExecutionOptions.HadoopDistributionDir	The directory containing a collection of Hadoop JARS on the cluster from the RPM Install locations. The directory contains the minimum set of JARS required to process Informatica mappings in a Hadoop environment. Type `/<PowerCenterBigDataEditionInstallationDirectory>/Informatica/services/shared/hadoop/[Hadoop_distribution_name]`.
ExecutionOptions.HadoopInfaHomeDir	The PowerCenter Big Data Edition home directory on every data node created by the Hadoop RPM install. Type `/<PowerCenterBigDataEditionInstallationDirectory>/Informatica`.

Option	Description
ExecutionOptions.MaxHadoopBatchExecutionPoolSize	Maximum number of deployed jobs that can run concurrently in the Hadoop environment. The Data Integration Service moves Hadoop jobs from the queue to the Hadoop job pool when enough resources are available. Default is 100.
ExecutionOptions.MaxMappingParallelism	Maximum number of parallel threads that process a single mapping pipeline stage. When you set the value greater than one, the Data Integration Service enables partitioning for mappings and for mappings converted from profiles. The service dynamically scales the number of partitions for a mapping pipeline at run time. Increase the value based on the number of CPUs available on the nodes where mappings run. In the Developer tool, developers can change the maximum parallelism value for each mapping. When maximum parallelism is set for both the Data Integration Service and the mapping, the Data Integration Service uses the minimum value when it runs the mapping. Default is 1. Maximum is 64.
ExecutionOptions.MaxMemorySize	Maximum amount of memory, in bytes, that the Data Integration Service can allocate for running all requests concurrently when the service runs jobs in the Data Integration Service process. When the Data Integration Service runs jobs in separate local or remote processes, the service ignores this value. If you do not want to limit the amount of memory the Data Integration Service can allocate, set this property to 0. If the value is greater than 0, the Data Integration Service uses the property to calculate the maximum total memory allowed for running all requests concurrently. The Data Integration Service calculates the maximum total memory as follows: Maximum Memory Size + Maximum Heap Size + memory required for loading program components Default is 0. **Note:** If you run profiles or data quality mappings, set this property to 0.
ExecutionOptions.MaxNativeBatchExecutionPoolSize	Maximum number of deployed jobs that can run concurrently in the native environment. The Data Integration Service moves native mapping jobs from the queue to the native job pool when enough resources are available. Default is 10.
ExecutionOptions.MaxOnDemandExecutionPoolSize	Maximum number of on-demand jobs that can run concurrently. Jobs include data previews, profiling jobs, REST and SQL queries, web service requests, and mappings run from the Developer tool. All jobs that the Data Integration Service receives contribute to the on-demand pool size. The Data Integration Service immediately runs on-demand jobs if enough resources are available. Otherwise, the Data Integration Service rejects the job. Default is 10.

Option	Description
ExecutionOptions.OutOfProcessExecution	Runs jobs in the Data Integration Service process, in separate DTM processes on the local node, or in separate DTM processes on remote nodes. Configure the property based on whether the Data Integration Service runs on a single node or a grid and based on the types of jobs that the service runs. Enter one of the following options: - IN_PROCESS. Runs jobs in the Data Integration Service process. Configure when you run SQL data service and web service jobs on a single node or on a grid where each node has both the service and compute roles. - OUT_OF_PROCESS. Runs jobs in separate DTM processes on the local node. Configure when you run mapping, profile, and workflow jobs on a single node or on a grid where each node has both the service and compute roles. - OUT_OF_PROCESS_REMOTE. Runs jobs in separate DTM processes on remote nodes. Configure when you run mapping, profile, and workflow jobs on a grid where nodes can have a different combination of roles. If you configure this option when the Data Integration Service runs on a single node, then the service runs jobs in separate local processes. Default is OUT_OF_PROCESS.
ExecutionOptions.RejectFilesDirectory	Directory for reject files. Reject files contain rows that were rejected when running a mapping. Default is `<home directory>/reject`. You cannot use the following characters in the directory path: `* ? < > " | ,`
ExecutionOptions.SourceDirectory	Directory for source flat files used in a mapping. Default is `<home directory>/source`. If the Data Integration Service runs on a grid, you can use a shared directory to create one directory for source files. If you configure a different directory for each node with the compute role, ensure that the source files are consistent among all source directories. You cannot use the following characters in the directory path: `* ? < > " | ,`
ExecutionOptions.TargetDirectory	Default directory for target flat files used in a mapping. Default is `<home directory>/target`. Enter a list of directories separated by semicolons to increase performance when multiple partitions write to the flat file target. If the Data Integration Service runs on a grid, you can use a shared directory to create one directory for target files. If you configure a different directory for each node with the compute role, ensure that the target files are consistent among all target directories. You cannot use the following characters in the directory path: `* ? < > " | ,`

Option	Description
ExecutionOptions.TemporaryDirectories	Directory for temporary files created when jobs are run. Default is `<home directory>/disTemp`. Enter a list of directories separated by semicolons to optimize performance during profile operations and during cache partitioning for Sorter transformations. You cannot use the following characters in the directory path: `* ? < > " | , [ ]`
HttpConfigurationOptions.AllowedHostNames	List of constants or Java regular expression patterns compared to the host name of the requesting machine. The host names are case sensitive. Use a space to separate multiple constants or expressions. If you configure this property, the Data Integration Service accepts requests from host names that match the allowed host name pattern. If you do not configure this property, the Data Integration Service uses the Denied Host Names property to determine which clients can send requests.
HttpConfigurationOptions.AllowedIPAddresses	List of constants or Java regular expression patterns compared to the IP address of the requesting machine. Use a space to separate multiple constants or expressions. If you configure this property, the Data Integration Service accepts requests from IP addresses that match the allowed address pattern. If you do not configure this property, the Data Integration Service uses the Denied IP Addresses property to determine which clients can send requests.
HttpConfigurationOptions.DeniedHostNames	List of constants or Java regular expression patterns compared to the host name of the requesting machine. The host names are case sensitive. Use a space to separate multiple constants or expressions. If you configure this property, the Data Integration Service accepts requests from host names that do not match the denied host name pattern. If you do not configure this property, the Data Integration Service uses the Allowed Host Names property to determine which clients can send requests.
HttpConfigurationOptions.DeniedIPAddresses	List of constants or Java regular expression patterns compared to the IP address of the requesting machine. Use a space to separate multiple constants or expressions. If you configure this property, the Data Integration Service accepts requests from IP addresses that do not match the denied IP address pattern. If you do not configure this property, the Data Integration Service uses the Allowed IP Addresses property to determine which clients can send requests.

Option	Description
HttpConfigurationOptions.HTTPProtocolType	Security protocol that the Data Integration Service uses. Enter one of the following values: - HTTP. Requests to the service must use an HTTP URL. - HTTPS. Requests to the service must use an HTTPS URL. - Both. Requests to the service can use either an HTTP or an HTTPS URL. When you set the HTTP protocol type to HTTPS or Both, you enable Transport Layer Security (TLS) for the service. You can also enable TLS for each web service deployed to an application. When you enable HTTPS for the Data Integration Service and enable TLS for the web service, the web service uses an HTTPS URL. When you enable HTTPS for the Data Integration Service and do not enable TLS for the web service, the web service can use an HTTP URL or an HTTPS URL. If you enable TLS for a web service and do not enable HTTPS for the Data Integration Service, the web service does not start. Default is HTTP.
HttpProxyServerOptions.HttpProxyServerDomain	Domain for authentication.
HttpProxyServerOptions.HttpProxyServerHost	Name of the HTTP proxy server.
HttpProxyServerOptions.HttpProxyServerPassword	Password for the authenticated user. The Service Manager encrypts the password. This is required if the proxy server requires authentication.
HttpProxyServerOptions.HttpProxyServerPort	Port number of the HTTP proxy server. Default is 8080.
HttpProxyServerOptions.HttpServerUser	Authenticated user name for the HTTP proxy server. This is required if the proxy server requires authentication.
LoggingOptions.LogLevel	Level of error messages that the Data Integration Service writes to the Service log. Choose one of the following message levels: Fatal, Error, Warning, Info, Trace, or Debug.

Option	Description
MappingServiceOptions.MaxMemPerRequest	The behavior of Maximum Memory Per Request depends on the following Data Integration Service configurations: - The service runs jobs in separate local or remote processes, or the service property Maximum Memory Size is 0 (default). In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to all transformations that use auto cache mode in a single request. The service allocates memory separately to transformations that have a specific cache size. The total memory used by the request can exceed the value of Maximum Memory Per Request. - The service runs jobs in the Data Integration Service process, and the service property Maximum Memory Size is greater than 0. In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to a single request. The total memory used by the request cannot exceed the value of Maximum Memory Per Request. Default is 536,870,912.
MappingServiceOptions.MaxNotificationThreadPoolSize	Allocates the number of threads that send notifications to the client.
Modules.MappingService	Enter false to disable the module that runs mappings and previews. Default is true.
Modules.ProfilingService	Enter false to disable the module that runs profiles and generates scorecards. Default is true.
Modules.RESTService	Enter false to disable the module that runs the REST web service. Default is true.
Modules.SQLService	Enter false to disable the module that runs SQL queries against an SQL data service. Default is true.
Modules.WebService	Enter false to disable the module that runs web service operation mappings. Default is true.
Modules.WorkflowOrchestrationService	Enter false to disable the module that runs workflows. Default is true.
PassThroughSecurityOptions.AllowCaching	Allows data object caching for all pass-through connections in the Data Integration Service. Populates data object cache using the credentials in the connection object. **Note:** When you enable data object caching with pass-through security, you might allow unauthorized access to some data.
ProfilingServiceOptions.ExportPath	Location to export profile results. Enter the file system path. Default is ./ProfileExport.
ProfilingServiceOptions.MaxExecutionConnections	Maximum number of database connections for each profiling job.
ProfilingServiceOptions.MaxPatterns	Maximum number of patterns to display for a profile.

Option	Description
ProfilingServiceOptions.MaxProfileExecutionPoolSize	Maximum number of threads to run profiling.
ProfilingServiceOptions.MaxRanks	Number of minimum and maximum values to display for a profile. Default is 5. Default is 10.
ProfilingServiceOptions.ProfileWarehouseConnectionName	Connection object name for the connection to the profiling warehouse.
RepositoryOptions.RepositoryPassword	User password to access the Model repository.
RepositoryOptions.RepositorySecurityDomain	LDAP security domain name if you are using LDAP. If you are not using LDAP the default domain is native.
RepositoryOptions.RepositoryServiceName	Service that stores run-time metadata required to run mappings and SQL data services.
RepositoryOptions.RepositoryUserName	User name to access the Model repository. The user must have the Create Project privilege for the Model Repository Service.
ResultSetCacheOptions.EnableEncryption	Indicates whether result set cache files are encrypted using 128-bit AES encryption. Valid values are true or false. Default is true.
ResultSetCacheOptions.FileNamePrefix	The prefix for the names of all result set cache files stored on disk. Default is RSCACHE.
SQLServiceOptions.DTMKeepAliveTime	Number of milliseconds that the DTM process stays open after it completes the last request. Identical SQL queries can reuse the open process. Use the keepalive time to increase performance when the time required to process the SQL query is small compared to the initialization time for the DTM process. If the query fails, the DTM process terminates. Must be greater than or equal to 0. 0 means that the Data Integration Service does not keep the DTM process in memory. Default is 0. You can also set this property for each SQL data service that is deployed to the Data Integration Service. If you set this property for a deployed SQL data service, the value for the deployed SQL data service overrides the value you set for the Data Integration Service.

Option	Description
SQLServiceOptions.MaxMemPerRequest	The behavior of Maximum Memory Per Request depends on the following Data Integration Service configurations: - The service runs jobs in separate local or remote processes, or the service property Maximum Memory Size is 0 (default). In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to all transformations that use auto cache mode in a single request. The service allocates memory separately to transformations that have a specific cache size. The total memory used by the request can exceed the value of Maximum Memory Per Request. - The service runs jobs in the Data Integration Service process, and the service property Maximum Memory Size is greater than 0. In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to a single request. The total memory used by the request cannot exceed the value of Maximum Memory Per Request. Default is 50,000,000.
SQLServiceOptions.SkipLogFiles	Prevents the Data Integration Service from generating log files when the SQL data service request completes successfully and the tracing level is set to INFO or higher. Default is false.
SQLServiceOptions.TableStorageConnection	Relational database connection that stores temporary tables for SQL data services. By default, no connection is selected.
WorkflowOrchestrationServiceOptions.DBName	Connection name of the database that stores run-time metadata for workflows.
WorkflowOrchestrationServiceOptions.MaxWorkerThreads	The maximum number of threads that the Data Integration Service can use to run parallel tasks between a pair of inclusive gateways in a workflow. The default value is 10. If the number of tasks between the inclusive gateways is greater than the maximum value, the Data Integration Service runs the tasks in batches that the value specifies. For example, if the Maximum Worker Threads value is 10, the Data Integration Service runs the tasks in batches of ten.
WSServiceOptions.DTMKeepAliveTime	Number of milliseconds that the DTM process stays open after it completes the last request. Web service requests that are issued against the same operation can reuse the open process. Use the keepalive time to increase performance when the time required to process the request is small compared to the initialization time for the DTM process. If the request fails, the DTM process terminates. Must be greater than or equal to 0. 0 means that the Data Integration Service does not keep the DTM process in memory. Default is 5000. You can also set this property for each web service that is deployed to the Data Integration Service. If you set this property for a deployed web service, the value for the deployed web service overrides the value you set for the Data Integration Service.

Option	Description
WSServiceOptions.MaxMemPerRequest	The behavior of Maximum Memory Per Request depends on the following Data Integration Service configurations: - The service runs jobs in separate local or remote processes, or the service property Maximum Memory Size is 0 (default). In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to all transformations that use auto cache mode in a single request. The service allocates memory separately to transformations that have a specific cache size. The total memory used by the request can exceed the value of Maximum Memory Per Request. - The service runs jobs in the Data Integration Service process, and the service property Maximum Memory Size is greater than 0. In this case, Maximum Memory Per Request is the maximum amount of memory, in bytes, that the Data Integration Service can allocate to a single request. The total memory used by the request cannot exceed the value of Maximum Memory Per Request. Default is 50,000,000.
WSServiceOptions.SkipLogFiles	Prevents the Data Integration Service from generating log files when the web service request completes successfully and the tracing level is set to INFO or higher. Default is false.
WSServiceOptions.WSDLLogicalURL	Prefix for the WSDL URL if you use an external HTTP load balancer. For example, http://loadbalancer:8080 The Data Integration Service requires an external HTTP load balancer to run a web service on a grid. If you run the Data Integration Service on a single node, you do not need to specify the logical URL.

UpdateServiceProcessOptions

Updates properties for a Data Integration Service process. To view current properties, run the infacmd dis ListServiceProcessOptions command.

Enter options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd dis UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-Options|-o> options
```

The following table describes infacmd dis UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
NodeName -nn	node_name	Required. Node where the Data Integration Service runs.
-Options -o	options	Required. Enter each option separated by a space. To view the options, run the infacmd dis ListServiceProcessOptions command.

Data Integration Service Process Options

Use the Data Integration Service process options with the infacmd dis UpdateServiceProcessOptions command.

Enter Data Integration Service process options in the following format:

- Separate multiple options with a space.
- Enclose all options and values in double quotation marks.
- Enclose parameters in single quotation marks.

```
... -o "option_type.option_name='value'"
```

The following table describes Data Integration Service process options:

Option	Description
GeneralOptions.JVMOptions	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties.
GeneralOptions.HttpPort	Unique HTTP port number for the Data Integration Service process when the service uses the HTTP protocol.
GeneralOptions.HttpsPort	Unique HTTPS port number for the Data Integration Service process when the service uses the HTTPS protocol.
LoggingOptions.LogDirectory	Directory for Data Integration Service node process logs. Default is `<INFA_HOME>\logs\dislogs`. If the Data Integration Service runs on a grid, use a shared directory to create one directory for log files. Use a shared directory to ensure that if the master service process fails over to another node, the new master service process can access previous log files.
ResultSetCacheOptions.MaxTotalDiskSize	Maximum number of bytes allowed for the total result set cache file storage. Default is 0.

Option	Description
ResultSetCacheOptions.MaxPerCacheMemorySize	Maximum number of bytes allocated for a single result set cache instance in memory. Default is 0.
ResultSetCacheOptions.MaxTotalMemorySize	Maximum number of bytes allocated for the total result set cache storage in memory. Default is 0.
ResultSetCacheOptions.MaxNumCaches	Maximum number of result set cache instances allowed for this Data Integration Service process. Default is 0.
HttpConfigurationOptions.MaxConcurrentRequests	Maximum number of HTTP or HTTPS connections that can be made to this Data Integration Service process. Minimum is 4. Default is 200.
HttpConfigurationOptions.MaxBacklogRequests	Maximum number of HTTP or HTTPS connections that can wait in a queue for this Data Integration Service process. Default is 100.
HttpConfigurationOptions.KeyStoreFile	Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the Data Integration Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority. If you run the Data Integration Service on a grid, the keystore file on each node in the grid must contain the same keys.
HttpConfigurationOptions.KeyStorePassword	Password for the keystore file.
HttpConfigurationOptions.TrustStoreFile	Path and file name of the truststore file that contains authentication certificates trusted by the Data Integration Service. If you run the Data Integration Service on a grid, the truststore file on each node in the grid must contain the same keys.
HttpConfigurationOptions.TrustStorePassword	Password for the truststore file.
HttpConfigurationOptions.SSLProtocol	Secure Sockets Layer protocol to use. Default is TLS.
SQLServiceOptions.MaxConcurrentConnections	Limits the number of database connections that the Data Integration Service can make for SQL data services. Default is 100.

Rules and Guidelines

Refer to the rules and guidelines to use the infacmd dis commands.

Consider the following rules and guidelines when you use the infacmd dis commands:

General Rules and Guidelines

- The timezone attribute accepts values only from java.time.ZoneID(). For example, IST is not supported.

- Passwords that are encrypted using the pmpasswd utility must be encrypted using the option -e=CRYPT_SYSTEM.
- You must have read permissions for an object to query it.
- You cannot query deleted objects, even if the deleted objects are part of a pending changelist on a Model repository that is integrated with a version control system.
- When you compare two mappings, the compare report prints a white space.
- When you compare two mappings and use Blaze as the execution environment, the compare report shows engine as CADIYarnExecutionEngine instead of Blaze.

Application Patch Rules and Guidelines

- When you deploy objects to an application patch archive file, the default location of the file is $INFA_HOME/tomcat/bin/target. If the Data Integration Service is configured to use operating system profiles and you specify the operating system profile, the archive file is written to $DISTargetDir instead.

CHAPTER 14

Infacmd dis Queries

This chapter includes the following topics:

Queries

Use queries to retrieve design-time and run-time objects.

You can retrieve design-time objects from a Model repository or run-time objects that were deployed to a Data Integration Service. To build a query, use query parameters to determine the objects that you want to retrieve. You can make a query more specific by using the where clause and operators.

The following commands accept a query as a command line option:

- compareObject
- deployObjectsToFile
- queryRunTimeObjects
- queryDesignTimeObjects
- replaceAllTag
- tag
- untag

When you pass a query to a command, the command operates only on the objects that the query returns. If you pass the query `name=mapping1` to the command infacmd dis tag, the command assigns tags only to objects with the name `mapping1`.

To pass a query to the commands, specify the query as a string. For example, see the value for the -q option in the command syntax for the following infacmd dis queryDesignTimeObjects command:

```
./infacmd.sh dis queryDesignTimeObjects -dn Domain_v299 -un Administrator
-pd Administrator -rs MRS_v299 -rsun Administrator -rspd Administrator
-q "all" -sn DIS_v299
```

Comparison Operators

Use the comparison operators with query parameters to build a query. You can use comparison operators to specify criteria when you query objects.

The following table lists the comparison operators that you can use with each type of query parameter:

Query Parameter Type	Includes Query Parameters	Comparison Operators	Examples
Subject	name tag createdBy lastModifiedBy	~contains~ ~not-contains~ ~not-ends-with~ ~not-starts-with~ ~ends-with~ ~starts-with~ = != ~in~ ~not-in~	name ~contains~ Mapping tag ~in~ (tg_1, tg_2, tg_3) createdBy = Administrator lastModifiedBy ~ends-with~ visitor
Subject	object type	= != ~in~ ~not-in~	type = Mapping object != Mapping $object_{in}$(P1/F1/Map1,P2/F1/Map2)
Time	lastModifiedTime checkInTime checkOutTime creationTime	> < ~within-last~ ~between~ ~not-between~	lastModifiedTime < 2019-02-26 20:32:54 checkInTime ~between~ (2018-12-26 20:32:54, 2018-05-26 20:32:54) checkOutTime ~within-last~ 10 (days)
Status	versionStatus	~is-checkedin~ ~is-checkedout~	versionStatus ~is-checkedin~ versionStatus ~is-checkedout~
Location	folder project application	~contains~ ~not-ends-with~ ~not-contains~ ~not-starts-with~ ~ends-with~ ~starts-with~ = != ~in~ ~not-in~	name ~contains~ Mapping where project ~ends-with~ _1 lastModifiedBy ~ends-with~ trator where folder ~not-in~ (Folder_3, Folder_2) all where project=Project_1, folder=Folder_1 name = Mapping where project=Project_1, folder=/Folder_1/Folder_2/ name = Mapping where project=Project_1, folder=/ name = captain_america where app~in~ (MapGenTest, MapGenEg)

If you have build a query specifying a criterion by using comparison operators, the query returns the object that satisfies the criterion to the client.

For example, you can build a query to fetch objects that have the name `mapping 1`.

```
name=mapping1
```

Note: The time format is YYYY-MM-DD HH24:MI:SS.

Specifying a Folder Path

Use a recursive or non-recursive folder path to build a query. You can specify the folder path to access objects inside a folder.

You can use the following types of folder paths:

- Recursive. Includes objects in the folder and all subfolders.
- Non-recursive. Includes only the objects inside the root folder.

Folder paths are recursive by default. To specify a non-recursive folder path, use a forward slash at the end of the folder path.

The following table describes sample queries with both recursive and non-recursive folder paths:

Sample Query	Description
name=map1 folder=/	Non-recursive. The query examines only the objects that are nested directly under the project.
name=map1 folder=/f1/f2/	Non-recursive. The query examines only the objects that are located in the path /f1/f2/.
name=map1 folder=f1	Recursive. The query examines all objects that are located in folder f1 and all subfolders within f1.
name=map1 folder=/f1/f2	Recursive. The query examines all objects that are located in the path /f1/f2 and all subfolders of f2.

Note: If you use a forward slash to specify a non-recursive folder path, you can only use the comparison operators `=`, `!=`, `~in~`, and `~not-in~`.

Logical Operators

Use logical operators to test whether one or more conditions in a query are TRUE or FALSE.

You can use the following logical operators:

Logical Operator	Description	Example
!	NOT	! name ~not-starts-with~ M_
&&	AND	name ~starts-with~ map_&& lastModifiedBy ~ends-with~ visitor
||	OR	checkInTime > 2018-12-26 20:32:54 || lastModifiedTime > 2019-02-26 20:32:54

Note: You cannot use logical operators to test location query parameters, including folder names, project names, and application names.

Query Parameters

Use query parameters to query design-time objects in a Model repository and run-time objects that are deployed to a Data Integration Service. You can use subject, time, status, and location to build a query.

Query parameters are divided into the following parameters types:

Subject

Parameters that test a subject such as specific object or user. The following table lists the subject parameters:

Parameter	Object Type	Description
name	Design-time object Run-time object	Name of the object that you want to query. You can specify the name of one of the following types of objects: - Mapping - Physical data object - Parameter set
tag	Design-time object	Tag that is assigned to the object.
createdBy	Design-time object	User that created the object.
lastModifiedBy	Design-time object	User that last modified the object.
type	Design-time object	Filters the type of object.
object	Design-time object	Filters and retrieves objects from a folder. Specify the full path to objects starting from root including the project name, folders, and object name.

Time

Parameters that test the time when an object was changed. The following table lists the time parameters:

Parameter	Object Type	Description
lastModifiedTime	Design-time object	Time when the object was last modified.
checkInTime	Design-time object	Time when the object was last checked in. **Note:** Applies only if the Model repository is integrated with a version control system.
checkOutTime	Design-time object	Time when the object was last checked out. **Note:** Applies only if the Model repository is integrated with a version control system.
creationTime	Design-time object	Time when the object was created.

Status

Parameters that test the status of an object. The following table lists the status parameters:

Parameter	Object Type	Description
versionStatus	Design-time object	Version status of the object. The version status can either be checked in or checked out. **Note:** Applies only if the Model repository is integrated with a version control system.

Location

Parameters that test where an object is located such as specific project, folder, or run-time application. The following table lists the location parameters:

Parameter	Object Type	Description
folder	Design-time object	Folder that contains the object.
project	Design-time object	Project that contains the object.
application	Run-time object	Name of the run-time application that contains the object.

Query Structure

Use parameters, operations, and the where clause to build a query.

You can structure a query by using parameters, comparison operators, logical operators, and the where clause. You can control the query precedence by using parentheses.

A query is structured with the following elements:

Query parameters

Query parameters are categorized into subject, time, status, and location. Each query parameter must be combined with a comparison operator. For example,

```
type = mapping
```

Comparison operators

Comparison operators are used to specify criteria to query objects. Comparison operators are used with the query parameters to build a query.

Logical operators

Logical operators are used to test a condition in a query. Logical operators can have multiple query parameters. For example,

```
type = mapping || createdBy = admin
```

Where clause

The where clause is used to restrict the query scope. For example,

```
name = mapping1 where project = project1, folder = folder1.
```

Where Clause

Use a where clause to restrict the scope of a query.

You can specify only location query parameters inside a where clause. Location query parameters do not support logical operators, so you cannot use logical operators inside the where clause.

For example, the following query locates a mapping within a specific project and folder:

```
name=mapping1 where project1, folder=folder1
```

You can use parentheses outside of the where clause. For example, the following query uses expressions `(name contains super && name ends-with boy)` and `(name contains ragnarok)` that are enclosed in parentheses and are outside of the where clause:

```
(name contains super && name ends-with boy) || (name contains ragnarok) where
project=MapGenTest
```

You can use `all` keyword to locate all design-time objects on a Model repository or all run-time objects that are deployed to a Data Integration Service. You can use `all` keyword with the where clause.

For example, the following query locates all objects within a specific folder:

```
all where folder=Folder_1
```

CHAPTER 15

infacmd dp Command Reference

This chapter includes the following topics:

startSparkJobServer

Starts the Spark Jobserver on the Data Integration Service machine. By default, the Spark Jobserver starts when you preview hierarchical data.

Run this command to manually start the Spark Jobserver in the background to save time when you preview hierarchical data.

The infacmd dp startSparkJobServer command uses the following syntax:

```
startSparkJobServer

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-ConfigurationName|-cn> configuration_name
```

The following table describes infacmd dp startSparkJobServer options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-ConfigurationName -cn	configuration_name	Required. Name of the cluster configuration.

stopSparkJobServer

Stops the Spark Jobserver running on specified Data Integration Service. By default, the Spark Jobserver stops if it is idle for 60 minutes or if the Data Integration Service is stopped or recycled.

The infacmd dp stopSparkJobServer command uses the following syntax:

```
stopSparkJobServer
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd dp stopSparkJobServer options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.

CHAPTER 16

infacmd idp Command Reference

This chapter includes the following topics:

createRepository

Creates a Data Preparation repository.

The infacmd idp createRepository command uses the following syntax:

```
createRepository
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd idp createRepository options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service associated with the Data Preparation repository.

createService

Creates an Interactive Data Preparation Service.

The infacmd idp createService command uses the following syntax:

```
createService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageF
ormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|
INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos
(default simple)),KerberosPrincipal(Principal Name for User
Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
00000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=500
00),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-
Default),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

[<-LicenseName|-ln> license_name]

<-RepositoryServiceName |-rs> repository_service_name

<-RepositoryUser|-rsun> repository_user

[<-RepositoryPassword|-rspd> repository_password]

[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
```

```
<-DISServiceName|-dsn> dis_service_name
<<-HttpPort|-hp> http_port|<-HttpsPort|-hsp> https_port>
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-TruststoreFile|-tsf> truststore_file_location]
[<-TruststorePassword|-tsp> truststore_password]
[<-RulesServerPort|-rpo> RulesServerPort]
[<-SolrPort|-spo> SolrPort]
<-maxHeapSize|-mxhs> maxHeapSize]
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd idp createService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service. You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: - HDFSConnection* - HiveConnection* - HadoopConnection* - HDFSSystemDirectory* - HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)) - LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)) - customLogDirectory - SecurityMode(simple|kerberos (default simple)) - KerberosPrincipal(Principal Name for User Impersonation) - KerberosKeyTabFileName(SPN Keytab File for User Impersonation) - LogAuditEvents(true|false (default false)) - JDBCPort - ZeppelinURL - MaxFileUploadSize(default=512MB) - DownloadRowsSize(default=1000000) - MaxRecommendations(default=10) - MaxSampleSize(default=50000) - SampleSize(default=50000) - hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default) - LocalSystemDirectory* - SolrJVMOptions - IndexDir
-LicenseName -ln	license_name	Optional. License object that allows the use of the service.
-RepositoryServiceName -rs	repository_service_name	Optional. Name of the Model Repository Service that manages the Model repository that contains rule objects and metadata. Set this property if rules are used during data preparation.
-RepositoryUser -rsun	-repository_username	Optional. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.

Option	Argument	Description
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service that runs rules during data preparation. Set this property if rules are used during data preparation.
-HttpPort -hp	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-HttpsPort -hsp	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-KeystoreFile -kf	keystore_file_location	Optional. Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Optional. Password for the keystore file.
-TruststoreFile -tsf	truststore_file_location	Optional. Path and the file name of the truststore file that contains authentication certificates for the HTTPS connection.
-TruststorePassword -tsp	truststore_password	Optional. Password for the truststore file.
-RulesServerPort -rpo	RulesServerPort	Optional. Port used by the rules server managed by the Interactive Data Preparation Service. Set the value to an available port on the node where the service runs.
-SolrPort -spo	SolrPort	Optional. Port number for the Apache Solr server used to provide data preparation recommendations.
-maxHeapSize -mxhs	maxHeapSize	Optional. Heap size to allocate to the service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the service. Must be in the following format: */parent_folder/child_folder*

updateService

Updates Interactive Data Preparation Service properties.

The infacmd idp updateService command uses the following syntax:

```
updateService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageF
ormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|
INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos
(default simple)),KerberosPrincipal(Principal Name for User
Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
00000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=500
00),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-
Default),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

<-RepositoryServiceName |-rs> repository_service_name

<-RepositoryUser|-rsun> repository_user

[<-RepositoryPassword|-rspd> repository_password]

[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]

<-DISServiceName|-dsn> dis_service_name

[<-NodeName|-nn> node_name]

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-ServiceProcessOptions|-po> option_name=value ...(HttpPort, HttpsPort, KeystoreFile,
KeystorePassword, TruststoreFile, TruststorePassword, RulesServerPort, SolrPort,
maxHeapSize ...)]
```

The following table describes infacmd idp updateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service. You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: - HDFSConnection* - HiveConnection* - HadoopConnection* - HDFSSystemDirectory* - HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)) - LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)) - customLogDirectory - SecurityMode(simple|kerberos (default simple)) - KerberosPrincipal(Principal Name for User Impersonation) - KerberosKeyTabFileName(SPN Keytab File for User Impersonation) - LogAuditEvents(true|false (default false)) - JDBCPort - ZeppelinURL - MaxFileUploadSize(default=512MB) - DownloadRowsSize(default=1000000) - MaxRecommendations(default=10) - MaxSampleSize(default=50000) - SampleSize(default=50000) - hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default) - LocalSystemDirectory* - SolrJVMOptions - IndexDir
-RepositoryServiceName -rs	repository_service_name	Optional. Name of the Model Repository Service that manages the Model repository that contains rule objects and metadata. Set this property if rules are used during data preparation.
-RepositoryUser -rsun	-repository_username	Optional. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.

Option	Argument	Description
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service that runs rules during data preparation. Set this property if rules are used during data preparation.
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceProcessOptions -po	option_name=value ...	Optional. Service process properties for the service. In a multi-node environment, infacmd applies these properties to the primary node and backup node.

upgradeRepository

Upgrades the contents of a Data Preparation repository.

The infacmd idp upgradeRepository command uses the following syntax:

```
upgradeRepository
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd idp upgradeRepository options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Interactive Data Preparation Service associated with the Data Preparation repository.

CHAPTER 17

infacmd edp Command Reference

This chapter includes the following topics:

createService

Creates an Enterprise Data Preparation Service.

The infacmd edp createService command uses the following syntax:

```
createService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

[<-Description|-des> description]

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name

[<-BackupNodes|-bn> node_name1,node_name2,...]

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageF
ormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|
INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos
(default simple)),KerberosPrincipal(Principal Name for User
Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
00000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=500
00),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-
Default),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

[<-LicenseName|-ln> license_name]
```

```
[<-HttpPort|-hp> http_port]
[<-HttpsPort|-hsp> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-TruststoreFile|-tf> truststore_file_location]
[<-TruststorePassword|-tp> truststore_password]
[<-FolderPath|-fp> full_folder_path]
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-rsun> repository_user
[<-RepositoryPassword|-rspd> repository_password]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]
<-DataPreparationServiceName|-dpsn> data_preparation_service_name
<-DISServiceName|-dsn> dis_service_name
<-CatalogService|-ct> catalog_service_name
<-CatalogServiceUser|-ctun> catalogservice_user
<-CatalogServicePassword|-ctpd> catalogservice_password
[<-CatalogSecurityDomain|-cssdn> catalog_security_domain]
```

The following table describes infacmd edp createService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service. You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
-Description -des	description	Optional. Description of the service.
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: - HDFSConnection* - HiveConnection* - HadoopConnection* - HDFSSystemDirectory* - HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)) - LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)) - customLogDirectory - SecurityMode(simple|kerberos (default simple)) - KerberosPrincipal(Principal Name for User Impersonation) - KerberosKeyTabFileName(SPN Keytab File for User Impersonation) - LogAuditEvents(true|false (default false)) - JDBCPort - ZeppelinURL - MaxFileUploadSize(default=512MB) - DownloadRowsSize(default=1000000) - MaxRecommendations(default=10) - MaxSampleSize(default=50000) - SampleSize(default=50000) - hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default) - LocalSystemDirectory* - SolrJVMOptions - IndexDir
-LicenseName -ln	license_name	Optional. License object that allows the use of the service.
-HttpPort -hp	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Data Integration Service process. After you create the service, you can define different port numbers for each service process.
-HttpsPort -hsp	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each service process. After you create the service, you can define different port numbers for each service process.

Option	Argument	Description
-KeystoreFile -kf	keystore_file_location	Optional. Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Optional. Password for the keystore file.
-TruststoreFile -tf	truststore_file_location	Optional. Path and the file name of the truststore file that contains authentication certificates for the HTTPS connection.
-TruststorePassword -tp	truststore_password	Optional. Password for the truststore file.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the service. Must be in the following format: */parent_folder/child_folder*
-RepositoryService -rs	repository_service_name	Required. Name of the Model Repository Service to associate with the Enterprise Data Preparation Service.
-RepositoryUser -rsun	-repository_username	Required. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
-DataPreparationServiceName -dpsn	data_preparation_service_name	Required. Name of the Interactive Data Preparation Service to associate with the Enterprise Data Preparation Service.
-DISServiceName -dsn	dis_service_name	Required. Name of the Data Integration Service to associate with the Enterprise Data Preparation Service.
-CatalogService -ct	catalog_service_name	Required. Name of the Catalog Service to associate with the.

Option	Argument	Description
-CatalogServiceUser -ctun	catalogservice_user	Required. User account to use to log in to the Catalog Service.
-CatalogServicePassword -ctpd	catalogservice_password	Optional. Password for the Catalog Service user account.
-CatalogSecurityDomain -cssdn	catalog_security_domain	Optional. Security domain to which the Catalog Service user account belongs.

purgeauditevents

Purges all Enterprise Data Preparation user activity events from the audit database. Optionally purges project history events from the audit database.

For more information about the events logged in the audit database, see the *Informatica Enterprise Data Preparation Administrator Guide*.

The infacmd edp purgeauditevents command uses the following syntax:

```
purgeauditevents
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-AuditDataRetentionPeriod|-rp> audit_data_retention_period_in_weeks
[<-PurgeProjectHistoryEvents|-phe> true|false]
```

The following table describes infacmd edp purgeauditevents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service for which to purge events.
-AuditDataRetentionPeriod -rp	audit_data_retention_period_in_weeks	Required. Number of weeks before the current calendar week for which to retain event data. The command does not purge data for the current calendar week. Specify 0 to retain data for one calendar week and purge prior log data. Specify 1 or greater to retain data for n + 1 calendar weeks and purge prior log data. For example, if you specify 1, the command retains data for two calendar weeks when it performs the purge. Minimum is 0.
PurgeProjectHistoryEvent -phe	true|false	Optional. Purges project history events from the audit database. Set to true to purge project history from the audit database. Default is false.

updateService

Updates an Enterprise Data Preparation Service.

The infacmd edp updateService command uses the following syntax:

```
updateService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-ServiceOptions|-so> option_name=value ...
(HDFSConnection*,HiveConnection*,HadoopConnection*,HDFSSystemDirectory*,HiveTableStorageF
ormat(DefaultFormat|Parquet|ORC (default DefaultFormat)),LogLevel(FATAL|ERROR|WARNING|
INFO|TRACE|DEBUG (default INFO)),customLogDirectory,SecurityMode(simple|kerberos
(default simple)),KerberosPrincipal(Principal Name for User
Impersonation),KerberosKeyTabFileName(SPN Keytab File for User Impersonation),
LogAuditEvents(true|false (default
false)),JDBCPort,ZeppelinURL,MaxFileUploadSize(default=512MB),DownloadRowsSize(default=10
00000),MaxRecommendations(default=10),MaxSampleSize(default=50000),SampleSize(default=500
00),hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-
Default),LocalSystemDirectory*,SolrJVMOptions,IndexDir)

<-NodeName|-nn> node_name | <-GridName|-gn> grid_name
```

```
[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-ServiceProcessOptions|-po> option_name=value ...(httpPort, httpsPort, keystoreFile,
keystorePwd, truststoreFile, truststorePwd...)]

[<-RepositoryService|-rs> repository_service_name]

[<-RepositoryUser|-rsun> repository_user]

[<-RepositoryPassword|-rspd> repository_password]
[<-RepositorySecurityDomain|-rssdn> model_repository_security_domain]

[<-DataPreparationServiceName|-dpsn> data_preparation_service_name]

[<-DISServiceName|-dsn> dis_service_name]

[<-CatalogService|-ct> catalog_service_name]

[<-CatalogServiceUser|-ctun> catalogservice_user]

[<-CatalogServicePassword|-ctpd> catalogservice_password]

[<-CatalogSecurityDomain|-cssdn> catalog_security_domain]
```

The following table describes infacmd edp updateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service. You cannot change the name of the service after you create it. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [

Option	Argument	Description
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the service runs. To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks. You can define the following available service options: - HDFSConnection* - HiveConnection* - HadoopConnection* - HDFSSystemDirectory* - HiveTableStorageFormat(DefaultFormat|Parquet|ORC (default DefaultFormat)) - LogLevel(FATAL|ERROR|WARNING|INFO|TRACE|DEBUG (default INFO)) - customLogDirectory - SecurityMode(simple|kerberos (default simple)) - KerberosPrincipal(Principal Name for User Impersonation) - KerberosKeyTabFileName(SPN Keytab File for User Impersonation) - LogAuditEvents(true|false (default false)) - JDBCPort - ZeppelinURL - MaxFileUploadSize(default=512MB) - DownloadRowsSize(default=1000000) - MaxRecommendations(default=10) - MaxSampleSize(default=50000) - SampleSize(default=50000) - hiveExecutionEngine(MR|Spark|Tez|Cluster-Default (default=Cluster-Default) - LocalSystemDirectory* - SolrJVMOptions - IndexDir
-NodeName -nn	node_name	Required if you do not specify grid name. Node where the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceProcessOptions -po	option_name=value ...	Optional. Service process properties for the service. In a multi-node environment, infacmd applies these properties to the primary node and backup node.
-RepositoryService -rs	repository_service_name	Optional. Name of the Model Repository Service to associate with the Enterprise Data Preparation Service.
-RepositoryUser -rsun	-repository_username	Optional. User account to use to log in to the Model Repository Service.
-RepositoryPassword -rspd	-repository_password	Optional. Password for the Model Repository Service user account.

Option	Argument	Description
-RepositorySecurityDomain -rssdn	model_repository_security_domain	Optional. Security domain to which the Model Repository Service user account belongs.
-DataPreparationServiceName -dpsn	data_preparation_service_name	Optional. Name of the Interactive Data Preparation Service to associate with the Enterprise Data Preparation Service.
-DISServiceName -dsn	dis_service_name	Optional. Name of the Data Integration Service to associate with the Enterprise Data Preparation Service.
-CatalogService -ct	catalog_service_name	Optional. Name of the Catalog Service to associate with the Enterprise Data Preparation Service.
-CatalogServiceUser -ctun	catalogservice_user	Optional. User account to use to log in to the Catalog Service.
-CatalogServicePassword -ctpd	catalogservice_password	Optional. Password for the Catalog Service user account.
-CatalogSecurityDomain -cssdn	catalog_security_domain	Optional. Security domain to which the Catalog Service user account belongs.

upgradeService

Upgrades an Enterprise Data Preparation Service.

The infacmd edp upgradeService command uses the following syntax:

```
upgradeService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd edp upgradeService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Enterprise Data Preparation Service to upgrade.

CHAPTER 18

Infacmd es Command Reference

This chapter includes the following topics:

ListServiceOptions

Returns a list of properties that are configured for the Email Service. To configure Email Service properties, run infacmd es updateServiceOptions. To configure Email Service email server properties, run infacmd es updateSMTPOptions.

The infacmd es listServiceOptions command uses the following syntax:

```
ListServiceOptions

<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: The infacmd program uses the following common options to connect to the domain: domain name, user name, password, security domain, and resilience timeout. The table of options has brief descriptions. To see detailed descriptions, refer to "Connecting to the Domain" on page 63.

The following table describes the infacmd es listServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-UserName -un	user_name	User name to connect to the domain

Option	Argument	Description
-Password -pd	password	Password for the user name.
-ServiceName -sn	service_name	Optional. Enter Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

UpdateServiceOptions

Updates Email Service properties. Run this command to configure domain properties and nodes for the Email Service. To view current Email Service properties, run infacmd es listServiceOptions.

The infacmd es updateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeName|nn> primary node name]
[<-BackupNodes|-bn> backup node names]
```

The following table describes the infacmd es updateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.

Option	Argument	Description
-ServiceName -sn	service_name	Optional. Enter Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-Options -o	options	Enter options in the following format: `OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2` To view valid options, run infacmd isp ListServiceOptions.
-NodeName -nn	primary node name	Optional. Primary node on which the service runs.
-BackupNodes -bn	backup node names	Optional. Nodes on which the service can run if the primary node is unavailable.

UpdateSMTPOptions

Updates the SMTP properties for the Email Service. Business glossaries and workflows use the Email Service SMTP configuration to email notifications.

The following notifications use the Email Service SMTP configuration to send emails:

- Business glossary notifications.
- Scorecard notifications.
- Workflow notifications. Workflow notifications include emails sent from Human tasks and Notification tasks in workflows that the Data Integration Service runs.

The infacmd es updateSMTPOptions command uses the following syntax:

```
UpdateSMTPOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SMTPServerHostName|-sa> smtp_host]
[<-SMTPUsername|-su> smtp_email_password]
[<-SMTPEmailPassword|-se> smtp_email_password]
[<-SMTPEmailAddress|-ss> smtp_email_address]
```

```
[<-SMTPPort|-sp> smtp_port]
[<-SMTPAuthEnabled|-sau> smtp_auth_enabled]
[<-SMTPTLSEnabled|-stls> smtp_tls_enabled]
[<-SMTPSSLEnabled|-sssl> smtp_ssl_enabled]
```

The following table describes the infacmd es updateSMTPOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-ServiceName -sn	service_name	Optional. Enter Email_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-SMTPServerHostName -sa	smtp_host	Optional. The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook. Default is localhost.
-SMTPUsername -su	smtp_user	Optional. The user name for authentication upon sending if required by the outbound mail server.
-SMTPEmailPassword -se	smtp_email_password	Optional. Password for authentication upon sending if required by the outbound SMTP mail server.
-SMTPEmailAddress -ss	smtp_email_address	Optional. Email address that the Email Service uses in the From field when sending notification emails from a workflow. Default is `admin@example.com`.
SMTPPort -sp	smtp_port	Optional. Port number used by the outbound SMTP mail server. Valid values are from 1 to 65535. Default is 25.
-SMTPAuthEnabled -sau	smtp_auth_enabled	Optional. Indicates that the SMTP server is enabled for authentication. If true, the outbound mail server requires a user name and password. If true, you must select whether the server uses the Transport Layer Security (TLS) protocol or the Secure Sockets Layer (SSL) protocol. Enter `true` or `false`. Default is false.

Option	Argument	Description
-SMTPTLSEnabled -stls	smtp_tls_enabled	Optional. Indicates that the SMTP server uses the TLS protocol. If true, enter the TLS port number for the SMTP server port property. Enter `true` or `false`. Default is false.
-SMTPSSLEnabled -sssl	smtp_ssl_enabled	Optional. Indicates that the SMTP server uses the SSL protocol. If true, enter the SSL port number for the SMTP server port property. Enter `true` or `false`. Default is false.

CHAPTER 19

infacmd ics Command Reference

This chapter includes the following topics:

cleanCluster

Cleans the Informatica Cluster Service. If the Catalog Service is custom SSL-enabled, you need to set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".`

Note: See the sample command to encrypt password: $INFA HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

The infacmd ics cleanCluster command uses the following syntax:

```
cleanCluster
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

Note: Verify that the Informatica Cluster Service is in the disabled state before you run the command.

The following table describes infacmd ics cleanCluster options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Informatica Cluster Service name.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

createservice

Creates an Informatica Cluster Service.

The infacmd ics createService command uses the following syntax:

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-HttpPort|-p> port_name]

[<-HttpsPort|-sp> https_port_name]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-SSLProtocol|-sslp> ssl_protocol]

<-GatewayHost|-hgh> FQDN Host name of the node that serves as the gateway to the cluster

[<-DataNodes|-hn> Comma-separated list of fqdn host names that are data nodes of the
cluster. Mandatory if advance config is not enabled]
```

```
<-ProcessingNodes|-pn> Comma-separated list of fqdn host names that are processing nodes
of the cluster

<-GatewayUser|-gu> Username for the Gateway Node. Enable a Passwordless SSH connection
from Informatica Domain to Gateway Host for this user. Must be non-root sudo user

[<-ClusterCustomDir|-ccd> Cluster Custom Dir (default /opt/informatica/ics)]

[<-ClusterSharedFilesystemPath|-csfp> Cluster Shared Filesystem Path]

[<-OtherOptions|-oo> other options (specified in format:
[OptionGroupName.OptionName=OptionValue]. Multiple options can be separated by comma.
OptionValue should be specified within double quotes if it contains a comma.)]

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-NomadServerHosts|-nsh> Nomad Server Hosts]

[<-NomadSerfPort|-nsp> Nomad Server Port (default 4648)]

[<-NomadHttpPort|-nhp> Nomad Http Port (default 4646)]

[<-NomadRpcPort|-nrp> Nomad RPC Port (default 4647)]

[<-NomadServerDir|-nsd> Nomad Server Dir (default $ClusterCustomDir/nomad/nomadserver)]

[<-NomadClientDir|-ncd> Nomad Client Dir (default $ClusterCustomDir/nomad/nomadclient)]

[<-NomadCustomOptions|-nco> Nomad Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.)]

[<-ZookeeperHosts|-zh> Zookeeper Hosts]

[<-ZookeeperPort|-zp> Zookeepr Port (default 2181)]

[<-ZookeeperPeerPort|-zpp> Zookeeper Peer Port (default 2888)]

[<-ZookeeperLeaderPort|-zlp> Zookeeper Leader Port (default 3888)]

[<-ZookeeperInstallDir|-zih> Zookeeper Install Dir (default $ClusterCustomDir/zk/
install)]

[<-ZookeeperDataDir|-zdd> Zookeeper Data Dir (default $ClusterCustomDir/zk/data)]

[<-ZookeeperCustomOptions|-zco> Zookeeper Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.)]

[<-SolrHosts|-sh> Solr Hosts]

[<-SolrPort|-sop> Solr Port (default 8983)]

[<-SolrInstallDir|-sih> Solr Install Dir (default $ClusterCustomDir/solr/install)]

[<-SolrDataDir|-sdd> Solr Data Dir (default $ClusterCustomDir/solr/data)]

[<-SolrCustomOptions|-sco> Solr Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.)]

[<-MongoHosts|-mdh> MongoDB Hosts]

[<-MongoPort|-mdp> MonogDB Port (default 27017)]

[<-MongoLogDir|-mdld> MongoDB Log Dir (default $ClusterCustomDir/mongo/log)]

[<-MongoDataDir|-mddd> MongoDB Data Dir (default $ClusterCustomDir/mongo/data)]

[<-MongoCustomOptions|-mco> MongoDB Custom Options. (specified in format:
```

```
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.)]

[<-PostgresHost|-pgh> Postgres Host]

[<-PostgresPort|-pgp> Postgres Port (default 5432)]

[<-PostgresInstallationDir|-pgdir> Postgres Install Dir (default $ClusterCustomDir/
postgres/install)]

[<-PostgresLogDir|-pgldir> Postgres Log Dir (default $ClusterCustomDir/postgres/log)]

[<-PostgresDataDir|-pgddir> Postgres Data Dir (default $ClusterCustomDir/postgres/data)]

[<-PostgresCustomOptions|-pgco> Postgres Custom Options. (specified in format:
[OptionName=OptionValue]. Multiple options can be separated by comma. OptionValue should
be specified within double quotes if it contains a comma.)]

[<-ElasticHosts|-esh> elastic_hosts]

[<-ElasticHttpPort|-eshp> elastic_httpport]

[<-ElasticTcpPort|-estp> elastic_tcpport]

[<-ElasticLogDir|-esld> elastic_log_dir]

[<-ElasticDataDir|-esdd> elastic_data_dir]

[<-ElasticClusterName|-escn> elastic_cluster_name]

[<-ElasticEnableTls|-etls> elastic_enable_tls true|false (default false)]

[<-ElasticUserName|-eun> elastic_user_name]

[<-ElasticPassword|-epswd> elastic_password]

[<-SparkMasterNode|-smn> spark_master_node]

[<-SparkMasterPort|-smp> spark_master_port]

[<-SparkSlaveNodes|-ssn> spark_slave_nodes]

[<-SparkExecutorCores|-sec> spark_executor_cores]

[<-SparkLogDir|-sld> spark_logdir]

[<-DPMEnable|-dpme> Enable DPM true|false (default false)]

[<-DPMEnableAdvanceConfig|-dpmeadvc> Enable DPM Advance Config true|false (default
false)]

[<-EnableAdvanceConfig|-eadvc> Enable Advance Config true|false (default false)]
```

The following table describes infacmd ics CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Informatica Domain node name.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Informatica Cluster Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-HttpPort -p	port_name	Optional. A unique HTTP port number used for Informatica Cluster Service. The default port number is 9075.
-HttpsPort -sp	https_port_name	Required if you enable the transport layer security. Port number for the HTTPS connection.
-KeystoreFile -kf	keystore_file_location	Required if you select the enable transport layer security. Path and file name of the keystore file. The keystore file contains the keys and certificates required if you use the SSL security protocol with Catalog® Administrator.
-KeystorePassword -kp	keystore_password	Required if you select the enable transport layer security. The password for the keystore file.
-SSLProtocol -sslp	ssl_protocol	Optional. Secure Sockets Layer (SSL) protocol to use.
-GatewayHost -hgh	gateway_host	Required. Fully Qualified Domain Name (FQDN) host name of the node that serves as the gateway to the Informatica cluster.

Option	Argument	Description
-DataNodes -hn	data_nodes	A comma-separated list of FQDN host names that are data nodes of the Informatica cluster. Mandatory if the advance configuration is not enabled.
-ProcessingNodes -pn	processing_nodes	A comma-separated list of FQDN host names that process nodes of the Informatica cluster.
-GatewayUser -gu	gateway_user	The username for the gateway node. Enable a Passwordless SSH connection from the Informatica domain to the gateway host for the current user. The user must be non-root sudo user.
-ClusterCustomDir -ccd	cluster_custom_dir	The custom cluster directory. For example `default /opt/informatica/ics`
-ClusterSharedFilesystemPath -csfp	cluster_shared_filesystem_path	Required if the Informatica Cluster Service is on multi-node set up. The path of the cluster shared filesystem.
-OtherOptions -oo	other_options	Multiple options that can be separated by comma. The option value should be specified within the double quotes if it contains a comma. The specified format is: `[OptionGroupName.OptionName=OptionValue].`
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-NomadServerHosts -nsh	nomad_server_hosts	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the comma-separated Nomad server hosts.
-NomadSerfPort -nsp	nomad_service_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Nomad Server Port. The default is 4648.
-NomadHttpPort -nhp	nomad_http_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Nomad HTTP Port. The default is 4646.

Option	Argument	Description
-NomadRpcPort -nrp	nomad_rpc_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Nomad RPC port. The default is 4647.
-NomadServerDir -nsd	nomad_server_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Nomad Server Directory. For example, `default $ClusterCustomDir/nomad/nomadserver`
-NomadClientDir -ncd	nomad_client_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Nomad Client Directory. For example, `default $ClusterCustomDir/nomad/nomadclient`
-NomadCustomOptions -nco	nomad_custom_options	Optional. Specify the comma-separated option value within the double quotes if the value contains a comma. Specified format: `[OptionName=OptionValue]`
-ZookeeperHosts -zh	zookeeper_hosts	Specify the Zookeeper Hosts with comma-separated values.
-ZookeeperPort -zp	zookeeper_port	Specify the Zookeeper Port. Default is 2181.
-ZookeeperPeerPort -zpp	zookeeper_peer_port	Specify the Zookeeper Peer Port. Default is 2888.
-ZookeeperLeaderPort -zlp	zookeeper_leader_port	Specify the Zookeeper Leader Port. Default is 3888.
-ZookeeperInstallDir -zih	zookeeper_install_dir	Specify the Zookeeper Installation directory: `(default $ClusterCustomDir/zk/install)]`
-ZookeeperDataDir -zdd	zookeeper_data_dir	Specify the Zookeeper data directory: `(default $ClusterCustomDir/zk/data)] .`
-ZookeeperCustomOptions -zco	zookeeper_custom_options	Optional. The comma-separated Zookeeper custom options. Specify the option in the following format: `[OptionName=OptionValue]` Specify the option values within double quotes if the values contain a comma.

Option	Argument	Description
-SolrHosts -sh	solr_hosts	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Solr hosts.
-SolrPort -sop	solr_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Solr port. The default is 8983.
-SolrInstallDir -sih	solr_install_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Solr installation directory. The default is `$ClusterCustomDir/solr/install`.
-SolrDataDir -sdd	solr_data_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Solr data directory. The default is `$ClusterCustomDir/solr/data`
-SolrCustomOptions -sco	solr_custom_options	Optional. Specify the Solr custom options. Specify the options in the following format: `[OptionName=OptionValue]`. Multiple options can be separated by a comma. Specify the option value within the double quotes if the value contains a comma.
-MongoHosts -mdh	mongo_db_hosts	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the MongoDB hosts.
-MongoPort -mdp	mongo_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the MonogDB port. The default port number is 27017.
-MongoLogDir -mdld	mongo_log_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the MongoDB Log Directory. The default is `$ClusterCustomDir/mongo/log`
-MongoDataDir -mddd	mongo_data_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the MongoDB data directory. The default directory is `$ClusterCustomDir/mongo/data`

Option	Argument	Description
-MongoCustomOptions -mco	mongo_custom_options	Optional. Specify the MongoDB custom options. Specify the custom options in the following format: `[OptionName=OptionValue]`. Separate multiple options by a comma. Specify the option value within double quotes if the values contain a comma.
-PostgresHost -pgh	postgres_host	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Postgres host.
-PostgresPort -pgp	postgres_port	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Postgres port. The default port number is 5432.
-PostgresInstallationDir -pgdir	postgres_installation_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Postgres installation directory. The default directory is `$ClusterCustomDir/postgres/install`.
-PostgresLogDir -pgldir	postgres_log_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the postgres log directory. The default directory is `$ClusterCustomDir/postgres/log`.
-PostgresDataDir -pgddir	postgres_data_dir	Required If you enable the advance configuration property "-eadvc" is set to true. Specify the Postgres data directory. The default directory is `$ClusterCustomDir/postgres/data`.
-PostgresCustomOptions -pgco	postgres_custom_options	Optional. Specify the Postgres custom options. Specify the cutom options in the following format: `[OptionName=OptionValue]`. Multiple options can be separated by a comma. Specify the option value within the double quotes if the value contains a comma.
-ElasticHosts -esh	elastic_hosts	Specify the elastic host name of the machine on which Elastic search is installed. You can enter multiple host names separated by commas.

Option	Argument	Description
-ElasticHttpPort -eshp	elastic_httpport	Specify the elastic search port number that Data Privacy Management uses to connect to the Elastic Search Web UI. Default is 9200.
-ElasticTcpPort -estp	elastic_tcpport	Specify the Elastic search port number that Data Privacy Management uses to connect to the Elastic Search application. Default is 9300.
-ElasticLogDir -esld	elastic_log_dir	Specify the elastic log directory. The location to store Elastic Search log files. Default is `/var/log/elasticsearch`.
-ElasticDataDir -esdd	elastic_data_dir	Specify the elastic data directory. The location to store Data Privacy Management data in Elastic Search. Default is `/var/lib/elasticsearch`.
-ElasticClusterName -escn	elastic_cluster_name	Specify the name of the Elastic search cluster.
-ElasticEnableTls -etls	elastic_enable_Tls	Select the option to enable Transport Layer Security (TLS) for the service. The default is false.
-ElasticUserName -eun	elastic_user_name	Specify the Elastic search SSL username.
-ElasticPassword -epswd	elastic_password	Specify the Elastic search SSL password.
-SparkMasterNode -smn	spark_master_node	Specify the name of the Spark master node. This must be the Informatica Cluster Service gateway node.
-SparkMasterPort -smp	spark_master_port	Specify the port number that Data Privacy Management uses to connect to the Spark master node.
-SparkSlaveNodes -ssn	spark_slave_nodes	Specify the Spark slave nodes. Slave nodes are usually on processing nodes. Can be multiple values separated by commas.
-SparkExecutorCores -sec	spark_executor_cores	Number of Spark executor cores used.

Option	Argument	Description
-SparkLogDir -sld	spark_log_dir	Specify the Spark log directory. The location to store Spark log files. Default is `/var/log/spark`.
-DPMEnable -dpme	dpm_enable	Enable User Activity that Informatica Cluster Services uses. The default is false.
-DPMEnableAdvanceConfig -dpmeadvc	dpm_enable_advance_config	Configure the properties of the applications and associated services of DPM. The default is false.
-EnableAdvanceConfig -eadvc	enable_advance_config	Configure the properties of the applications and associated services. The default is false.

ListServiceOptions

Lists options for the Informatica Cluster Service.

The infacmd ics ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ics ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Informatica Cluster Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists process options for the Informatica Cluster Service.

The infacmd ics ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd ics ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Informatica Cluster Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-NodeName -nn	node_name	Required. Name of the node where the service process runs.

shutdownCluster

Shuts down the Informatica Cluster Service and the corresponding services, such as Nomad, Solr, MongoDB, and Postgres SQL. If the Catalog Service is custom SSL-enabled, you need to set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".`

Note: See the sample command to encrypt password: $INFA HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

The infacmd.sh ics shutdownCluster command uses the following syntax:

```
shutdownCluster
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd.sh ics shutdownCluster options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Refers to the name of the Informatica Cluster Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

UpdateServiceOptions

Updates service options for the Informatica Cluster Service. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd ics UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
```

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
[<-PrimaryNode|-nn> node_name]
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

The following table describes infacmd ics UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Informatica Cluster Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter name-value pair separated by spaces. If you applied service pack 10.5.1.1 or any later version, you can configure the SSL protocol for the Informatica Cluster Service to TLS 1.1 or TLS 1.2 using the `GeneralOptions.SSLProtocol` option. Specify any one of the following values: - TLSv1.1 - TLSv1.2
-PrimaryNode -nn	node_name	Optional. Primary node on which the Informatica Cluster Service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the Informatica Cluster Service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

UpdateServiceProcessOptions

Updates service process options for the Informatica Cluster Service. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd ics UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

The following table describes infacmd ics UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Name of the node where the service process runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Informatica Cluster Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter name-value pair separated by spaces.

CHAPTER 20

infacmd ipc Command Reference

This chapter includes the following topics:

ExportToPC

Exports objects from the Model repository or an export file and converts them to PowerCenter objects.

The ExportToPC command converts objects from the Model repository or from an XML file that you exported from the Model repository. You must choose either a Model repository or a source file for export. If you choose both options, the source file option takes precedence. Run ExportToPC command to create an XML file that you can import into PowerCenter with the pmrep program.

The infacmd ipc ExportToPC command uses the following syntax:

```
ExportToPC
<-Release|-rel> release_number
[<-SourceFile|-sf> source_file]
[<-SourceRepository|-sr> source_repository]
[<-SourceFolders|-f> folder1 folder2|<-SourceObjects|-so> source_objects]
[<-Recursive|-r>]
[<-TargetLocation|-tl> target_location]
[<-TargetFolder|-tf> target_folder_name]
[<-CodePage|-cp> target_code_page]
[<-Check|-c>]
[<-ReferenceDataLocation|-rdl> reference_data_output_location]
[<-ConvertMappletTargets|-cmt>]
[<-ConvertMappingsToMapplets|-cmm>]
[<-NoValidation|-nv>]
[<-DSTErrorFormat|-def>]
```

```
[<-OptimizationLevel|- O optimization_level 1 or Optimization_level 2]
```

The following table describes infacmd ipc ExportToPC command options and arguments:

Option	Argument	Description
-Release -rel	release_number	Required. The PowerCenter release number.
-SourceFile -sf	source_file	Optional. The full path to an XML file containing source objects that you exported with the Developer tool.

-SourceRepository
-sr
	source_repository	Optional. The Model repository that contains the objects to export to PowerCenter.
		To specify the gateway host and port to connect to the Model Repository Service, use the following command syntax in a non-Kerberos domain:
		`<Model repository name>@<host>:<port>#<projectname>?user=<username>[&namespace=<namespace>]&password=<password>`
		To specify the domain name when you have multiple gateway nodes, use the following command syntax to establish a resilient connection to the Model Repository Service in a non-Kerberos domain:
		`<Model repository name>@<domainname>#<projectname>?user=<username>[&namespace=<namespace>]&password=<password>`
		To specify the domain name with the logged-in credentials, use the following command syntax to run the command with single sign on:
		`<Model repository name>@<domainname>#<projectname>?isloggedinuser=true[&namespace=<namespace>]`
		To specify the gateway host and port with the logged-in credentials, use the following command syntax to run the command with single sign on:
		`<Model repository name>@<host>:<port>#<projectname>?isloggedinuser=true[&namespace=<namespace>]`
		To specify the gateway host and port with the user credentials you specify instead of the logged-in credentials, use the following command syntax in a Kerberos domain:
		`<Model repository name>@<host>:<port>#<projectname>?iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm>`
		To specify the domain name with the user credentials you specify instead of the logged-in credentials, use the following command syntax in a Kerberos domain:
		`<Model repository name>@<domainname>#<projectname>?iskerberos=true&user=<username>[&namespace=<namespace>]&password=<password> &Kerberosrealm=<kerberosrealm>`
		The port parameter is the HTTP port. The &namespace parameter is optional. The default namespace is native.

Option	Argument	Description
-SourceFolders -f	source_folders	If you use -sr, you must use -f or -so. List of source folders that you want to export from the Model repository. You can export mapplets, mappings, and logical data object models from the source folders to PowerCenter. If you export more than one object, you must separate each object in the list with a space.
SourceObjects -so	source_objects	If you use -sr, you must use -f or -so. List of source objects that you want to export from the Model repository. You can export mapplets, mappings, and logical data object models to PowerCenter. You can describe the object as a name. Use the following syntax: `name=/<path>/<objectname>[&type=<typename>]` You must include the full path of the object. If you export more than one object, you must separate each object in the list with a space. You can enter the following types: - Mapping. Use to export mapping and mapplets. - DataObjectModel. Use to export logical data object models. The type is not case sensitive. Default is Mapping.
-Recursive -r	-	Optional. Exports all mappings and logical data object models from the source folders. Exports each subfolder below the objects, and any subfolders below that. Default is false.
-TargetLocation -tl	target_location	Optional. The full path to the target XML file.
-TargetFolder -tf	target_folder_name	Optional. The PowerCenter folder to export the objects to. The ExportToPC command places the folder name in the target XML file. If you do not configure a folder name, the ExportToPC command creates a folder name.
-CodePage -cp	target_code_page	Optional. Code page of the PowerCenter repository. Default is UTF-8.
-Check -c	-	Optional. Tests the conversion without creating a target file. Default is false.
-ReferenceDataLocation -rdl	reference_data_output_location	Optional. Location where you want to save reference table data. The ExportToPC command saves the reference table data as one or more dictionary .dic files.
-ConvertMappletTargets -cmt	-	Optional. Converts targets in mapplets to output transformations in the PowerCenter mapplet. PowerCenter mapplets cannot contain targets. If the export includes a mapplet that contains a target and you do not select this option, the export fails. Default is false.
-ConvertMappingstoMapplets -cmm	-	Optional. Converts Developer tool mappings to PowerCenter mapplets. The Developer tool converts sources and targets in the mappings to Input and Output transformations in a PowerCenter mapplet. Default is false.

Option	Argument	Description
-NoValidation -nv	-	Optional. The ExportToPC command does not validate source objects before converting them. Default is false.
-DSTErrorFormat -def	-	Optional. The error messages appear in a format that the Developer tool can parse. The full path of each object displays in the error messages. Default is to display errors in a user-friendly format.
OptimizationLevel - O	optimization_level	Optional. Controls the optimization methods that the Data Integration Service applies to the mapping. Enter the numeric value that is associated with the optimization level that you want to configure. Enter one of the following numeric values: - 0 (None). The Data Integration Service does not apply any optimization. - 1 (Minimal). The Data Integration Service applies the early projection optimization method. - 2 (Normal). The Data Integration Service applies the early projection, early selection, branch pruning, push-into, pushdown, and predicate optimization methods. Normal is the default optimization level. - 3 (Full). The Data Integration Service applies the cost-based, early projection, early selection, branch pruning, predicate, push-into, pushdown, and semi-join optimization methods. If you do not use this option, the Data Integration Service applies the optimization level configured in the mapping properties for the deployed application in the Administrator tool.

ImportFromPC

Converts a PowerCenter repository object XML file to a Model repository object XML file. Export PowerCenter repository objects to an XML file. Run the importFromPC command to create a target XML file with objects that you can import into a Model repository.

You can import the target XML file to a Model respository with the infacmd tools ImportObjects command or from the Developer tool. If you use the command line to import the target XML file, ImportFromPC does not assign connections to the Model repository objects in the target XML file. You can assign connections with the infacmd oie ImportObjects command or from the Developer tool.

The infacmd ipc importFromPC command uses the following syntax:

```
importFromPC

<-Release|-rel> release_number

[<-SourceFile|-sf> source_file]

[<-TargetFile|-tf> target_location]

[<-Check|-c>]

[<-Db2Type|-dt> default_db2_type]

[<-Db2TypesFile|-df> db2_types_file]

[<-DefaultLookUpConType|-dl> default_lookup_con_type]
```

```
[<-LookUpConTypesFile|-lcf> lookup_connection_types_file]

[<-ConvertOverriddenProps|-orprops> recreate_transformation_with_overridden_properties_
in_mappings]

[<-LogFile|-lf> log_file]
```

The following table describes infacmd ipc ImportFromPC command options and arguments:

Option	Argument	Description
-Release -rel	release_number	Required. The version of the Model repository.
-SourceFile -sf	source_file	Required. The full path to a PowerCenter XML file containing the source objects.
-TargetFile -tf	target_location	Required if you do not specify -Check or -c. The full path to a target XML file.
-Check -c	-	Optional. Tests the conversion without creating a target file. When you test object conversion, you do not require target location.
-Db2Type -dt	default_db2_type	Optional. The DB2 subsystem type used for conversion. You can specify either Db2Type or Db2TypesFile, or both. If you specify both Db2Type and Db2TypesFile for IBM DB2 objects, the DB2 source and target that are not listed in the Db2TypesFile gets converted to the Db2Type. If you do not specify a DB2 subsystem type, the default DB2 subsystem type is used. Default is LUW.
-Db2TypesFile -df	db2_types_file	Optional. A property file that contains the PowerCenter DB2 source and Db2 subsystem type. You can use a Db2 types file if the Db2 source and target are from different subsystems such as LUW, z/OS, or i/OS. You can specify either Db2Type or Db2TypesFile, or both. If you specify both Db2Type and Db2TypesFile for IBM DB2 objects, the DB2 source and target that are not listed in the Db2TypesFile gets converted to the Db2Type. If you do not specify the DB2 subsystem type, the default DB2 subsystem type is used. Default is LUW.
-DefaultLookUpConType -dl	default_lookup_con_type	Optional. The lookup connection type used for conversion. You can specify either DefaultLookUpConType or LookUpConTypesFile, or both. If you specify both DefaultLookUpConType and LookUpConTypesFile for the lookup objects, the Lookup transformations that are not listed in the LookUpConTypesFile are converted to the DefaultLookUpConType. If you do not specify the DefaultLookUpConType for a lookup object during conversion, the default connection type is used. Default is ODBC.

Option	Argument	Description
-LookUpConTypesFile -lcf	lookup_connection_type_file	Optional. A property file that contains the lookup source and the lookup connection type. You can use a lookup connection type file if the lookup objects are from different databases, such as Oracle or IBM DB2. You can specify either DefaultLookUpConType or LookUpConTypesFile, or both. If you specify both the files for the lookup objects, the Lookup transformations that are not listed in the LookUpConTypesFile converts to the DefaultLookUpConType. If you do not specify the DefaultLookUpConType for a lookup object during conversion, the default connection type is used. Default is ODBC.
-ConvertOverridenprops -orprops	True|False	Optional. Preserves override properties for reusable PowerCenter source, target, and transformations during conversion. The command creates nonreusable transformations for PowerCenter transformations with override properties. It also creates reusable data objects for PowerCenter sources and targets with override properties. Valid values are True or False. Default is True.
-LogFile -lf	log_file	Optional. Path and file name of the output log file. Default is STDOUT.

genReuseReportFromPC

Generates a report that estimates how many PowerCenter mappings can be reused in the Model repository for a native or Hadoop environment. You can generate the report as a PDF or Excel file.

Note: If you generate the report as an Excel file, click **Enable Content** in the message bar to load all sheets.

Before you run the infacmd ipc genReuseReportFromPC command, verify that you complete the following tasks:

- Configure the required environment variables for the pmrep command.
- If you use a Linux environment, grant the read, write, and execute permissions on each release folder located in the following directory: `<informatica server installation directory>/tools/pcutils`

The infacmd ipc genReuseReportFromPC command uses the following syntax:

```
genReuseReportFromPC
<-RepositoryName|-r> Pc_Repository_Name
<-HostName|-h> Pc_Domain_HostName
<-PortNumber|-o> Pc_Domain_PortNumber
[<-UserName|-n> Domain_UserName]
[<-Password|-x> Domain_Password]
[<-SecurityDomain|-s> Pc_Repository_Security_domain]
```

```
<-folderNames|-f> Pc_Folder_Names

<-SrcRelease|-srel> Pc_Release_version

[<-targetRelease|-trel> Target_Release_version]

[<-CodePage|-cp>  Pc_Repository_code_page]

<-targetDir|-td> Target_Directory

<-authenticationType|-at> authentication_Type

[<-LogFile|-lf> Log_file_Name]

[<-Font> Font_to_use_for_PDF]

[<-ExecutionEnvironment|-execMode> Execution_Environment]

[<-BlockSize> Block_Size]
```

The following table describes infacmd ipc genreusereportfrompc command options and arguments:

Option	Argument	Description
-RepositoryName -r	Pc_Repository_Name	Required. The PowerCenter repository name.
-HostName -h	Pc_Domain_HostName	Required. The host name of the PowerCenter repository.
-PortNumber -o	Pc_Domain_PortNumber	Required. The port number of the gateway node.
-UserName -n	Domain_UserName	Optional. User name of the PowerCenter domain. If you do not enter a user name, the command uses the value in the INFA_DEFAULT_DOMAIN_USER environment variable.
Password -x	Domain_Password	Optional. Password of the PowerCenter domain. If you do not enter a user name, the command uses the value in the INFA_DEFAULT_DOMAIN_PASSWORD environment variable.
-SecurityDomain -s	Pc_Repository_Security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. If you do not enter a security domain, the command uses the value in the INFA_DEFAULT_SECURITY_DOMAIN environment variable. You can use Native, LDAP, or SSO as the value. The default value is Native.
-folderNames -f	Pc_Folder_Names	Required. PowerCenter folders that contain the objects to be reused. The folder names can contain expressions. The folder names can contain * as expressions. **Note:** If you use the Linux environment, you cannot use $ in the folder name.

Option	Argument	Description

-SrcRelease
-srel
	Pc_Release_version	Required. The release associated with the PowerCenter repository.
		Enter the version in the following format:
		`10.x.x`
		For example, enter a version in the following format:
		`10.2.0`

-targetRelease
-trel
	Target_Release_version	Optional. The release associated with the Model repository. If you do not enter a version, the command uses the product version. You can enter versions from 10.0.0 and above.
		Enter the version in the following format:
		`10.x.x`
		For example, enter a version in the following format:
		`10.2.1`

-CodePage -cp	Pc_Repository_code_page	Optional. Code page of the PowerCenter repository. Default is UTF-8.

-targetDir
-td
	Target_Directory	Required. Location of the target directory on the machine on which the infacmd client and server runs. You must have the read, write, and execute permissions on the target directory folder.
		For example, enter the infacmd client location in the following format:
		`installed_location_of_client\clients\DeveloperClient\infacmd`
		For example, enter the infacmd server location in the following format:
		`installed_location_of_server\isp\bin`
		Note: On a Linux machine, you cannot use $ in the target directory name.

authenticationType -at	authentication_Type	Required. The type of user authentication for the domain. Enter one of the following values: LDAP, Native, or Kerberos Single Sign On.
-LogFile -lf	Log_file_Name	Optional. Name of the generated log file. If you do not enter a name, the command prints the logs on the console. Uses the value of file_path/file_name. If you enter a file name, the log file with the same name appears in the infacmd folder. If you enter a directory path that is not valid, the log file with the path name appears in the infacmd folder. For example, if you enter x as the directory path, the log file named x appears in the infacmd folder.
-Font	Font_to_use_for_PDF	Optional. The location for the font file to have Unicode characters in the report.

Option	Argument	Description
-ExecutionEnvironment -execMode	Execution_Environment	Optional. The run-time engine in the Hadoop environment. The report validates mappings based on the run-time engine that you choose. You can use Blaze or Spark as the value. If you do not enter a value, the report will run against all engines and include only the engine with the fewest errors.
-BlockSize	Block_Size	Optional. The number of mappings that you want to run the infacmd ipc genReuseReportFromPC command against. If you do not enter a value, the report runs and converts all the mappings within each folder at a time. When the memory required to run the command is unavailable, use the -BlockSize option to control the number of mappings instead of running the command on all the mappings in the repository.

CHAPTER 21

infacmd isp Command Reference

The infacmd isp program administers the Informatica domain, the security, and the PowerCenter application services. You can enable and disable Informatica services with infacmd isp commands.

This chapter includes the commands that you can use with the infacmd isp program.

AddAlertUser

Subscribes a user to alert notification emails. Before you can subscribe any user to alerts, you must configure SMTP settings for the outgoing mail server. You can run infacmd isp AddAlertUser for any user.

When you subscribe to alerts, you receive domain and service notification emails for the objects on which you have permission.

The infacmd isp AddAlertUser command uses the following syntax:

```
AddAlertUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

[<-SecurityDomain|-sdn> security_domain]

<-Password|-pd> password

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-AlertUser|-au> user_name
```

The following table describes infacmd isp AddAlertUser options and arguments:

Option	Argument	Description
–DomainName –dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
–ResilienceTimeout –re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
–AlertUser –au	user_name	Required. Name of user you want to subscribes to alerts.

Related Topics:

- "UpdateSMTPOptions" on page 718

AddConnectionPermissions

Assigns connection permissions to a user or group.

The infacmd isp AddConnectionPermissions command uses the following syntax:

```
AddConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name

[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

The following table describes infacmd isp AddConnectionPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RecipientUserName -run	recipient_user_name	Required if you do not specify the recipient group name. Name of the user to whom the connection permission is assigned.
-RecipientGroupName -rgn	recipient_group_name	Required if you do not specify the recipient user name. Name of the group to whom the connection permission is assigned.
-RecipientSecurityDomain -rsd	recipient_security_domain_name	Required if recipient belongs to an LDAP security domain. Name of the security domain that the recipient belongs to. Default is Native.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection
-Permission -p	permission	Required. Type of permission to assign. Enter one or more of the following values separated by spaces: - READ - WRITE. Read and Write - EXECUTE - GRANT. Read and Grant - ALL. Read, Write, Execute Grant

addCustomLDAPType

Adds a custom LDAP type that defines an LDAP directory service from which you import users into an LDAP security domain.

The infacmd isp addCustomLDAPType command uses the following syntax:

```
addCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
<-DisplayName|-dpn> display_name
<-Uid> uid
[<-GroupMembershipAttr|-gm> group_membership_attr]
[<-GroupDescriptionAttr|-gd> group_description_attr]
[<-UserSurnameAttr|-usn> user_surname_attr]
[<-UserGivenNameAttr|-ugn> user_given_name_attr]
[<-UserEmailAttr|-ue> user_email_attr]
[<-UserEnableAttr|-uen> user_enable_attr]
[<-UserTelephoneAttr|-utn> user_telephone_attr]
[<-UserDescriptionAttr|-ud> user_description_attr]
[<-CN> cn]
[<-FetchRangedAttr|-fr> fetch_ranged_attr]
```

The following table describes infacmd isp addCustomLDAPType options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
- -CustomLDAPTypeName -lt	custom_LDAP_type_name	Required. Name of the custom LDAP type.

Option	Argument	Description
- -DisplayName -dpn	display_name	Required. Name of the custom LDAP type displayed in the Administrator tool.
-Uid	uid	Required. Name of the attribute in the LDAP directory service that contains the unique identifier (UID) that the Service Manager uses to identify users.
- -GroupMembershipAttr -gm	group_membership_attr	Optional. Name of the attribute in the LDAP directory service that contains group membership information for a user.
-GroupDescriptionAttr -gd	group_description_attr	Optional. Name of the attribute in the LDAP directory service that contains descriptive text about the groups in the directory service.
-UserSurnameAttr -usn	user_surname_attr	Optional. Name of the attribute in the LDAP directory service that contains the last name for a user.
-UserGivenNameAttr -ugn	user_given_name_attr	Optional. Name of the attribute in the LDAP directory service that contains the first name for a user.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name of the attribute in the LDAP directory service that contains the names of groups in the directory service.
--UserEmailAttr -ue	user_email_attr	Optional. Name of the attribute in the LDAP directory service that contains the email address for a user.
-UserEnableAttr -uen	user_enable_attr	Optional. Name of the attribute in the LDAP directory service that contains
- UserTelephoneAttrr -utn	user_telephone_attr	Optional. Name of the attribute in the LDAP directory service that contains th telephone number for a user.
- User DescriptionAttrr -ud	user_description_attr	Optional. Name of the attribute in the LDAP directory service that contains a description for a user.
-CN	cn	Optional. Name of the attribute in the LDAP directory service that contains the attribute that holds the full name or common name for a user.
- FetchRangedAttr -fr	fetch_ranged_attr	Optional. Set to true to retrieve all of the values contained in multivalued attributes. Use this option with Microsoft Active Directory only.

AddDomainLink

Adds a link to a domain. records connection properties to a remote, or linked, domain so that you can exchange repository metadata between the local domain and the linked domain.

You may want to add a link to a domain if you need to access a PowerCenter Repository Service in that domain.

You can add a link to another Informatica domain when you register or unregister a local repository with a global repository in another Informatica domain.

The infacmd isp AddDomainLink command uses the following syntax:

```
AddDomainLink
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LinkedDomainName|-ld> linked_domain_name
<-DomainLink|-dl> domain_host1:port domain_host2:port...
```

The following table describes infacmd isp AddDomainLink options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the local domain.
–ResilienceTimeout –re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the local domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
–LinkedDomainName –ld	linked_domain_name	Required. Name of the domain that you want to establish a connection with.
–DomainLink –dl	gateway_host1:port gateway_host2:port ...	Required. The host names and port numbers for the gateway nodes in the linked domain.

AddDomainNode

Adds a node to the domain. Before you can start the node, you must define it by running infasetup DefineGatewayNode or DefineWorkerNode on the node.

The infacmd isp AddDomainNode command uses the following syntax:

```
AddDomainNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-FolderPath|-fp> full_folder_path]
```

```
[<-EnableServiceRole|-esr> true|false]
[<-EnableComputeRole|-ecr> true|false]
```

The following table describes infacmd isp AddDomainNode options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node you want to add to the domain.

Option	Argument	Description
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to add the node. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).
-EnableServiceRole -esr	true | false	Optional. Enables the service role on the node. If true, application services can run on the node. If false, application services cannot run on the node. Set to false only if the node is assigned to a Data Integration Service grid and you want to dedicate the node to running mappings. Default is true.
-EnableComputeRole -esr	true | false	Optional. Enables the compute role on the node. If true, the node can perform computations requested by remote application services. If false, the node cannot perform computations requested by remote application services. A node requires the compute role when the Data Integration Service runs jobs on the node. If the Data Integration Service does not run jobs on the node, you can disable the compute role. However, enabling or disabling the compute role does not have a performance impact. Default is true.

AddGroupPrivilege

Assigns a privilege to a group in the domain. You can assign privileges to a group for the domain. You can also assign group privileges for each application service in the domain.

The infacmd isp AddGroupPrivilege command uses the following syntax:

```
AddGroupPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-ServiceName|-sn> service_name
<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp AddGroupPrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. Security domain is case sensitive. Default is Native.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group to which you are assigning the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group to which you are assigning the privilege belongs to. Default is Native.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

-PrivilegePath
-pp
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "\" before it as follows:
		`"Model/View Model/Export\/Import Models"`

addLDAPConnectivity

Configures a connection to an LDAP server. If you specify a security domain, the Service Manager imports users and groups from the LDAP directory service into the security domain.

The infacmd isp addLDAPConnectivity command uses the following syntax:

```
addLDAPConnectivity

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LDAPAddress|-la> ldap_server_address

[<-LDAPPrincipal|-lp> ldap_principal]

[<-LDAPCredential|-lc> ldap_credential]

[<-UseSSL|-us> use_ssl]

[<-TrustLDAPCertificate|-tc> trust_ldap_certificate]

<-LDAPType|-lt> ldap_types=MicrosoftActiveDirectory, MicrosoftAzureActiveDirectory,
SunJavaSystemDirectory, NovellE-Directory, IBMTivoliDirectory, OpenLDAP,
OracleDirectoryServerODSEE, OracleUnifiedDirectory, <Custom LDAP Type Name>

[<-MaxSecurityDomainSize|-ms> Max_Security_Domain_size]

[<-GroupMembershipAttr|-gm> LDAP_Group_Membership_Attribute]

[<-LDAPNotCaseSensitive|-lnc> ldap_not_case_sensitive]

<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

The following table describes infacmd isp addLDAPConnectivity options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LDAPAddress -la	ldap_server_address	Required. Host name and port number for the machine hosting the LDAP directory service. Typically, the LDAP server port number is 389. If the LDAP server uses SSL, the LDAP server port number is 636.

Option	Argument	Description
-LDAPPrincipal -lp	ldap_principal	Optional. Distinguished name (DN) for the principal user. Omit this option to log in as an anonymous user. For more information, refer to the documentation for the LDAP directory service.
-LDAPCredential -lc	ldap_credential	Optional. Password for the principal user. You can set a password with the -lc option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -lc option takes precedence. Omit this option to log in as an anonymous user.
-UseSSL -us	use_ssl	Optional. If you include the option, the LDAP directory service uses Secure Socket Layer (SSL) protocol.
-TrustLDAPCertificate -tc	trust_ldap_certificate	Optional. If you include the option, PowerCenter connects to the LDAP server without verifying the SSL certificate. If you do not include the option, PowerCenter verifies that the SSL certificate is signed by a Certificate Authority before connecting to the LDAP server
-LDAPType -lt	ldap_types=value	Required. Type of LDAP directory service. Directory services include: - MicrosoftActiveDirectory - Microsoft Azure Active Directory - SunJavaSystemDirectory - NovellE-Directory - IBMTivoliDirectory - OpenLDAP - Oracle Directory Server (ODSEE) - Oracle Unified Directory If you use a custom LDAP directory service, specify the name of the service.
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Optional. Maximum number of user accounts to import into a security domain. Default is 1000.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name of the attribute that contains group membership information for a user.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Optional. Indicates that the user names from the LDAP directory service are not case sensitive. Default is false.
LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Required. The name of the LDAP configuration.

AddLicense

Adds a license to the domain. After you add a license, you can assign it to an application service using the AssignLicense command. You must assign a license to a service before you can use the service.

The infacmd isp AddLicense command uses the following syntax:

```
AddLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> securitydomain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-LicenseKeyFile|-lf> license_key_file
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd isp AddLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: `/ * ? < > " |`
-LicenseKeyFile -lf	license_key_file	Required. Path to the license key file.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to add the license. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).

AddNamespace

Creates an LDAP security domain and sets the filters to search for users or groups in the directory service. Creates the LDAP security domain if the Informatica domain uses LDAP or Kerberos authentication.

The infacmd isp AddNamespace command uses the following syntax:

```
AddNamespace
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NameSpace|-ns> namespace

[<-UserSearchBase|-usb> usersearchbase]

[<-UserFilter|-uf> userfilter]

[<-GroupSearchBase|-gsb> groupsearchbase]

[<-GroupFilter|-gf> groupfilter]

<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

The following table describes infacmd isp AddNamespace options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd tries to establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If you do not specify the environment variable, the default value used is 180 seconds.
-NameSpace -ns	namespace	Required. Name of the LDAP or Kerberos security domain that you want to add. The name is not case sensitive and must be unique within the domain. The name cannot contain spaces or any of the following special characters: , + / < > @ ; \ % ? The name cannot exceed 128 characters. The name can contain an ASCII space character except for the first and last character. You cannot use any other space characters.
-UserSearchBase -usb	usersearchbase	Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The LDAP directory service searches for an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName. The series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.
-UserFilter -uf	userfilter	An LDAP query string that specifies the search criteria to search for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: The filter `(objectclass=*)` searches all objects. The filter `(&(objectClass=user)(!(cn=susan)))` searches all user objects except “susan.” For more information about search filters, see the documentation for the LDAP directory service.
-GroupSearchBase -gsb	groupsearchbase	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
-GroupFilter -gf	groupfilter	An LDAP query string that specifies the criteria for searching for groups in the directory service.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Required. The name of the LDAP configuration associated with the security domain.

AddNodeResource

Adds a custom resource or a file directory resource to a node.

When a PowerCenter Integration Service runs on a grid, the Load Balancer can use resources to distribute Session, Command, and predefined Event-Wait tasks. If the PowerCenter Integration Service is configured to check resources, the Load Balancer distributes tasks to nodes where the resources are added and enabled.

The infacmd isp AddNodeResource command uses the following syntax:

```
AddNodeResource
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
<-ResourceType|-rt> resource_type("Custom", "File Directory")
<-ResourceName|-rn> resource_name
[<-ResourceValue|-rv> resource_value]
```

The following table describes infacmd isp AddNodeResource options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node where you want to add a resource.
-ResourceCategory -rc	resource_category	Optional. Category of the resource. Valid categories include: - PCIS. Resource for the PowerCenter Integration Service. - DIS. Reserved for future use. Default is PCIS.
-ResourceType -rt	resource_type	Required. Type of resource. Valid types include: - Custom - File Directory
-ResourceName -rn	resource_name	Required. Name of the resource. The name cannot exceed 79 characters, have leading or trailing spaces, or contains carriage returns, tabs, or the following characters: \ / * ? < > " | $
-ResourceValue -rv	resource_value	Optional. Reserved for future use.

AddRolePrivilege

Assigns a privilege to a role in the domain. You can assign privileges to a role for the domain. You can also assign role privileges for each application service in the domain.

The infacmd isp AddRolePrivilege command uses the following syntax:

```
AddRolePrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
<-ServiceType|-st> service_type AS|CMS|DIS|DOMAIN|LDM|MM|MRS|RS|SATS|SCH|TDM|TDW
<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp AddRolePrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RoleName -rn	role_name	Required. Name of the role to which you are assigning the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ServiceType -st	service_type	Required. Domain or application service type to which you assign the privilege for the role. Service types include: - AS. Analyst Service - CMS. Content Management Service - CS. Catalog Service - DIS. Data Integration Service - DOMAIN. Domain - MM. Metadata Manager Service - MRS. Model Repository Service - RS. PowerCenter Repository Service - TDM. Test Data Manager Service - TDW. Test Data Warehouse Service - SATS. Secure At Source Service. - SCH. Scheduler Service

-PrivilegePath
-pp
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "/"before it as follows:
		`"Model/View Model/Export\/Import Models"`

AddServiceLevel

Adds a service level.

Service levels establish priority among tasks that are waiting to be dispatched. You can create different service levels that a task developer can assign to workflows.

Each service level you create has a name, dispatch priority, and maximum dispatch wait time. The dispatch priority is a number that establishes the priority for dispatch. The Load Balancer dispatches high priority tasks before low priority tasks. The maximum dispatch wait time specifies the amount of time the Load Balancer waits before it changes the dispatch priority for a task to the highest priority.

The infacmd isp AddServiceLevel command uses the following syntax:

```
AddServiceLevel

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> securitydomain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceLevelName|-ln> service_level_name

<-ServiceLevel|-sl> option_name=value ...
```

The following table describes infacmd isp AddServiceLevel options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceLevelName -ln	service_level_name	Required. Name of the service level.
-ServiceLevel -sl	option_name=value	Required. The service level properties. You can set the following properties: - DispatchPriority. The initial priority for dispatch. Smaller numbers have higher priority. Priority 1 is the highest priority. Default is 5. - MaxDispatchWaitTime. The amount of time in seconds that can elapse before the Load Balancer changes the dispatch priority for a task to the highest priority. Default is 1800.

AddUserPrivilege

Assigns a privilege to a user in the domain. You can assign user privileges for each application in the domain.

The infacmd isp AddUserPrivilege command uses the following syntax:

```
AddUserPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]

<-ServiceName|-sn> service_name

<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp AddUserPrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_name	Required. User account to which you are assigning the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user to which you are assigning the privilege belongs to. Default is Native.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

-PrivilegePath
-pp
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/ Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "\" before it as follows:
		`"Model/View Model/Export\ /Import Models"`

AddUserToGroup

Adds a native or LDAP user to a native group in the domain. The user inherits all permissions and privileges associated with the group.

The infacmd isp AddUserToGroup command uses the following syntax:

```
AddUserToGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-GroupName|-gn> group_name
```

The following table describes infacmd isp AddUserToGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_Name	Required. Name of the user you want to add.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user you want to add belongs to. Default is Native.
-GroupName -gn	group_name	Required. Name of the group to which you want to add the user.

AssignDefaultOSProfile

Assigns a default operating system profile to a user or group.

The infacmd isp AssignDefaultOSProfile command uses the following syntax:

```
AssignDefaultOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
<-RecipientName|-nm> recipient_name
<-RecipientSecurityDomain|-ns> security_domain_of_recipient
<-RecipientType|-ty> recipient_type
```

The following table describes infacmd isp AssignDefaultOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-OSProfileName -on	OSProfile_name	Required. Name of the operating system profile. The operating system profile name can be up to 80 characters. It cannot include spaces or the following special characters: `% * + \ / ? ; < >`
-RecipientName -nm	recipient_name	Required. User name or group name to assign default operating system profile.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-RecipientType -ty	recipient_type	Required. Specify whether to assign the default operating system profile to a user or a group. Enter any of the following values: - UserIdentity - GroupIdentity

AssignedToLicense

Lists the services assigned to a license. You can list services currently assigned to a license.

The infacmd isp AssignedToLicense command uses the following syntax:

```
AssignedToLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name
```

The following table describes infacmd isp AssignedToLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license.

AssignGroupPermission

Assigns a group permission on an object.

Permissions allow a group to access objects in a domain. Objects include the domain, folders, nodes, grids, licenses, and application services. For example, if you assign a group permission on a folder, the group inherits permission on all objects in the folder.

The infacmd isp AssignGroupPermission command uses the following syntax:

```
AssignGroupPermission

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingGroup|-eg> existing_group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ObjectName|-on> object_name

<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

The following table describes infacmd isp AssignGroupPermission options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ExistingGroup -eg	existing_group_name	Required. Name of the group to which you want to assign a permission on an object.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group to which you want to assign a permission belongs to. Default is Native.
-ObjectName -on	object_name	Required. Name of the object that you want to assign the group access permission.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Required. Type of object. Enter one of the following values: - Service - License - Node - Grid - Folder - OSProfile

AssignISToMMService

Assigns the associated PowerCenter Integration Service for a Metadata Manager Service.

The infacmd isp AssignISToMMService command uses the following syntax:

```
AssignISToMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> securitydomain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-IntegrationService|-is> integration_service_name
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
<-RepositoryUser|-ru> repository_user
<-RepositoryPassword|-rp> repository_password
```

The following table describes infacmd isp AssignISToMMService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Metadata Manager Service to which you want to assign the Integration Service.
-IntegrationService -is	integration_service_name	Required. Name of the PowerCenter Integration Service that you want to associate with the Metadata Manager Service.

Option	Argument	Description
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If you do not specify this option, the command sets the repository user security domain to the security domain you specify in the -sdn option.
-RepositoryUser -ru	repository_user	Required. Name of the PowerCenter repository user.
-RepositoryPassword -rp	repository_password	Required. Password for the PowerCenter repository user. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.

AssignLicense

Assigns a license to an application service. You must assign a license to an application service before you can enable the service.

Note: You cannot assign a license to a service if the service is assigned to another license. To assign a different license to a service, use the RemoveLicense command to remove the existing license from the service, and then assign the new license to the service.

The infacmd isp AssignLicense command uses the following syntax:

```
AssignLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-ServiceNames|-sn> service1_name service2_name ...
```

The following table describes infacmd isp AssignLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license you want to assign to a service.
-ServiceNames -sn	service_name1 service_name2 ...	Required. Names of the services for which you want to assign a license. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks. Restart the service to apply changes.

AssignRoleToGroup

Assigns a role to a group for a domain or an application service.

The infacmd isp AssignRoleToGroup command uses the following syntax:

```
AssignRoleToGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp AssignRoleToGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group to which you are assigning the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication.Name of the security domain that the group to which you are assigning the role belongs to. Default is Native.
-RoleName -rn	role_name	Required. Name of the role you want to assign to the group.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to assign the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

AssignRoleToUser

Assigns a role to a user for a domain or an application service.

The infacmd isp AssignRoleToUser command uses the following syntax:

```
AssignRoleToUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp AssignRoleToUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_Name	Required. User account to which you are assigning the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication.Name of the security domain that the user to which you are assigning the role belongs to. Default is Native.
-RoleName -rn	role_name	Required. Name of the role you want to assign to the user.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to assign the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

AssignRSToWSHubService

Associates a PowerCenter repository with a Web Services Hub in the domain.

The infacmd isp AssignRSToWSHubService command uses the following syntax:

```
AssignRSToWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-ru> user
```

```
<-RepositoryPassword|-rp> password
```

The following table describes infacmd isp AssignRSToWSHubService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Web Services Hub with which you want to associate a repository.

Option	Argument	Description
-NodeName -nn	node_name	Required. Name of the node where you want the Web Services Hub process to run. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node.
-RepositoryService -rs	repository_service_name	Required. Name of the PowerCenter Repository Service that the Web Services Hub depends on. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryUser -ru	user	Required. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryPassword -rp	password	Required. User password. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.

AssignUserPermission

Assigns a user permission on an object.

Permissions allow a user to access objects in a domain. Objects include the domain, folders, nodes, grids, licenses, and application services. For example, if you assign a user permission on a folder, the user inherits permission on all objects in the folder.

The infacmd isp AssignUserPermission command uses the following syntax:

```
AssignUserPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

The following table describes *infacmd isp* AssignUserPermission options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable.
-ExistingUserName -eu	existing_user_name	Required. Name of the user to which you want to assign a permission on an object.

Option	Argument	Description
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user to which you want to assign a permission belongs to. Default is Native.
-ObjectName -on	object_name	Required. Name of the object that you want to assign the user access permission.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Required. Type of object. Enter one of the following values: - Service - License - Node - Grid - Folder - OSProfile

ConvertLogFile

Converts binary log files to text files, XML files, or readable text on the screen.

The infacmd isp ConvertLogFile command uses the following syntax:

```
ConvertLogFile
<-InputFile|-in> input_file_name
[<-Format|-fm> format_TEXT_XML]
[<-OutputFile|-lo> output_file_name]
```

The following table describes infacmd isp ConvertLogFile options and arguments:

Option	Argument	Description
-InputFile -in	input_file_name	Required. Name and path for the log file you want to convert. By default, the Service Manager writes log files to the server\infa_shared\log directory on the master gateway node.
-Format -fm	format	Optional. Output file format. Valid types include: - Text - XML If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	output_file_name	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.

convertUserActivityLogFile

Converts a binary user activity log file retrieved with the getUserActivityLog command to text or XML format.

The infacmd isp convertUserActivityLogFile command uses the following syntax:

```
convertUserActivityLogFile
<-InputFile|-in> input_file_name
[<-Format|-fm> format_TEXT_XML]
[<-OutputFile|-lo> output_file_name]
```

The following table describes infacmd isp convertUserActivityLogFile options and arguments:

Option	Argument	Description
-InputFile -in	input_file_name	Required. Name of the log file to convert.
-Format -fm	format_TEXT_XML	Optional. Output file format. Valid formats include: - Text - XML Default is text.
-OutputFile -lo	output_file_name	Optional. Name of the output file. If you do not specify an output file name, the command displays the log on the command line.

CreateConnection

Defines a connection and the connection options.

To list connection options for an existing connection, run infacmd isp ListConnectionOptions.

The infacmd isp CreateConnection command uses the following syntax:

```
CreateConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
[<-ConnectionId|-cid> connection_id]
<-ConnectionType|-ct> connection_type
[<-ConnectionUserName|-cun> connection_user_name]
[<-ConnectionPassword|-cpd> connection_password]
```

```
[<-VendorId|-vid> vendor_id]

[-o options] (name-value pairs separated by space)
```

The following table describes infacmd isp CreateConnection options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /

Option	Argument	Description
- ConnectionId -cid	connection_id	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.

Option	Argument	Description
-ConnectionType -ct	connection_type	Required. Type of connection. Use one of the following connection types: - ADABAS - ADLSGEN1 (Microsoft Azure Data Lake Storage Gen1) - ADLSGEN2 (Microsoft Azure Data Lake Storage Gen2) - AMAZONKINESIS - AMAZONREDSHIFT - AMAZONS3 - AZUREBLOB (Microsoft Azure Blob Storage) - BIGQUERY (Google BigQuery) - BLOCKCHAIN - CASSANDRA - ConfluentKafka - DATABRICKS - DATASIFT - DB2 - DB2I - DB2Z - FACEBOOK - GreenplumPT - GOOGLEANALYTICS - GOOGLESTORAGEV2 - HADOOP - HBASE - HDFS - HIVE - IBMDB2 - IMS - JDBC - JDBCV2 - JDEDWARDSENTERPRISEONE - KAFKA - LDAP - LINKEDIN - MAPR-DB - Microsoft Azure SQL Data Warehouse - MSDYNAMICS - NETEZZA - ODATA - ODBC - ORACLE - SALESFORCE - SFMC (Salesforce Marketing Cloud) - SAPAPPLICATIONS - SEQ - SFDC - SNOWFLAKE - SPANNERGOOGLE (Google Cloud Spanner) - SQLSERVER - TABLEAU - TABLEAU V3 - TERADATAPARALLELTRANSPORTER - TWITTER - TWITTERSTREAMING - VSAM - WEBCONTENT - KAPOWKATALYST You can use the infacmd isp ListConnections command to view connection types.

Option	Argument	Description
ConnectionUserName -cun	connection_user_name	Required. Database user name.
-ConnectionPassword -cpd	connection_password	Required. Password for the database user name. You can set a password with the -cpd option or the environment variable INFA_DEFAULT_CONNECTION_PASSWORD, If you set the password with both options, the -cpd option takes precedence. If you are creating an ADABAS, DB2I, DB2Z, IMS, SEQ, or VSAM connection, you can enter a valid PowerExchange passphrase instead of a password. Passphrases for access to databases and data sets on z/OS can be from 9 to 128 characters in length. Passphrases for access to DB2 for i5/OS can be up to 31 characters in length. Passphrases can contain the following characters: - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Note:** The first character is an apostrophe. Passphrases cannot include single quotation marks (‘), double quotation marks (“), or currency symbols. If a passphrase contains spaces, you must enclose it with double-quotation marks ("), for example, `"This is an example passphrase"`. If a passphrase contains special characters, you must enclose it with triple double-quotation characters ("""), for example, `"""This passphrase contains special characters ! % & *."""`. If a passphrase contains only alphanumeric characters without spaces, you can enter it without delimiters. **Note:** On z/OS, a valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation. To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the *PowerExchange Reference Manual*. To use passphrases for IMS connections, ensure that the following additional requirements are met: - You must configure ODBA access to IMS as described in the *PowerExchange Navigator User Guide*. - You must use IMS data maps that specify IMS ODBA as the access method. Do not use data maps that specify the DL/1 BATCH access method because this access method requires the use of netport jobs, which do not support passphrases. - The IMS database must be online in the IMS control region to use ODBA access to IMS.

Option	Argument	Description
-VendorId -vid	vendor_id	Optional. ID of the external partner who built the adapter.
-Options -o	options	Required. Enter name-value pairs separated by spaces. The connection options are different for each connection type. Use single quote to escape any equal sign or space in the value.

Adabas Connection Options

Use connection options to define an Adabas connection.

Enter connection options in the following format:

- Separate multiple options with a space.
- Enclose parameters that contain a equal sign (=) in single quotation marks.

```
... -o option_name=value option_name=value ...
```

The following table describes Adabas connection options:

Option	Description
CodePage	Required. Code to read from or write to the database. Use the ISO code page name, such as ISO-8859-6. The code page name is not case sensitive.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.
Compression	Optional. Compresses the data to decrease the amount of data Informatica applications write over the network. True or false. Default is false.
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.
InterpretAsRows	Optional. If true, the pacing size value represents a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange Listener node that can connect to the database. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.

Option	Description
OffLoadProcessing	Optional. Moves bulk data processing from the source machine to the Data Integration Service machine. Enter one of the following values: - Auto. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is Auto.
PacingSize	Optional. Slows the data transfer rate in order to reduce bottlenecks. The lower the value, the greater the session performance. Minimum value is 0. Enter 0 for optimal performance. Default is 0.
WorkerThread	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listerner without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the PowerExchangeListener asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. True or false. Default is false.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Amazon Kinesis Connection Options

Use connection options to define an Amazon Kinesis connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example, to create an Amazon Kinesis connection to Kinesis Streams on UNIX using cross-account IAM role, run the following command:

```
infacmd createConnection -dn <domain name> -un <domain user> -pd <domain password> -cn
<connection name> -cid <connection id> -ct AMAZONKINESIS -o "AWS_ACCESS_KEY_ID=<access
```

```
key id> AWS_SECRET_ACCESS_KEY=<secret access key> ConnectionTimeOut=10000
Region=<RegionName> ServiceType='Kinesis Streams' RoleArn=<ARN of IAM role>
ExternalID=<External ID> AuthenticationType='Cross-account IAM Role'"
```

To create an Amazon Kinesis connection to Kinesis Firehose on UNIX using AWS credential profile, run the following command:

```
infacmd createConnection -dn <domain name> -un <domain user> -pd <domain password> -cn
<connection name> -cid <connection id> -ct AMAZONKINESIS -o "AWS_ACCESS_KEY_ID=<access
key id> AWS_SECRET_ACCESS_KEY=<secret access key> ConnectionTimeOut=10000
Region=<RegionName> ServiceType='Kinesis Firehose' Profilename=<AWS credential profile>
AuthenticationType='AWS Credential Profile'"
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Amazon Kinesis connection options for the infacmd isp CreateConnection:

Property	Description
AWS_ACCESS_KEY_ID	The access key ID of the Amazon AWS user account.
AWS_SECRET_ACCESS_KEY	The secret access key for your Amazon AWS user account.
ConnectionTimeOut	Number of milliseconds that the Integration service waits to establish a connection to the Kinesis Stream or Kinesis Firehose after which it times out.
Region	Region where the endpoint for your service is available. You can select one of the following values: - us-east-2. Indicates the US East (Ohio) region. - us-east-1. Indicates the US East (N. Virginia) region. - us-west-1. Indicates the US West (N. California) region. - us-west-2. Indicates the US West (Oregon) region. - ap-northeast-1. Indicates the Asia Pacific (Tokyo) region. - ap-northeast-2. Indicates the Asia Pacific (Seoul) region. - ap-northeast-3. Indicates the Asia Pacific (Osaka-Local) region. - ap-south-1. Indicates the Asia Pacific (Mumbai) region. - ap-southeast-1. Indicates the Asia Pacific (Singapore) region. - ap-southeast-2. Indicates the Asia Pacific (Sydney) region. - ca-central-1. Indicates the Canada (Central) region. - cn-north-1. Indicates the China (Beijing) region. - cn-northwest-1. Indicates the China (Ningxia) region. - eu-central-1. Indicates the EU (Frankfurt) region. - eu-west-1. Indicates the EU (Ireland) region. - eu-west-2. Indicates the EU (London) region. - eu-west-3. Indicates the EU (Paris) region. - sa-east-1. Indicates the South America (São Paulo) region.
ServiceType	The type of Kinesis Service that the connection is associated with. Select one of the following service types: - Kinesis Firehose. Select this service to write to Kinesis Firehose Delivery Stream. - Kinesis Streams. Select this service to read from Kinesis Streams.
Profilename	Required if you use the AWS credential profile authentication type. An AWS credential profile defined in the credentials file. A mapping accesses the AWS credentials through the profile name at run time. If you do not provide an AWS credential profile name, the mapping uses the access key ID and secret access key that you specify when you create the connection.

Property	Description
RoleArn	Required if you use the cross-account IAM role authentication type. The Amazon Resource Name specifying the role of an IAM user.
ExternalID	Required if you use the cross-account IAM role authentication type and if the external ID is defined by the AWS account. The external ID for an IAM role is an additional restriction that you can use in an IAM role trust policy to designate who can assume the IAM role.
AuthenticationType	The type of authentication. Select one of the following values: - AWS Credential Profile - Cross-account IAM Role The default value is AWS Credential Profile.

Amazon Redshift Connection Options

Use connection options to define an Amazon Redshift connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory Amazon Redshift connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
Username	User name of the Amazon Redshift account.
Password	Password for the Amazon Redshift account.
Access Key ID	Amazon S3 bucket access key ID. **Note:** Required if you do not use AWS Identity and Access Management (IAM) authentication.
Secret Access Key	Amazon S3 bucket secret access key ID. **Note:** Required if you do not use AWS Identity and Access Management (IAM) authentication.
Master Symmetric Key	Optional. Provide a 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a key using a third-party tool. If you specify a value, ensure that you specify the encryption type as client side encryption in the advanced target properties.
JDBC URL	Amazon Redshift connection URL.

Property	Description
Cluster Region	Optional. The AWS cluster region in which the bucket you want to access resides. Select a cluster region if you choose to provide a custom JDBC URL that does not contain a cluster region name in the **JDBC URL** connection property. If you specify a cluster region in both **Cluster Region** and **JDBC URL** connection properties, the Data Integration Service ignores the cluster region that you specify in the **JDBC URL** connection property. To use the cluster region name that you specify in the **JDBC URL** connection property, select **None** as the cluster region in this property. Select one of the following cluster regions: Select one of the following regions: - Asia Pacific (Mumbai) - Asia Pacific (Seoul) - Asia Pacific (Singapore) - Asia Pacific (Sydney) - Asia Pacific (Tokyo) - AWS GovCloud (US) - Canada (Central) - China (Beijing) - China (Ningxia) - EU (Ireland) - EU (Frankfurt) - EU (London) - EU (Paris) - South America (Sao Paulo) - US East (Ohio) - US East (N. Virginia) - US West (N. California) - US West (Oregon) Default is None. You can only read data from or write data to the cluster regions supported by AWS SDK used by PowerExchange for Amazon Redshift.
Customer Master Key ID	Optional. Specify the customer master key ID generated by AWS Key Management Service (AWS KMS) or the Amazon Resource Name (ARN) of your custom key for cross-account access. You must generate the customer master key corresponding to the region where Amazon S3 bucket resides. You can specify any of the following values: **Customer generated customer master key** Enables client-side or server-side encryption. **Default customer master key** Enables client-side or server-side encryption. Only the administrator user of the account can use the default customer master key ID to enable client-side encryption.

Amazon S3 Connection Options

Use connection options to define an Amazon S3.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory Amazon S3 connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Optional. The description of the connection. The description cannot exceed 4,000 characters.
Location	The domain where you want to create the connection.
Type	The Amazon S3 connection type.
Access Key	Access key to access the Amazon S3 bucket. Provide the access key value based on the following authentication methods: - Basic authentication: provide the actual access key value. - IAM authentication: do not provide the access key value. - Temporary security credentials via assume role: provide access key of an IAM user with no permissions to access Amazon S3 bucket.
Secret Key	Secret access key to access the Amazon S3 bucket. The secret key is associated with the access key and uniquely identifies the account. Provide the access key value based on the following authentication methods: - Basic authentication: provide the actual access secret value. - IAM authentication: do not provide the access secret value. - Temporary security credentials via assume role: provide access secret of an IAM user with no permissions to access Amazon S3 bucket.
IAM Role ARN	The ARN of the IAM role assumed by the user to use the dynamically generated temporary security credentials. Enter the value of this property if you want to use the temporary security credentials to access the AWS resources. If you want to use the temporary security credentials with IAM authentication, do not provide the Access Key and Secret Key connection properties. If you want to use the temporary security credentials without IAM authentication, you must enter the value of the Access Key and Secret Key connection properties. For more information about how to obtain the ARN of the IAM role, see the AWS documentation.
Folder Path	The complete path to Amazon S3 objects. The path must include the bucket name and any folder name. Do not use a slash at the end of the folder path. For example, `<bucket name>/<my folder name>`.
Master Symmetric Key	Optional. Provide a 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a master symmetric key using a third-party tool.

Property	Description
S3 Account Type	The type of the Amazon S3 account. Select **Amazon S3 Storage** or **S3 Compatible Storage**. Select the Amazon S3 storage option to use the Amazon S3 services. Select the S3 compatible storage option to specify the endpoint for a third-party storage provider such as Scality RING. By default, Amazon S3 storage is selected.
REST Endpoint	The S3 storage endpoint. Specify the S3 storage endpoint in HTTP/HTTPs format when you select the S3 compatible storage option. For example, `http://s3.isv.scality.com`.
Region Name	Select the AWS region in which the bucket you want to access resides. Select one of the following regions: - Asia Pacific (Mumbai) - Asia Pacific (Seoul) - Asia Pacific (Singapore) - Asia Pacific (Sydney) - Asia Pacific (Tokyo) - AWS GovCloud (US) - Canada (Central) - China (Beijing) - China (Hong Kong) - China (Ningxia) - EU (Ireland) - EU (Frankfurt) - EU (London) - EU (Paris) - South America (Sao Paulo) - US East (Ohio) - US East (N. Virginia) - US West (N. California) - US West (Oregon) Default is US East (N. Virginia). Not applicable for S3 compatible storage.
Customer Master Key ID	Optional. Specify the customer master key ID or alias name generated by AWS Key Management Service (AWS KMS) or the Amazon Resource Name (ARN) of your custom key for cross-account access. You must generate the customer master key for the same region where Amazon S3 bucket reside. You can specify any of the following values: **Customer generated customer master key** Enables client-side or server-side encryption. **Default customer master key** Enables client-side or server-side encryption. Only the administrator user of the account can use the default customer master key ID to enable client-side encryption.
Federated SSO IdP	SAML 2.0-enabled identity provider for the federated user single sign-on to use with the AWS account. PowerExchange for Amazon S3 supports only the `ADFS 3.0` identity provider. Select `None` if you do not want to use federated user single sign-on.

Federated user single sign-on connection properties

Configure the following properties when you select `ADFS 3.0` in **Federated SSO IdP**:

Property	Description
Federated User Name	User name of the federated user to access the AWS account through the identity provider.
Federated User Password	Password for the federated user to access the AWS account through the identity provider.
IdP SSO URL	Single sign-on URL of the identity provider for AWS.
SAML Identity Provider ARN	ARN of the SAML identity provider that the AWS administrator created to register the identity provider as a trusted provider.
Role ARN	ARN of the IAM role assumed by the federated user.

Blockchain Connection Options

Use connection options to define a blockchain connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes blockchain connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
swaggerFilePath	The absolute path of the swagger file path that contains the REST API to communicate with the blockchain. The swagger file must be a JSON file that is stored on the Data Integration Service machine. If the swagger file is in a different file format, such as YAML, convert the file to JSON format.
authType*	Authentication method that the run-time engine uses to connect to the REST server. You can use none, basic, digest, or OAuth.
authUserID*	User name to authenticate to the REST server.
authPassword*	Password for the user name to authenticate to the REST server.
oAuthConsumerKey*	Required for the OAuth authentication type. Client key that is associated with the REST server.
oAuthConsumerSecret*	Required for the OAuth authentication type. Client password to connect to the REST server.
oAuthToken*	Required for the OAuth authentication type. Access token to connect to the REST server.
oAuthTokenSecret*	Required for the OAuth authentication type. Password associated with the OAuth token.
proxyType*	Type of proxy. You can use no proxy, platform proxy, or custom.

Property	Description
proxyDetails*	Proxy configuration using the format <host>:<port>.
trustStoreFilePath*	The absolute path of the truststore file that contains the SSL certificate.
trustStorePassword*	Password for the truststore file.
keyStoreFilePath*	The absolute path of the keystore file that contains the keys and certificates required to establish a two-way secure connection with the REST server.
keyStorePassword*	Password for the keystore file.
advancedProperties	List of advanced properties to access an asset on the blockchain. Specify the advanced properties using name-value pairs that are separated by a semicolon. You can use the following advanced properties: - X-API-KEY. Required if you authenticate to the REST server using an API key. The advanced properties that you configure in the connection override the values for the corresponding advanced properties in the blockchain data object. For example, if the connection and the data object both specify a base URL, the value in the connection overrides the value in the data object.
cookies	Required based on how the REST API is implemented. List of cookie properties to specify the cookie information that is passed to the REST server. Specify the properties using name-value pairs that are separated by a semicolon. The cookie properties that you configure in the connection override the values for the corresponding cookie properties in the blockchain data object.
* The property is ignored. To use the functionality, configure the property as an advanced property and provide a name-value pair based on the property name in the swagger file. For example, configure the following name-value pair to use basic authorization: `Authorization=Basic <credentials>`	

Cassandra Connection Options

Use connection options to define the Cassandra connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example,

```
./infacmd.sh createConnection -dn Domain_Adapters_1020_Uni -un Administrator -pd
Administrator -cn Cassandra_test2 -ct CASSANDRA -cun cloud2 -cpd cloud2 -o
HostName=invrlx7acdb01 DefaultKeyspace=cloud SQLIDENTIFIERCHARACTER='"(quotes)'
SSLMODE=disabled
AdditonalConnectionProperties='BinaryColumnLength=10000;DecimalColumnScale=19;EnableCaseS
ensitive=0;EnableNullInsert=1;EnablePaging=0;
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Cassandra connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
HostName	Host name or IP address of the Cassandra server.
Port	Cassandra server port number. Default is 9042.
User Name -cun	User name to access the Cassandra server.
Password -cpd	Password corresponding to the user name to access the Cassandra server.
DefaultKeyspace	Name of the Cassandra keyspace to use by default.
SQLIDENTIFIERCHARACTER	Type of character that the database uses to enclose delimited identifiers in SQL or CQL queries. The available characters depend on the database type. Specify **None** if the database uses regular identifiers. When the Data Integration Service generates SQL or CQL queries, the service does not place delimited characters around any identifiers. Specify a character if the database uses delimited identifiers. When the Data Integration Service generates SQL or CQL queries, the service encloses delimited identifiers within this character.
SSLMODE	Not applicable for PowerExchange for Cassandra JDBC. Enter **disabled**.
AdditionalConnectionProperties	Enter one or more JDBC connection parameters in the following format: `<param1>=<value>;<param2>=<value>;<param3>=<value>` PowerExchange for Cassandra JDBC supports the following JDBC connection parameters: - BinaryColumnLength - DecimalColumnScale - EnableCaseSensitive - EnableNullInsert - EnablePaging - RowsPerPage - StringColumnLength - VTTableNameSeparator

Confluent Kafka Connection Options

Use connection options to define a Confluent Kafka connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example, to create a Confluent Kafka connection on UNIX, run the following command:

```
sh infacmd.sh createConnection -dn <domain name> -un <domain user> -pd <domain password>
-cn <connection name> -cid <connection id> -ct ConfluentKafka -o
"kfkBrkList='<host1:port1>,<host2:port2>,<host3:port3>' kafkabrokerversion='<version>'
schemaregistryurl='<schema registry URL>'"
```

Databricks Connection Options

Use connection options to define a Databricks connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Databricks connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
connectionId	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
connectionType	Required. Type of connection is Databricks.
name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
databricksExecutionParameterList	Advanced properties that are unique to the Databricks Spark engine. To enter multiple properties, separate each name-value pair with the following text: `&:`. Use Informatica advanced properties only at the request of Informatica Global Customer Support.
clusterConfigID	Name of the cluster configuration associated with the Databricks environment. Required if you do not configure the cloud provisioning configuration.
provisionConnectionId	Name of the cloud provisioning configuration associated with a cloud platform such as Microsoft Azure. Required if you do not configure the cluster configuration.
stagingDirectory	The directory where the Databricks Spark engine stages run-time files. If you specify a directory that does not exist, the Data Integration Service creates it at run time. If you do not provide a directory path, the run-time staging files are written to */<cluster staging directory>/DATABRICKS*.

DataSift Connection Options

Use connection options to define a DataSift connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes DataSift connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
userName	DataSift username for the DataSift user account.
apiKey	API key. The Developer API key is displayed in the Dashboard or Settings page in the DataSift account.

DB2 for i5/OS Connection Options

Use DB2I connection options to define the DB2 for i5/OS connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes DB2 for i5/OS connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
DatabaseName	Database instance name.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. **Note:** Enclose special characters in double quotes.
CodePage	Required. Code page used to read from a source database or write to a target database or file.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.
Compression	Optional. Compresses the data to decrease the amount of data to write over the network. Default is false.
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.

Option	Description
InterpretAsRows	Optional. Represent pacing size as a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange Listener node that can connect to the database. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
PacingSize	Optional. Amount of data the source system can pass to the PowerExchange Listener. Configure the pacing size if an external application, a database, or the Data Integration Service node is a bottleneck. The lower the value, the faster the performance. Minimum value is 0. Enter 0 for maximum performance. Default is 0.
RejectFile	Optional. Enter the reject file name and path. Reject files contain rows that were not written to the database.
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the PowerExchange Listener asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.
DatabaseFileOverrides	Specifies the i5/OS database file override. The format is: `from_file/to_library/to_file/to_member` Where: - *from_file* is the file to be overridden - *to_library* is the new library to use - *to_file* is the file in the new library to use - *to_member* is optional and is the member in the new library and file to use. *FIRST is used if nothing is specified. You can specify up to 8 unique file overrides on a single connection. A single override applies to a single source or target. When you specify more than one file override, enclose the string of file overrides in double quotes and include a space between each file override. **Note:** If both LibraryList and DatabaseFileOverrides are specified and a table exists in both, DatabaseFileOverrides takes precedence.
IsolationLevel	Commit scope of the transaction. Select one of the following values: - None - CS. Cursor stability. - RR. Repeatable Read. - CHG. Change. - ALL Default is CS.

Option	Description
LibraryList	List of libraries that PowerExchange searches to qualify the table name for Select, Insert, Delete, or Update statements. PowerExchange searches the list if the table name is unqualified. Separate libraries with commas. **Note:** If both LibraryList and DatabaseFileOverrides are specified and a table exists in both, DatabaseFileOverrides takes precedence.
EnableConnectionPool	Optional. Enables parallel processing when loading data into a table in bulk mode. Used for Oracle. True or false. Default is true.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

DB2 for z/OS Connection Options

Use DB2Z connection options to define the IBM for DB2 z/OS connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes DB2Z connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
DataAccessConnectString	Connection string used to access data from the database. <database name>
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. **Note:** Enclose special characters in double quotes.
CodePage	Required. Code page used to read from a source database or write to a target database or file.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.

Option	Description
Compression	Optional. Compresses the data to decrease the amount of data to write over the network. Default is false.
CorrelationID	Optional. Label to apply to a DB2 task or query to allow DB2 for z/OS to account for the resource. Enter up to 8 bytes of alphanumeric characters.
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.
InterpretAsRows	Optional. Represent pacing size as a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange listener node that can connect to the database. The node is defined in the PowerExchange dbmover.cfg configuration file.
OffloadProcessing	Optional. Moves bulk data processing from the VSAM source to the Data Integration Service machine. Enter one of the following values: - Auto. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is Auto.
PacingSize	Optional. Amount of data the source system can pass to the PowerExchange Listener. Configure the pacing size if an external application, a database, or the Data Integration Service node is a bottleneck. The lower the value, the faster the performance. Minimum value is 0. Enter 0 for maximum performance. Default is 0.
RejectFile	Optional. Enter the reject file name and path. Reject files contain rows that were not written to the database.
WorkerThread	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the PowerExchange Listener asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.

Option	Description
EnableConnectionPool	Optional. Enables parallel processing when loading data into a table in bulk mode. Used for Oracle. True or false. Default is true.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Facebook Connection Options

Use connection options to define a Facebook connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Facebook connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
ConsumerKey	The App ID that you get when you create the application in Facebook. Facebook uses the key to identify the application.
ConsumerSecret	The App Secret that you get when you create the application in Facebook. Facebook uses the secret to establish ownership of the consumer key.
AccessToken	Access token that the OAuth Utility returns. Facebook uses this token instead of the user credentials to access the protected resources.
AccessSecret	Access secret is not required for Facebook connection.
Scope	Permissions for the application. Enter the permissions you used to configure OAuth.

Greenplum Connection Options

Use connection options to define a Greenplum connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Greenplum connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
UserName	Required. User name with permissions to access the Greenplum database.
Password	Required. Password to connect to the Greenplum database.
driverName	Required. Name of the Greenplum JDBC driver. For example:`com.pivotal.jdbc.GreenplumDriver` For more information about the driver, see the Greenplum documentation.
connectionString	Required. Greenplum JDBC connection URL. For example: `jdbc:pivotal:greenplum://<hostname>:<port>;DatabaseName=<database_name>` For more information about the connection URL, see the Greenplum documentation.
hostName	Required. Host name or IP address of the Greenplum server.
portNumber	Optional. Greenplum server port number. If you enter 0, the gpload utility reads from the environment variable $PGPORT. Default is 5432.
databaseName	Required. Name of the database that you want to connect to.
enableSSL	Required. Set this option to true to establish secure communication between the gpload utility and the Greenplum server over SSL.
SSLCertificatePath	Required if you enable SSL. Path where the SSL certificates for the Greenplum server are stored.

Google Analytics Connection Options

Use connection options to define the Google Analytics connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

For example,

```
./infacmd.sh createconnection dn Domain_Google -un Administrator -pd Administrator -cn
GA_cmd -ct GOOGLEANALYTICS -o "SERVICEACCOUNTID=serviceaccount@api-
project-12345.iam.gserviceaccount.com SERVICEACCOUNTKEY='---BEGIN PRIVATE KEY---
\nabcd1234322dsa\n---END PRIVATE KEY----\n' PROJECTID=api-project-12333667"
```

The following table describes Google Analytics connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
SERVICEACCOUNTID	Required. Specifies the client_email value present in the JSON file that you download after you create a service account.
SERVICEACCOUNTKEY	Required. Specifies the private_key value present in the JSON file that you download after you create a service account.

Google BigQuery Connection Options

Use connection options to define the Google BigQuery connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

For example,

```
./infacmd.sh createconnection -dn Domain_Adapters_1041_Uni -un Administrator -pd
Administrator -cn GBQ_BDM -ct BIGQUERY -o "CLIENTEMAIL='ics-test@api-
project-80697026669.iam.gserviceaccount.com' PRIVATEKEY='-----BEGIN PRIVATE KEY-----
\nMIIgfdzhgy74587igu787tio9QEFAASCBKgwggSkAgEAAoIBAQCy+2Dbh\n-----END PRIVATE KEY-----
\n' PROJECTID=api-project-86699686669 CONNECTORTYPE=Simple SCHEMALOCATION='gs://0_europe-
west6_region' STORAGEPATH='gs://0_europe-west6_region'
DATASETNAMEFORCUSTOMQUERY='europe_west6' REGIONID='europe-west6'" ;
```

The following table describes Google BigQuery connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
CLIENTEMAIL	Required. Specifies the client_email value present in the JSON file that you download after you create a service account in Google BigQuery.
PRIVATEKEY	Required. Specifies the private_key value present in the JSON file that you download after you create a service account in Google BigQuery.
Connection Mode CONNECTORTYPE	Required. The connection mode that you want to use to read data from or write data to Google BigQuery. Enter one of the following connection modes: - Simple. Flattens each field within the Record data type field as a separate field in the mapping. - Hybrid. Displays all the top-level fields in the Google BigQuery table including Record data type fields. PowerExchange for Google BigQuery displays the top-level Record data type field as a single field of the String data type in the mapping. - Complex. Displays all the columns in the Google BigQuery table as a single field of the String data type in the mapping. Default is Simple.

Property	Description
Schema Definition File Path SCHEMALOCATION	Required. Specifies a directory on the client machine where the PowerExchange for Google BigQuery must create a JSON file with the sample schema of the Google BigQuery table. The JSON file name is the same as the Google BigQuery table name. Alternatively, you can specify a storage path in Google Cloud Storage where the PowerExchange for Google BigQuery must create a JSON file with the sample schema of the Google BigQuery table. You can download the JSON file from the specified storage path in Google Cloud Storage to a local machine.
PROJECTID	Required. Specifies the project_id value present in the JSON file that you download after you create a service account in Google BigQuery. If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.
STORAGEPATH	Required when you read or write large volumes of data. Path in Google Cloud Storage where PowerExchange for Google BigQuery creates a local stage file to store the data temporarily. You can either enter the bucket name or the bucket name and folder name. For example, enter `gs://<bucket_name>` or `gs://<bucket_name>/<folder_name>`
REGIONID	The region name where the Google BigQuery dataset resides. For example, if you want to connect to a Google BigQuery dataset that resides in Las Vegas region, specify **us-west4** as the **Region ID**. **Note:** In the **Storage Path** connection property, ensure that you specify a bucket name or the bucket name and folder name that resides in the same region as the dataset in Google BigQuery. For more information about the regions supported by Google BigQuery, see the following Google BigQuery documentation:https://cloud.google.com/bigquery/docs/locations

Google Cloud Spanner Connection Options

Use connection options to define the Google Cloud Spanner connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

For example,

```
./infacmd.sh createconnection dn Domain_Google -un Administrator -pd Administrator -cn
Spanner_cmd -ct SPANNERGOOGLE -o "CLIENTEMAIL=serviceaccount@api-
project-12345.iam.gserviceaccount.com PRIVATEKEY='---BEGIN PRIVATE KEY---\nabcd1234322dsa
\n---END PRIVATE KEY----\n' INSTANCEID=spanner-testing PROJECTID=api-project-12333667"
```

The following table describes Google Cloud Spanner connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
CLIENTEMAIL	Required. Specifies the client_email value present in the JSON file that you download after you create a service account in Google Cloud Spanner.
PRIVATEKEY	Required. Specifies the private_key value present in the JSON file that you download after you create a service account in Google Cloud Spanner.
PROJECTID	Required. Specifies the project_id value present in the JSON file that you download after you create a service account in Google Cloud Spanner. If you have created multiple projects with the same service account, enter the ID of the project that contains the dataset that you want to connect to.
INSTANCEID	Required. Name of the instance that you created in Google Cloud Spanner.

Google Cloud Storage Connection Options

Use connection options to define the Google Cloud Storage connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

For example,

```
./infacmd.sh createconnection dn Domain_Google -un Administrator -pd Administrator -cn
GCS_cmd -ct GOOGLESTORAGEV2 -o "CLIENTEMAIL=serviceaccount@api-
project-12345.iam.gserviceaccount.com PRIVATEKEY='---BEGIN PRIVATE KEY---\nabcd1234322dsa
\n---END PRIVATE KEY----\n' PROJECTID=api-project-12333667"
```

The following table describes Google Cloud Storage connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
CLIENTEMAIL	Required. Specifies the client_email value present in the JSON file that you download after you create a service account.
PRIVATEKEY	Required. Specifies the private_key value present in the JSON file that you download after you create a service account.
PROJECTID	Required. Specifies the project_id value present in the JSON file that you download after you create a service account. If you have created multiple projects with the same service account, enter the ID of the project that contains the bucket that you want to connect to.

Hadoop Connection Options

Use connection options to define a Hadoop connection.

Enter connection options in the following format:

```
... -o option_name='value' option_name='value' ...
```

To enter multiple options, separate them with a space.

To enter advanced properties, use the following format:

```
... -o engine_nameAdvancedProperties="'advanced.property.name=value'"
```

For example:

```
... -o blazeAdvancedProperties="'infrgrid.orchestrator.svc.sunset.time=3'"
```

The following table describes Hadoop connection options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hadoop connection:

Option	Description
connectionId	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
connectionType	Required. Type of connection is Hadoop.
name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
blazeJobMonitorURL	The host name and port number for the Blaze Job Monitor. Use the following format: <hostname>:<port> Where - <hostname> is the host name or IP address of the Blaze Job Monitor server. - <port> is the port on which the Blaze Job Monitor listens for remote procedure calls (RPC). For example, enter: myhostname:9080
blazeYarnQueueName	The YARN scheduler queue name used by the Blaze engine that specifies available resources on a cluster. The name is case sensitive.
blazeAdvancedProperties	Advanced properties that are unique to the Blaze engine. To enter multiple properties, separate each name-value pair with the following text: &:. Use Informatica custom properties only at the request of Informatica Global Customer Support.
blazeMaxPort	The maximum value for the port number range for the Blaze engine. Default value is 12600
blazeMinPort	The minimum value for the port number range for the Blaze engine. Default value is 12300
blazeUserName	The owner of the Blaze service and Blaze service logs. When the Hadoop cluster uses Kerberos authentication, the default user is the Data Integration Service SPN user. When the Hadoop cluster does not use Kerberos authentication and the Blaze user is not configured, the default user is the Data Integration Service user.

Option	Description
blazeStagingDirectory	The HDFS file path of the directory that the Blaze engine uses to store temporary files. Verify that the directory exists. The YARN user, Blaze engine user, and mapping impersonation user must have write permission on this directory. Default is `/blaze/workdir`. If you clear this property, the staging files are written to the Hadoop staging directory `/tmp/blaze_<user name>`.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.
hiveStagingDatabaseName	Namespace for Hive staging tables. Use the name `default` for tables that do not have a specified database name.
engineType	Execution engine to run HiveServer2 tasks on the Spark engine. Default is MRv2. You can choose MRv2 or Tez according to the engine type that the Hadoop distribution uses: - Amazon EMR. Tez - Azure HDI. Tez - Cloudera CDH. MRv2 - Cloudera CDP. Tez - Dataproc. MRv2 - Hortonworks HDP. Tez - MapR. MRv2
environmentSQL	SQL commands to set the Hadoop environment. The Data Integration Service executes the environment SQL at the beginning of each Hive script generated in a Hive execution plan. The following rules and guidelines apply to the usage of environment SQL: - Use the environment SQL to specify Hive queries. - Use the environment SQL to set the classpath for Hive user-defined functions and then use environment SQL or PreSQL to specify the Hive user-defined functions. You cannot use PreSQL in the data object properties to specify the classpath. If you use Hive user-defined functions, you must copy the .jar files to the following directory:`<Informatica installation directory>/services/shared/hadoop/<Hadoop distribution name>/extras/hive-auxjars` - You can use environment SQL to define Hadoop or Hive parameters that you want to use in the PreSQL commands or in custom queries.
hadoopExecEnvExecutionParameterList	Custom properties that are unique to the Hadoop connection. You can specify multiple properties. Use the following format: `<property1>=<value>` To specify multiple properties use `&:` as the property separator. If more than one Hadoop connection is associated with the same cluster configuration, you can override configuration set property values. Use Informatica custom properties only at the request of Informatica Global Customer Support.
hadoopRejDir	The remote directory where the Data Integration Service moves reject files when you run mappings. Enable the reject directory using rejDirOnHadoop.

Option	Description
impersonationUserName	Required if the Hadoop cluster uses Kerberos authentication. Hadoop impersonation user. The user name that the Data Integration Service impersonates to run mappings in the Hadoop environment. The Data Integration Service runs mappings based on the user that is configured. Refer the following order to determine which user the Data Integration Services uses to run mappings: 1. Operating system profile user. The mapping runs with the operating system profile user if the profile user is configured. If there is no operating system profile user, the mapping runs with the Hadoop impersonation user. 2. Hadoop impersonation user. The mapping runs with the Hadoop impersonation user if the operating system profile user is not configured. If the Hadoop impersonation user is not configured, the Data Integration Service runs mappings with the Data Integration Service user. 3. Data Integration Service user. The mapping runs with the Data Integration Service user if the operating system profile user and the Hadoop impersonation user are not configured.
hiveWarehouseDirectoryOnHDFS	Optional. The absolute HDFS file path of the default database for the warehouse that is local to the cluster. If you do not configure the Hive warehouse directory, the Hive engine first tries to write to the directory specified in the cluster configuration property `hive.metastore.warehouse.dir`. If the cluster configuration does not have the property, the Hive engine writes to the default directory `/user/hive/warehouse`.

metastoreDatabaseDriver	Driver class name for the JDBC data store. For example, the following class name specifies a MySQL driver:
	`com.mysql.jdbc.Driver`
	You can get the value for the Metastore Database Driver from hive-site.xml. The Metastore Database Driver appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionDriverName</name>`
	`  <value>com.mysql.jdbc.Driver</value>`
	`</property>`

metastoreDatabasePassword	The password for the metastore user name.
	You can get the value for the Metastore Database Password from hive-site.xml. The Metastore Database Password appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionPassword</name>`
	`  <value>password</value>`
	`</property>`

Option	Description

metastoreDatabaseURI	The JDBC connection URI used to access the data store in a local metastore setup. Use the following connection URI:
	`jdbc:<datastore type>://<node name>:<port>/<database name>`
	where
	- <node name> is the host name or IP address of the data store.
	- <data store type> is the type of the data store.
	- <port> is the port on which the data store listens for remote procedure calls (RPC).
	- <database name> is the name of the database.
	For example, the following URI specifies a local metastore that uses MySQL as a data store:
	`jdbc:mysql://hostname23:3306/metastore`
	You can get the value for the Metastore Database URI from hive-site.xml. The Metastore Database URI appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionURL</name>`
	`  <value>jdbc:mysql://MYHOST/metastore</value>`
	`</property>`

metastoreDatabaseUserName	The metastore database user name.
	You can get the value for the Metastore Database User Name from hive-site.xml. The Metastore Database User Name appears as the following property in hive-site.xml:
	`<property>`
	`  <name>javax.jdo.option.ConnectionUserName</name>`
	`  <value>hiveuser</value>`
	`</property>`

metastoreMode	Controls whether to connect to a remote metastore or a local metastore. By default, local is selected. For a local metastore, you must specify the Metastore Database URI, Metastore Database Driver, Username, and Password. For a remote metastore, you must specify only the Remote Metastore URI.
	You can get the value for the Metastore Execution Mode from hive-site.xml. The Metastore Execution Mode appears as the following property in hive-site.xml:
	`<property>`
	`<name>hive.metastore.local</name>`
	`<value>true</true>`
	`</property>`
	Note: The `hive.metastore.local` property is deprecated in hive-site.xml for Hive server versions 0.9 and above. If the `hive.metastore.local` property does not exist but the `hive.metastore.uris` property exists, and you know that the Hive server has started, you can set the connection to a remote metastore.

Option	Description

remoteMetastoreURI	The metastore URI used to access metadata in a remote metastore setup. For a remote metastore, you must specify the Thrift server details.
	Use the following connection URI:
	`thrift://<hostname>:<port>`
	Where
	- <hostname> is name or IP address of the Thrift metastore server.
	- <port> is the port on which the Thrift server is listening.
	For example, enter: `thrift://myhostname:9083/`
	You can get the value for the Remote Metastore URI from hive-site.xml. The Remote Metastore URI appears as the following property in hive-site.xml:
	`<property>`
	`<name>hive.metastore.uris</name>`
	`<value>thrift://<n.n.n.n>:9083</value>`
	`<description> IP address or fully-qualified domain name and port of the metastore host</description>`
	`</property>`

rejDirOnHadoop	Enables hadoopRejDir. Used to specify a location to move reject files when you run mappings. If enabled, the Data Integration Service moves mapping files to the HDFS location listed in hadoopRejDir. By default, the Data Integration Service stores the mapping files based on the RejectDir system parameter.
sparkEventLogDir	Optional. The HDFS file path of the directory that the Spark engine uses to log events.
sparkAdvancedProperties	Advanced properties that are unique to the Spark engine. To enter multiple properties, separate each name-value pair with the following text: `&:`. Use Informatica custom properties only at the request of Informatica Global Customer Support.
sparkStagingDirectory	The HDFS file path of the directory that the Spark engine uses to store temporary files for running jobs. The YARN user, Data Integration Service user, and mapping impersonation user must have write permission on this directory. By default, the temporary files are written to the Hadoop staging directory `/tmp/spark_<user name>`.
sparkYarnQueueName	The YARN scheduler queue name used by the Spark engine that specifies available resources on a cluster. The name is case sensitive.
stgDataCompressionCodecClass	Codec class name that enables data compression and improves performance on temporary staging tables. The codec class name corresponds to the code type.
stgDataCompressionCodecType	Hadoop compression library for a compression codec class name. You can choose None, Zlib, Gzip, Snappy, Bz2, LZO, or Custom. Default is None.

HBase Connection Options

Use connection options to define an HBase connection. You can use an HBase connection to connect to an HBase table or a MapR-DB table.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the HBase connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
DATABASETYPE	Required when you create an HBase connection for a MapR-DB table. Set the value to MapR-DB. Default is HBase.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.
maprdbpath	Required if you create an HBase connection to connect to a MapR-DB table. Set the value to the database path that contains the MapR-DB table that you want to connect to. Enter a valid MapR cluster path. Enclose the value in single quotes. When you create an HBase data object for MapR-DB, you can browse only tables that exist in the path that you specify in this option. You cannot access tables that are available in sub-directories in the specified path. For example, if you specify the maprdbpath as `/user/customers/`, you can access the tables in the `customers` directory. However, if the `customers` directory contains a sub-directory named `regions`, you cannot access the tables in the following directory: `/user/customers/regions`

HDFS Connection Options

Use connection options to define an HDFS connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the HDFS connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
userName	User name to access HDFS.
nameNodeURI	The URI to access the storage system. You can find the value for `fs.defaultFS` in the `core-site.xml` configuration set of the cluster configuration.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.

Hive Connection Options

Use connection options to define a Hive connection.

Enter connection options in the following format:

```
... -o option_name='value' option_name='value' ...
```

To enter multiple options, separate them with a space.

The following table describes Hive connection options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hive connection:

Option	Description
connectionType	Required. Type of connection is HIVE.
name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
environmentSQL	SQL commands to set the Hadoop environment. In native environment type, the Data Integration Service executes the environment SQL each time it creates a connection to Hive metastore. If the Hive connection is used to run mappings in the Hadoop cluster, the Data Integration Service executes the environment SQL at the beginning of each Hive session. The following rules and guidelines apply to the usage of environment SQL in both the connection modes: - Use the environment SQL to specify Hive queries. - Use the environment SQL to set the classpath for Hive user-defined functions and then use either environment SQL or PreSQL to specify the Hive user-defined functions. You cannot use PreSQL in the data object properties to specify the classpath. If you use Hive user-defined functions, you must copy the .jar files to the following directory: `<Informatica installation directory>/services/shared/hadoop/<Hadoop distribution name>/extras/hive-auxjars` - You can also use environment SQL to define Hadoop or Hive parameters that you intend to use in the PreSQL commands or in custom queries. If the Hive connection is used to run mappings in the Hadoop cluster, only the environment SQL of the Hive connection is executed. The different environment SQL commands for the connections of the Hive source or target are not executed, even if the Hive sources and targets are on different clusters.
quoteChar	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the **Support mixed-case identifiers** property.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up a Hadoop connection.

Properties to Access Hive as Source or Target

The following table describes the mandatory options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hive connection to access Hive data:

Property	Description
hiveJdbcDriverClassName	Name of the JDBC driver class.
metadataConnString	The JDBC connection URI used to access the metadata from the Hadoop server. The connection string uses the following format: `jdbc:hive://<hostname>:<port>/<db>` Where - `hostname` is name or IP address of the machine on which the Hive server is running. - `port` is the port on which the Hive server is listening. - `db` is the database to which you want to connect. If you do not provide the database details, the Data Integration Service uses the default database details. To connect to HiveServer 2, use the connection string format that Apache Hive implements for that specific Hadoop Distribution. For more information about Apache Hive connection string formats, see the Apache Hive documentation. If the Hadoop cluster uses SSL or TLS authentication, you must add ssl=true to the JDBC connection URI. For example: `jdbc:hive2://<hostname>:<port>/<db>;ssl=true` If you use self-signed certificate for SSL or TLS authentication, ensure that the certificate file is available on the client machine and the Data Integration Service machine. For more information, see the *Informatica Big Data Management Cluster Integration Guide*.
bypassHiveJDBCServer	JDBC driver mode. Enable this option to use the embedded JDBC driver (embedded mode). To use the JDBC embedded mode, perform the following tasks: - Verify that Hive client and Informatica Services are installed on the same machine. - Configure the Hive connection properties to run mappings in the Hadoop cluster. If you choose the non-embedded mode, you must configure the Data Access Connection String. The JDBC embedded mode is preferred to the non-embedded mode.

Property	Description
sqlAuthorized	When you select the option to observe fine-grained SQL authentication in a Hive source, the mapping observes row and column-level restrictions on data access. If you do not select the option, the Blaze run-time engine ignores the restrictions, and results include restricted data. Applicable to Hadoop clusters where Sentry or Ranger security modes are enabled.
connectString	The connection string used to access data from the Hadoop data store. The non-embedded JDBC mode connection string must be in the following format: `jdbc:hive://<hostname>:<port>/<db>` Where - `hostname` is name or IP address of the machine on which the Hive server is running. - `port` is the port on which the Hive server is listening. Default is 10000. - `db` is the database to which you want to connect. If you do not provide the database details, the Data Integration Service uses the default database details. To connect to HiveServer 2, use the connection string format that Apache Hive implements for that specific Hadoop Distribution. For more information about Apache Hive connection string formats, see the Apache Hive documentation. If the Hadoop cluster uses SSL or TLS authentication, you must add ssl=true to the JDBC connection URI. For example: `jdbc:hive2://<hostname>:<port>/<db>;ssl=true` If you use self-signed certificate for SSL or TLS authentication, ensure that the certificate file is available on the client machine and the Data Integration Service machine. For more information, see the *Informatica Big Data Management Cluster Integration Guide*.

Properties to Run Mappings in the Hadoop Cluster

The following table describes the mandatory options for infacmd isp CreateConnection and UpdateConnection commands that you configure when you want to use the Hive connection to run Informatica mappings in the Hadoop cluster:

Property	Description
databaseName	Namespace for tables. Use the name `default` for tables that do not have a specified database name.

customProperties	Configures or overrides Hive or Hadoop cluster properties in the hive-site.xml configuration set on the machine on which the Data Integration Service runs. You can specify multiple properties.
	Select **Edit** to specify the name and value for the property. The property appears in the following format:
	`<property1>=<value>`
	When you specify multiple properties, `&:` appears as the property separator.
	The maximum length for the format is 1 MB.
	If you enter a required property for a Hive connection, it overrides the property that you configure in the Advanced Hive/Hadoop Properties.
	The Data Integration Service adds or sets these properties for each map-reduce job. You can verify these properties in the JobConf of each mapper and reducer job. Access the JobConf of each job from the Jobtracker URL under each map-reduce job.
	The Data Integration Service writes messages for these properties to the Data Integration Service logs. The Data Integration Service must have the log tracing level set to log each row or have the log tracing level set to verbose initialization tracing.
	For example, specify the following properties to control and limit the number of reducers to run a mapping job:
	`mapred.reduce.tasks=2&:hive.exec.reducers.max=10`

stgDataCompressionCodecClass	Codec class name that enables data compression and improves performance on temporary staging tables. The codec class name corresponds to the code type.
stgDataCompressionCodecType	Hadoop compression library for a compression codec class name. You can choose None, Zlib, Gzip, Snappy, Bz2, LZO, or Custom. Default is None.

IBM DB2 Connection Options

Use connection options to define the IBM DB2 connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes IBM DB2 connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
PassThruEnabled	Optional. Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.

MetadataAccessConnectString	Required. JDBC connection URL used to access metadata from the database.
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>`
	When you import a table from the Developer tool or Analyst tool, by default, all tables are displayed under the default schema name. To view tables under a specific schema instead of the default schema, you can specify the schema name from which you want to import the table. Include the ischemaname parameter in the URL to specify the schema name. For example, use the following syntax to import a table from a specific schema:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>;ischemaname=<schema_name>`
	To search for a table in multiple schemas and import it, you can specify multiple schema names in the ischemaname parameter. The schema name is case sensitive. You cannot use special characters when you specify multiple schema names. Use the pipe (|) character to separate multiple schema names. For example, use the following syntax to search for a table in three schemas and import it:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>;ischemaname=<schema_name1>|<schema_name2>|<schema_name3>`

AdvancedJDBCSecurityOptions	Optional. Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and encrypts the parameter string. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. **Note:** For a complete list of the secure JDBC parameters, see the DataDirect JDBC documentation. Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly in the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.
DataAccessConnectString	Connection string used to access data from the database. Enter the connection string in the following format: `<database name>`

Option	Description
CodePage	Required. Code page used to read from a source database or write to a target database.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Note:** Enclose special characters in double quotes.
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Note:** Enclose special characters in double quotes.
Tablespace	Optional. The tablespace name of the database.
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is 0.
EnableQuotes	Optional. Select to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is True.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. Valid values are True or False. Default is True.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

IMS Connection Options

Use connection options to define an IMS connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes IMS connection options:

Option	Description
CodePage	Required. Code to read from or write to the database. Use the ISO code page name, such as ISO-8859-6. The code page name is not case sensitive.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.
Compression	Optional. Compresses the data to decrease the amount of data Informatica applications write over the network. True or false. Default is false.
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.
InterpretAsRows	Optional. If true, the pacing size value represents a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange Listener node that can connect to the database. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
OffLoadProcessing	Optional. Moves bulk data processing from the source machine to the Data Integration Service machine. Enter one of the following values: - Auto. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is Auto.
PacingSize	Optional. Slows the data transfer rate in order to reduce bottlenecks. The lower the value, the greater the session performance. Minimum value is 0. Enter 0 for optimal performance. Default is 0.
WorkerThread	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.

Option	Description
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listerner without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the PowerExchangeListener asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. True or false. Default is false.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

JDBC Connection Options

Use connection options to define a JDBC connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes JDBC connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
JDBCDriverClassName	The Java class that you use to connect to the database. The following list provides the driver class name that you can enter for the applicable database type: - DataDirect JDBC driver class name for Oracle: `com.informatica.jdbc.oracle.OracleDriver` - DataDirect JDBC driver class name for IBM DB2: `com.informatica.jdbc.db2.DB2Driver` - DataDirect JDBC driver class name for Microsoft SQL Server: `com.informatica.jdbc.sqlserver.SQLServerDriver` - DataDirect JDBC driver class name for Sybase ASE: `com.informatica.jdbc.sybase.SybaseDriver` - DataDirect JDBC driver class name for Informix: `com.informatica.jdbc.informix.InformixDriver` - DataDirect JDBC driver class name for MySQL: `com.informatica.jdbc.mysql.MySQLDriver` For more information about which driver class to use with specific databases, see the vendor documentation.
MetadataConnString	The URL that you use to connect to the database. The following list provides the connection string that you can enter for the applicable database type: - DataDirect JDBC driver for Oracle: `jdbc:informatica:oracle://<hostname>:<port>;SID=<sid>` - DataDirect JDBC driver for IBM DB2: `jdbc:informatica:db2://<hostname>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Microsoft SQL Server: `jdbc:informatica:sqlserver://<host>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Sybase ASE: `jdbc:informatica:sybase://<host>:<port>;DatabaseName=<database name>` - DataDirect JDBC driver for Informix: `jdbc:informatica:informix://<host>:<port>;informixServer=<informix server name>;databaseName=<dbName>` - DataDirect JDBC driver for MySQL: `jdbc:informatica:mysql://<host>:<port>;DatabaseName=<database name>` For more information about the connection string to use for specific databases, see the vendor documentation for the URL syntax.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Note:** Enclose special characters in double quotation marks.
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Note:** Enclose special characters in double quotes.

Option	Description
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is DOUBLE_QUOTE.
EnableQuotes	Optional. Select to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is True.
hadoopConnector	Required if you want to enable Sqoop connectivity for the data object that uses the JDBC connection. The Data Integration Service runs the mapping in the Hadoop run-time environment through Sqoop. You can configure Sqoop connectivity for relational data objects, customized data objects, and logical data objects that are based on a JDBC-compliant database. Set the value to `SQOOP_146` to enable Sqoop connectivity.

hadoopConnectorArgs	Optional. Enter the arguments that Sqoop must use to connect to the database. Enclose the Sqoop arguments within single quotes. Separate multiple arguments with a space.
	For example, `hadoopConnectorArgs='--<Sqoop argument 1> --<Sqoop argument 2>'`
	To read data from or write data to Teradata through Teradata Connector for Hadoop (TDCH) specialized connectors for Sqoop, define the TDCH connection factory class in the hadoopConnectorArgs argument. The connection factory class varies based on the TDCH Sqoop Connector that you want to use.
	- To use Cloudera Connector Powered by Teradata, configure the hadoopConnectorArgs argument as follows:
	`hadoopConnectorArgs='-Dsqoop.connection.factories=com.cloudera.connector.teradata.TeradataManagerFactory'`
	- To use Hortonworks Connector for Teradata (powered by the Teradata Connector for Hadoop), configure the hadoopConnectorArgs argument as follows:
	`hadoopConnectorArgs='-Dsqoop.connection.factories=org.apache.sqoop.teradata.TeradataManagerFactory'`
	If you do not enter Sqoop arguments, the Data Integration Service constructs the Sqoop command based on the JDBC connection properties.

JDBC V2 Connection Options

Use connection options to define a JDBC V2 connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example,

```
./infacmd.sh createConnection -dn Domain_irl63ppd06 -un Administrator -pd SAM123 -cn
PostgreSQL -cid PostgreSQL -ct JDBC_V2 -cun
adaptersX1 -cpd adaptersX1 -o "connectionstring=' jdbc:postgresql://aurorapostgres-
appsdk.c5wj9sntucrg.ap-south-1.rds.amazonaws.com:5432/
JDBCV2' jdbcdriverclassname='org.postgresql.Driver' schemaname='public'
subtype='PostgreSQL' supportmixedcaseidentifier='true'
quoteChar='(quotes)'"
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes JDBC V2 connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
username	The database user name. User name with permissions to either access the Azure SQL Database, PostgreSQL, or relational database.
password	The password for the database user name.
schemaname	The schema name to connect in the database.

jdbcdriverclassname	Name of the JDBC driver class.
	The following list provides the driver class name that you can enter for the applicable database type:
	- JDBC driver class name for Azure SQL Database:
	`com.microsoft.sqlserver.jdbc.SQLServerDriver`
	- JDBC driver class name for Aurora PostgreSQL:
	`org.postgresql.Driver`
	For more information about which driver class to use with specific databases, see the vendor documentation.

connectionstring	Connection string to connect to the database.
	Use the following connection string:
	`'jdbc:<subprotocol>:<subname>'`
	Enclose the connection string in double quotes.
	The following list provides sample connection strings that you can enter for the applicable database type:
	- Connection string for Azure SQL Database JDBC driver:
	`'jdbc:informatica:oracle://<host>:<port>;SID=<'value'>'`
	- Connection string for Aurora PostgreSQL JDBC driver:
	`'jdbc:postgresql://<host>:<port>[/dbname]'`
	For more information about the connection string to use with specific drivers, see the vendor documentation.

subtype	The database type to which you want to connect. You can select from the following database types to connect: - **Azure SQL Database**. Connects to Azure SQL Database. - **PostgreSQL**. Connects to Aurora PostgreSQL database. - **Others** . Connects to any database that supports the Type 4 JDBC driver.

Option	Description
supportmixedcaseidentifier	Enable if the database uses case-sensitive identifiers. When enabled, the Data Integration Service encloses all identifiers within the character selected for the **SQL Identifier Character** property. For example, PostgreSQL database supports mixed-cased characters. You must enable this property to connect to the PostgreSQL database. When the **SQL Identifier Character** property is set to none, the **Support Mixed-case Identifiers** property is disabled.
quoteChar	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select (None) if the database uses regular identifiers. When the Data Integration Service generates SQL queries, the service does not place delimited characters around any identifiers. Select a character if the database uses delimited identifiers. When the Data Integration Service generates SQL queries, the service encloses delimited identifiers within this character.

JD Edwards EnterpriseOne Connection Options

Use connection options to define a JD Edwards EnterpriseOne connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

For example,

```
infacmd.bat createConnection -dn DomainName  -un Domain_UserName -pd Domain_Pwd -cn
conName -cid
 conID -ct JDEE1 -o userName=JDEE1_DB_UserName password=JDEE1_DB_Pwd
enterpriseServer=JDE_ServerName
enterprisePort=JDE_DB_Port environment=JDE_Environment role=role
JDBCUserName=JDEE1_DB_UserName
JDBCPassword=JDEE1_DB_Pwd JDBCCONNECTIONSTRING='DB connection string'
JDBCDriverClassName='jdbc driver classname'
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other nonalphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory JD Edwards EnterpriseOne connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
userName	JD Edwards EnterpriseOne user name.
password	Password for the JD Edwards EnterpriseOne user name. The password is case sensitive.
enterpriseServer	The host name of the JD Edwards EnterpriseOne server that you want to access.
enterprisePort	The port number to access the JD Edwards EnterpriseOne server.
environment	Name of the JD Edwards EnterpriseOne environment you want to connect to.
role	Role of the JD Edwards EnterpriseOne user.

Kafka Connection Options

Use connection options to define a Kafka connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Kafka connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
connectionId	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
connectionType	Required. Type of connection is KAFKA.
name	Required. The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
connRetryTimeout	Number of seconds the Integration Service attempts to reconnect to the Kafka broker. If the source or target is not available for the time you specify, the mapping execution stops to avoid any data loss.
kafkaBrokerVersion	The version of the Kafka messaging broker. You can enter one of the following values: - 0.10.1.x-2.0.0
kfkBrkList	The IP address and port combinations of the Kafka messaging system broker list. The IP address and port combination has the following format: <IP Address>:<port> You can enter multiple comma-separated IP address and port combinations
zkHostPortList	The IP address and port combination of Apache ZooKeeper which maintains the configuration of the Kafka messaging broker. The IP address and port combination has the following format: <IP Address>:<port> You can enter multiple comma-separated IP address and port combinations.

Kudu Connection Options

Use connection options to define an Kudu connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Kudu connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 4,000 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select Kudu.

LDAP Connection Options

Use connection options to define an LDAP connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

For example,

```
infacmd.sh createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
conname -cid conname -ct ldap -o
 hostName=hostIPAddress port=port_number userName=ldapUserName password=LDAPPWD
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other nonalphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory LDAP connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
hostName	The host name of the LDAP directory server that you want to access.
port	The port number to access the LDAP directory server.
userName	LDAP user name.
password	Password for the LDAP user name. The password is case sensitive.

LinkedIn Connection Options

Use connection options to define a LinkedIn connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes LinkedIn connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
ConsumerKey	The API key that you get when you create the application in LinkedIn. LinkedIn uses the key to identify the application.
ConsumerSecret	The Secret key that you get when you create the application in LinkedIn. LinkedIn uses the secret to establish ownership of the consumer key.
AccessToken	Access token that the OAuth Utility returns. The LinkedIn application uses this token instead of the user credentials to access the protected resources.
AccessSecret	Access secret that the OAuth Utility returns. The secret establishes ownership of a token.

MapR-DB Connection Options

Use connection options to define an HBase connection for MapR-DB.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the HBase connection options for MapR-DB for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
DATABASETYPE	Required. Set the value to `MapR-DB` and enclose the value in single quotes.
clusterConfigId	The cluster configuration ID associated with the Hadoop cluster. You must enter a configuration ID to set up an HBase connection for MapR-DB.
maprdbpath	Required. Set the value to the database path that contains the MapR-DB table that you want to connect to. Enter a valid MapR cluster path. Enclose the value in single quotes. When you create an HBase data object for MapR-DB, you can browse only tables that exist in the path that you specify in this option. You cannot access tables that are available in sub-directories in the specified path. For example, if you specify the maprdbpath as `/user/customers/`, you can access the tables in the `customers` directory. However, if the `customers` directory contains a sub-directory named `regions`, you cannot access the tables in the following directory: `/user/customers/regions`

Microsoft Azure Blob Storage Connection Options

Use connection options to define a Microsoft Azure Blob Storage Connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Microsoft Azure Blob Storage Connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
accountName	Name of the Microsoft Azure Blob Storage account.
authenticationtype	Authorization type. You can select any of the following authorization mechanisms: - Shared Key Authorization - Shared Access Signatures
accountKey	Microsoft Azure Blob Storage access key.
sharedaccesssignature	Shared Access Signatures. **Note:** Even if you do not want to use shared access permission to create a connection, define the option in the command line as follows: `sharedaccesssignature=' '`
containerName	The root container or sub-folders with the absolute path.
enspointSuffix	Type of Microsoft Azure end-points. You can specify any of the following end-points: - `core.windows.net`: Default - `core.usgovcloudapi.net`: To select the US government Microsoft Azure end-points - `core.chinacloudapi.cn`: Not applicable

Microsoft Azure Data Lake Storage Gen1 Connection Options

Use connection options to define a Microsoft Azure Data Lake Storage Gen1 Connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Microsoft Azure Data Lake Storage Gen1 Connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
ADLSAccountName	Microsoft Azure Data Lake Storage Gen1 account name or the service name.
ClientId	The ID of your application to complete the OAuth Authentication in the Active Directory.
ClientSecret	The client secret key to complete the OAuth Authentication in the Active Directory.
Directory	Path of an existing directory under given file system. The default is root directory.
AuthEndpoint	The OAuth 2.0 token endpoint from where access code is generated based on the Client ID and Client secret is completed.

For more information about creating a client ID and client secret, contact the Azure administrator or see Microsoft Azure Data Lake Storage Gen1 documentation.

Microsoft Azure Data Lake Storage Gen2 Connection Options

Use connection options to define a Microsoft Azure Data Lake Storage Gen2 Connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Microsoft Azure Data Lake Storage Gen2 Connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
accountName	Microsoft Azure Data Lake Storage Gen2 account name or the service name.
clientID	The ID of your application to complete the OAuth Authentication in the Active Directory.
clientSecret	Client secret key to complete the OAuth Authentication in the Active Directory.
tenantID	Directory ID of the Azure Active Directory.

Option	Description
fileSystemName	Name of an existing file system in Microsoft Azure Data Lake Storage Gen2.
directoryPath	Path of an existing directory under given file system. The default is root directory.

For more information about creating a client ID, client secret, tenant ID, and file system name, contact the Azure administrator or see Microsoft Azure Data Lake Storage Gen2 documentation.

Microsoft Azure SQL Data Warehouse Connection Options

Use connection options to define a Microsoft Azure SQL Data Warehouse Connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Microsoft Azure SQL Data Warehouse Connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
JdbcUrl	Microsoft Azure SQL Data Warehouse JDBC connection string. For example, you can enter the following connection string: `jdbc:sqlserver://<Server>.database.windows.net:1433;database=<Database>`
JdbcUsername	User name to connect to the Microsoft Azure SQL Data Warehouse account.
JdbcPassword	Password to connect to the Microsoft Azure SQL Data Warehouse account.
SchemaName	Name of the schema in Microsoft Azure SQL Data Warehouse.
BlobAccountName	Name of the Microsoft Azure Storage account to stage the files.
BlobAccountKey	Microsoft Azure Storage access key to stage the files.
EndPointSuffix	Type of Microsoft Azure end-points. You can specify any of the following end-points: - `core.windows.net`: Default - `core.usgovcloudapi.net`: To select the US government Microsoft Azure end-points - `core.chinacloudapi.cn`: Not applicable
VNetRule	Enable to connect to a Microsoft Azure SQL Data Warehouse endpoint residing in a virtual network (VNet).
ADLSAccountName	Name of the Azure Data Lake Storage account to stage the files.
ADLSAccountKey	Azure Data Lake Storage access key to stage the files.

Microsoft SQL Server Connection Options

Use connection options to define the Microsoft SQL Server connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Microsoft SQL Server connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
UseTrustedConnection	Optional. The Integration Service uses Windows authentication to access the Microsoft SQL Server database. The user name that starts the Integration Service must be a valid Windows user with access to the Microsoft SQL Server database. True or false. Default is false.
PassThruEnabled	Optional. Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.

MetadataAccessConnectString	JDBC connection URL to access metadata from the database.
	Use the following connection URL:
	`jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name>`
	To test the connection with NTLM authentication, include the following parameters in the connection string:
	- AuthenticationMethod. The NTLM authentication version to use.
	Note: UNIX supports NTLMv1 and NTLMv2 but not NTLM.
	- Domain. The domain that the SQL server belongs to.
	The following example shows the connection string for an SQL server that uses NTLMv2 authentication in an NT domain named Informatica.com:
	`jdbc:informatica:sqlserver://host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com`
	If you connect with NTLM authentication, you can enable the **Use trusted connection** option in the MS SQL Server connection properties. If you connect with NTLMv1 or NTLMv2 authentication, you must provide the user name and password in the connection properties.

Option	Description
AdvancedJDBCSecurityOptions	Optional. Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and encrypts the parameter string. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. **Note:** For a complete list of the secure JDBC parameters, see the DataDirect JDBC documentation. Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.
DataAccessConnectString	Required. Connection string used to access data from the database. Enter the connection string in the following format: `<server name>@<database name>`
DomainName	Optional. The name of the domain where Microsoft SQL Server is running.
PacketSize	Optional. Increase the network packet size to allow larger packets of data to cross the network at one time.
CodePage	Required. Code to read from or write to the database. Use the ISO code page name, such as ISO-8859-6. The code page name is not case sensitive.
UseDSN	Required. Determines whether the Data Integration Service must use the Data Source Name for the connection. If you set the option value to true, the Data Integration Service retrieves the database name and server name from the DSN. If you set the option value to false, you must enter the database name and server name.
ProviderType	Required. The connection provider that you want to use to connect to the Microsoft SQL Server database. You can define one of the following values: - 0. Set the value to 0 if you want to use the ODBC provider type. Default is 0. - 1. Set the value to 1 if you want to use the OLEDB provider type.
OwnerName	Optional. The table owner name.

Option	Description
SchemaName	Optional. The name of the schema in the database. You must specify the schema name for the Profiling Warehouse if the schema name is different from the database user name. You must specify the schema name for the data object cache database if the schema name is different from the database user name and if you configure user-managed cache tables.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Note:** Enclose special characters in double quotes.
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Note:** Enclose special characters in double quotes.
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is 0.
EnableQuotes	Optional. Choose to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is True.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. Valid values are True or False. Default is True.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Microsoft Dynamics CRM Connection Options

Use connection options to define a Microsoft Dynamics CRM connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example,

```
./infacmd.sh createconnection -dn Domain_Adapters_1020_Uni -un Administrator -pd
Administrator -cn msd_cmdline_AD -cid msd_cmdline_edit -ct MSDYNAMICS -o
"AuthenticationType=Passport DiscoveryServiceURL=https://disco.crm8.dynamics.com/
XRMServices/2011/Discovery.svc Username=skmanja@InformaticaLLC.onmicrosoft.com
Password=AwesomeDay103 OrganizationName=org00faf3b6 Domain=<dummy value>
SECURITYTOKENSERVICE=<dummy value>"
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Microsoft Dynamics CRM connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
AuthenticationType	Required. Authentication type for the connection. Provide one of the following authentication types: - Passport. Often used for online deployment and online deployment combined with Internet-facing deployment of Microsoft Dynamics CRM. - Claims-based. Often used for on-premise and Internet-facing deployment of Microsoft Dynamics CRM. - Active directory. Often used for on-premise deployment of Microsoft Dynamics CRM.
DiscoveryServiceURL	Required. URL of the Microsoft Dynamics CRM service. Use the following format: `<http/https>://<Application server name>:<port>/XRMService/2011/Discovery.svc` To find the Discovery Service URL, log in to the Microsoft Live instance and click **Settings** > **Customization** > **Developer Resources**.
Domain	Required. Domain to which the user belongs. You must provide the complete domain name. For example, `msd.sampledomain.com`. Configure domain for active directory and claims-based authentication. **Note:** If you select Passport authentication type, you must provide a dummy value for Domain.
ConfigFilesForMetadata	Configuration directory for the client. Default directory is: `<INFA_HOME>/clients/DeveloperClient/msdcrm/conf`
OrganizationName	Required. Microsoft Dynamics CRM organization name. Organization names are case sensitive. For Microsoft Live authentication, use the Microsoft Live Organization Unique Name. To find the Organization Unique Name, log in to the Microsoft Live instance and click **Settings** > **Customization** > **Developer Resources**
Password	Required. Password to authenticate the user.
ConfigFilesForData	Configuration directory for the server. If the server file is located in a different directory, specify the directory path.
SecurityTokenService	Required. Microsoft Dynamics CRM security token service URL. For example, `https://sts1.<company>.com`. Configure for claims-based authentication. **Note:** If you select Passport or Active Directory authentication type, you must provide a dummy value for SecurityTokenService.

Option	Description
Username	Required. User ID registered with Microsoft Dynamics CRM.
UseMetadataConfigForDataAccess	Select this option if the configuration file and server file are in the same directory. If the server file is in a different directory, uncheck this option and specify the directory path in the Data Access field. Provide one of the following values: - true for checked - false for unchecked
KeyStoreFileName	Contains the keys and certificates required for secure communication. If you want to use the Java cacerts file, clear this field.
KeyStorePassword	Password for the `infa_keystore.jks` file. If you want to use the Java cacerts file, clear this field.
TrustStoreFileName	Set the INFA_TRUSTSTORE in the environment variables. The directory must contain the truststore file `infa_truststore.jks`. If the file is not available at the path specified, the Data Integration Service checks for the certificate in the Java cacerts file. If you want to use the Java cacerts file, clear this field.
TrustStorePassword	Password for the `infa_keystore.jks` file. If you want to use the Java cacerts file, clear this field.

Netezza Connection Options

Use connection options to define a Netezza connection.

Enter connection options in the following format:
... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Netezza connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
connectionString	Required. Name of the ODBC data source that you create to connect to the Netezza database.
jdbcUrl	Required. JDBC URL that the Developer tool must use when it connects to the Netezza database. Use the following format: jdbc:netezza://<hostname>:<port>/<database name>
username	Required. User name with the appropriate permissions to access the Netezza database.
password	Required. Password for the database user name.
timeout	Required. Number of seconds that the Developer tool waits for a response from the Netezza database before it closes the connection.

OData Connection Options

Use connection options to define an OData connection.

Enter connection options in the following format:
... -o option_name=value option_name=value ...

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the OData connection options for infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
URL	Required. OData service root URL that exposes the data that you want to read.
securityType	Optional. Security protocol that the Developer tool must use to establish a secure connection with the OData server. Enter one of the following values: - None - SSL - TLS
trustStoreFileName	Required if you enter a security type. Name of the truststore file that contains the public certificate for the OData server.
trustStorePassword	Required if you enter a security type. Password for the truststore file that contains the public certificate for the OData server.
keyStoreFileName	Required if you enter a security type. Name of the keystore file that contains the private key for the OData server.
keyStorePassword	Required if you enter a security type. Password for the keystore file that contains the private key for the OData server.

ODBC Connection Options

Use connection options to define the ODBC connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes ODBC connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
PassThruEnabled	Optional. Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
DataAccessConnectString	Connection string used to access data from the database. Enter the connection string in the following format: `<database name>`
CodePage	Required. Code page used to read from a source database or write to a target database or file.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Note:** Enclose special characters in double quotes.
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Note:** Enclose special characters in double quotes.
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is 4.
ODBC Provider	Optional. The type of database to which the Data Integration Service connects using ODBC. For pushdown optimization, specify the database type to enable the Data Integration Service to generate native database SQL. The options are as follows: - Other - Sybase - Microsoft_SQL_Server - Teradata - Netezza - Greenplum Default is Other.
EnableQuotes	Optional. Choose to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is False.

Option	Description
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. Valid values are True or False. Default is True.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idle time when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Oracle Connection Options

Use connection options to define the Oracle connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Oracle connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
PassThruEnabled	Optional. Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
MetadataAccessConnectString	JDBC connection URL used to access metadata from the database. jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>

Option	Description
AdvancedJDBCSecurityOptions	Optional. Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and encrypts the parameter string. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to true, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. - KeyStore. Required. Path and file name of the keystore file. - KeyStorePassword. Password for the keystore file for the secure database. **Note:** For a complete list of the secure JDBC parameters, see the DataDirect JDBC documentation. Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.
DataAccessConnectString	Connection string used to access data from the database. Enter the connection string in the following format from the TNSNAMES entry: `<database name>`
CodePage	Required. Code page used to read from a source database or write to a target database or file.
EnvironmentSQL	Optional. SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database. For example, `ALTER SESSION SET CURRENT_SCHEMA=INFA_USR;` **Note:** Enclose special characters in double quotes.
TransactionSQL	Optional. SQL commands to execute before each transaction. The Data Integration Service executes the transaction SQL at the beginning of each transaction. For example, `SET TRANSACTION ISOLATION LEVEL SERIALIZABLE;` **Note:** Enclose special characters in double quotes.
EnableParallelMode	Optional. Enables parallel processing when loading data into a table in bulk mode. Used for Oracle. True or false. Default is false.

Option	Description
QuoteChar	Optional. The character that you will use for quotes in this connection. The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the QuoteChar property. Default is 0.
EnableQuotes	Optional. Choose to enable quotes or not for this connection. When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. Valid values are True or False. Default is True.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. Valid values are True or False. Default is True.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdleTime	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinConnections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Salesforce Connection Options

Use connection options to define a Salesforce connection.

Enter connection options in the following format:
... -o option_name=value option_name=value ...

Example for Salesforce connection using `infacmd`

```
infacmd createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -cid Connection_ID -ct SALESFORCE -o userName=salesforceUserName
password=salesforcePWD SERVICE_URL=https://login.salesforce.com/services/Soap/u/42.0
```

Example for OAuth Salesforce connection using `pmcmd`

```
pmcmd createConnection -s Salesforce -n ConnectionName -u -p -l CodePage -k
ConnectionType=OAuth RefreshToken=salesforceRefreshToken
ConsumerKey=salesforceConsumerKey ConsumerSecret= salesforceConsumerSecret
Service_URL=https://login.salesforce.com/services/Soap/u/42.0
```

Example for Standard Salesforce connection using `pmcmd`

```
pmcmd createConnection -s Salesforce -n ConnectionName -u salesforceUserName -p
salesforcePWD -l CodePage -k ConnectionType=Standard Service_URL=https://
login.salesforce.com/services/Soap/u/42.0
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Salesforce connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
Username	Salesforce username.
Password	Password for the Salesforce user name. The password is case sensitive. To access Salesforce outside the trusted network of your organization, you must append a security token to your password to log in to the API or a desktop client. To receive or reset your security token, log in to Salesforce and click **Setup** > **My Personal Information** > **Reset My Security Token**.
Refresh Token	For OAuth Salesforce connection. The Refresh Token of Salesforce generated using the Consumer Key and Consumer Secret.
Consumer Key	For OAuth Salesforce connection. The Consumer Key obtained from Salesforce, required to generate the Refresh Token. For more information about how to generate the Consumer Key, see the Salesforce documentation.
Consumer Secret	For OAuth Salesforce connection. The Consumer Secret obtained from Salesforce, required to generate the Refresh Token. For more information about how to generate the Consumer Secret, see the Salesforce documentation.
Connection Type	Select the Standard or OAuth Salesforce connection.
Service URL	URL of the Salesforce service that you want to access. In a test or development environment, you might want to access the Salesforce Sandbox testing environment. For more information about the Salesforce Sandbox, see the Salesforce documentation.

Salesforce Marketing Cloud Connection Options

Use connection options to define a Salesforce Marketing Cloud connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

Example for infacmd createConnection command:

```
./infacmd.sh createConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -cid Connection_ID -ct SFMC -o salesforce_marketing_cloud_url=https://
webservice.s7.exacttarget.com/etframework.wsdl userName=SFMCUserName password=SFMCpwd
clientid=SFMCclientid clientsecret=SFMCclientsecret enable_logging=true UTC_Offset=UTC+05:30
Batch_Size=1
```

Example for infacmd updateConnection command:

```
./infacmd.sh updateConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name -o salesforce_marketing_cloud_url=https://
mc6tbszr9y72l86wknwg5w3c3k7q.soap.marketingcloudapis.com/etframework.wsdl
```

```
userName=SFMCUserName password=SFMCpwd clientid=SFMCclientid clientsecret=SFMCclientsecret
enable_logging=true UTC_Offset=UTC+05:30 Batch_Size=1
```

Example for infacmd removeConnection command:

```
./infacmd.sh removeConnection -dn DomainName -un Domain_UserName -pd Domain_Pwd -cn
Connection_Name
```

The following table describes Salesforce Marketing Cloud connection options for infacmd.sh createConnection, updateConnection, and remove commands:

Connection property	Description
Domain Name	Informatica domain where you want to create the connection.
Domain User Name	User name of the domain.
Domain Password	Password for the domain.
Connection Name	Name of the Salesforce Marketing Cloud connection.
Connection ID	The Data Integration Service uses the ID to identify the connection.

Salesforce Marketing Cloud Url	The URL that the Data Integration Service uses to connect to the Salesforce Marketing Cloud WSDL.
	The following URL is an example for OAuth 1.0 URL:
	`https://webservice.s7.exacttarget.com/etframework.wsdl`
	The following URL is an example for OAuth 2.0 URL:
	`https://<SUBDOMAIN>.soap.marketingcloudapis.com/etframework.wsdl`
	Informatica recommends that you upgrade to OAuth 2.0 before Salesforce Marketing Cloud drops support for OAuth 1.0.

Username	User name of the Salesforce Marketing Cloud account.
Password	Password for the Salesforce Marketing Cloud account.
ClientId	The client ID of Salesforce Marketing Cloud required to generate a valid access token.
ClientSecret	The client secret of Salesforce Marketing Cloud required to generate a valid access token.
Enable Logging	When you enable logging you can see the session log for the tasks.
UTC Offset	The Secure Agent uses the UTC offset connection property to read data from and write data to Salesforce Marketing Cloud in UTC offset time zone.
Batch Size	Number of rows that the Secure Agent writes in a batch to the target. When you insert or update data and specify the contact key, the data associated with the specified contact ID is inserted or updated in a batch to Salesforce Marketing Cloud. When you upsert data to Salesforce Marketing Cloud, do not specify the contact key.

SAPAPPLICATIONS Connection Options

Use connection options to define the SAPAPPLICATIONS connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes SAPAPPLICATIONS connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
UserName	Required. SAP system user name.
Password	Required. Password for the user name.
HostName	Required. Host name of the SAP application.
ClientNumber	Required. SAP client number.
SystemNumber	Required. SAP system number.
Language	Optional. SAP Logon language.

Sequential Connection Options

Use SEQ connection options to define a connection to a sequential z/OS data set.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes SEQ connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
CodePage	Required. Code to read from or write to the sequential file. Use the ISO code page name, such as ISO-8859-6. The code page name is not case sensitive.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.
Compression	Optional. Compresses the data to decrease the amount of data that Informatica applications write over the network. True or false. Default is false.

Option	Description
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Enter one of the following values for the encryption type: - None - AES Default is None. Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.
InterpretAsRows	Optional. If true, the pacing size value represents a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange Listener node that can connect to the data source. The location is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
OffLoadProcessing	Optional. Moves bulk data processing from the data source machine to the Data Integration Service machine. Enter one of the following values: - Auto. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is Auto.
PacingSize	Optional. Slows the data transfer rate in order to reduce bottlenecks. The lower the value, the greater the session performance. Minimum value is 0. Enter 0 for optimal performance. Default is 0.
WorkerThread	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the Data Integration Service and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the Data Integration Service without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the Data Integration Service asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. True or false. Default is false.

Option	Description
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdle Time	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinCon nections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Snowflake Connection Options

Use connection options to define a Snowflake connection.

Enter connection options in the following format:

... -o option_name=value option_name=value ...

For example,

```
./infacmd.sh createconnection -dn Domain_Snowflake -un Administartor -pd Administrator -
cn Snowflake_CLI -ct SNOWFLAKE -o "user=INFAADPQA password=passwd account=informatica
role=ROLE_PC_AUTO  warehouse=QAAUTO_WH"
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other nonalphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory Snowflake connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Property	Description
connectionId	String that the Data Integration Service uses to identify the connection.
connectionType	The connection type. Type of connection is SnowFlake.
name	The name of the connection.
account	The name of the Snowflake account.

additionalparam	Enter one or more JDBC connection parameters in the following format:
	`<param1>=<value>&<param2>=<value>&<param3>=<value>....`
	For example:
	`user=jon&warehouse=mywh&db=mydb&schema=public`

password	The password to connect to the Snowflake account.
role	The Snowflake role assigned to the user.

Property	Description
user	The user name to connect to the Snowflake account.
warehouse	The Snowflake warehouse name.

Tableau Connection Options

Use connection options to define a Tableau connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example,

```
./infacmd.sh createconnection -dn Domain -un Username -pd Password -cn Connection name -
ct TABLEAU -o "connectionURL= contentURL= password= tableauProduct='Tableau Server'
username=infaadmin site='' tabcmdInstallLocation='' tableauServer=true"
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other nonalphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory Tableau connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Connection Property	Description
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the TDE or TWBX file: - Tableau Desktop. Creates a TDE file in the Data Integration Service machine. You can then manually import the TDE file to Tableau Desktop. - Tableau Server. Publishes the generated TDE or TWBX file to Tableau Server. - Tableau Online. Publishes the generated TDE or TWBX file to Tableau Online.
Connection URL	URL of Tableau Server or Tableau Online to which you want to publish the TDE or TWBX file. The URL has the following format: `http://<Host name of Tableau Server or Tableau Online>:<port>`
User Name	User name of the Tableau Server or Tableau Online account.
Password	Password for the Tableau Server or Tableau Online account.
Content URL	The name of the site on Tableau Server or Tableau Online where you want to publish the TDE or TWBX file. Contact the Tableau administrator to provide the site name.

Tableau V3 Connection Options

Use connection options to define a Tableau V3 connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

For example,

```
./infacmd.sh createConnection -dn Domain -un Username -pd Password -cn Connection name -
ct tableau_server -ct TABLEAU V3 -o "connectionURL= site= password=
tableauProduct='Tableau Server' username="
```

To enter multiple options, separate options with spaces. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the mandatory Tableau V3 connection options for the infacmd isp CreateConnection and UpdateConnection commands:

Connection Property	Description
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the `.hyper` or TWBX file: **Tableau Desktop** Creates a `.hyper` file in the Data Integration Service machine. You can then manually import the `.hyper` file to Tableau Desktop. **Tableau Server** Publishes the generated `.hyper` or TWBX file to Tableau Server. **Tableau Online** Publishes the generated `.hyper` or TWBX file to Tableau Online.
Connection URL	The URL of Tableau Server or Tableau Online to which you want to publish the `.hyper` or TWBX file. Enter the URL in the following format: `http://<Host name of Tableau Server or Tableau Online>:<port>`
User Name	The user name of the Tableau Server or Tableau Online account.
Password	The password for the Tableau Server or Tableau Online account.
Site ID	The ID of the site on Tableau Server or Tableau Online where you want to publish the or TWBX file. **Note:** Contact the Tableau administrator to provide the site ID.
Schema File Path	The path to a sample `.hyper` file from where the Data Integration Service imports the Tableau metadata. Enter one of the following options for the schema file path: - Absolute path to the `.hyper` file. - Directory path for the `.hyper` files. - Empty directory path. The path you specify for the schema file becomes the default path for the target `.hyper` file. If you do not specify a file path, the Data Integration Service uses the following default file path for the target `.hyper` file: `<Data Integration Service installation directory>/apps/Data_Integration_Server/<latest version>/bin/rtdm`

Teradata Parallel Transporter Connection Options

Use connection options to define a Teradata PT connection.

Enter connection options in the following format:

```
... -o option_name='value' option_name='value' ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Teradata PT connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
UserName	Required. Teradata database user name with the appropriate write permissions to access the database.
Password	Required. Password for the Teradata database user name.
DriverName	Required. Name of the Teradata JDBC driver.
ConnectionString	Required. JDBC URL to fetch metadata.
TDPID	Required. Name or IP address of the Teradata database machine.
databaseName	Required. Teradata database name. If you do not enter a database name, Teradata PT API uses the default login database name.
DataCodePage	Optional. Code page associated with the database. When you run a mapping that loads to a Teradata target, the code page of the Teradata PT connection must be the same as the code page of the Teradata target. Default is UTF-8.
Tenacity	Optional. Number of hours that Teradata PT API continues trying to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 4.
MaxSessions	Optional. Maximum number of sessions that Teradata PT API establishes with the Teradata database. Must be a positive, non-zero integer. Default is 4.
MinSessions	Optional. Minimum number of Teradata PT API sessions required for the Teradata PT API job to continue. Must be a positive integer between 1 and the Max Sessions value. Default is 1.
Sleep	Optional. Number of minutes that Teradata PT API pauses before it retries to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 6.
useMetadataJdbcUrl	Optional. Set this option to true to Indicate that the Teradata Connector for Hadoop (TDCH) must use the JDBC URL that you specified in the connection string. Set this option to false to specify a different JDBC URL that TDCH must use when it runs the mapping.

Option	Description
tdchJdbcUrl	Required. JDBC URL that TDCH must use when it runs the mapping.
dataEncryption	Required. Enables full security encryption of SQL requests, responses, and data on Windows. To enable data encryption on Unix, add the command UseDataEncryption=Yes to the DSN in the odbc.ini file.
authenticationType	Required. Authenticates the user. Enter of the following values for the type of the authentication: - Native. Authenticates your user name and password against the Teradata database specified in the connection. - LDAP. Authenticates user credentials against the external LDAP directory service. Default is Native.
hadoopConnector	Required if you want to enable Sqoop connectivity for the data object that uses the JDBC connection. The Data Integration Service runs the mapping in the Hadoop run-time environment through Sqoop. You can configure Sqoop connectivity for relational data objects, customized data objects, and logical data objects that are based on a JDBC-compliant database. Set the value to `SQOOP_146` to enable Sqoop connectivity.

hadoopConnectorArgs	Optional. Enter the arguments that Sqoop must use to connect to the database. Enclose the Sqoop arguments within single quotes. Separate multiple arguments with a space.
	For example, `hadoopConnectorArgs='--<Sqoop argument 1> --<Sqoop argument 2>'`
	To read data from or write data to Teradata through Teradata Connector for Hadoop (TDCH) specialized connectors for Sqoop, define the TDCH connection factory class in the hadoopConnectorArgs argument. The connection factory class varies based on the TDCH Sqoop Connector that you want to use.
	- To use Cloudera Connector Powered by Teradata, configure the hadoopConnectorArgs argument as follows:
	`hadoopConnectorArgs='-Dsqoop.connection.factories=com.cloudera.connector.teradata.TeradataManagerFactory'`
	- To use Hortonworks Connector for Teradata (powered by the Teradata Connector for Hadoop), configure the hadoopConnectorArgs argument as follows:
	`hadoopConnectorArgs='-Dsqoop.connection.factories=org.apache.sqoop.teradata.TeradataManagerFactory'`
	If you do not enter Sqoop arguments, the Data Integration Service constructs the Sqoop command based on the JDBC connection properties.

Twitter Connection Options

Use connection options to define a Twitter connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Twitter connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
ConsumerKey	The consumer key that you get when you create the application in Twitter. Twitter uses the key to identify the application.
ConsumerSecret	The consumer secret that you get when you create the Twitter application. Twitter uses the secret to establish ownership of the consumer key.
AccessToken	Access token that the OAuth Utility returns. Twitter uses this token instead of the user credentials to access the protected resources.
AccessSecret	Access secret that the OAuth Utility returns. The secret establishes ownership of a token.

Twitter Streaming Connection Options

Use connection options to define a Twitter Streaming connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Twitter Streaming connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
HoseType	Streaming API methods. You can specify the following methods: - Filter. The Twitter `statuses/filter` method returns public statuses that match the search criteria. - Sample. The Twitter `statuses/sample` method returns a random sample of all public statuses.
UserName	Twitter user screen name.
Password	Twitter password.

VSAM Connection Options

Use connection options to define a VSAM connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes VSAM connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
CodePage	Required. Code to read from or write to the VSAM file. Use the ISO code page name, such as ISO-8859-6. The code page name is not case sensitive.
ArraySize	Optional. Determines the number of records in the storage array for the threads when the worker threads value is greater than 0. Valid values are from 1 through 5000. Default is 25.
Compression	Optional. Compresses the data to decrease the amount of data Informatica applications write over the network. True or false. Default is false.
EncryptionLevel	Optional. Level of encryption. If you specify AES for the EncryptionType option, specify one of the following values to indicate the level of AES encryption: - 1. Use a 128-bit encryption key. - 2. Use a 192-bit encryption key. - 3. Use a 256-bit encryption key. Default is 1. **Note:** If you specify None for encryption type, the Data Integration Service ignores the encryption level value.
EncryptionType	Optional. Controls whether to use encryption. Specify one of the following values: - None - AES Default is None.
InterpretAsRows	Optional. If true, the pacing size value represents a number of rows. If false, the pacing size represents kilobytes. Default is false.
Location	Location of the PowerExchange listener node that can connect to VSAM. The node is defined in the PowerExchange dbmover.cfg configuration file.
OffLoadProcessing	Optional. Moves bulk data processing from the VSAM source to the Data Integration Service machine. Enter one of the following values: - Auto. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is Auto.
PacingSize	Optional. Slows the data transfer rate in order to reduce bottlenecks. The lower the value, the greater the session performance. Minimum value is 0. Enter 0 for optimal performance. Default is 0.
WorkerThread	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.

Option	Description
WriteMode	Enter one of the following write modes: - CONFIRMWRITEON. Sends data to the Data Integration Service and waits for a success/no success response before sending more data. - CONFIRMWRITEOFF. Sends data to the Data Integration Service without waiting for a success/no success response. Use this option when the target table can be reloaded if an error occurs. - ASYNCHRONOUSWITHFAULTT. Sends data to the Data Integration Service asynchronously with the ability to detect errors. Default is CONFIRMWRITEON.
EnableConnectionPool	Optional. Enables connection pooling. When you enable connection pooling, the connection pool retains idle connection instances in memory. When you disable connection pooling, the Data Integration Service stops all pooling activity. True or false. Default is false.
ConnectionPoolSize	Optional. Maximum number of idle connections instances that the Data Integration Service maintains for a database connection. Set this value to be more than the minimum number of idle connection instances. Default is 15.
ConnectionPoolMaxIdle Time	Optional. Number of seconds that a connection exceeding the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idletime when it does not exceed the minimum number of idle connection instances. Default is 120.
ConnectionPoolMinCon nections	Optional. Minimum number of idle connection instances that the pool maintains for a database connection. Set this value to be equal to or less than the idle connection pool size. Default is 0.

Web Content-Kapow Katalyst Connection Options

Use connection options to define a Web Content-Kapow Katalyst connection.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Web Content-Kapow Katalyst connection options for infacmd isp CreateConnection and UpdateConnection commands:

Option	Description
ManagementConsoleURL	URL of the Local Management Console where the robot is uploaded. The URL must start with http or https. For example, http://localhost:50080.
RQLServicePort	The port number where the socket service listens for the RQL service. Enter a value from 1 through 65535. Default is 50000.
Username	User name required to access the Local Management Console.
Password	Password to access the Local Management Console.

CreateFolder

Creates a folder in the domain. When you create a folder, infacmd creates the folder in the domain or folder you specify.

You can use folders to organize objects and to manage security. Folders can contain nodes, services, grids, licenses, and other folders.

The infacmd isp CreateFolder command uses the following syntax:

```
CreateFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderName|-fn> folder_name
<-FolderPath|-fp> full_folder_path
[<-FolderDescription|-fd> description_of_folder]
```

The following table describes infacmd isp CreateFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-FolderName -fn	folder_name	Required. Name of the folder. Folder names must be unique within a folder or the domain. It cannot contain spaces or exceed 79 characters in length.
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, where you want to create the folder. Must be in the following format: */parent_folder/child_folder*
-FolderDescription -fd	description_of_folder	Optional. Description of the folder. If the folder description contains spaces or other non-alphanumeric characters, enclose it in quotation marks.

CreateGrid

Creates a grid in the domain and assigns nodes to the grid. Create a grid to distribute jobs to service processes running on nodes in the grid.

The infacmd isp CreateGrid command uses the following syntax:

```
CreateGrid

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
<-NodeList|-nl> node1 node2 ...
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd isp CreateGrid options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GridName -gn	grid_name	Required. Name of the grid.

Option	Argument	Description
-NodeList -nl	node1 node2 ...	Required. Names of the nodes you want to assign to the grid.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the grid. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).

CreateGroup

Creates a group in the native security domain. You can assign roles, permissions, and privileges to a group in the native or an LDAP security domain. The roles, permissions, and privileges assigned to the group determines the tasks that users in the group can perform within the domain.

The infacmd isp CreateGroup command uses the following syntax:

```
CreateGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupDescription|-ds> group_description]
```

The following table describes infacmd isp CreateGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group. The group name is not case sensitive and can be between 1 and 80 characters long. It cannot include a tab, newline character, or the following special characters: `, + " \ < > ; / * % ?` The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
-GroupDescription -ds	group_description	Optional. Description of the group. To enter a description that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The description cannot include the following special characters: `< > “`

CreateIntegrationService

Creates a PowerCenter Integration Service in a domain.

By default, the PowerCenter Integration Service is enabled when you create it.

The infacmd isp CreateIntegrationService command uses the following syntax:

```
CreateIntegrationService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-FolderPath|-fp> full_folder_path]
<<-NodeName|-nn> node_name|<-GridName|-gn> grid_name>
[<-BackupNodes|-bn> node1 node2 ...]
<-RepositoryService|-rs> repository_service_name
[<-RepositoryUser|-ru> repository_user]
[<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceDisable|-sd>]
[<-ServiceOptions|-so> option_name=value ...]
[<-ServiceProcessOptions|-po> option_name=value ...]
[<-EnvironmentVariables|-ev> name=value ...]
[<-LicenseName|-ln> license_name]
```

Note: For infacmd isp CreateIntegrationService, you must not use the -ru, -rp, and the -rsdn options in Kerberos authentication. If you use these options in Kerberos mode, the command will fail.

The following table describes infacmd isp CreateIntegrationService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the PowerCenter Integration Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot have leading or trailing spaces, include carriage returns or tabs, exceed 79 characters, or contain the following characters: `/ * ? < > " |`
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the Integration Service. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).
-NodeName -nn	node_name	Required if you do not specify the grid name. Name of the node where you want the PowerCenter Integration Service process to run. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node. To apply changes, restart the Integration Service.

Option	Argument	Description
-GridName -gn	grid_name	Required if you do not specify the node name. Name of the grid where you want the PowerCenter Integration Service process to run. To apply changes, restart the PowerCenter Integration Service.
-BackupNodes -bn	node1 node2 ...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-RepositoryService -rs	repository_service_name	Required. Name of the PowerCenter Repository Service that the PowerCenter Integration Service depends on. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks. To apply changes, restart the PowerCenter Integration Service.
-RepositoryUser -ru	repository_user	Required for native or LDAP authentication. User name used to connect to the PowerCenter repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks. To apply changes, restart the PowerCenter Integration Service.
-RepositoryPassword -rp	repository_password	Required for native or LDAP authentication. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence. To apply changes, restart the PowerCenter Integration Service.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required for LDAP. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If you do not specify this option, the command sets the repository user security domain to native.
-ServiceDisable -sd	-	Optional. Creates a disabled service. You must enable the service before you can run it.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the PowerCenter Integration Service runs.
-ServiceProcessOptions -po	option_name=value	Optional. Service process properties for the PowerCenter Integration Service. In a grid or multi-node environment, infacmd applies these properties to the primary node, grid, and backup node.

Option	Argument	Description
-EnvironmentVariables -ev	name=value	Optional. Specify environment variables as PowerCenter Integration Service process options. You may want to include additional variables that are unique to your PowerCenter environment. To apply changes, restart the node.
-LicenseName -ln	license_name	Required if you create an enabled service. Name of the license you want to assign to the PowerCenter Integration Service. To apply changes, restart the PowerCenter Integration Service.

Integration Service Options

Enter Integration Service options in the following format:

```
infacmd CreateIntegrationService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Integration Service options:

Option	Description
$PMFailureEmailUser	Optional. Email address of the user to receive email when a session fails to complete. To enter multiple addresses on Windows, use a distribution list. To enter multiple addresses on UNIX, separate them with a comma.
$PMSessionErrorThreshold	Optional. Number of non-fatal errors the Integration Service allows before failing the session. Default is 0 (non-fatal errors do not cause the session to stop).
$PMSessionLogCount	Optional. Number of session logs the Integration Service archives for the session. Minimum value is 0. Default is 0.
$PMSuccessEmailUser	Optional. Email address of the user to receive email when a session completes successfully. To enter multiple addresses on Windows, use a distribution list. To enter multiple addresses on UNIX, separate them with a comma.
$PMWorkflowLogCount	Optional. Number of workflow logs the Integration Service archives for the workflow. Minimum value is 0. Default is 0.
AggregateTreatNullAsZero	Optional. Treats nulls as zero in Aggregator transformations. Default is No.
AggregateTreatRowAsInsert	Optional. Performs aggregate calculations before flagging records for insert, update, delete, or reject in Update Strategy expressions. Default is No.

Option	Description

ClientStore	Optional. Enter the value for ClientStore using the following syntax:
	`<path>/<filename>`
	For example:
	`./Certs/client.keystore`

CreateIndicatorFiles	Optional. Creates indicator files when you run a workflow with a flat file target. Default is No.
DataMovementMode	Optional. Mode that determines how the Integration Service handles character data: - ASCII - Unicode Default is ASCII.
DateDisplayFormat	Optional. Date format the Integration Service uses in log entries. Default is DY MON DD HH 24:MI:SS YYYY.
DateHandling40Compatibility	Optional. Handles dates as in PowerCenter 1.0/PowerMart 4.0. Default is No.
DeadlockSleep	Optional. Number of seconds before the Integration Service retries writing to a target on database deadlock. Minimum value is 0. Maximum value is 2592000. Default is 0 (retry the target write immediately).
ErrorSeverityLevel	Optional. Minimum level of error logging for the Integration Service logs: - Fatal - Error - Warning - Info - Trace - Debug Default is Info.
ExportSessionLogLibName	Optional. Name of an external library file to write session log messages.
FlushGMDWrite	Required if you enable session recovery. Flushes session recovery data for the recovery file from the operating system buffer to the disk. Specify one of the following levels: - Auto. Flushes recovery data for all real-time sessions with a JMS or WebSphere MQ source and a non-relational target. - Yes. Flushes recovery data for all sessions. - No. Does not flush recovery data. Select this option if you have highly available external systems or if you need to optimize performance. Default is Auto.
HttpProxyDomain	Optional. Domain for authentication.

Option	Description
HttpProxyPassword	Required if the proxy server requires authentication. Password for the authenticated user.
HttpProxyPort	Optional. Port number of the HTTP proxy server.
HttpProxyServer	Optional. Name of the HTTP proxy server.
HttpProxyUser	Required if the proxy server requires authentication. Authenticated user name for the HTTP proxy server.
IgnoreResourceRequirements	Optional. Ignores task resource requirements when distributing tasks across the nodes of a grid. Default is Yes.
JCEProvider	Optional. JCEProvider class name to support NTLM authentication. For example: `com.unix.crypto.provider.UnixJCE.`
JoinerSourceOrder6xCompatibility	Optional. Processes master and detail pipelines sequentially as in PowerCenter versions prior to 7.0. Default is No.
LoadManagerAllowDebugging	Optional. Allows you to use this Integration Service to run debugger sessions from the Designer. Default is Yes.
LogsInUTF8	Optional. Writes all logs using the UTF-8 character set. Default is Yes (Unicode) or No (ASCII).
MSExchangeProfile	Optional. Microsoft Exchange profile used by the Service Start Account to send post-session email.
MaxLookupSPDBConnections	Optional. Maximum number of connections to a lookup or stored procedure database when you start a session. Minimum value is 0. Default is 0.
MaxMSSQLConnections	Optional. Maximum number of connections to a Microsoft SQL Server database when you start a session. Minimum value is 100. Maximum value is 2,147,483,647. Default is 100.
MaxResilienceTimeout	Optional. Maximum amount of time in seconds that the service holds on to resources for resilience purposes. Minimum value is 0. Maximum value is 2592000. Default is 180.
MaxSybaseConnections	Optional. Maximum number of connections to a Sybase database when you start a session. Minimum value is 100. Maximum value is 2,147,483,647. Default is 100.
NumOfDeadlockRetries	Optional. Number of times the Integration Service retries writing to a target on a database deadlock. Minimum value is 10. Maximum value is 1,000,000,000. Default is 10.
OperatingMode	Optional. Operating mode for the Integration Service: - Normal - Safe Default is Normal.

Option	Description
OperatingModeOnFailover	Optional. Operating mode for the Integration Service when the service process fails over: - Normal - Safe Default is Normal.
OutputMetaDataForFF	Optional. Writes column headers to flat file targets. Default is No.
PersistRuntimeStatsToRepo	Optional. Level of run-time information stored in the repository. Specify one of the following levels: - None. Integration Service does not store any session or workflow run-time information in the repository. - Normal. Integration Service stores workflow details, task details, session statistics, and source and target statistics in the repository. - Verbose. Integration Service stores workflow details, task details, session statistics, source and target statistics, partition details, and performance details in the repository. Default is Normal.
Pmserver3XCompatibility	Optional. Handles Aggregator transformations as the PowerMart Server did in PowerMart 3.5. Default is No.
RunImpactedSessions	Optional. Runs sessions that are impacted by dependency updates. Default is No.
ServiceResilienceTimeout	Optional. Amount of time in seconds that the service tries to establish or reestablish a connection to another service. Minimum value is 0. Maximum value is 2592000. Default is 180.
StoreHAPersistenceInDB	Optional. Stores process state information in persistence database tables in the associated PowerCenter repository database. Default is no.
TimestampWorkflowLogMessages	Optional. Appends a timestamp to messages written to the workflow log. Default is No.
TreatCharAsCharOnRead	Optional. Keeps trailing spaces when reading SAP or PeopleSoft CHAR data. Default is Yes.
TreatDBPartitionAsPassThrough	Optional. Uses pass-through partitioning for non-DB2 targets when the partition type is Database Partitioning. Default is No.
TreatNullInComparisonOperatorsAs	Optional. Determines how the Integration Service evaluates null values in comparison operations: - Null - Low - High Default is Null.

Option	Description

TrustStore	Optional. Enter the value for TrustStore using the following syntax:
	`<path>/<filename>`
	For example:
	`./Certs/trust.keystore`

UseOperatingSystemProfiles	Optional. Enables use of operating system profiles. Use this option if the Integration Service runs on UNIX.
ValidateDataCodePages	Optional. Enforces data code page compatibility. Default is Yes.
WriterWaitTimeOut	Optional. In target-based commit mode, the amount of time in seconds the writer remains idle before it issues a commit when the following conditions are true: - The PowerCenter Integration Service has written data to the target. - The PowerCenter Integration Service has not issued a commit. The PowerCenter Integration Service may commit to the target before or after the configured commit interval. Minimum value is 60. Maximum value is 2592000. Default is 60.
XMLWarnDupRows	Optional. Writes duplicate row warnings and duplicate rows for XML targets to the session log. Default is Yes.

Integration Service Process Options

Enter service process options in the following format:

```
infacmd CreateIntegrationService ... -po option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Integration Service process options:

Option	Description
$PMBadFileDir	Optional. Default directory for reject files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/BadFiles.
$PMCacheDir	Optional. Default directory for index and data cache files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Cache.
$PMExtProcDir	Optional. Default directory for external procedures. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/ExtProc.

Option	Description
$PMLookupFileDir	Optional. Default directory for lookup files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/LkpFiles.
$PMRootDir	Optional. Root directory accessible by the node. It cannot include the following special characters: * ? < > " | , Default is C:\Informatica\PowerCenter8.6\server\infa_shared.
$PMSessionLogDir	Optional. Default directory for session logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SessLogs.
$PMSourceFileDir	Optional. Default directory for source files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SrcFiles.
$PMStorageDir	Optional. Default directory for run-time files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Storage.
$PMTargetFileDir	Optional. Default directory for target files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/TgtFiles.
$PMTempDir	Optional. Default directory for temporary files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Temp.
$PMWorkflowLogDir	Optional. Default directory for workflow logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/WorkflowLogs.
Codepage_ID	Required. Code page ID number for the Integration Service process.
JVMClassPath	Optional. Java SDK classpath.
JVMMaxMemory	Optional. Maximum amount of memory the Java SDK uses during a PowerCenter session. Default is 64 MB.
JVMMinMemory	Optional. Minimum amount of memory the Java SDK uses during a PowerCenter session. Default is 32 MB.

CreateMMService

Creates a Metadata Manager Service in the domain. By default, the Metadata Manager Service is disabled when you create it. Run infacmd EnableService to enable the Metadata Manager Service.

The infacmd isp CreateMMService command uses the following syntax:

```
CreateMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-ServiceOptions|-so> option_name=value ...>
[<-LicenseName|-ln> license_name]
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd isp CreateMMService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Metadata Manager Service. The name is not case sensitive and must be unique within the domain. The name cannot have contain spaces, include carriage returns or tabs, exceed 79 characters, or contain the following characters: `/ * ? < > " |`
-NodeName -nn	node_name	Required. Name of the node where you want the Metadata Manager application to run.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the Metadata Manager Service runs.
-LicenseName -ln	license_name	Required. Name of the license you want to assign to the Metadata Manager Service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the Metadata Manager Service. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).

Metadata Manager Service Options

Enter Metadata Manager Service options in the following format:

```
infacmd isp CreateMMService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Metadata Manager Service options:

Option	Description
AgentPort	Required. Port number for the Metadata Manager Agent. The agent uses this port to communicate with metadata source repositories. Default is 10251.
CodePage	Required. Code page description for the Metadata Manager repository. To enter a code page description that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
ConnectString	Required. Native connect string for the Metadata Manager repository database.
DBUser	Required. User account for the Metadata Manager repository database.
DBPassword	Required. Password for the Metadata Manager repository database user. User password. You can set a password with the -so option or the environment variable INFA_DEFAULT_DATABASE_PASSWORD. If you set a password with both methods, the password set with the -so option takes precedence.
DatabaseHostname	Required. Host name for the Metadata Manager repository database.
DatabaseName	Required. Full service name or SID for Oracle databases. Service name for IBM DB2 databases. Database name for Microsoft SQL Server database.
DatabasePort	Required. Port number for the Metadata Manager repository database.
DatabaseType	Required. Type of database for the Metadata Manager repository.
ErrorSeverityLevel	Optional. Level of error messages written to the Metadata Manager Service log. Default is ERROR.
FileLocation	Required. Location of the files used by the Metadata Manager application.
JdbcOptions	Optional. Additional JDBC options. You can use this property to specify the following information: - Backup server location - Oracle Advanced Security Option (ASO) parameters - Microsoft SQL Server authentication parameters - Additional JDBC parameters when secure communication is enabled for the Metadata Manager repository database For more information about these parameters, see the *Informatica Application Service Guide*.
MaxConcurrentRequests	Optional. Maximum number of request processing threads available, which determines the maximum number of client requests that Metadata Manager can handle simultaneously. Default is 100.
MaxHeapSize	Optional. Amount of RAM in megabytes allocated to the Java Virtual Manager (JVM) that runs Metadata Manager. Default is 512.
MaxQueueLength	Optional. Maximum queue length for incoming connection requests when all possible request processing threads are in use by the Metadata Manager application. Default is 500.

Option	Description
MaximumActiveConnections	Optional. Number of active connections to the Metadata Manager repository database available. The Metadata Manager application maintains a connection pool for connections to the repository database. Default is 20.
MaximumWaitTime	Optional. Amount of time in seconds that Metadata Manager holds database connection requests in the connection pool. Default is 180.
MetadataTreeMaxFolderChilds	Optional. Number of child objects that appear in the Metadata Manager metadata catalog for any parent object. Default is 100.
ODBCConnectionMode	Connection mode the Integration Service uses to connect to metadata sources and the Metadata Manager repository when loading resources. Value can be true or false. You must set this property to True if the Integration Service runs on a UNIX machine and you want to load metadata from a Microsoft SQL Server database or if you use a Microsoft SQL Server database for the Metadata Manager repository.
OracleConnType	Required if you select Oracle for the DatabaseType. Oracle connection type. You can enter one of the following options: - OracleSID - OracleServiceName
PortNumber	Required. Port number the Metadata Manager application runs on. Default is 10250.
StagePoolSize	Optional. Maximum number of resources that Metadata Manager can load simultaneously. Default is 3.
TablespaceName	Tablespace name for the Metadata Manager repository on IBM DB2.
TimeoutInterval	Optional. Amount of time in minutes that Metadata Manager holds a failed resource load in the load queue. Default is 30.
URLScheme	Required. Indicates the security protocol that you configure for the Metadata Manager application: HTTP or HTTPS.
keystoreFile	Required if you use HTTPS. Keystore file that contains the keys and certificates required if you use the SSL security protocol with the Metadata Manager application.

CreateOSProfile

Creates an operating system profile in the domain. Before you run workflows that use operating system profiles, you must configure the PowerCenter Integration Service to use operating system profiles.

The infacmd isp CreateOSProfile command uses the following syntax:

```
CreateOSProfile

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
<-SystemName|-sn> system_username
[<-IntegrationServiceProcessOptions|-po> option_name=value ...
[<-EnvironmentVariables|-ev> name=value ...]
[<-DISProcessVariables|-diso> option_name=value ...]
[<-DISEnvironmentVariables|-dise> name=value ...]
[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]
[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]
[<-ProductExtensionName|-pe> product_extension_name]
[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

The following table describes infacmd isp CreateOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-OSProfileName -on	OSProfile_name	Required. Name of the operating system profile. The operating system profile name can be up to 80 characters. It cannot include spaces or the following special characters: `% * + \ / ? ; < >`
-SystemName -sn	system_username	Required. Name of an operating system user that exists on the machines where the Integration Service runs. The Integration Service runs workflows using the system access of the system user defined for the operating system profile.
-IntegrationServiceProcessOptions -po	option_name=value	Optional. Service process properties that define how the PowerCenter Integration Service runs.
-EnvironmentVariables -ev	name=value	Optional. Name and value of environment variables used by the PowerCenter Integration Service at run time.
-DISProcessVariables -diso	option_name=value	Optional. Service process properties that define how the Data Integration Service runs.
-DISEnvironmentVariables -dise	name=value	Optional. Name and value of environment variables used by the Data Integration Service at run time.

Option	Argument	Description
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Indicates whether the Data Integration Service uses the Hadoop impersonation user to run mappings, workflows, and profiling jobs in a Hadoop environment. Valid values are true or false.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Enter a user name for the Data Integration Service to impersonate when it runs jobs in a Hadoop environment.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Indicates whether to use the logged in user as the Hadoop impersonation user. Valid values are true or false.
-ProductExtensionName -pe	product_extension_name	Optional. Reserved for future use.
-ProductOptions -o	optionGroupName.optionName=Value	Required. Name and value of each option that you set. Use the option to create a flat file cache directory that the operating system profile can use. For example, the following command sets the cache directory to $PMRootDir/OSPCache: `infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'="$PMRootDir/OSPCache"`

Data Integration Service Process Options for Operating System Profiles

Enter the Data Integration Service process options in the following format:

```
infacmd CreateOSProfile ... -diso option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the Data Integration Service process options:

Option	Description
$DISRootDir	Root directory accessible by the node. This is the root directory for other service process variables. It cannot include the following special characters: * ? < > " | , [ ]
$DISTempDir	Directory for temporary files created when jobs are run. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/disTemp. **Note:** If the Data Integration Service is configured to use multiple operating system profiles, specify a common directory for all the profiles because a separate directory for each profile results in excessive usage of disk space.

Option	Description
$DISCacheDir	Directory for index and data cache files for transformations. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/cache.
$DISSourceDir	Directory for source flat files used in a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/source.
$DISTargetDir	Directory for target flat files used in a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/target.
$DISRejectedFilesDir	Directory for reject files. Reject files contain rows that were rejected when running a mapping. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/reject.
$DISLogDir	Directory for logs. It cannot include the following special characters: * ? < > " | , [ ] Default is <root directory>/disLogs.

PowerCenter Integration Service Process Options for Operating System Profiles

Enter the PowerCenter Integration Service process options in the following format:

```
infacmd CreateOSProfile ... -po option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the PowerCenter Integration Service process options:

Option	Description
$PMBadFileDir	Optional. Directory for reject files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/BadFiles.
$PMCacheDir	Optional. Directory for index and data cache files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Cache.
$PMExtProcDir	Optional. Directory for external procedures. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/ExtProc.

Option	Description
$PMLookupFileDir	Optional. Directory for lookup files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/LkpFiles.
$PMRootDir	Optional. Root directory accessible by the node. It cannot include the following special characters: * ? < > " | , Default is C:\Informatica\PowerCenter\server\infa_shared.
$PMSessionLogDir	Optional. Directory for session logs. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SessLogs.
$PMSourceFileDir	Optional. Directory for source files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/SrcFiles.
$PMStorageDir	Optional. Directory for run-time files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Storage.
$PMTargetFileDir	Optional. Directory for target files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/TgtFiles.
$PMTempDir	Optional. Directory for temporary files. It cannot include the following special characters: * ? < > " | , Default is $PMRootDir/Temp.

CreateRepositoryService

Creates a PowerCenter Repository Service in a domain.

By default, the PowerCenter Repository Service is enabled when you create it.

A PowerCenter Repository Service manages one repository. It performs all metadata transactions between the repository and repository clients.

The infacmd isp CreateRepositoryService command uses the following syntax:

```
CreateRepositoryService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
[<-BackupNodes|-bn> node1 node2 ...]
[<-ServiceDisable|-sd>]
<-ServiceOptions|-so> option_name=value ...
[<-LicenseName|-ln> license_name]
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd isp CreateRepositoryService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the PowerCenter Repository Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot have leading or trailing spaces, include carriage returns or tabs, exceed 79 characters, or contain the following characters: `\ / : * ? < > " |`
-NodeName -nn	node_name	Required. Name of the node where you want the PowerCenter Repository Service process to run. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node.
-BackupNodes -bn	node1 node2 ...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceDisable -sd	-	Optional. Creates a disabled service. You must enable the service before you can run it.
-ServiceOptions -so	option_name=value	Required. Service properties that define how the PowerCenter Repository Service runs.
-LicenseName -ln	license_name	Required if you create an enabled service. Name of the license you want to assign to the PowerCenter Repository Service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the PowerCenter Repository Service. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).

Repository Service Options (-so)

Enter Repository Service options in the following format:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Repository Service options:

Option	Description
AllowWritesWithRACaching	Optional. Uses PowerCenter Client tools to modify metadata in the repository when repagent caching is enabled. Default is Yes.
CheckinCommentsRequired	Optional. Requires users to add comments when checking in repository objects. Default is Yes. To apply changes, restart the PowerCenter Repository Service.
CodePage	Required. Code page description for the database. To enter a code page description that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
ConnectString	Required. Database connection string specified during PowerCenter Repository Service setup. To apply changes, restart the PowerCenter Repository Service.
DBPassword	Required. Repository database password corresponding to the database user. You can set a password with the -so option or the environment variable INFA_DEFAULT_DATABASE_PASSWORD. If you set a password with both methods, the password set with the -so option takes precedence. To apply changes, restart the PowerCenter Repository Service.
DBPoolExpiryThreshold	Optional. The minimum number of idle database connections allowed by the PowerCenter Repository Service. For example, if there are 20 idle connections, and you set this threshold to 5, the PowerCenter Repository Service closes no more than 15 connections. Minimum is 3. Default is 5.
DBPoolExpiryTimeout	Optional. The interval, in seconds, at which the PowerCenter Repository Service checks for idle database connections. If a connection is idle for a period of time greater than this value, the PowerCenter Repository Service can close the connection. Minimum is 300. Maximum is 2,592,000 (30 days). Default is 3,600 (1 hour).
DBUser	Required. Account for the database containing the repository. To apply changes, restart the PowerCenter Repository Service.
DatabaseArrayOperationSize	Optional. Number of rows to fetch each time an array database operation is issued, such as insert or fetch. Default is 100. To apply changes, restart the PowerCenter Repository Service.
DatabaseConnectionTimeout	Optional. Amount of time in seconds that the PowerCenter Repository Service attempts to establish a connection to the database management system. Default is 180.
DatabasePoolSize	Optional. Maximum number of connections to the repository database that the PowerCenter Repository Service can establish. Minimum is 20. Default is 500.
DatabaseType	Required. Type of database that stores the repository metadata. To apply changes, restart the PowerCenter Repository Service.
EnableRepAgentCaching	Optional. Enables the repository agent caching feature. Default is Yes.

Option	Description
ErrorSeverityLevel	Optional. Minimum level of error messages written to the PowerCenter Repository Service log: - Fatal - Error Warning - Info - Trace - Debug Default is Info.
HeartBeatInterval	Optional. Interval at which the PowerCenter Repository Service verifies its connections with clients of the service. Default is 60 seconds.
MaxResilienceTimeout	Optional. Maximum amount of time in seconds that the service holds on to resources for resilience purposes. Default is 180.
MaximumConnections	Optional. Maximum number of connections the repository accepts from repository clients. Default is 200.
MaximumLocks	Optional. Maximum number of locks the repository places on metadata objects. Default is 50,000.
OperatingMode	Optional. Mode in which the PowerCenter Repository Service is running: - Normal - Exclusive Default is Normal. To apply changes, restart the PowerCenter Repository Service.
OptimizeDatabaseSchema	Optional. Optimizes the repository database schema when you create repository contents or back up and restore an IBM DB2 or Microsoft SQL Server repository. When enabled, the PowerCenter Repository Service tries to create repository tables that contain Varchar columns with a precision of 2000 instead of CLOB columns. Use Varchar columns to increase repository performance. When you use Varchar columns, you reduce disk input and output, and the database can cache the columns. To use this option, verify the page size requirements for the following repository databases: - IBM DB2. Database page size 4 KB or greater. At least one temporary tablespace with page size 16 KB or greater. - Microsoft SQL Server. Database page size 8 KB or greater. Default is disabled.
PreserveMXData	Optional. Preserves MX data for prior versions of mappings. Default is disabled.
RACacheCapacity	Optional. Number of objects that the cache can contain when repository agent caching is enabled. Default is 10,000.
SecurityAuditTrail	Optional. Tracks changes made to users, groups, privileges, and permissions. Default is No.
ServiceResilienceTimeout	Optional. Amount of time in seconds that the service tries to establish or reestablish a connection to another service. Default is 180. To apply changes, restart the PowerCenter Repository Service.

Option	Description
TableOwnerName	Optional. Name of the owner of the repository tables for an IBM DB2 repository.
TablespaceName	Optional. Tablespace name for IBM DB2 repositories. To apply changes, restart the PowerCenter Repository Service.
TrustedConnection	Optional. Uses Windows authentication to access the Microsoft SQL Server database. Default is No. To apply changes, restart the PowerCenter Repository Service.

CreateRole

Creates a custom role in the domain. You can then assign privileges to the role for the domain or for an application service type. You cannot create system-defined roles.

The infacmd isp CreateRole command uses the following syntax:

```
CreateRole
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
[<-SecurityDomain|-sdn> securitydomain]
<-Password|-pd> password
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
[<-RoleDescription|-rd> role_description]
```

The following table describes infacmd isp CreateRole options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RoleName -rn	role_name	Required. Name of the role. The role name is case insensitive and can be between 1 and 80 characters long. It cannot include a tab, newline character, or the following special characters: `, + " \ < > ; / * % ?` The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
-RoleDescription -rd	role_description	Optional. Description of the role. The description can have a maximum of 1,000 characters and cannot include a tab, newline character, or the following special characters: `< > "` To enter a description that contains spaces or other non-alphanumeric characters, enclose it in quotation marks.

CreateSAPBWService

Creates an SAP BW Service in the domain. By default, the SAP BW Service is enabled when you create it.

The infacmd isp CreateSAPBWService command uses the following syntax:

```
CreateSAPBWService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-IntegrationService|-is> integration_service_name
<-RepositoryUser|-ru> user
<-RepositoryPassword|-rp> password
[<-ServiceOptions|-so> option_name=value ...]
[<-ServiceProcessOptions|-po> option_name=value ...]
[<-ServiceDisable|-sd>]
[<-LicenseName|-ln> license_name]
[<-FolderPath|-fp> full_folder_path]
```

The following table describes infacmd isp CreateSAPBWService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the SAP BW Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot have leading or trailing spaces, include carriage returns or tabs, exceed 79 characters, or contain the following characters: / * ? < > " |
-NodeName -nn	node_name	Required. Name of the node where you want the SAP BW Service process to run. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node.
-IntegrationService -is	integration_service_name	Required. Name of the Integration Service to which the SAP BW Service connects. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-RepositoryUser -ru	user	Required. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryPassword -rp	password	Required if secure communication is not enabled for the domain. Optional if secure communication is enabled for the domain. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the SAP BW Service runs.
-ServiceProcessOptions -po	option_name=value	Optional. Service process properties for the SAP BW Service.
-ServiceDisable -sd	-	Optional. Creates a disabled service. You must enable the service before you can run it.
-LicenseName -ln	license_name	Required if you create an enabled service. Name of the license you want to assign to the SAP BW Service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the SAP BW Service. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).

SAP BW Service Options

Enter SAP BW Service options in the following format:

```
infacmd CreateSAPBWService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes SAP BW Service options:

Option	Description
BWSystemConxString	Optional. DEST entry defined in the `sapnwrfc.ini` file for a connection to an RFC server program. Edit this property if you have created a different DEST entry in the `sapnwrfc.ini` file for the SAP BW Service.
RetryPeriod	Optional. Number of seconds the SAP BW Service waits before trying to connect to the BW system if a previous connection attempt failed. Default is 5.

SAP BW Service Process Option

Enter the service process option in the following format:

```
infacmd CreateSAPBWService ... -po option_name=value
```

To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes the SAP BW Service process option:

Option	Description
ParamFileDir	Optional. Temporary parameter file directory. Default is /Infa_Home/server/infa_shared/BWParam.

CreateUser

Creates a user account in the native security domain. You can then assign roles, permissions, and privileges to a user account. The roles, permissions, and privileges assigned to the user determine the tasks that the user can perform within the domain.

The infacmd isp CreateUser command uses the following syntax:

```
CreateUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NewUserName|-nu> new_user_name

<-NewUserPassword|-np> new_user_password

[<-NewUserFullName|-nf> new_user_full_name]

[<-NewUserDescription|-ds> new_user_description]

[<-NewUserEMailAddress|-em> new_user_email_address]

[<-NewUserPhoneNumber|-pn> new_user_phone_number]
```

The following table describes infacmd isp CreateUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-NewUserName -nu	new_user_name	Required. Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The login name is not case sensitive and can be between 1 and 80 characters long. It cannot include a tab, newline character, or the following special characters: `, + " \ < > ; / * & % ?` The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
-NewUserPassword -np	new_user_password	Required. Password for the user account. You can set a password with the -np option or the environment variable INFA_PASSWORD. If you set a password with both these methods, the password set with the -np option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.
-NewUserFullName -nf	new_user_full_name	Optional. Full name for the user account. To enter a name that contains spaces or other non-alphanumeric characters, enclose the name in quotation marks. The full name cannot include the following special characters: `< > “`
-NewUserDescription -ds	new_user_description	Optional. Description of the user account. To enter a description that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The description cannot include the following special characters: `< > “`

Option	Argument	Description
-NewUserEMailAddress -em	new_user_email_address	Optional. Email address for the user. To enter an address that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The email address cannot include the following special characters: < > " Enter the email address in the format `UserName@Domain`.
-NewUserPhoneNumber -pn	new_user_phone_number	Optional. Telephone number for the user. To enter a telephone number that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The telephone number cannot include the following special characters: < > "

CreateWSHubService

Creates a Web Services Hub in the domain. By default, the Web Services Hub is enabled when you create it.

The infacmd isp CreateWSHubService command uses the following syntax:

```
CreateWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-FolderPath|-fp> full_folder_path]
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
<-RepositoryUser|-ru> repository_user
<-RepositoryPassword|-rp> repository_password
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceDisable|-sd>]
[<-ServiceOptions|-so> option_name=value ...
<-LicenseName|-ln> license_name
```

The following table describes infacmd isp CreateWSHubService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the domain.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Name of the Web Services Hub you want to create. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot have leading or trailing spaces, include carriage returns or tabs, exceed 79 characters, or contain the following characters: `/ * ? < > " |`

Option	Argument	Description
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the Web Services Hub. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).
-NodeName -nn	node_name	Required. Name of the node where you want to run the Web Services Hub process.
-RepositoryService -rs	repository_service_name	Required. Name of the Repository Service that the Web Services Hub depends on. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryUser -ru	repository_user	Required. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryPassword -rp	repository_password	Required. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password that you set with the -rp option takes precedence.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required if the domain uses LDAP authentication or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ServiceDisable -sd	-	Optional. Creates a disabled service. You must enable the service before you can run it.
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the Web Services Hub runs.
-LicenseName -ln	license_name	Required. Name of the license you want to assign to the Web Services Hub.

Web Services Hub Options

Enter Web Services Hub options in the following format:

```
infacmd CreateWSHubService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Web Services Hub options:

Option	Description
DTMTimeout	Optional. Amount of time in seconds that *infacmd* attempts to establish or reestablish a connection to the DTM. Default is 60.
ErrorSeverityLevel	Optional. Minimum level of error logging for the Web Services Hub logs: - Fatal - Error - Warning - Info - Trace - Debug Default is Info.
HubHostName	Optional. Name of the machine hosting the Web Services Hub. Default is localhost. To apply changes, restart the Web Services Hub.
HubPortNumber(http)	Optional. Port number on which the Web Services Hub runs in Tomcat. Default is 7333. To apply changes, restart the Web Services Hub.
HubPortNumber (https)	Port number on which the Web Services Hub runs in Tomcat. Required if you choose to run the Web Services Hub on HTTPS. Default is 7343.
InternalHostName	Optional. Host name at which the Web Services Hub listens for connections from the Integration Service. Default is localhost. To apply changes, restart the Web Services Hub.
InternalPortNumber	Optional. Port number at which the Web Services Hub listens for connections from the Integration Service. Default is 15555. To apply changes, restart the Web Services Hub.
MaxConcurrentRequests	Optional. Maximum number of request processing threads available, which determines the maximum number of simultaneous requests that can be handled. Default is 100.
MaxLMConnections	Optional. Maximum number of connections to the Integration Service that can be open at one time for the Web Services Hub. Default is 20.
MaxQueueLength	Optional. Maximum queue length for incoming connection requests when all possible request processing threads are in use. Default is 5000.
SessionExpiryPeriod	Optional. Number of seconds that a session can remain unused before its session ID becomes invalid. Default is 3600 seconds.
URLScheme	Optional. Security protocol that you configure for the Web Services Hub: HTTP or HTTPS. Default is HTTP. To apply changes, restart the Web Services Hub.
WSH_ENCODING	Optional. Character encoding for the Web Services Hub. Default is UTF-8. To apply changes, restart the Web Services Hub.
KeystoreFile	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol with the Web Services Hub.

DeleteNamespace

Deletes an LDAP security domain and the users and groups in the security domain. Deletes the LDAP security domain if the Informatica domain uses LDAP or Kerberos authentication.

The infacmd isp DeleteNamespace command uses the following syntax:

```
DeleteNamespace
 <-DomainName|-dn> domain_name
 <-UserName|-un> user_name
 <-Password|-pd> password
 [<-SecurityDomain|-sdn> security_domain]
 [<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
 [<-ResilienceTimeout|-re> timeout_period_in_seconds]
 <-NameSpace|-ns> namespace
```

The following table describes infacmd isp DeleteNamespace options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Name of the security domain that you want to create to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd tries to establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If you do not specify the environment variable, the default value used is 180 seconds.
-NameSpace -ns	namespace	Required. Name of the LDAP or Kerberos security domain. The name is not case sensitive and must be unique within the domain. The name cannot contain spaces or any of the following special characters: , + / < > @ ; \ % ? The name cannot exceed 128 characters. The name can contain an ASCII space character except for the first and last character. You cannot use any other space characters.

DisableNodeResource

Disables an Informatica resource. Informatica resources include file directory resources, custom resources, and connection resources. Disable the resources that are not available to prevent the Load Balancer from dispatching a task to a node that does not have the required resources.

You can disable file directory resources, custom resources, and connection resources.

When a PowerCenter Integration Service runs on a grid, the Load Balancer can use resources to distribute Session, Command, and predefined Event-Wait tasks. If the PowerCenter Integration Service is configured to check resources, the Load Balancer distributes tasks to nodes with available resources.

By default, all connection resources are enabled on a node.

The infacmd isp DisableNodeResource command uses the following syntax:

```
DisableNodeResource
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")
<-ResourceName|-rn> resource_name
```

The following table describes infacmd isp DisableNodeResource options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node where the resource is defined.
-ResourceCategory -rc	resource_category	Optional. Category of the resource. Valid categories include: - PCIS. Resource for the PowerCenter Integration Service. - DIS. Reserved for future use. Default is PCIS.
-ResourceType -rt	resource_type	Required. Type of resource. Valid types include: - Custom - File Directory - Connection
-ResourceName -rn	resource_name	Required. Entire name of the resource. To list the names of all resources available to a node, run the infacmd isp ListNodeResources command.

DisableService

Disables the application service corresponding to the service name. When you disable a service, all service processes stop.

Disables any application service type, including system services.

The infacmd isp DisableService command uses the following syntax:

```
DisableService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Mode|-mo> disable_mode
```

The following table describes infacmd isp DisableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service you want to disable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-Mode -mo	disable_mode	Required. Defines how the service is disabled: - Complete. Disables the service after all service processes stop. - Stop. If the service is a PowerCenter Integration Service, stops all running workflows, and then disables the PowerCenter Integration Service. If the service is an Analyst Service, stops all the jobs, and then disables the service. - Abort. Stops all processes immediately, and then disables the service.

Note: If you specify a disable mode of Stop for a Listener Service, the command waits up to 30 seconds for Listener subtasks to complete and then shuts down the service and the Listener Service process.

DisableServiceProcess

Disables the service process on a specified node.

You can disable a service process on a specified node if the node requires maintenance.

The infacmd isp DisableServiceProcess command uses the following syntax:

```
DisableServiceProcess
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-Mode|-mo> disable_mode
```

The following table describes infacmd isp DisableServiceProcess options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service associated with the process you want to disable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where the service process is running.
-Mode -mo	disable_mode	Required. Defines how the service process is disabled: - Complete. Allows the service process to complete the current tasks before disabling. - Stop. If the process is an Integration Service process, stops all running workflows, and then disables the Integration Service process. - Abort. Disables the service process before the current task completes.

DisableUser

Disables a user account in the domain. If you do not want a user to access the domain temporarily, you can disable the user account.

When you disable a user account, the user cannot log in to the PowerCenter applications.

The infacmd isp DisableUser command uses the following syntax:

```
DisableUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

The following table describes infacmd isp DisableUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
ExistingUserName -eu	existing_user_name	Required. User account you want to disable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user you want to disable belongs to. Default is Native.

EditUser

Edits the general properties for a user account in the native security domain.

You cannot modify the properties of user accounts in the LDAP security domains.

You cannot change the login name of a native user.

The infacmd isp EditUser command uses the following syntax:

```
EditUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserFullName|-ef> Existing_user_full_name]
[<-ExistingUserDescription|-ds> Existing_user_description]
[<-ExistingUserEMailAddress|-em> Existing_user_email_address]
[<-ExistingUserPhoneNumber|-pn> Existing_user_phone_number]
```

The following table describes infacmd isp EditUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_name	Required. User account you want to edit.
-ExistingUserFullName -sf	existing_user_full_name	Optional. Changed full name for the user account. To enter a name that contains spaces or other non-alphanumeric characters, enclose the name in quotation marks. The full name cannot include the following special characters: < > "
-ExistingUserDescription -ds	existing_user_description	Optional. Changed description for the user account. To enter a description that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The description cannot include the following special characters: < > "
-ExistingUserEMailAddress -em	existing_user_email_address	Optional. Changed email address for the user. To enter an address that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The email address cannot include the following special characters: < > "
-ExistingUserPhoneNumber -pn	existing_user_phone_number	Optional. Changed telephone number for the user. To enter a telephone number that contains spaces or other non-alphanumeric characters, enclose it in quotation marks. The phone number cannot include the following special characters: < > "

EnableNodeResource

Enables an Informatica resource. Informatica resources include file or directory, custom, and connection resources. When you enable a resource on a node, you allow the Load Balancer to distribute tasks that require the resource to that node.

When a PowerCenter Integration Service runs on a grid, the Load Balancer can use resources to distribute Session, Command, and predefined Event-Wait tasks. If the PowerCenter Integration Service is configured to check resources, the Load Balancer distributes tasks to nodes where the resources are added and enabled.

The infacmd isp EnableNodeResource command uses the following syntax:

```
EnableNodeResource
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
<-ResourceType|-rt> resource_type ("Custom", "File Directory", "Connection")
<-ResourceName|-rn> resource_name
```

The following table describes infacmd isp EnableNodeResource options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node where the resource is defined.
-ResourceCategory -rc	resource_category	Optional. Category of the resource. Valid categories include: - PCIS. Resource for the PowerCenter Integration Service. - DIS. Reserved for future use. Default is PCIS.
-ResourceType -rt	resource_type	Required. Type of resource. Valid types include: - Custom - File Directory - Connection
-ResourceName -rn	resource_name	Required. Entire name of the resource. To list the names of all resources available to a node, run the ListNodeResources command.

EnableService

Enables the application service corresponding to the service name.

Enables any application service type, including system services. You can also enable the Informatica Administrator.

The infacmd isp EnableService command uses the following syntax:

```
EnableService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

The following table describes infacmd isp EnableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service you want to enable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks. To start the Administrator tool, enter `_adminconsole`.

EnableServiceProcess

Enables a service process on a specified node.

The infacmd isp EnableServiceProcess command uses the following syntax:

```
EnableServiceProcess
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
```

The following table describes infacmd isp EnableServiceProcess options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service associated with the process you want to enable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where you want to enable a service process.

EnableUser

Enables a user account in the domain.

The infacmd isp EnableUser command uses the following syntax:

```
EnableUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

The following table describes infacmd isp EnableUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
ExistingUserName -eu	existing_user_name	Required. User account you want to enable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user you want to enable belongs to. Default is Native.

ExportDomainObjects

Exports native users, native groups, roles, connections, and cluster configurations from the Informatica domain to an XML file.

If you do not want to export all objects in the domain, use an infacmd export control file to filter the objects that you want to export.

Use the ExportDomainObjects and ImportDomainObjects commands to migrate objects between two different domains of the same version. To export native users and groups from domains of different versions, use the infacmd isp ExportUsersAndGroups command.

When you export a group, you export all subgroups and users in the group.

You cannot export the Administrator user, the Administrator group, users in the Administrator group, the Everyone group, or the LDAP users or groups. To replicate LDAP users and groups in an Informatica domain, import the LDAP users and groups directly from the LDAP directory service.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd isp ExportDomainObjects command uses the following syntax:

```
ExportDomainObjects

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ExportFile|-fp> export_file_name
[<-ExportControlFile|-cp> export_control_file_name]
[<-RetainPassword|-rp> retain_password]
[<-Force|-f>]
```

The following table describes infacmd isp ExportDomainObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExportFile -fp	export_file_name	Required. Path and file name of the export file. If you do not specify the file path, infacmd creates the file in the directory where you run infacmd.
-ExportControlFile -cp	export_control_file	Optional.Name and path for the export control file that filters the objects that are exported.
-RetainPassword -rp	retain_password	Optional. Set to true to retain encrypted passwords for users and connections in the exported file. When set to false, user and connection passwords are exported as empty strings. Default is false.
-Force -f	-	Optional. Overwrites the export file if a file with the same name already exists. If you omit this option, the command prompts you for a confirmation before it overwrites the file.

ExportUsersAndGroups

Exports native users and groups to an XML file.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd isp ExportUsersAndGroups command uses the following syntax:

```
ExportUsersAndGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExportFile|-ef> export_file_name
[<-Force|-f>]
```

The following table describes infacmd isp ExportUsersAndGroups options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~ When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExportFile -ef	export_file_name	Required. Name and file path where you want to write the export file. If you do not specify the file path, infacmd creates the backup file in the directory where you run infacmd.
-Force -f	-	Optional. Overwrites the export file, if a file with the same name already exists. If you omit this option, the command prompts you for a confirmation before it deletes the file.

Related Topics:

- "ImportUsersAndGroups" on page 534

GetFolderInfo

Gets folder information. Folder information includes folder path, name, and description.

To run the infacmd isp GetFolderInfo command, you must have permission on the folder.

The infacmd isp GetFolderInfo command uses the following syntax:

```
GetFolderInfo

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderPath|-fp> full_folder_path
```

The following table describes infacmd isp GetFolderInfo options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, to the folder. Must be in the format: */parent_folder/child_folder*

GetLastError

Gets the most recent error messages for an application service running on a node.

The error messages are log events that have a severity level of *error* or *fatal*. This command does not return errors that occurred before Informatica Services were last started.

You can fetch error messages in a file or display them on the screen.

The infacmd isp GetLastError command uses the following syntax:

```
GetLastError
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
[<-Format|-fm> format_TEXT_XML]
[<-MaxEvents|-me> maximum_number_of_error_events]
```

The following table describes infacmd isp GetLastError options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Optional. Name of the service for which you want to fetch error messages. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where the service runs.

Option	Argument	Description
-Format -fm	format	Optional. Format for error messages. Valid types include: - Text - XML If you do not specify a format, infacmd displays the messages in text format with lines wrapped at 80 characters.
-MaxEvents -me	maximum_number_of_error_events	Optional. Maximum number of error messages to fetch. Default is 1. Maximum value is 20.

GetLog

Gets log events. You can get log events for a domain or services. You can write log events to a file or display them on the screen.

To fetch log events for a domain, you must have permission on the domain. To fetch log events for a service, you must have permission on the service.

The infacmd isp GetLog command uses the following syntax:

```
GetLog

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-StartDate|-sd> start_date_time]

[<-EndDate|-ed> end_date_time]

[<-ReverseOrder|-ro>]

[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|ES|IS|MM|MRS|RMS|RS|SCH|SEARCH|TDM|TDW|WS|
DOMAIN]

[<-ServiceName|-sn> service_name]

[<-Severity|-svt> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
```

The following table describes infacmd isp GetLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-StartDate -sd	start_date_time	Optional. Returns log events starting from this date and time. Enter date and time in one of the following formats: - MM/dd/yyyy_hh:mm:ssa_Z - MM/dd/yyyy_hh:mma_Z - MM/dd/yyyy_hh:mm:ssa - MM/dd/yyyy_hh:mma - yyyy-MM-dd_HH:mm:ss_Z - yyyy-MM-dd_HH:mm_Z - yyyy-MM-dd_HH:mm:ss - yyyy-MM-dd_HH:mm - MM/dd/yyyy hh:mm:ssa Z - MM/dd/yyyy hh:mma Z - MM/dd/yyyy hh:mm:ssa - MM/dd/yyyy hh:mma - yyyy-MM-dd HH:mm:ss_Z - yyyy-MM-dd HH:mm_Z - yyyy-MM-dd HH:mm:ss - yyyy-MM-dd HH:mm - MM/dd/yyyy - yyyy-MM-dd Where “a” is an am/pm marker (“a” for a.m. and “p” for p.m.) and “Z” is a time zone marker (for example,“-0800” or “GMT”).
-EndDate -ed	end_date_time	Optional. Returns log events ending by this date and time. Enter date and time in the same format as the StartDate option. If you enter an end date that is before the start date, GetLog returns no log events.
-ReverseOrder -ro	-	Optional. Fetches log events according to most recent timestamp.
-Format -fm	format	Optional. Format for log events. Valid types include: - Text - XML - Bin (binary) If you choose binary, then you must specify a file name using the OutputFile option. If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -lo	output_file_name	Name and file path where you want to write the log file. By default, the Service Manager uses the server\infa_shared\log directory on the master gateway node. Omit this option to display the log events on the screen. If you choose binary as the output file type, you must specify a file name using this option.

Option	Argument	Description
-ServiceType -st	service_type	Optional. Type of service for which you want to fetch log events. You can specify one service type. Omit this option to fetch log events for all service types. Service types include: - AS. Analyst Service - BW. SAP BW Service - CMS. Content Management Service - DIS. Data Integration Service - ES. Email Service - IS. PowerCenter Integration Service - MM. Metadata Manager Service - MRS. Model Repository Service - RMS. Resource Manager Service - RS. PowerCenter Repository Service - SCH. Scheduler Service - SEARCH. Search Service - TDM. Test Data Manager Service - TDW. Test Data Warehouse Service - WS. Web Services Hub - DOMAIN. Domain
-ServiceName -sn	service_name	Optional. Name of the service for which you want to fetch log events. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-Severity -svt	severity_level	Optional. Message severity. Severity types include: - Fatal - Error - Warning - Info - Trace - Debug

GetNodeName

Returns the name of a node.

Gets the node name from the nodemeta.xml file on the node. You must enter this command on the node for which you want to fetch the name.

The infacmd isp GetNodeName command uses the following syntax:

```
GetNodeName
[<-OutputFile|-o>] output_file
```

When you use the command without the -o option, the command prints the node name to the command window. When you use the -o option to specify an output file, you provide the file name and path. For example:

```
isp\bin\infacmd.bat getNodeName -o c:\node_name.txt
```

The command creates a file, node_name.txt, in the path that you specify. It prints the node name in the file. If the file exists, the command overwrites the file.

GetPasswordConfig

Returns the password configuration for the domain users.

The infacmd GetPasswordConfig command uses the following syntax:

```
GetPasswordConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd GetPasswordConfig options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. Specify the host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.

getDomainSamlConfig

Returns the Secure Assertion Markup Language (SAML) authentication status for an Informatica domain. If SAML authentication is enabled, the command also returns the identity provider URL and the allowed time difference between the identity provider host system clock and the system clock on the master gateway node.

Run the command on any gateway node within the Informatica domain. You must have the administrator role to run this command.

The infacmd isp getDomainSamlConfig command uses the following syntax:

```
getDomainSamlConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
[<-SecurityDomain|-sdn> security_domain]
<-Password|-pd> password
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp getDomainSamlConfig options and arguments:

Option	Argument	Description
–DomainName –dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
–ResilienceTimeout –re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

GetServiceOption

Gets the value of a service property for a PowerCenter Integration Service, PowerCenter Repository Service, SAP BW Service, or Web Services Hub. For Data Integration Service or Analyst Service options, run infacmd dis or infacmd as ListServiceOptions.

For example, you can retrieve the repository database type.

The infacmd isp GetServiceOption command uses the following syntax:

```
GetServiceOption

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-OptionName|-op> option_name
```

The following table describes infacmd isp GetServiceOption options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Name of the service for which you want to fetch a value. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-OptionName -op	option_name	Required. Name of the option for which you want to retrieve a value. The options you specify depend on the service type: - For more information about Integration Service options, see "Integration Service Options" on page 452. - For an SAP BW Service, specify "BWSystemConXString" (the SAP Destination R type) or "RetryPeriod" (the retry period in seconds). - For more information about Web Services Hub options, see "Web Services Hub Options" on page 481.

GetServiceProcessOption

Gets the value for a property on a PowerCenter Integration Service process running on a node.

The infacmd isp GetServiceProcessOption command uses the following syntax:

```
GetServiceProcessOption
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-OptionName|-op> option_name
```

The following table describes infacmd isp GetServiceProcessOption options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service for which you want to fetch a value. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where the service process is running.
-OptionName -op	option_name	Required. Name of the option for which you want to retrieve a value.

Related Topics:

- "Integration Service Process Options" on page 456

GetServiceProcessStatus

Gets the status of an application service process on a node. A service process can be enabled or disabled.

The infacmd isp GetServiceProcessStatus command uses the following syntax:

```
GetServiceProcessStatus
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
```

The following table describes infacmd isp GetServiceProcessStatus options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service running the process for which you want the status. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where the service process is running.

GetServiceStatus

Gets the status of an application service.

You can fetch the status of a service such as the Repository Service, Data Integration Service, Analyst Service, Integration Service, Web Services Hub, or SAP BW Service. A service can be enabled or disabled.

The infacmd isp GetServiceStatus command uses the following syntax:

```
GetServiceStatus
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp GetServiceStatus options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service for which you want the status. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

GetSessionLog

Gets log events for the most recent run of a session. The PowerCenter Repository Service must be running when you run this command.

The infacmd isp GetSessionLog command uses the following syntax:

```
GetSessionLog

<-DomainName|-dn> domain_name

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Format|-fm> format_TEXT_XML_BIN]

[<-OutputFile|-lo> output_file_name]

<-IntegrationService|-is> integration_service_name

<-RepositoryService|-rs> repository_service_name

[<-RepositoryDomain|-rd> domain_of_repository]

<-RepositoryUser|-ru> repository_user]

<-RepositoryPassword|-rp> repository_password]

[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]

<-FolderName|-fn> repository_folder_name

<-Workflow|-wf> workflow_name

[<-RunInstance|-in> run_instance_name] | <-RunId|-id> workflow_run_id]

<-Session|-ss> session_name
```

Note: If you do not specify -un, -pd, and -sdn options, the infacmd isp GetSessionLog command uses the corresponding values from the -ru, -rp, and the -rsdn options.

The following table describes infacmd isp GetSessionLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-Format -fm	format	Optional. Format for the session log. Valid types include: - Text - XML - Bin (binary) If you choose binary, then you must specify a file name using the OutputFile option. If you do not specify a format, *infacmd* uses text format with lines wrapped at 80 characters.

Option	Argument	Description
-OutputFile -lo	output_file_name	Name and file path for the session log file. By default, the Service Manager uses the server\infa_shared\log directory on the master gateway node. Omit this option to display the log events on the screen. If you choose binary as the output file type, you must specify a file name using this option.
-IntegrationService -is	integration_service_name	Required. Name of the Integration Service that runs the session. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryService -rs	repository_service_name	Required. Name of the Repository Service that contains the session. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryDomain -rd	domain_of_repository	Required if the repository is in a domain other than the local domain. Domain of the Repository Service. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryUser -ru	repository_user	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryPassword -rp	repository_password	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required for LDAP or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If you do not specify this option, the command sets the repository user security domain to native.
-FolderName -fn	repository_folder_name	Required. Name of the folder containing the session. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-Workflow -wf	workflow_name	Required. Name of the workflow containing the session. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RunInstance -in	run_instance_name	Name of the workflow run instance that contains the session. Use this option if you are running concurrent workflows. Use the -in or the -id option, not both.

Option	Argument	Description
-RunId -id	workflow_run_id	Run identifier number (Run ID) of the workflow run instance that contains the session. Use this option if you are running concurrent workflows. Use the -in or the -id option, not both. **Note:** Use this option if the workflow does not have a unique run instance name.
-Session -ss	session_name	Required. Session name. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

GetSystemLogDirectory

Returns the path of the system log directory.

You must enter this command on the domain for which you want to fetch the system log directory path.

The infacmd isp GetSystemLogDirectory command uses the following syntax:

```
GetSystemLogDirectory
[<-OutputFile|-o> output_file]
```

When you use the command without the -o option, the command prints the directory path to the command window. When you use the -o option to specify an output file, you provide the file name and path for the output file. For example:

```
isp\bin\infacmd.bat getSystemLogDirectory -o c:\sys_log_dir.txt
```

The command creates a file, sys_log_dir.txt, in the path that you specify, and prints the path of the system log directory in the file. If the file exists, the command overwrites the file.

getUserActivityLog

Gets user activity logs for a single user or multiple users. You can write user activity logs to a file or display them in the console.

The user activity log data includes successful and unsuccessful user login attempts from Informatica clients. If the client includes custom properties set by the clients on login requests, the data includes the properties.

Note: User login attempts are not captured in the user activity logs in a domain configured to use Kerberos authentication.

The infacmd isp getUserActivityLog command uses the following syntax:

```
getUserActivityLog
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Users|-usrs> user1:[securitydomain] user2:[securitydomain]...
[<-StartDate|-sd> start_date]
[<-EndDate|-ed> end_date]
```

```
[<-ActivityCode|-ac> activity_code]
[<-ActivityText|-atxt> activity_text]
[<-ReverseOrder|-ro> true]
[<-OutputFile|-lo> output_file_name]
[<-Format|-fm> output_format_BIN_TEXT_XML]
```

The following table describes infacmd isp getUserActivityLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description

-Users
-usrs
	user1:[securitydomain]
	user2:[securitydomain]
	...
		Optional. The list of users that you want to get log events for. Separate multiple users with a space. Use the wildcard symbol (*) to view logs for multiple users on a single security domain or all security domains. For example, the following strings are valid values for the option:
		`user:Native`
		`"user:*"`
		`"user*"`
		`"*_users_*"`
		`"*:Native"`
		If you use the wildcard symbol, enclose the argument in quotation marks.
		If you do not enter a user, the command retrieves the log events for all users.

-StartDate -sd	start_date	Optional. Returns log events starting from the date and time that you specify. Enter the date and time in one of the following formats: - MM/dd/yyyy - MM/dd/yyyy HH:mm:ss - yyyy-MM-dd - yyyy-MM-dd HH:mm:ss
-EndDate -ed	end_date	Optional. Returns log events ending by the date and time. Enter the date and time in the same format as the StartDate option. If you enter an end date that is before the start date, the command returns no log events.
-ActivityCode -ac	activity_code	Optional. Returns log events based on the activity code. Use the wildcard symbol (*) to retrieve log events for multiple activity codes. Valid activity codes include: - CCM_10437. Indicates that an activity succeeded. - CCM_10438. Indicates that an activity failed. - CCM_10778. Indicates that a login attempt with custom properties succeeded. - CCM_10779. Indicates that a login attempt with custom properties failed. - CCM_10786. Indicates that a login attempt without custom properties succeeded. - CCM_10787. Indicates that a login attempt without custom properties failed.
-atxt	activity_text	-ActivityText Optional. Returns log events based on a string found in the activity text. Use the wildcard symbol (*) to retrieve logs for multiple events. For example, the following parameter returns all log events that contain the phrase "Enabling service" in their description: `"*Enabling service*"` If you use the wildcard symbol, enclose the argument in quotation marks.

Option	Argument	Description
-ReverseOrder -ro	true	Optional. Prints log events in reverse chronological order. If you do not specify this parameter, the command displays log events in chronological order.
-OutputFile -lo	output_file_name	Optional. Name of the output file. If you do not specify this parameter, the command displays the log on the command line.
-Format -fm	output_format_BIN_TEXT_XML	Optional. Format of the log output file. Valid formats include: - Bin (binary) - Text - XML Default format is text. If you set the format to binary, then you must specify a file name using the -OutputFile option.

GetWorkflowLog

Gets log events for the most recent run of a workflow. The PowerCenter Repository Service must be running when you run this command.

The infacmd isp GetWorkflowLog command uses the following syntax:

```
GetWorkflowLog
<-DomainName|-dn> domain_name
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Format|-fm> format_TEXT_XML_BIN]
[<-OutputFile|-lo> output_file_name]
<-IntegrationService|-is> integration_service_name
<-RepositoryService|-rs> repository_service_name
[<-RepositoryDomain|-rd> domain_of_repository]
<-RepositoryUser|-ru> repository_user
<-RepositoryPassword|-rp> repository_password
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
<-FolderName|-fn> repository_folder_name
<-Workflow|-wf> workflow_name
[<-RunInstance|-in> run_instance_name] | <-RunId|-id> workflow_run_id]
```

Note: If you do not specify -un, -pd, and -sdn options, the infacmd isp GetWorkflowLog command uses the corresponding values from the -ru, -rp, and the -rsdn options.

The following table describes infacmd isp GetWorkflowLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-Format -fm	format	Optional. Format for the session log. Valid types include: - Text - XML - Bin (binary) If you choose binary, then you must specify a file name using the OutputFile option. If you do not specify a format, *infacmd* uses text format with lines wrapped at 80 characters.
-OutputFile -lo	output_file_name	Name and file path for the workflow log file. By default, the Service Manager uses the server\infa_shared\log directory on the master gateway node. Omit this option to display the log events on the screen. If you choose binary as the output file type, you must specify a file name using this option.
-IntegrationService -is	integration_service_name	Required. Name of the Integration Service that runs the workflow. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryService -rs	repository_service_name	Required. Name of the Repository Service that contains the workflow. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryDomain -rd	domain_of_repository	Required if the repository is in a domain other than the local domain. Domain of the Repository Service. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryUser -ru	user	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryPassword -rp	password	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required for LDAP or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If you do not specify this option, the command sets the repository user security domain to native.
-FolderName -fn	repository_folder_name	Required. Name of the folder containing the workflow. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-Workflow -wf	workflow_name	Required. Name of the workflow. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-RunInstance -in	run_instance_name	Name of the workflow run instance. Use this option if you are running concurrent workflows. Use the -in or the -id option, not both.
-RunId -id	workflow_run_id	Run identifier number (Run ID) of the workflow run instance. Use this option if you are running concurrent workflows. Use the -in or the -id option, not both. **Note:** Use this option if the workflow does not have a unique run instance name.

Help

Displays the options and arguments for an infacmd command.

If you omit the command name, infacmd lists all commands.

The infacmd Help command uses the following syntax:

```
Help <-plugin_ID> [command]
```

For example, if you type `infacmd isp Help GetServiceStatus`, infacmd returns the following options and arguments for the infacmd isp GetServiceStatus command:

```
GetServiceStatus
<-DomainName|-dn> domain_name <-UserName|-un> user_name <-Password|-pd> password [<-
Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds] <-ServiceName|-sn> service_name
```

The following table describes the infacmd Help option and arguments:

Option	Argument	Description
-	plugin_ID	Optional. Describes which infacmd program to display help for. Default is isp.
-	command	Optional. Name of command. If you omit the command name, infacmd lists all commands.

ImportDomainObjects

Imports native users, native groups, roles, connections, and cluster configurations from an XML file into an Informatica domain.

If you do not want to import all objects in the file, use an infacmd import control file to filter the objects that you want to import.

Use the ExportDomainObjects and ImportDomainObjects commands to migrate objects between two different domains of the same version. To import native users and groups from domains of different versions, use the infacmd isp ImportUsersAndGroups command.

When you import a group, you import all subgroups and users in the group.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd isp ImportDomainObjects command uses the following syntax:

```
ImportDomainObjects
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ImportFilePath|-fp> import_file_path
[<-ImportControlFile|-cp> import_control_file]
[<-ConflictResolution|-cr> resolution_type]
```

The following table describes infacmd isp ImportDomainObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ImportFilePath -fp	import_file_path	Required. Path and file name of the XML file from which you import the objects.
-ImportControlFile -cp	import_control_file	Optional. Path and file name of the import control file that filters the objects that are imported.
-ConflictResolution -cr	resolution_type	Optional. Conflict resolution strategy. You can specify one of the following options: - rename - replace - reuse The option is ignored if you specify a conflict resolution strategy in the import control file. If you do not define a conflict resolution strategy and a conflict occurs, the import fails. **Note:** You cannot use the rename option with a cluster configuration. **Note:** Password complexity is not required when you use it with reuse option.

ImportUsersAndGroups

Imports native users and groups into the domain.

Run infacmd isp ImportUsersAndGroups to import users and groups from an XML file.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd isp ImportUsersAndGroups command uses the following syntax:

```
ImportUsersAndGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ExportFile|-ef> export_file_name

[<-ReuseDomainUsersAndGroups|-rd> If there is a conflict use the users and groups
defined in the target domain]

[<-exportedFromPowercenter|-epc> The export file containing users and groups has been
exported from an Informatica PowerCenter 8.6.1 domain]
```

The following table describes infacmd isp ImportUsersAndGroups options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExportFile -ef	export_file_name	Required. Name and file path of the export file that contains the information about the users and groups.
-ReuseDomainUsersAndGroups -rd	-	Optional. If there is a name conflict, infacmd retains the users and groups defined in the target domain. By default, the command fails if it encounters a conflict.
-exportedFromPowercenter -epc	-	Required if the export file was exported from a PowerCenter version 8.6.1 domain.

Related Topics:

- "ExportUsersAndGroups" on page 502

ListAlertUsers

Lists users that subscribe to alerts.

The infacmd isp ListAlertUsers command uses the following syntax:

```
ListAlertUsers

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListAlertUsers options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

listAllCustomLDAPTypes

Lists the configuration information for all custom LDAP types used by the specified domain.

The infacmd isp ListLDAPConnectivity command uses the following syntax:

```
listAllCustomLDAPTypes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp listAllCustomLDAPTypes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListAllGroups

Lists all the groups in the native security domain.

The infacmd isp ListAllGroups command uses the following syntax:

```
ListAllGroups
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd isp ListAllGroups options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

listAllLDAPConnectivity

Lists the configuration information for all LDAP configurations used by the specified domain.

The infacmd isp ListLDAPConnectivity command uses the following syntax:

```
listAllLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp listAllLDAPConnectivity options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListAllRoles

Lists all the roles in the domain.

The infacmd isp ListAllRoles command uses the following syntax:

```
ListAllRoles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd isp ListAllRoles options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListAllUsers

Lists all the user accounts in the domain.

The infacmd isp ListAllUsers command uses the following syntax:

```
ListAllUsers
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd isp ListAllUsers options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListConnectionOptions

Lists options for a connection. Run this command to view available options to configure when you update a connection.

The infacmd isp ListConnectionOptions command uses the following syntax:

```
ListConnectionOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp ListConnectionOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection.

ListConnectionPermissions

Lists the permissions that a user or group has for a connection.

The infacmd isp ListConnectionPermissions command uses the following syntax:

```
ListConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp ListConnectionPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RecipientUserName -run	recipient_user_name	Required if you do not specify the recipient group name. Name of the user to list permissions for.
-RecipientGroupName -rgn	recipient_group_name	Required if you do not specify the recipient user name. Name of the group to list permissions for.
-RecipientSecurityDomain -rsd	recipient_security_domainth_name	Required if recipient belongs to an LDAP security domain. Name of the security domain that the recipient belongs to. Default is Native.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection.

ListConnectionPermissionsByGroup

Lists all groups that have permissions on a connection and lists the type of permissions.

The infacmd isp ListConnectionPermissionsByGroup command uses the following syntax:

```
ListConnectionPermissionsByGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp ListConnectionPermissionsByGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection.

ListConnectionPermissionsByUser

Lists the users that have permissions for a connection and lists the type of permissions.

The infacmd isp ListConnectionPermissionsByUser command uses the following syntax:

```
ListConnectionPermissionsByUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp ListConnectionPermissionsByUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection.

ListConnections

Lists connection names by type. You can list by all connection types or filter the results by one connection type.

The infacmd isp ListConnections command uses the following syntax:

```
ListConnections
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-ConnectionType|-ct> connection_type]
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListConnections options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ConnectionType -ct	connection_type	Optional. You can filter results with the -ct option. Use any supported connection type as the value for the -ct option. The input is not case sensitive. To see a list of connection types to use with this option, run the following command: `./infacmd.sh isp listConnections` The command lists all connection types and the connections that you configured on the domain.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListConnectionOptions

Lists options for a connection. Run this command to view available options to configure when you update a connection.

The infacmd isp ListConnectionOptions command uses the following syntax:

```
ListConnectionOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp ListConnectionOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection.

listCustomLDAPType

Lists the configuration information for a custom LDAP type.

The infacmd isp listCustomLDAPType command uses the following syntax:

```
listCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
```

The following table describes infacmd isp listCustomLDAPType options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Required. The name of the custom LDAP type.

ListDefaultOSProfiles

Lists the default operating system profiles for the given user or group.

The infacmd isp ListDefaultOSProfiles command uses the following syntax:

```
ListDefaultOSProfiles
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-RecipientName|-nm> recipient_name]
[<-RecipientSecurityDomain|-ns> security_domain_of_recipient]
[<-RecipientType|-ty> recipient_type]
[<-IndirectInheritance|-in> indirect_inheritance]
```

The following table describes infacmd isp ListDefaultOSProfiles options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-RecipientName -nm	recipient_name	Optional. User name or group name to assign default operating system profile.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Optional. Name of the security domain that the user belongs to, if you use LDAP authentication.
-RecipientType -ty	recipient_type	Optional. Specify whether the recipient is a user or a group. Enter any of the following values: - UserIdentity - GroupIdentity
-IndirectInheritance -in	indirect_inheritance	Optional. Enter one of the following values: - true. Lists the operating system profiles that the users or groups inherited from. - false. Lists the operating system profile that are directly assigned to the users or groups.

ListDomainCiphers

Lists one or more of the following cipher suite lists: blacklist, default list, effective list, or whitelist.

When you use secure communication within the domain and secure connections to web clients, Informatica uses an effective list of cipher suites to encrypt traffic. Informatica determines the effective list of cipher suites based on the following lists:

Blacklist

List of cipher suites that you want the Informatica domain to block. When you add a cipher suite to the blacklist, the Informatica domain removes the cipher suite from the effective list. You can add cipher suites that are on the default list to the blacklist.

Default list

List of cipher suites that the Informatica domain supports by default.

Whitelist

List of cipher suites that you want the Informatica domain to support in addition to the default list. When you add a cipher suite to the whitelist, the Informatica domain adds the cipher suite to the effective list. You do not need to add cipher suites that are on the default list to the whitelist.

Use the ListDomainCiphers command to view the cipher suite lists.

The infacmd isp ListDomainCiphers command uses the following syntax:

```
ListDomainCiphers

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-lists|-l> comma_separated_list_of_cipher_configurations...
(ALL,BLACK,WHITE,EFFECTIVE,DEFAULT)]
```

The following table describes infacmd isp ListDomainCiphers options and arguments:

Option	Argument	Description
–DomainName –dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
–Gateway –hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-lists -l	comma_separated_list_of_cipher_configurations	Optional. Comma-separated list of arguments that specifies the cipher suites that you want to display. The argument ALL displays the blacklist, default list, effective list, and whitelist. The argument BLACK displays the blacklist. The argument DEFAULT displays the default list. The argument EFFECTIVE displays the list of cipher suites that the Informatica domain supports. The argument WHITE displays the whitelist. **Note:** The arguments are case-sensitive. When you run the command on a gateway node and omit this option, the command displays all cipher suite lists. When you run the command on a worker node and omit this option, the command displays the default and effective cipher suite lists.

ListDomainLinks

Lists the domains to which the local domain can connect. You establish links between two domains if you want to exchange repository metadata between them.

The infacmd isp ListDomainLinks command uses the following syntax:

```
ListDomainLinks
```

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListDomainLinks options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the local domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the local domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListDomainOptions

Lists general properties of the domain. Properties include resilience timeout, limit on resilience timeouts, maximum restart attempts, restart period, SSL mode, and dispatch mode.

To run the infacmd isp ListDomainOptions command, you must have permission on the domain.

The infacmd isp ListDomainOptions command uses the following syntax:

```
ListDomainOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListDomainOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListExpiredPasswordUsers

Lists the users whose passwords exceed the duration of password validity.

You must have the administrator role to run this command.

The infacmd isp ListExpiredPasswordUsers command uses the following syntax:

```
ListExpiredPasswordUsers
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-maxPasswordValidDuration|-pvd> max_Password_Valid_Duration_in_days]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListExpiredPasswordUsers options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-maxPasswordValidDuration -pvd	max_Password_Valid_Duration_in_days	The duration of password validity. You can get a list of users whose passwords exceed the duration. Default is the duration configured in the domain.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. Specify the host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.

ListFolders

Lists the folders in the domain.

The infacmd isp ListFolders command uses the following syntax:

```
ListFolders

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListFolders options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListGridNodes

Lists the nodes assigned to a grid.

To run the infacmd isp ListGridNodes command, you must have permission on the grid.

The infacmd isp ListGridNodes command uses the following syntax:

```
ListGridNodes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
```

The following table describes *infacmd isp* ListGridNodes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GridName -gn	grid_name	Required. Name of the grid.

ListGroupPermissions

Lists group permissions on an object.

The infacmd isp ListGroupPermissions command uses the following syntax:

```
ListGroupPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingGroup|-eg> existing_group_name
[<-ExistingGroupSecurityDomain|-egn> existing_group_security_domain]
[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

The following table describes infacmd isp ListGroupPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file if out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ExistingGroup -eg	existing_group_name	Required. Name of the group to which you want to assign a permission on an object.
-ExistingGroupSecurityDomain -egn	existing_group_security_domainth_name	Required if you use LDAP authentication. Name of the security domain that the group to which you want to assign a permission belongs to. Default is Native.
-ObjectType -ot	object_type	Required. Type of object you want to list: - Service - License - Node - Grid - Folder - OSProfile

ListGroupPrivileges

Lists privileges assigned to a group in the domain. You can list group privileges for each application in the domain.

The infacmd isp ListGroupPrivileges command uses the following syntax:

```
ListGroupPrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-GroupName|-gn> group_name

[<-GroupSecurityDomain|-gsf> group_security_domain]

<-ServiceName|-sn> service_name
```

The following table describes infacmd isp ListGroupPrivileges options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group for which you want to list privileges.

Option	Argument	Description
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group for which you want to list privileges belongs to. Default is Native.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

ListGroupsForUser

Lists the native groups to which the user is assigned.

The infacmd isp ListGroupsForUser command uses the following syntax:

```
ListGroupsForUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
```

The following table describes infacmd isp ListGroupsForUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_Name	Required. Name of the user for which you want to list the groups.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain to which the user belongs. Default is Native.

ListLDAPConnectivity

Lists the details for the specified LDAP configuration.

The infacmd isp ListLDAPConnectivity command uses the following syntax:

```
ListLDAPConnectivity

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

The following table describes infacmd isp ListLDAPConnectivity options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Required. The name of the LDAP configuration.

ListLicenses

Lists the licenses in the domain. You can display the license name and serial number for each license.

To run the infacmd isp ListLicenses command, you must have permission on the licenses.

The infacmd isp ListLicenses command uses the following syntax:

```
ListLicenses
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port ...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListLicenses options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListMonitoringOptions

List monitoring general properties.

The infacmd isp listMonitoringOptions command uses the following syntax:

```
listMonitoringOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp listMonitoringOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of seconds that infacmd attempts to establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.

ListNodeOptions

Lists general properties for a node. General properties include backup directory, CPU profile, error severity level, maximum and minimum process ports, and resource provision thresholds.

To run the infacmd isp ListNodeOptions command, you must have permission on the node.

The infacmd isp ListNodeOptions command uses the following syntax:

```
ListNodeOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp ListNodeOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node for which you want to list the options.

ListNodeResources

Lists all resources defined for a node. For each resource, this command returns the resource type and whether the resource is available.

To run the infacmd isp ListNodeResources command, you must have permission on the node.

The infacmd isp ListNodeResources command uses the following syntax:

```
ListNodeResources
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]
```

The following table describes infacmd isp ListNodeResources options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node for which you want to list the resources.
-ResourceCategory -rc	resource_category	Optional. Category of resources that you want to list. Valid categories include: - PCIS. Resource for the PowerCenter Integration Service. - DIS. Reserved for future use. Default is PCIS.

ListNodeRoles

Lists all roles on a node in the domain.

The infacmd isp ListNodeRoles command uses the following syntax:

```
ListNodeRoles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name
```

The following table describes infacmd isp ListNodeRoles options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node.

ListNodes

Lists the nodes in the domain. If you do not use the node role option, the command lists all the nodes in the domain. If you use the node role option, the command lists the nodes with the specified role.

The infacmd isp ListNodes command uses the following syntax:

```
ListNodes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeRole|-nr> node_role SERVICE|COMPUTE|SERVICE_COMPUTE]
```

The following table describes infacmd isp ListNodes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeRole -nr	node_role	Optional. Role enabled on the nodes that you want to list. Enter one of the following values: - Service. Lists nodes with at least the service role. - Compute. Lists nodes with at least the compute role. - Service_compute. Lists nodes with both the service and compute roles. If you omit the option, the command lists all nodes in the domain.

ListOSProfiles

Lists the operating system profiles in the domain.

The infacmd isp ListOSProfile command uses the following syntax:

```
ListOSProfiles

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListRepositoryLDAPConfiguration

Lists the LDAP server configuration options such as LDAP server address, search scope, and login attributes.

Use this command after you install Informatica to verify the connection between the domain and the LDAP external directory service.

Use infacmd isp SetRepositoryLDAPConfiguration to update the LDAP server configuration options for an Informatica domain. You use this command when you upgrade a repository that uses LDAP authentication.

The infacmd isp ListRepositoryLDAPConfiguration command uses the following syntax:

```
ListRepositoryLDAPConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListRepositoryLDAPConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListRolePrivileges

Lists privileges assigned to a role in the domain. You can list role privileges for each application service in the domain.

You can list privileges assigned to a role for the domain and for each application service type in the domain.

The infacmd isp ListRolePrivileges command uses the following syntax:

```
ListRolePrivileges

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RoleName|-rn> role_name
```

The following table describes ListRolePrivileges options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RoleName -rn	role_name	Required. Name of the role to list privileges for. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

ListSecurityDomains

Lists the native and LDAP security domains in the domain.

The infacmd isp ListSecurityDomains command uses the following syntax:

```
ListSecurityDomains
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd isp ListSecurityDomains options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListServiceLevels

Lists the service levels defined for the domain. You can list the name, dispatch priority, and maximum dispatch wait time for each service level.

The infacmd isp ListServiceLevels command uses the following syntax:

```
ListServiceLevels
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListServiceLevels options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListServiceNodes

Lists the nodes or grid assigned to a service.

If this command returns a grid name, you can run the infacmd isp ListGridNodes command to list the nodes in the grid.

To run the infacmd isp ListServiceNodes command, you must have permission on the service.

The infacmd isp ListServiceNodes command uses the following syntax:

```
ListServiceNodes
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp ListServiceNodes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service.

Related Topics:

- "ListGridNodes" on page 563

ListServicePrivileges

Lists the privileges for a domain or application service type.

The infacmd isp ListServicePrivileges command uses the following syntax:

```
ListServicePrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceType|-st> service_type AS|CMS|LDM|MM|MRS|RS|TDM|TDW|DOMAIN]
```

The following table describes infacmd isp ListServicePrivileges options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceType -st	service_type	Optional. Domain or application service type for which you want to view privileges. Service types include: - AS. Analyst Service - CMS. Content Management Service - CS. Catalog Service - MM. Metadata Manager Service - MRS. Model Repository Service - RS. PowerCenter Repository Service - TDM. Test Data Manager Service - TDW. Test Data Warehouse Service - DOMAIN. Domain

ListServices

Lists the services in the domain.

The infacmd isp ListServices command uses the following syntax:

```
ListServices

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceType|-st> service_type AS|BW|CMS|DIS|EDP|ES|IDP|IHS|IS|LDM|MAS|MM|MRS|RMS|ROH|
RPS|RS|SATS|SCH|SEARCH|TDM|TDW|WS]
```

The following table describes infacmd isp ListServices options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceType -st	service_type	Optional. List all services of a specific type. You can choose to list the following service types: - AS. Analyst Service - BW. SAP BW Service - CMS. Content Management Service - DIS. Data Integration Service - EDP. Enterprise Data Preparation Service - ES. Email Service - IDP. Interactive Data Preparation Service - IHS. Informatica Cluster Service - IS. PowerCenter Integration Service - LDM. Catalog Service - MAS. Metadata Access Service - MM. Metadata Manager Service - MRS. Model Repository Service - RMS. Resource Manager Service - ROH. Rest Operations Hub Service - RPS. Reverse Proxy Server Service - RS. PowerCenter Repository Service - SATS. Data Privacy Management Service - SCH. Scheduler Service - SEARCH. Search Service - TDM. Test Data Manager Service - TDW. Test Data Warehouse Service - WS. Web Services Hub Service

ListSMTPOptions

Lists the SMTP configuration properties for the domain. The SMTP configuration is used to send domain alerts and scorecard notifications.

The infacmd isp ListSMTPOptions command uses the following syntax:

```
ListSMTPOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp ListSMTPOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Related Topics:

- "UpdateSMTPOptions" on page 718

ListUserPermissions

Lists the domain objects on which a user has permissions.

The infacmd isp ListUserPermissions command uses the following syntax:

```
ListUserPermissions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
[<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE]
```

The following table describes infacmd isp ListUserPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file if out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_name	Required. User account for which you want to list privileges. To enter a name that contains space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domainth_name	Required if you use LDAP authentication. Name of the security domain that the user for which you want to list privileges belongs to. Default is Native.
-ObjectType -ot	object_type	Required. Type of object you want to list: - Service - License - Node - Grid - Folder - OSProfile

ListUserPrivileges

Lists privileges assigned to a user in the domain. You can list user privileges for each application service in the domain.

The infacmd isp ListUserPrivileges command uses the following syntax:

```
ListUserPrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-ServiceName|-sn> service_name
```

The following table describes the infacmd isp ListUserPrivileges options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
ExistingUserName -eu	existing_user_name	Required. User account for which you want to list privileges. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user for which you want to list privileges belongs to. Default is Native.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

infacmd ListWeakPasswordUsers

Lists the users with passwords that do not meet the password policy.

The infacmd ListWeakPasswordUsers command uses the following syntax:

```
ListWeakPasswordUsers
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ListWeakPasswordUsers options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. Specify the host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.

migrateUsers

Migrates the groups, roles, privileges, and permissions of users in the native security domain to users in one or more LDAP security domains. Before you configure a domain to use Kerberos authentication, you must migrate the users to an LDAP security domain.

For more information about the migrateUsers command, see the *Informatica Security Guide*.

The infacmd isp migrateUsers command uses the following syntax:

```
migrateUsers

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> administrator_user_name

<-Password|-pd> administrator_password

[<-SecurityDomain|-sdn>|security_domain]

[<-Gateway|-hp>|gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds ]

<-UserMigrationFile|-umf> user_migration_file
```

The following table describes infacmd isp migrateUsers options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	administrator_user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	administrator_password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. **Note:** This security domain is the security domain of the user account used to connect to the domain, not the security domain to which the users will be migrated.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. Use if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

-UserMigrationFile
-umf
	user_migration_file	Required. Path and file name of the user migration file. The user migration file is a text file that contains the list of native users and the corresponding LDAP users. Entries must be in the following format:
		`Native/<SourceUserName>,LDAP/<TargetUsername>`
		For example, to migrate a user named User1 from the native security domain to a user named User1 in an LDAP security domain, add the following line to the user migration file:
		`Native/User1,LDAP/User1`
		The command skips entries with a duplicate source user name or target user name.

MoveFolder

Moves a folder.

The infacmd isp MoveFolder command uses the following syntax:

```
MoveFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OriginalPath|-op> original_folder_path
<-FolderPath|-fp> full_folder_path
```

The following table describes infacmd isp MoveFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-OriginalPath -op	original_folder_path	Required. Full path, excluding the domain name, to the folder you want to move. Must be in the following format: */parent_folder/child_folder*
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, to the target folder location. Must be in the following format: */parent_folder/child_folder*

MoveObject

Moves an object to another folder.

The infacmd isp MoveObject command uses the following syntax:

```
MoveObject
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID
<-FolderPath|-fp> full_folder_path
```

The following table describes infacmd isp MoveObject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ObjectName -on	object_name	Required. Name of the object you want to move.
-ObjectType -ot	object_type	Required. Type of object you want to move: - Service - License - Node - Grid
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, to the folder into which you want to move the object. Must be in the following format: */parent_folder/child_folder*

Ping

Pings a domain, service, domain gateway host, or node. If the object is available, this command displays a message that the object is available at a specific port on the gateway host machine. If the object is unavailable, this command displays a message saying that it failed to receive a response from the object.

Use this command to troubleshoot network connections. To run the infacmd isp Ping command, you must have permission on the object you want to ping.

The infacmd isp Ping command does not display results for individual service processes.

The infacmd isp Ping command uses the following syntax:

```
Ping
[<-DomainName|-dn> domain_name]
[<-ServiceName|-sn> service_name]
[<-GatewayAddress|-dg> domain_gateway_host:port]
[<-NodeName|-nn> node_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd isp Ping options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Optional. Name of the service you want to ping. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-GatewayAddress -dg	domain_gateway_host:port	Required if you do not specify the -DomainName option, or if you need to ping another domain. Gateway host machine name and port number.
-NodeName -nn	node_name	Optional. Name of the node.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

PingDomain

Pings all nodes and services in a domain. Displays the status of the domain, nodes, and services. You can choose to write the output to a text or .csv file.

The output uses the following formats to display the status of the domain, nodes, and services:

- Domain. MASTER_NODE_NAME, STATUS, HOST:PORT.
- Node. DOMAIN_NAME, NODE_NAME, STATUS, HOST:PORT.
- Service. SERVICE_NAME, NODE_NAME, STATUS, HOST:PORT.

If a service is disabled in the domain, the status displays DISABLED. The output does not display the node name, and the host name and port number.

If the service runs on a grid, the command pings each node in the grid. The output displays the status of the service on each node.

The infacmd isp PingDomain command uses the following syntax:

```
PingDomain
[<-DomainName|-dn> domain_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-of> output_file_name]
```

The following table describes infacmd isp PingDomain options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-Format -fm	format_TEXT_CSV	Optional. Format to display the status of the domain, nodes, and services. You can specify TEXT or CSV. The default format is TEXT.
-OutputFile -of	output_file_name	Name and file path where you want to write the output file.

PrintSPNAndKeytabNames

Generates the list of SPN and keytab file names for the nodes and services in the domain. The Informatica domain requires a keytab file for each SPN. You might need to ask the Kerberos administrator to add the SPNs to the principal database and create the keytab files. The SPN and keytab file names are case sensitive.

The infacmd isp PrintSPNAndKeytabNames command uses the following syntax:

```
PrintSPNAndKeytabNames
<-DomainName|-dn> domain_name
<-ServiceRealmName|-srn> realm_name_of_node_spn
[<-Format|-fm> format_TEXT_CSV]
[<-OutputFile|-of> output_file_name]
[<-DomainNodes|-dns> Node1:HostName1 Node2:HostName2 ...]
[<-ServiceProcesses|-sps> ServiceName1:NodeName1 ServiceName2:NodeName2...]
[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

The following table describes infacmd isp PrintSPNAndKeytabNames options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceRealmName -srn	realm_name_of_node_spn	Required. Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase and is case sensitive.

Option	Argument	Description
-Format -fm	format_TEXT_CSV	Optional. Output file format. Valid types include: - Text - CSV If you do not specify a format, infacmd uses text format with lines wrapped at 80 characters.
-OutputFile -of	output_file_name	Optional. Name and file path for the output file. If you do not specify an output file name, infacmd displays the log events on the screen.
-DomainNodes -dns	NodeName:HostName [NodeName:Hostname]	Name of the node and the fully qualified host name of the machine that hosts the node. Use the following format: NodeName:HostName You can generate SPNs and keytab file names for multiple nodes. Separate each node name and host name pair with a space.
-ServiceProcesses -sps	ServiceName:Nodena me [ServiceName:Nodena me]	Optional. Name of the service that you want to create in the Informatica domain and the name of the node on which the service will run. Use the following format: ServiceName:NodeName You can generate SPNs and keytab file names for multiple services. Separate each service name and node name pair with a space. **Note:** The keytab files for application services in the domain do not have to be available when you configure the domain to use Kerberos authentication. You can add the service SPN to the principal database and create the keytab after you change the Informatica domain authentication but before you enable the service.
SPNShareLevel -spnSL	SPNShareLevel PROCESS|NODE]	Optional. Indicates the service principal level for the domain. Set the property to one of the following levels: - Process. The domain requires a unique service principal name (SPN) and keytab file for each node and each service on a node. The number of SPNs and keytab files required for each node depends on the number of service processes that run on the node. Recommended for production domains. - Node. The domain uses one SPN and keytab file for the node and all services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Recommended for test and development domains. Recommended for test and development domains. Default is process.

PurgeLog

Purges log events. You can purge log events for a domain or for application services, such as the PowerCenter Integration Service, the Data Integration Service, and the Web Services Hub.

The infacmd isp PurgeLog command uses the following syntax:

```
PurgeLog
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-BeforeDate|-bd> before_date
```

The following table describes infacmd isp PurgeLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-BeforeDate -bd	before_date	Required. Purges log events that occurred before this date and time. Enter date and time in one of the following formats: - MM/dd/yyyy - yyyy-MM-dd

PurgeMonitoringData

Purges monitoring data from the Model repository.

The purgeMonitoringData command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NumDaysToRetain|-ndr> num_days_to_retain]

[<-NumDaysToRetainDetailedStat|-ndrds> num_days_to_retain_detailed_stat]
```

The following table describes the purgeMonitoringData options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain of the user. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the `domains.infa` file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of seconds that infacmd attempts to establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-NumDaysToRetain -ndr	num_days_to_retain	Optional. Number of days of averaged data to retain in the Model repository. For example, if you enter 180, then the Model Repository Service purges all averaged data that is older than 180 days. Minimum is 0. Maximum is 366. By default, the -ndr option uses the value of the **Preserve Summary Historical Data** option from the monitoring configuration.
-NumDaysToRetainDetailedStat -ndrds	num_days_to_retain_detailed_stat	Optional. Number of days of per-minute data to retain in the Model repository. For example, if you enter 7, then the Model Repository Service purges all averaged data that is older than 7 days. Minimum is 0. Maximum is 14. By default, the -ndrds option uses the value in the **Preserve Detailed Historical Data** option from the monitoring configuration.

RemoveAlertUser

Unsubscribes a user from alert notification emails. You can run infacmd isp RemoveAlertUser for any user.

The infacmd isp RemoveAlertUser command uses the following syntax:

```
RemoveAlertUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-AlertUser|-au> user_name
```

The following table describes infacmd isp RemoveAlertUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-AlertUser -au	user_name	Required. Name of user you want to unsubscribes from alerts.

RemoveConnection

Removes a connection from the domain.

The infacmd isp RemoveConnection command uses the following syntax:

```
RemoveConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp RemoveConnection options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name	Name of the connection to remove.

RemoveConnectionPermissions

Removes connection permissions for a user or group.

The infacmd isp RemoveConnectionPermissions command uses the following syntax:

```
RemoveConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<ReceipeintGroupName|-rgn>
recipeint_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name
```

The following table describes infacmd isp RemoveConnectionPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RecipientUserName -run	recipient_user_name	Required if you do not specify the recipient group name. Name of the user to remove permissions from.

Option	Argument	Description
-RecipientGroupName -rgn	recipient_group_name	Required if you do not specify the recipient user name. Name of the group to remove permissions for the connection.
-RecipientSecurityDomain -rsd	recipient_security_domain th_name	Required if recipient belongs to an LDAP security domain. Name of the security domain that the recipient belongs to. Default is Native.
-ConnectionName -cn	connection_name_security _domain	Required. Name of the connection.

removeCustomLDAPType

Removes the specified custom LDAP type.

The infacmd isp removeCustomLDAPType command uses the following syntax:

```
removeCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
```

The following table describes infacmd isp removeCustomLDAPType options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-CustomLDAPTypeName -lt	custom_LDAP_type_name	Required. The name of the custom LDAP type to remove.

RemoveDomainLink

Removes a linked domain. When you remove a linked domain, you cannot exchange repository metadata between the local and linked domains. You might want to do this if you no longer need to access a PowerCenter Repository Service in another domain.

The infacmd isp RemoveDomainLink command uses the following syntax:

```
RemoveDomainLink
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LinkedDomainName|-ld> linked_domain_name
```

The following table describes infacmd isp RemoveDomainLink options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the local domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the local domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LinkedDomainName -ld	linked_domain_name	Required. Name of the domain from which you want to remove a connection.

RemoveFolder

Removes a folder from the domain. Before you remove a folder, make sure that the folder is empty.

The folder must be empty.

The infacmd isp RemoveFolder command uses the following syntax:

```
RemoveFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderPath|-fp> full_folder_path
```

The following table describes infacmd isp RemoveFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, to the folder you want to remove. Must be in the following format: */parent_folder/child_folder*

RemoveGrid

Removes a grid from the domain. Before you can remove a grid, you must unassign the grid from the PowerCenter Integration Service or Data Integration Service.

The infacmd isp RemoveGrid command uses the following syntax:

```
RemoveGrid
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
```

The following table describes infacmd isp RemoveGrid options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.

Option	Argument	Description
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GridName -gn	grid_name	Required. Name of the grid you want to remove.

RemoveGroup

Removes a group from the native security domain.

The infacmd isp RemoveGroup command uses the following syntax:

```
RemoveGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
```

The following table describes infacmd isp RemoveGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group you want to remove.

RemoveGroupPermission

Removes a group permission on an object.

The infacmd isp RemoveGroupPermission command uses the following syntax:

```
RemoveGroupPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingGroup|-eg> existing_group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

The following table describes infacmd isp RemoveGroupPermission options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingGroup -eg	existing_group_name	Required. Name of the group to which you want to assign a permission on an object.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group to which you want to assign a permission belongs to. Default is Native.
-ObjectName -on	object_name	Name of the object that you want to remove the group access permission.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Required. Type of object. Enter one of the following values: - Service - License - Node - Grid - Folder - OSProfile

RemoveGroupPrivilege

Removes a privilege from a group in the domain. You can remove a privilege from a group for the domain or an application service in the domain.

The infacmd isp RemoveGroupPrivilege command uses the following syntax:

```
RemoveGroupPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-ServiceName|-sn> service_name
<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp RemoveGroupPrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group from which you are removing the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group from which you are removing privileges belongs to. Default is Native.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

-PrivilegePath
-pp
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "\" before it as follows:
		`"Model/View Model/Export\/Import Models"`

removeLDAPConnectivity

Removes the specified LDAP configuration.

The infacmd isp removeLDAPConnectivity command uses the following syntax:

```
removeLDAPConnectivity
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

The following table describes infacmd isp removeLDAPConnectivity options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Required. The name of the LDAP configuration to remove.

RemoveLicense

Removes a license from the domain. Before you run this command, you must first disable the services assigned to the license.

Removes a license from a domain when it expires or when you want to move the license to another domain.

The infacmd isp RemoveLicense command uses the following syntax:

```
RemoveLicense

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LicenseName|-ln> license_name
```

The following table describes infacmd isp RemoveLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license you want to remove.

Related Topics:

- "DisableService" on page 486
- "UnassignLicense" on page 668

RemoveNode

Removes a node from the domain. If the node is running, you must shut it down first.

The infacmd isp RemoveNode command uses the following syntax:

```
RemoveNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp RemoveNode options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node you want to remove.

RemoveNodeResource

Removes a resource from a node. You can remove a custom or file or directory resource from a node. You cannot remove a connection resource from a node.

When a PowerCenter Integration Service runs on a grid, the Load Balancer can use resources to distribute Session, Command, and predefined Event-Wait tasks. If the PowerCenter Integration Service is configured to check resources, the Load Balancer distributes tasks to nodes where the resources are added and enabled. If you remove a resource that is required by the Session or Command task, the task can no longer run on that node.

The infacmd isp RemoveNodeResource command uses the following syntax:

```
RemoveNodeResource

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

[<-ResourceCategory|-rc> resource_category ("PCIS", "DIS")]

<-ResourceType|-rt> resource_type("Custom", "File Directory")

<-ResourceName|-rn> resource_name
```

The following table describes infacmd isp RemoveNodeResource options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node that has the resource you want to remove.
-ResourceCategory -rc	resource_category	Optional. Category of resource you want to remove. Valid categories include: - PCIS. Resource for the PowerCenter Integration Service. - DIS. Reserved for future use. Default is PCIS.

Option	Argument	Description
-ResourceType -rt	resource_type	Required. Type of resource you want to remove. Valid types include: - Custom - File Directory
-ResourceName -rn	resource_name	Required. Entire name of the resource you want to remove. To list the names of all resources available to a node, run the infacmd isp ListNodeResources command.

RemoveOSProfile

Removes an operating system profile from the domain.

The infacmd isp RemoveOSProfile command uses the following syntax:

```
RemoveOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
```

The following table describes infacmd isp RemoveOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-OSProfileName -on	OSProfile_name	Required. Name of the operating system profile you want to remove.

RemoveRole

Removes a custom role from the domain. When you remove a custom role, the custom role and all privileges that it included are removed from any user or group assigned the role.

The infacmd isp RemoveRole command uses the following syntax:

```
RemoveRole
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
```

The following table describes infacmd isp RemoveRole options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RoleName -rn	role_name	Required. Name of the role you want to remove.

RemoveRolePrivilege

Removes a privilege from a role in the domain or from a role in an application service within the domain.

The infacmd isp RemoveRolePrivilege command uses the following syntax:

```
RemoveRolePrivileges
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RoleName|-rn> role_name
<-ServiceType|-st> service_type AS|CMS|LDM|MM|MRS|RS|TDM|TDW|DOMAIN]
<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp RemoveRolePrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RoleName -rn	role_name	Required. Name of the role from which you are removing the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ServiceType -st	service_type	Required. Domain or application service type from which you want to remove the privilege for the role. Service types include: - AS. Analyst Service - CMS. Content Management Service - CS. Catalog Service - MM. Metadata Manager Service - MRS. Model Repository Service - RS. PowerCenter Repository Service - TDM. Test Data Manager Service - TDW. Test Data Warehouse Service - DOMAIN. Domain

-PrivilegePath
-pp>
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "\" before it as follows:
		`"Model/View Model/Export\/Import Models"`

RemoveService

Removes an application service from the domain. Before you remove a service, you must disable it.

The infacmd isp RemoveService command uses the following syntax:

```
RemoveService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp RemoveService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of service you want to remove. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

RemoveServiceLevel

Removes a service level. When you remove a service level, the Workflow Manager does not update tasks that use the service level. If a workflow service level does not exist in the domain, the Load Balancer dispatches the tasks with the default service level.

The infacmd isp RemoveServiceLevel command uses the following syntax:

```
RemoveServiceLevel
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceLevelName|-ln> service_level_name
```

The following table describes infacmd isp RemoveServiceLevel options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceLevelName -ln	service_level_name	Required. Name of the service level you want to remove.

RemoveUser

Removes a user account from the native security domain. You cannot remove user accounts in the LDAP security domains.

The infacmd isp RemoveUser command uses the following syntax:

```
RemoveUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
```

The following table describes infacmd isp RemoveUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port .. .	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_name	Required. User account you want to remove.

RemoveUserFromGroup

Removes a native or LDAP user from a native group in the domain.

The infacmd isp RemoveUserFromGroup command uses the following syntax:

```
RemoveUserFromGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-GroupName|-gn> group_name
```

The following table describes infacmd isp RemoveUserFromGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_name	Required. Name of the user you want to remove.

Option	Argument	Description
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user you want to remove belongs to. Default is Native.
-GroupName -gn	group_name	Required. Name of the group from which you want to remove the user.

RemoveUserPermission

Removes a user permission on an object.

The infacmd isp RemoveUserPermission command uses the following syntax:

```
RemoveUserPermission
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_name
[<-ExistingUserSecurityDomain|-esd> existing_user_security_domain]
<-ObjectName|-on> object_name
<-ObjectType|-ot> object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE
```

The following table describes infacmd isp RemoveUserPermission options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable.
-ExistingUserName -eu	existing_user_name	Required. Name of the user to which you want to assign a permission on an object.

Option	Argument	Description
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user to which you want to assign a permission belongs to. Default is Native.
-ObjectName -on	object_name	Name of the object that you want to remove the user access permission.
-ObjectType -ot	object_type_SERVICE_LICENSE_NODE_GRID_FOLDER_OSPROFILE	Required. Type of object. Enter one of the following values: - Service - License - Node - Grid - Folder - OSProfile

RemoveUserPrivilege

Removes a privilege from a user in the domain or from a user in an application service within the domain.

The infacmd isp RemoveUserPrivilege command uses the following syntax:

```
RemoveUserPrivilege
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ExistingUserName|-eu> existing_user_Name
[<-ExistingUserSecurityDomain|-esd> existing_user_security
<-ServiceName|-sn> service_name
<-PrivilegePath|-pp> path_of_privilege
```

The following table describes infacmd isp RemoveUserPrivilege options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
ExistingUserName -eu	existing_user_name	Required. User account from which you are removing the privilege. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user from which you are removing the privilege belongs to. Default is Native.
-ServiceName -sn	service_name	Required. Domain or application service name for which you want to view privileges.

-PrivilegePath
-pp
	path_of_privilege	Required. Fully-qualified name of the privilege you want to assign to the group. A fully-qualified name includes privilege group name and privilege name. For example, a fully-qualified privilege name for the Repository Service is folder/create. If the privilege name includes spaces, enclose the path in quotation marks as follows:
		`"Runtime Objects/Monitor/Execute/Manage Execution"`
		If the privilege name includes the special character "/", add the escape character "\" before it as follows:
		`"Model/View Model/Export\ /Import Models"`

RenameConnection

Renames a connection. When you rename a connection, the Developer tool and the Analyst tool update the jobs that use the connection.

Note: Deployed applications and parameter files identify a connection by name, not by connection ID. Therefore, when you rename a connection, you must redeploy all applications that use the connection. You must also update all parameter files that use the connection parameter.

The infacmd isp RenameConnection command uses the following syntax:

```
RenameConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
<-NewConnectionName|-ncn> new_connection_name
```

The following table describes infacmd isp RenameConnection options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ConnectionName -cn	connection_name	Required. Existing connection name.
-NewConnectionName -ncn	new_connection_name	Required. New connection name. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /

ResetPassword

Resets the password for a user in the domain.

The infacmd isp ResetPassword command uses the following syntax:

```
ResetPassword
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ResetUserName|-ru> reset_user_name
<-ResetUserPassword|-rp> reset_user_password
```

The following table describes infacmd isp ResetPassword options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ResetUserName -ru	reset_user_name	Required. Name of the user whose password you want to reset.
-ResetUserPassword -rp	reset_user_password	Required. New password for the user. You can set a password with the -rp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

RunCPUProfile

Calculates the CPU profile for a node.

Note: This command takes approximately five minutes and uses 100% of one CPU on the machine.

The infacmd isp RunCPUProfile command uses the following syntax:

```
RunCPUProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp RunCPUProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node for which you want to calculate the CPU profile.

SetConnectionPermissions

Assigns permissions on connection to a user or a group after removing previous permissions.

The infacmd isp SetConnectionPermissions command uses the following syntax:

```
SetConnectionPermissions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<<-RecipientUserName|-run> recipient_user_name|<RecipientGroupName|-rgn>
recipient_group_name>

<-RecipientSecurityDomain|-rsd> recipient_security_domain]

<-ConnectionName|-cn> connection_name

[<-Permission|-p> permission_READ|WRITE|EXECUTE|GRANT|ALL
```

The following table describes infacmd isp SetConnectionPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-RecipientUserName -run	recipient_user_name	Required if you do not specify the recipient group name. Name of the user to assign permissions for the connection

Option	Argument	Description
-RecipientGroupName -rgn	recipient_group_name	Required if you do not specify the recipient user name. Name of the group to assign permissions for the connection.
-RecipientSecurityDomain -rsd	recipient_security_domain th_name	Required if recipient belongs to an LDAP security domain. Name of the security domain that the recipient belongs to. Default is Native.
-ConnectionName -cn	connection_name_security _domain	Required. Name of the connection.
-Permission -p	permission	Required. Type of permission to assign. Enter one or more of the following values separated by spaces: - READ - WRITE. Read and Write. - EXECUTE - GRANT. Read and Grant. - ALL. Read, Write, Execute, Grant

SetRepositoryLDAPConfiguration

Updates the LDAP server configuration options for a PowerCenter repository.

You may need to update the connection information between the repository and the LDAP external directory service after you install Informatica.

Use infacmd isp ListRepositoryLDAPConfiguration to view the current values for LDAP server configuration options.

The infacmd isp SetRepositoryLDAPConfiguration command uses the following syntax:

```
SetRepositoryLDAPConfiguration
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LDAPAddress|-la> ldap_server_address
<-SearchBase|-sb> search base
<-SearchScope|-ss> search scope
<-LDAPPrincipal|-lp> ldap_principal
<-LDAPCredential|-lc> ldap_credential
<-LoginAttribute|-lt> login attribute
```

```
<-LoginFilter|-lf> login filter

[<-UseSSL|-us> use_ssl]

[<-CertificateDatabase|-cd> certificate database for ssl]
```

The following table describes infacmd isp SetRepositoryLDAPConfiguration options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-LDAPAddress -la	ldap_server_address	Required. Host name and port number for the machine hosting the LDAP directory service. Typically, the LDAP server port number is 389.
-SearchBase -sb	search base	Required. Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory tree. LDAP finds an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName, where the series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.
-SearchScope -ss	search scope	Required. Scope of the user search. Choose one of the following options: - Base. Search the entry identified by search base. - One level. Search all entries one level beneath the search base entry but not including the search base entry. - Subtree. Search the entire subtree at all levels beneath the search base entry.
-LDAPPrincipal -lp	ldap_principal	Required. Distinguished name (DN) for the principal user. The user name often consists of a common name (CN), an organization (O), and a country (C). The Principal User Name is an administrative user with access to the directory and is not the name to authenticate. Specify a user who has permission to read other user entries in the LDAP server. Omit this option to log in as an anonymous user. For more information, refer to the LDAP Server documentation.
-LDAPCredential -lc	ldap_credential	Required. Password for the principal user. You can set a password with the -lc option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -lc option takes precedence. Omit this option to log in as an anonymous user.
-LoginAttribute -lt	login_attribute	Required. Directory attribute that contains login names.
-LoginFilter -lf	login_filter	Required. An LDAP query string to filter results for user search. The filter can specify attribute types, assertion values, and matching criteria. For example: (objectclass=*) searches all objects. (&(objectClass=user)(!(cn=susan))) searches all user objects except “susan.” For more information about search filters, see the LDAP server documentation.
-UseSSL -us	use_ssl	Do not use this option. Informatica does not support an LDAP server that uses SSL for versions 8.1.1 .
-CertificateDatabase -cd	certificate_database_for_ssl	Do not use this option. Informatica does not support an LDAP server that uses SSL for versions 8.1.1 .

ShowLicense

Displays license details. The license details you see are a cumulative result of all license keys applied. The Service Manager updates the existing license details when you add an incremental key to the license.

To run the infacmd isp ShowLicense command, you must have permission on the license.

The infacmd isp ShowLicense command uses the following syntax:

```
ShowLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
```

The following table describes infacmd isp ShowLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license.

ShutdownNode

Shuts down a node. After you shut down a node, you can restart the node by starting the Informatica service on the machine. You cannot restart a node using infacmd.

The infacmd isp ShutdownNode command uses the following syntax:

```
ShutdownNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp ShutdownNode options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node you want to shut down.

SwitchToGatewayNode

Converts an existing worker node to a gateway node. The worker node must have the service role enabled.

The infacmd isp SwitchToGatewayNode command uses the following syntax:

```
SwitchToGatewayNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-EnableSaml|-saml> true|false]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
<-LogServiceDirectory|-ld> log_service_directory
```

```
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes infacmd isp SwitchToGatewayNode options and arguments:

Option	Description
-DomainName -dn	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	Required. Name of the node you want to make a gateway node.
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-SamlTrustStoreDir -std	Optional. The directory containing the custom truststore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.

Option	Description
-SamlTrustStorePassword -stp	Required if you use a custom truststore for SAML authentication. The password for the custom truststore.
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore. *
-AdminconsolePort -ap	Port to access Informatica Administrator.
-AdminconsoleShutdownPort -asp	Port number that controls shutdown for Informatica Administrator.
-LogServiceDirectory -ld	Required. Shared directory path used by the Log Manager to store log event files. Ensure that the -ld value does not match or contain the specified -sld value.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database. Required if you configure a secure domain repository database for the domain.
-DatabaseTruststoreLocation -dbtl	Path and file name of the truststore file for the secure database. Required if you configure a secure domain repository database for the domain.
Note: If you currently run scripts that use this command to enable a custom keystore for SAML authentication, you must update them to include this option.	

SwitchToWorkerNode

Converts a gateway node to a worker node. The command fails if the node you want to switch is the only gateway node in the domain.

If the node serves as the master gateway node, you must shut down the node before you can convert it to a worker node. Shut down the node and wait for the master gateway to fail over to another node. You can then restart the node and run the infacmd isp SwitchToWorkerNode command.

The infacmd isp SwitchToWorkerNode command uses the following syntax:

```
SwitchToWorkerNode

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp SwitchToWorkerNode options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node you want to make a worker node.

SyncSecurityDomains

Synchronizes users and groups in a security domain with the users and groups in the LDAP directory service.

The infacmd isp SyncSecurityDomains command uses the following syntax:

```
SyncSecurityDomains
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SynchronizingNamespace|-sn> namespace_to_sync
```

The following table describes infacmd isp SyncSecurityDomain options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-SynchronizingNamespace -sn	namespace_to_sync	Name of the security domain you want to synchronize with the LDAP directory service.
-WaitCompletion -wc	true|false	Optional. Indicates whether infacmd waits for the command to complete before reporting the success or failure of synchronization. If true, reports if the command fails to start. If the command starts successfully, reports whether synchronization succeeds or fails. If false, reports whether the command starts successfully or fails to start, without waiting for synchronization to complete. Default is false.

UnassignDefaultOSProfile

Removes the default operating system profile that is assigned to a user or group.

The infacmd isp UnassignDefaultOSProfile command uses the following syntax:

```
UnassignDefaultOSProfile
<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-RecipientName|-nm> recipient_name

<-RecipientSecurityDomain|-ns> security_domain_of_recipient

<-RecipientType|-ty> recipient_type
```

The following table describes infacmd isp UnassignDefaultOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-RecipientName -nm	recipient_name	Required. User name or group name to assign default operating system profile.
-RecipientSecurityDomain -ns	security_domain_of_recipient	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-RecipientType -ty	recipient_type	Required. Specify whether to assign the default operating system profile to a user or a group. Enter any of the following values: - UserIdentity - GroupIdentity

UnassignISMMService

Disassociates a PowerCenter Integration Service from a Metadata Manager Service. If you remove a PowerCenter Integration Service, you must associate another PowerCenter Integration Service before you load resources.

The infacmd isp UnassignISMMService command uses the following syntax:

```
UnassignISMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> securitydomain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-IntegrationService|-is> integration_service_name
```

The following table describes infacmd isp UnassignISMMService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Metadata Manager Service for which you want to unassign the Integration Service.
-IntegrationService -is	integration_service_name	Required. Name of the Integration Service you want to unassociate from the Metadata Manager Service.

UnassignLicense

Removes a license from an application service. The service must be stopped. After you remove the license from the service, you must assign a valid license to re-enable the service.

The UnassignLicense command uses the following syntax:

```
UnassignLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-ServiceNames|-sn> service1_name service2_name ...
```

The following table describes *infacmd isp* UnassignLicense options and arguments:

Option	Arguments	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that *infacmd* attempts to establish or reestablish a connection to the domain. If you omit this option, *infacmd* uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license you want to unassign.
-ServiceNames -sn	service_name1 service_name2 ...	Required. Names of the services for which you want to remove the license. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

UnassignRoleFromGroup

Removes a role from a group for a domain or an application service.

The infacmd isp UnassignRoleFromGroup command uses the following syntax:

```
UnassignRoleFromGroup
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GroupName|-gn> group_name
[<-GroupSecurityDomain|-gsf> group_security_domain]
<-RoleName|-rn> role_name
<-ServiceName|-sn> service_name
```

The following table describes infacmd isp UnassignRoleFromGroup options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GroupName -gn	group_name	Required. Name of the group from which you want to remove a role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-GroupSecurityDomain -gsf	group_security_domain	Required if you use LDAP authentication. Name of the security domain that the group from which you are removing the role belongs to. Default is Native.
-RoleName -rn	role_name	Required. Name of the role you want to remove from the group.
-ServiceName -sn	service_name	Required. Domain or application service name from which you want to remove the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

UnassignRoleFromUser

Removes a role from a user for a domain or an application service.

The infacmd isp UnassignRoleFromUser command uses the following syntax:

```
UnassignRoleFromUser

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ExistingUserName|-eu> existing_user_Name

[<-ExistingUserSecurityDomain|-esd> existing_user_securit

<-RoleName|-rn> role_name

<-ServiceName|-sn> service_name
```

The following table describes infacmd isp UnassignRoleFromUser options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ExistingUserName -eu	existing_user_Name	Required. User account from which you are removing the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-ExistingUserSecurityDomain -esd	existing_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user from which you are removing the role belongs to. Default is Native.
-RoleName -rn	role_name	Required. Name of the role you want to remove from the user.
-ServiceName -sn	service_name	Required. Domain or application service name from which you want to remove the role. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

UnassignRSWSHubService

Disassociates a PowerCenter repository from a Web Services Hub in the domain.

The infacmd isp UnassignRSWSHubService command uses the following syntax:

```
UnassignRSWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
```

The following table describes infacmd isp UnassignRSWSHubService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Web Services Hub from which you want to disassociate a repository.

Option	Argument	Description
-NodeName -nn	node_name	Required. Name of the node where the Web Services Hub process runs. If the Informatica environment is configured for high availability, this option specifies the name of the primary node.
-RepositoryService -rs	repository_service_name	Required. Name of the Repository Service that the Web Services Hub depends on. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

UnassociateDomainNode

Disassociates a node in a domain from its address. The node name remains part of the domain, but it has no physical address.

For example, in a domain, “Node1” is associated with machine “MyHost:9090.” When you run this command, the connection between the name “Node1” and the host address “MyHost:9090” is removed. You can then associate “Node1” with a new host. You must run the infasetup DefineGatewayNode or DefineWorkerNode command on the new host to define “Node1” on that machine.

The infacmd isp UnassociateDomainNode command uses the following syntax:

```
UnassociateDomainNode
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd isp UnassociateDomainNode options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node you want to disassociate from the domain.

UpdateConnection

Updates a connection. To list connection options, run infacmd isp ListConnectionOptions.

The infacmd isp UpdateConnection command uses the following syntax:

```
UpdateConnection
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ConnectionName|-cn> connection_name
[<-ConnectionUserName|-cun> connection_user_name]
[<-ConnectionPassword|-cpd> connection_password]
[-o options] (name-value pairs separated by space)
```

The following table describes infacmd isp UpdateConnection options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ConnectionName -cn	connection_name_security_domain	Required. Name of the connection to update.
ConnectionUserName -cun	connection_user_name	Required. Database user name.

Option	Argument	Description
-ConnectionPassword -cpd	connection_password	Required. Password for the database user name. If you are updating an ADABAS, DB2I, DB2Z, IMS, SEQ, or VSAM connection, you can enter a valid PowerExchange passphrase instead of a password. Passphrases for access to databases and data sets on z/OS can be from 9 to 128 characters in length. Passphrases for access to DB2 for i5/OS can be up to 31 characters in length. Passphrases can contain the following characters: - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Note:** The first character is an apostrophe. Passphrases cannot include single quotation marks (‘), double quotation marks (“), or currency symbols. If a passphrase contains spaces, you must enclose it with double-quotation marks ("), for example, `"This is an example passphrase"`. If a passphrase contains special characters, you must enclose it with triple double-quotation characters ("""), for example, `"""This passphrase contains special characters ! % & *."""`. If a passphrase contains only alphanumeric characters without spaces, you can enter it without delimiters. **Note:** On z/OS, a valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation. To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the *PowerExchange Reference Manual*. To use passphrases for IMS connections, ensure that the following additional requirements are met: - You must configure ODBA access to IMS as described in the *PowerExchange Navigator User Guide*. - You must use IMS data maps that specify IMS ODBA as the access method. Do not use data maps that specify the DL/1 BATCH access method because this access method requires the use of netport jobs, which do not support passphrases. - The IMS database must be online in the IMS control region to use ODBA access to IMS.
- Options -o	options	Space separated name-value pairs.

Option	Argument	Description
		To enter a value that contains spaces or other non-alphanumeric characters, enclose the value in single quotes. Enclose the options in double quotes. To view valid options, run infacmd isp ListConnectionOptions.

updateCustomLDAPType

Updates a custom LDAP type that defines an LDAP directory service from which you import users into an LDAP security domain.

The infacmd isp updateCustomLDAPType command uses the following syntax:

```
updateCustomLDAPType
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-CustomLDAPTypeName|-lt> custom_LDAP_type_name
[<-DisplayName|-dpn> display_name]
[<-Uid> uid]
[<-GroupMembershipAttr|-gm> group_membership_attr]
[<-GroupDescriptionAttr|-gd> group_description_attr]
[<-UserSurnameAttr|-usn> user_surname_attr]
[<-UserGivenNameAttr|-ugn> user_given_name_attr]
[<-UserEmailAttr|-ue> user_email_attr]
[<-UserEnableAttr|-uen> user_enable_attr]
[<-UserTelephoneAttr|-utn> user_telephone_attr]
[<-UserDescriptionAttr|-ud> user_description_attr]
[<-CN> cn]
[<-FetchRangedAttr|-fr> fetch_ranged_attr]
```

The following table describes infacmd isp updateCustomLDAPType options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
- -CustomLDAPTypeName -lt	custom_LDAP_type_name	Required. Name of the custom LDAP type to update.

Option	Argument	Description
- -DisplayName -dpn	display_name	Optional. Name of the custom LDAP type displayed in the Administrator tool.
-Uid	uid	Optional. Name of the attribute in the LDAP directory service that contains the unique identifier (UID) that the Service Manager uses to identify users.
- -GroupMembershipAttr -gm	group_membership_attr	Optional. Name of the attribute in the LDAP directory service that contains group membership information for a user.
-GroupDescriptionAttr -gd	group_description_attr	Optional. Name of the attribute in the LDAP directory service that contains descriptive text about the groups in the directory service.
-UserSurnameAttr -usn	user_surname_attr	Optional. Name of the attribute in the LDAP directory service that contains the last name for a user.
-UserGivenNameAttr -ugn	user_given_name_attr	Optional. Name of the attribute in the LDAP directory service that contains the first name for a user.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name of the attribute in the LDAP directory service that contains the names of groups in the directory service.
--UserEmailAttr -ue	user_email_attr	Optional. Name of the attribute in the LDAP directory service that contains the email address for a user.
-UserEnableAttr -uen	user_enable_attr	Optional. Name of the attribute in the LDAP directory service that contains
- UserTelephoneAttrr -utn	user_telephone_attr	Optional. Name of the attribute in the LDAP directory service that contains th telephone number for a user.
- User DescriptionAttrr -ud	user_description_attr	Optional. Name of the attribute in the LDAP directory service that contains a description for a user.
-CN	cn	Optional. Name of the attribute in the LDAP directory service that contains the attribute that holds the full name or common name for a user.
- FetchRangedAttr -fr	fetch_ranged_attr	Optional. Set to true to retrieve all of the values contained in multivalued attributes. Use this option with Microsoft Active Directory only.

UpdateDomainOptions

Updates domain properties. Domain properties include resilience timeout, limit on resilience timeouts, maximum restart attempts, restart period, TLS mode, and dispatch mode.

The infacmd isp UpdateDomainOptions command uses the following syntax:

```
UpdateDomainOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-DomainOptions|-do> option_name=value ...
```

The following table describes infacmd isp UpdateDomainOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-DomainOptions -do	option_name=value	Required. Domain properties you want to update. You can update the following properties: - LicenseUsageDetailMinDays. Minimum number of days the Log Manager keeps log events for license usage. - LicenseUsageSummaryMinDays. Minimum number of days the Log Manager keeps database records for license usage. - ResilTimeout. Amount of time in seconds services attempt to connect as clients to other services. - RestartsMaxAttempts. Number of times within a specified period that the domain attempts to restart an application service process when it fails. - RestartsWithinSeconds. Maximum period of time in seconds that the domain spends attempting to restart an application service process when it fails. - ServiceResilTimeout. Maximum amount of time that the service holds on to resources to accommodate resilience timeouts. - TaskDispatchMode. Load Balancer dispatch mode for tasks: RoundRobin, MetricBased, or Adaptive. Restart the Integration Service to apply changes. - TLSMode. Configures secure communication between services within the domain. To apply changes, restart the domain. Valid values are true or false.

UpdateFolder

Updates the folder description.

The infacmd isp UpdateFolder command uses the following syntax:

```
UpdateFolder
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FolderPath|-fp> full_folder_path
<-FolderDescription|-fd> description_of_folder
```

The following table describes infacmd isp UpdateFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-FolderPath -fp	full_folder_path	Required. Full path, excluding the domain name, to the folder you want to update. Must be in the following format: */parent_folder/child_folder*
-FolderDescription -fd	description_of_folder	Required. Description of the folder. If the folder description contains spaces or other non-alphanumeric characters, enclose it in quotation marks.

UpdateGatewayInfo

Updates gateway node connectivity information in the domains.infa file.

Run infacmd isp UpdateGatewayInfo to create a domains.infa file or update a domains.infa file. The domains.infa file contains the connectivity information for a gateway node in a domain along with the TLS and Kerberos configuration of the domain. The connectivity information includes the domain name, domain host name, and domain host HTTP port.

You might need to generate a domains.infa file to run infacmd oie commands on a client machine. To generate the domains.infa file, run infacmd isp UpdateGatewayInfo. The updateGatewayInfo command generates a domains.infa file in the DeveloperClient directory. Define the domain gateway host name and port when you run the command.

The infacmd isp UpdateGatewayInfo command uses the following syntax:

```
UpdateGatewayInfo

<-DomainName|-dn> domain_name

<-GatewayAddress|-dg> domain_gateway_host:port

[<-Force|-f>]
```

The following table describes infacmd isp UpdateGatewayInfo options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-GatewayAddress -dg	domain_gateway_host:port	Required. Gateway host machine name and port number. Enter the gateway address in the following format: `domain_gateway_host:port`
-Force -f	-	Optional. Updates or creates the domains.infa file even when the connection to the domain fails. The -Force option sets the Kerberos and TLS enabled options as false in the domains.infa file if the connection to domain fails. If you do not specify the -Force option, the command does not update the domains.infa file if the connection to the domain fails.

UpdateGrid

Updates the list of nodes assigned to a grid.

The infacmd isp UpdateGrid command uses the following syntax:

```
UpdateGrid
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-GridName|-gn> grid_name
<-NodeList|-nl> node1 node2 ...
[<-UpdateNodeList|-ul> true|false]
```

The following table describes infacmd isp UpdateGrid options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-GridName -gn	grid_name	Required. Name of the grid.
-NodeList -nl	node1 node2 ...	Required. Names of the nodes that you want to assign to the grid. This list of nodes replaces or updates the list of nodes previously assigned to the grid based on the -ul option defined. If you specify the -ul option, the -nl option updates the list of nodes previously assigned to the grid. If you do not specify the -ul option, the -nl option replaces the list of nodes previously assigned to the grid.
-UpdateNodeList -ul	true|false	Optional. Updates the current node list with the values in the -nl option instead of replacing the list of nodes previously assigned to the grid. If true, infacmd updates the node list with the list of nodes specified using the -nl option along with the nodes previously assigned to the grid. If false, infacmd replaces the node list with the list of nodes specified using the -nl option. Default is false.

UpdateIntegrationService

Updates the configuration properties for the PowerCenter Integration Service.

The infacmd isp UpdateIntegrationService command uses the following syntax:

```
UpdateIntegrationService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-NodeName|-nn> node_name|<-GridName|-gn> grid_name]
[<-BackupNodes|-bn> node1 node2 ...]
[<-RepositoryService|-rs> repository_service_name]
[<-RepositoryUser|-ru> repository_user]
[<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
[<-ServiceOptions|-so> option_name=value ...]
```

Note: For infacmd isp UpdateIntegrationService, you must not use the -ru, -rp, and the -rsdn options in Kerberos authentication. If you use these options in Kerberos mode, the command will fail.

The following table describes infacmd isp UpdateIntegrationService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Integration Service name. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Optional. Name of the node where the Integration Service process runs. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node. Do not enter a value for this option if you specify the grid name.
-GridName -gn	grid_name	Optional. Name of the grid where the Integration Service process runs. Do not enter a value for this option if you specify the node name.
-BackupNodes -bn	node1 node2 ...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-RepositoryService -rs	repository_service_name	Optional. Name of the Repository Service that the Integration Service depends on. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-RepositoryUser -ru	user	Required for native or LDAP authentication. User name used to connect to the repository. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-RepositoryPassword -rp	password	Required for native or LDAP authentication. User password. You can set a password with the -rp option or the environment variable INFA_REPOSITORY_PASSWORD. If you set a password with both methods, the password set with the -rp option takes precedence.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Required for LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain name is case sensitive. If you do not specify this option, the command sets the repository user security domain to native.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the PowerCenter Integration Service runs.

updateLDAPConnectivity

Updates the specified LDAP configuration.

The infacmd isp updateLDAPConnectivity command uses the following syntax:

```
updateLDAPConnectivity

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-LDAPAddress|-la> ldap_server_address

[<-LDAPPrincipal|-lp> ldap_principal]

[<-LDAPCredential|-lc> ldap_credential]

[<-UseSSL|-us> use_ssl]

[<-TrustLDAPCertificate|-tc> trust_ldap_certificate]

<-LDAPType|-lt> ldap_types=MicrosoftActiveDirectory, MicrosoftAzureActiveDirectory,
SunJavaSystemDirectory, NovellE-Directory, IBMTivoliDirectory, OpenLDAP,
OracleDirectoryServerODSEE, OracleUnifiedDirectory, <Custom LDAP Type Name>

[<-MaxSecurityDomainSize|-ms> Max_Security_Domain_size]

[<-GroupMembershipAttr|-gm> LDAP_Group_Membership_Attribute]

[<-LDAPNotCaseSensitive|-lnc> ldap_not_case_sensitive]

<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name
```

The following table describes infacmd isp updateLDAPConnectivity options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LDAPAddress -la	ldap_server_address	Required. Host name and port number for the machine hosting the LDAP directory service. Typically, the LDAP server port number is 389. If the LDAP server uses SSL, the LDAP server port number is 636.

Option	Argument	Description
-LDAPPrincipal -lp	ldap_principal	Optional. Distinguished name (DN) for the principal user. Omit this option to log in as an anonymous user. For more information, refer to the documentation for the LDAP directory service.
-LDAPCredential -lc	ldap_credential	Optional. Password for the principal user. You can set a password with the -lc option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -lc option takes precedence. Omit this option to log in as an anonymous user.
-UseSSL -us	use_ssl	Optional. If you include the option, the LDAP directory service uses Secure Socket Layer (SSL) protocol.
-TrustLDAPCertificate -tc	trust_ldap_certificate	Optional. If you include the option, PowerCenter connects to the LDAP server without verifying the SSL certificate. If you do not include the option, PowerCenter verifies that the SSL certificate is signed by a Certificate Authority before connecting to the LDAP server
-LDAPType -lt	ldap_types=value	Required. Type of LDAP directory service. Directory services include: - MicrosoftActiveDirectory - Microsoft Azure Active Directory - SunJavaSystemDirectory - NovellE-Directory - IBMTivoliDirectory - OpenLDAP - Oracle Directory Server (ODSEE) - Oracle Unified Directory If you use a custom LDAP directory service, specify the name of the service.
-MaxSecurityDomainSize -ms	Max_Security_Domain_size	Optional. Maximum number of user accounts to import into a security domain. Default is 1000.
-GroupMembershipAttr -gm	LDAP_Group_Membership_Attribute	Optional. Name of the attribute that contains group membership information for a user.
-LDAPNotCaseSensitive -lnc	LDAP_Not_Case_Sensitive	Optional. Indicates that the user names from the LDAP directory service are not case sensitive. Default is false.
-LDAPHostConfigurationName -lcn	LDAP_host_configuration_name	Required. The name of the LDAP configuration to update.

UpdateLicense

Updates license information for the domain. Run this command to upgrade your license using an incremental license key. You use the key to add or remove licensed options.

When you add an incremental key to a license, the Service Manager updates the license expiration date if the expiration date on the incremental key is later than the original key.

The infacmd isp UpdateLicense command uses the following syntax:

```
UpdateLicense
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-LicenseName|-ln> license_name
<-LicenseKeyFile|-lf> license_key_file
```

The following table describes infacmd isp UpdateLicense options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-LicenseName -ln	license_name	Required. Name of the license object you want to update.
-LicenseKeyFile -lf	license_key_file	Required. Name and path to the file that contains the incremental keys.

UpdateMMService

Updates or creates the service options for a Metadata Manager Service. To update or create the service options, disable the Metadata Manager Service, update the options, and re-enable the service.

The infacmd isp UpdateMMService command uses the following syntax:

```
UpdateMMService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-LicenseName|-ln> license_name]
<-ServiceOptions|-so> option_name=value ...>
```

The following table describes infacmd isp UpdateMMService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Metadata Manager Service you want to update.
-LicenseName -ln	license_name	Required. Name of the license you want to assign to the Metadata Manager Service.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the Metadata Manager Service runs.

UpdateMonitoringOptions

Updates general properties to monitor actions in the domain.

When you specify a Model Repository Service with the -ModelRepositoryService option, you must also enter values for the -RepositoryUserName and -RepositoryPassword options. You must include values for all three options or for none of them.

The infacmd isp UpdateMonitoringOptions command uses the following syntax:

```
UpdateMonitoringOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ModelRepositoryService|-rs> model_repository_service]

[<-RepositoryUserName|-rsun> model_repository_user_name]

[<-RepositoryPassword|-rspd> model_repository_password]

[<-RepositorySecurityDomain|-rsdn> model_repository_security_domain]

[<-AdministratorOptions|-ao> option_name=value ...(MaxSortedRecords, ShowMilliSeconds)]

[<-CachingOption|-co> option_name=value ...(DefaultNotificationDelay)]

[<-PurgeOptions|-po> option_name=value ...(PurgeScheduleTime, PurgeTaskFrequency,
StatisticsExpiryTime, DetailedStatisticsExpiryTime)]
```

The following table describes infacmd isp UpdateMonitoringOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of seconds that infacmd attempts to establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-ModelRepositoryService -rs	model_repository_service	Optional. Name of the Model Repository Service that stores the historical information.
-RepositoryUserName -rsun	model_repository_user_name	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User name to access the Model Repository Service.
-RepositoryPassword -rspd	model_repository_password	Required for native or LDAP authentication. Optional if the domain uses Kerberos authentication. User password to access the Model Repository Service.
-RepositorySecurityDomain -rsdn	model_repository_security_domain	Required for LDAP or Kerberos authentication. Optional if the domain uses native authentication. Name of the security domain to which the PowerCenter repository user belongs. The security domain is case sensitive. If you do not specify this option, the command sets the repository user security domain to native.

Option	Argument	Description
-AdministratorOptions -ao	option_name=value	Optional. General administrative settings for records and monitoring reports. You can set the following options: - MaxSortedRecords. Maximum number of records that can be sorted. Default is 3,000. - ShowMilliseconds. Include milliseconds for date and time field in monitoring reports. You can set to true or false. Default is false.
-CachingOption -co	option_name=value	Optional. Settings for caching statistics. You can set the following options: - DefaultNotificationDelay. Maximum number of seconds that the Data Integration Service buffers the statistics before persisting the statistics in the Model Repository and writing them to a monitoring report. Default is 10.
-PurgeOptions -po	option_name=value	Optional. Settings for purging statistics. You can set the following options: - PurgeScheduleTime. Time of day when the Model Repository Service purges statistics. Default is 1:00 a.m. - PurgeTaskFrequency. Interval, in days, at which the Model Repository Service purges statistics that are older than the values configured for the ExpiryTime options. Default is 1. - StatisticsExpiryTime. Number of days that the Model repository saves averaged statistics. If purging is disabled, then the Model repository saves the statistics indefinitely. Default is 180. Minimum is 0. Maximum is 366. - DetailedStatisticsExpiryTime. Number of days that the Model repository saves per-minute statistics. If purging is disabled, then Model repository saves the statistics indefinitely. Default is 14. Minimum is 1. Maximum is 14.

UpdateNamespace

Updates an LDAP security domain with the filters provided for the user and group. Updates the LDAP security domain if the Informatica domain uses LDAP or Kerberos authentication.

The infacmd isp UpdateNamespace command uses the following syntax:

```
UpdateNamespace
 <-DomainName|-dn> domain_name
 <-UserName|-un> user_name
 <-Password|-pd> password
 [<-SecurityDomain|-sdn> security_domain]
 [<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NameSpace|-ns> namespace
[<-UserSearchBase|-usb> usersearchbase]
[<-UserFilter|-uf> userfilter]
[<-GroupSearchBase|-gsb> groupsearchbase]
[<-GroupFilter|-gf> groupfilter]
[<-LDAPHostConfigurationName|-lcn> LDAP_host_configuration_name]
```

The following table describes infacmd isp UpdateNamespace options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd tries to establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If you do not specify the environment variable, the default value used is 180 seconds.
-NameSpace -ns	namespace	Required. Name of the LDAP or Kerberos security domain. The name is not case sensitive and must be unique within the domain. The name cannot contain spaces or any of the following special characters: , + / < > @ ; \ % ? The name cannot exceed 128 characters. The name can contain an ASCII space character except for the first and last character. You cannot use any other space characters.
-UserSearchBase -usb	usersearchbasesu	Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The LDAP directory service searches for an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName. The series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.
-UserFilter -uf	userfilter	An LDAP query string that specifies the search criteria to search for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: The filter `(objectclass=*)` searches all objects. The filter `(&(objectClass=user)(!(cn=susan)))` searches all user objects except “susan.” For more information about search filters, see the documentation for the LDAP directory service.
-GroupSearchBase -gsb	groupsearchbase	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
-GroupFilter -gf	groupfilter	An LDAP query string that specifies the criteria for searching for groups in the directory service.
-LDAPHostConfigurationName -lcn	ldapName	Optional. The name of the LDAP configuration associated with the security domain.

UpdateNodeOptions

Updates node general properties such as backup directory, CPU profile, error severity level, service process ports, and resource provision thresholds.

The infacmd isp UpdateNodeOptions command uses the following syntax:

```
UpdateNodeOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-NodeOptions|-no> option_name=value ...]
[<-ResourceProvision|-rp> option_name=value ...]
```

The following table describes infacmd isp UpdateNodeOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Optional. Name of the node whose resource provision thresholds you want to update.
-NodeOptions -no	option_name=value	Optional. The node options you want to update. You can update the following options: - BackupDir. Directory to store repository backup files. - CPUProfile. Ranking of the CPU performance of the node compared to a baseline system. ErrorSeverityLevel. Level of error logging for the node: error, warning, info, trace, debug. - MaxProcessPort. Maximum port number used by service processes on the node. - MinProcessPort. Minimum port number used by service processes on the node. The following example sets MaxProcessPort to 1515: `infacmd UpdateNodeOptions ... -no MaxProcessPort=1515`
-ResourceProvision -rp	option_name=value	Optional. The resource provision thresholds you want to update. You can update the following thresholds: - MaxCPURunQueueLength. The maximum number of runnable threads waiting for CPU resources on the node. - MaxMemoryPercent. The maximum percentage of virtual memory allocated on the node relative to the total physical memory size. - MaxProcesses. The maximum number of Session and Command tasks that can run on each Integration Service running on the node. The following example sets MaxProcesses to 15: `infacmd UpdateNodeOptions ... -rp MaxProcesses=15`

UpdateNodeRole

Updates the role on a node in the domain. You can enable or disable the service role or the compute role on a node.

By default, each node has both the service and compute roles. If a node is assigned to a Data Integration Service grid, you might want to update the node role. Enable only the service role to dedicate the node to running the Data Integration Service process. Enable only the compute role to dedicate the node to running Data Integration Service mappings.

If you update the role on a node assigned to a Data Integration Service or a Data Integration Service grid, you must recycle the Data Integration Service for the changes to take effect.

The infacmd isp UpdateNodeRole command uses the following syntax:

```
UpdateNodeRole
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
[<-EnableServiceRole|-esr> true|false]
[<-EnableComputeRole|-ecr> true|false]
[<-disableComputeRoleMode|-mo> disable_mode]
```

The following table describes infacmd isp UpdateNodeRole options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-NodeName -nn	node_name	Required. Name of the node that you want to update.
-EnableServiceRole -esr	true | false	Optional. Enables the service role on the node. If true, application services can run on the node. If false, application services cannot run on the node. Set to false only if the node is assigned to a Data Integration Service grid and you want to dedicate the node to running mappings. Default is true.
-EnableComputeRole -esr	true | false	Optional. Enables the compute role on the node. If true, the node can perform computations requested by remote application services. If false, the node cannot perform computations requested by remote application services. A node requires the compute role when the Data Integration Service runs jobs on the node. If the Data Integration Service does not run jobs on the node, you can disable the compute role. However, enabling or disabling the compute role does not have a performance impact. Default is true.
-disableComputeRoleMode -mo	disable_mode	Optional. Defines how the compute role is disabled: - Complete. Allows computations to run to completion before disabling the compute role. - Stop. Stops all running computations and then disables the compute role. - Abort. Tries to stop all running computations before aborting them and disabling the compute role. Default is abort.

UpdateOSProfile

Updates properties for an operating system profile in the domain.

Note: To run workflows that use operating system profiles, you must have the operating system profiles option.

The infacmd isp UpdateOSProfile command uses the following syntax:

```
UpdateOSProfile
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-OSProfileName|-on> OSProfile_name
[<-IntegrationServiceProcessOptions|-po> option_name=value ...
[<-DISProcessVariables|-diso> option_name=value ...]
[<-DISEnvironmentVariables|-dise> name=value ...]
[<-HadoopImpersonationProperties|-hipr> hadoop_impersonation_properties]
[<-HadoopImpersonationUser|-hu> hadoop_impersonation_user]
[<-UseLoggedInUserAsProxy|-ip> use_logged_in_user_as_proxy]
[<-ProductExtensionName|-pe> product_extension_name]
[<-ProductOptions|-o> optionGroupName.optionName=Value ...]
```

The following table describes infacmd isp UpdateOSProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-OSProfileName -on	OSProfile_name	Required. Name of the operating system profile.
-IntegrationServiceProcessOptions -po	option_name=value	Optional. Service process properties that define how the PowerCenter Integration Service runs.
-EnvironmentVariables -ev	name=value	Optional. Name and value of environment variables used by the PowerCenter Integration Service at run time.
-DISProcessVariables -diso	option_name=value	Optional. Service process properties that define how the Data Integration Service runs.
-DISEnvironmentVariables -dise	name=value	Optional. Name and value of environment variables used by the Data Integration Service at run time.

Option	Argument	Description
-HadoopImpersonationProperties -hipr	hadoop_impersonation_properties	Optional. Indicates whether the Data Integration Service uses the Hadoop impersonation user to run mappings, workflows, and profiling jobs in a Hadoop environment. Valid values are true or false.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Enter a user name for the Data Integration Service to impersonate when it runs jobs in a Hadoop environment.
-UseLoggedInUserAsProxy -ip	use_logged_in_user_as_proxy	Optional. Indicates whether to use the logged in user as the Hadoop impersonation user. Valid values are true or false.
-ProductExtensionName -pe	product_extension_name	Optional. Reserved for future use.
-ProductOptions -o	optionGroupName.optionName=Value	Required. Name and value of each option that you set. Use the option to create a flat file cache directory that the operating system profile can use. For example, the following command sets the cache directory to $PMRootDir/OSPCache: `infacmd isp createOSProfile ... -o 'runTimeVariables.flatFileCacheDirectory'="$PMRootDir/OSPCache"`

UpdateRepositoryService

Updates or creates service options for the PowerCenter Repository Service.

For example, you can update the PowerCenter Repository Service operating mode, which you can set to normal or exclusive. Normal mode allows multiple users to access the PowerCenter Repository Service and update repository contents. Exclusive mode allows a single user to access the PowerCenter Repository Service and update repository contents. Set the operating mode to exclusive when you perform administrative tasks that require a single user to log in and update the configuration. To update the PowerCenter Repository Service operating mode, disable the PowerCenter Repository Service, update the operating mode, and then re-enable the PowerCenter Repository Service.

The infacmd isp UpdateRepositoryService command uses the following syntax:

```
UpdateRepositoryService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

```
[<-NodeName|-nn> node_name]

[<-BackupNodes|-bn> node1 node2 ...]

[<-ServiceOptions|-so> option_name=value ...]
```

The following table describes infacmd isp UpdateRepositoryService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the PowerCenter Repository Service you want to update. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-NodeName -nn	node_name	Optional. Name of the node where the PowerCenter Repository Service process runs. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node.
-BackupNodes -bn	node1 node2 ...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-ServiceOptions -so	option_name=value	Required. Service properties that define how the PowerCenter Repository Service runs.

Repository Service Options (-so)

Enter Repository Service options in the following format:

```
infacmd CreateRepositoryService ... -so option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Repository Service options:

Option	Description
AllowWritesWithRACaching	Optional. Uses PowerCenter Client tools to modify metadata in the repository when repagent caching is enabled. Default is Yes.
CheckinCommentsRequired	Optional. Requires users to add comments when checking in repository objects. Default is Yes. To apply changes, restart the PowerCenter Repository Service.
CodePage	Required. Code page description for the database. To enter a code page description that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
ConnectString	Required. Database connection string specified during PowerCenter Repository Service setup. To apply changes, restart the PowerCenter Repository Service.
DBPassword	Required. Repository database password corresponding to the database user. You can set a password with the -so option or the environment variable INFA_DEFAULT_DATABASE_PASSWORD. If you set a password with both methods, the password set with the -so option takes precedence. To apply changes, restart the PowerCenter Repository Service.
DBPoolExpiryThreshold	Optional. The minimum number of idle database connections allowed by the PowerCenter Repository Service. For example, if there are 20 idle connections, and you set this threshold to 5, the PowerCenter Repository Service closes no more than 15 connections. Minimum is 3. Default is 5.
DBPoolExpiryTimeout	Optional. The interval, in seconds, at which the PowerCenter Repository Service checks for idle database connections. If a connection is idle for a period of time greater than this value, the PowerCenter Repository Service can close the connection. Minimum is 300. Maximum is 2,592,000 (30 days). Default is 3,600 (1 hour).

Option	Description
DBUser	Required. Account for the database containing the repository. To apply changes, restart the PowerCenter Repository Service.
DatabaseArrayOperationSize	Optional. Number of rows to fetch each time an array database operation is issued, such as insert or fetch. Default is 100. To apply changes, restart the PowerCenter Repository Service.
DatabaseConnectionTimeout	Optional. Amount of time in seconds that the PowerCenter Repository Service attempts to establish a connection to the database management system. Default is 180.
DatabasePoolSize	Optional. Maximum number of connections to the repository database that the PowerCenter Repository Service can establish. Minimum is 20. Default is 500.
DatabaseType	Required. Type of database that stores the repository metadata. To apply changes, restart the PowerCenter Repository Service.
EnableRepAgentCaching	Optional. Enables the repository agent caching feature. Default is Yes.
ErrorSeverityLevel	Optional. Minimum level of error messages written to the PowerCenter Repository Service log: - Fatal - Error Warning - Info - Trace - Debug Default is Info.
HeartBeatInterval	Optional. Interval at which the PowerCenter Repository Service verifies its connections with clients of the service. Default is 60 seconds.
MaxResilienceTimeout	Optional. Maximum amount of time in seconds that the service holds on to resources for resilience purposes. Default is 180.
MaximumConnections	Optional. Maximum number of connections the repository accepts from repository clients. Default is 200.
MaximumLocks	Optional. Maximum number of locks the repository places on metadata objects. Default is 50,000.
OperatingMode	Optional. Mode in which the PowerCenter Repository Service is running: - Normal - Exclusive Default is Normal. To apply changes, restart the PowerCenter Repository Service.

Option	Description
OptimizeDatabaseSchema	Optional. Optimizes the repository database schema when you create repository contents or back up and restore an IBM DB2 or Microsoft SQL Server repository. When enabled, the PowerCenter Repository Service tries to create repository tables that contain Varchar columns with a precision of 2000 instead of CLOB columns. Use Varchar columns to increase repository performance. When you use Varchar columns, you reduce disk input and output, and the database can cache the columns. To use this option, verify the page size requirements for the following repository databases: - IBM DB2. Database page size 4 KB or greater. At least one temporary tablespace with page size 16 KB or greater. - Microsoft SQL Server. Database page size 8 KB or greater. Default is disabled.
PreserveMXData	Optional. Preserves MX data for prior versions of mappings. Default is disabled.
RACacheCapacity	Optional. Number of objects that the cache can contain when repository agent caching is enabled. Default is 10,000.
SecurityAuditTrail	Optional. Tracks changes made to users, groups, privileges, and permissions. Default is No.
ServiceResilienceTimeout	Optional. Amount of time in seconds that the service tries to establish or reestablish a connection to another service. Default is 180. To apply changes, restart the PowerCenter Repository Service.
TableOwnerName	Optional. Name of the owner of the repository tables for an IBM DB2 repository.
TablespaceName	Optional. Tablespace name for IBM DB2 repositories. To apply changes, restart the PowerCenter Repository Service.
TrustedConnection	Optional. Uses Windows authentication to access the Microsoft SQL Server database. Default is No. To apply changes, restart the PowerCenter Repository Service.

UpdateSAPBWService

Updates the service and service process options for the SAP BW Service.

The infacmd isp UpdateSAPBWService command uses the following syntax:

```
UpdateSAPBWService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ServiceName|-sn> service_name
[<-NodeName|-nn> node_name]
[<-ServiceOptions|-so> option_name=value ...]
[<-ServiceProcessOptions|-po> option_name=value ...]
```

The following table describes infacmd isp UpdateSAPBWService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Option	Argument	Description
-ServiceName -sn	service_name	Required.SAP BW Service name. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Optional. Name of the node where the SAP BW Service process runs. If the PowerCenter environment is configured for high availability, this option specifies the name of the primary node.
-ServiceOptions -so	option_name=value	Optional. Service properties that define how the SAP BW Service runs.
-ServiceProcessOptions -po	option_name=value	Optional. Service process properties that define how the SAP BW Service process runs.

UpdateServiceLevel

Updates service level properties. You can update the dispatch priority and maximum dispatch wait time.

The infacmd isp UpdateServiceLevel command uses the following syntax:

```
UpdateServiceLevel
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceLevelName|-ln> service_level_name
<-ServiceLevel|-sl> option_name=value ...
```

The following table describes infacmd isp UpdateServiceLevel options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceLevelName -ln	service_level_name	Required. Name of the service level you want to update.
-ServiceLevel -sl	option_name=value	Required. The service level properties you want to update. You can update the following properties: - DispatchPriority. The initial priority for dispatch. Smaller numbers have higher priority. Priority 1 is the highest priority. - MaxDispatchWaitTime. The amount of time in seconds that can elapse before the Load Balancer escalates the dispatch priority for a task to the highest priority.

UpdateServiceProcess

Updates the values of the PowerCenter Integration Service process options.

The infacmd isp UpdateServiceProcess command uses the following syntax:

```
UpdateServiceProcess

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

<-ServiceProcessOptions|-po> option_name=value
[<-ProcessEnvironmentVariables|-ev> option_name=value ...]
```

The following table describes infacmd isp UpdateServiceProcess options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-NodeName -nn	node_name	Required. Name of the node where you want to update configuration information.
-ServiceProcessOptions -po	option_name=value	Name and new values of the options whose values you want to update. You can specify multiple option_name=value pairs. You can use a process variable in the value. For example, the following command sets the cache directory to “$PMRootDir/NewCache” and the reject file directory to “$PMRootDir/NewBadFiles”: `infacmd UpdateServiceProcess ... -po $PMCacheDir=$PMRootDir/NewCache $PMBadFileDir=$PMRootDir/NewBadFiles` Required if you do not specify ProcessEnvironmentVariables.
-ProcessEnvironmentVariables -ev	option_name=value	Environment variables for the service process. You can specify multiple environment variables. For example, the following command adds or updates the JAVA_HOME directory to "$HOME/java" and the INFA_HOME directory to “$HOME/Informatica/9.0.1/install” for the specified service process: `infacmd ProcessEnvironmentVariables ... -ev JAVA_HOME=$HOME/java INFA_HOME=$HOME/Informatica/9.0.1/install` Required if you do not specify ServiceProcessOptions.

UpdateSMTPOptions

Updates the domain SMTP configuration. The SMTP configuration is used to send domain alerts and scorecard notifications.

After you configure the SMTP settings, you must subscribe the user to alerts using the AddAlertUser command.

The infacmd isp UpdateSMTPOptions command uses the following syntax:

```
UpdateSMTPOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SMTPAddress|-sa> smtp_server_address
[<-SMTPUsername|-su> user_name]
[<-SMTPPassword|-sp> password]
[<-SMTPSenderAddress|-ss> sender_email_address]
[<-ResetSMTPUserNameAndPassword|-re> reset_smtp_username_password]
[<-TLSEnabled|-tls> is_tls_enabled]
```

The following table describes infacmd isp UpdateSMTPOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. Security domain is case sensitive. Default is Native.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-SMTPAddress -sa	SMTP_server_address	Required. The host name and port number for the SMTP outbound mail server. Enter this information in the following format: *host_name:port_number*
-SMTPUserName -su	user_name	Optional. The user name for authentication upon sending if required by the outbound mail server.
-SMTPPassword -sp	password	User password for authentication upon sending if required by the outbound mail server. You can set a password with the -sp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -sp option takes precedence.
-SMTPSenderAddress -ss	sender_email_address	Optional. Email address the Service Manager uses to send notification emails. If you leave this field blank, the Service Manager uses the default “Administrator@<host>” as the sender.
-ResetSMTPUserNameAndPassword -re	reset_smtp_username_password	Optional. Configure the settings for the SMTP outbound mail server to enable a user to subscribe to alerts.
-TLSEnabled -tls	is_tls_enabled	Optional. Indicates that the SMTP server uses the TLS protocol. If true, enter the TLS port number for the SMTP server port property. Enter `true` or `false`. Default is false.

Related Topics:

- "AddAlertUser" on page 328

UpdateWSHubService

Updates a Web Services Hub in the domain.

The infacmd isp UpdateWSHubService command uses the following syntax:

```
UpdateWSHubService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
[<-NodeName|-nn> node_name]
[<-ServiceOptions|-so> option_name=value ...]
```

The following table describes infacmd isp UpdateWSHubService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the Web Services Hub you want to update.
-NodeName -nn	node_name	Optional. Name of the node where the Web Services Hub process runs.
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the Web Services Hub runs.

UpgradeGatewayNodeMetadata

Updates metadata for a gateway node on the current machine. Before you update the gateway node, run the infacmd isp ShutDownNode command to shut down the node.

The UpgradeGatewayNodeMetadata command uses the following syntax:

```
UpdateGatewayNode
[<-LogServiceDirectory|-ld> log_service_directory (used for GatewayNode only)]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-HttpsPort|-hs> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePass|-kp> keystore_password]
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
```

```
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
<-PreviousInfaHome|-ph> previous_infa_home
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* UpgradeGatewayNodeMetadata options and arguments:

Option	Description
-LogServiceDirectory -ld	Required. Shared directory path used by the Log Manager to store log event files. Verify that -ld does not match or contain the specified -sld value.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Verify that -ld does not match or contain the specified -sld value. Default is <INFA_home>/logs.
-HttpsPort -hs	Optional. Port number that the node uses for communication between the Administrator tool and the Service Manager. Set this port number if you want to configure HTTPS for a node. To disable HTTPS support for a node, set this port number to zero.
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Connection string used to connect to the domain configuration database. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in quotes.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql

Option	Description
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-PreviousInfaHome -ph	Required. Path to the previous Informatica home directory.
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.
-DatabaseTruststoreLocation -dbtl	Optional. Path and file name of the truststore file for the gateway node.

validateFeature

Validates that the feature in the specified plug-in file is registered in the domain.

The infacmd isp validateFeature command uses the following syntax:

```
validateFeature
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-FeatureFilename|-ff> feature_filename
```

The following table describes infacmd isp validateFeature options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date.The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-FeatureFilename -ff	feature_filename	Required. Path and file name of the plug-in xml file of the registered feature that you want to validate.

Version

Displays the PowerCenter version and Informatica trademark and copyright information.

The version command uses the following syntax:

```
infacmd version
```

CHAPTER 22

infacmd ldm Command Reference

This chapter includes the following topics:

BackupContents

The Catalog Service takes backup of the MongoDB, Solr, PostgresSQL, and scanner staging data.

Before you backup the Catalog Service, you need to set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`. Default location is `$INFA_HOME/services/shared/security`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`. Default location is `$INFA_HOME/services/shared/security`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.

.

Note: See the sample command to encrypt password: $INFA HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

Note the following points before you run this command:

- When the Catalog Service is up and running and the backup is in progress, you can perform the read operation in the Catalog Service.
- If Solr is deployed on multiple nodes, the cluster shared file path system should be common for all the Solr hosts, the cluster shared path system should be NFS mount, and gateway user ID should be same for all the Solr hosts.
- The BackupContents command requires the INFA_KEYSTORE and INFA_KEYSTORE_PASSWORD environment variables to connect to Solr and MongoDB services of Informatica Cluster Service.
- Set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on both SSL and non-SSL enabled Informatica domain.
- If Solr is installed on multi-node setup, you need to configure the `ClusterSharedFilesystemPath` option in Informatica Cluster Service to restore the Solr.

The infacmd ldm BackupContents command uses the following syntax:

```
BackupContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-OutputFilename|-of> output_file_name

[<-Force|-fr> force

[<-StoreType|-st> Comma separated values of backup store type to be taken. Accepted
types are Asset,Orchestration,Search,Similarity. Example value:
'Asset,Search,Orchestration' or simply 'Search'). By default, it will take backup for
all stores.]
```

The following table describes infacmd ldm BackupContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Catalog Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-OutputFilename -of	output_file_name	Required. Complete path and filename of the backup ZIP file on the local machine. The backup command creates the zip file name.

Option	Argument	Description
-Force -fr	force	Optional. Forcefully takes backup and overwrites the existing backup.
-StoreType -st	Data store type values: - Asset - Orchestration - Search - Similarity	Optional. Provide the required data store that you want to back up or a comma-separated list of data stores that you want to back up. Based on the issues you want to troubleshoot, you can back up the required data stores instead of taking a complete backup of the catalog. You can back up the following data stores in the catalog: - Asset - Orchestration - Search - Similarity You must back up the **Asset**, **Search**, and **Similarity** if you want to view data after you restore data from the backup. **Note:** By default, the command backs up all the data stores in the catalog. See the following samples for more information: - To back up data stores that include Asset, Similarity, Search, and Orchestration, add the arguments to the `-st` option as shown: `-st Asset,Similarity, Search, and Orchestration`.

You can see the status of the backup in the following log file on the node where you run the command: `<Informatica installation directory>/logs/<Node name>/services/CatalogService/<Catalog Service name>/LDMBackup.log`. The maximum file size for each log file is 100 MB. After the maximum file size is reached, a new file is created. The maximum number of log files that are stored is 20. After this limit is reached, the oldest log file is replaced with the latest log file.

The backup file is encrypted using the Advanced Encryption Standard (AES) algorithm.

CreateService

Creates a Catalog Service.

The infacmd ldm CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ModelRepositoryService|-mrs> model_repository_service_name

<-MRSUserName|-mrsun> model_repository_service_user_name

<-MRSPassword|-mrspd> model_repository_service_user_password

[<-MRSSecurityDomain|-mrssdn> model_repository_service_user_security_domain]

[<-HttpPort|-p> port_name]

[<-HttpsPort|-sp> https_port_name]

[<-EnableTls|-tls> enable_tls true|false]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-SSLProtocol|-sslp> ssl_protocol]

<-InfaClusterServiceName|-icsn> infa_cluster_service_name

[<-isEmailEnabled|-iee> is_email_enabled true:false (default false)]

[<-OtherOptions|-oo> other options (specified in format:
[OptionGroupName.OptionName=OptionValue]. Multiple options can be separated by space.
OptionValue should be specified within double quotes if it contains a space.)]

[<-BackupNodes|-bn> node_name1,node_name2,...]

[<-isNotifyChangeEmailEnabled|-cne> is_notify_change_email_enabled true:false (default
false)]

<-EnableDataAssetAnalytics|-ed> Enable Data Asset Analytics(true, false). If you enable
this option, make sure that you configure the following parameters:
DataAssetAnalyticsDBSelect, DataAssetAnalyticsDBUsername, DataAssetAnalyticsDBPassword,
DataAssetAnalyticsDBURL

[<-DataAssetAnalyticsDBSelect|-ddt> Select the database for Data Asset Analytics
(ORACLE, SQLSERVER or POSTGRESQL)]

[<-DataAssetAnalyticsDBUsername|-ddu> Username to access the database]

[<-DataAssetAnalyticsDBPassword|-ddp> Password configured for the username]

[<-DataAssetAnalyticsDBURL|-ddl> Database connection string. Make sure that the
connection string starts with 'jdbc:informatica:']

[<-DataAssetAnalyticsDBSchema|-dds> Database schema name (applicable if you had selected
SQL Server or PostgreSQL as the database type.)]

[<-DataAssetAnalyticsSecureJDBCParameters|-dsjdbcp> Secure JDBC connection parameters]
```

The following table describes infacmd ldm CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Node where you want to run the Catalog Service to run.
-SecurityDomain |-sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ModelRepositoryService -mrs	model_repository_service_name	Required. Model Repository Service name to associate with the Catalog Service.
-MRSUserName -mrsun	model_repository_service_user_name	Required if you specify a Model Repository Service. User name to connect to the Model repository. If you enter a user name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-MRSPassword -mrspd	model_repository_service_user_password	Required if you specify a Model Repository Service. User password for the Model Repository Service.
-MRSSecurityDomain -mrssdn	model_repository_service_user_security_domain	Required if you use LDAP authentication. Name of the security domain to which the Administrator user belongs.
-HttpPort -p	port_name	Required. A unique HTTP port number used for each Catalog Service process. The default port number is 9085.
-HttpsPort -sp	https_port_name	Required if you enable Transport Layer Security. Port number for the HTTPS connection.

Option	Argument	Description
-EnableTls -tls	enable_tls	Select this option to enable Transport Layer Security.
-KeystoreFile -kf	keystore_file_location	Required if you select Enable Transport layer Security. Path and file name of the keystore file. The keystore file contains the keys and certificates required if you use the SSL security protocol with Catalog Administrator.
-KeystorePassword -kp	keystore_password	Required if you select Enable Transport layer Security. The password for the keystore file.
-SSLProtocol -sslp	ssl_protocol	Optional. Secure Sockets Layer protocol to use.
-InfaClusterServiceName -icsn	Infa_cluster_service_name	Required. Name of the Informatica Cluster Service.
-isEmailEnabled -iee	is_email_enabled	Optional. Specify True if you want to enable email notification. Default is False.
-OtherOptions -oo	other options	Optional. Enter name-value pair separated by spaces. To enter an option value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-isNotifyChangeEmailEnabled -cne	is_notify_change_email_enabled	Optional. Specify True if you want to enable asset change notifications. Default is False.
-EnableDataAssetAnalytics -ed	Enable Data Asset Analytics(true, false)	Required. Specify True if you want to enable Data Asset Analytics with Enterprise Data Catalog. If you enable this option, make sure that you configure the following parameters: - DataAssetAnalyticsDBSelect - DataAssetAnalyticsDBUsername - DataAssetAnalyticsDBPassword - DataAssetAnalyticsDBURL

Option	Argument	Description
-DataAssetAnalyticsDBSelect -ddt	Select the database for Data Asset Analytics (ORACLE, SQLSERVER or POSTGRESQL)	Required if the `EnableDataAssetAnalytics` option value is set to true. Applies to the following databases: - Oracle - SQL Server - PostgreSQL
-DataAssetAnalyticsDBUsername -ddu	Username to access the database	Required if the `EnableDataAssetAnalytics` option value is set to true. Specify the username to access the database for Data Asset Analytics.
DataAssetAnalyticsDBPassword -ddp	Password configured for the username	Required if the `EnableDataAssetAnalytics` option value is set to true. Specify the password to access the database for Data Asset Analytics.
DataAssetAnalyticsDBURL -ddl	Database connection string	Required if the `EnableDataAssetAnalytics` option value is set to true. Specify the database connection string. Make sure that the connection string starts with `'jdbc:informatica:'`
DataAssetAnalyticsDBSchema -dds	Database schema name	Optional. Specify the database schema name. Applicable if you had selected SQL Server or PostgreSQL as the database type.
DataAssetAnalyticsSecureJDBCParameters -dsjdbcp	Secure JDBC connection parameters	Optional. If the database for Data Asset Analytics is secured with the SSL protocol, you must enter the secure database parameters. Enter the parameters in the form of key-value pairs separated by a semi-colon. For example: `param1=value1;param2=value2`

ListServiceOptions

Lists service options for the Catalog Service.

The infacmd ldm ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ldm ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Catalog Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists service process options for the Catalog Administrator process.

The infacmd ldm ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
```

The following table describes infacmd ldm ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-NodeName -nn	node_name	Required. Required. Name of the node where the service process runs.

migrateContents

Migrates content. Provide the input directory from where you want to migrate or verify the content. Run the migrateContents command when the Catalog Service, Informatica Cluster Service, and the required stores are enabled. Before you migrate the catalog data, you must set the following environment variables

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`. Default location is `$INFA_HOME/services/shared/security`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`. Default location is `$INFA_HOME/services/shared/security`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".` This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.

Note: See the sample command to encrypt password: $INFA_HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=

- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

Note the following points before you run this command:

- The migrateContents command requires the INFA_KEYSTORE and INFA_KEYSTORE_PASSWORD environment variables to connect to Solr and MongoDB services of Informatica Cluster Service.
- The administrator users or users who are part of the administrator group can run the migrateContents command.
- To run the migrateContents command from the backup node for the Catalog Service, you must enable passwordless SSH between the backup node and all nodes in the cluster.
- Set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on both SSL and non-SSL enabled Informatica domain.

The infacmd ldm migrateContents command uses the following syntax:

```
LDM migrateContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-InputDirectory|-id> full path to backup directory. For eg. - /backup/export

[<-Resume> This is to resume migrating contents from the last checkpoint available. If
set to false, migration will start from scratch.]

[<-Force> This is to forcefully launch another migration process ignoring the lock held
by previous process.]

[<-Verify> This is to verify restored data after migration is complete.]
```

The following table describes infacmd ldm migrateContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence. The domain name is case sensitive.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Catalog Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-InputDirectory -id	Input-directory	Full path to the backup directory. For example, `- /backup/export`
-Resume	resume	Use this option to resume the migrating contents from the last available checkpoint. If set false as the value, the migration will start from the beginning.
-Force	force	Use this option to force launch another migration process by ignoring the lock held by the previous process.
-Verify	verify	Use this option to verify restored data after migration is complete.

publishArchive

Creates a resource in offline mode and runs the scan.

The infacmd ldm publishArchive command uses the following syntax:

```
publishArchive
<-DomainName|-dn> Fully qualified domain name
<-UserName|-un> user_name
<-Password|-pd> The Encryped user password to access the ISP
<-ServiceName|-sn> Name of the Catalog Service
<-ResourceName|-rn> Name of the resource
[<-SecurityDomain|-sd> Name of the security domain]
<-DomainHost|-dh> Name of the host machine where the domain runs
<-DomainPort|-dp> Port number of the domain
[<-DomainSslEnabled|-dse> is domain SSL enabled]
[<-SslLocation|-ts> Path to the truststore]
[<-SslPassword|-tsp> Password to access the truststore]
<-ArchiveFilePath|-arf> Path to the metadata archive file
```

```
[<-Verbose|-v> Verbose]
[<-WaitToCatalog|-w> Wait for the metadata ingestion to catalog to complete]
[<-Force|-f> Force resource creation or update]
```

The following table describes infacmd ldm CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-ResourceName -rn	Name of the resource	Required. Name of the resource. The name cannot exceed 79 characters, have leading or trailing spaces, or contains carriage returns, tabs, or the following characters: \ / * ? < > " | $
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-DomainHost -dh	Domain host name	Required. Name of the host machine where the domain runs.
-DomainPort -dp	Domain port number	Required. The port number of the domain.

Option	Argument	Description
-DomainSslEnabled -dse	is_Domain_SSL_Enabled	Optional. Specify true to enable SSL domain. Default is False.
-SslLocation -ts	-	Optional. Path to the truststore.
-SslPassword -tsp	-	Optional. Password to access the truststore.
-ArchiveFilePath -arf	-	Required. Path to the metadata archive file.
-Verbose -v	Verbose	Optional. Displays or saves purge information in verbose mode. Verbose mode provides detailed information about object versions, including repository name, folder name, version number, and status. You can use the -b option with -o and -p.
-WaitToCatalog -w	-	Optional. Waits for the metadata ingestion to complete into the catalog.
-Force -f	-	Optional. Creates or updates the resource.

removeDeletedMigratedResources

Retrieves the list of deleted resources migrated by the export.jar utility and removes the deleted resources from the catalog.

When you use the export.jar utility to back up catalog data as part of the upgrade from version 10.4 or 10.4.1, certain deleted resources are backed up. After you migrate the catalog data using the infacmd ldm migrateContents command, the deleted resources might appear in the catalog.
Run the removeDeletedMigratedResources command with the -generate option to generate a text file that contains the list of deleted resources. Review the list of deleted resources, and then run the command again with the -delete option to remove the deleted resources.

Note: The removeDeletedMigratedResources command is available in Enterprise Data Catalog version 10.5.2.0.3 and later versions.

The command uses the following syntax:

```
removeDeletedMigratedResources

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-SecurityDomain|-sdn> security_domain

<-generate|-delete>
```

The following table describes the options and arguments for the infacmd ldm removeDeletedMigratedResources command:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
<-generate|-delete>	-	Required. Run the command with the -generate option to generate a text file that contains the list of deleted resources for review. A text file Unwantedresources.txt is generated and stored at the following location: `<Informatica installation directory>/logs/<Node>/services/CatalogService/CS_App/deletedResources` Run the command with the -delete option to remove the deleted resources listed in the text file that is generated.

restoreContents

Restores the catalog data.

Before you restore the catalog data, you need set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`. Default location is `$INFA_HOME/services/shared/security`.

- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`. Default location is `$INFA_HOME/services/shared/security`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA=="`.
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI=="`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.

Note: See the sample command to encrypt password: $INFA_HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

Note the following points before you run this command:

- The restoreContents command requires the INFA_KEYSTORE and INFA_KEYSTORE_PASSWORD environment variables to connect to Solr and MongoDB services of Informatica Cluster Service.
- You should not use the restoreContents command to restore one node backup in multinode setup. The constraint applies to the SEARCH store restore option.
- Set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on both SSL and non-SSL enabled Informatica domain.
- If Solr is installed on multi-node setup, you need to configure the `ClusterSharedFilesystemPath` option in Informatica Cluster Service to restore the Solr.

You cannot use catalog data from the current version to restore data for a previous version. However, if you have applied a cumulative patch release or a service pack, you can use the existing catalog data to restore data for a previous version.

You must verify that the base versions are the same for both the existing and previous versions.

The infacmd ldm restoreContents command uses the following syntax:

```
 restoreContents

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-InputFileName|-if> input_file_name (Complete path of backup ZIP file on local machine.
The content of ZIP file will be copied to cluster.)

[<-Force|-fr> force(This is to forcefully clean the existing contents of cluster where
data is to be restored and restore the backup data from scratch)]
```

The following table describes infacmd ldm restoreContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-InputFileName -if	input_file_name	Required. Complete path of backup .zip file on the Catalog Service host.
-Force -fr	force	Optional. Use this option to forcefully clean the existing contents of the Informatica cluster where data is to be restored and restore the backup data from scratch. If the backup does not contain the SEARCH store, you must recycle the Informatica Cluster Service and then re-index the Catalog Service to populate the data for Apache Solr.

Effective in Enterprise Data Catalog version 10.5.1.1, you can see the status of the restore operation in the following log file on the node where you run the command: `<Informatica installation directory>/logs/<Node name>/services/CatalogService/<Catalog Service name>/LDMRestore.log`. The maximum file size for each log file is 100 MB. After the maximum file size is reached, a new file is created. The maximum number of log files that are stored is 20. After this limit is reached, the oldest log file is replaced with the latest log file.

UpdateServiceOptions

Updates options for the Catalog Service. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd ldm UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-Options|-o> options

[<-PrimaryNode|-nn> node_name]

[<-BackupNodes|-bn> node_name1,node_name2,...]
```

The following table describes infacmd ldm UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Catalog Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description

-Options
-o
	options	Optional. Enter name-value pair separated by spaces.
		If you applied service pack 10.5.1.1 or any later version, you can configure the SSL protocol for the Catalog Service to TLS 1.1 or TLS 1.2 using the `GeneralOptions.SSLProtocol` option. Specify any one of the following values:
		- TLSv1.1
		- TLSv1.2
		You can update the following options related to Data Asset Analytics:
		- `DAARepository.EnableDataAssetAnalytics`: Specify `True` to enable Data Asset Analytics.
		- `DAARepository.DataAssetAnalyticsDBSelect`:Specify any one of the following databases:
		  - Oracle
		  - SQL Server
		  - PostgreSQL
		- `DAARepository.DataAssetAnalyticsDBUsername`: Specify the username to access the Data Asset Analytics database.
		- `DAARepository.DataAssetAnalyticsDBPassword`: Specify the password to access the Data Asset Analytics database.
		- `DAARepository.DataAssetAnalyticsDBURL`: Specify the database connection string.
		- `DAARepository.DataAssetAnalyticsDBSchema`: Specify the database schema name.
		- `DAARepository.DataAssetAnalyticsSecureJDBCParameters`: Specify the JDBC parameters. For example, `param1=value1;param2=value2`

-PrimaryNode -nn	node_name	Optional. If you want to configure high availability for Enterprise Data Catalog, specify the primary node name.
-BackupNodes -bn	node_names	Optional, If you want to configure high availability for Enterprise Data Catalog, specify a list of comma-separated backup node names.

UpdateServiceProcessOptions

Updates process options for the Catalog Service. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd ldm UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

The following table describes infacmd ldm UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Name of the node where the service process runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Catalog Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter name-value pair separated by spaces.

upgrade

Upgrades the Catalog Service. If the Catalog Service is SSL-enabled, before upgrade, you need to set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`. Default location is `$INFA_HOME/services/shared/security`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`. Default location is `$INFA_HOME/services/shared/security`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".` This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.

Note: See the sample command to encrypt password: $INFA HOME/server/bin/pmpasswd <password>

For example,

- export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
- export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
- export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
- export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security

Note: Set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on both SSL and non-SSL enabled Informatica domain.

The infacmd ldm upgrade command uses the following syntax:

```
 upgrade
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd ldm upgrade options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

upgradePropagationStageFrom105

The upgradePropagationStageFrom105 command modifies the `term_association_results.csv` in MongoDB for all resources present in the 10.5 backup file.

Run this command if the data domain propagation results are missing after you upgrade from version 10.5. If the Catalog Service is SSL-enabled, before upgrade, you need to set the following environment variables:

- INFA_TRUSTSTORE. See the following sample command to set the variable: `export INFA_TRUSTSTORE=<Location of the Informatica truststore file>`. Default location is `$INFA_HOME/services/shared/security`.
- INFA_KEYSTORE. See the following sample command to set the variable: `export INFA_KEYSTORE=<Location of the keystore file>`. Default location is `$INFA_HOME/services/shared/security`. This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.
- Encrypted INFA_TRUSTSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_TRUSTSTORE_PASSWORD="84Ve/soUbpQ/Aae5uGKXQA==".`
- Encrypted INFA_KEYSTORE_PASSWORD. Encrypt the password that you set. See the following sample command to set the encrypted password: `export INFA_KEYSTORE_PASSWORD="6cDE/ItyUL/Rtui9nhVRI==".` This variable is required only if you used custom SSL configuration for the Informatica domain. For default SSL and non-SSL configurations, you must unset the variable.

Note: See the sample command to encrypt password: $INFA HOME/server/bin/pmpasswd <password>

For example,

```
export INFA_KEYSTORE_PASSWORD=hQDP8O8tfwxRSwbeANEptl4AIQqJcSj9ZMDkVK+9S+Y=
export INFA_TRUSTSTORE_PASSWORD=hx/nRWisSjnQ0zEGV3N7j1FCGFOm5RfisQxKTdf5f8Y=
export INFA_TRUSTSTORE=/data/Informatica/LDM1051/services/shared/security/
export INFA_KEYSTORE=/data/Informatica/LDM1051/services/shared/security
```

Note: Set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on both SSL and non-SSL enabled Informatica domain.

The infacmd ldm upgradePropagationStageFrom105 command uses the following syntax:

```
 upgradePropagationStageFrom105

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-SecurityDomain|-sdn> security_domain]

<-InputDirectory|-id> Full path to the 10.5 backup zip file

<-Force|-force> Forcefully launch the upgradePropagationStageFrom105 process
```

The following table describes infacmd ldm upgradePropagationStageFrom105 options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Catalog Service name.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-InputDirectory -id	Input-directory	Required. Full path to the 10.5 backup zip file.
-force	true	Required. Forcefully launches the upgradePropagationStageFrom105 process. You can set the force option as true to forcefully launch the upgradePropagationStageFrom105 process by ignoring the lock held by the previous process.

CHAPTER 23

infacmd mas Command Reference

This chapter includes the following topics:

CreateService

Creates a Metadata Access Service. The Metadata Access Service is an application service that allows the Developer tool to access Hadoop connection information to import and preview metadata.

The infacmd mas CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
<-HTTPProtocolType|-hp> HTTPProtocolType
[<-HTTPPort|-pt> HTTPPort]
[<-HTTPSPort|-spt> HTTPSPort]
[<-HadoopServicePrincipalName|-hpn> HadoopServicePrincipalName]
[<-HadoopKeyTab|-hkt> HadoopKeyTab]
[<-ServiceDescription|-sd> ServiceDescription]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

```
[<-FolderPath|-fp> FolderPath]
[<-BackupNodes|-bn> BackupNodes]
[<-KeyStoreFile|-kf> KeyStoreFile]
[<-KeystorePassword|-kp> KeystorePassword]
[<-TruststoreFile|-tf> TruststoreFile]
[<-TruststorePassword|-tp> TruststorePassword]
[<-SecurityDomain|-sdn> SecurityDomain]
[<-SSLProtocol|-sp> SSLProtocol]
[<-loggedInUserAsImpersonationUser|-uiu> UseLoggedInUserAsImpersonationUser]
[<-enableOSProfile|-osp> EnableOSProfile]
```

The following table describes infacmd mas CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Node where the Metadata Access Service runs. You can run the Data Integration Service only on a node.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Metadata Access Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-HTTPProtocolType -hp	http_protocol_type	Security protocol that the Metadata Access Service uses. Enter one of the following values: - HTTP. Requests to the service must use an HTTP URL. - HTTPS. Requests to the service must use an HTTPS URL. When you set the HTTP protocol type to HTTPS, you enable Transport Layer Security (TLS) for the service. Default is HTTP.
-HTTPPort -pt	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Metadata Access Service process. After you create the service, you can define different port numbers for each Metadata Access Service process. Default is 7080. The Metadata Access Service uses consecutive port numbers to connect to multiple Hadoop distributions.
-HTTPSPort -spt	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each Metadata Access Service process. After you create the service, you can define different port numbers for each Metadata Access Service process. The Metadata Access Service uses consecutive port numbers to connect to multiple Hadoop distributions.
-HadoopServicePrincipalName -hpn	hadoop_spn	Service Principal Name (SPN) of the Metadata Access Service to connect to a Hadoop cluster that uses Kerberos authentication. Not applicable for the MapR distribution.
-HadoopKeyTab -hkt	keytab_file_path	The file path to the Kerberos keytab file on the machine on which the Metadata Access Service runs. Not applicable for the MapR distribution.
-ServiceDescription -sd	service_description	Optional. Service description.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the Metadata Access Service. Must be in the following format: `/parent_folder/child_folder` Default is “/” (the domain).
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

Option	Argument	Description
-KeystoreFile -kf	keystore_file_location	Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the Metadata Access Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Password for the keystore file.
-TruststoreFile -tf	trust_store_file	Required when the domain is SSL- enabled. Domain truststore file location in the cluster.
-TruststorePassword -tp	trust_store_password	Required when the domain is SSL- enabled. Truststore domain password.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-SSLProtocol -sp	ssl_protocol	Optional. Secure Sockets Layer protocol to use.
-HadoopImpersonationUser -hu	hadoop_impersonation_user	Optional. Enter a user name for the Metadata Access Service to impersonate when it connects to a Hadoop environment.
-loggedInUserAsImpersonationUser -uiu	use_logged_in_user_as_proxy	Required if the Hadoop cluster uses Kerberos authentication. Hadoop impersonation user. The user name that the Metadata Access Service impersonates to import metadata from the Hadoop environment at design time.
-enableOSProfile -osp	enable_OS_profile	Indicates that the Metadata Access Service can use operating system profiles for metadata preview. Default is false.

ListServiceOptions

Lists the properties for a Metadata Access Service.

The infacmd mas ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> DomainName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

The following table describes infacmd mas ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Metadata Access Service.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists the properties of a Metadata Access Service process.

The infacmd mas ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> DomainName
<-NodeName|-nn> NodeName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
```

The following table describes infacmd mas ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Name of node where the service process runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Metadata Access Service.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

UpdateServiceOptions

Updates Metadata Access Service properties. To view current properties run the infacmd mas ListServiceOptions command.

You can change the properties while the service is running, but you must recycle the service for the changed properties to take effect.

The infacmd mas UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> DomainName
<-UserName|-un> Username
<-Password|-pd> Password
<-ServiceName|-sn> ServiceName
[<-SecurityDomain|-sdn> SecurityDomain]
[<-ResilienceTimeout|-re> ResilienceTimeout]
[<-Options|-o> options]
<-PrimaryNode|-nn> PrimaryNodeName
[<-BackupNodes|-bn> node_name1,node_name2,...]
[<-SearchIndexRoot|-si> SearchIndexRoot]
```

The following table describes infacmd mas UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Metadata Access Service that the application is deployed to.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Optional. Enter each option separated by a space. To view options, run the infacmd mas ListServiceOptions command.
-PrimaryNode -nn	node_name	Enter the node where the Metadata Access Service will run. The Metadata Access Service can run only on a node.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-SearchIndexRoot -si	search_index_root	Optional. Changes the directory for the search index. Enter the full path to the directory. Default is the Informatica installation directory.

Metadata Access Service Options

Use the Metadata Access Service options with the infacmd mas UpdateServiceOptions command.

Enter Metadata Access Service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Metadata Access Service options:

Option	Description
ExecutionContextOptions.HadoopDistribution	The Hadoop distribution directory on the Metadata Access Service node. The contents of the Metadata Access Service Hadoop distribution directory must be identical to Hadoop distribution directory on the data nodes. Type `<Informatica Installation directory/Informatica/services/shared/hadoop/[Hadoop_distribution_name]`.
HttpConfigurationOptions.HTTPProtocolType	Security protocol that the Metadata Access Service uses. Enter one of the following values: - HTTP. Requests to the service must use an HTTP URL. - HTTPS. Requests to the service must use an HTTPS URL. When you set the HTTP protocol type to HTTPS, you enable Transport Layer Security (TLS) for the service. Default is HTTP.
MASProperties.EnableOSProfile	Flag to indicate if the Metadata Access Service can use operating system profiles for metadata preview. Default is false.
MASProperties.HadoopKeytab	The file path to the Kerberos keytab file on the machine on which the Metadata Access Service runs. Not applicable for the MapR distribution.
MASProperties.HadoopPrincipal	Service Principal Name (SPN) of the Metadata Access Service to connect to a Hadoop cluster that uses Kerberos authentication. Not applicable for the MapR distribution.
MASProperties.LoggedInUserAsImperUser	Required if the Hadoop cluster uses Kerberos authentication.

UpdateServiceProcessOptions

Updates properties for a Metadata Access Service process. To view current properties, run the infacmd mas ListServiceProcessOptions command.

Enter options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd mas UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions

<-DomainName|-dn> DomainName

<-NodeName|-nn> NodeName

<-UserName|-un> Username

<-Password|-pd> Password

<-ServiceName|-sn> ServiceName
```

```
[<-SecurityDomain|-sdn> SecurityDomain]

[<-ResilienceTimeout|-re> ResilienceTimeout]
```

The following table describes infacmd mas UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
NodeName -nn	node_name	Required. Node where the Metadata Access Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Metadata Access Service.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Metadata Access Service Process Options

Use the Metadata Access Service process options with the infacmd mas UpdateServiceProcessOptions command.

Enter Metadata Access Service process options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Metadata Access Service process options:

Option	Description
GeneralOptions.JVMOptions	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties.
HttpConfigurationOptions.KeyStoreFile	Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the Metadata Access Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
HttpConfigurationOptions.KeyStorePassword	Password for the keystore file.

Option	Description
HttpConfigurationOptions.MaxBacklogRequests	Maximum number of HTTP or HTTPS connections that can wait in a queue for this Metadata Access Service process. Default is 100.
HttpConfigurationOptions.MaxConcurrentRequests	Maximum number of HTTP or HTTPS connections that can be made to this Metadata Access Service process. Minimum is 4. Default is 200.
HttpConfigurationOptions.SSLProtocol	Secure Sockets Layer protocol to use. Default is TLS.
HttpConfigurationOptions.TrustStoreFile	Path and file name of the truststore file that contains authentication certificates trusted by the Metadata Access Service.
HttpConfigurationOptions.TrustStorePassword	Password for the truststore file.

CHAPTER 24

infacmd mi Command Reference

This chapter includes the following topics:

abortRun

Aborts the ingestion mapping jobs in a run instance of a mass ingestion specification. When you abort the ingestion mapping jobs, the command aborts the mappings that perform the ingestion jobs for all source tables that are running or queued. The command does not abort mappings for the ingestion jobs that are completed.

To abort the ingestion mapping jobs, you must specify a RunID. To find the RunID for a run instance, list the specification run instances using infacmd mi listSpecRuns.

The infacmd mi abortRun command uses the following syntax:

```
abortRun

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-runID|-rid> run_id
```

The following table describes infacmd mi abortRun options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-runID -rid	run_id	Required. Run identifier number, or the Run ID, of the mass ingestion specification run instance. To find the RunID for a run instance, list the specification run instances using infacmd mi listSpecRuns.

clearSamlConfig

Clears the Mass Ingestion Service SAML configuration to reset it to the default values.

The infacmd mi clearSamlConfig command uses the following syntax:

```
clearSamlConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
```

The following table describes the infacmd mi clearSamlConfig options and arguments:

Option	Argument	Description
–DomainName –dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.

createService

Creates a Mass Ingestion Service. When you create the Mass Ingestion Service, you must specify a Model Repository Service. The Mass Ingestion Service is disabled by default. To enable the Mass Ingestion Service, use infacmd isp enableService.

The infacmd mi createService command uses the following syntax:

```
createService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-HttpPort|-http> http_port
[<-HttpsPort|-https> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
<-LicenseName|-ln> license_name
[<-FolderPath|-fp> full_folder_path]
<-NodeName|-nn> node_name
<-RepositoryService|-rs> repository_service_name
[<-RepositoryUser|-ru> repository_user]
[<-RepositoryPassword|-rp> repository_password]
[<-RepositoryUserSecurityDomain|-rsdn> repository_user_security_domain]
```

The following table describes infacmd mi createService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |
-HttpPort -http	http_port	Required if you do not specify an HTTPS port. Unique HTTP port number used for each Mass Ingestion Service process. After you create the service, you can define different port numbers for each Mass Ingestion Service process. Default is 9050. **Note:** You cannot specify both an HTTP port and an HTTPS port.
-HttpsPort -https	https_port	Required if you do not specify an HTTP port. Unique HTTPS port number used for each Mass Ingestion Service process. After you create the service, you can define different port numbers for each Mass Ingestion Service process. **Note:** You cannot specify both an HTTP port and an HTTPS port.
-KeystoreFile -kf	keystore_file_location	Required if you specify an HTTPS port. Path and file name of the keystore file that contains the keys and certificates required if you use the HTTPS protocol for the Mass Ingestion Service. You can create a keystore file with a keytool. keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
-KeystorePassword -kp	keystore_password	Required if you specify an HTTPS port. Password for the keystore file.

Option	Argument	Description
-LicenseName -ln	license_name	Required. Name of the license you want to assign to the Mass Ingestion Service. To apply changes, restart the Mass Ingestion Service.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the Mass Ingestion Service. Must be in the following format: */parent_folder/child_folder* Default is the domain: */*
-NodeName -nn	node_name	Required. Node where the Mass Ingestion Service runs.
-RepositoryService -rs	repository_service_name	Required. Model Repository Service that stores the metadata for mass ingestion specifications.
-RepositoryUser -ru	repository_user	Optional. User name to access the Model Repository Service.
-RepositoryPassword -rp	repository_password	Required if you specify the user name. User password to access the Model Repository Service.
-RepositoryUserSecurityDomain -rsdn	repository_user_security_domain	Optional. Name of the security domain that the Model repository user belongs to.

deploySpec

Deploys a mass ingestion specification. When you deploy the specification, you must specify the Data Integration Service and the Hadoop connection. You must deploy a mass ingestion specification before you can run it. After you deploy the specification, run the specification using infacmd mi runSpec.

The infacmd mi deploySpec command uses the following syntax:

```
deploySpec

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-DISServiceName|-dsn> dis_service_name
```

```
<-MISpecName|-spec> mi_spec_name

<-HadoopConnection|-hc> hadoop_connection
```

The following table describes infacmd mi deploySpec options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-DISServiceName -dis	data_integration_service	Required. Name of the Data Integration Service where you want to deploy the mass ingestion specification.
-MISpecName -spec	mi_spec_name	Required. Name of the mass ingestion specification that you want to deploy to the Data Integration Service.
-HadoopConnection -hc	hadoop_connection	Required. The Hadoop connection that the Data Integration Service uses to push the mass ingestion specification to the Hadoop environment.

exportSpec

Exports the mass ingestion specification to an application archive file. When you export the specification, you must specify the directory where you want to save the file. You can deploy the application archive file to a Data Integration Service using infacmd dis DeployApplication.

The infacmd mi exportSpec command uses the following syntax:

```
exportSpec

<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-MISpecName|-spec> mi_spec_name

<-Directory|-dir> dir_path

<-HadoopConnection|-hc> hadoop_connection
```

The following table describes infacmd mi exportSpec options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-MISpecName -spec	mi_spec_name	Required. Name of the mass ingestion specification that you want to export.
-Directory -dir	dir_path	Required. The directory where you want to write the application archive file.
-HadoopConnection -hc	hadoop_connection	Required. The Hadoop connection that the Data Integration Service will use to run the mass ingestion job when you import the application archive file and run the application. You must specify the Hadoop connection because a Hadoop connection does not persist for the mass ingestion specification while the specification is stored in the Model repository.

extendedRunStats

Gets the extended ingestion statistics for a specific source table in a deployed mass ingestion specification. To get the extended statistics, you must specify the RunID of the mass ingestion specification, the name of the source table, and the mapping type.

The extended statistics report the ingestion statistics for table rows ingested from the source and the ingestion statistics for table rows ingested in the target. The statistics list the number of rows that were ingested successfully and the number of rows that contain errors.

If the run instance uses an incremental load, the extended statistics also report the incremental key and the start value. The incremental key is the name of the column that the Spark engine used to fetch incremental data in the source table. The start value is the value that the Spark engine used to start ingesting incremental data.

The infacmd mi extendedRunStats command uses the following syntax:

```
extendedRunStats

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-RunID|-rid> run_id

<-SourceName|-srcName> source_name

<-MappingTp|-mtp> mapping_type
```

The following table describes infacmd mi extendedRunStats options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification associated with the ingestion mapping job.

Option	Argument	Description
-RunID -rid	run_id	Required. Run identifier number, or the Run ID, of the mass ingestion specification run instance. To find the RunID for a run instance, list the specification run instances using infacmd mi listSpecRuns.
-SourceName -srcName	source_name	Required. Name of the source table in the run instance of the mass ingestion specification. To find the name of the source table, get the ingestion run statistics using infacmd mi getSpecRunStats.
-MappingTp -mtp	mapping_type	Required. The mapping type corresponds to the run-time engine that runs the ingestion mapping job for the source table. To find the mapping type, get the ingestion run statistics using infacmd mi getSpecRunStats.

getSpecRunStats

Gets the detailed run statistics for a deployed mass ingestion specification. To get the statistics, you must specify a RunID. To find the RunID for a run instance, list the specification run instances using infacmd mi listSpecRuns.

The detailed run statistics report the JobID for each ingestion mapping job in the deployed mass ingestion specification, the name of the source table that each mapping job ingests, the run start time, the end time, the run-time engine that runs the mapping job, and the job status. The JobID is the ID of the ingestion mapping job that ingests the source table. The status might display Completed, Failed, Canceled, Running, Aborted, Queued, or Unknown.

The infacmd mi getSpecRunStats command uses the following syntax:

```
getSpecRunStats

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-runID|-rid> run_id
```

The following table describes infacmd mi getSpecRunStats options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-runID -rid	run_id	Required. Run identifier number, or the Run ID, of the mass ingestion specification run instance. To find the RunID for a run instance, list the specification run instances using infacmd mi listSpecRuns.

listSpecRuns

Lists the run instances of a deployed mass ingestion specification. Each run instance is defined by a RunID. When you list the run instances, you must specify the Mass Ingestion Service.

The detailed run statistics report the RunID for each specification run instance, the load type, the run instance start time, the Data Integration Service where the mass ingestion specification is deployed, the user who started the run, and the job status for each run instance. The status might display Completed, Failed, Cancelled, Running, Queued, or Unknown.

The infacmd mi listSpecRuns command uses the following syntax:

```
listSpecRuns

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-ServiceName|-sn> service_name

<-MISpecName|-spec> mi_spec_name
```

The following table describes infacmd mi listSpecRuns options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-MISpecName -spec	mi_spec_name	Required. Name of the mass ingestion specification.

listSpecs

Lists the mass ingestion specifications. When you list specifications, you must specify the Mass Ingestion Service.

The infacmd mi listSpecs command uses the following syntax:

```
listSpecs
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
```

The following table describes infacmd mi listSpecs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specifications.

restartMapping

Restarts the ingestion mapping jobs in a mass ingestion specification. Specify the list of source tables to restart. You must specify the Mass Ingestion Service and the RunID for the run instance of the mass ingestion specification. You can also specify whether you want to restart only the source tables that failed.

The infacmd mi restartMapping command uses the following syntax:

```
restartMapping
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
<-RunID|-rid> run_id
<-SourceList|-srcList> comma_separated_source_list
[<-OnlyFailed|-failed> true|false]
```

The following table describes infacmd mi restartMapping options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the ingestion of the source tables.
-runID -rid	run_id	Required. Run identifier number (Run ID) of the mass ingestion specification run instance.
-SourceList -srcList	comma_separated_source_list	Required. The list of source tables to restart. Separate each source table with a comma.
-OnlyFailed -failed	true|false	Optional. Enter true to restart only the source tables that failed to be ingested. Enter false to restart all source tables.

runSpec

Runs a mass ingestion specification that is deployed to a Data Integration Service. Before you can run a specification, you must deploy the specification using infacmd mi deploySpec.

The infacmd mi runSpec command uses the following syntax:

```
runSpec
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
<-ServiceName|-sn> service_name

<-MISpecName|-spec> mi_spec_name

[<-LoadType|-lt> load_type]

<-DISServiceName|-dsn> dis_service_name

[<-OperatingSystemProfile|-osp> operating_system_profile_name]
```

The following table describes infacmd mi runSpec options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.
-Password -pd	password	Required. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-MISpecName -spec	mi_spec_name	Required. Name of the mass ingestion specification that is deployed to the Data Integration Service.
-LoadType -lt	load_type	Optional. Type of load to ingest the data in the mass ingestion specification. Use `full` or `incremental`. Default is `full`. If incremental load is not enabled in the mass ingestion specification, you cannot use an incremental load to ingest the data.

Option	Argument	Description
-DISServiceName -dis	data_integration_service	Required. Name of the Data Integration Service where the mass ingestion specification is deployed.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name of the operating system profile configured for the Data Integration Service.

updateSamlConfig

Updates the Mass Ingestion Service SAML configuration. You can configure the identity provider URL, the service provider ID, clock skew tolerance, and the assertion signing certificate alias.

The infacmd mi updateSamlConfig command uses the following syntax:

```
updateSamlConfig
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-idpUrl|-iu> identity_provider_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
```

The following table describes the infacmd mi updateSamlConfig options and arguments:

Option	Argument	Description
–DomainName –dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
–UserName –un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Optional. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. Default is Native.
-ServiceName -sn	service_name	Required. Name of the Mass Ingestion Service that manages the mass ingestion specification.
-idpUrl -iu	identity_provider_url	Optional. Specify the identity provider URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	service_provider_id	Optional. The relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you specified "Informatica" as the relying party trust name in AD FS, you do not need to specify a value.
-ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	Optional. The allowed time difference between the identity provider host system clock and the system clock on the master gateway node. The lifetime of SAML tokens issued by the identity provider is set according to the identity provider host system clock. The lifetime is valid if the start time or end time set in the token is within the specified number seconds of the system clock on the master gateway node. Values must be from 0 to 600 seconds. Default is 120 seconds.
-AssertionSigningCertificateAlias -asca	idp_assertion_signing_certificate_alias	Optional. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication. If you change the alias name, import the corresponding certificate into the truststore file on each gateway node, and then restart the node.

CHAPTER 25

infacmd mrs Command Reference

This chapter includes the following topics:

BackupContents

Backs up the Model repository content to a file. If the repository content does not exist, the command fails.

To ensure that a consistent backup file is created, the backup operation blocks all other repository operations until the backup completes.

The infacmd mrs BackupContents command uses the following syntax:

```
BackupContents

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-OutputFileName|-of> output_file_name

[<-OverwriteFile|-ow> overwrite_file]

[<-Description|-ds> description]

[<-BackupSearchIndices|-bsi> backup search index]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs BackupContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
OutputFileName -of	output_file_name	Required. Name of the backup file.
OverwriteFile -ow	overwrite_file	You must include this option to overwrite a backup file that has the same name.
Description -ds	description	Description of backup file. If the description contains spaces or other non-alphabetic characters, enclose the description in quotation marks.

Option	Argument	Description
-BackupSearchIndices -bsi	-	Optional. Set to true to save the search index to the backup file and reduce the amount of time needed to restore the file. Set to false to not save the search index to the backup file. When you restore the file, the Model Repository Service re-indexes the search index. Default is true.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CheckInObject

Checks in a single object that is checked out. The object is checked in to the Model repository.

The infacmd mrs CheckInObject command uses the following syntax:

```
infacmd mrs checkInObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
[<-Description|-ds> description]
```

The following table describes infacmd mrs CheckInObject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-ObjectPathAndName -opn	MRS_object_path	Required. Path to the Model repository object, including the object name. Enclose the path in double quotes. Use the following syntax: `"ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}"`
-Description -ds	description	Optional. You can use this parameter for the check-in description or comments.

CreateContents

Creates repository content for a Model repository. The command fails if the content exists for the Model repository.

The infacmd mrs CreateContents command uses the following syntax:

```
CreateContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs CreateContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CreateFolder

Creates a folder in a project in a Model repository.

The infacmd mrs CreateFolder command uses the following syntax:

```
infacmd mrs createFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-CreatePath|-cp> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs CreateFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.

Option	Argument	Description
-ProjectName -pn	project_name	Required. Name of the project to create the folder in. The project name is not case sensitive. The project name cannot exceed 128 characters. The project name cannot start with a number, and can contain alphanumeric characters and the following characters: @ # _
-Path -p	folder_path_and_name	Required. Path and name of the folder to create. The path name must start with a forward slash (/).
-CreatePath -cp	true|false	Optional. If true, creates the folder in the specified path. Default is false.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CreateProject

Creates a project in a Model repository.

The infacmd mrs CreateProject command uses the following syntax:

```
infacmd mrs createProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs CreateProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ProjectName -pn	project_name	Required. Name of the project to create. The project name is not case sensitive. The project name cannot exceed 128 characters. The project name cannot start with a number, and can contain alphanumeric characters and the following characters: `@ # _`
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CreateService

Creates a Model Repository Service. Before you create the Model Repository Service, you need to create a database to store repository tables. Use the database client to create the database.

Each Model repository must meet the following database requirements:

- The Model repository must have a unique schema. Two Model repositories or the Model repository and the domain configuration database cannot share the same schema.
- The Model repository must have a unique repository database name.

The infacmd mrs CreateService command uses the following syntax:

```
CreateService

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

<-DbUser|-du> db_user

<-DbPassword|-dp> db_password

<-DbUrl|-dl> db_url

[<-DbDriver|-dr> db_driver]

[<-DbDialect|-dd> db_dialect]

[<-SearchIndexRoot|-si> search_index_root]

[<-DbType|-dt> db_type (ORACLE, DB2, SQLSERVER, OR POSTGRESQL)]

[<-DbSchema|-ds> db_schema (Used only for Microsoft SQL Server and
PostgreSQL databases)]

[<-DbTablespace|-db> db_tablespace (used for IBM DB2 only)]

[<-SecureJDBCParameters|-sjdbcp> secure_jdbc_parameters]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-FolderPath|-fp> full_folder_path]

[<-BackupNodes|-bn> nodename1,nodename2,...]
```

The following table describes infacmd mrs CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
NodeName -nn	node_name	Required. Node where you want to run the Model Repository Service to run.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-DbUser -du	db_user	Required. Account for the repository database. Set up this account using the database client.
-DbPassword -dp	db_password	Required. Repository database password for the database user.

Option	Argument	Description
-DbUrl -dl	db_url	Required. The JDBC connection string to connect to the Model repository database. Enclose the connection string in double quotes. Use the following syntax for each supported database: - IBM Db2. `"jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000"` - Microsoft SQL Server that uses the default instance. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true"` - Microsoft SQL Server that uses a named instance. `"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true"` - Microsoft SQL Server that uses the default instance with Windows NT credentials. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"` - Microsoft SQL Server that uses a named instance with Windows NT credentials. `"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"` - Azure SQL Server. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnameincertificate>;ValidateServerCertificate=true"` - Azure SQL Database with Active Directory authentication. `"jdbc:informatica:sqlserver://<host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"` - Oracle. `"jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"`

Option	Argument	Description
		To connect to Oracle using Oracle Connection Manager, use the following connection string: " `jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>; "` - PostgreSQL. `"jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName= "`
-DbDriver -dr	db_driver	Optional. The Data Direct driver to connect to the database. For example: com.informatica.jdbc.oracle.OracleDriver
-DbDialect -dd	db_dialect	Optional. The SQL dialect for a particular database. The dialect maps java objects to database objects. For example: org.hibernate.dialect.Oracle9Dialect
-SearchIndexRoot -si	search_index_root	Optional. Changes the directory for the search index. Enter the full path to the directory. Default is the Informatica installation directory.
-DbType -dt	db_type	Optional. Values are Oracle, SQL Server, DB2, or PostgreSQL.
-DbSchema -ds	db_schema	Optional. The schema name for a Microsoft SQL Server database or PostgreSQL database.
-DbTablespace -dt	db_tablespace	Required for a DB2 database only. When you configure a tablespace name, the Model Repository Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name.
[<-SecureJDBCParameters|-sjdbcp> secure_jdbc_parameters]	Secure JDBC Parameters	If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters. Enter the parameters as name=value pairs separated by semicolon characters (;). For example:param1=value1;param2=value2
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to create the service. Must be in the following format: */parent_folder/child_folder* Default is "/" (the domain).
-BackupNodes -bn	nodename1,nodename2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

DeleteContents

Deletes the Model repository content. The command fails if the content does not exist for the Model repository.

The infacmd mrs DeleteContents command uses the following syntax:

```
DeleteContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs DeleteContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

DeleteFolder

Deletes a folder from a project in a Model repository.

To delete a folder that contains objects, set the -ForceDelete option to true.

The infacmd mrs DeleteFolder command uses the following syntax:

```
infacmd mrs deleteFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> folder_path_and_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs DeleteFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.

Option	Argument	Description
-ProjectName -pn	project_name	Required. Name of the project that contains the folder.
-Path -p	folder_path_and_name	Required. Path and name of the folder to delete. Path must start with a forward slash (/).
-ForceDelete -f	true|false	Optional. If true, deletes a folder that contains objects. Default is false.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

DeleteProject

Deletes a project in a Model repository.

To delete a project that contains folders and objects, set the -ForceDelete option to true.

The infacmd mrs DeleteProject command uses the following syntax:

```
infacmd mrs deleteProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
[<-ForceDelete|-f> true|false]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs DeleteProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ProjectName -pn	project_name	Required. Name of the project to delete.
-ForceDelete -f	true|false	Optional. If true, deletes a project that contains folders and objects. Default is false.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

disableMappingValidationEnvironment

Disables the selected mapping validation environment for mappings that you run from the Developer tool.

Use the ValidationEnvironment parameter to disable a validation environment for a mapping. Repeat the command for each environment you want to remove.

Use filters to update one or more mappings in a project. If you do include filters, the command updates all mappings that are not deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

The infacmd mrs disableMappingValidationEnvironment uses the following syntax:

```
disableMappingValidationEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the disableMappingValidationEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Model Repository Service.
ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository. You can specify only one project at a time.
MappingNamesFilter -mnf	mapping_names	Optional. The names of mappings that you want to disable the validation environment for. Separate mapping names with commas. Default is all mappings in the Model repository.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Specify the execution environment for the validation environment you want to remove. You can enter either Native, Hadoop, or Databricks. By default, the validation environment is changed for all engines based on other filter criteria.

Option	Argument	Description
ValidationEnvironment -ve	validation_environment_name	Required. Name of the validation environment to remove from a mapping. You can enter one of the following values: - native - blaze - spark - spark-databricks Run the command for each validation environment to remove.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Selects only mappings whose parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks`
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Selects only mappings whose default parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks`
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

enableMappingValidationEnvironment

Enables a mapping validation environment for mappings that you run from the Developer tool. The mapping validation environment properties indicate the engines that the mapping will be validated to run in.

Use the ValidationEnvironment parameter to specify a validation environment to enable on a mapping. Repeat the command and specify a different validation environment to enable an additional validation environment for the mapping.

Use filters to update one or more mappings in a project. If you do not include filters, the command updates all mappings that are not deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

The infacmd mrs enableMappingValidationEnvironment uses the following syntax:

```
enableMappingValidationEnvironment
<-DomainName|-dn> domain_name
```

```
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-ConnectionName|-cn> connection_name]
[<-MappingNamesFilter|-mnf> mapping_names]
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> parameter name]
[<-ExecutionEnvironmentParameterDefaultValueFilter|-pdvf> parameter default value]
<-ValidationEnvironment|-ve> validation_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the enableMappingValidationEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Model Repository Service.
ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository. You can specify only one project at a time.
ConnectionName -cn	connection_name	Name of the connection for the mapping validation environment to use. The connection overwrites an existing connection or connection parameter that was set for the environment. Required to enable the native or non-native environment if no connection is present in the specified mapping. Optional to enable the native environment or if a connection is already present.
MappingNamesFilter -mnf	mapping_names	Optional. The names of mappings that you want to enable the validation environment for. Separate mapping names with commas. Default is all mappings in the Model repository.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Specify the execution environment to filter on. You can enter either Native, Hadoop, or Databricks. By default, the validation environment is changed for all engines based on other filter criteria.

Option	Argument	Description
ValidationEnvironment -ve	validation_environment_name	Required. Name of the validation environment to enable on a mapping. You can enter one of the following values: - native - blaze - spark - spark-databricks Run the command for each validation environment to enable.
ExecutionEnvironmentParameterNameFilter -pnf	name_of_parameter	Optional. Selects only mappings whose parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pnf MyParam -ve Databricks`
ExecutionEnvironmentParameterDefaultValueFilter -pdvf	parameter_default_value	Optional. Selects only mappings whose default parameter name matches this value. Example: `infacmd.sh mrs enableValidationEnvironment -pdvf Hadoop -ve Databricks`
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

ListBackupFiles

Lists files in the backup folder.

The infacmd mrs ListBackupFiles command uses the following syntax:

```
ListBackupFiles
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ListBackupFiles options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListCheckedOutObjects

Displays a list of objects that are checked out by a user. Run this command against a repository that is integrated with a version control system.

The infacmd mrs listCheckedOutObjects command uses the following syntax:

```
infacmd mrs listCheckedOutObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> by_user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-operationType|-optype> operation_type]
```

The following table describes infacmd mrs listCheckedOutObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ByUser -bu	checkedout_by_user	Optional. User account that has checked out objects in the Model repository.
-ObjectType -ot	object_type	Optional. Type of the object to search. For example, mapping.
-ByObjectPathandName -bopn	object_path_and_name	Optional. Path and name of the object to search.
-ObjectName -objn	object_name	Optional. Name of the object to search.
-LastOperationType -optype	operation_type	Optional. Type of the operation to search. Enter one of the following values: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

listFolders

Lists the names of all of the folders in the project folder path that you specify.

Use the -Path option to list all the folders in a project, or all the folders that a subfolder contains. Use a slash character (/) to specify the top level of a project.

For example, the following command lists all the folders in /MRS_1/Project_A/:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /
```

If the contents of Project _A are Folder_1 and Folder_2, then the following command lists all the subfolders in Folder_1:

```
infacmd mrs listFolders ... -sn MRS_1 -pn Project_A -p /Folder_1/
```

The infacmd mrs ListFolders command uses the following syntax:

```
infacmd mrs listFolders
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-Path|-p> path
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ListFolders options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.

Option	Argument	Description
-ProjectName -pn	project_name	Required. Name of the project for which you want to list the folders. The project name is not case sensitive. The project name cannot exceed 128 characters. The project name cannot start with a number, and can contain alphanumeric characters and the following characters: @ # _
-Path -p	path	Required. Path to the parent folder in which you want to list folder contents. The path must start with a slash (/). The name is not case sensitive.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListLockedObjects

Displays a list of objects that are locked by a user. Run this command against a repository that is not integrated with a version control system.

Note: If you run this command against a versioned repository, the command fails.

The infacmd mrs listLockedObjects command uses the following syntax:

```
infacmd mrs listLockedObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ByUser|-bu> user_name]
[<-ByUserSecurityDomain|-bsd> by_user_security_domain]
[<-ObjectType|-ot> object_type]
[<-ByObjectPathandName|-bopn> object_path_and_name]
[<-objectName|-objn> object_name]
[<-lastOperationType|-optype> operation_type]
```

The following table describes infacmd mrs listLockedObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ByUser -bu	locked_by_user	Optional. User account that owns the lock on objects in the Model repository. Default is objects locked by all users.

Option	Argument	Description
-ObjectType -ot	object_type	Optional. Type of the object to search. You can run the command against one object type. If you omit the parameter, the command runs against all object types.
-ByObjectPathAndName -bopn	object_path_and_name	Optional. Model repository path and name of the object to search.
-ObjectName -objn	object_name	Optional. Name of the object to search.
-LastOperationType -optype	operation_type	Optional. Type of the operation to search. Enter one of the following values: - ADD_OP - EDIT_OP - MOVE_OP - DELETE_OP

listMappingEngines

Lists the run-time engines of the mappings that are run from the Developer Tool. You can filter the results based on project, validation environment, run-time environment, and run-time environment parameters.

The infacmd mrs listMappingEngines command uses the following syntax:

```
listMappingEngines
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectNames|-pn>] project_name
[-ValidationEnvironmentFilter|-vef] validation_environment_name
[<-ExecutionEnvironmentFilter|-eef> execution_environment_name]
[<-ExecutionEnvironmentParameterNameFilter|-pnf> execution_environment_parameter_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs listMappingEngines options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command lists all the projects and the mappings within the projects. You can specify only one project at a time.

Option	Argument	Description
ValidationEnvironmentFilter -ve	validation_environment_name	Optional. Name of the validation environment for which you want to view the list of mappings. Choose one of the following values: - native - blaze - spark - spark-databricks Run the command for each validation environment to list the mappings.
ExecutionEnvironmentFilter -eef	execution_environment_name	Optional. Specify the run-time environment based on which you want to filter the mappings. Choose either Native, Hadoop, or Databricks. For example, when you specify the native option, the command lists the mappings that are configured to run on the Data Integration Service.
ExecutionEnvironmentParameterNameFilter|- -pnf	execution_environment_parameter_name	Optional. Specify the parameter name based on which you can parameterise the run-time environment and filter. You can parameterize the run-time environments in the parameter file along with a variable and use the variable in the infacmd command.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listPermissionOnProject

List all the permissions on multiple projects for groups and users. Separate multiple project names with a comma. You need read permission on the project to view the list of permissions for the groups and users.

The infacmd mrs listPermissionOnProject command uses the following syntax:

```
listPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectNames|-pn> project_name_list
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs listPermissionOnProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ProjectNames -pn	project_name_list	Required. Names of the projects for which you want to list the permissions for users and groups. The project names are not case sensitive. Separate multiple project names with a comma.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListProjects

Lists projects in the Model repository. The command fails if the Model repository does not have repository content.

The infacmd mrs ListProjects command uses the following syntax:

```
ListProjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ListProjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceOptions

Lists options for the Model Repository Service.

The infacmd mrs ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists service process options for the Model Repository Service.

The infacmd mrs ListServiceProcessOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
NodeName -nn	node_name	Required. Node name for which you want to list the service process options.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ManageGroupPermissionOnProject

Manages permissions on multiple projects for a group.

The infacmd mrs manageGroupPermissionOnProject command uses the following syntax:

```
infacmd mrs manageGroupPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain |-sdn> security_domain]
[<-recipientSecurityDomain|-rdn> recipient_security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectNames|-pn> project_name_list
<-Permission|-pm> permission_name
<-RecipientName|-rn> recipient_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ManageGroupPermissionOnProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the recipient group belongs. To set the recipient security domain, refer to the same guidelines that you use to set the security domain for the authorizing user.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ProjectNames -pn	project_name_list	Required. Names of the projects for which you want to allow or revoke permissions. The project names are not case sensitive. Separate multiple project names with a comma.

Option	Argument	Description
-Permission -pm	permission_name	Required. The permissions that you want to allow or revoke from the recipient group. Enter the permission in double quotes and use a backslash (\ ) as the escape character. The following arguments are valid: `+r, +w, +g, -r, -w, -g` Use these arguments to allow or revoke read, write, and grant permissions. For example, a valid argument to revoke read permissions and allow write permissions is `\"-r+w\"`.
-RecipientName -rn	recipient_name	Required. The name of the recipient group for which you want to manage permissions.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ManageUserPermissionOnProject

Manages permissions on multiple projects for a user.

The infacmd mrs manageUserPermissionOnProject command uses the following syntax:

```
infacmd mrs manageUserPermissionOnProject
<-DomainName|-dn> domain_name
[<-SecurityDomain |-sdn> security_domain]
[<-recipientSecurityDomain|-rdn> recipient_security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectNames|-pn> project_name_list
<-Permission|-pm> permission_name
<-RecipientName|-rn> recipient_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs ManageUserPermissionOnProject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-recipientSecurityDomain -rdn	recipient_security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the recipient user belongs. To set the recipient security domain, refer to the same guidelines that you use to set the security domain for the authorizing user.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ProjectNames -pn	project_name_list	Required. Names of the projects for which you want to allow or revoke permissions. The project names are not case sensitive. Separate multiple project names with a comma.

Option	Argument	Description
-Permission -pm	permission_name	Required. The permissions that you want to allow or revoke from the recipient group. Enter the permission in double quotes and use a backslash (\ ) as the escape character. The following arguments are valid: `+r, +w, +g, -r, -w, -g` Use these arguments to allow or revoke read, write, and grant permissions. For example, a valid argument to revoke read permissions and allow write permissions is `\"-r+w\"`.
-RecipientName -rn	recipient_name	Required. The user name of the recipient user for which you want to manage permissions.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

PopulateVCS

Synchronizes the Model repository with a version control system. Before you synchronize the Model repository with a version control system, you configure versioning properties.

When you configure versioning properties, you restart the Model repository, and then you run the PopulateVCS command.

Note: After you run the command, the Model repository is unavailable until synchronization completes.

The infacmd mrs populateVCS command uses the following syntax:

```
infacmd mrs populateVcs
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs populateVCS options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ReassignCheckedOutObject

Reassigns the ownership of a checked-out object to another user. If the owner of a checked-out object saved changes, the changes are retained when you reassign the object. If the changes are not saved, the changes are lost when you reassign the object.

The infacmd mrs reassignCheckedOutObject command uses the following syntax:

```
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathandName|-opn> object_path_and_name
<-ToUser|-tu> to_user
[<-ToUserSecurityDomain|-tsd> to_user_security_domain]
```

The following table describes infacmd mrs reassignCheckedOutObject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ObjectPathAndName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ToUser -tu	Username	Required. Username of the user who you want to own the object checked-out state.
-ToUserSecurityDomain -tsd	Security domain	Optional. Security domain of the user who you want to own the object checked-out state.

rebuildDependencyGraph

Rebuilds the object dependency graph so that you can view object dependencies after an upgrade. Run this command if the upgrade of the Model Repository Service failed to rebuild the object dependency graph.

Users must not access Model repository objects until the rebuild process completes, or the object dependency graph might not be accurate. You might want to run the command when users are not logged in.

The infacmd mrs rebuildDependencyGraph command uses the following syntax:

```
rebuildDependencyGraph
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs rebuildDependencyGraph options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

RenameFolder

Renames a folder in a project.

The infacmd mrs RenameFolder command uses the following syntax:

```
infacmd mrs renameFolder
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-ProjectName|-pn> project_name
<-SourceFolder|-sf> source_folder
<-TargetFolder|-tn> target_folder
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs RenameFolder options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.

Option	Argument	Description
-ProjectName -pn	project_name	Required. Name of the project that contains the folder to rename.
-SourceFolder -sf	source_folder_path_and_name	Required. Path and name of the folder to rename. Path must start with a forward slash (/).
-TargetFolder -tn	target_folder_path_and_name	Required. New name for the folder. You can specify a folder name, or a path and folder name. The path must start with a forward slash (/).
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

replaceMappingHadoopRuntimeConnections

Replaces the Hadoop connection of all mappings in the repository with another Hadoop connection. The Data Integration Service uses the Hadoop connection to connect to the Hadoop cluster to run mappings in the Hadoop environment.

The command does not modify Hadoop connections in the transformations. You can specify the project name to replace the Hadoop connection of the mappings in the project.

The infacmd mrs replaceMappingHadoopRuntimeConnections uses the following syntax:

```
replaceMappingHadoopRuntimeConnections
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
<-OldConnectionName|-oc> connection_name_of_old_connection_to_replace
<-NewConnectionName|-nc> connection_name_of_new_connection
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the replaceMappingHadoopRuntimeConnections options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Data Integration Service.

Option	Argument	Description
ProjectName -an	application_name	Optional. Name of the project that contains the mapping. If you specify this option, the command replaces the Hadoop connection only for the project.
OldConnectionName -oc	connection_name_of_old_connection_to_replace	Required. Name of the Hadoop connection that you want to replace.
NewConnectionName -nc	connection_name_of_new_connection	Required. Name of the Hadoop connection that the Data Integration Service must use to connect to Hadoop cluster to run mappings in the Hadoop environment.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

RestoreContents

Restores content of a Model repository from a backup file.

The infacmd mrs RestoreContents command uses the following syntax:

```
RestoreContents
 <-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
 <-UserName|-un> user_name
 <-Password|-pd> password
 <-ServiceName|-sn> service_name
 <-InputFileName|-if> input_file_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds
```

The following table describes infacmd mrs RestoreContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model RepositoryService to back up.
InputFileName -if	input_file_name	Required. Name of the backup file to restore.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

UndoCheckout

Reverts the checkout of a Model repository object. The object is checked in to the Model repository. The Model repository discards any changes to the object since it was checked out. The version control system does not increment the version number or add to the version history.

The infacmd mrs undoCheckout command uses the following syntax:

```
infacmd mrs undoCheckout
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

The following table describes infacmd mrs undoCheckout options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ObjectPathAndName -opn	MRS_object_path	Required. Path to the Model repository object, including the object name. Enclose the path in double quotes. Use the following syntax: `"ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}"`

setMappingExecutionEnvironment

Specifies the mapping execution environment for mappings that you run from the Developer tool.

Use filters to update one or more mappings in a project. If you do not include filters, the command updates all mappings that are not deployed to the Data Integration Service. A mapping must match all specified filters to be modified.

The infacmd mrs setMappingExecutionEnvironment uses the following syntax:

```
setMappingExecutionEnvironment
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ProjectName|-pn> project_name]
[<-MappingNamesFilter|-mnf> mapping_names]
<-ExecutionEnvironment|-ee> execution_environment_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the setMappingExecutionEnvironment options and arguments:

Option	Argument	Description
DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
ServiceName -sn	service_name	Required. Name of the Model Repository Service.
ProjectName -pn	project_name	Optional. Name of the project that contains the mapping. If you do not specify a project name, the command updates all projects in the Model repository.
MappingNamesFilter -mnf	mapping_names	Optional. The names of mappings that you want to set the execution environment for. Separate mapping names with commas. Default is all undeployed mappings.

Option	Argument	Description
ExecutionEnvironment -ee	execution_environment_name	Required. Name of the execution environment to set. Choose either Native, Hadoop, or Databricks.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

UndoCheckout

Reverts the checkout of a Model repository object. The object is checked in to the Model repository. The Model repository discards any changes to the object since it was checked out. The version control system does not increment the version number or add to the version history.

The infacmd mrs undoCheckout command uses the following syntax:

```
infacmd mrs undoCheckout
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

The following table describes infacmd mrs undoCheckout options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ObjectPathAndName -opn	MRS_object_path	Required. Path to the Model repository object, including the object name. Enclose the path in double quotes. Use the following syntax: `"ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}"`

UnlockObject

Unlocks a Model repository object that is locked by a user. Run this command against a repository that is not integrated with a version control system.

Note: If you run this command against a versioned repository, the command fails.

You can unlock one object at a time.

The infacmd mrs unlockObject command uses the following syntax:

```
infacmd mrs unlockObject
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ObjectPathAndName|-opn> Object_path_and_name
```

The following table describes infacmd mrs unlockObject options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Model Repository Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ObjectPathAndName -opn	MRS_object_path	Required. Path to the Model repository object, including the object name. For example, use the following syntax: `ProjectName/FolderName/SubFolder_Name/ObjectName`

UpdateServiceOptions

Updates options for the Model Repository Service. Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd mrs UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
[<-PrimaryNode|-nn> primary node name]
[<-BackupNode|-bn> nodename1,nodename2,...]
[<-SearchIndexRoot|-si> search_index_root]
```

The following table describes infacmd mrs UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Space separated name-value pairs. To enter a value that contains spaces or other non-alphanumeric characters, enclose the value in single quotes. Enclose the options in double quotes.
-PrimaryNode -nn	primary node name	Optional. Node where you want to run the Model Repository Service to run.
-BackupNodes -bn	nodename1,nodename2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-SearchIndexRoot -si		Optional. Changes the directory for the search index. Enter the full path to the directory. Default is the Informatica installation directory.

Model Repository Service Options

Use the Model Repository Service options with the infacmd mrs UpdateServiceOptions command.

Enter Model Repository Service options in the following format:

```
... -o option_name=value option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Model Repository Service options:

Option	Argument	Description
CACHE.EnableCache	true | false	Enables the Model Repository Service to store Model repository objects in cache memory. To apply changes, restart the Model Repository Service.
CACHE.CacheJVMOptions	-Xmx[heap_size]	JVM options for the Model Repository Service cache. To configure the amount of memory allocated to cache, configure the maximum heap size. This field must include the maximum heap size, specified by the -Xmx option. The default value and minimum value for the maximum heap size is -Xmx128m. The options you configure apply when Model Repository Service cache is enabled. To apply changes, restart the Model Repository Service. The options you configure in this field do not apply to the JVM that runs the Model Repository Service.
PERSISTENCE_DB.Username	db_user	Required. Account for the repository database. Set up this account using the database client.
PERSISTENCE_DB.Password	db_password	Required. Repository database password for the database user.
PERSISTENCE_DB.DatabaseSchema	db_schema	Optional. The schema name for a particular database.
PERSISTENCE_DB.DatabaseTablespace	db_tablespace	Required for a DB2 database only. When you configure a tablespace name, the Model Repository Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.
PERSISTENCE_DB.DatabaseType	DatabaseType	Required. Database types include: - db2 - oracle - mssqlserver - sybase

Option	Argument	Description
PERSISTENCE_DB.JDBCConnect String	JDBC Connect String	The JDBC connection string to connect to the Model repository database. Use the following syntax for each supported database: - IBM Db2. `"jdbc:informatica:db2://<host name>:<port number>;DatabaseName=<database name>;BatchPerformanceWorkaround=true;DynamicSections=3000"` - Microsoft SQL Server that uses the default instance. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true"` - Microsoft SQL Server that uses a named instance. `"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true"` - Microsoft SQL Server that uses the default instance with Windows NT credentials. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"` - Microsoft SQL Server that uses a named instance with Windows NT credentials. `"jdbc:informatica:sqlserver://<host name>\<named instance name>;DatabaseName=<database name>;SnapshotSerializable=true;authenticationMethod=NTLM"` - Azure SQL Server. `"jdbc:informatica:sqlserver://<host name>:<port number>;DatabaseName=<database name>;SnapshotSerializable=true; SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.<hostnameincertificate>;ValidateServerCertificate=true"` - Azure SQL Database with Active Directory authentication. `"jdbc:informatica:sqlserver:// <host_name>:<port_number>;database=<database_name>;encrypt=true;AuthenticationMethod=ActiveDirectoryPassword;trustServerCertificate=false;hostNameInCertificate=*.database.windows.net;loginTimeout=<seconds>"` - Oracle. `"jdbc:informatica:oracle://<host name>:<port number>;SID=<database name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true"` To connect to Oracle using Oracle Connection Manager, use the following connection string:

Option	Argument	Description

		"
		`jdbc:Informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>; "`
		- PostgreSQL.
		`"jdbc:informatica:postgresql://<host name>:<port number>;DatabaseName= "`

PERSISTENCE_DB.SecureJDBCParameters	Secure JDBC Parameters	If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters. Enter the parameters as `name=value` pairs separated by semicolon characters (;). For example: `param1=value1;param2=value2`
PERSISTENCE_DB.Dialect	Dialect	The SQL dialect for a particular database. The dialect maps java objects to database objects. For example: `org.hibernate.dialect.Oracle9Dialect`
PERSISTENCE_DB.Driver	Driver	The Data Direct driver used to connect to the database. For example: `com.informatica.jdbc.oracle.OracleDriver`

SEARCH.SearchAnalyzer	Fully qualified Java class name	Fully qualified Java class name of the search analyzer.
		By default, the Model Repository Service uses the following search analyzer for English:
		`com.informatica.repository.service.provider.search.analysis.MMStandardAnalyzer`
		You can specify the following Java class name of the search analyzer for Chinese, Japanese and Korean languages:
		`org.apache.lucene.analysis.cjk.CJKAnalyzer`
		Or, you can create and specify a custom search analyzer.

SEARCH.SearchAnalyzerFactory	Fully qualified Java class name	Fully qualified Java class name of the factory class if you used a factory class when you created a custom search analyzer. If you use a custom search analyzer, enter the name of either the search analyzer class or the search analyzer factory class.
VCS.Host	IP_address or host name	Required to configure versioning properties for the Model repository on Perforce. The URL, IP address, or host name of the machine where the Perforce version control system runs. Do not use this option when you configure SVN or Git as the version control system.

Option	Argument	Description
VCS.URL	URL of the Subversion repository	Required to configure versioning properties for the Model repository on SVN and Git. URL of the Subversion repository. For example: `VCS.URL=https://myserver.company.com/svn/` Do not use this option when you configure Perforce as the version control system.
VCS.Port	VCS_port	Required to configure versioning properties for the Model repository. Port number that the version control system host uses to listen for packets from the Model repository.
VCS.User	VCS_user	Required to configure versioning properties for the Model repository. User account for the version control system user. This account must have write permissions on the version control system. After you configure the connection with this single version control system user and password, all Model repository users connect to the version control system through this account. For the Perforce version control system, the account type must be a Standard user.
VCS.Password	VCS_password	Required to configure versioning properties for the Model repository. Password for the version control system user.
VCS.Type	VCS_type	Required to configure versioning properties for the Model repository. The supported version control system that you want to connect to. You can choose Perforce, SVN, or Git.

VCS.MRSPath	MRS_path	Required to configure versioning properties for the Model repository with Perforce.
		Path to the root directory of the version control system copy of Model repository objects.
		Note: When you run the command, the Model repository connects to the version control system and generates the specified directory if the directory does not exist yet.
		Only one Model Repository Service can use this directory.
		For Perforce, use the syntax:
		`//directory/path`
		where `directory` is the Perforce directory root, and `path` is the remainder of the path to the root directory of Model repository objects.
		Example:
		`//depot/Informatica/repository_copy`
		Do not use this option when you configure SVN or Git as the version control system.

UpdateServiceProcessOptions

Updates service process options for the Model Repository Service. Separate multiple options with a space. To enter a value that contains a space or other nonalphanumeric character, enclose the value in quotation marks.

Enter service process options in the following format:

```
... -o "option_name=value option_name=value" ...
```

Enclose all option names and values in double quotation marks.

The infacmd mrs UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-Options|-o> options
```

The following table describes infacmd mrs UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
NodeName -nn	node_name	Required. Node name for which you want to set the process options.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter name-value pair separated by spaces. Enter options in the following format: `OptionGroupName.OptionName=OptionValue OptionGroupName2.OptionName2=OptionValue2`

UpdateStatistics

Update statistics for Model repository on Microsoft SQL Server. You can run this command if you have the system administrator privilege for the Microsoft SQL Server database.

The infacmd mrs updateStatistics command uses the following syntax:

```
updateStatistics

<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs updateStatistics options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

UpgradeContents

Upgrades the contents of the Model repository. The command fails if the Model repository does not have repository content.

The infacmd mrs UpgradeContents command uses the following syntax:

```
UpgradeContents
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs UpgradeContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

updateviews

Updates views by dropping the existing views and re-creating the new views from the latest view specification file. To run this command, ensure that you have the administrative privileges.

The infacmd mrs updateviews command uses the following syntax:

```
updateviews

 <-DomainName|-dn> domain_name

 [<-SecurityDomain |-sdn> security_domain]
  <-UserName|-un> user_name

  <-Password|-pd> password

  <-ServiceName|-sn> service_name

  [<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs updateviews options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Model Repository Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

UpgradeExportedObjects

Upgrades objects exported to an .xml file from a previous Informatica release to the current metadata format. The command then generates an .xml file that contains the upgraded objects.

The command upgrades objects exported from the Model repository. Import the .xml file containing the upgraded objects into a current version Model repository.

The upgrade process is dependent on the Model Repository Service. You must supply the service name of a Model Repository Service running within the domain when you run the command.

The infacmd mrs UpgradeExportedObjects command uses the following syntax:

```
UpgradeExportedObjects
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
<-SourceFile|-sf> source_file
<-TargetFile|-tf> target_file
[<-OverwriteFile|-ow> overwrite_file]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd mrs UpgradeExportedObjects options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of a Model Repository Service running within the domain.
-SourceFile -sf	source_file	Required. Path and file name of the .xml file that contains the objects to be upgraded. You can specify an absolute path or a relative path to the file.
-TargetFile -tf	target_file	Required. Path and file name of the generated .xml file that contains the upgraded objects. You can specify an absolute path or a relative path to the file.
OverwriteFile -ow	overwrite_file	Optional. You must include this option to overwrite the target file that has the same name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

CHAPTER 26

infacmd ms Command Reference

This chapter includes the following topics:

abortAllJobs

Aborts all mapping jobs deployed to the Data Integration Service.

The command affects deployed jobs that are configured to run on the Spark engine. The command affects jobs in the queue stored in the Model repository that is configured in the Data Integration Service properties. The command aborts batch jobs that you run from infacmd.

For on-demand jobs, the command aborts jobs on one of the Data Integration Service nodes, and does not affect other domain nodes.

Note: It is not possible to specify the node on which the command aborts on-demand jobs.

You can use optional flags to apply the command only to queued jobs or running jobs. If you include neither option, the command affects all jobs.

The command fails if you run it during Spark cleanup operations.

The infacmd ms abortAllJobs command uses the following syntax:

```
abortAllJobs
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-OnlyQueuedJobs|-q> true|false]
[<-OnlyRunningJobs|-r> true|false]
```

The following table describes infacmd ms abortAllJobs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-OnlyQueuedJobs -q	true | false	Optional. Use this option to filter the affected jobs to include only jobs that the Data Integration Service has queued to run.
-OnlyRunningJobs -r	true | false	Optional. Use this option to filter the affected jobs to include only jobs that the Data Integration Service is running.

deleteMappingPersistedOutputs

Deletes all persisted mapping outputs for a deployed mapping. Specify the outputs to delete using the name of the application and the run-time instance name of the mapping. To delete specific outputs, use the option -OutputNamesToDelete.

The infacmd ms deleteMappingPersistedOutputs command uses the following syntax:

```
deleteMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
<-RuntimeInstanceName|-rin> runtime_instance_name
[<-OutputNamesToDelete|-ontd> output_names_to_delete]
```

The following table describes infacmd ms deleteMappingPersistedOutputs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the mapping.
-Application -a	application_name	Required. Name of the application that contains the mapping.

Option	Argument	Description
-RuntimeInstanceName -rin	runtime_instance_name	Required. Name of the run-time instance of the mapping. Use the name specified in the infacmd ms runMapping command to run the commands listMappingPersistedOutputs and deleteMappingPersistedOutputs.
-OutputNamesToDelete -ontd	output_names_to_delete	Optional. Names of the persisted outputs to be deleted. To specify multiple outputs for deletion, separate names with a comma.

fetchAggregatedClusterLogs

Gets .zip or tar.gz file of the aggregated cluster logs for a mapping based on the job ID and writes the compressed aggregated log file to a target directory.

The infacmd ms fetchAggregatedClusterLogs command uses the following syntax:

```
fetchAggregatedClusterLogs
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RequestId|-id> request_id
[<-TargetLogDirectory|-tld> target_log_directory]
[<-TargetFilename|-tf> target filename without extension]
[<-ClusterLoginUsername|-clu> cluster_login_username]
[<-ClusterLoginPassword|-clp> cluster_login_password]
[<-CustomProperties|-cp> custom_properties]
```

The following table describes infacmd ms fetchAggregatedClusterLogs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the mapping.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-RequestId -id	request_id	Required. The job ID for the mapping that you want to write the log file for. Enter the job ID that the infacmd ms runMapping command returns.
-TargetLogDirectory -tld	target_log_directory	Optional. The directory to which you want to write the compressed aggregated log file.

Option	Argument	Description
-TargetFilename -tf	target filename without extension	Optional. Name and file path of the compressed aggregated log file.
-ClusterLoginUsername -clu	cluster_login_username	Required if you use Kerberos-enabled YARN ResourceManager application. User name to access YARN application.
-ClusterLoginPassword -clp	cluster_login_password	Required if you specify the cluster login user name. Password to access YARN application. The password is case sensitive.
-CustomProperties -cp	custom_properties	Optional. Define custom properties for a mapping at the request of Informatica Global Customer Support. Enter custom properties as name-value pairs separated by semicolons. For example: `... -cp custom_property_name=value` To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

getMappingStatus

Gets the current status of a deployed mapping job by job ID. Enter the job ID returned by the infacmd ms runMapping command.

Note: You must configure the Monitoring Model Repository Service in the Administrator tool before you use this command.

The infacmd ms getMappingStatus command uses the following syntax:

```
getMappingStatus
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
<-JobId|-ji> job_id
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The command returns information about a mapping run including job name, job state, and log file path.

If a run-time instance name was passed with the runMapping command, the job name is the run-time instance name. Otherwise, the job name is one of the following options:

- <mapping name>
- <mapping name>_<parameter set name>

- <mapping name>_<parameter file name>

The following table describes infacmd ms getMappingStatus options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the mapping.

Option	Argument	Description
-JobId -jl	job_id	Required. The job ID for the mapping that you want to get the status of. Enter the job ID returned by the infacmd ms runMapping command.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.

getRequestLog

Writes the mapping log to the specified file. Enter the job ID returned by the infacmd ms runMapping command.

The infacmd ms getRequestLog command uses the following syntax:

```
getRequestLog
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-RequestId|-id> request_id
<-FileName|-f> file_name
```

The following table describes infacmd ms getRequestLog options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the mapping.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-RequestId -id	request_id	Required. The job ID for the mapping that you want to write the log file for. Enter the job ID returned by the infacmd ms runMapping command.
-FileName -f	file_name	Required. Name and file path where you want to write the log file.

ListMappingOptions

Lists mapping options in an application.

The infacmd ms listMappingOptions command uses the following syntax:

```
listMappingOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
```

The following table describes infacmd ms listMappingOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-Mapping -m	mapping_name	Required. Name of the mapping.

listMappingParams

Lists the parameters for a mapping and creates a mapping parameter file that you can use when you run a mapping. The command returns an XML file with default values that you can update. Enter the parameter file name when you run the mapping with infacmd ms runMapping.

The infacmd ms listMappingParams command uses the following syntax:

```
listMappingParams
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
[<-OutputFile|-o> output file_to_write_to]
```

The following table describes infacmd ms listMappingParams options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-Mapping -m	mapping_name	Required. Name of the mapping.
- OutputFile - o	output file_to_write_to	Optional. Path and file name of the parameter file to create. If you do not specify a file, the command displays the parameters in the command prompt.

listMappingParams Output

The listMappingParams command returns a parameter file as an XML file with default values that you can update.

For example, you run the listMappingParams command on application "MyApp" and mapping "MyMapping." Mapping "MyMapping" has one parameter "MyParameter." The listMappingParams command returns an XML file in the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema">
    <!--
    <application name="MyApp">
        <mapping name="MyMapping">
            <!-- Specify deployed application specific parameters here. -->
        </mapping>
    </application>
    -->
    <project name="MyProject">
        <mapping name="MyMapping">
            <parameter name="MyParameter">DefaultValue</parameter>
        </mapping>
    </project>
</root>
```

The output XML file has the following top-level elements:

Application element

When you define a parameter within the application top-level element, the Data Integration Service applies the parameter value when you run the specified mapping in the specified application. You must include at least one project element within an application/mapping element.

By default, this top-level element is in comments. Remove the comments (!-- and -->) to use this element.

Project element

When you define a parameter within a project top-level element, the Data Integration Service applies the parameter value to the specified mapping in the project in any deployed application. The service also applies the parameter value to any mapping that uses the objects in the project.

If you define the same parameter in a project and an application top-level element in the same parameter file, the parameter value defined in the application element takes precedence.

listMappingPersistedOutputs

Lists the persisted mapping outputs for a deployed mapping. The outputs are listed based on the name of the application and the run-time instance name of the mapping.

The infacmd ms listMappingPersistedOutputs command uses the following syntax:

```
listMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
<-RuntimeInstanceName|-rin> runtime_instance_name
```

The following table describes infacmd ms listMappingPersistedOutputs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the mapping.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-RuntimeInstanceName -rin	runtime_instance_name	Required. Name of the run-time instance of the mapping. Use the name specified in the infacmd ms runMapping command to run the commands listMappingPersistedOutputs and deleteMappingPersistedOutputs.

listMappings

Lists the mappings in an application.

The infacmd ms listMappings command uses the following syntax:

```
listMappings
<-DomainName|-dn> domain_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-Application|-a> application_name
```

The following table describes infacmd ms listMappings options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-Application -a	application_name	Required. Name of the application that contains the mapping.

purgeDatabaseWorkTables

Purges all job information from the queue when you enable data engineering recovery for the Data Integration Service.

The command purges work queues, certain information about running jobs, and data engineering recovery information. The command removes rows from database tables of queued and running jobs. Use the command to remove leftover job information in the Model repository database after you delete the Data Integration Service that was configured for data engineering recovery.

The command affects jobs in the Model repository that is configured in the Data Integration Service properties. You can use the -msn option to specify a different Model repository.

You can use the -q option to apply the command only to queued jobs.

You can issue the command only when the Data Integration Service is stopped.

The infacmd ms purgeDatabaseWorkTables command uses the following syntax:

```
purgeDatabaseWorkTables
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-OnlyQueuedJobs|-q> true|false]
[<-MrsName|-msn> mrs_service_name]
```

The following table describes infacmd ms purgeDatabaseWorkTables options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.

Option	Argument	Description
-OnlyQueuedJobs -q	true | false	Optional. Use this option to filter the results to include only jobs that the Data Integration Service has queued to run.
-MrsName -msn	Model_repository_service_name	Optional. Name of the Model Repository Service from which to purge database work tables. Use this option only when you want to purge database work tables when the Data Integration Service is deleted. The option permanently removes all the rows from work tables.

runMapping

Runs a mapping that is deployed to a Data Integration Service. You can run the mapping with a parameter set or a parameter file.

To create a parameter file for a mapping, run infacmd ms listMappingParams. Before you run infacmd ms listMappingParams, run the infacmd dis startApplication command for the application.

To view the parameters and values for a parameter set, run the command infacmd dis listParameterSetEntries.

The infacmd ms runMapping command uses the following syntax:

```
runMapping
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
[<-Wait|-w> true|false]
[<-ParameterFile|-pf> parameter_file_path]
[<-ParameterSet|-ps> parameter_set_name]
[<-OperatingSystemProfile|-osp> operating_system_profile_name]
[<-NodeName|-nn> node_name]
[<-OptimizationLevel|-ol> optimization_level]
[<-PushdownType|-pt> pushdown_type]
[<-RuntimeInstanceName|-rin> runtime_instance_name]
```

```
[<-EnableAudit|-ea> true|false]

[<-CustomProperties|-cp> custom_properties]
```

The command returns the job ID for the mapping run.

You must enable monitoring to store the run-time instance name. If you purge monitoring statistics, run-time instance names are deleted and will not be returned by infacmd ms getMappingStatus. The mapping log might still contain the run-time instance name and the persisted mapping outputs associated with the run-time instance name can still be used.

The following table describes infacmd ms runMapping options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-Mapping -m	mapping_name	Required. Name of the mapping to run.
-Wait -w	true|false	Optional. Indicates whether infacmd waits for the mapping to complete before returning to the shell or command prompt. If true, infacmd returns to the shell or command prompt after the mapping completes. You cannot run subsequent commands until the mapping completes. If false, infacmd returns to the shell or command prompt immediately. You do not have to wait for the mapping to complete before running the next command. Default is false.
-ParameterFile -pf	parameter_file_path	Optional. Name and path of the parameter file. Do not enter a parameter file and a parameter set.
-ParameterSet -ps	parameter_set_name	Optional. Name of a parameter set to use at run time. The parameter set option overrides any parameter set deployed with the application. Do not enter a parameter set and a parameter file.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name of the operating system profile to run the mapping. If you do not use this option when the Data Integration Service is enabled to use operating system profiles, the Data Integration Service runs the mapping with the default profile.
-NodeName -nn	node_name	Optional. Name of the node in a Data Integration Service grid to dispatch the mapping job to. A Data Integration Service process must be running on the node. If you do not use this option, the mapping job is dispatched to the node where the master Data Integration Service process runs.

Option	Argument	Description
-OptimizationLevel -ol	optimization_level	Optional. Controls the optimization methods that the Data Integration Service applies to the mapping. Enter the numeric value that is associated with the optimization level that you want to configure. Enter one of the following values: **-1 (Auto)** The Data Integration Service applies optimizations based on the execution mode and mapping contents. **0 (None)** The Data Integration Service does not apply any optimization. **1 (Minimal)** The Data Integration Service applies the early projection optimization method. **2 (Normal)** The Data Integration Service applies the early projection, early selection, branch pruning, push-into, global predicate optimization, and predicate optimization methods. **3 (Full)** The Data Integration Service applies the cost-based, early projection, early selection, branch pruning, predicate, push-into, semi-join, and dataship-join optimization methods. Default is -1 (Auto).
-PushdownType -pt	pushdown_type	Optional. Controls the pushdown type that the Data Integration Service applies to a mapping. Enter one of the following values: - None. Select no pushdown type for the mapping. - Source. The Data Integration Service tries to push down as much transformation logic as it can to the source database. - Full. The Data Integration Service pushes the full transformation logic to the source database. This option overrides the pushdown type set in the mapping run-time properties or in a parameter file or parameter set. If you do not use this option, the Data Integration Service applies the pushdown type set in the mapping run-time properties or in a parameter file or parameter set.

Option	Argument	Description
-RuntimeInstanceName -rin	runtime_instance_name	Optional. Name of the run-time instance of the mapping. The name must be unique. The run-time instance name cannot contain slash characters. You must specify a run-time instance name in runMapping to persist mapping outputs and run the commands listMappingPersistedOutputs and deleteMappingPersistedOutputs. **Tip:** You can set the value as follows to standardize run-time instance names: - If all the mappings in an application use the same persisted mapping outputs, use the application name. - If the mappings use different persisted mapping outputs, use a combination of the application name, mapping name, and parameter set or file name.
-EnableAudit -ea	true|false	Optional. Indicates whether the audit rules and conditions run with the mapping. Default is false. This option overrides the **Enable Audit** configuration in the Developer tool. For example, if you select **Enable Audit** in the Developer tool and use the default value for this option, the audit rules and conditions do not run.
-CustomProperties -cp	custom_properties	Optional. Define custom properties for a mapping at the request of Informatica Global Customer Support. Enter custom properties as name-value pairs separated by semicolons. For example: `... -cp custom_property_name=value` To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

UpdateMappingOptions

Updates mapping options in an application.

The infacmd ms updateMappingOptions command uses the following syntax:

```
updateMappingOptions
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Application|-a> application_name
```

```
<-Mapping|-m> mapping_name

<-Options|-o> options
```

The following table describes infacmd ms updateMappingOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both these methods, the -re option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-Mapping -m	mapping_name	Required. Name of the mapping.
-Options -o	options	Optional. List of options to configure. Separate each option with a space. To view options, run the infacmd as ListServiceOptions.

UpdateOptimizationDefaultLevel

Updates the optimization level to -1 (Auto) for all the mappings in an application with optimization level 2 (Normal). Prior to version 10.4.0, Normal was the default optimization level. Auto is the default for all new mappings. The command does not affect mappings in the application with an optimization level other than Normal.

The infacmd ms updateOptimizationDefaultLevel command uses the following syntax:

```
updateOptimizationDefaultLevel
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

The following table describes infacmd ms updateOptimizationDefaultLevel options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both these methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the mapping or mappings.

UpdateOptimizationLevel

Updates optimization level for multiple mappings in an application.

The infacmd ms updateOptimizationLevel command uses the following syntax:

```
updateoptimizationLevel
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
[<-Mapping|-m> mapping_name]
[<-OptimizationLevel|-ol> optimization_level]
```

The following table describes infacmd ms updateOptimizationLevel options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both these methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the mapping or mappings.

Option	Argument	Description
-Mapping -m	mapping_name	Optional. Name of the mapping that you want to modify. To update the optimization level for multiple mappings, separate each mapping name with a comma. Default is all mappings in an application.
-OptimizationLevel -ol	optimization_level	Optional. The optimization method that the Data Integration Service applies to a mapping. Enter one of the following values: **-1 (Auto)** The Data Integration Service applies optimizations based on the execution mode and mapping contents. **0 (None)** The Data Integration Service does not apply any optimization. **1 (Minimal)** The Data Integration Service applies the early projection optimization method. **2 (Normal)** The Data Integration Service applies the early projection, early selection, branch pruning, push-into, global predicate optimization, and predicate optimization methods. **3 (Full)** The Data Integration Service applies the cost-based, early projection, early selection, branch pruning, predicate, push-into, semi-join, and dataship-join optimization methods. Default is -1 (Auto).

upgradeMappingParameterFile

Converts a parameter file you created in a previous Informatica version to a parameter file format that is valid for Informatica version 10.0.

In Informatica version 10.0, a parameter file can contain mapping parameters and workflow parameters, but it no longer contains transformation parameters. When you run a mapping or workflow with the previous version parameter file, the Data Integration Service must convert the parameter file to the Informatica 10.0 version at run time. You can increase performance by converting parameter files to the Informatica 10.0 format.

The infacmd ms upgradeMappingParameterFile command uses the following syntax:

```
upgradeMappingParameterFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Mapping|-m> mapping_name
[<-OutputFile|-o> output file_to_write_to]
<-ParameterFile|-pf> parameter_file_to_upgrade
```

The following table describes infacmd ms upgradeMappingParameterFile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the mapping. The application that contains the mapping must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the mapping.
-Mapping -m	mapping_name	Required. Name of the mapping.
- OutputFile - o	output file_to_write_to	Optional. Path and file name of the parameter file to create. If you do not specify a file, the command displays the parameters in the command prompt.
-ParameterFile -pf	parameter_file_to_upgrade	Required. The name of the parameter file to upgrade.

CHAPTER 27

infacmd oie Command Reference

The oie plugin is deprecated and support for the oie plugin will be dropped in a future release. The infacmd oie commands have migrated to the tools plugin. To view the command descriptions, see Chapter 37, “infacmd tools Command Reference” on page 1084.

CHAPTER 28

infacmd ps Command Reference

This chapter includes the following topics:

cancelProfileExecution

Stops all the profile runs including profiles and enterprise discovery profile.

The infacmd ps cancelProfileExecution command uses the following syntax:

```
cancelProfileExecution
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectPathAndName|-opn> MRS_object_path
```

The following table describes infacmd ps cancelProfileExecution options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.

Option	Argument	Description
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.
-ObjectPathAndName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`

CreateWH

Creates the content of the profiling warehouse.

The infacmd ps CreateWH command uses the following syntax:

```
CreateWH
<-DomainName|-dn> domain_name
[<-Gateway|-hp>] gateway_name]
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-DsServiceName|-dsn> data_integration_service_name
```

The following table describes infacmd ps CreateWH options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional. Use this option if the gateway connectivity information in the domains.infa file is out of date. Enter the host name and port number for the gateway node in the domain. Use the following syntax: gateway_hostname:port.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.

detectOrphanResults

Detects profile results in the profiling warehouse that do not have an associated profile in the Model repository. When you delete a profile before you open it, the Developer tool or the Analyst tool removes the profile and its metadata from the Model repository. The action results in orphan profile results in the profiling warehouse. To detect the orphan profile results, you can run the infacmd ps detectOrphanResults command. To save the command output to a file, run the `infacmd ps detectOrphanResults > <filename>` command.

The infacmd ps detectOrphanResults command uses the following syntax:

```
detectOrphanResults
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
```

The following table describes infacmd ps detectOrphanResults options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. The name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional if you run the command from the Informatica installation \bin directory. Required if you run the command from another location. The gateway node name. Use the following syntax: `[Domain_Host]:[HTTP_Port]`
-NodeName -nn	node_name	Required. The name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. The Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. The Data Integration Service name

DropWH

Removes the content of the profiling warehouse.

The infacmd ps DropWH command uses the following syntax:

```
DropWH
<-DomainName|-dn> domain_name
[<-Gateway|-hp>] gateway_name]
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-DsServiceName|-dsn> data_integration_service_name
```

The following table describes infacmd ps DropWH options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional. Use this option if the gateway connectivity information in the domains.infa file is out of date. Enter the host name and port number for the gateway node in the domain. Use the following syntax: gateway_hostname:port.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.

.

Execute

Runs a profile or scorecard.

The infacmd ps Execute command uses the following syntax:

```
Execute
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectType|-ot> object_type
<-ObjectPathAndName|-opn> MRS_object_path
[<-ProfileName|-pt> profile_task_name]
[<-wait|-w> true|false]
[<-ospn|-OsProfileName> os_profile_name]
```

The following table describes infacmd ps Execute options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_inetgration_service_name	Required. Data Integration Service name.
-ObjectType -ot	object_type	Required. Enter profile or scorecard.

Option	Argument	Description
-ObjectPathandName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ProfileName -pt	profile_task_name	Optional. Name of a profile task in the enterprise discovery profile.
-Wait -w	true|false	Optional. If true, waits until the command completes before returning the command prompt. If false, returns the command prompt before the command completes. Default is false.
-ospn -OsProfileName	os_profile_name	Optional. Name of the operating system profile if the Data Integration Service is enabled to use operating system profiles.

executeProfile

Runs an enterprise discovery profile.

The infacmd ps executeProfile command uses the following syntax:

```
executeProfile
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectPathAndName|-opn> MRS_object_path
[<-WaitForModelExecToFinish|-w> true|false]
[<-ospn|-OsProfileName> os_profile_name]
```

The following table describes infacmd ps executeProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_inetgration_service_name	Required. Data Integration Service name.
-ObjectPathandName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`

Option	Argument	Description
-WaitForModelExecToFinish -w	true|false	Optional. If true, waits until the command completes before returning the command prompt. If false, returns the command prompt before the command completes. Default is false.
-ospn -OsProfileName	os_profile_name	Optional. Name of the operating system profile if the Data Integration Service is enabled to use operating system profiles.

getExecutionStatus

Gets the run-time status of profile tasks in an enterprise discovery profile.

The infacmd ps getExecutionStatus command uses the following syntax:

```
getExecutionStatus
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectType|-ot> object_type
<-ObjectPathAndName|-opn> MRS_object_path
<-ProfileTaskName|-pt> profile_task_name
```

The following table describes infacmd ps getExecutionStatus options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.
-ObjectType -ot	object_type	Required. Enter profile or scorecard.
-ObjectPathAndName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`
-ProfileTaskName -pt	profile_task_name	Optional. Name of a profile task in the enterprise discovery profile.

getProfileExecutionStatus

Gets the run-time status of an enterprise discovery profile. The command also lists all the profile tasks in the enterprise discovery profile and their run-time statuses.

The infacmd ps getProfileExecutionStatus command uses the following syntax:

```
getProfileExecutionStatus
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-ObjectPathAndName|-opn> MRS_object_path
```

The following table describes infacmd ps getProfileExecutionStatus options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.
-ObjectPathAndName -opn	MRS_object_path	Required. Use the following syntax: `ProjectName/FolderName/.../SubFolder_Name/{ObjectName|ProjectName/ObjectName}`

List

Lists profiles or scorecards.

The infacmd ps List command uses the following syntax:

```
List
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-MrsServiceName|-msn> MRS_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ObjectType|-ot>
<-FolderPath|-fp> full_folder_path
[<-Recursive|-r>]
```

The following table describes infacmd ps List options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ObjectType -ot	-	Required. Enter profile or scorecard.

Option	Argument	Description
-FolderPath -fp	full_folder_path	Required. Enter the path of the folder that contains the objects you want to list. Use the following syntax: `Project_name/folder_name/../SubFolderName`
-Recursive -r	-	Optional. Applies the command to objects in the folder that you specify and its subfolders.

ListAllProfiles

Lists all the profiles in an enterprise discovery profile.

The infacmd ps ListAllProfiles command uses the following syntax:

```
ListAllProfiles
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-MrsServiceName|-msn> MRS_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ProfilePathAndName|-pn>
```

The following table describes infacmd ps ListAllProfiles options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ProfilePathAndName -pn	profile_path_and_name	Required. Enter the path to the enterprise discovery profile and its name.

migrateProfileResults

Migrates column profile results and data domain discovery results from version 9.1.0, 9.5.0, or 9.5.1.

The infacmd ps migrateProfileResults command uses the following syntax:

```
migrateProfileResults
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
```

The following table describes infacmd ps migrateProfileResults options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.

migrateScorecards

Migrates scorecard results from Informatica 9.1.0 or 9.5.0 to 9.5.1.

The infacmd ps migrateScorecards command uses the following syntax:

```
migrateScorecards
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn> node_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-migrateFrom|-mfr> migrate_from_release
```

The following table describes infacmd ps migrateScorecards options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.
-migrateFrom -mfr	migrate_from_release	Required. Version of Data Explorer migrating from. The version can be either 9.1.0 or 9.5.0. If you have run profiles and scorecards in versions 9.0, 9.0.1, or 9.1.0, then enter the value 9.1.0. If you have run profiles and scorecards in version 9.5.0, then enter 9.5.0 as the value.

Purge

Purges profile and scorecard results from the profiling warehouse. The infacmd ps Purge command purges all the profile and scorecard results except for the results from the latest profile or scorecard run.

The infacmd ps Purge command uses the following syntax:

```
Purge

<-DomainName|-dn> domain_name

[<-Gateway|-hp> gateway_name]

[<-NodeName|-nn>] node_name

<-UserName|-un> user_name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ObjectType|-ot> object_type

<-ObjectPathAndName|-opn> MRS_object_path
```

```
[<-RetainDays|-rd> results_retain_days]
[<-ProjectFolderPath|-pf> project_folder_path]
[<-ProfileName|-pt> profile_task_name]
[<-Recursive|-r> recursive]
[<-PurgeAllResults|-pa> purge_all_results]
```

The following table describes infacmd ps Purge options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. The name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional if you run the command from the Informatica installation \bin directory. Required if you run the command from another location. The gateway node name. Use the following syntax: `[Domain_Host]:[HTTP_Port]`
-NodeName -nn	node_name	Required. The name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. The Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. The Data Integration Service name
-ObjectType -ot	-	Required. Enter profile or scorecard.
-ObjectPathAndName -opn *	MRS_object_path	Optional. Do not use with ProjectFolderPath or Recursive. The path to the profile or scorecard in the Model repository. Use the following syntax: `ProjectName/FolderName/.../{SubFolder_Name/ObjectName|ProjectName/ObjectName}`
-RetainDays -rd	results_retain_days	Optional. Specifies the time range for the profile and scorecard results to be eligible for retention in the profiling warehouse. The Data Integration Service purges the rest of the profile and scorecard results. For example, if you enter -rd 10, then the results from the current day and past nine days are retained and the rest of the results are purged from the profiling warehouse.
-ProjectFolderPath -pf *	project_folder_path	Optional. Do not use with ObjectPathAndName or ProfileTaskName. The names of the project and folder where the profile or scorecard is stored. Use the following syntax: `ProjectName/FolderName`
-ProfileName -pt *	profile_task_name	Optional. The name of the profile task that you want to purge. If a folder has only one profile, then you can use only the ProjectFolderPath option because the ProjectFolderPath includes the name of the profile that contains the profile task. If a folder has multiple profiles in a folder, then use the ProfileName option along with the ProjectFolderPath option to specify the profile name.

Option	Argument	Description
-Recursive -r	recursive	Optional. Do not use with ObjectPathAndName. Applies the command to objects in the folder that you specify and its subfolders.
-PurgeAllResults -pa	purge_all_results	Optional. Set this option to purge all results for the profile or scorecard object. Use with the -recursive option to apply the command to profile and scorecard results in the folder that you specify and its subfolders.
* To run the command, you need to specify ObjectPathAndName or ProjectFolderPath or ProfileTaskName.		

purgeOrphanResults

Purges the orphan profile results from the profiling warehouse. You can run this command after you run the infacmd ps detectOrphanResults command to detect the orphan profile results.

The infacmd ps purgeOrphanResults command uses the following syntax:

```
purgeOrphanResults
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
<-filePathName|-fpn> filePathName
```

The following table describes infacmd ps purgeOrphanResults options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. The name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional if you run the command from the Informatica installation \bin directory. Required if you run the command from another location. The gateway node name. Use the following syntax: `[Domain_Host]:[HTTP_Port]`
-NodeName -nn	node_name	Required. The name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. The Model Repository Service name.

Option	Argument	Description
-DsServiceName -dsn	data_integration_service_name	Required. The Data Integration Service name
-filePathName -fpn	filePathName	Required. The file path with the name of the file that contains a list of profile IDs. The profile IDs map to the orphan profile results that need to be purged.

restoreProfilesAndScorecards

Restores profiles and scorecards from a previous version to the current version.

Sometimes, after you upgrade and drill down on the existing profile results or scorecard results, rule columns might not appear in the drilldown results. To include rule columns in the results, run the infacmd ps restoreProfilesAndScorecards command. Make sure that you create a backup of the Model repository content before you run the command.

The infacmd ps restoreProfilesAndScorecards command uses the following syntax:

```
restoreProfilesAndScorecards
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
[<-NodeName|-nn>] node_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-MrsServiceName|-msn> MRS_name
<-DsServiceName|-dsn> data_integration_service_name
```

The following table describes infacmd ps restoreProfilesAndScorecards options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. The name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_name	Optional if you run the command from the Informatica installation \bin directory. Required if you run the command from another location. The gateway node name. Use the following syntax: `[Domain_Host]:[HTTP_Port]`

Option	Argument	Description
-NodeName -nn	node_name	Required. The name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-MrsServiceName -msn	MRS_name	Required. The Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. The Data Integration Service name.

synchronizeProfile

Migrates documented, user-defined, and committed primary keys and foreign keys for all the profiles in a project from version 9.1.0, 9.5.0, or 9.5.1.

The infacmd ps synchronizeProfile command uses the following syntax:

```
synchronizeProfile
<-DomainName|-dn> domain_name
[<-Gateway|-hp> gateway_name]
```

```
[<-NodeName|-nn> node_name]

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-MrsServiceName|-msn> MRS_name

<-DsServiceName|-dsn> data_integration_service_name

<-ProjectName|-pn> project_name
```

The following table describes infacmd ps synchronizeProfile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-NodeName -nn	node_name	Optional. Name of the node where the Data Integration Service runs.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-MrsServiceName -msn	MRS_name	Required. Model Repository Service name.
-DsServiceName -dsn	data_integration_service_name	Required. Data Integration Service name.
-ProjectName -pn	project_name	Required. Project name.

CHAPTER 29

infacmd pwx Command Reference

This chapter includes the following topics:

CloseForceListener

Forces the cancellation of long-running subtasks on the PowerExchange Listener Service and stops the Listener Service.

When you issue the infacmd pwx CloseForceListener command, PowerExchange completes the following actions:

1. Checks if any subtasks on the Listener Service are active.
2. If active subtasks exist, polls the number of active subtasks every second until 30 seconds have elapsed.
3. During this period, stops any subtask that is waiting for TCP/IP network input.
4. Cancels any remaining active subtasks.
5. Stops the Listener Service.

The infacmd pwx CloseForceListener command uses the following syntax:

```
CloseForceListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx CloseForceListener options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands. For more information, see the *PowerExchange Reference Manual*.

Option	Argument	Description
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

CloseListener

Stops the PowerExchange Listener Service after waiting for all outstanding subtasks on the Listener Service to complete.

Note: If you have long-running subtasks on the Listener Service, issue the infacmd pwx closeforceListener command instead to force the cancellation of all user subtasks and stop the Listener Service.

The infacmd pwx CloseListener command uses the following syntax:

```
CloseListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx CloseListener options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

CondenseLogger

Starts another logging cycle before the wait period for starting another cycle has elapsed when the PowerExchange Logger Service is running in continuous mode. Specify the wait period in the NO_DATA_WAIT parameter of the pwxccl.cfg configuration file.

The infacmd pwx CondenseLogger command uses the following syntax:

```
CondenseLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx CondenseLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

createdatamaps

Creates data maps for bulk data movement operations.

Use the createdatamaps command to generate data maps for IMS, SEQ, and VSAM data sources from the command line. This command provides an alternative to using the PowerExchange Navigator in certain cases and allows you to generate or regenerate data maps noninteractively.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable. For more information, see “ICMD_JAVA_OPTS” on page 44.

The infacmd pwx createdatamaps command uses the following syntax:

```
createdatamaps
[<-pwxLocation|-loc> pwx_location]
[<-pwxUserName|-pun> pwx_user_name]
[<-pwxPassword|-ppd> pwx_password]
[<-pwxEncryptedPassword|-epwd> pwx_encrypted_password]
[<-datamapOutputDir|-dod> datamap_output_directory]
[<-replace|-r> replace_existing_datamaps
<-controlFile|-cf> file_path_for_control_file
[<-logFile|-lf> file_path_for_log_file]
[<-verbosity|-v> logging_verbosity]
```

The following table describes infacmd pwx createdatamaps options and arguments:

Option	Argument	Description
-pwxLocation -loc	pwx_location	Optional. The location of the data source as specified in a NODE statement in the PowerExchange dbmover configuration file. If pwxLocation is not specified, the createdatamaps utility accesses the copybook and DBD metadata on the local file system. If you configure the control file to find record IDs, pwxLocation is required.
-pwxUserName -pun	pwx_user_name	Optional. The user ID for connecting to the PowerExchange Listener, if pwxLocation is specified.

Option	Argument	Description
-pwxPassword -ppd	pwx_password	Optional. Password for connecting to the PowerExchange Listener, if pwxLocation is specified. Instead of a password, you can enter a valid PowerExchange passphrase. Passphrases for accessing a PowerExchange Listener on z/OS can be from 9 to 128 characters in length and can contain the following characters: - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Note:** The first character is an apostrophe. Passphrases cannot include single quotation marks (‘), double quotation marks (“), or currency symbols. If a passphrase contains spaces, you must enclose it with double-quotation marks ("), for example, `"This is an example passphrase"`. If a passphrase contains special characters, you must enclose it with triple double-quotation characters ("""), for example, `"""This passphrase contains special characters ! % & *."""`. If a passphrase contains only alphanumeric characters without spaces, you can enter it without delimiters. **Note:** On z/OS, a valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation. To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the *PowerExchange Reference Manual*.
-pwxEncryptedPassword -epwd	pwx_encrypted_password	Optional. Encrypted password for connecting to the PowerExchange Listener, if pwxLocation is specified. If the PowerExchange Listener runs on a z/OS or i5/OS system, you can enter an encrypted PowerExchange passphrase instead of an encrypted password. Do not encrypt a passphrase that contains characters that are not valid, such as double-quotation marks, single quotation marks, or currency symbols.
-datamapOutputDir -dod	datamap_output_directory	Optional. The local file directory to which to write the output data maps. Default is the current working directory.
-replace -r	replace_existing_datamaps	Optional. Specifies whether to replace existing data maps. If replace=Y, replaces any data maps in datamap_output_directory that have the same name as the data map that you are creating. If replace=N, skips the creation of a data map if a data map with the same name already exists in datamap_output_directory. Default is N.

Option	Argument	Description
-controlFile -cf	file_path_for_control_file	Required. Path and file name of the control file that controls data map generation.
-logFile -lf	file_path_for_log_file	Optional. Path and file name of the output log file. Default is STDOUT.
-verbosity -v	logging_verbosity	Optional. Verbosity for log files. Default is INFO. Valid values: - DEBUG. Most detailed logging. Might show stack traces. - INFO. Informational messages. - WARN. Indicates a potential problem. - ERROR. Indicates a failure. Processing continues. - FATAL. Indicates a fatal condition. Process terminates.

The PowerExchange node name and credentials are optional. If you do not include the pwxLocation option, the command accesses the local file system directly to read metadata. In this case, PowerExchange does not need to be installed on the machine on which you run createdatamaps.

For more information about the createdatamaps command, see the *PowerExchange Utilities Guide*.

CreateListenerService

Creates a PowerExchange Listener Service in a domain. By default, the Listener Service is disabled when you create it. Run the infacmd isp EnableService command to enable the service.

The infacmd pwx CreateListenerService command uses the following syntax:

```
CreateListenerService

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

<-StartParameters|-sp> start_parameters

<-SvcPort|-vp> service_port
```

The following table describes infacmd pwx CreateListenerService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if -DomainName is not specified. The host names and port numbers for the gateway nodes in the domain.
ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service. The name is not case sensitive. The name cannot exceed 128 characters or contain carriage returns, tabs, spaces, or the following characters: `/ * ? < > " |`
-NodeName -nn	node_name	Required. Name of the node where you want the Listener Service to run.

Option	Argument	Description
-LicenseName -ln	license_name	Optional. License to assign to the service. If you do not select a license now, you can assign a license to the service later. Required before you can enable the service.
-BackupNode -bn	backup_node	Optional. If the PowerCenter environment is configured for high availability, this option specifies the name of the backup node.
-StartParameters -sp	start_parameters	Parameters to include when you start the Listener Service. Separate the parameters with the space character. The *node_name* parameter is required. You can include the following parameters: - *node_name* Required. Node name that identifies the Listener Service. This name must match the name in the LISTENER statement in the DBMOVER configuration file. - config=*directory* Optional. Specifies the full path and file name for any dbmover.cfg configuration file that you want to use instead of the default dbmover.cfg file. This alternative configuration file takes precedence over any alternative configuration file that you specify in the PWX_CONFIG environment variable. - license=*directory/license_key_file* Optional. Specifies the full path and file name for any license key file that you want to use instead of the default license.key file. The alternative license key file must have a file name or path that is different from that of the default file. This alternative license key file takes precedence over any alternative license key file that you specify in the PWX_LICENSE environment variable. **Note:** In the config and license parameters, you must provide the full path only if the file does *not* reside in the installation directory. Include quotes around any path and file name that contains spaces.
-SvcPort -vp	service_port	Required. Port on which the Listener Service listens for commands from the Service Manager.

CreateLoggerService

Creates a PowerExchange Logger Service in a domain. By default, the Logger Service is disabled when you create it. Run the infacmd isp EnableService command to enable the service.

The infacmd pwx CreateLoggerService command uses the following syntax:

```
CreateLoggerService
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

<-SvcPort|-vp> service_port
```

The following table describes infacmd pwx CreateLoggerService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Optional. If -DomainName is not specified. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service. The name is not case sensitive. The name cannot exceed 128 characters or contain carriage returns, tabs, spaces, or the following characters: / * ? < > " |
-NodeName -nn	node_name	Required. Name of the node where you want the Logger Service to run.
-LicenseName -ln	license_name	Optional. License to assign to the service. If you do not select a license now, you can assign a license to the service later. Required before you can enable the service.
-BackupNode -bn	backup_node	Optional. If the PowerCenter environment is configured for high availability, this option specifies the name of the backup node.

Option	Argument	Description
-StartParameters -sp	start_parameters	Optional. Parameters to include when you start the Logger Service. Separate the parameters with the space character. You can include the following parameters: - coldstart={Y|N} Indicates whether to cold start or warm start the Logger Service. Enter Y to cold start the Logger Service. If the CDCT file contains log records, the Logger Service deletes these records. Enter N to warm start the Logger Service from the restart point that is indicated in the CDCT file. Default is N. - config=*directory/pwx_config_file* Specifies the full path and file name for any dbmover.cfg configuration file that you want to use instead of the default dbmover.cfg file. This alternative configuration file takes precedence over any alternative configuration file that you specify in the PWX_CONFIG environment variable. - cs=*directory/pwxlogger_config_file* Specifies the path and file name for the Logger Service configuration file. You can also use the cs parameter to specify a Logger Service configuration file that overrides the default pwxccl.cfg file. The override file must have a path or file name that is different from that of the default file. - encryptepwd=*encrypted_password* A password in encrypted format for enabling the encryption of PowerExchange Logger log files. With this password, the PowerExchange Logger can generate a unique encryption key for each Logger log file. The password is stored in the CDCT file in encrypted format. For security purposes, the password is not stored in CDCT backup files and is not displayed in the CDCT reports that you can generate with the PowerExchange PWXUCDCT utility. If you specify this parameter, you must also specify coldstart=Y. If you specify this parameter and also specify the ENCRYPTEPWD parameter in the PowerExchange Logger configuration file, pwxccl.cfg, the parameter in the configuration file takes precedence. If you specify this parameter and also specify the ENCRYPTPWD parameter in the PowerExchange Logger configuration file, an error occurs. You can set the AES algorithm to use for log file encryption in the ENCRYPTOPT parameter of the pwxccl.cfg file. The default is AES128. **Tip:** For optimal security, Informatica recommends that you specify the encryption password when cold starting the PowerExchange Logger rather than in the pwxccl.cfg configuration file. This practice can reduce the risk of malicious access to the encryption password for the following reasons: 1) The encryption password is not stored in the pwxccl.cfg file, and 2) You can remove the password from the command line after a successful cold start. If you specify the encryption password for a cold start and then need to restore the CDCT file later, you must enter the same encryption password in the RESTORE_CDCT command of the PWXUCDCT utility.

Option	Argument	Description
		To *not* encrypt PowerExchange Logger log files, do not enter an encryption password. - license=*directory*/*license_key_file* Specifies the full path and file name for any license key file that you want to use instead of the default license.key file. The alternative license key file must have a file name or path that is different from that of the default file. This alternative license key file takes precedence over any alternative license key file that you specify in the PWX_LICENSE environment variable. - specialstart={Y|N} Indicates whether to perform a special start of the PowerExchange Logger. A special start begins PowerExchange capture processing from the point in the change stream that you specify in the pwxccl.cfg file. This start point overrides the restart point from the CDCT file for the PowerExchange Logger run. A special start does not delete any content from the CDCT file. Use this parameter to skip beyond problematic parts in the source logs without losing captured data. For example, use a special start in the following situations: - You do not want the PowerExchange Logger to capture an upgrade of an Oracle catalog. In this case, stop the PowerExchange Logger before the upgrade. After the upgrade is complete, generate new sequence and restart tokens for the PowerExchange Logger based on the post-upgrade SCN. Enter these token values in the SEQUENCE_TOKEN and RESTART_TOKEN parameters in the pwxccl.cfg, and then special start the PowerExchange Logger. - You do not want the PowerExchange Logger to reprocess old, unavailable logs that were caused by outstanding UOWs that are not of CDC interest. In this case, stop the PowerExchange Logger. Edit the RESTART_TOKEN value to reflect the SCN of the earliest available log, and then perform a special start. If any of the outstanding UOWs that started before this restart point are of CDC interest, data might be lost. Valid values: - Y. Perform a special start of the PowerExchange Logger from the point in the change stream that is defined by the SEQUENCE_TOKEN and RESTART_TOKEN parameter values in the pwxccl.cfg configuration file. You must specify valid token values in the pwxccl.cfg file to perform a special start. These token values override the token values from the CDCT file. Ensure that the SEQUENCE_TOKEN value in the pwxccl.cfg is greater than or equal to the current sequence token from the CDCT file. Do not also specify the coldstart=Y parameter. If you do, the coldstart=Y parameter takes precedence. - N. Do not perform a special start. Perform a cold start or warm start as indicated by the coldstart parameter. Default is N. **Note:** In the config, cs, and license parameters, the full path is required only if the file does *not* reside in the installation

Option	Argument	Description
		directory. Include quotes around any path and file name that contains spaces.
-SvcPort -vp	service_port	Optional. Port on which the Logger Service listens for commands from the Service Manager.

DisplayAllLogger

Displays all messages that can be produced by the other PowerExchange Logger Service display commands, arranged by command.

The infacmd pwx DisplayAllLogger command displays the consolidated output for the following commands:

- DisplayCPULogger
- DisplayEventsLogger
- DisplayMemoryLogger
- DisplayRecordsLogger
- DisplayStatusLogger

The infacmd pwx DisplayAllLogger command uses the following syntax:

```
DisplayAllLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayAllLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

DisplayCPULogger

Displays the amount of CPU time, in microseconds, that the PowerExchange Logger Service spends for each phase of processing during the current logging cycle. Also includes the total CPU time for all Logger Service processing.

For example, the infacmd pwx DisplayCPULogger command might report the amount of CPU time that the Logger Service spent to complete the following actions:

- Read source data
- Write data to Logger Service log files
- Perform file switches
- Perform other processing, such as initialize and process commands

The infacmd pwx DisplayCPULogger command uses the following syntax:

```
DisplayCPULogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayCPULogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

DisplayEventsLogger

Displays events that the Controller, Command Handler, and Writer tasks for the PowerExchange Logger Service are waiting on. Also indicates if the Writer is processing data or is in a sleep state waiting for an event or timeout to occur.

The infacmd pwx DisplayEventsLogger command uses the following syntax:

```
DisplayEventsLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayEventsLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.

Option	Argument	Description
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

DisplayMemoryLogger

Displays memory use, in bytes, for each PowerExchange Logger Service task and subtask, with totals for the entire Logger Service process.

PowerExchange reports memory use for the following categories:

- Application. Memory that the Logger Service application requested for its own use.
- Total. Total memory in use for the Logger Service application and for related header overhead. This value fluctuates as PowerExchange allocates and frees memory during Logger Service processing.
- Maximum. The largest memory amount that has been recorded for the Total category up to the point in time when this command runs.

The infacmd pwx DisplayMemoryLogger command uses the following syntax:

```
DisplayMemoryLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayMemoryLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

DisplayRecordsLogger

Displays counts of change records that the PowerExchange Logger Service processed during the current processing cycle. If the Logger Service did not receive changes in the current cycle, displays counts of change records for the current set of Logger Service log files.

The infacmd pwx DisplayRecordsLogger command displays counts of records for each type of change record processed and for total records processed. Change record types include Delete, Insert, Update, and Commit.

Depending on whether the command displays counts for the current cycle or the current log files, the output includes all or some of the following types of information:

- Cycle. Counts of change records for the current Logger Service processing cycle. The Logger Service resets these counts to zero when the wait interval that is specified in the NO_DATA_WAIT2 parameter of the pwxccl.cfg file expires and no change data has been received.
- File. Counts of change records for the current set of PowerExchange log files. The Logger Service resets these counts to zero when a file switch occurs.

- Total. Counts of change records that the Logger Service received since it started. PowerExchange does not reset these counts to zero.

The infacmd pwx DisplayRecordsLogger command uses the following syntax:

```
DisplayRecordsLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayRecordsLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

displayStatsListener

Displays monitoring statistics for a PowerExchange Listener on Linux, UNIX, or Windows that the PowerExchange Listener Service manages. Also displays statistics for the client tasks and source or target connections that are associated with the Listener.

The command can print the following types of statistics, depending on the -type option that you specify:

- PowerExchange Listener summary statistics on memory usage, CPU processing time, and activity on behalf of client requests. These statistics include counts of client tasks, connections, messages sent and received, and bytes of data sent and received.
- Message and data volumes that client tasks sent and received for client requests, by task ID and access method. The message and data volumes are totals as of the time the statistics are generated.
- Information about the active tasks that are running under the Listener to process client requests. These statistics include the task start time, CPU processing time, access method, read or write mode, and associated process and session IDs. Also includes the port number and IP address of the client that issued the request to the PowerExchange Listener.

Important: For PowerExchange to collect PowerExchange Listener monitoring statistics, you must specify the MONITOR parameter in the STATS statement in the DBMOVER configuration file where the Listener runs.

The infacmd pwx displayStatsListener command uses the following syntax:

```
displayStatsListener

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> domain_host1:port domain_host2:port...]

[<-OSUser|-oun> OS_user_name]

[<-OSPassword|-oup> OS_password]

[<-OSEPassword|-ouep> OS_epassword]

[<-Type|-tp> report_type]
```

The following table describes infacmd pwx displayStatsListener options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.

Option	Argument	Description
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.
-type -tp	report_type	Optional. The type of monitoring statistics to report for the PowerExchange Listener and its client tasks and connections. The report_type must be one of the following values: - listener. For a specific PowerExchange Listener, reports memory usage, CPU processing time, total number of client tasks, active tasks, high-watermark tasks, maximum allowed tasks, total number of connections attempted, connections accepted, active connections, number of messages sent and received, and bytes of data sent and received. - accessmethods. For each access method of each active task, reports the number of rows read and written, bytes of data read and written, the source or target file name or data map file name depending on the access method, and the CPU processing time. - clients. For each active task, reports the task ID, status, access method, read or write mode, process and session IDs if available, CPU processing time, and start date and time. Also reports the port number and IP address of the client that issued the request for which the task was created. If the client is PowerCenter, reports the PowerCenter session ID and the application name for CDC. Default is listener. **Note:** In these reports, an access method can be a source type such as NRDB. A client task might be associated with multiple access methods: one for reading the source data, and one for mapping nonrelational data to a relational format.

DisplayStatusLogger

Displays the status of the Writer subtask for a PowerExchange Logger Service.

For example, the infacmd pwx DisplayStatusLogger command can report when the Writer completes the following actions:

- Initializes
- Reads or waits for source data
- Writes source data to a Logger Service log file
- Writes CDCT records during a file switch
- Deletes of expired CDCT records
- Shuts down

The infacmd pwx DisplayStatusLogger command uses the following syntax:

```
DisplayStatusLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx DisplayStatusLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

FileSwitchLogger

Closes open log files for the PowerExchange Logger Service and then switches to a new set of log files. If the open log files do not contain any data, the file switch does not occur.

Note: If you use continuous extraction mode, you generally do not need to complete file switches manually.

The infacmd pwx FileSwitchLogger command uses the following syntax:

```
FileSwitchLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx FileSwitchLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.

Option	Argument	Description
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

ListTaskListener

Displays information about each active task for the PowerExchange Listener Service, including the TCP/IP address, port number, application name, access type, and status.

The infacmd pwx ListTaskListener command uses the following syntax:

```
ListTaskListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx ListTaskListener options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

ShutDownLogger

Stops the PowerExchange Logger Service in a controlled manner. The command closes the Logger Service log files and then writes the latest restart position to the CDCT file.

Use this command to stop a PowerExchange Logger Service that is running in continuous mode.

During shutdown processing, the Logger Service completes the following actions:

- Closes open log files
- Writes updated information to the CDCT file, including restart and sequence tokens
- Closes the CAPI
- Stops the Writer and Command Handler subtasks
- Ends the pwxccl program
- Reports CPU usage

The infacmd pwx ShutDownLogger command uses the following syntax:

```
ShutDownLogger
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
```

The following table describes infacmd pwx ShutDownLogger options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.

StopTaskListener

Stops a PowerExchange Listener Service task based on an application name or task ID that you specify. During change data extraction, infacmd pwx StopTaskListener waits to stop the task until either the end UOW is encountered or the commit threshold is reached.

The infacmd pwx StopTaskListener command uses the following syntax:

```
StopTaskListener
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-OSUser|-oun> OS_user_name]
[<-OSPassword|-oup> OS_password]
[<-OSEPassword|-ouep> OS_epassword]
[<-applicationid|-a> appname]
[<-taskid|-t> taskid]
```

The following table describes infacmd pwx StopTaskListener options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-OSUser -oun	OS_user_name	Required if you enable operating system security. User name for the operating system. Enable operating system security as follows: - To require users to enter a valid operating system user ID and password on the command, specify 1 or 2 for the first parameter of the SECURITY statement in the DBMOVER configuration file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange uses operating system facilities on the target system to authenticate the user ID and password for use of the infacmd pwx program. - To authorize users to run specific infacmd pwx commands, specify 2 for the first parameter of the SECURITY statement and define AUTHGROUP and USER statements in the PowerExchange sign-on file on each Linux, UNIX, or Windows system that is the target of the command. PowerExchange checks the sign-on file to determine whether to allow the user ID supplied on the infacmd pwx program to run commands.
-OSPassword -oup	OS_password	Required if you specify a user name and do not specify an encrypted password. Password for the operating system. You can set a plain text password with the -p option or the environment variable INFA_DEFAULT_PWX_OSPASSWORD. If you set a password with both methods, the password set with the -p option takes precedence.

Option	Argument	Description
-OSEPassword -ouep	OS_epassword	Required if you specify a user name and do not specify a plain text password. Encrypted password for the operating system. You can set an encrypted password with the -e option or the environment variable INFA_DEFAULT_PWX_OSEPASSWORD. If you set a password with both methods, the password set with the -e option takes precedence.
-applicationid -a	appname	Required if you do not specify -taskid. Application name. The name for the active extraction process that you want to stop. The PWX-00712 message of the infacmd pwx listtaskListener command output displays this name.
-taskid -t	taskid	Required if you do not specify -application. Task ID of the Listener Service. The numeric identifier for the Listener Service task that you want to stop. **Tip:** To determine the name of the active task, issue the infacmd pwx listtaskListener command. In the command output, the name value in the PWX-00712 message shows the task ID.

UpgradeModels

Upgrades PowerExchange 9.0.1 nonrelational data objects. You must upgrade the data objects before you can use them.

The command displays the results of the upgrade, sorted by connection name and then schema and map name. You can run the UpgradeModels command multiple times if some objects are not upgraded the first time.

The command verifies that the data map is consistent with the nonrelational operations that were defined for it when the nonrelational object was imported. If discrepancies exist, the nonrelational operations are deleted and re-created to match the data map. You must modify any affected mappings or mapplets to use the re-created nonrelational operations.

The infacmd pwx UpgradeModels command uses the following syntax:

```
UpgradeModels

[<-DomainName|-dn> domain_name]

[<-UserName|-un> user_name]

[<-Password|-pd> password]

<-MrsServiceName|-msn> mrs_service_name

<-ConnectionName|-cn> connection_name

<-DataObjectSchemaName|ds> data_object_schema_name

<-DataObjectName|do> data_object_name

<-Preview|pr> preview
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-ServiceName|-sn> service_name]
```

The following table describes infacmd pwx UpgradeModels options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-MrsServiceName -msn	mrs_service_name	Required. Name of the Model Repository Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |
-ConnectionName -cn	connection_name	Required. Name of the connection that contains the nonrelational data objects that you want to upgrade. To specify all connections or all connections with the same initial name pattern, include the asterisk (*) wildcard character in double quotes, for example "*" or ABC"*".
-DataObjectSchemaName -ds	data_object_schema_name	Required. Name of the schema that contains the data maps of the nonrelational data objects that you want to upgrade. To specify all schemas or all schemas with the same initial name pattern, include the asterisk (*) wildcard character in double quotes, for example "*" or ABC"*".
-DataObjectName -do	data_object_name	Required. Name of the data map of the nonrelational data object that you want to upgrade. To specify all data maps or all data maps with the same initial name pattern, include the asterisk (*) wildcard character in double quotes, for example "*" or ABC"*".

Option	Argument	Description
-Preview -pr	preview	Required. Specify Y to preview the upgrade results without committing them or N to upgrade the objects. To verify that the command will run successfully, run the UpgradeModels command with Preview set to Y before performing the actual upgrade.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Optional. Name of the Listener Service. The command first uses the connection name to retrieve the specified data maps. If the attempt fails, the command uses the Listener Service name to retrieve the data maps. The name is not case sensitive. The name cannot exceed 128 characters or contain carriage returns, tabs, spaces, or the following characters: / * ? < > " |

UpdateListenerService

Updates the properties of a PowerExchange Listener Service.

The infacmd pwx UpdateListenerService command uses the following syntax:

```
UpdateListenerService
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

```
[<-LicenseName|-ln> license_name]
[<-NodeName|-nn> node_name]
[<-BackupNode|-bn> backup_node]
[<-StartParameters|-sp> start_parameters>]
[<-SvcPort|-sp> service_port]
```

The following table describes infacmd pwx UpdateListenerService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Listener Service.
-LicenseName -ln	license_name	Optional. License to assign to the service. If not already provided, required before you can enable the service.
-NodeName -nn	node_name	Required. Name of the node where you want the Listener Service to run.
-BackupNode -bn	backup_node	Optional. If the PowerCenter environment is configured for high availability, this option specifies the name of the backup node.

Option	Argument	Description
-StartParameters -sp	start_parameters	Optional. Parameters to include when you start the Listener Service. Separate the parameters with the space character. You can include the following parameters: - *node_name* Node name that identifies the Listener Service. This name must match the name in the LISTENER statement in the DBMOVER configuration file. - config=*directory* Specifies the full path and file name for any dbmover.cfg configuration file that you want to use instead of the default dbmover.cfg file. This alternative configuration file takes precedence over any alternative configuration file that you specify in the PWX_CONFIG environment variable. - license=*directory*/*license_key_file* Specifies the full path and file name for any license key file that you want to use instead of the default license.key file. The alternative license key file must have a file name or path that is different from that of the default file. This alternative license key file takes precedence over any alternative license key file that you specify in the PWX_LICENSE environment variable. **Note:** In the config and license parameters, you must provide the full path only if the file does *not* reside in the installation directory. Include quotes around any path and file name that contains spaces.
-SvcPort -sp	service_port	Optional. Port on which the Listener Service listens for commands from the Service Manager.

UpdateLoggerService

Updates the properties of a PowerExchange Logger Service.

The infacmd pwx UpdateLoggerService command uses the following syntax:

```
UpdateLoggerService
[<-DomainName|-dn> domain_name]
[<-UserName|-un> user_name]
[<-Password|-pd> password]
[<-SecurityDomain|-sdn> security_domain]
```

```
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

<-NodeName|-nn> node_name

[<-LicenseName|-ln> license_name]

[<-BackupNode|-bn> backup_node]

[<-StartParameters|-sp> start_parameters>]

[<-SvcPort|-sp> service_port]
```

The following table describes infacmd pwx UpdateLoggerService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Logger Service.
-NodeName -nn	node_name	Required. Name of the node where you want the Logger Service to run.
-LicenseName -ln	license_name	License to assign to the service. If not already provided, required before you can enable the service.
-BackupNode -bn	backup_node	Optional. If the PowerCenter environment is configured for high availability, this option specifies the name of the backup node.

Option	Argument	Description
-StartParameters -sp	start_parameters	Optional. Parameters to include when you start the Logger Service. Separate the parameters with the space character. You can include the following parameters: - coldstart={Y|N} Indicates whether to cold start or warm start the Logger Service. Enter Y to cold start the Logger Service. If the CDCT file contains log records, the Logger Service deletes these records. Enter N to warm start the Logger Service from the restart point that is indicated in the CDCT file. Default is N. - config=*directory/pwx_config_file* Specifies the full path and file name for any dbmover.cfg configuration file that you want to use instead of the default dbmover.cfg file. This alternative configuration file takes precedence over any alternative configuration file that you specify in the PWX_CONFIG environment variable. - cs=*directory/pwxlogger_config_file* Specifies the path and file name for the Logger Service configuration file. You can also use the cs parameter to specify a Logger Service configuration file that overrides the default pwxccl.cfg file. The override file must have a path or file name that is different from that of the default file. - encryptepwd=*encrypted_password* A password in encrypted format for enabling the encryption of PowerExchange Logger log files. With this password, the PowerExchange Logger can generate a unique encryption key for each Logger log file. The password is stored in the CDCT file in encrypted format. For security purposes, the password is not stored in CDCT backup files and is not displayed in the CDCT reports that you can generate with the PowerExchange PWXUCDCT utility. If you specify this parameter, you must also specify coldstart=Y. If you specify this parameter and also specify the ENCRYPTEPWD parameter in the PowerExchange Logger configuration file, pwxccl.cfg, the parameter in the configuration file takes precedence. If you specify this parameter and also specify the ENCRYPTPWD parameter in the PowerExchange Logger configuration file, an error occurs. You can set the AES algorithm to use for log file encryption in the ENCRYPTOPT parameter of the pwxccl.cfg file. The default is AES128. **Tip:** For optimal security, Informatica recommends that you specify the encryption password when cold starting the PowerExchange Logger rather than in the pwxccl.cfg configuration file. This practice can reduce the risk of malicious access to the encryption password for the following reasons: 1) The encryption password is not stored in the pwxccl.cfg file, and 2) You can remove the password from the command line after a successful cold start. If you specify the encryption password for a cold start and then need to restore the CDCT file later, you must

Option	Argument	Description
		enter the same encryption password in the RESTORE_CDCT command of the PWXUCDCT utility. To *not* encrypt PowerExchange Logger log files, do not enter an encryption password. - license=*directory/license_key_file* Specifies the full path and file name for any license key file that you want to use instead of the default license.key file. The alternative license key file must have a file name or path that is different from that of the default file. This alternative license key file takes precedence over any alternative license key file that you specify in the PWX_LICENSE environment variable. - specialstart={Y|N} Indicates whether to perform a special start of the PowerExchange Logger. A special start begins PowerExchange capture processing from the point in the change stream that you specify in the pwxccl.cfg file. This start point overrides the restart point from the CDCT file for the PowerExchange Logger run. A special start does not delete any content from the CDCT file. Use this parameter to skip beyond problematic parts in the source logs without losing captured data. For example, use a special start in the following situations: - You do not want the PowerExchange Logger to capture an upgrade of an Oracle catalog. In this case, stop the PowerExchange Logger before the upgrade. After the upgrade is complete, generate new sequence and restart tokens for the PowerExchange Logger based on the post-upgrade SCN. Enter these token values in the SEQUENCE_TOKEN and RESTART_TOKEN parameters in the pwxccl.cfg, and then special start the PowerExchange Logger. - You do not want the PowerExchange Logger to reprocess old, unavailable logs that were caused by outstanding UOWs that are not of CDC interest. In this case, stop the PowerExchange Logger. Edit the RESTART_TOKEN value to reflect the SCN of the earliest available log, and then perform a special start. If any of the outstanding UOWs that started before this restart point are of CDC interest, data might be lost. Valid values: - Y. Perform a special start of the PowerExchange Logger from the point in the change stream that is defined by the SEQUENCE_TOKEN and RESTART_TOKEN parameter values in the pwxccl.cfg configuration file. You must specify valid token values in the pwxccl.cfg file to perform a special start. These token values override the token values from the CDCT file. Ensure that the SEQUENCE_TOKEN value in the pwxccl.cfg is greater than or equal to the current sequence token from the CDCT file. Do not also specify the coldstart=Y parameter. If you do, the coldstart=Y parameter takes precedence. - N. Do not perform a special start. Perform a cold start or warm start as indicated by the coldstart parameter. Default is N.

Option	Argument	Description
		Note: In the config, cs, and license parameters, you must provide the full path only if the file does *not* reside in the installation directory. Include quotes around any path and file name that contains spaces.
-SvcPort -sp	service_port	Port on which the Logger Service listens for commands from the Service Manager.

CHAPTER 30

infacmd roh Command Reference

This chapter includes the following topics:

listProcessProperties

Lists the REST Operations Hub process properties.

The infacmd roh listProcessProperties command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh listProcessProperties options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user-name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	Domain gateway host:port	Required if the gateway connectivity information in the domains.infa file is out of date. Enter the host name and port number for the gateway node in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listReverseProxyServerOptions

Lists the reverse proxy server properties.

The infacmd roh listReverseProxyServerOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-NodeName|-nn> Node_name]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh listReverseProxyServerOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-NodeName -nn	Node_name	Required. Node where the service process runs.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listServiceProcessOptions

Lists the REST Operations Hub Service Process properties.

The infacmd roh listServiceProcessOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-NodeName|-nn> Node_name]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh listServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-NodeName -nn	Node_name	Required. Node where the service process runs.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listServiceOptions

Lists the REST Operations Hub Service properties.

The infacmd roh listServiceOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh listServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

updateReverseProxyServerOptions

Updates the reverse proxy server properties.

The infacmd roh updateReverseProxyServerOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-NodeName|-nn> Node_name

 [<-ServiceProcessReverseProxyServerOptions|-so> option_name=value ...
(EnableReverseProxyServer, URLScheme, httpPortForRPS, httpsPortForRPS,
ReverseProxyServerSSLCertificate,
ReverseProxyServerSSLCertificateKey, ReverseProxyServerSSLCertificatePassPhrasePath,
VerifyIncomingClients,
SSLClientCertificatePathForIncomingClients, SSLCertificatePathForUpstreamServer,
SSLCertificateKeyForUpstreamServer, SSLCertificatePassPhrasePathForUpstreamServer)

Information regarding ReverseProxyServer https mode...(ReverseProxyServerSSLCertificate,
ReverseProxyServerSSLCertificateKey, SSLClientCertificatePathForIncomingClients,
VerifyIncomingClients are applicable when https mode is enabled)]

[<-Options|-o options]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh updateReverseProxyServerOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-NodeName -nn	Node_name	Required. Node where the service process runs.
-ServiceProcessReverseProxyServerOptions -so	option_name=value ...	Optional. Service Process properties that define how the reverse proxy server runs.
-Options -o	option	Optional. Enter each custom property option separated by a space. Use the prefix `RPS:` with name and value pair. For example, `RPS:<custom_property>=<custom_value>`.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

updateServiceProcessOptions

Updates REST Operations Hub Service process properties in a domain.

The infacmd roh updateServiceProcessOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

<-NodeName|-nn> Node_name

[<-ServiceOptions|-so> option_name=value ...(httpPort, httpsPort, keystoreFile,
keystorePass, SSLProtocol)]

[<-Options|-o options]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd roh updateServiceProcessOption options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-NodeName -nn	Node_name	Required. Node where the service process runs.
-ServiceOptions -so	option_name=value ...	Optional. Service properties that define how the REST Operations Hub Service runs.
-Options -o	option	Optional. Enter each custom property option separated by a space. Use the prefix `ROH:` with name and value pair. For example, `ROH:<custom_property>=<custom_value>`.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

updateServiceOptions

Updates the REST Operations Hub Service properties.

The infacmd roh updateServiceOptions command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

[<-NodeName|-nn> node_name|<-GridName|-gn> grid_name]

[<-Options|-o options]
```

The following table describes the infacmd roh updateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-NodeName -nn	Node_name	Required. Node name that belongs to a grid where the service process runs.
-GridName -gn	grid_name	Required. Name of the grid.
-Gateway -hp	gateway_host1:port gateway_host2:port...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	option	Optional. Enter each custom property option separated by a space. Use prefix `RPS:` to set reverse proxy server or `ROH:` to set Rest Operations Hub custom property. For example, `RPS:<custom_property>=<custom_value>`.

CHAPTER 31

infacmd rms Command Reference

This chapter includes the following topics:

ListComputeNodeAttributes

Lists the compute node attributes that have been overridden for the specified node or for all nodes. Use the infacmd rms SetComputeNodeAttributes command to override compute node attributes.

The default values for the attributes are the actual number of cores and memory available on the machine. If the infacmd rms ListComputeNodeAttributes command does not list a value for an attribute, then the Resource Manager Service is using the default values.

The infacmd rms ListComputeNodeAttributes command uses the following syntax:

```
ListComputeNodeAttributes
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-NodeName|-nn> node_name]
[<-ServiceName|-sn> service_name]
```

The following table describes infacmd rms ListComputeNodeAttributes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-NodeName -nn	node_name	Optional. Name of the compute node that you want to list the attributes for. If you omit the option, the command lists the attributes set for all compute nodes in the domain.
-ServiceName -sn	service_name	Optional. Enter Resource_Manager_Service.

ListServiceOptions

Lists the properties for the Resource Manager Service.

The infacmd rms ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd rms ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Optional. Enter Resource_Manager_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

SetComputeNodeAttributes

Overrides the compute node attributes for the specified node.

The default values for the attributes are the actual number of cores and memory available on the machine. To reset an option to its default value, specify -1 as the value.

The infacmd rms SetComputeNodeAttributes command uses the following syntax:

```
SetComputeNodeAttributes
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-NodeName|-nn> node_name
[<-MaxCores|-mc> max_number_of_cores_to_allocate]
[<-MaxMem|-mm> max_memory_in_mb_to_allocate]
[<-ServiceName|-sn> service_name]
```

The following table describes infacmd rms SetComputeNodeAttributes options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-NodeName -nn	node_name	Required. Name of the compute node that you want to set attributes for.
-MaxCores -mc	max_number_of_cores_to_allocate	Optional. Maximum number of cores that the Resource Manager Service can allocate for jobs that run on the compute node. A compute node requires at least five available cores to initialize a container to start a DTM process. If any compute node assigned to the grid has fewer than five cores, then that number is used as the minimum number of cores required to initialize a container. By default, the maximum number of cores is the actual number of cores available on the machine.

Option	Argument	Description
-MaxMem -mm	max_memory_in_mb_to_allocate	Optional. Maximum amount of memory in megabytes that the Resource Manager Service can allocate for jobs that run on the compute node. A compute node requires at least 2.5 GB of memory to initialize a container to start a DTM process. By default, the maximum memory is the actual memory available on the machine.
-ServiceName -sn	service_name	Optional. Enter Resource_Manager_Service.

UpdateServiceOptions

Updates Resource Manager Service properties. Run this command to configure the primary and back-up nodes for the Resource Manager Service.

You can change the properties while the service is running, but you must recycle the service for the changed properties to take effect.

The infacmd rms UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
[<-ServiceName|-sn> service_name]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options|-o> options]
[<-NodeName|-nn> primary_node_name]
[<-BackupNodes|-bn> backup_node_name1,backup_node_name2,...]
```

The following table describes infacmd rms UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Optional. Enter Resource_Manager_Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Optional. Enter each option separated by a space.

Option	Argument	Description
-NodeName -nn	primary_node_name	Optional. Primary node on which the Resource Manager Service runs.
-BackupNodes -bn	backup_node_name1,backup_node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable.

Resource Manager Service Options

Use the Resource Manager Service options with the infacmd rms UpdateServiceOptions command.

Enter Resource Manager Service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Resource Manager Service options:

Option	Description
ResourceManagerServiceOptions.Log_Level	Level of error messages that the Resource Manager Service writes to the service log. Choose one of the following message levels: Fatal, Error, Warning, Info, Trace, or Debug.

CHAPTER 32

infacmd rtm Command Reference

This chapter includes the following topics:

DeployImport

Imports content from an application file to the database that is read by the Model repository.

The infacmd rtm DeployImport command uses the following syntax:

```
DeployImport
<-DomainName|-dn> Domain name
<-UserName|-un> User name
<-Password|-pd> Password
<-securityDomain|-sdn> Security domain
[<-Gateway|-hp> Domain gateway host:port]
[<-NodeName|-nn> Node name]
<-DataIntegrationService|-ds> Data Integration Service name
<-CodePage|-cp> Code page
<-Folder|-f> The folder to import from
<-MetadataFile|-mf> Metadata file
```

The following table describes infacmd rtm DeployImport options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-securityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	Domain gateway host:port	Required if the gateway connectivity information in the domains.infa file is out of date. Enter the host name and port number for the gateway node in the domain. Use the following syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Node name	Optional. Name of the gateway node for the Model Repository Service.
-DataIntegrationService -ds	Data Integration Service name	Required. Data Integration Service name.
-CodePage -cp	Code page	Required. Code page for the reference data to import.

Option	Argument	Description
-Folder -f	The folder to import from	Required. Path to the folder that contains the files to import. You run the DeployImport command on the machine that stores the folder. The folder option describes a path on the machine that runs the command.
-MetadataFile -mf	Metadata file	Required. Full name and path for the application file that you apply the command to.

Export

Exports data from reference tables. You can export reference table objects or just the data. You can export data from managed and unmanaged reference tables.

Define the export data with one of the following options:

- ProjectFolder. Name of a project or folder to export.
- MetadataFile. Name of a metadata.xml file that refers to the reference tables to export.
- ObjectList. Full path to a text file that contains a list of objects to export.

When you configure an object list, create a text file that contains a list of objects with the following syntax:

```
ProjectName/FolderName/reference_table_object1
ProjectName/FolderName/reference_table_object2
ProjectName/FolderName/reference_table_object3
```

Note: You must configure each path in the object list to have slashes. Do not use backslash in the path.

The infacmd rtm Export command uses the following syntax:

```
Export

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-SecurityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-RepositoryService|-rs> Model Repository Service name

<-CodePage|-cp> Code Page

<-Folder|-f> The folder to export to

[<-ObjectList|-ol> List of Obects to export]

[<-ProjectFolder|-pf> Name of the project folder to export]

[<-metadataFile|-mf> Metadata file]

[<-Recursive|-r> Include subfolders when exporting project folder]

[<-SkipDatGeneration|-sdg> Skip Data Generation]
```

The following table describes infacmd rtm Export options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	Domain gateway hostname:portnumber	Required if the gateway connectivity information in the domains.infa file is out of date. Enter the host name and port number for the gateway node in the domain. Use the following syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Node name	Optional. Name of the gateway node for the Model Repository Service.
-RepositoryService -rs	Model Repository Service name	Model Repository Service name.
-CodePage -cp	Code Page	Required. Code page for the reference data.
-Folder -f	The folder to export to	Required. Target location for the export file.

Option	Argument	Description
-ObjectList -ol	List of Obects to export	Fully qualified file name containing the list of reference table objects. Do not configure this option with the ProjectFolder or metadataFile option.
-ProjectFolder -pf	Name of the project folder to export	Name of the project and folder to export. Use the following syntax: `ProjectName/FolderName` Do not configure with the metadataFile or ObjectList option.
-metadataFile -mf	Metadata file	Required for object export. Full path and name for a metadata.xml file that you want to apply the command to. Exports all reference tables that the metadata. xml file contains. Do not configure this option with the ProjectFolder or ObjectList option.
-Recursive -r	Include subfolders when exporting project folder	Optional. Use with the ProjectFolder option. Export more than one level of object. Default is not recursive.
-SkipDatGeneration -sdg	Skip Data Generation	Optional. Writes a .dat file that describes the reference table structure to the directory set in the folder property. The reference table import process does not use this file. Default is False.

Import

Performs a metadata and data import from object export files. Imports reference table metadata into the Model repository and imports the data into the reference data database. Also imports reference data without the metadata.

Before you import reference table data, the destination project must exist in the Model repository.

The infacmd rtm Import command uses the following syntax:

```
Import

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

<-securityDomain|-sdn> Security domain

[<-Gateway|-hp> Domain gateway host:port]

[<-NodeName|-nn> Node name]

<-RepositoryService|-rs> Model Repository Service name

<-CodePage|-cp> Code page
```

```
<-ConflictResolution|-cr> Conflict resolution

<-ImportType|-it> Import type

<-Folder|-f> The folder to import from

[<-FileName|-fn> Required only for importing a single dictionary]

[<-MetadataFile|-mf> Required only for Object import]

[<-ProjectFolder|-pf> Name of the project folder to import into]

[<-NotRecursive|-nr> Don't include subfolders]
```

The following table describes infacmd rtm Import options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable *INFA_DEFAULT_DOMAIN*. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-securityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	Domain gateway host:port	Required if the gateway connectivity information in the domains.infa file is out of date. Host name and port number for the gateway node in the domain. Use the following syntax: `gateway_hostname:HttpPort`
-NodeName -nn	Node name	Optional. Name of the gateway node for the Model Repository Service.

Option	Argument	Description
-RepositoryService -rs	Model Repository Service name	Required. Model Repository Service name.
-CodePage -cp	Code page	Required. Code page for the reference data.
-ConflictResolution -cr	Conflict resolution	Required. Defines the behavior when a name conflict occurs. Enter one of the following arguments: - Replace. Replace the current reference table object with the object that you import. - Rename. Create a reference table object with a different name. - Skip. Do not import the reference table. **Note:** The Replace argument specifies the resolution policy for the reference table object and not for the underlying table in the reference data database. When you use the Replace argument, the import command creates a table for the data that the new object represents in the reference data database. The command does not drop the table that the previous object identified. To remove unused tables from the reference data database, run the infacmd cms Purge command.
-ImportType -it	Import type	Required. The type of content to import. Enter MetadataAndData for metadata and data import.
-Folder -f	The folder to import from	Required for metadata and data import. Full path to the folder that contains the reference data file you want to import.
-FileName -fn	Required only for importing a single dictionary	Required for metadata and data import if you are importing data from a single file. Name of the file that contains the reference data you want to import. The file name is relative to the folder path.
-MetadataFile -mf	Required only for Object import	Required when you import reference data values only. Full path and name for the metadata.xml file that you apply the command to. The metadata.xml file contains the metadata associated with the reference data values. Do not use with the ProjectFolder option.
-ProjectFolder -pf	Name of the project folder to import into	Required when you import reference data and metadata. Name of the Model repository project that you want to import into. Do not use with the MetadataFile option.
-NotRecursive -nr	- Don't include subfolders	Optional. Use with metadata and data import. Import one level of objects only. Default is recursive.

CHAPTER 33

infacmd sch Command Reference

This chapter includes the following topics:

CreateSchedule

Creates a schedule for deployed mappings and deployed workflows.

The infacmd sch CreateSchedule command uses the following syntax:

```
CreateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
```

```
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleDescription|-scd> schedule_description]
<-Recurrence|-r> once|daily|weekly|monthly
<-StartTime|-st> yyyy-MM-dd HH:mm
[<-EndTime|-et> yyyy-MM-dd HH:mm]
[<-TimeZone|-tz> time_zone]
[<-DailyRunEvery|-dre> daily_run_every]
[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]
[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]
[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]
[<-RepeatCount|-rc> repeat_count]
[<-RunnableObjects|-ro> runnable_objects]
[<-Status|-ss> SCHEDULED|SUSPENDED]
[<-RunNow|-rn> true|false]
```

To configure multiple values for an argument, separate the values with commas.

The following table describes infacmd sch CreateSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Required. Name of the schedule. The schedule name is case sensitive.
-Description -scd	schedule_description	Optional. Schedule description.

Option	Argument	Description
-Recurrence -r	once|daily|weekly|monthly	Required. Specify whether the schedule runs once or recurs.
-StartTime -st	yyyy-MM-dd HH:mm	Required. Date and time that the recurrence starts.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Date and time that the recurrence ends.
-TimeZone -tz	timezone	Optional. Time zone for the schedule start time. To configure the time zone, you can enter the time zone ID number or the Olson Database ID. Default is locale of the client machine.
-DailyRunEvery -dre	daily_run_every	Optional. Run the schedule on an interval. The following list describes the options that you can configure: - minute(s). Run the schedule daily every n minutes. - hour(s). Run the schedule daily every n hours. - day(s). Run the schedule every n days. - week(s). Run the schedule every n weeks. - month(s). Run the schedule every n months. - year(s). Run the schedule every n years. - FIRST. Run the schedule every first n day of the month. Use the -rdwm option to specify the day or days of the week. - SECOND. Run the schedule every second n day of the month. Use the -rdwm option to specify the day or days of the week. - THIRD. Run the schedule every third n day of the month. Use the -rdwm option to specify the day or days of the week. - FOURTH. Run the schedule every fourth n day of the month. Use the -rdwm option to specify the day or days of the week. - LAST. Run the schedule every last n day of the month. Use the -rdwm option to specify the day or days of the week.
-RunDaysOfWeek -rdw	mon|tue|wed|thu|fri|sat|sun	Optional. Run the schedule on certain days of the week.
-RunDayOfWeekMonth -rdwm	monday|tuesday| wednesday|thursday|friday| saturday|sunday	Optional. Run the schedule on certain days of the week every month. Use the -dre options to run the schedule every first, second, third, fourth, or last n day of the month.
-RunDayofMonth -rdm	1-30|LAST_DAY_OF_MONTH	Optional. Run the schedule on day n of the month.
-RepeatCount -rc	repeat_count	Optional. End the recurrence after a number of runs instead of on a date.

Option	Argument	Description

-RunnableObjects
-ro
	runnableObjects	Optional. Objects that you would like to schedule. Enter the object type, followed by the path to the object on the Data Integration Service. For example:
		`"workflow://DIS_hw2288/App_DMPA_run/wf_run_DMPA"`
		Optionally, use the following arguments to configure a parameter file, parameter set, run as user, or operating system profile for the object:
		- parameterFilePath=PATH_TO_PARAMETER_FILE
		- parameterSet=PARAMETER_SET_NAME
		- runAsUser=USER_NAME
		&runAsUserSecurityDomain=SECURITY_DOMAIN
		&runAsUserPassword=PASSWORD
		- osProfileName=OS_PROFILE_NAME
		For example:
		`"workflow:DIS_1234/Application_workflow/Workflow_abc?`
		`parameterFilePath=C://Informatica/Parameter Files/Parameter.xml`
		`&runAsUser=Administrator`
		`&runAsUserSecurityDomain=Native`
		`&runAsUserPassword=Administrator"`

-Status -ss	SCHEDULED|PAUSED	Optional. Create the schedule in scheduled or paused state.
-RunNow -rn	true|false	Run the schedule immediately.

Valid Time Zone Parameters

When you enter the Time Zone parameter, you can enter a time zone ID or you can enter the Olson Database ID.

The following table lists the values you can enter for the time zone:

ID	Olson Database ID	Name
0	Etc/GMT+12	(UTC-12:00) International Date Line West
110	Etc/GMT+11	(UTC-11:00) Coordinated Universal Time-11
200	Pacific/Honolulu	(UTC-10:00) Hawaii
300	America/Anchorage	(UTC-09:00) Alaska
410	America/Santa_Isabel	(UTC-08:00) Baja California
400	America/Los_Angeles	(UTC-08:00) Pacific Time (US & Canada)

ID	Olson Database ID	Name
520	America/Phoenix	(UTC-07:00) Arizona
510	America/Chihuahua	(UTC-07:00) Chihuahua, La Paz, Mazatlan
500	America/Denver	(UTC-07:00) Mountain Time (US & Canada)
610	America/Guatemala	(UTC-06:00) Central America
620	America/Chicago	(UTC-06:00) Central Time (US & Canada)
630	America/Mexico_City	(UTC-06:00) Guadalajara, Mexico City, Monterrey
600	America/Regina	(UTC-06:00) Saskatchewan
710	America/Bogota	(UTC-05:00) Bogota, Lima, Quito, Rio Branco
700	America/New_York	(UTC-05:00) Eastern Time (US & Canada)
720	America/Indianapolis	(UTC-05:00) Indiana (East)
840	America/Caracas	(UTC-04:30) Caracas
850	America/Asuncion	(UTC-04:00) Asuncion
800	America/Halifax	(UTC-04:00) Atlantic Time (Canada)
810	America/Cuiaba	(UTC-04:00) Cuiaba
830	America/La_Paz	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
900	America/St_Johns	(UTC-03:30) Newfoundland
910	America/Sao_Paulo	(UTC-03:00) Brasilia
940	America/Cayenne	(UTC-03:00) Cayenne, Fortaleza
950	America/Buenos_Aires	(UTC-03:00) City of Buenos Aires
920	America/Godthab	(UTC-03:00) Greenland
930	America/Montevideo	(UTC-03:00) Montevideo
820	America/Santiago	(UTC-03:00) Santiago
1010	Etc/GMT+2	(UTC-02:00) Coordinated Universal Time-02
1100	Atlantic/Azores	(UTC-01:00) Azores
1110	Atlantic/Cape_Verde	(UTC-01:00) Cabo Verde Is.
1220	Africa/Casablanca	(UTC) Casablanca
1230	Etc/GMT	(UTC) Coordinated Universal Time

ID	Olson Database ID	Name
1200	Europe/London	(UTC) Dublin, Edinburgh, Lisbon, London
1210	Atlantic/Reykjavik	(UTC) Monrovia, Reykjavik
1340	Europe/Berlin	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
1300	Europe/Budapest	(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
1320	Europe/Paris	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
1310	Europe/Warsaw	(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
1330	Africa/Lagos	(UTC+01:00) West Central Africa
1350	Africa/Windhoek	(UTC+01:00) Windhoek
1450	Asia/Amman	(UTC+02:00) Amman
1430	Europe/Bucharest	(UTC+02:00) Athens, Bucharest
1460	Asia/Beirut	(UTC+02:00) Beirut
1410	Africa/Cairo	(UTC+02:00) Cairo
1480	Asia/Damascus	(UTC+02:00) Damascus
1470	Africa/Johannesburg	(UTC+02:00) Harare, Pretoria
1420	Europe/Kiev	(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
1490	Europe/Istanbul	(UTC+02:00) Istanbul
1440	Asia/Jerusalem	(UTC+02:00) Jerusalem
1530	Europe/Kaliningrad	(UTC+02:00) Kaliningrad (RTZ 1)
1510	Asia/Baghdad	(UTC+03:00) Baghdad
1500	Asia/Riyadh	(UTC+03:00) Kuwait, Riyadh
1400	Europe/Minsk	(UTC+03:00) Minsk
1540	Europe/Moscow	(UTC+03:00) Moscow, St. Petersburg, Volgograd (RTZ 2)
1520	Africa/Nairobi	(UTC+03:00) Nairobi
1550	Asia/Tehran	(UTC+03:30) Tehran
1600	Asia/Dubai	(UTC+04:00) Abu Dhabi, Muscat
1610	Asia/Baku	(UTC+04:00) Baku

ID	Olson Database ID	Name
1650	Indian/Mauritius	(UTC+04:00) Port Louis
1640	Asia/Tbilisi	(UTC+04:00) Tbilisi
1620	Asia/Yerevan	(UTC+04:00) Yerevan
1630	Asia/Kabul	(UTC+04:30) Kabul
1710	Asia/Tashkent	(UTC+05:00) Ashgabat, Tashkent
1700	Asia/Yekaterinburg	(UTC+05:00) Ekaterinburg (RTZ 4)
1750	Asia/Karachi	(UTC+05:00) Islamabad, Karachi
1720	Asia/Calcutta	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
1730	Asia/Colombo	(UTC+05:30) Sri Jayawardenepura
1740	Asia/Katmandu	(UTC+05:45) Kathmandu
1800	Asia/Almaty	(UTC+06:00) Astana
1830	Asia/Dhaka	(UTC+06:00) Astana
1810	Asia/Novosibirsk	(UTC+06:00) Novosibirsk (RTZ 5)
1820	Asia/Rangoon	(UTC+06:30) Yangon (Rangoon)
1910	Asia/Bangkok	(UTC+07:00) Bangkok, Hanoi, Jakarta
1900	Asia/Krasnoyarsk	(UTC+07:00) Krasnoyarsk (RTZ 6)
2000	Asia/Shanghai	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
2010	Asia/Irkutsk	(UTC+08:00) Irkutsk (RTZ 7)
2020	Asia/Singapore	(UTC+08:00) Kuala Lumpur, Singapore
2040	Australia/Perth	(UTC+08:00) Perth
2030	Asia/Taipei	(UTC+08:00) Taipei
2050	Asia/Ulaanbaatar	(UTC+08:00) Ulaanbaatar
2110	Asia/Tokyo	(UTC+09:00) Osaka, Sapporo, Tokyo
2100	Asia/Seoul	(UTC+09:00) Seoul
2120	Asia/Yakutsk	(UTC+09:00) Yakutsk (RTZ 8)
2140	Australia/Adelaide	(UTC+09:30) Adelaide
2130	Australia/Darwin	(UTC+09:30) Darwin

ID	Olson Database ID	Name
2210	Australia/Brisbane	(UTC+10:00) Brisbane
2200	Australia/Sydney	(UTC+10:00) Canberra, Melbourne, Sydney
2240	Pacific/Port_Moresby	(UTC+10:00) Guam, Port Moresby
2220	Australia/Hobart	(UTC+10:00) Hobart
2310	Asia/Magadan	(UTC+10:00) Magadan
2230	Asia/Vladivostok	(UTC+10:00) Vladivostok, Magadan (RTZ 9)
2300	Pacific/Guadalcanal	(UTC+11:00) Solomon Is., New Caledonia
2410	Pacific/Auckland	(UTC+12:00) Auckland, Wellington
2430	Etc/GMT-12	(UTC+12:00) Coordinated Universal Time+12
2400	Pacific/Fiji	(UTC+12:00) Fiji
2500	Pacific/Tongatapu	(UTC+13:00) Nuku'alofa
2510	Pacific/Apia	(UTC+13:00) Samoa

DeleteSchedule

Deletes one or more schedules that the Scheduler Service manages.

The infacmd sch DeleteSchedule command uses the following syntax:

```
DeleteSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

The following table describes infacmd sch DeleteSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Name of the schedule that you want to delete.

ListSchedule

Lists schedules or scheduled objects that the Scheduler Service manages. The command returns schedules or scheduled objects that meet all of the entered options.

The infacmd sch ListSchedule command uses the following syntax:

```
ListSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ScheduleName|-scn> schedule_name]
[<-Description|-scd> description]
[<-RunnableObjects|-ro> runnable_objects]
[<-ScheduleStatus|-ss> created|scheduled|paused|complete]
[<-NumberOfFireTimes|-n> number_of_fire_times]
[<-MaxResults|-m> max_results]
```

The following table describes infacmd isp ListSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
ScheduleName -scn	schedule_name	Optional. Returns schedules with n name.
Description -scd	description	Optional. Returns schedules with n description.

RunnableObjects
-ro
	runnableObjects	Optional. Lists the schedules that run an object. Enter the object type and path on the Data Integration Service in the following format:
		`'{mapping|workflow}://dis_name/app_name/obj_name'`
		For example,
		`'mapping://dis_demo/app_demo/mapping_demo'`

ScheduleStatus -ss	created|scheduled|paused|completed	Optional. Returns schedules with n status.
NumberOfFireTimes -n	number_of_fire_times	Optional. Returns schedules that have run n number of times.
Maxresults -m	max_results	Optional. Maximum number of schedules you would like the command to return.

listScheduleOfUser

Lists all the scheduled jobs associated with a user.

The infacmd sch listScheduleOfUser command uses the following syntax:

```
listScheduleOfUser
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-ScheduleUserName|-sun> schedules_of_user_name]
```

The following table describes infacmd sch listScheduleOfUser options and arguments:

Option	Argument	Description
-UserName -un	user_name	User name to connect to the Informatica domain.
-Password -pd	password	Password for the user.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleUserName -sun	schedule_user_name	User name associated to the scheduled job. If you do not specify this value, the schedules are listed for the user specified in the -UserName option.

ListServiceOptions

Returns a list of the properties that are configured for the Scheduler Service.

The infacmd sch ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
```

```
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd sch ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-ServiceName -sn	service_name	Required. Enter Scheduler_Service.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

ListServiceProcessOptions

Returns a list of the properties that are configured for a Scheduler Service process.

The infacmd sch ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-NodeName|-nn> node_name
```

The following table describes infacmd sch ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-ServiceName -sn	service_name	Required. Enter Scheduler_Service.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-NodeName -nn	node_name	Name of the node on which the service process runs.

PauseAll

Pauses all schedules that the Scheduler Service manages. When you pause the schedules, the objects that run on the schedules stop running until you resume the schedules.

The infacmd sch PauseAll command uses the following syntax:

```
PauseAll
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd sch PauseAll options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

PauseSchedule

Pauses a schedule that the Scheduler Service manages. When you a pause a schedule, the objects that run on the schedule stop running until you resume the schedule.

The infacmd sch PauseSchedule command uses the following syntax:

```
PauseSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

The following table describes infacmd sch PauseSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain

Option	Argument	Description
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Name of the schedule that you want to pause. The schedule name is case sensitive.

ResumeAll

Resumes all paused schedules that the Scheduler Service manages.

The infacmd sch ResumeAll command uses the following syntax:

```
ResumeAll
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd sch ResumeAll options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.

Option	Argument	Description
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

ResumeSchedule

Resumes a paused schedule that the Scheduler Service manages.

The infacmd sch ResumeSchedule command uses the following syntax:

```
ResumeSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
```

The following table describes infacmd sch ResumeSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
ScheduleName -scn	schedule_name	Name of the paused schedule that you want to resume.

UpdateSchedule

Updates a schedule that the Scheduler Service manages. Update a schedule to change the start or end times, recurrence, or objects that run on the schedule. To view the current options, run the infacmd sch ListSchedule command.

The infacmd sch UpdateSchedule command uses the following syntax:

```
UpdateSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleDescription|-scd> schedule_description]
<-Recurrence|-r> once|daily|weekly|monthly
<-StartTime|-st> yyyy-MM-dd HH:mm
[<-EndTime|-et> yyyy-MM-dd HH:mm]
[<-TimeZone|-tz> time_zone]
[<-DailyRunEvery|-dre> daily_run_every]
[<-RunDaysOfWeek|-rdw> mon|tue|wed|thu|fri|sat|sun]
[<-RunDayOfWeekMonth|-rdwm> monday|tuesday|wednesday|thursday|friday|saturday|sunday]
[<-RunDayOfMonth|-rdm> 1-30|LAST_DAY_OF_MONTH]
[<-RepeatCount|-rc> repeat_count]
[<-RemoveRunnableObjects|-rro> removeRunnableObjects]
[<-AddRunnableObjects|-aro> addRunnableObjects]
```

To configure multiple values for an argument, separate the values with commas.

The following table describes infacmd sch UpdateSchedule options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Required. Name of the schedule. The schedule name is case sensitive.
-Description -scd	schedule_description	Optional. Schedule description.
-Recurrence -r	once|daily|weekly|monthly	Required. Specify whether the schedule runs once or recurs.
-StartTime -st	yyyy-MM-dd HH:mm	Required. Date and time that the recurrence starts.
-EndTime -et	yyyy-MM-dd HH:mm	Optional. Date and time that the recurrence ends.
-TimeZone -tz	timezone	Optional. Time zone for the schedule start time. To configure the time zone, you can enter the time zone ID number or the Olson Database ID. Default is locale of the client machine.

Option	Argument	Description
-DailyRunEvery -dre	daily_run_every	Optional. Run the schedule on an interval. The following list describes the options that you can configure: - minute(s). Run the schedule daily every n minutes. - hour(s). Run the schedule daily every n hours. - day(s). Run the schedule every n days. - week(s). Run the schedule every n weeks. - month(s). Run the schedule every n months. - year(s). Run the schedule every n years. - FIRST. Run the schedule every first n day of the month. Use the -rdwm option to specify the day or days of the week. - SECOND. Run the schedule every second n day of the month. Use the -rdwm option to specify the day or days of the week. - THIRD. Run the schedule every third n day of the month. Use the -rdwm option to specify the day or days of the week. - FOURTH. Run the schedule every fourth n day of the month. Use the -rdwm option to specify the day or days of the week. - LAST. Run the schedule every last n day of the month. Use the -rdwm option to specify the day or days of the week.
-RunDaysOfWeek -rdw	mon|tue|wed|thu|fri|sat|sun	Optional. Run the schedule on certain days of the week.
-RunDayOfWeekMonth -rdwm	monday|tuesday| wednesday|thursday|friday| saturday|sunday	Optional. Run the schedule on certain days of the week every month. Use the -dre options to run the schedule every first, second, third, fourth, or last n day of the month.
-RunDayofMonth -rdm	1-30| LAST_DAY_OF_MONTH	Optional. Run the schedule on day n of the month.
-RepeatCount -rc	repeat_count	Optional. End the recurrence after a number of runs instead of on a date.

Option	Argument	Description
RemoveRunnableObjects -rro	removeRunnableObjects	Optional. Removes objects from the schedule. Enter objects in the following format: `"{mapping|workflow}:Data Integration Service/Application/{Mapping|Workflow}[[?][parameterFilePath=PATH_TO_PARAMETER_FILE|parameterSet=PARAMETER_SET_NAME]&runAsUser=USER_NAME&runAsUserSecurityDomain=SECURITY_DOMAIN&runAsUserPassword=PASSWORD]]"]`

-AddRunnableObjects
-aro
	addRunnableObjects	Optional. Adds objects to the schedule. Objects that you would like to schedule. Enter the object type, followed by the path to the object on the Data Integration Service. For example:
		`"mapping:DIS_1234/Application_mapping/Mapping_abc"`
		Optionally, use the following arguments to configure a parameter file, parameter set, run as user, or operating system profile for the object:
		- parameterFilePath=PATH_TO_PARAMETER_FILE
		- parameterSet=PARAMETER_SET_NAME
		- runAsUser=USER_NAME &runAsUserSecurityDomain=SECURITY_DOMAIN &runAsUserPassword=PASSWORD
		- osProfileName=OS_PROFILE_NAME
		For example:
		`"workflow:DIS_1234/Application_workflow/Workflow_abc?parameterFilePath=C://Informatica/Parameter Files/Parameter.xml&runAsUser=Administrator&runAsUserSecurityDomain=Native&runAsUserPassword=Administrator"`

For a list of the valid time zone values, see "Valid Time Zone Parameters" on page 1002.

UpdateServiceOptions

Updates the properties for the Scheduler Service. To view the current options, run the infacmd sch ListServiceOptions command.

The infacmd sch UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName:-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeName|-nn> primary node name]
[<-BackupNodes|-bn> node_name1,node_name2,...]
<-Options|-o> options
```

The following table describes infacmd sch UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-ServiceName -sn	service_name	Required. Enter Scheduler_Service.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-NodeName -nn	primary node name	Optional. Primary node on which the service runs.
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable.
Options -o	options	Optional. Enter each option separated by a space.

Scheduler Service Options

Use the Scheduler Service options with the infacmd sch UpdateServiceOptions command.

Enter Scheduler Service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Scheduler Service options:

Option	Description
SchedulerPersistenceOptions.SchedulerRepositoryServiceName	Model Repository Service associated with the Scheduler Service.
SchedulerPersistenceOptions.SchedulerRepositoryUsername	User name of an administrator user in the Informatica domain. Not available for a domain with Kerberos authentication.
SchedulerPersistenceOptions.SchedulerRepositoryPassword	Password of the administrator user in the Informatica domain. Not available for a domain with Kerberos authentication.
SchedulerPersistenceOptions.SchedulerRepositorySecurityDomain	LDAP security domain for the user who manages the Scheduler Service. The security domain field does not appear for users with Native or Kerberos authentication.
SchedulerLoggingOptions.SchedulerLogLevel	Determines the default severity level for the service logs. Choose one of the following options: - Fatal. Writes FATAL messages to the log. FATAL messages include nonrecoverable system failures that cause the service to shut down or become unavailable. - Error. Writes FATAL and ERROR code messages to the log. ERROR messages include connection failures, failures to save or retrieve metadata, service errors. - Warning. Writes FATAL, WARNING, and ERROR messages to the log. WARNING errors include recoverable system failures or warnings. - Info. Writes FATAL, INFO, WARNING, and ERROR messages to the log. INFO messages include system and service change messages. - Trace. Write FATAL, TRACE, INFO, WARNING, and ERROR code messages to the log. TRACE messages log user request failures. - Debug. Write FATAL, DEBUG, TRACE, INFO, WARNING, and ERROR messages to the log. DEBUG messages are user request logs.
SchedulerStorageOptions.SchedulerTempFileLocation	Path to the directory where parameter files are read from and written to. Configure the temporary file location to a directory that is accessible to all of the nodes in the domain.

UpdateServiceProcessOptions

Updates the properties for a Scheduler Service process. To view the current process configuration, run the infacmd sch ListServiceProcessOptions command.

The infacmd sch UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions
<-DomainName:-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-NodeName|-nn> node_name]
<-Options|-o> options
```

The following table describes infacmd sch UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-ServiceName -sn	service_name	Required. Enter Scheduler_Service.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
NodeName -nn	node_name	Name of the node on which the service process runs.
Options -o	options	Optional. Enter each option separated by a space.

Scheduler Service Process Options

Use the Scheduler Service options with the infacmd sch UpdateServiceOptions command.

Enter Scheduler Service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes Scheduler Service options:

Option	Description
SchedulerServiceAdvancedOptions.JVMOptions	Java Virtual Machine (JVM) command line options to run Java-based programs. When you configure the JVM options, you must set the Java SDK classpath, Java SDK minimum memory, and Java SDK maximum memory properties. You must set the following JVM command line options: - Xms. Minimum heap size. Default value is 256 m. - MaxPermSize. Maximum permanent generation size. Default is 128 m. - Dfile.encoding. File encoding. Default is UTF-8.
HttpConfigurationOptions.KeyStoreFile	Path and file name of the keystore file that contains the keys and certificates. Required if you use HTTPS connections for the service. You can create a keystore file with a keytool. Keytool is a utility that generates and stores private or public key pairs and associated certificates in a keystore file. You can use the self-signed certificate or use a certificate signed by a certificate authority.
HttpConfigurationOptions.KeyStorePassword	Password for the keystore file.
HttpConfigurationOptions.TrustStoreFile	Path and file name of the truststore file that contains authentication certificates trusted by the service.
HttpConfigurationOptions.TrustStorePassword	Password for the keystore file.
HttpConfigurationOptions.SSLProtocol	Secure Sockets Layer protocol to use. Default is TLS.
SchedulerServiceSecurityOptions.HttpPort	Unique HTTP port number for the Scheduler Service process when the service uses the HTTP protocol. Default is 6211.
SchedulerServiceSecurityOptions.HttpsPort	Unique HTTPS port number for the Scheduler Service process when the service uses the HTTPS protocol. When you set an HTTPS port number, you must also define the keystore file that contains the required keys and certificates.

updateUserPasswordInSchedule

When the password for a user is changed, the scheduled jobs associated with the user start to fail. The updateUserPasswordInSchedule command updates the password in the scheduler for a specified schedule name.

The infacmd sch updateUserPasswordInSchedule command uses the following syntax:

```
updateUserPasswordInSchedule
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ScheduleName|-scn> schedule_name
[<-ScheduleUserName|-sun> schedule_user_name]
[<-ScheduleUserPassword|-sup> schedule_user_password]
```

The following table describes infacmd sch updateUserPasswordInSchedule options and arguments:

Option	Argument	Description
-UserName -un	user_name	User name to connect to the Informatica domain.
-Password -pd	password	Updated password for the user.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.
-ScheduleName -scn	schedule_name	Name of the schedule for which you want to update the password.
-ScheduleUserName -sun	schedule_user_name	User name associated to the scheduled job. If you do not specify this value, -UserName is used to update the password.
-ScheduleUserPassword -sup	schedule_user_password	Updated password for the scheduler user. If you do not specify this value, -Password is used to update the password.

Upgrade

Upgrades the Scheduler Service configuration. Run sch Upgrade when you upgrade to the current version of Informatica.

The infacmd sch Upgrade command uses the following syntax:

```
Upgrade
<-DomainName:-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gatway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd sch Upgrade options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Name of the Informatica domain.
-ServiceName -sn	service_name	Required. Enter Scheduler_Service.
-UserName -un	user_name	User name to connect to the domain
-Password -pd	password	Password for the user name.
-SecurityDomain -sdn	security_domain	Name of the security domain to which the domain user belongs.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infa file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain.

CHAPTER 34

infacmd search Command Reference

This chapter includes the following topics:

CreateService

Creates a Search Service. By default, the Search Service is enabled when you create it.

The infacmd search CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-FolderPath|-fp> full_folder_path]
[<-BackupNodes|-bn> node_name1,node_name2,...]
<-SearchServicePort|-sp> search_service_port_number
<-IndexLocation|-il> search_index_location
<-ExtractionInterval|-ei> search_extraction_interval
<-RepositoryService|-rsn> model_repository_service_name
```

```
<-searchUserName|-sun> username_for_search_repositories
<-searchPassword|-spd> password_for_search_repositories
[<-searchSecurityDomain|-ssd> security_domain_of_search_repositories]
```

The following table describes infacmd search CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Node where the Search Service runs.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Search Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-FolderPath -fp	full_folder_path	Optional. Full path, excluding the domain name, to the folder in which you want to add the Search Service. Must be in the following format: /parent_folder/child_folder Default is "/" (the domain).
-BackupNodes -bn	node_name1,node_name2,...	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.
-SearchServicePort -sp	search_service_port_number	Required. Port on which the Search Service runs.
-IndexLocation -il	search_index_location	Directory that contains the search index files.
-ExtractionInterval -ei	search_extraction_interval	Interval in seconds at which the Search Service updates the search index.
-RepositoryService -rsn	model_repository_service_name	Model Repository Service to associate with the Search Service. The Model Repository Service cannot be assigned to another Search Service.
-searchUserName -sun	username_for_search_repositories	User name to access the Model Repository Service. The Model repository user must have the Administrator role.
-searchPassword -spd	password_for_search_repositories	User password to access the Model Repository Service.
-searchSecurityDomain -ssdn	security_domain_of_search_repositories	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the Model repository user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

ListServiceOptions

Lists the properties for a Search Service.

The infacmd search ListServiceOptions command uses the following syntax:

```
ListServiceOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd search ListServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Node where the Search Service runs.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Search Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

ListServiceProcessOptions

Lists the properties of a Search Service process.

The infacmd search ListServiceProcessOptions command uses the following syntax:

```
ListServiceProcessOptions
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd search ListServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-NodeName -nn	node_name	Required. Name of node where the service process runs.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Search Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

.

UpdateServiceOptions

Updates Search Service properties. To view current properties run the infacmd search ListServiceOptions command.

You can change the properties while the service is running. However, you must recycle the service for changes to take effect.

The infacmd search UpdateServiceOptions command uses the following syntax:

```
UpdateServiceOptions
<-DomainName|-dn> domain_name
[<-SecurityDomain|-sdn> security_domain]
<-UserName|-un> user_name
<-Password|-pd> password
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
[<-Options|-o> options]
[<-NodeName|-nn> node name]
[<-BackupNodes|-bn> node_name1,node_name2,...]
```

The following table describes infacmd search UpdateServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Search Service.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Optional. Enter each option separated by a space. Include an option value within double quotes if it has a space. To view options, run the infacmd search ListServiceOptions command.
-NodeName -nn	node name	Optional. Node on which the Search Service runs.
-BackupNodes -bn	node_name1,node_name2,..	Optional. Nodes on which the service can run if the primary node is unavailable. You can configure backup nodes if you have high availability.

UpdateServiceProcessOptions

Updates properties for a Search Service process. To view current properties, run the infacmd search ListServiceProcessOptions command.

Enter connection options in the following format:

```
... -o option_name=value option_name=value ...
```

Separate multiple options with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The infacmd search UpdateServiceProcessOptions command uses the following syntax:

```
UpdateServiceProcessOptions

<-DomainName|-dn> domain_name

<-NodeName|-nn> node_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password
```

```
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Options|-o> options
```

The following table describes infacmd search UpdateServiceProcessOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
NodeName -nn	node_name	Required. Node where the Search Service runs.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Search Service.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Options -o	options	Required. Enter each option separated by a space. To view the options, run the infacmd search ListServiceProcessOptions command.

CHAPTER 35

infacmd sql Command Reference

This chapter includes the following topics:

ExecuteSQL

Runs SQL statements that access an SQL data service.

Run infacmd sql ExecuteSQL in interactive or non-interactive mode. When you run ExecuteSQL in interactive mode, you can enter SQL statements without writing a script. When you use the interactive mode, enter the connect string without the -Sql option. You can run subsequent SQL statements without entering the connection information for each statement.

The infacmd sql ExecuteSQL command uses the following syntax:

```
ExecuteSQL
<-ConnectString|-cs> connection_string
[<-Sql> sql_statement]
```

The following table describes infacmd sql ExecuteSQL options and arguments:

Option	Argument	Description
-ConnectString -cs	connection_string	Required. Enter an SQL data service connect string with the following syntax: `jdbc:informatica:sqlds/ <optional security domain\> <optional user name>/ <optional user password>@ <domain host name>: <domain HTTP port>?dis= <Data Integration Service name>&sqlds= <runtime SQL data service name>` Optionally, add options in the following format: `... &<option_name>=<option_value>` Enclose the connect string in single quotes. The connect string has the following option and value: **SQLDataServiceOptions.disableResultSetCache=true** Disables result set caching for a SQL data service query when the SQL data service is configured to cache the result set.
-Sql	sql_statement	Optional. Enter an SQL statement if you do not want to run in interactive mode.

ListColumnOptions

Lists the properties for columns in a virtual table.

The infacmd sql ListColumnOptions command uses the following syntax:

```
ListColumnOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
```

The following table describes infacmd sql ListColumnOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service.
-Table -t	schema.table	Required. Name of the table. Define the table with the following syntax: `<schema_name>.<table_name>`
-Column -c	column	Required. Name of the column.

ListColumnPermissions

Lists user and group permissions for a virtual column.

The infacmd sql ListColumnPermissions command uses the following syntax:

```
ListColumnPermissions

<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd sql ListTablePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Duration of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-Table -t	schema.table	Required. Name of the table. Define the table with the following syntax: <schema_name>.<table_name>
-Column -c	column	Required. Name of the column to update.
-Direct | -Effective>	direct | effective	Required. Enter either direct or effective. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

ListSQLDataServiceOptions

Lists the properties of an SQL data service that is deployed to a Data Integration Service.

The infacmd sql ListSQLDataServiceOptions command uses the following syntax:

```
ListSQLDataServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
```

The following table describes infacmd sql ListSQLDataServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`

ListSQLDataServicePermissions

Lists the permissions for an SQL data service.

The infacmd sql ListSQLDataServicePermissions command uses the following syntax:

```
ListSQLDataServicePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd sql ListSQLDataServicePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-Direct | -Effective>	direct | effective	Required. Level of permissions to list. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

ListSQLDataServices

Lists the SQL data services for a Data Integration Service.

The infacmd sql ListSQLDataServices command uses the following syntax:

```
ListSQLDataServices
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
```

The following table describes infacmd sql ListSQLDataServices options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Data Integration Service where the application is deployed.

ListStoredProcedurePermissions

Lists the permissions for a stored procedure.

The infacmd sql ListStoredProcedurePermissions command uses the following syntax:

```
ListStoredProcedurePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-StoredProcedure|-sp> stored_procedure
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd sql ListStoredProcedurePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
StoredProcedure -sp	stored_procedure	Required. Stored procedure name.
-Direct | -Effective>	direct | effective	Required. Level of permissions to list. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

ListTableOptions

Lists the properties for a virtual table.

The infacmd sql ListTableOptions command uses the following syntax:

```
ListTableOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table
```

The following table describes infacmd sql ListTableOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Required. Name of the table. Define the table with the following syntax: `<schema_name>.<table_name>`

ListTablePermissions

Lists user and group permissions for a virtual table.

The infacmd sql ListTablePermissions command uses the following syntax:

```
ListTablePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<<-Direct> direct_permission_only|<-Effective> effective_permission_only>
```

The following table describes infacmd sql ListTablePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	schema.table	Required. Name of the table. Define the table with the following syntax: `<schema_name>.<table_name>`
-Direct | -Effective>	direct | effective	Required. Enter either direct or effective. Direct permissions are permissions assigned directly to the user or group. Effective permissions include direct permissions and inherited permissions.

PurgeTableCache

Purges virtual table cache.

The infacmd sql PurgeTableCache command uses the following syntax:

```
PurgeTableCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> table
```

The following table describes infacmd sql PurgeTableCache options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix -sqlds with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-Table -t	table	Required. Name of virtual table cache to delete.

RefreshTableCache

Refreshes a virtual table cache.

The infacmd sql RefreshTableCache command uses the following syntax:

```
RefreshTableCache
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> table
```

The following table describes infacmd sql RefreshTableCache options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix -sqlds with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`
-Table -t	table	Required. Name of virtual table cache to refresh.

RenameSQLDataService

Renames a SQL data service that is deployed to a Data Integration Service.

The infacmd sql RenameSQLDataService command uses the following syntax:

```
RenameSQLDataService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
<-NewName|-n> new_name
```

The following table describes infacmd sql RenameSQLDataService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the SQL data service is deployed.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service to rename. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
NewName -n	new_name	Required. New name for the SQL data service.

SetColumnPermissions

Denies a group or user from accessing a column in a SQL query.

The infacmd sql SetColumnPermissions command uses the following syntax:

```
SetColumnPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Column|-c> column_name
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-DeniedPermissions|-dp> denied_permissions
```

The following table describes infacmd sql SetColumnPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service with the virtual table. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`

Option	Argument	Description
-Table -t	schema.table	Required. Name of the virtual table. Enter table in the following format: <schema_name>.<table_name>
-Column -c	column	Name of the column to update.
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
- GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-DeniedPermissions -dp	denied_permissions	Required. Enter SQL_Select to restrict a user from including the column in a SELECT.

SetSQLDataServicePermissions

Sets permissions to groups or users for an SQL data service. You can also deny permissions.

The infacmd sql SetSQLDataServicePermissions command uses the following syntax:

```
SetSQLDataServicePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-AllowedPermissions|-ap> allowed_permissions
<-DeniedPermissions|-dp> denied_permissions
```

The following table describes infacmd sql SetSQLDataServicePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that *infacmd* attempts to establish or reestablish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-AllowedPermissions -ap	allowed_permissions	Required. List of permissions separated by spaces. Enter any of the following permissions: - Grant. Users can grant and revoke permissions on the SQL data service using the Administrator tool or using the infacmd command line program. - Execute. Users can run all virtual stored procedures in the SQL data service using a JDBC or ODBC client tool. - SQL_Select. Users can run SQL SELECT statements on virtual tables in the SQL data service using a JDBC or ODBC client tool.
-DeniedPermissions -dp	denied_permissions	Optional. List of permissions to deny users. Separate each parameter by a space. Enter any of the following permissions: - EXECUTE. Users cannot run any virtual stored procedure in the SQL data service. - SQL_SELECT. Users cannot run SELECT statements on any table in the SQL data service.

SetStoredProcedurePermissions

Sets user and group permissions for a stored procedure. You can also deny permissions.

The infacmd sql SetStoredProcedurePermissions command uses the following syntax:

```
SetStoredProcedurePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
```

```
<-StoredProcedure|-sp> stored_procedure
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-AllowedPermissions|-ap> allowed_permissions
<-DeniedPermissions|-dp> denied_permissions
```

The following table describes infacmd sql SetStoredProcedurePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service with the stored procedure. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`
-StoredProcedure -sp	stored_procedure	Required. Name of the stored procedure.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.

Option	Argument	Description
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_space	Required. List of permissions to allow. Enter any of the following parameters separated by a space: - Grant. Users can grant and revoke permissions on the stored procedure objects using the Administrator tool or using the infacmd command line program - Execute. Users can run virtual stored procedures in the SQL data service using a JDBC or ODBC client tool.
-DeniedPermissions -dp	denied_permissions	Optional. List of permissions to deny users. Enter any of the following parameters separated by a space: - GRANT. Users cannot grant and revoke permissions on the stored procedure objects. - EXECUTE. Users can not run a stored procedure in the SQL data service.

SetTablePermissions

Sets group and user permissions on a virtual table.

The infacmd sql SetTablePermissions command uses the following syntax:

```
SetTablePermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<<-GranteeUserName|-gun> grantee_user_name|<-GranteeGroupName|-ggn> grantee_group_name>
[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]
<-AllowedPermissions|-ap> allowed_permissions
<-DeniedPermissions|-dp> denied_permissions
[<-RLSPredicate|-rls> row_level_security_predicate]
```

The following table describes infacmd sql SetTablePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service with the virtual table. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-Table -t	schema.table	Required. Name of the virtual table. Enter table in the following format: <schema_name>.<table_name>
-GranteeUserName| GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-AllowedPermissions -ap	list_of_allowed_permissions	Required. List of permissions to allow. Enter any of the following parameters separated by space: - Grant. Users can grant and revoke permissions on the stored procedure objects using the Administrator tool or using the infacmd command line program. - SQL_Select. Users can run SQL queries against the table.
-DeniedPermissions -dp	denied_permissions	Optional. List of permissions to deny users. Enter any of the following parameters separated by space: - GRANT. Users cannot grant and revoke permissions on the table. - SQL_SELECT. Users can not run SQL queries against the table.
-RLSPredicate -rls	row_level_security_predicate	Optional. Lists the row level security predicate to apply to SELECT statements.

StartSQLDataService

Starts an SQL data service.

The infacmd sql StartSQLDataService command uses the following syntax:

```
StartSQLDataServiceOptions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name
```

```
<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service
```

The following table describes infacmd sql StartSQLDataService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>

StopSQLDataService

Stops an SQL data service from running.

The infacmd sql StopSQLDataService command uses the following syntax:

```
StopSQLDataService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-SQLDataService|-sqlds> sql_data_service
```

The following table describes infacmd sql StopSQLDataService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the SQL data service is deployed.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service to stop. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`

UpdateColumnOptions

Sets column options to determine what happens when a user selects a restricted column in a query. You can substitute the value with NULL or with a constant value.

The infacmd sql UpdateColumnOptions command uses the following syntax:

```
UpdateColumnOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
```

```
[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-SQLDataService|-sqlds> sql_data_service

<-Table|-t> schema.table

<-Column|-c> column_name

<-Options|-o> options
```

The following table describes infacmd sql UpdateColumnOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service with the virtual table. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
-Table -t	schema.table	Required. Name of the virtual table. Enter table in the following format: <schema_name>.<table_name>
-Column -c	column	Column name.
-Options -o	options	Required. Enter each option separated by a space. To view current options, run the infacmd sql ListColumnOptions command.

Column Options

Use column options to update a column. Use the column options with the infacmd sql UpdateColumnOptions command.

Enter column options in the following format:

```
... -o UpdateColumnOptions.option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes column options:

Options	Description
ColumnOptions.DenyWith	When you use column level security, this property determines whether to substitute the restricted column value or to fail the query. If you substitute the column value, you can choose to substitute the value with NULL or with a constant value. Select one of the following options: - ERROR. Fails the query and returns an error. - NULL. Returns null values for a restricted column in each row. - VALUE. Returns a constant value in place of the restricted column in each row. Configure the constant value in the InsufficientPermissionValue option.
ColumnOptions.InsuffiicientPermissionValue	Substitutes the restricted column value with a constant value. The default is an empty string. If you do not configure ColumnOptions.DenyWith the Data Integration Service ignores the InsufficientPermissionValue option.

UpdateSQLDataServiceOptions

Updates SQL data service properties. You must stop the SQL data service before you update the properties.

The infacmd sql UpdateSQLDataServiceOptions command uses the following syntax:

```
UpdateSQLDataServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Options|-o> options
```

The following table describes infacmd sql UpdateSQLDataServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: <application_name>.<SQL_data_service_name>
options -o	options	Required. List of options to update. Enter options and values separated by spaces. To view options for a SQL data service, run infacmd sql ListSQLDataServiceOptions.

SQL Data Service Options

Use SQL data service options to update a SQL data service. Use the SQL data service options with the infacmd sql UpdateSQLDataServiceOptions command.

Enter SQL data service options in the following format:

```
... -o SQLDataServiceOptions.option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes connection options for infacmd sql UpdateSQLDataServiceOptions:

Option	Description
SQLDataServiceOptions.startupType	Determines whether the SQL data service is enabled to run when the application starts or when you start the SQL data service. Enter ENABLED to allow the SQL data service to run. Enter DISABLED to prevent the SQL data service from running.
SQLDataServiceOptions.traceLevel	Level of error messages written to the session log. Specify one of the following message levels: - Fatal - Error - Info - Trace - Debug
SQLDataServiceOptions.connectionTimeout	Maximum number of milliseconds to wait for a connection to the SQL data service. Default is 3,600,000.
SQLDataServiceOptions.requestTimeout	Maximum number of milliseconds for a SQL request to wait for a SQL Data Service response. Default is 3,600,000.
SQLDataServiceOptions.sortOrder	Sort order that the Data Integration Service uses for sorting and comparing data when running in Unicode mode. You can choose the sort order based on your code page. When the Data Integration runs in ASCII mode, it ignores the sort order value and uses a binary sort order. Default is binary.
SQLDataServiceOptions.maxActiveConnections	Maximum number of active connections to the SQL data service. Default is 10.
SQLDataServiceOptions.ResultSetCacheExpirationPeriod	The number of milliseconds that the result set cache is available for use. If set to -1, the cache never expires. If set to 0, result set caching is disabled. Changes to the expiration period do not apply to existing caches. If you want all caches to use the same expiration period, purge the result set cache after you change the expiration period. Default is 0.

Option	Description
SQLDataServiceOptions.DTMKeepAliveTime	Number of milliseconds that the DTM instance stays open after it completes the last request. Identical SQL queries can reuse the open instance. Use the keep alive time to increase performance when the time required to process the SQL query is small compared to the initialization time for the DTM instance. If the query fails, the DTM instance terminates. Must be an integer. A negative integer value means that the DTM Keep Alive Time for the Data Integration Service is used. 0 means that the Data Integration Service does not keep the DTM instance in memory. Default is -1.
SQLDataServiceOptions.optimizeLevel	The optimizer level that the Data Integration Service applies to the object. Enter the numeric value that is associated with the optimizer level that you want to configure. You can enter one of the following numeric values: - 0. The Data Integration Service does not apply optimization. - 1. The Data Integration Service applies the early projection optimization method. - 2. The Data Integration Service applies the early projection, early selection, push-into, and predicate optimization methods. - 3. The Data Integration Service applies the cost-based, early projection, early selection, push-into, predicate, and semi-join optimization methods.

UpdateTableOptions

Updates virtual table properties. You must stop the SQL data service before you update the properties.

The infacmd sql UpdateTableOptions command uses the following syntax:

```
UpdateTableOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-SQLDataService|-sqlds> sql_data_service
<-Table|-t> schema.table
<-Options|-o> options
```

The following table describes infacmd sql UpdateTableOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the application is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
SQLDataService -sqlds	sql_data_service	Required. Name of the SQL data service. You must prefix the SQL data service name with the application name. Use the following syntax: `<application_name>.<SQL_data_service_name>`

Option	Argument	Description
-Table -t	schema.table	Required. Name of the table. Use the following syntax: `<schema_name>.<table_name>`
Options -o	options	Required. Enter the name-value pair separated by spaces.

Virtual Table Options

Use the virtual table options to configure caching for a virtual table. Use the virtual table options with the infacmd sql UpdateTableOptions command.

Enter virtual table options in the following format:

```
... -o option_type.option_name=value ...
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes virtual table options:

Option	Description
VirtualTableOptions.CachingEnabled	Cache the virtual table in the data object cache database. True or false. Default is true.
VirtualTableOptions.CacheRefreshPeriod	Number of minutes between cache refreshes. Default is zero.
VirtualTableOptions.CacheTableName	The name of the user-managed table from which the Data Integration Service accesses the virtual table cache. A user-managed cache table is a table in the data object cache database that you create, populate, and manually refresh when needed. If you specify a cache table name, the Data Object Cache Manager does not manage the cache for the object and ignores the cache refresh period. If you do not specify a cache table name, the Data Object Cache Manager manages the cache for the object.

CHAPTER 36

infacmd tdm Command Reference

The *infacmd* tdm program administers the Test Data Manager Service.

You can create the service, add content to the service, enable the service and disable the service with the *infacmd* tdm commands.

CreateService

Creates a Test Data Manager Service in a domain.

The infacmd tdm CreateService command uses the following syntax:

```
CreateService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-NodeName|-nn> node_name
<-LicenseName|-ln> license_name

<-MRSServiceName|-mrs> model_repo_service
<-MRSUserName|-rsun> model_repo_service_username
<-MRSPassword|-rspd> model_repo_service_password
[<-MRSSecurityDomain|-rsdn> model_repo_security_domain]

<-EnableProfiling|-ep> enable_profiling

<-DISServiceName|-dis> data_integration_service
<-db_type|-dt> database_type (ORACLE, DB2, SQLSERVER or CUSTOM)
```

```
<-DBUsername|-du> db_user
<-DBPassword|-dp> db_password
<-DBUrl|-dl> db_url
<-DBConnString|-dc> db_conn_string
[<-DbSchema|-ds> db_schema (used for SQL Server only)]
[<-DbTablespace|-db> db_tablespace (used for DB2 only)]
[<-HttpPort> http_port]
[<-HttpsPort> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePassword|-kp> keystore_password]
[<-SSLProtocol|-sp> ssl_protocol]
[<-jvmParams|-jp> jvmParameters]
[<-connPoolSize|-cp> conn_pool_size]
[<-jmxPort> jmx_port]
[<-shutdownPort> shutdown_port]
[<-hadoopDistDir> Hadoop Distribution Directory]
[<-hadoopKerbSPN> Hadoop Kerberos Service Principal Name]
[<-hadoopKerbKeytab> Hadoop Kerberos Keytab]
```

The following table describes infacmd tdm CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Test Data Manager Service. The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-NodeName -nn	node_name	Required. Name of the node where the service will run.
-LicenseName -ln	license_name	Required. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Argument	Description
-MRSServiceName -mrs	model_repo_service	Name of the Model Repository Service to which TDM connects.
-MRSUserName -rsun	model_repo_service_username	Required. User name to connect to the Model repository.
-MRSPassword -rspd	model_repo_service_password	Required. Password for the user name to connect to the Model repository. The password is case sensitive.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Security domain is case sensitive. Default is Native.
-EnableProfiling -ep	enable_profiling	Indicates data discovery settings. Set to true to enable data discovery. Set to false to disable data discovery.
-DISServiceName -dis	data_integration_service	Name of the Data Integration Service to which TDM connects.
-db_type -dt	database_type	Type of TDM repository database. Values are Oracle, SQL Server, DB2, or Custom.
-DBUsername -du	db_user	Required. Account for the repository database. Use the database client to set up this account.
-DBPassword -dp	db_password	Required. Repository database password for the database user.

-DBUrl
-dl
	db_url	Required. JDBC connect string to the database for the TDM repository. Use one of the following syntaxes:
		Oracle:
		`jdbc:informatica:oracle: //<machineName>:<PortNo>;ServiceName=<DBName>; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true`
		DB2:
		`jdbc:informatica:db2: //<host>:<port>; DatabaseName=<dbname>; BatchPerformanceWorkaround=true;DynamicSections=1000`
		SQLServer:
		`jdbc:informatica:sqlserver: //<host>:<port>; DatabaseName=<dbname>; SnapshotSerializable=true`

Option	Argument	Description
-DBConnString -dc	db_conn_string	Native connect string to the TDM repository database. The service uses the connect string to create a connection object to the Test Data Manager repository and the PowerCenter repository or Model repository.
-DbSchema -ds	db_schema	Optional. The schema name for a Microsoft SQL Server database.
-DbTablespace -db	db_tablespace	Required for a DB2 database only. When you configure a tablespace name, the Test Data Manager Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name. The tablespace must be defined on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the installer creates the tables in the default tablespace.
-HttpPort	http_port	Required. Port number for the service.
-HttpsPort	https_port	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	keystore_file_location]	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol with PowerCenter.
-KeystorePassword -kp	keystore_password	Optional. If TLS is enabled, you must specify a password.
-SSLProtocol -pt	SSL Protocol	Optional. Secure Sockets Layer protocol to use. Editable if you enable Transport Layer Security (TLS).

Option	Argument	Description
-jvmParams -jp	jvmParameters	JVM parameters to set: - The heap size allocated for Test Data Manager. - The time after which database connections are renewed if the TDM UI remains idle. Required if you have modified the database configuration settings to values less than the TDM defaults. Edit the values in TDM such that the values are less than the database values. Include the JVM parameters in single quotes and then in double quotes. For example, 'value' and then "'value'". The -Xms option is case sensitive. For example: "'- **X**ms512m - **X**mx1024m - **XX**:MaxPermSize=512m'" - IDLE_TIME. `-DIDLE_TIME=<seconds>`. Default is 300 seconds. - CONNECT_TIME. `-DCONNECT_TIME=<seconds>`. Default is 5000 seconds.
-connPoolSize -cp	conn_pool_size	Optional. The maximum number of idle connection instances that a pool maintains for a database connection before the maximum idle time is met. Set this value to be more than the minimum number of idle connection instances. Default is 15.
-jmxPort	jmx_port	Port number for the JMX/RMI connections to TDM. Default is 6675.
-shutdownPort	shutdown_port	Port number that controls shutdown for TDM.
-hadoopDistDir -hdd	Hadoop Distribution Directory	The Hadoop distribution directory on the Test Data Manager Service node.
-hadoopKerbSPN -hks	Hadoop Kerberos Service Principal Name	Service Principal Name (SPN) of the Data Integration Service to connect to a Hadoop cluster that uses Kerberos authentication. Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.
-hadoopKerbKeytab -hkt	Hadoop Kerberos Keytab	The file path to the Kerberos keytab file on the machine on which the Data Integration Service runs. Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.

CreateContents

Creates repository content for the Test Data Manager repository.

The infacmd tdm CreateContents command uses the following syntax:

```
<-DomainName|-dn> domain_name

[<-SecurityDomain|-sdn> security_domain]

<-UserName|-un> user_name

<-Password|-pd> password

<-ServiceName|-sn> service_name

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm CreateContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. The Test Data Manager Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

EnableService

Enables the Test Data Manager Service.

The infacmd tdm EnableService command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm EnableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

DisableService

Disables the Test Data Manager Service. When you disable the Test Data Manager Service, all the service processes stop.

The infacmd tdm DisableService command uses the following syntax:

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-DisableMode|-dm> disable_mode: COMPLETE|ABORT|STOP
```

The following table describes infacmd tdm DisableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-DisableMode -dm	disable_mode	Required. Defines how the service is disabled: - Complete. Disables the service after all service processes stop. - Abort. Stops all processes immediately, and then disables the service. - Stop. Stops all running workflows, and then disables the service.

CHAPTER 37

infacmd tools Command Reference

This chapter includes the following topics:

deployApplication

Deploys an application to an .iar file.

Deploy an application to a file when the application contains a large number of objects. After you run the infacmd tools deployApplication command, run the infacmd dis deployApplication command to deploy the application to a Data Integration Service.

The infacmd tools deployApplication command uses the following syntax:

```
deployApplication

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

<-RepositoryService|-rs> Model Repository Service name

<-OutputDirectory|-od> Output directory

<-ApplicationPath|-ap> Application path
```

The following table describes infacmd tools deployApplication options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
- RepositoryService -rs	Model Repository Service name	Required. Model Repository Service name.
- OutputDirectory -od	Output Directory	Required. Directory where you want to write the .iar file.
- ApplicationPath -ap	Application Path	Required. Application path, starting with the project name, folder names, and followed by the application name. Separate the project name, folder names, and the application name with a slash (/). For example, "Project/Folder1/Folder2/Application".

exportObjects

Exports objects from a project in the Model repository to an XML file.

If you do not want to export all objects in the project, use an infacmd export control file to filter the Model repository objects that you want to export.

If the project being exported contains reference tables, you must run the command from the Informatica services installation directory. The command exports the reference table metadata from the Model repository to the XML file. The command exports the reference table data to a zip file. When you run the command, specify the path and file name of both the XML and zip files to be created.

The command does not export empty folders.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd tools exportObjects command uses the following syntax:

```
exportObjects

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

<-ProjectName|-pn> Project name

<-RepositoryService|-rs> Model Repository Service name

<-ExportFilePath|-fp> Path of file to export to

[<-OverwriteExportFile|-ow> Set to "true" to overwrite export file if it exists.]

[<-ControlFilePath|-cp> Path of export control file]

[<-OtherOptions|-oo>]
```

The following table describes infacmd tools exportObjects options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ProjectName -pn	Project name	Required. Name of the project from which you export the objects.
-RepositoryService -rs	Model Repository Service name	Required. Model Repository Service name.
-ExportFilePath -fp	Path of file to export to	Required. Path and XML file name of the export file to be created. You can specify an absolute path or a relative path to the file name.Use an easily distinguishable name for the file. For example, use the following suggested naming convention: `exp_<project_name>` **Note:** The command appends the .xml file extension to the output file.
-OverwriteExportFile -ow	Set to "true" to overwrite export file if it exists.	Optional. Set to true to overwrite an existing export file. If an export file exists and this option is set to false, the export fails. Default is false.
-ControlFilePath -cp	Path of export control file	Optional. Path and file name of the export control file that filters the objects that are exported. You can specify an absolute path or a relative path to the file name.

-OtherOptions
-oo
	-	Required if the project being exported contains reference tables. Additional options to export reference table data to a zip file. Enter options using the following format:
		`rtm:<option_name>=<value>,<option_name>=<value>`
		Required option names include:
		- disName. Name of the Data Integration Service.
		- codePage. Code page of the reference data.
		- refDataFile. Path and file name of the zip file where you want to export the reference table data.
		For example:
		`rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip`

exportResources

Exports the scorecard objects and lineage information in a project or folder to an XML file that you use in Metadata Manager.

If you do not want to export all objects in the project, use an infacmd export control file to filter the objects that you want to export. The command does not export empty folders.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase system memory, set the `-Xmx` value in the `ICMD_JAVA_OPTS` environment variable.

The infacmd tools exportResources command uses the following syntax:

```
exportResources
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ProjectName|-pn> project_name
<-RepositoryService|-rs> model_repository_service_name
<-ExportFilePath|-fp> export_file_path
[<-OverwriteExportFile|-ow> overwrite_export_file]
[<-ControlFilePath|-cp> control_file_path]
```

The following table describes infacmd tools exportResources options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ProjectName -pn	project_name	Required. Name of the project from which you export the objects.
-RepositoryService -rs	model_repository_service_name	Required. Model Repository Service name.
-ExportFilePath -fp	export_file_path	Required. Path and XML file name of the export file the command line program creates when you run the command. You can specify an absolute path or a relative path to the file name. Use an easily distinguishable name for the file. For example, use the following suggested naming convention: `exp_<project_name>.xml`
-OverwriteExportFile -ow	overwrite_export_file	Optional. Set to true to overwrite an existing export file. If an export file exists and you set this option to false, the export fails. Default is false.
-ControlFilePath -cp	control_file_path	Optional. Path and file name of the export control file that filters the objects that the command line program exports. You can specify an absolute path or a relative path to the file name.

importObjects

Imports objects from an XML file into an existing project in the Model repository.

If you do not want to import all objects in the file, use an infacmd import control file to filter the Model repository objects that you want to import.

If the file being imported contains reference tables, you must run the command from the Informatica services installation directory. The command imports the reference table metadata from the XML file into the Model repository. The command imports the reference table data from a zip file. When you run the command, specify the path and file name of both the XML and zip files to be imported.

If the command fails with a Java memory error, increase the system memory available for infacmd. To increase the system memory, set the -Xmx value in the ICMD_JAVA_OPTS environment variable.

The infacmd tools importObjects command uses the following syntax:

```
importObjects

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

[<-TargetProject|-tp> Target project name <ignored if control file is specified>]

<-RepositoryService|-rs> Model Repository Service name

<-ImportFilePath|-fp> import_file_path

[<-SourceProject|-sp> Source project name in import file <ignored if control file is
specified>]

[<-TargetFolder|-tf> Target folder to import to <omit for root, ignored if control file
is specified>]

[<-SkipCRC|-sc> Set to "true" to skip CRC check on imported file.]

[<-ConflictResolution|-cr> Resolution type]

[<-ControlFilePath|-cp> Path of import control file]

[<-SkipCnxValidation|-scv> Set to "true" to skip connection validation.]

[<-OtherOptions|-oo>]
```

The following table describes infacmd tools importObjects options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-TargetProject -tp	Target Project name <ignored if control file is specified>	Optional. Name of the project into which you want to import the objects. The project must exist in the repository before you import the objects. The option is ignored if you use an import control file.
-RepositoryService - rs	Model Repository Service name	Required. Model Repository Service name.
-ImportFilePath -fp	import_file_path	Required. Path and file name of the XML file to import the objects from. You can specify an absolute path or a relative path to the file name.
-SourceProject -sp	Source project name in import file <ignored if control file is specified>	Optional. Source project name in the file to import. The option is ignored if you use an import control file.
-TargetFolder -tf	Target folder to import to <omit for root, ignored if control file is specified>	Optional. Target folder into which you want to import the objects. If you do not specify a target folder, the objects are imported into the target project. The folder must exist in the repository before you import the objects. The option is ignored if you use an import control file.

Option	Argument	Description
-SkipCRC -sc	Set to "true" to skip CRC check on imported file.	Indicates whether to skip the cyclic redundancy check (CRC) that detects whether the file to import was modified. Set to true to skip the check. Default is false.
-ConflictResolution -cr	Resolution type specified	Optional. Conflict resolution strategy. You can specify one of the following options for all objects being imported: - rename - replace - reuse - none The option is ignored if you use an import control file. If the conflict resolution strategy is set to none and a conflict occurs, the import fails. Default is none.
-ControlFilePath -cp	Path of import control file	Optional. Path and file name of the import control file that filters the objects that are imported. You can specify an absolute path or a relative path.

Option	Argument	Description
-SkipCnxValidation -scv	Set to "true" to skip connection validation.	Optional. Indicates whether to skip target connection validation during the import. By default, the import process verifies that connections used by the imported objects exist in the target repository. If the connections do not exist, the import fails. To skip target connection validation and continue with the import, set this option to true. If the imported objects use connections that do not exist in the target repository, the import process imports the objects with an "Unspecified" connection. Use the Developer tool to select the correct connection after the import process has completed. Default is false. **Note:** If an import control file specifies a source connection that does not exist in the file that you are importing, the import process fails regardless of the value for this option. To correct the error, verify that the connection rebind element in the import control file includes source connections that exist in the file that you are importing.

-OtherOptions
-oo
	-	Required if the import file contains reference tables. Additional options to import reference table data from a zip file. Enter options using the following format:
		`rtm:<option_name>=<value>,<option_name>=<value>`
		Required option names include:
		- disName. Name of the Data Integration Service.
		- codePage. Code page of the reference data.
		- refDataFile. Path and file name of the zip file from where you want to import the reference table data.
		For example:
		`rtm:disName=ds,codePage=UTF-8,refDataFile=/folder1/data.zip`

patchApplication

Deploys an application patch using a .piar file to a Data Integration Service. The Data Integration Service applies the patch to the corresponding incremental application. The incremental application must be deployed on the same Data Integration Service where you want to deploy the patch.

If you created the patch based on a previous version of the incremental application, the patch might not be valid. A patch is not valid if the application objects in the patch have been updated by other application

patches since the patch that you currently want to deploy was created. To proceed, you can force the Data Integration Service to apply the patch.

You can also choose to retain or discard state information. State information refers to mapping properties and the properties of run-time objects such as mapping outputs or the Sequence Generator transformation.

For more information about state information, see the "Application Deployment" chapter in the *Informatica Developer Tool Guide*.

Note: If you deploy a previous version of a patch, the Data Integration Service does not roll back the incremental application to the time that the patch was created. The Data Integration Service updates the application based on the application objects in the patch.

The infacmd tools patchApplication command uses the following syntax:

```
patchApplication

<-DomainName|-dn> Domain name

<-UserName|-un> User name

<-Password|-pd> Password

[<-SecurityDomain|-sdn> Security domain]

<-DataIntegrationService|-dis> Data Integration Service name

<-FilePath|-fp> Patch file path

[<-force|-f> True | False]

[<-RetainStateInformation|-rsi> True | False]
```

The following table describes infacmd tools patchApplication options and arguments:

Option	Argument	Description
-DomainName -dn	Domain name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	User name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	Security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-DataIntegrationService -dis	Data Integration Service name	Required. The name of the Data Integration Service where the incremental application is deployed.
-FilePath -fp	Patch file path	Required. Path and .piar file name of the patch to deploy. You can specify an absolute path or a relative path to the file name.
-force -f	True | False	Optional. Use `true` to ignore the validity of the patch and force the Data Integration Service to apply the patch to the application. Default is `false`.
-RetainStateInformation -rsi	True | False	Optional. Indicates whether state information is retained or discarded. **Note:** This option overrides the setting to retain or discard state information in the application patch archive file.

CHAPTER 38

infacmd wfs Command Reference

This chapter includes the following topics:

abortWorkflow

Aborts a running workflow instance.

If an Assignment task or an Exclusive gateway is running, the Data Integration Service completes the task or gateway. After the task aborts or completes, the service aborts the workflow instance. The service does not start running any subsequent workflow objects.

The infacmd wfs abortWorkflow command uses the following syntax:

```
abortWorkflow
```

```
<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

<-InstanceId|-iid> instance_id

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs abortWorkflow options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service running the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-InstanceId -iid	instance ID of the workflow to be aborted	Required. Workflow instance ID to abort. You can read the workflow instance ID from the workflow properties on the Monitoring tab of the Administrator tool. Or, run infacmd wfs ListActiveWorkflowInstances to find the workflow instance ID.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

bulkComplete

Stops all operations for a Human task in a workflow that you specify, and passes the records that the task identifies to the next stage in the workflow. The bulkComplete command updates the status of the steps in the Human task to indicate that the steps are complete. The command does not edit or update the status of the records that the task identifies.

The bulkComplete command uses the following syntax:

```
bulkComplete
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-InstanceId|-iid> Instance_id
<-StepName|-sid> Step_name
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs bulkComplete options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
InstanceID -iid	Instance_ID	Required. Unique identifier for the workflow that runs the Human task that you want to complete. You can read the workflow instance ID from the workflow properties on the Monitoring tab of the Administrator tool. Or, run infacmd wfs ListActiveWorkflowInstances to find the workflow instance ID.
StepName -sid	Step_name	Required. The name of the Human task that the workflow uses to create the Human task instances.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

cancelWorkflow

Cancels a running workflow instance. When you cancel a workflow instance, the Data Integration Service finishes processing any running task and then stops processing the workflow instance. The service does not start running any subsequent objects.

The infacmd wfs cancelWorkflow command uses the following syntax:

```
cancelWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-InstanceID|-iid> instance_ID
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs cancelWorkflow options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service running the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-InstanceID -iid	instance_ID	Required. Workflow instance ID to cancel. You can read the workflow instance ID from the workflow properties on the Monitoring tab of the Administrator tool. Or, run infacmd wfs ListActiveWorkflowInstances to find the workflow instance ID.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

completeTask

Completes a Human task instance that you specify.

A Human task instance is a set of records that a workflow assigns to a user or group for analysis in Informatica Analyst. The completeTask command updates the status of the task instance to Complete and passes the records in the task instance to another step in the workflow. For example, you might configure the command to send the records to another task instance for review.

Each Human task instance has a unique task instance ID. When you run infacmd wfs completeTask, you enter an ID value to identify the task instance to complete.

You can find the task instance ID in the following ways:

- Log in to Informatica Analyst and read the task instance ID in the Monitoring tool.
- Run infacmd wfs listTasks.
- Ask the business administrator or the user who owns the task instance. The business administrator or the user can read the task instance ID in Informatica Analyst.

The infacmd wfs completeTask command uses the following syntax:

```
completeTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
<-NextTask|-to> next_task
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs completeTask options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-TaskID -tid	task_id	Required. Unique identifier for the Human task instance.
-NextTask -to	next_task	Required. The name of the step in the workflow to which the command passes the task instance records. The Human task configuration in the workflow determines the steps that the task instance records can pass to.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

createTables

Creates the database tables that store run-time metadata for the workflow. The command creates empty tables. Identify the service that runs the workflows when you run the command.

Before you create the database tables, verify the following options on the Data Integration Service that runs the workflows:

- The Workflow Orchestration Service module is active on the Data Integration Service.
- The Workflow Orchestration Service properties identify the connection for the database that stores the workflow metadata.

The createTables command uses the following syntax:

```
createTables
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs createTables options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflows that write metadata to the tables.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

delegateTask

Assigns ownership of a Human task instance to another user or group.

You might assign to another user or group a task instance when the task instance has no owner. Or, you might assign a task instance to another user or group when the current user cannot complete the task instance.

You can assign a task instance to a user or group if you are the task instance owner or the business administrator on the task. You can also assign the task instance to another user or group if you are a potential owner of the task instance. You are a potential owner if you are one of a set of users to whom the Human task assigned the task instance and no user owns the task.

When you run infacmd wfs delegateTask, enter the task instance ID of the task instance that you want to assign.

You can find the task instance ID in the following ways:

- Log in to Informatica Analyst and read the task instance ID in the Monitoring tool.
- Run infacmd wfs listTasks.
- Ask the business administrator or the user who owns the task instance. The business administrator or the user can read the task instance ID in Informatica Analyst.

The infacmd wfs delegateTask command uses the following syntax:

```
delegateTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
<-Entity|-to> to_entity
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs delegateTask options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-TaskID -tid	task_id	Required. Identifier of the Human task instance to delegate.
-Entity -to	to_entity	Required. Name of the user or group in the domain to whom the command must delegate the task instance. For example, `Native\Mary`.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

dropTables

Drops the database tables that store run-time metadata for the workflow.

The dropTables command uses the following syntax:

```
dropTables
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> Password
[<-SecurityDomain|-sdn> security_domain]
<-ServiceName|-sn> service_name
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs dropTables options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ServiceName -sn	service_name	Required. Name of the service that runs the workflows for which you want to delete data.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listActiveWorkflowInstances

Lists active workflow instances. An active workflow instance is an instance on which an action can be performed. Lists the state, workflow instance ID, workflow name, and application name for each active workflow instance.

Active workflow instances include workflow instances that are running and workflow instances enabled for recovery that are canceled.

The infacmd wfs listActiveWorkflowInstances command uses the following syntax:

```
listActiveWorkflowInstances
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs listActiveWorkflowInstances options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service running the workflow instances.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listMappingPersistedOutputs

Lists the state of each mapping output that is persisted. You can update the persisted mapping output values with the infacmd wfs setMappingPersistedOutputs command.

The infacmd wfs listMappingPersistedOutputs command uses the following syntax:

```
listMappingPersistedOutputs
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
<-MappingTaskInstance|-mti> mapping_task_instance_name
```

The following table describes infacmd wfs listMappingPersistedOutputs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflow. The application that contains the workflow must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the workflow.
-Workflow -wf	workflow_name	Required. Name of the workflow.
- mti	MappingTaskInstance	Required. The name of a mapping task that created the mapping outputs.

listTasks

Lists the Human task instances in the workflow database in which you have a role and that meet the filter criteria that you specify. Use the command options to set one or more filters.

If you do not set a filter option, the command returns a list of the first ten Human task instances in the database in which you have a role. Use the -MaxTasks option to change the number of task instances that the command returns.

You have a role in a task instance in any of the following cases:

- You are the current task instance owner.
- You are a potential owner of a task instance that another user does not own. For example, you are a member of a group whose members can claim ownership of the task.
- You are the business administrator for the task instance.

The filter options that you set for the command are cumulative. If you set multiple filter options, the command returns a list of the Human task instances that satisfy all of the options that you set.

The command applies the user name that you submit as a filter on the task instances in the workflow database. For example, you run the listTasks command with the user name "Native\Mary" and you set the -FilterByOwner option to "Native\John." The command returns a list of the task instances that John owns and for which Mary is a potential owner or the business administrator.

The infacmd wfs listTasks command uses the following syntax:

```
listTasks

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-MaxTasks|-max> max_tasks]

[<-FilterByOwner|-ow> e.g. Native\user_name]

[<-FilterByStatus|-st> READY|RESERVED|IN_PROGRESS|SUSPENDED]

[<-FilterByCreationDate|-cd> e.g. 2024-12-31]

[<-FilterByType|-tt> CleanseTask|ClusterTask|CleanseTaskReviewTask|ClusterTaskReviewTask]

[<-FilterByDueDate|-dd> e.g. 2024-12-31]

[<-FilterByID|-tid> e.g. 42]

[<-FilterByName|-tn> e.g. "ExceptionStep {1 - 9}"]

[<-FilterByNameLike|-tnl> e.g. "Step {% - %}"]

[<-TasksOffset|-offset> tasks_offset]

[<-Role> role]

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes the infacmd wfs listTasks options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-MaxTasks -max	max_tasks	Optional. Defines an upper limit for the number of Human task instances in the list that the command returns. By default, infacmd wfs listTasks command returns a list of the first ten task instances. You can use the max option in conjunction with the -offset option.
-FilterByOwner -ow	e.g. Native\user_name	Optional. Filters the list of the Human task instances in the workflow database by the name of the user or group that owns the task.
-FilterByStatus -st	READY|RESERVED| IN_PROGRESS|SUSPENDED	Optional. Filters the list of the Human task instances in the workflow database by the task status.
-FilterByCreationDate -cd	e.g. 2024-12-31	Optional. Filters the list of the Human task instances in the workflow database by the creation date of the tasks.
-FilterByType -tt	CleanseTask|ClusterTask| CleanseTaskReviewTask| ClusterTaskReviewTask	Optional. Filters the list of the Human task instances in the workflow database by the task type.
-FilterByDueDate -dd	e.g. 2024-12-31	Optional. Filters the list of the Human task instances in the workflow database by the task due date. The due date indicates the current deadline for task completion.
-FilterByID -tid	e.g. 42	Optional. Filters the list of the Human task instances in the workflow database by the Human task instance ID.
-FilterByName -tn	e.g. "ExceptionStep {1 - 9}"	Optional. Filters the list of the Human task instances in the workflow database by the Human task instance name that you specify. Do not use -FilterByName and -FilterByNameLike in the same command.

Option	Argument	Description
-FilterByNameLike -tnl	e.g. "Step {% - %}"	Optional. Filters the list of the Human task instances in the workflow database by the Human task name and allows a wildcard character in the filter string. You can use the percent (%) wildcard character. Do not use -FilterByName and -FilterByNameLike in the same command.
-TasksOffset -offset	tasks_offset	Optional. Specifies an offset from the first task instance in the list of task instances that meet the filter criteria. When you specify an offset, the command skips the task instances that the offset specifies and returns a list that begins with the next task instance that meets the filter criteria. You can use the -offset option with the -max option to organize the results of successive listTasks commands. For example, if you run infacmd wfs listTasks with a -max value of 50, you return a list of task instances in the range 1 through 50. If you run the command with a -max value of 50 and an -offset value of 51, you return the list of tasks in the range 51 through 100.
-Role	-role	Optional. Filters the list of the Human task instances in the workflow database by the Human task role. You can enter the following values: - ADMINISTRATORS - ALL - OWNERS - POTENTIAL_OWNERS If you do not set the option, the command returns task instances for all roles.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

listWorkflowParams

Lists the parameters for a workflow and creates a parameter file that you can use when you run a workflow. The command returns an XML file with default values that you can update. Enter the parameter file name when you run the workflow with infacmd wfs startWorkflow.

The infacmd wfs listWorkflowParams command uses the following syntax:

```
listWorkflowParams
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
[<-OutputFile|-o> output file_to_write_to]
```

The following table describes infacmd wfs listWorkflowParams options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflow. The application that contains the workflow must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout perioud with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the workflow.
-Workflow -wf	workflow_name	Required. Name of the workflow.
- OutputFile - o	output file_to_write_to	Optional. Path and file name of the parameter file to create. If you do not specify a file, the command displays the parameters in the command prompt.

listWorkflowParams Output

The listWorkflowParams command returns a parameter file as an XML file with default values that you can update.

For example, you run the listWorkflowParams command on application "MyApp" and workflow "MyWorkflow." Workflow "MyWorkflow" has one parameter, "MyParameter."

The listWorkflowParams command returns an XML file in the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<root xmlns="http://www.informatica.com/Parameterization/1.0"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema"
      version="2.0"><!--Specify deployed application specific parameters here.--><!--
    <application name="MyApp">
   <workflow name="MyWorkflow"/>
</application>--><project name="MyProject">
      <workflow name="MyWorkflow">
         <parameter name="MyParameter">Default</parameter>
      </workflow>
   </project>
</root>
```

The output XML file has the following top-level elements:

Application element

When you define a parameter within the application top-level element, the Data Integration Service applies the parameter value when you run the specified workflow in the specified application. You must include at least one project element within an application/workflow element.

By default, this top-level element is in comments. Remove the comments (!-- and -->) to use this element.

Project element

When you define a parameter within a project top-level element, the Data Integration Service applies the parameter value to the specified workflow in the project in any deployed application. The service also applies the parameter value to any workflow that uses the objects in the project.

If you define the same parameter in a project and an application top-level element in the same parameter file, the parameter value defined in the application element takes precedence.

listWorkflows

Lists the workflows in an application.

The infacmd wfs listWorkflows command uses the following syntax:

```
listWorkflows
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
```

The following table describes infacmd wfs listWorkflows options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflows. The application that contains the workflows must be deployed to a Data Integration Service.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both these methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the workflows.

pruneOldInstances

Deletes workflow process data from the workflow database.

When the Data Integration Service runs a workflow, the workflow process writes process data to the workflow database. Over time, the quantity of process data in the database can adversely affect the startup performance of workflow processes. To delete the process data from the database, run the wfs

pruneOldInstances command. You can configure the command to delete all of the process data in the workflow database. Or, you can delete the process data that the workflows generated during a time period that you specify.

The pruneOldInstances command deletes process data only. The command does not delete any data that a workflow instance or any object in the workflow reads or writes. Likewise, the command does not delete any workflow object metadata.

To delete the process data, you must have the Manage Service privilege on the domain.

The infacmd wfs pruneOldInstances command uses the following syntax:

```
pruneOldInstances
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
<-Days|-d> days
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs pruneOldInstances options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service running the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Days -d	days	The time period for which the command deletes the process data. To calculate the time period, the command subtracts the number of days that you specify from the date and time at which you run the command. The command deletes all process data that the workflow processes generated over the time period. Enter a value from 0 through 24855. If you enter 0, the command deletes all process data in the workflow database.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

recoverWorkflow

Recovers a workflow instance. You can recover a workflow instance that you canceled or that was interrupted by a recoverable error. When you recover a workflow instance, the Data Integration Service restarts the workflow instance at the task that was interrupted and reruns the interrupted task.

The infacmd wfs recoverWorkflow command uses the following syntax:

```
recoverWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-InstanceID|-iid> instance_ID
```

```
[<-Wait|-w> true|false]

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs recoverWorkflow options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that ran the original workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-InstanceID -iid	instance ID of the workflow to be recovered	Required. Workflow instance ID to recover. You can read the workflow instance ID from the workflow properties on the Monitoring tab of the Administrator tool. Or, run infacmd wfs ListActiveWorkflowInstances to find the workflow instance ID.
-Wait -w	true|false	Optional. Indicates whether infacmd waits for the workflow instance to recover before returning to the shell or command prompt. If true, infacmd returns to the shell or command prompt after the workflow instance recovers. You cannot run subsequent commands until the workflow instance recovers. If false, infacmd returns to the shell or command prompt immediately. You do not have to wait for the workflow instance to recover before running the next command. Default is false.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

releaseTask

Releases a Human task instance from the current owner. You can release a task instance if you are the owner or the business administrator on the task instance.

When you release a task instance, the task instance has no owner. If you release a task instance that you own, the task instance remains available to you in the Analyst tool. If the Human task identifies multiple users as potential owners of the task instance that you release, the task instance is available to all of the potential owners.

The infacmd wfs releaseTask command uses the following syntax:

```
releaseTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs releaseTask options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-TaskID -tid	task_id	Required. Identifier of the Human task instance in the workflow database.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

setMappingPersistedOutputs

Updates the persisted mapping outputs for a Mapping task instance in a workflow. Or, sets the persisted mapping outputs to null values. The command options specify the Mapping task instance name, the application name, and the workflow name.

To update a value, enter a name-value pair that contains the mapping output name and the value to change it to. To reset a persisted value to null values, use the reset option. You can reset some of the mapping outputs or you can reset all of the mapping outputs for a Mapping task instance. To view persisted mapping outputs, use the infacmd listMappingPersistedOutputs command.

The infacmd wfs setMappingPersistedOutputs command uses the following syntax:

```
setMappingPersistedOutputs
<-DomainName|-dn> domain_name
[<-ServiceName|-sn> service_name]
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
<-MappingTaskInstance|-mti> mapping_task_instance_name]
<-outputValues|-onvp> space_separated_output_value_pairs
[<-resetOutputs |-reset> reset_outputs]
```

The following table describes infacmd wfs setMappingPersistedOutputs options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflow. The application that contains the workflow must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the workflow.
-Workflow -wf	workflow_name	Required. Name of the workflow.
-MappingTaskInstance -mti	mappingTaskInstancename	Required. The name of a mapping task that created the mapping outputs.
-outputvalues -onvp	space_separated_output_value_pairs	Optional. Changes the persisted value of specific mapping outputs. Enter space-separated name-value pairs in the following syntax: output_name=value output2_name=value output3_name=value
-ResetOutputs -reset	reset_outputs	Optional. Removes the mapping output value from the repository. To reset specific mapping outputs, enter the reset option with mapping output names separated by spaces in the following syntax: -reset mapping_output_name mapping_output2_name mapping_output3_name

startTask

Starts a Human task instance in a workflow. The start operation changes the status of the task instance to IN_PROGRESS.

The infacmd wfs startTask command uses the following syntax:

```
startTask
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
<-TaskId|-tid> task_id
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd wfs startTask options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service that runs the workflow instance.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-TaskID -tid	task_id	Required. Identifier of the Human task to start.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

startWorkflow

Starts an instance of a workflow. You can run multiple instances of a workflow at the same time. You can use a parameter file for the workflow or a parameter set.

The infacmd wfs startWorkflow command uses the following syntax:

```
startWorkflow
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
[<-Wait|-w> true|false]
[<-ParameterFile|-pf> parameter_file_path]
[<-ParameterSet|-ps> parameter_set_name]
[<-OperatingSystemProfile|-osp> operating_system_profile_name]
```

The command returns the workflow instance ID.

The following table describes infacmd wfs startWorkflow options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflow. The application that contains the workflow must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-Application -a	application_name	Required. Name of the application that contains the workflow.

Option	Argument	Description
-Workflow -wf	workflow_name	Required. Name of the workflow to start.
-Wait -w	true|false	Optional. Indicates whether infacmd waits for the workflow instance to complete before returning to the shell or command prompt. If true, infacmd returns to the shell or command prompt after the workflow instance completes. You cannot run subsequent commands until the workflow instance completes. If false, infacmd returns to the shell or command prompt immediately. You do not have to wait for the workflow instance to complete before running the next command. Default is false.
-ParameterFile -pf	parameter_file_path	Optional. Name and path of the parameter file. Do not enter a parameter file name and a parameter set name in the same command.
-ParameterSet -ps	parameter_set_name	Optional. Name of parameter set to use at run time. The parameter set option overrides any parameter set deployed with the application. Do not enter a parameter file name and a parameter set name in the same command.
-OperatingSystemProfile -osp	operating_system_profile_name	Optional. Name of the operating system profile under which the workflow runs.

upgradeWorkflowParameterFile

Upgrades a workflow parameter file so that the file format is compatible with the current release. Run the command on workflow parameter files that users created in an Informatica 9.x release. When you run the command, you identify a workflow parameter file to upgrade and you specify a target file.

The infacmd wfs upgradeWorkflowParameterFile command uses the following syntax:

```
upgradeWorkflowParameterFile
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-Application|-a> application_name
<-Workflow|-wf> workflow_name
<-ParameterFile|-pf> parameter file path
```

```
<-TargetOutputFile|-of> output_file_path
```

The following table describes infacmd wfs upgradeWorkflowParameterFile options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service to run the workflow. The application that contains the workflow must be deployed to a Data Integration Service.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-Application -a	application_name	Required. Name of the application that contains the workflow.
-Workflow -wf	workflow_name	Required. Name of the workflow that reads the values parameter file.
-Wait -w	true|false	Optional. Indicates whether infacmd waits for the workflow instance to complete before returning to the shell or command prompt. If true, infacmd returns to the shell or command prompt after the workflow instance completes. You cannot run subsequent commands until the workflow instance completes. If false, infacmd returns to the shell or command prompt immediately. You do not have to wait for the workflow instance to complete before running the next command. Default is false.
-ParameterFile -pf	parameter file path	Required. Name and location of the parameter file that contains the values to upgrade.
-TargetOutputFile -of	parameter file path	Required. Name and location of the output file from the command. The output file contains the valid parameters for the current release.

CHAPTER 39

infacmd ws Command Reference

This chapter includes the following topics:

ListOperationOptions

Lists the properties of a web service operation that is deployed to a Data Integration Service.

The infacmd ws ListOperationOptions command uses the following syntax:

```
ListOperationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
```

The following table describes infacmd ws ListOperationOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
Operation -op	operation	Required. Name of the web service operation to list properties for.

ListOperationPermissions

Lists user and group permissions for a web service operation. You must indicate direct or effective permissions.

The infacmd ws ListOperationPermissions command uses the following syntax:

```
ListOperationPermissions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

The following table describes infacmd ws ListOperationPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
-Operation -op	operation	Required. Name of the web service operation to list properties for.
-Direct or -Effective	direct_permission_only effective_permission_only	Required. Enter Direct to list assigned permissions. Enter Effective to list inherited permissions.

ListWebServiceOptions

List the properties of a web service that is deployed to a Data Integration Service. You can configure the properties using the Administrator tool or infacmd ws UpdateWebServiceOptions.

The infacmd ws ListWebServiceOptions command uses the following syntax:

```
ListWebServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
```

The following table describes infacmd ws ListWebServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.

ListWebServicePermissions

Lists group and user permissions for a web service that is deployed to a Data Integration Service. You must indicate direct or effective permissions.

The following table describes infacmd ws ListWebServicePermissions options and arguments:

```
ListWebServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<<-Direct> direct_permission_only|<-Effective> effective_permission_only
```

The following table describes infacmd ws ListWebServicePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
-Direct or -Effective	direct_permission_only effective_permission_only	Required. Enter Direct to list assigned permissions. Enter Effective to list inherited permissions.

ListWebServices

Lists the web services for an application. If you do not enter an application name, infacmd lists all the web services for a Data Integration Service.

The infacmd ws ListWebServices command uses the following syntax:

```
ListWebServices
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
[<-Application|-a> application]
```

The following table describes infacmd ws ListWebServices options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web services are deployed.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-application -ap	application	Optional. Name of the application to list web services for.

RenameWebService

Rename a web service.

The infacmd ws RenameWebService command uses the following syntax:

```
RenameWebService
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
```

```
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-NewName|-n> new_name
```

The following table describes infacmd ws RenameWebService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-WebService -ws	web_service	Required. Name of the web service.
-NewName -n	new_name	Required. New name for the web service.

SetOperationPermissions

Sets the user or group permissions for a web service operation. You can set permissions or deny permissions for a user or group.

The infacmd ws SetOperationPermissions command uses the following syntax:

```
SetOperationPermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service

<-Operation|-op> operation

<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]

[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

The following table describes infacmd ws SetOperationPermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

Option	Argument	Description
-WebService -ws	web_service	Required. Name of the web service service.
-Operation -op	operation	Required. Name of the web service operation.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_spac e	Required. List of permissions to allow. Enter any of the following parameters separated by space: - GRANT. Users can grant and revoke permissions on the operation using the Administrator tool or using the infacmd command line program. - EXECUTE. Users can run the operation.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. List of permissions to deny users. Enter any of the following parameters separated by space: - GRANT. Users cannot grant and revoke permissions on the operation. - EXECUTE. Users cannot run the operation.

SetWebServicePermissions

Sets user or group permissions for a web service. You can set permissions or deny the permissions for one user or group.

The infacmd ws SetWebServicePermissions command uses the following syntax:

```
SetWebServicePermissions

<-DomainName|-dn> domain_name

<-ServiceName|-sn> service_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-WebService|-ws> web_service
```

```
<-GranteeUserName|-gun> grantee_user_name|
<-GranteeGroupName|-ggn> grantee_group_name>

[<-GranteeSecurityDomain|-gsdn> grantee_security_domain]

[<-AllowedPermissions|-ap> list_of_allowed_permissions_separated_by_space]

[<-DeniedPermissions|-dp> list_of_denied_permissions_separated_by_space]
```

The following table describes infacmd ws SetWebServicePermissions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
-GranteeUserName|GranteeGroupName -gun|-ggn	grantee_user_name| grantee_group_name	Required. User name or group name to set or deny permissions for.
-GranteeSecurityDomain -gsdn	grantee_security_domain	Required if you use LDAP authentication and you are granting user permissions. Name of the security domain that the user belongs to.

Option	Argument	Description
-AllowedPermissions -ap	list_of_allowed_permissions_separated_by_spac e	Required. List of permissions to allow. Enter any of the following parameters separated by space: - GRANT. Users can grant and revoke permissions on the web service using the Administrator tool or using the infacmd command line program. - EXECUTE. Users can run the web service.
-DeniedPermissions -dp	list_of_denied_permissions_separated_by_space	Optional. List of permissions to deny users. Enter any of the following parameters separated by space: - GRANT. Users cannot grant and revoke permissions on the web service. - EXECUTE. Users cannot run the web service.

StartWebService

Starts a web service that is deployed to a Data Integration Service.

The infacmd ws StartWebService command uses the following syntax:

```
StartWebService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-WebService|-ws> web_service
```

The following table describes infacmd ws StartWebService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Data Integration Service name where the web service is deployed.
-WebService -ws	web_service	Required. Name of the web service to start.

StopWebService

Stops a running web service.

The infacmd ws StopWebService command uses the following syntax:

```
StopWebService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-WebService|-ws> web_service
```

The following table describes infacmd ws StopWebService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-ServiceName -sn	service_name	Data Integration Service name where the web service is deployed.
-WebService -ws	web_service	Required. Name of the web service service to stop.

UpdateOperationOptions

Updates properties for a web service operation that is deployed to a Data Integration Service.

The infacmd ws UpdateOperationOptions command uses the following syntax:

```
UpdateOperationOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Operation|-op> operation
<-Options|-o> options
```

The following table describes infacmd ws UpdateOperationOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
Operation -op	operation	Required. Name of the web service operation to update.
-Options -o> options	options	Enter the web service option in the following format: `... -o option_type.option_name=value`

Operation Options

Use operation options to update a web service operation. Use the operation options with infacmd ws UpdateOperationOptions.

Enter operation options in the following format:

```
... -o OperationOptions.option_name=value ...
```

The following table describes an option for infacmd ws UpdateOperationOptions:

Option	Description
WebServiceOperationOptions.ResultSetCacheExpirationPeriod	Amount of time in milliseconds that the result set cache is available for use. If set to -1, the cache never expires. If set to 0, result set caching is disabled. If you want all caches to use the same expiration period, purge the result set cache after you change the expiration period. Default is 0.

UpdateWebServiceOptions

Update the properties for a web service that is deployed to a Data Integration Service. To view the properties for the web service you can use infacmd ws ListWebServiceOptions.

The infacmd ws UpdateWebServiceOptions command uses the following syntax:

```
UpdateWebServiceOptions
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-WebService|-ws> web_service
<-Options|-o> options
```

The following table describes infacmd ws UpdateWebServiceOptions options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Data Integration Service where the web service is deployed.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.
-WebService -ws	web_service	Required. Name of the web service.
-Options -o> options	options	Enter each option separated by a space.

Web Service Options

Use a specific syntax to enter web service options.

Enter web service options in the following format:

```
... -o option_type.option_name=value
```

To enter multiple options, separate them with a space. To enter a value that contains a space or other non-alphanumeric character, enclose the value in quotation marks.

The following table describes web service options:

Option	Description
WebServiceOptions.startupType	Determines whether the web service is enabled to run when the application starts or when you start the web service. Enter enabled or disabled.
WebServiceOptions.traceLevel	Level of error messages written to the run-time web service log. Enter one of the following message levels: - OFF - SEVERE - WARNING - INFO - FINE - FINEST - ALL
WebServiceOptions.requestTimeout	Maximum number of milliseconds that the Data Integration Service runs an operation mapping before the web service request times out. Default is 3,600,000.
WebServiceOptions.maxConcurrentRequests	Maximum number of requests that a web service can process at one time. Default is 10.
WebServiceOptions.sortOrder	Sort order that the Data Integration Service uses to sort and compare data when running in Unicode mode. Default is binary.
WebServiceOptions.EnableTransportLayerSecurity	Indicates that the web service must use HTTPS. If the Data Integration Service is not configured to use HTTPS, the web service will not start. Enter true or false.
WebServiceOptions.EnableWSSecurity	Enables the Data Integration Service to validate the user credentials and verify that the user has permission to run each web service operation. Enter true or false.

Option	Description
WebServiceOptions.optimizeLevel	The optimizer level that the Data Integration Service applies to the object. Enter the numeric value that is associated with the optimizer level that you want to configure. You can enter one of the following numeric values: - 0. The Data Integration Service does not apply optimization. - 1. The Data Integration Service applies the early projection optimization method. - 2. The Data Integration Service applies the early projection, early selection, push-into, and predicate optimization methods. - 3. The Data Integration Service applies the cost-based, early projection, early selection, push-into, predicate, and semi-join optimization methods.
WebServiceOptions.DTMKeepAliveTime	Number of milliseconds that the DTM instance stays open after it completes the last request. Web service requests that are issued against the same operation can reuse the open instance. Use the keep alive time to increase performance when the time required to process the request is small compared to the initialization time for the DTM instance. If the request fails, the DTM instance terminates. Must be an integer. A negative integer value means that the DTM Keep Alive Time for the Data Integration Service is used. 0 means that the Data Integration Service does not keep the DTM instance in memory. Default is -1.

CHAPTER 40

infacmd xrf Command Reference

This chapter includes the following topics:

generateReadableViewXML

Generates a readable XML file from an export XML file. The export XML file can contain exported domain or Model repository contents.

The command infacmd xrf generateReadableViewXML simplifies the process of editing an export XML file by exposing the values that you can edit. Use the readable XML file to modify values generated from the export XML file. For example, if you export a mapping saved in the Model repository, you can change the names of columns or edit the precision and scale of data types. If you want to make structural changes to values in the export XML file, use the Administrator tool or the Developer tool depending on whether you exported domain or Model repository contents.

The infacmd xrf generateReadableViewXML command uses the following syntax:

```
generateReadableViewXML

<-SourceExportFile|-sxf> source_export_file

<-TargetFile|-tf> target_file_Name
```

The following table describes infacmd xrf generateReadableViewXML options and arguments:

Option	Argument	Description
-SourceExportFile -sxf	source_export_file	Required. Path and file name of the export XML file.
-TargetFile -tf	target_file_Name	Required. Path and file name of the readable XML file.

updateExportXML

Updates an export XML file with the changes made to the corresponding readable XML file. You can update a readable XML file that contains Model repository contents and regenerate the export XML file with the changes.

The infacmd xrf updateExportXML command uses the following syntax:

```
updateExportXML

<SourceExportFile|-sxf> source_file
<generatedViewFile|-vf> view_file
<TargetFile|-tf> target_file_Name
```

The following table describes infacmd xrf updateExportXML options and arguments:

Option	Argument	Description
-SourceExportFile -sxf	source_file	Required. Path and file name of the export XML file.
-generatedViewFile -vf	view_file	Required. Path and file name of the readable XML file that contains the required changes.
-TargetFile -tf	target_file_Name	Required. Path and file name of the updated export XML file.

CHAPTER 41

infacmd Control Files

This chapter includes the following topics:

infacmd Control Files Overview

When you use the infacmd command line program to export and import objects, you can use a control file to filter the objects that the command exports or imports.

You can use the following control files with infacmd:

- Export control file. Use an export control file to specify the objects to export from the domain or Model repository to an export file.
- Import control file. Use an import control file to specify the objects to import from the export file into the domain or Model repository.

If you do not use an export control file during export, infacmd does not filter the objects exported from the domain or the specified Model repository project. If you do not use an import control file during import into the domain, infacmd imports all objects included in the export file. If you do not use an import control file during import into the Model repository, infacmd imports all objects included in the specified project in the export file.

Control File Configuration

A control file is an XML file based on an export or import schema file. You can create a control file based on the following schema files:

- exportControl.xsd. Defines the layout and syntax of export control files.
- importControl.xsd. Defines the layout and syntax of import control files.

You can access the schema files as part of the oie-util.jar in the following installation directory:

```
<InformaticaInstallationDir>/services/shared/jars/shapp
```

To access exportControl.xsd and importControl.xsd from the command line, navigate to the oie-util.jar location and extract the jar file with the following command:

```
jar -xvf <jar_name>
```

Also, you can extract the oie-util jar with decompression software, such as WinRAR, or view the xsd files from the oie-util jar with the Java decompiler to access the schema files.

To create an export control file, create an XML file based on the exportControl.xsd schema file. The file must begin with an XML declaration and the location of the hosted schema file in the exportParams root element. Include the following lines in the file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
...
</exportParams>
```

To create an import control file, create an XML file based on the importControl.xsd schema file. The file must begin with an XML declaration and the location of the hosted schema file in the importParams root element. Include the following lines in the file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
...
</importParams>
```

Include the remaining elements and attributes in the XML file based on the objects that you want to export or import.

Control File Naming Conventions

Use an easily distinguishable file name for the control files.

Add a prefix to each file name to indicate whether it is an export or import control file. For example, use the following suggested naming conventions:

- ecf_<file_name>.xml for export control files
- icf_<file_name>.xml for import control files

For control files for domain objects, you might also include the object type considered for export or import in the file name.

Export Control Files

An export control file is an XML file that you use with infacmd commands. The control file filters the objects that infacmd exports from a domain or Model repository.

You can use an export control file with the following commands:

infacmd isp ExportDomainObjects

Exports native users, native groups, roles, connections, and cluster configurations from the domain to an export file in XML format. When you specify an export control file for the command, you filter the objects that you want to export. For example, use a control file to export all objects created after a certain date or to export connections but no other object types.

infacmd oie ExportObjects

Exports all Model repository object types from a specified project to an export file in XML format. When you specify an export control file for the command, you filter the objects that you want to export. For example, use a control file to export all objects created by a specific user or to export specific object types in the project.

Infacmd does not export empty folders. When you export Model repository objects, infacmd also exports the dependent objects. A dependent object is an object that is used by another object. Dependent objects can be in the same or different projects.

An export control file uses different parameters based on whether you configure the file to export domain objects or Model repository objects.

Export Control File Parameters for Domain Objects

Use the export control file parameters to configure the objects that you want to export from the domain.

An export control file for domain objects can contain the following elements:

- exportParams. Can contain multiple objectList elements.
- objectList. Contains attributes to filter objects by type. Can contain multiple object elements.
- object. Contains an attribute to filter objects by name.

The following table lists the export control file elements that have configurable attributes:

Element	Attribute Name	Attribute Description
objectList	type	Required. Type of domain object to export. Specify one of the following values: - User - Group - Role - Cluster configuration. - Connection The value is not case sensitive.
objectList	createdBefore	Optional. Date and time. Exports objects of the specified type created before this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
objectList	createdAfter	Optional. Date and time. Exports objects of the specified type created after this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
objectList	lastUpdatedBefore	Optional. Date and time. Exports objects of the specified type updated before this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`

Element	Attribute Name	Attribute Description
objectList	lastUpdatedAfter	Optional. Date and time. Exports objects of the specified type updated after this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
object	name	Required. Name of the object to export. If the containing objectList element includes a time attribute, infacmd exports objects that match both the specified object name and the time filter. The value is not case sensitive.

Export Control File Sample for Domain Objects

The following code shows an example export control file for domain objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">

  <!-- Export a specific connection. -->
  <objectList type="connection" >
    <object name="connection1" />
  </objectList>

  <!-- Export groups created before the specified date and time. -->
  <objectList type="group" createdBefore="2010-11-12 10:00:00 +0530" />

  <!-- Export role1 and role2 if created after the specified date and time. -->
  <objectList type="role" createdAfter="2010-12-25 10:00:00 +0530">
    <object name="role1" />
    <object name="role2" />
  </objectList>

  <!-- Export all users. -->
  <objectList type="user" />
</exportParams>
```

Export Control File Parameters for Model Repository Objects

Use the export control file parameters to configure the objects that you want to export from the Model repository.

An export control file for Model repository objects can contain the following elements:

- exportParams. Can contain a single folders element.
- folders. Can contain multiple folder elements.
- folder. Contains attributes to filter objects in a specific folder. Can contain multiple objectList elements.
- objectList. Contains attributes to filter objects by type. Can contain multiple object elements.
- object. Contains an attribute to filter objects by name.

The following table describes the configurable attributes for the folder element in the export control file:

Attribute Name	Attribute Description
path	Optional. Path of the folder that contains the objects you want to export. Use the following format: "/<folder_name>/<folder_name>" For example, if a project contains a folder named F1, then the folder path of F1 is "/F1." To export all objects in the project, specify "/." The value is not case sensitive. Default is "/."
recursive	Optional. Indicates whether to export objects from subfolders of the specified folder. Set to true to export from subfolders. Valid values are true and false. The value is case sensitive. Default is true.
select	Optional. Indicates whether infacmd exports all remaining objects in the specified folder when you define an objectList element for the folder. Set to all to export all remaining objects. For example, the following lines export mappings that were created by user1. The lines export all remaining objects in the specified folder: <folder path="/Testfolder" select="all"> <objectList type="Mapping" createdBy="user1" /> </folder> If you define an objectList element and do not use the select attribute, then infacmd exports objects that satisfy the attributes defined in objectList. For example, the following lines export mappings that were created by user1 in the specified folder: <folder path="/Testfolder"> <objectList type="Mapping" createdBy="user1" /> </folder> If you do not define an objectList element for the folder, then the default value of the select attribute is all. For example, the following line exports all objects in the specified folder: <folder path="/Testfolder" /> Valid value is all.
createdBy	Optional. User name. Exports objects created by this user. The value is not case sensitive.
createdBefore	Optional. Date and time. Exports objects created before this date and time. Enter the date and time in the following format: yyyy-MM-dd HH:mm:ssZ
createdAfter	Optional. Date and time. Exports objects created after this date and time. Enter the date and time in the following format: yyyy-MM-dd HH:mm:ssZ
lastUpdatedBefore	Optional. Date and time. Exports objects updated before this date and time. Enter the date and time in the following format: yyyy-MM-dd HH:mm:ssZ
lastUpdatedAfter	Optional. Date and time. Exports objects updated after this date and time. Enter the date and time in the following format: yyyy-MM-dd HH:mm:ssZ
lastUpdatedBy	Optional. User name. Exports objects that were last updated by this user. The value is not case sensitive.

The following table describes the configurable attributes for the objectList element in the export control file:

Attribute Name	Attribute Description
type	Required. Type of Model repository object to export from the specified folder path. Valid values include all object types present in the Model repository. You can view the type of the object in the Properties view in the Developer tool. For example, you can enter "Relational Data Object" or "Profile." The value is not case sensitive.
createdBy	Optional. User name. Exports objects of the specified type created by this user. The value is not case sensitive.
createdBefore	Optional. Date and time. Exports objects of the specified type created before this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
createdAfter	Optional. Date and time. Exports objects of the specified type created after this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBefore	Optional. Date and time. Exports objects of the specified type updated before this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedAfter	Optional. Date and time. Exports objects of the specified type updated after this date and time. Enter the date and time in the following format: `yyyy-MM-dd HH:mm:ssZ`
lastUpdatedBy	Optional. User name. Exports objects of the specified type that were last updated by this user. The value is not case sensitive.

The following table describes the configurable attribute for the object element in the export control file:

Attribute Name	Attribute Description
name	Required. Name of the object to export. If the containing objectList element includes a user or time attribute, infacmd exports objects that match both the specified object name and the user or time filter. The value is case sensitive.

Export Control File Sample for Model Repository Objects

The following code shows an example export control file for Model repository objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
 <folders>

   <!-- Consider exporting all objects in the project. Do not export from subfolders. -->
   <folder recursive="false" select="all">

      <!-- Export mapping1 if created by the specified user. -->
      <objectList type="Mapping" createdBy="user1">
        <object name="mapping1"/>
      <!-- Export all other mappings. -->
      </objectList>

      <!-- Export Aggregator transformations created by the specified user. -->
```

```
      <objectList type="Aggregator" createdBy="user1" />

    <!-- Export all remaining objects. -->
    </folder>
 </folders>
</exportParams>
```

Import Control Files

An import control file is an XML file that you use with infacmd commands. The control file filters the objects that infacmd imports from an export file into a domain or Model repository.

You can use an import control file with the following commands:

infacmd isp ImportDomainObjects

Imports native users, native groups, roles, connections, and cluster configurations from an export file into a domain. When you specify an import control file for the command, you can complete the following tasks:

- Filter the objects that you want to import. For example, use the control file to import a specific object type.
- Configure conflict resolution strategies for specific object types or objects.

infacmd oie ImportObjects

Imports Model repository objects from an export file into a Model repository. When you specify an import control file for the command, you can complete the following tasks:

- Filter the objects that you want to import. For example, use the control file to import a specific object type.
- Configure conflict resolution strategies for specific object types or objects.
- Map connections in the source repository to connections in the target repository.

Dependent Model repository objects may exist in different folders or projects. You must include all dependent objects using folderMap elements in the import control file. Otherwise, the import might fail with an error message because a dependent object does not exist in the target repository.

You can define a conflict resolution strategy through the command line or control file when you import the objects. The control file takes precedence if you define conflict resolution in the command line and control file. The import fails if there is a conflict and you did not define a conflict resolution strategy.

If you define the rename conflict resolution strategy, you can specify a name in the control file for a specific object. Or, infacmd can generate a name by appending a sequential number to the end of the name.

An import control file uses different parameters based on whether you configure the file to import domain objects or Model repository objects.

Import Control File Parameters for Domain Objects

Use the import control file parameters to configure the objects that you want to import from an XML file into the domain.

An import control file for domain objects can contain the following elements:

- importParams. Can contain multiple objectList elements.

- objectList. Contains attributes to filter the objects by type. Can contain multiple object elements.
- object. Contains attributes to filter the objects by name.

The following table lists the import control file elements that have configurable attributes:

Element	Attribute Name	Attribute Description
objectList	type	Required. Type of domain object that you want to import. Specify one of the following values: - User - Group - Role - Cluster configuration - Connection The value is not case sensitive.

objectList	select	Optional. Indicates whether infacmd imports all remaining objects of the specified type when you define an object element for the objectList. Set to all to import all remaining objects. For example, the following lines import Group1 with a Reuse resolution strategy. The lines import all remaining groups with a Merge resolution strategy:
		`<objectList type="group" select="all" resolution="merge">`
		`  <object name="Group1" resolution="reuse" />`
		`</objectList>`
		If you define an object element and do not use the select attribute, then infacmd imports objects that satisfy the attributes defined in the object element. For example, the following lines import Group1 with a Merge resolution strategy:
		`<objectList type="group" resolution="merge">`
		`  <object name="Group1" />`
		`</objectList>`
		If you do not define an object element for the objectList, then the default value of the select attribute is all. For example, the following line imports all groups with a Merge resolution strategy:
		`<objectList type="group" resolution="merge" />`
		Valid value is all.

objectList	resolution	Optional. Resolution strategy when a name conflict occurs. Applies to all objects of the specified type. Specify one of the following values: - Replace. Replace target object with the source object. - Rename. Rename source object using a generated name, and then import it. You cannot use the Rename option with the cluster configuration type. - Reuse. Reuse object in the target domain. - Merge. Merge the objects into one object. This option is applicable for groups. The values are not case sensitive.
object	name	Required. Name of a specific object to import of the specified object type. The value is not case sensitive.

Element	Attribute Name	Attribute Description
object	resolution	Optional. Resolution strategy when a name conflict occurs for this object. Specify one of the following values: - Replace. Replace target object with the source object. - Rename. Rename source object, and then import it. You cannot use the Rename option with the cluster configuration type. - Reuse. Reuse object in the target domain. - Merge. Merge the objects into one object. This option is applicable for groups. The values are not case sensitive.
object	renameTo	Optional. Name to use when the conflict resolution strategy is Rename. If you do not specify a name, then infacmd generates a name by appending a number to the end of the name. Infacmd ignores the value if there are no conflicts or if the conflict resolution strategy is not Rename.
object	renameIdTo	Optional. ID string to use when you import a connection object and the conflict resolution strategy is Rename. If you do not specify a connection ID, then infacmd generates an ID by appending a number to the end of the connection ID. Infacmd ignores the value if there are no conflicts or if the conflict resolution strategy is not Rename.

Import Control File Sample for Domain Objects

The following code shows an example import control file for domain objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">

 <! -- Import all connections, roles, and users. -->
 <objectList type="connection" resolution="replace" />
 <objectList type="role" resolution="reuse" />
 <objectList type="user" resolution="rename" />

 <! -- Import specific groups. -->
 <objectList type="group">
  <object name="g1" resolution="replace" />
  <object name="g2" resolution="merge" />
 </objectList>
</importParams>
```

Import Control File Parameters for Model Repository Objects

Use the import control file parameters to configure the objects that you want to import from an XML file into the Model repository.

An import control file for Model repository objects can contain the following elements:

- importParams. Can contain a single folderMaps element and a single connectionInfo element.
- folderMaps. Can contain multiple folderMap elements.
- folderMap. Contains attributes to filter objects in a specific folder. Can contain multiple objectList elements.
- objectList. Contains attributes to filter objects by type. Can contain multiple object elements.
- object. Contains attributes to filter objects by name.
- connectionInfo. Can contain a single rebindMap element.

- rebindMap. Can contain multiple rebind elements.
- rebind. Contains attributes to map connections in the source repository to connections in the target repository.

The following table describes the configurable attributes for the folderMap element in the import control file:

Attribute Name	Attribute Description
sourceProject	Required. Name of the source project in the export file that contains the objects you want to import. The value is not case sensitive.
sourceFolderPath	Optional. Path of the source folder in the export file that contains the objects you want to import. Use the following format: "/<folder_name>/<folder_name>" For example, if a project contains a folder named F1, then the folder path of F1 is "/F1." To consider importing all objects in the project, specify "/." The value is not case sensitive. Default is "/."
targetProject	Required. Name of the project in the target repository into which you want to import objects. The project must exist in the repository before you import the objects. The value is not case sensitive.
targetFolderPath	Optional. Path of the folder in the target repository into which you want to import objects. Use the following format: "/<folder_name>/<folder_name>" For example, if a project contains a folder named F1, then the folder path of F1 is "/F1." To import all objects into the target project, specify "/." The folder must exist in the repository before you import the objects. The value is not case sensitive. Default is "/."
recursive	Optional. Indicates whether to import objects from subfolders of the specified folder. Set to true to import from subfolders. Valid values are true and false. The value is case sensitive. Default is true.

Attribute Name	Attribute Description

select	Optional. Indicates whether infacmd imports all remaining objects in the specified project when you define an objectList element for the folderMap. Set to all to import all remaining objects. For example, the following lines import mappings with a Reuse resolution strategy. The lines import all remaining objects with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2" select="all" resolution="replace">`
	`  <objectList type="Mapping" resolution="reuse" />`
	`</folderMap>`
	If you define an objectList element and do not use the select attribute, then infacmd imports objects that satisfy the attributes defined in objectList. For example, the following lines import mappings with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2" resolution="replace">`
	`  <objectList type="Mapping" />`
	`</folderMap>`
	If you do not define an objectList element for the folderMap, then the default value is all. For example, the following line imports all objects with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2" resolution="replace" />`
	Valid value is all.

resolution	Optional. Resolution strategy when a name conflict occurs. Applies to all objects in this folder. Specify one of the following values: - Rename. Rename source object using a generated name, and then import it. - Replace. Replace target object with the source object. - Reuse. Reuse object in the target Model repository. - None. The values are not case sensitive. Default is none.

The following table describes the configurable attributes for the objectList element in the import control file:

Attribute Name	Attribute Description
type	Required. Type of Model repository object to import to the specified folder path. Valid values include all object types present in the Model repository. You can view the type of the object in the Properties view in the Developer tool. For example, you can enter "Relational Data Object" or "Profile." The value is not case sensitive.

select	Optional. Indicates whether infacmd imports all remaining objects of the specified type when you define an object element for the objectList. Set to all to import all remaining objects. For example, the following lines import MyMapping with a Reuse resolution strategy. The lines import all remaining mappings with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" select="all" resolution="replace">`
	`  <object name="MyMapping" resolution="reuse" />`
	`  </objectList>`
	`</folderMap>`
	If you define an object element and do not use the select attribute, then infacmd imports objects that satisfy the attributes defined in the object element. For example, the following lines import the mapping named MyMapping with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" resolution="replace">`
	`  <object name="MyMapping"/>`
	`  </objectList>`
	`</folderMap>`
	If you do not define an object element for the objectList, then the default value is all. For example, the following lines import all mappings with a Replace resolution strategy:
	`<folderMap sourceProject="p1" targetProject="p2">`
	`  <objectList type="Mapping" resolution="replace" />`
	`</folderMap>`
	Valid value is all.

resolution	Optional. Resolution strategy when a name conflict occurs. Applies to all objects of the specified type. Specify one of the following values: - Rename. Rename source object using a generated name, and then import it. - Replace. Replace target object with the source object. - Reuse. Reuse object in the target Model repository. - None. The values are not case sensitive. Default is none.

The following table describes the configurable attributes for the object element in the import control file:

Attribute Name	Attribute Description
name	Required. Name of a specific object to import of the specified object type. The value is not case sensitive.
resolution	Optional. Resolution strategy when a name conflict occurs for this object. Specify one of the following values: - Rename. Rename source object, and then import it. - Replace. Replace target object with the source object. - Reuse. Reuse object in the target Model repository. - None. The values are not case sensitive. Default is none.

Attribute Name	Attribute Description
renameTo	Optional. Name to use when the conflict resolution strategy is Rename. If you do not specify a name, then infacmd generates a name by appending a number to the end of the name. Infacmd ignores the value if there are no conflicts or if the conflict resolution strategy is not Rename.
renameIdTo	Optional. ID string to use when you import a connection object and the conflict resolution strategy is Rename. If you do not specify a connection ID, then infacmd generates an ID by appending a number to the end of the connection ID. Infacmd ignores the value if there are no conflicts or if the conflict resolution strategy is not Rename.

The following table describes the configurable attributes for the rebind element in the import control file:

Attribute Name	Attribute Description
source	Required. Name of a source connection in the file that you are importing. The value is not case sensitive.
target	Required. Name of a connection in the target Model repository to map to the source connection. By default, the connection must exist in the target repository before you import the objects. If the connection does not exist, the import fails. When you run infacmd, you can choose to skip target connection validation during the import. When you skip target connection validation, the import succeeds if a connection does not exist in the target repository. The value is not case sensitive.

Import Control File Sample for Model Repository Objects

The following code shows an example import control file for Model Repository objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
 <folderMaps>
  <folderMap sourceProject="project1" sourceFolderPath="/f1" targetProject="project2"
targetFolderPath="/f1" recursive="true">

    <! -- Import mapping1 with the Rename resolution strategy. -->
    <objectList type="Mapping" select="all" resolution="replace">
      <object name="mapping1" resolution="rename" renameTo="mapping1_new"/>

    <! -- Import all remaining mappings with the Replace resolution strategy. -->
    </objectList>

    <! -- Import all Aggregator transformations with the Replace resolution strategy. -->
    <objectList type="Aggregator" resolution="replace"/>

    <! -- Import all Filter transformations with no resolution strategy. -->
    <objectList type="Filter" resolution="none"/>
  </folderMap>
 </folderMaps>

 <! -- Map connections in the source repository to connections in the target repository.
-->
 <connectionInfo>
  <rebindMap>
   <rebind source="src_Conn1" target="tgt_Conn1"/>
   <rebind source="src_Conn2" target="tgt_Conn2"/>
  </rebindMap>
 </connectionInfo>
</importParams>
```

Rules and Guidelines for Control Files

Review the following rules and guidelines before you create control files:

- Element and attribute names are case sensitive.
- Control files contain a hierarchy of XML elements. Elements at different levels can contain the same attribute. A child element inherits an attribute value defined for the parent element when the same attribute is not defined for the child element. The attribute values defined for a child element override the value of the same attribute defined for the parent element.
- When an element defines multiple attributes, infacmd exports or imports objects that match all attribute filters. For example, you define the createdBefore and lastUpdatedAfter attributes for an objectList element in an export control file. Infacmd exports objects of the specified type created before the specified date and last updated after the specified date.
- The values of time attributes are not inclusive. For example, you set createdAfter to “2011-02-01 16:00:00-0800” in an export control file. Infacmd considers exporting all objects created after 4 p.m. on February 1, 2011. Infacmd does not export objects created at 4 p.m. on February 1, 2011.
- You can specify an objectList of a specific type once in a control file for domain objects. For example, you specify an objectList where type is "connection." You cannot specify another objectList of type "connection" in the same file.
- You can specify an objectList of a specific type once in a folder or folderMap element for Model repository objects. For example, you specify an objectList where type is "Flat File Data Object." You cannot specify another objectList of the "Flat File Data Object" type in the same folder or folderMap element.

Control File Examples for Domain Objects

You can filter domain objects to export by time. You can filter domain objects to export and import by object type or object name.

Export Domain Objects by Time

To export users created after 2010-12-25 10:00:00 +0530, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="user" createdAfter="2010-12-25 10:00:00 +0530" />
</exportParams>
```

Export and Import Domain Objects by Type

To export all users, groups, and roles but not connections from a domain, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="role" />
  <objectList type="user" />
</exportParams>
```

To import the users and groups but not roles into the target domain, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="merge"/>
```

```
  <objectList type="user" resolution="replace" />
</importParams>
```

Export and Import Domain Objects by Name

You want to export all users and groups and the Developer and Analyst roles from the source domain. You want to export specific connections if they were created after 2011-02-01 16:00:00-0800. You might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
  <objectList type="group"/>
  <objectList type="user" />
  <objectList type="role">
    <object name="Developer" />
    <object name="Analyst" />
  </objectList>
  <objectList type="connection" createdAfter="2011-02-01 16:00:00-0800">
    <object name="Connection1" />
    <object name="Connection2" />
    <object name="Connection3" />
  </objectList>
</exportParams>
```

To import all users and groups and specific roles and connections into the target domain, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
  <objectList type="group" resolution="reuse" />
  <objectList type="user" resolution="reuse" />
  <objectList type="role">
    <object name="Developer" resolution="replace" />
    <object name="Analyst" resolution="replace" />
  </objectList>
  <objectList type="connection">
    <object name="Connection1" resolution="rename" renameTo="ProdConnection1" />
    <object name="Connection2" resolution="rename" renameTo="ProdConnection2" />
    <object name="Connection3" resolution="rename" renameTo="ProdConnection3" />
  </objectList>
</importParams>
```

Control File Examples for Model Repository Objects

You can filter the export of Model repository objects by time or user. You can filter the export or import of Model repository objects by object type or object name.

Export Model Repository Objects by Time

To export all objects in a folder named Folder1 that were created before 2011-02-01 16:00:00-0800, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" createdBefore="2011-02-01 16:00:00-0800" />
</folders>
</exportParams>
```

Export Model Repository Objects by User

To export all objects in the project last updated by Administrator, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder lastUpdatedBy="Administrator" />
</folders>
</exportParams>
```

Export and Import Model Repository Objects by Type

To export all mappings from a folder named Folder1, you might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" />
    <objectList type="Mapping" />
  </folder>
</folders>
</exportParams>
```

You want to export all mappings created by user2 and export all remaining objects created by user1. The createdBy attribute defined for the child objectList element overrides the same attribute defined for the parent folder element. You might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
  <folder path="/Folder1" select="all" createdBy="user1" />
    <objectList type="Mapping" createdBy="user2" />
  </folder>
</folders>
</exportParams>
```

You want to import all mappings from the export file. Some of the mappings exported from Folder1 contain dependent objects that existed in Folder2 in the source repository. To import dependent objects, you must include all dependent objects using folderMap elements in the import control file. You also want to map the connections in the source repository to connections in the target repository. You might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
<folderMaps>
  <folderMap sourceProject="DevProject" sourceFolderpath="/Folder1"
targetProject="TestProject" targetFolderPath="/TestFolder1" resolution="reuse">
    <objectList type="Mapping" />
  </folderMap>
  <folderMap sourceProject="DevProject" sourceFolderpath="/Folder2"
targetProject="TestProject" targetFolderPath="/TestFolder2" resolution="reuse" />
</folderMaps>
<connectionInfo>
  <rebindMap>
    <rebind source="src_connection1" target="tgt_connection1" />
    <rebind source="src_connection2" target="tgt_connection2" />
  </rebindMap>
</connectionInfo>
</importParams>
```

Export and Import Model Repository Objects by Name

You want to export a mapping named TestMapping that was created after 2010-11-11 23:59:59-0800. You want to export all remaining objects in the same folder. You might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<exportParams xmlns="http://www.informatica.com/oie/exportControl/9">
<folders>
```

```
  <folder path="/Folder1" select="all" />
    <objectList type="Mapping" createdAfter="2010-11-11 23:59:59-0800" >
      <object name="TestMapping" />
    </objectList>
  </folder>
</folders>
</exportParams>
```

An export file contains flat file and relational data objects. You want to import the flat file data object named NewFlatFileDataObject and all relational data objects from the export file. You might create the following control file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<importParams xmlns="http://www.informatica.com/oie/importControl/9">
 <folderMaps>
  <folderMap sourceProject="SampleProject" targetProject="SampleProject"
            targetFolderPath="/TestFolder">
   <objectList type="Flat File Data Object" resolution="replace" >
    <object name="NewFlatFileDataObject" />
   </objectList>
   <objectList type="Relational Data Object" resolution="replace" />
  </folderMap>
 </folderMaps>
</importParams>
```

CHAPTER 42

infasetup Command Reference

This chapter includes the following topics:

Using infasetup

infasetup is a command line program that you use to administer Informatica domains and nodes.

Use *infasetup* to modify domain and node properties after you install Informatica services with the Informatica installation program. For example, you can use *infasetup* to change the port number for a node after you install Informatica services on the node.

You can use *infasetup* to back up, restore, define, and delete domains, and to define and update nodes.

Running Commands

You invoke *infasetup* from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, *infasetup* is a batch file with a .bat extension. On UNIX, *infasetup* is a script file with a .sh extension.

To run infasetup commands:

1. Open a command prompt.

   On Windows, open the command prompt as administrator. If you do not open the command prompt as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.
2. At the command prompt, switch to the directory where the *infasetup* executable is located.

   By default, *infasetup* installs in the <InformaticaInstallationDir>/isp/bin directory.
3. Enter `infasetup` on Windows or `infasetup.sh` on UNIX followed by the command name and its required options and arguments. The command names are not case sensitive.

   For example:

   ```
   infasetup(.sh) command_name [-option1] argument_1 [-option2] argument_2...
   ```

Command Options

When you run *infasetup*, you enter options for each command, followed by the required arguments. Command options are preceded by a hyphen and are not case sensitive. Arguments follow the option.

For example, the following command updates a worker node with the name “Node1” and the address “Host1:9090”:

```
infasetup UpdateWorkerNode -nn Node1 -na Host1:9090
```

If you omit or incorrectly enter one of the required options, the command fails, and *infasetup* returns an error message.

infasetup Return Codes

infasetup indicates the success or failure of a command with a return code. Return code (0) indicates that the command succeeded. Return code (-1) indicates that the command failed.

Use the DOS or UNIX echo command immediately after running an *infasetup* command to see the return code for the command:

- In a DOS shell: `echo %ERRORLEVEL%`
- In a UNIX Bourne or Korn shell: `echo $?`
- In a UNIX C shell: `echo $status`

Using Database Connection Strings

Some *infasetup* commands use connection strings to connect to the domain configuration database. Specify the database host, database port, and database service name as part of the connection string.

You can use connection strings with the following *infasetup* commands:

- BackupDomain
- DefineDomain
- DefineGatewayNode
- DeleteDomain
- RestoreDomain
- UpdateGatewayNode

The following table lists the connection string syntax for each supported database:

Database Name	Connection String

Oracle	Oracle:
	`jdbc:informatica:oracle://host_name:port;SID=sid`
	Oracle RAC:
	`jdbc:informatica:oracle://host_name:port; ServiceName=[Service Name];AlternateServers=(server2:port);LoadBalancing=true`

Microsoft SQL Server	`jdbc:informatica:sqlserver://host_name:port; SelectMethod=cursor;DatabaseName=database_name`
IBM DB2	`jdbc:informatica:db2://host_name:port; DatabaseName=database_name`

BackupDomain

Backs up the configuration metadata for the domain. infasetup stores the backup domain metadata in a backup file with an extension of .mrep.

You must shut down the domain before you run this command.

When you run this command, *infasetup* backs up the domain configuration database tables to restore the domain to another database. You must back up the ISP_RUN_LOG table contents manually to get the previous workflow and session logs.

If the command fails with a Java memory error, increase the system memory available for infasetup. To increase the system memory, set the -Xmx value in the INFA_JAVA_CMD_OPTS environment variable.

The BackupDomain command uses the following syntax:

```
BackupDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
```

```
<-DatabaseType|-dt> database_type
[<-DatabaseServiceName|-ds> database_service_name]
<-BackupFile|-bf> backup_file_name
[<-Force|-f> overwrite_file]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]
<-DomainName|-dn> domain_name
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]
[<-EncryptionKeyLocation|-kl> encryption_key_location]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* BackupDomain options and arguments:

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	database_connection_string	Connection string used to connect to the domain configuration database. Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in double quotes.
-DatabaseUserName -du	database_user_name	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	database_password	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	database_type	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase

Option	Argument	Description
-DatabaseServiceName -ds	database_service_name	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-BackupFile -bf	backup_file_name	Required. Name and path for the backup file. If you do not specify a file path, *infasetup* creates the backup file in the current directory.
-Force -f	-	Optional. Overwrites the backup file if a file with the same name already exists.
-DomainName -dn	domain_name	Required. Name of the domain.
-Tablespace -ts	tablespace_name	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	schema_name	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Password for the database truststore file for the secure database.
-TrustedConnection -tc	-	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Directory that contains the current encryption key. You must specify the key location if the encryption key does not exist in the isp/config/nodemeta.xml file. The name of the encryption file is sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Path and file name of the truststore file for the secure domain repository database. Required if you configure a secure domain repository database for the domain.

DefineDomain

Creates a domain on the current machine. If you define a domain on a machine that hosts a domain, you must first stop the Informatica services on the machine. infasetup removes the existing domain and node settings. After you define the new domain, restart Informatica services.

To create a domain on a Windows machine, you must first open the host port or disable the firewall.

Do not include any characters after the option (-f) in the DefineDomain command. If you include extra characters, the command might fail with an unexpected error.

The DefineDomain command uses the following syntax:

```
DefineDomain
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
<-DomainName|-dn> domain_name
[<-DomainDescription|-de> domain_description]
<-AdministratorName|-ad> administrator_name
[<-Password|-pd> password]
[<-LicenseName|-ln> license_name]
[<-LicenseKeyFile|-lf> license_key_file]
<-LogServiceDirectory|-ld> log_service_directory
[<-SystemLogDirectory|-sld> system_log_directory]
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
[<-EnableSaml|-saml> enable_saml]
[<-IdpUrl|-iu> idp_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-SamlAssertionSigned|-sas> saml_assertion_signed]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AuthnContextComparsion|-acc> saml_requested_authn_context_comparsion_type]
[<-AuthnContextClassRef|-accr> saml_requested_authn_context_class_reference]
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
```

```
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypted_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypted_assertion_private_key_password]
[<-EnablePasswordComplexity|-pc> enable_password_complexity]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
<-MinProcessPort|-mi> minimum_port
<-MaxProcessPort|-ma> maximum_port
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ServiceResilienceTimeout|-sr> timeout_period_in_seconds]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-Timezone|-tz> log_service_timezone_GMT+00:00]
[<-Force|-f>]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-EnableHsts|-hsts> enable_http_strict_transport_security]
[<-PasswordLength|-pl> password_length]
[<-DigitCharacterCount|-dc> digit_character_count]
[<-SpecialCharacterCount|-scc> special_character_count]
[<-AlphabetCount|-ac> alphabet_count]
[<-maxPasswordValidDuration|-pvd> max_password_valid_duration_in_days]
[<-NotAllowedPreviousPasswordsCount|-ppc> not_allowed_previous_passwords_count]
```

The following table describes the infasetup DefineDomain options and arguments:

Option	Description
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Connection string used to connect to the domain configuration database. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in quotes.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If you do not see a value specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql

Option	Description
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	Optional. Name of the Microsoft SQL Server or PostgreSQL schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.
-DomainName -dn	Required. Name of the domain. Domain names must be between 1 and 79 characters and cannot contain spaces or the following characters: / * ? < > " |
-DomainDescription -de	Optional. Description of the domain.
-AdministratorName -ad	Required. Domain administrator user name. If the domain uses a single Kerberos realm to authenticate users, specify the samAccount name. If the domain uses Kerberos cross realm authentication, specify the fully qualified user principal name, including the realm name. For example: sysadmin@COMPANY.COM
-Password -pd	Optional for Kerberos domain. Domain administrator password. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~ When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.
-LicenseName -ln	Optional. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > " |

Option	Description
-LicenseKeyFile -lf	Optional. Path to the license key file.
-LogServiceDirectory -ld	Required. Shared directory path used by the Log Manager to store log event files. Verify that -ld does not match or contain the specified -sld value.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Verify that -ld does not match or contain the specified -sld value. Default is <INFA_home>/logs.
-NodeName -nn	Required. Name of the node. Node names must be between 1 and 79 characters and cannot contain spaces or the following characters: \ / * ? < > " |
-NodeAddress -na	Required. Host name and port number for the machine hosting the node. Choose an available port number.
-ServiceManagerPort -sp	Optional. Port number used by the Service Manager to listen for incoming connection requests.
-EnableTLS -tls	Optional. Configures secure communication among the services in the Informatica domain. If you use the default SSL certificates provided by Informatica, you do not need to specify the keystore and truststore options. If you do not use the default SSL certificate, you must specify the keystore and truststore options. Valid values are true or false. Default is false. If you specify the -tls option without a value, the Informatica domain uses secure communication among the services. To enable secure communication for the associated services or web applications, such as Administrator tool, Analyst tool, or Web Services Hub, configure the secure communication separately within the applications.
-NodeKeystore- -nk	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the keystore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem. If the keystore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_keystore.jks and infa_keystore.pem. You must use the same keystore file for all the nodes in the domain.
-NodeKeystorePass -nkp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the keystore infa_keystore.jks file.
-NodeTruststore -nt	Optional if you use the default SSL certificates from Informatica. Directory that contains the truststore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. If the truststore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_truststore.jks and infa_truststore.pem.

Option	Description
-NodeTruststorePass -ntp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the infa_truststore.jks file.
-CipherWhiteList -cwl	Optional. Comma-separated list of JSSE cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackList -cbl	Optional. Comma-separated list of JSSE cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherWhiteListFile -cwlf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackListFile -cblf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-EnableKerberos -krb	Optional. Configures the Informatica domain to use Kerberos authentication. Valid values are true or false. If true, the domain uses Kerberos authentication, and you cannot later change the authentication mode. After you enable Kerberos authentication, you cannot disable it. Default is false. If you specify the -krb option without a value, the Informatica domain uses Kerberos authentication.
-ServiceRealmName -srn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM

Option	Description
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<Informatica installation directory>/isp/config/keys`.
-SPNShareLevel -spnSL	Optional. Indicates the service principal level for the domain. Set the property to one of the following levels: - Process. The domain requires a unique service principal name (SPN) and keytab file for each node and each service on a node. The number of SPNs and keytab files required for each node depends on the number of service processes that run on the node. Use the node level option if the domain does not require a high level of security. - Node. The domain uses one SPN and keytab file for the node and all services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Default is process.
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-idpUrl -iu	Required if the -saml option is true. Specify the SAML identity provider URL.
-ServiceProviderId -spid	Optional. The relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you specified "Informatica" as the relying party trust name in AD FS, you do not need to specify a value.
-ClockSkewTolerance -cst	Optional. The allowed time difference between the identity provider host system clock and the system clock on the master gateway node. The lifetime of SAML tokens issued by the identity provider by is set according to the identity provider host system clock. The lifetime of a SAML token issued by the identity provider is valid if the start time or end time set in the token is within the specified number seconds of the system clock on the master gateway node. Values must be from 0 to 600 seconds. Default is 120 seconds.
-SamlAssertionSigned -sas	Optional. Set to TRUE to enable assertion signing by the identity provider. Default is FALSE.
-AssertionSigningCertificateAlias -asca	Required if SamlAssertionSigned is set to TRUE. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.
-SamlTrustStoreDir -std	Optional. The directory containing the custom truststore file required to use SAML authentication on gateway nodes within the domain. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.
-SamlTrustStorePassword -stp	Required if you use a custom truststore for SAML authentication. The password for the custom truststore file.

Option	Description
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore.
-AuthnContextComparsion -acc	Specifies the comparison method used to evaluate the requested authorization statement. One of the following: - MINIMUM. The authentication context in the authentication statement must be the exact match of at least one of the authentication contexts specified. - MAXIMUM. The authentication context in the authentication statement must be at least as strong (as deemed by the responder) as one of the authentication contexts specified. - BETTER. The authentication context in the authentication statement must be stronger (as deemed by the responder) than any one of the authentication contexts specified. - EXACT. The authentication context in the authentication statement must be as strong as possible (as deemed by the responder) without exceeding the strength of at least one of the authentication contexts specified. Default is Exact.
-AuthnContextClassRef -accr	The authentication context class. One of the following: - PASSWORD - PASSWORDPROTECTEDTRANSPORT
-SignSamlRequest -ssr	Set to true to enable signed request. Default is False.
-RequestSigningPrivateKeyAlias -rspa	Required if you enable signed request. Alias name of the private key present in the node SAML keystore using which SAML request should be signed.
-RequestSigningPrivateKeyPassword -rspp	Required if you enable signed request. Password to access the private key used for signing the SAML request.
-RequestSigningAlgorithm -rsa	Required if you enable signed request. Algorithm used to sign the request. One of the following: - RSA_SHA256 - DSA_SHA1 - DSA_SHA256 - RSA_SHA1 - RSA_SHA224 - RSA_SHA384 - RSA_SHA512 - ECDSA_SHA1 - ECDSA_SHA224 - ECDSA_SHA256 - ECDSA_SHA384 - ECDSA_SHA512 - RIPEMD160 - RSA_MD5

Option	Description
-SamlResponseSigned -srs	Set to true to enable signed response. Default is False.
-ResponseSigningCertificateAlias -rsca	Required if you enable signed response. Alias name of the certificate present in the gateway node SAML truststore using which SAML response signature will be validated.
-SamlAssertionEncrypted -sae	Required if you enable signed response. Set to true to enable encrypted assertion. Default is False.
-EncyptedAssertionPrivateKeyAlias -espa	Required if you enable encrypted assertion. Alias name of the private key present in the gateway node SAML keystore using which key used for encrypting the assertion will be decrypted.
-EncyptedAssertionPrivateKeyPassword -espp	Required if you enable encrypted assertion. Password to access the private key used for decrypting the assertion encryption key.
-EnablePasswordComplexity -pc	Optional. Enable password complexity to validate the password strength. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.
-AdminconsolePort -ap	Port to access Informatica Administrator.
-HttpsPort -hs	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-MinProcessPort -mi	Required. Minimum port number for application service processes that run on the node.
-MaxProcessPort -ma	Required. Maximum port number for application service processes that run on the node.

Option	Description
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from domain components on this port. Set this port number if you have multiple nodes on one machine or if the default port number is in use. Default is the node port number plus one.
-AdminconsoleShutdownPort -asp	Port number that controls shutdown for Informatica Administrator.
-BackupDirectory -bd	Optional. Directory to store repository backup files. The directory must be accessible by the node.
-ServiceResilienceTimeout -sr	Optional. Amount of time in seconds that *infasetup* tries to establish or reestablish a connection to the local domain. If you omit this option, *infasetup* uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If you do not see a value specified in the environment variable, the default of 180 seconds is used.
-ErrorLogLevel -el	Optional. Severity level for log events in the domain log. Default is info.
-ResourceFile -rf	Required. File that contains the list of available resources for the node. Use the file, nodeoptions.xml, located in the following location: `<Informatica installation directory>/isp/bin`
-TimeZone -tz	Optional. Time zone used by the Log Manager when it generates log event files. Default is GMT+00:00. Configure the time zone in the following format: `GMT(+/-)hh:mm`
-Force -f	Optional. Overwrites the database if a database with the same name already exists. Do not include any characters after this option.
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server. **Note:** If you use a trusted connection, configure the DatabaseConnectionString option.
-DatabaseTruststoreLocation -dbtl	Path and file name of the truststore file for the secure domain repository database. Required if you configure a secure domain repository database for the domain.
EnableHsts -hsts	Optional. Set to TRUE to enable HTTP strict transport security. HTTP strict transport security requires webapps to use HTTPS.
-PasswordLength -pl	Required if you enable the complexity of the password. The minimum number of characters required in a password. Enter a value between 8 and 255. Default is 8 characters.
-DigitCharacterCount -dc	Required if you enable the complexity of the password. The minimum number of numeric characters required in a password. Enter a value between 0 and 255. Default is 1 numeric character.

Option	Description
-SpecialCharacterCount -scc	Required if you enable the complexity of the password. The minimum number of special characters required in a password. Enter a value between 0 and 255. Default is 1 special character. You can use the following special characters: ! " # $ % & '( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~
-AlphabetCount -ac	Required if you enable the complexity of the password. The minimum number of alphabetic characters required in a password. Enter a value between 0 and 255. Default is 1 alphabetic character.
-maxPasswordValidDuration -pvd	Required if you enable the complexity of the password. The duration of password validity. If you don't want passwords to expire, set to 0. Default is 0.
-NotAllowedPreviousPasswordsCount -ppc	Required if you enable the complexity of the password. The number of consecutive previous passwords that can't be reused. Enter a value between 0 and 12. Default is 0.

If you run DefineDomain on a node that currently hosts a domain, reconfigure the following domain properties:

- **Application services.** Recreate any application service that ran on the domain.
- **Users.** Recreate users.
- **Gateway nodes.** Configure the gateway nodes in the domain.
- **General domain properties.** Configure resilience timeout and maximum restart attempts for the domain.
- **Grids.** Recreate any grid in the domain.
- **LDAP authentication**. Configure LDAP authentication for the domain.
- **Log Manager properties.** Configure the Log Manager shared directory path, purge properties, and time zone.

If you change the gateway node host name or port number, you must also add each node to the domain using the *infacmd* AddDomainNode command.

DefineGatewayNode

Defines a gateway node on the current machine. This command overwrites the nodemeta.xml file that stores the configuration metadata for the node. After you define the node, run the infacmd isp AddDomainNode command to add it to the domain.

The DefineGatewayNode command uses the following syntax:

```
DefineGatewayNode
<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
<-DomainName|-dn> domain_name
```

```
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-MinProcessPort|-mi> minimum_port]
[<-MaxProcessPort|-ma> maximum_port]
<-LogServiceDirectory|-ld> log_service_directory
[<-SystemLogDirectory|-sld> system_log_directory]
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* DefineGatewayNode options and arguments:

Option	Description
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	Connection string used to connect to the domain configuration database. Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in double quotes.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.

Option	Description
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-DomainName -dn	Required. Name of the domain.
-NodeName -nn	Optional. Name of the node. Node names must be between 1 and 79 characters and cannot contain spaces or the following characters: \ / * ? < > " |
-NodeAddress -na	Optional. Host name and port number for the machine hosting the node. Choose an available port number.
-ServiceManagerPort -sp	Optional. Port number used by the Service Manager to listen for incoming connection requests.
-EnableTLS -tls	Optional. Configures secure communication among the services in the Informatica domain. If you use the default SSL certificates provided by Informatica, you do not need to specify the keystore and truststore options. If you do not use the default SSL certificate, you must specify the keystore and truststore options. Valid values are true or false. Default is false. If you specify the -tls option without a value, the Informatica domain uses secure communication among the services. To enable secure communication for the associated services or web applications, such as Administrator tool, Analyst tool, or Web Services Hub, configure the secure communication separately within the applications.

Option	Description
-NodeKeystore -nk	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the keystore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem. If the keystore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_keystore.jks and infa_keystore.pem. You must use the same keystore file for all the nodes in the domain.
-NodeKeystorePass -nkp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the keystore infa_keystore.jks file.
-NodeTruststore -nt	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the truststore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. If the truststore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_truststore.jks and infa_truststore.pem.
-NodeTruststorePass -ntp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the infa_truststore.jks file.
-CipherWhiteList -cwl	Optional. Comma-separated list of JSSE cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackList -cbl	Optional. Comma-separated list of JSSE cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherWhiteListFile -cwlf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackListFile -cblf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-EnableKerberos -krb	Optional. Configures the Informatica domain to use Kerberos authentication. Valid values are true or false. If true, the domain uses Kerberos authentication, and you cannot later change the authentication mode. After you enable Kerberos authentication, you cannot disable it. Default is false. If you specify the -krb option without a value, the Informatica domain uses Kerberos authentication.

Option	Description
-ServiceRealmName -srn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-SamlTrustStoreDir -std	Optional. The directory containing the custom truststore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.
-SamlTrustStorePassword -stp	Required if you use a custom truststore for SAML authentication. The password for the custom truststore.
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore. *
-AdminconsolePort -ap	Optional. Port to access Informatica Administrator.
-HttpsPort -hs	Optional. Port number that the node uses for communication between the Administrator tool and the Service Manager. Set this port number if you want to configure HTTPS for a node. To disable HTTPS support for a node, set this port number to zero.

Option	Description
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-MinProcessPort -mi	Optional. Minimum port number for application service processes that run on the node. Default is 11000.
-MaxProcessPort -ma	Optional. Maximum port number for application service processes that run on the node. Default is 11999.
-LogServiceDirectory -ld	Required. Shared directory path used by the Log Manager to store log event files. Verify that -ld does not match or contain the specified -sld value.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Verify that -ld does not match or contain the specified -sld value. Default is <INFA_home>/logs.
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from PowerCenter components on this port. Set this port number if you have multiple nodes on one machine or if the default port number is in use. Default is 8005.
-AdminconsoleShutdownPort -asp	Optional. Port number that controls shutdown for Informatica Administrator.
-BackupDirectory -bd	Optional. Directory to store repository backup files. The directory must be accessible by the node.
-ErrorLogLevel -el	Optional. Severity level for log events in the domain log. Default is info.
-ResourceFile -rf	Required. File that contains the list of available resources for the node. Use the file nodeoptions.xml, located in the following directory: `<INFA_HOME>\isp\bin`.
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.

Option	Description
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-DatabaseTruststoreLocation -dbtl	Path and file name of the truststore file for the secure domain repository database. Required if you configure a secure domain repository database for the domain.
* Note: If you currently run scripts that use this command to enable a custom keystore for SAML authentication, you must update them to include this option.	

Related Topics:

- "AddDomainNode" on page 336

DefineWorkerNode

Defines a worker node on the current machine. infasetup creates the nodemeta.xml file that stores the configuration metadata for the node. If you run this command on an existing node, it overwrites the node configuration metadata. After you define the node, run infacmd isp AddDomainNode to add it to the domain.

The DefineWorkerNode command uses the following syntax:

```
DefineWorkerNode
<-DomainName|-dn> domain_name
<-NodeName|-nn> node_name
<-NodeAddress|-na> node_host:port
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-NodeKeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
<-GatewayAddress|-dg> domain_gateway_host:port
[<-UserName|-un> user_name]
[<-SecurityDomain|-sdn> security domain]
[<-Password|-pd> password]
[<-MinProcessPort|-mi> minimum_port]
[<-MaxProcessPort|-ma> maximum_port]
[<-ServerPort|-sv> server_shutdown_port]
[<-BackupDirectory|-bd> backup_directory]
[<-ErrorLogLevel|-el> FATAL_ERROR_WARNING_INFO_TRACE_DEBUG]
<-ResourceFile|-rf> resource_file
[<-SystemLogDirectory|-sld> system_log_directory]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
```

The following table describes *infasetup* DefineWorkerNode options and arguments:

Option	Description
-DomainName -dn	Required. Name of the domain the worker node links to.
-NodeName -nn	Required. Name of the node. Node names must be between 1 and 79 characters and cannot contain spaces or the following characters: \ / * ? < > " |
-NodeAddress -na	Required. Host name and port number for the machine hosting the node. Choose an available port number.
-ServiceManagerPort -sp	Optional. Port number used by the Service Manager to listen for incoming connection requests.
-EnableTLS -tls	Optional. Configures secure communication among the services in the Informatica domain. If you use the default SSL certificates provided by Informatica, you do not need to specify the keystore and truststore options. If you do not use the default SSL certificate, you must specify the keystore and truststore options. Valid values are true or false. Default is false. If you specify the -tls option without a value, the Informatica domain uses secure communication among the services. To enable secure communication for the associated services or web applications, such as Administrator tool, Analyst tool, or Web Services Hub, configure the secure communication separately within the applications.
-NodeKeystore -nk	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the keystore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem. If the keystore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_keystore.jks and infa_keystore.pem. You must use the same keystore file for all the nodes in the domain.
-NodeKeystorePass -nkp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the keystore infa_keystore.jks file.
-NodeTruststore -nt	Optional if you use the default SSL certificates from Informatica. Directory that contains the truststore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. If the truststore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_truststore.jks and infa_truststore.pem.
-NodeTruststorePass -ntp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the infa_truststore.jks file.
-CipherWhiteList -cwl	Optional. Comma-separated list of JSSE cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackList -cbl	Optional. Comma-separated list of JSSE cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.

Option	Description
-CipherWhiteListFile -cwlf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackListFile -cblf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-EnableKerberos -krb	Optional. Configures the Informatica domain to use Kerberos authentication. Valid values are true or false. If true, the domain uses Kerberos authentication, and you cannot later change the authentication mode. After you enable Kerberos authentication, you cannot disable it. Default is false. If you specify the -krb option without a value, the Informatica domain uses Kerberos authentication.
-ServiceRealmName -srn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-HttpsPort -hs	Optional. Port number that the node uses for communication between the Administrator tool and the Service Manager. Set this port number if you want to configure HTTPS for a node. To disable HTTPS support for a node, set this port number to zero.
-NodeKeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-GatewayAddress -dg	Required. Gateway host machine name and port number.

Option	Description
-UserName -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-SecurityDomain -sdn	Name of the security domain that you want to create to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-MinProcessPort -mi	Optional. Minimum port number for application service processes that run on the node. Default is 11000.
-MaxProcessPort -ma	Optional. Maximum port number for application service processes that run on the node. Default is 11999.
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from PowerCenter components on this port. Set this port number if you have multiple nodes on one machine or if the default port number is in use. Default is 8005.
-BackupDirectory -bd	Optional. Directory to store repository backup files. The directory must be accessible by the node.
-ErrorLogLevel -el	Optional. Severity level for log events in the domain log. One of the following: - fatal - error - warning - info - trace - debug Default is info.
-ResourceFile -rf	Required. File that contains the list of available resources for the node. Use the file nodeoptions.xml, located in the following directory: `<INFA_HOME>\isp\bin`.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Default is <INFA_home>/logs.

Option	Description
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-SamlTrustStoreDir -std	Optional. The directory containing the custom truststore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.
-SamlTrustStorePassword -stp	Required if you use a custom truststore for SAML authentication. The password for the custom truststore.
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore. *
* Note: If you currently run scripts that use this command to enable a custom keystore for SAML authentication, you must update them to include this option.	

DeleteDomain

Deletes domain metadata tables. Before you run this command, you must stop the Informatica services on the machine. To delete a domain on a Windows machine, you must also open the host port or disable the firewall.

If the command fails with a Java memory error, increase the system memory available for infasetup. To increase the system memory, set the -Xmx value in the INFA_JAVA_CMD_OPTS environment variable.

The DeleteDomain command uses the following syntax:

```
DeleteDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTrustStorePassword|-dbtp> database_truststore_password]
```

```
[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]
[<-EncryptionKeyLocation|-kl> encryption_key_location]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* DeleteDomain options and arguments:

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	database_connection_string	Connection string used to connect to the domain configuration database. Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in double quotes.
-DatabaseUserName -du	database_user_name	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	database_password	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	database_type	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	database_service_name	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-Tablespace -ts	tablespace_name	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.

Option	Argument	Description
SchemaName -sc	schema_name	Optional. Name of the Microsoft SQL Server or PostgreSQL schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Password for the database truststore file for the secure database.
-TrustedConnection -tc	-	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Directory that contains the current encryption key. The name of the encryption file is sitekey. Informatica renames the current sitekey file to sitekey_old and generates an encryption key in a new file named sitekey in the same directory.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Path and file name of the truststore file for the secure domain repository database. Required if you configure a secure domain repository database for the domain.

ExtendPasswordExpiry

Extends the password validity of users in a domain that uses native authentication.

The ExtendPasswordExpiry command uses the following syntax:

```
ExtendPasswordExpiry
<-UserName|-un> user_name
<-ExtensionPeriod|-exp> extend_password_expiry_in_days
```

The following table describes *infasetup* ExtendPasswordExpiry options and arguments:

Option	Argument	Description
-UserName -un	user_name	Required. Native user name.
-ExtensionPeriod -exp	extend_password_expiry_in_days	Required. The number of days to extend the duration of password validity.

GenerateEncryptionKey

Generate an encryption key to secure sensitive data, such as passwords, in the Informatica domain.

The GenerateEncryptionKey command uses the following syntax:

```
GenerateEncryptionKey [<-EncryptionKeyLocation|-kl> encryption_key_location]
```

-EncryptionKeyLocation. Directory that contains the current encryption key. The name of the encryption file is *sitekey*. Informatica renames the current *sitekey* file to *sitekey_old* and generates an encryption key in a new file named *sitekey* in the same directory.

To run the command again when there are at least two sitekey files in the directory, ensure that you back up the sitekey files. You can then run the command to create the sitekey file before you restore the backup sitekey files.

The *sitekey* is unique. Make sure that you save a copy of this unique site key. If you lose the site key, you cannot generate the site key again. Do not share the unique site key with others.

Help

The Help command displays the options and arguments for a command. If you omit the command name, *infasetup* lists all commands.

The Help command uses the following syntax:

```
Help [command]
```

For example, if you type `infasetup Help UpdateWorkerNode`, *infasetup* returns the following options and arguments for the UpdateWorkerNode command:

```
UpdateWorkerNode [<-DomainName|-dn> domain_name] <-NodeName|-nn> node_name][<-
NodeAddress|-na> node_host:port]
[<-GatewayAddress|-dg> domain_gateway_host:port][<-UserName|-un> user_name][<-Password|-
pd> password][<-ServerPort|-sv> server_admin_port_number]
```

The following table describes the *infasetup* Help option and argument:

Option	Argument	Description
-	command	Optional. Name of command. If you omit the command name, *infasetup* lists all commands.

ListDomainCiphers

Display one or more of the following cipher suite lists: blacklist, default list, effective list, or whitelist.

Blacklist

List of cipher suites that you want the Informatica domain to block. When you add a cipher suite to the blacklist, the Informatica domain removes the cipher suite from the effective list. You can add cipher suites that are on the default list to the blacklist.

Default list

List of cipher suites that the Informatica domain supports by default.

Whitelist

List of cipher suites that you want the Informatica domain to support in addition to the default list. When you add a cipher suite to the whitelist, the Informatica domain adds the cipher suite to the effective list. You do not need to add cipher suites that are on the default list to the whitelist.

The ListDomainCiphers command uses the following syntax:

```
[<-list|-l>] ALL|BLACK|DEFAULT|EFFECTIVE|WHITE

[<-domainConfig|-dc> true|false]
```

Note: You cannot run this command on a worker node.

The following table describes infasetup listDomainCiphers options and arguments:

Option	Argument	Description
-list -l	ALL BLACK DEFAULT EFFECTIVE WHITE	Optional. The cipher suite configuration list to display. The argument ALL displays the blacklist, default list, effective list, and whitelist. The argument BLACK displays the blacklist. The argument DEFAULT displays the default list. The argument EFFECTIVE displays the effective list. The argument WHITE displays the whitelist. **Note:** The arguments are case-sensitive. When you run the command on a gateway node and omit this option, the command displays all cipher suite configuration lists.
-domainConfig -dc	true false	Optional. Display the cipher suite lists for the Informatica domain or for the gateway node where you run the command. By default, the command displays cipher suite lists for the domain. Set this option to true to display the cipher suite lists for the domain. Set this option to false to display the cipher suite list for the gateway node where you run the command. **Note:** You cannot view whitelists or blacklists on gateway nodes.

MigrateEncryptionKey

Change the encryption key used to secure sensitive data, such as passwords, in the Informatica domain.

```
MigrateEncryptionKey

<-LocationOfEncryptionKeys|-loc> location_of_encryption_keys

[<-IsDomainMigrated|-mig> is_domain_migrated]
```

The following table describes *infasetup* MigrateEncryptionKey options and arguments:

Option	Argument	Description
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	Required. Directory in which the old encryption key file named siteKey_old and the new encryption key file named siteKey are stored. The directory must contain the old and new encryption key files. If the old and new encryption key files are stored in different directories, copy the encryption key files to the same directory. If the domain has multiple nodes, this directory must be accessible to any node in the domain where you run the migrateEncryptionKey command.
-IsDomainMigrated -mig	is_domain_migrated	Optional. Indicates whether the domain has been updated to use the latest encryption key. When you run the migrateEncryptionKey command for the first time, set this option to False to indicate that the domain uses the old encryption key. After the first time, when you run the migrateEncryptionKey command to update other nodes in the domain, set this option to True to indicate that the domain has been updated to use the latest encryption key. Or you can run the migrateEncryptionKey command without this option. Default is True.

RestoreDomain

Restores the configuration metadata for the domain from a backup .mrep file. If you have a backup file from an earlier version of Informatica, you must use the earlier version to restore the domain.

You must shut down the domain before you run this command.

If you restore the domain into a database other than the original backup database, you must restore the ISP_RUN_LOG table contents to get the previous workflow and session logs.

If the command fails with a Java memory error, increase the system memory available for infasetup. To increase the system memory, set the -Xmx value in the INFA_JAVA_CMD_OPTS environment variable.

The RestoreDomain command uses the following syntax:

```
RestoreDomain
<<-DatabaseAddress|-da> database_hostname:database_port|
<-DatabaseConnectionString|-cs> database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type
[<-DatabaseServiceName|-ds> database_service_name]
<-BackupFile|-bf> backup_file_name
```

```
[<-Force|-f>]
[<-ClearNodeAssociation|-ca>]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-EncryptionKeyLocation|-kl> encryption_key_location]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* RestoreDomain options and arguments:

Option	Argument	Description
-DatabaseAddress -da	database_hostname:database_port	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	database_connection_string	Connection string used to connect to the domain configuration database. Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in double quotes.
-DatabaseUserName -du	database_user_name	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	database_password	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	database_type	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	database_service_name	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.

Option	Argument	Description
-BackupFile -bf	backup_file_name	Required. Name and path for the backup file. If you do not specify a file path, *infasetup* creates the backup file in the current directory.
-Force -f	-	Optional. Overwrites the database if a database with the same name already exists. Do not include any characters after this option.
-ClearNodeAssociation -ca	-	Optional. Clears node associations when restoring the domain. For example, a backed up domain contains node “Node1” on machine “MyHost:9090.” If you specify this option, the connection between the node name “Node1” and the address “MyHost:9090” is broken when you restore the domain. You can then associate another node with “MyHost:9090.” If you do not specify this option, “Node1” retains its connection to “MyHost:9090.” If you restore the domain and associate another node with “MyHost:9090,” the node does not start.
-Tablespace -ts	tablespace_name	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	schema_name	Optional. Name of the Microsoft SQL Server or PostgreSQL schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	database_tls_enabled	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Optional. Password for the database truststore file for the secure database.
-TrustedConnection -tc	-	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-EncryptionKeyLocation -kl	encryption_key_location	Optional. Directory that contains the current encryption key. You must specify the key location if the encryption key does not exist in the isp/config/keys/sitekey file. The name of the encryption file is sitekey.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Optional. Path and file name of the truststore file for the secure database. Required if you configure a secure domain repository database for the domain.

restoreMitKerberosLinkage

Restores the linkages to the default Kerberos libraries that the Informatica domain uses for Kerberos authentication. The command also removes linkages to any custom Kerberos libraries that exist within the Informatica domain.

To use the default Kerberos libraries in an Informatica domain, do the following:

1. Shut down the domain.
2. Run the infasetup restoreMitKerberosLinkage command on each node in the domain.
3. Start the domain after the command is run on all nodes in the domain.

The command does not use any options or arguments. You must Read and Write permissions on every node in the Informatica domain to run the command.

SwitchToKerberosMode

Configure the Informatica domain to use Kerberos authentication.

The SwitchToKerberosMode command uses the following syntax:

```
SwitchToKerberosMode

<-administratorName|-ad> administrator_name

<-ServiceRealmName|-srn> realm_name_of_node_spn

<-UserRealmName|-urn> realm_name_of_user_spn

[<-SPNShareLevel|-spnSL> SPNShareLevel PROCESS|NODE]
```

The following table describes *infasetup* SwitchToKerberosMode options and arguments:

Option	Argument	Description
-administratorName -ad	administrator_name	Required. User name for the domain administrator account that is created when you configure Kerberos authentication. Specify the name of an account that exists in Active Directory. After you configure Kerberos authentication, this user is included in the *_infaInternalNamespace* security domain that the command creates. If the domain uses a single Kerberos realm to authenticate users, specify the samAccount name. If the domain uses Kerberos cross realm authentication, specify the fully qualified user principal name, including the realm name. For example: sysadmin@COMPANY.COM
-ServiceRealmName -srn	realm_name_of_node_spn	Required. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM

Option	Argument	Description
-UserRealmName -urn	realm_name_of_user_spn	Required. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
SPNShareLevel -spnSL	SPNShareLevel PROCESS|NODE]	Optional. Indicates the service principal level for the domain. Set the property to one of the following levels: - Process. The domain requires a unique service principal name (SPN) and keytab file for each node and each service on a node. The number of SPNs and keytab files required for each node depends on the number of service processes that run on the node. Recommended for production domains. - Node. The domain uses one SPN and keytab file for the node and all services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Recommended for test and development domains. Recommended for test and development domains. Default is process.

UpdateDomainCiphers

Update the Informatica domain to use a new effective list. Modify the whitelist to add cipher suites to the effective list. Modify the blacklist to remove cipher suites from the effective list.

Before you run the command verify that the following requirements are met:

- The domain uses secure communication within the domain or secure connections to web clients.
- The domain is shutdown.
- You are able to run the command on a gateway node in the domain.

The effective list of cipher suites contains the cipher suites that the Informatica domain supports. When you run the UpdateDomainCiphers command, the Informatica domain creates the effective list of cipher suites based on the following lists:

Blacklist

List of cipher suites that you want the Informatica domain to block. When you add a cipher suite to the blacklist, the Informatica domain removes the cipher suite from the effective list. You can add cipher suites that are on the default list to the blacklist.

Default list

List of cipher suites that the Informatica domain supports by default.

Whitelist

List of cipher suites that you want the Informatica domain to support in addition to the default list. When you add a cipher suite to the whitelist, the Informatica domain adds the cipher suite to the effective list. You do not need to add cipher suites that are on the default list to the whitelist.

Consider the following guidelines when you run the UpdateDomainCiphers command:

- When you run the command, you create a new effective that overrides the previous effective list.
- When you run the command and specify a whitelist or blacklist, the new whitelist or blacklist overwrites the previous list.
- The effective list includes the cipher suites in the default list and whitelist and excludes the cipher suites in the blacklist.
- When you run the command and do not specify a white or blacklist, the command creates an effective list that uses the cipher suites in the default list.
- The effective list must contain at least one cipher suite that TLS v1.1 or 1.2 supports.
- The effective list must be a valid cipher suite for Windows, the Java Runtime Environment, and OpenSSL.

For more information about how to create whitelists and blacklists to update the effective list that the Informatica domain uses, see the *Informatica Security Guide*.

The UpdateDomainCiphers command uses the following syntax:

```
[<-preview|-p> true|false]

[<-cipherWhiteList|-cwl> ciphersuite1,ciphersuite2,...]

[<-cipherWhiteListFile|-cwlf> whitelist_file_name]

[<-cipherBlackList|-cbl> ciphersuite1,ciphersuite2,...]

[<-cipherBlackListFile|-cblf> blacklist_file_name]
```

The following table describes infasetup UpdateDomainCiphers options and arguments:

Option	Argument	Description
-preview -p	true false	Optional. If true, the command displays the effective list of cipher suites that the domain will use. If false, the command updates the cipher suites for the Informatica domain to use the effective list of cipher suites. The default is false.
-cipherWhiteList -cwl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Comma-separated list of cipher suites that you want to add to the effective list. Use the full IANA TLS Cipher Suite Registry name or a regular Java expression. This list overwrites the previous whitelist. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.

Option	Argument	Description
-cipherWhiteListFile -cwlf	whitelist_file_location	Optional. Absolute file path and filename of a plain-text file that contains a comma-separated list of cipher suites that you want to add to the effective list. This list overwrites the previous whitelist. Use the full IANA TLS Cipher Suite Registry name or a regular Java expression. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-cipherBlackList -cbl	CipherSuiteName01,CiphersuiteName02, ...	Optional. Comma-separated list of cipher suites that you want to remove from the effective list. Use the full IANA TLS Cipher Suite Registry name or a regular Java expression. This list overwrites the previous blacklist. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-cipherBlackListFile -cblf	blacklist_file_location	Optional. Absolute file path and filename of a plain-text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. Use the full IANA TLS Cipher Suite Registry name or a regular Java expression. This list overwrites the previous. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.

updateDomainName

Changes the domain name in the domain configuration database.

Before you update the domain name, you must back up the domain, the site specific key, and keytab files. If the PowerCenter repository contains a global repository, you must unregister all local repositories from the global repository.

To update the domain name, run the infasetup updateDomainName command from any gateway node.

After you update the domain, perform the following steps:

1. Run the updateGatewayNode and updateWorkerNode commands with the updated domain name for all the gateway and worker nodes.
2. You can register the local repository with a connected global repository with the updated domain name with the pmrep Register command.
3. You can create SPN and keytab files with the updated domain name for Kerberos authentication. Copy the keytab files in the keys directory. You can continue to use the older site key file. If you need to regenerate the site key when it is missing or corrupted, you must provide the older domain name.
4. You must configure the Informatica clients to use the updated domain name.

The updateDomainName command uses the following syntax:

```
updateDomainName
-dn <domain_name>
```

The following table describes the *infasetup* updateDomainName option and argument:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Changes the domain name. Domain names must be between 1 and 79 characters and cannot contain spaces or the following characters: / * ? < > " |

UpdateGatewayNode

Updates connectivity information for a gateway node on the current machine. Before you update the gateway node, run the infacmd isp ShutDownNode command to shut down the node.

The UpdateGatewayNode command uses the following syntax:

```
UpdateGatewayNode
[<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string]
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
[<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL]
[<-DatabaseServiceName|-ds> database_service_name]
[<-DomainName|-dn> domain_name]
[<-NodeName|-nn> node_name]
[<-NodeAddress|-na> node_host:port]
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-EnableSaml|-saml> enable_saml]
[<-SamlTrustStoreDir|-std> saml_truststore_directory]
[<-SamlTrustStorePassword|-stp> saml_truststore_password]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
[<-AdminconsolePort|-ap> admin_tool_port]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-LogServiceDirectory|-ld> log_service_directory]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-ServerPort|-sv> server_shutdown_port]
[<-AdminconsoleShutdownPort|-asp> admin_tool_shutdown_port]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer only)]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-resetHostPort|-rst> resetHostPort]
```

The following table describes *infasetup* UpdateGatewayNode options and arguments:

Option	Description
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	Connection string used to connect to the domain configuration database. Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in double quotes.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-DomainName -dn	Optional. Name of the domain.
-NodeName -nn	Optional. Name of the node. Node names must be between 1 and 79 characters and cannot contain spaces or the following characters: \ / * ? < > " |
-NodeAddress -na	Optional. Host name and port number for the machine hosting the node. Choose an available port number.
-ServiceManagerPort -sp	Optional. Port number used by the Service Manager to listen for incoming connection requests.

Option	Description
-EnableTLS -tls	Optional. Configures secure communication among the services in the Informatica domain. If you use the default SSL certificates provided by Informatica, you do not need to specify the keystore and truststore options. If you do not use the default SSL certificate, you must specify the keystore and truststore options. Valid values are true or false. Default is false. If you specify the -tls option without a value, the Informatica domain uses secure communication among the services. To enable secure communication for the associated services or web applications, such as Administrator tool, Analyst tool, or Web Services Hub, configure the secure communication separately within the applications.
-NodeKeystore -nk	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the keystore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem. If the keystore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_keystore.jks and infa_keystore.pem. You must use the same keystore file for all the nodes in the domain.
-NodeKeystorePass -nkp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the keystore infa_keystore.jks file.
-NodeTruststore -nt	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the truststore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. If the truststore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_truststore.jks and infa_truststore.pem.
-NodeTruststorePass -ntp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the infa_truststore.jks file.
-CipherWhiteList -cwl	Optional. Comma-separated list of JSSE cipher suites that you want to add to the effective list. This list overwrites the previous whitelist. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackList -cbl	Optional. Comma-separated list of JSSE cipher suites that you want to remove from the effective list. This list overwrites the previous blacklist. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherWhiteListFile -cwlf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to add to the effective list. This list overwrites the previous whitelist. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.

Option	Description
-CipherBlackListFile -cblf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. This list overwrites the previous blacklist. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-EnableKerberos -krb	Optional. Configures the Informatica domain to use Kerberos authentication. Valid values are true or false. If true, the domain uses Kerberos authentication, and you cannot later change the authentication mode. After you enable Kerberos authentication, you cannot disable it. Default is false. If you specify the -krb option without a value, the Informatica domain uses Kerberos authentication.
-ServiceRealmName -srn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-SamlTrustStoreDir -std	Optional. The directory containing the custom truststore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.
-SamlTrustStorePassword -stp	Required if you use a custom truststore for SAML authentication. The password for the custom truststore.

Option	Description
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore.
-AdminconsolePort -ap	Optional. Port to access Informatica Administrator.
-HttpsPort -hs	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node. To disable HTTPS support for a node, set this port number to zero.
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-LogServiceDirectory -ld	Optional. Shared directory path used by the Log Manager to store log event files. Verify that -ld does not match or contain the specified -sld value.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Verify that -ld does not match or contain the specified -sld value. Default is <INFA_home>/logs.
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from PowerCenter components on this port. Set this port number if you have multiple nodes on one machine or if the default port - number is in use. Default is 8005.
-AdminconsoleShutdownPort -asp	Optional. Port number that controls shutdown for Informatica Administrator.
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.

Option	Description
-resetHostPort -rst	Required if you specify the NodeAddress or ServiceManager option. Resets the host port number.
-DatabaseTruststoreLocation -dbtl	Optional. Path and file name of the truststore file for the gateway node.

UpdateKerberosAdminUser

Updates the default Kerberos administrator user in the domain repository.

The UpdateKerberosAdminUser command uses the following syntax:

```
UpdateKerberosAdminUser

<-KerberosAdminName|-kan> kerberos_admin_name
```

The following table describes *infasetup* UpdateKerberosAdminUser options and arguments:

Option	Argument	Description
-KerberosAdminName -kan	kerberos_admin_name	Required. Name of the user to select as the default administrator. If the domain uses a single Kerberos realm to authenticate users, specify the samAccount name. If the domain uses Kerberos cross realm authentication, specify the fully qualified user principal name, including the realm name. For example: sysadmin@COMPANY.COM

UpdateKerberosConfig

Use the UpdateKerberosConfig command to correct the realm name or service realm name in the Informatica configuration. You can change the user realm that the Informatica domain users belong to. You can change the service realm that the Informatica domain services belong to.

Note: This command does not change the Kerberos configuration. You cannot use this command to migrate users from one user realm or service realm to another user realm or service realm.

The UpdateKerberosConfig command uses the following syntax:

```
UpdateKerberosConfig

[<-ServiceRealmName|-srn> realm_name_of_node_spn]

[<-UserRealmName|-urn> realm_name_of_user_spn]
```

The following table describes *infasetup* UpdateKerberosConfig options and arguments:

Option	Argument	Description
-ServiceRealmName -srn	realm_name_of_node_spn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	realm_name_of_user_spn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM

updateMitKerberosLinkage

Configures custom database clients and the Informatica domain to use the specified custom Kerberos libraries instead of the default libraries that Informatica uses.

To use custom Kerberos libraries, do the following:

1. Copy the custom Kerberos libraries you want to use to each node, or to a location that is accessible to all nodes in the Informatica domain.
2. Shut down the domain.
3. Run the infasetup updateMitKerberosLinkage command on each node in the domain.
4. Start the domain after running the command on all nodes in the domain.

The updateMitKerberosLinkage command uses the following syntax:

```
updateMitKerberosLinkage
<-useKeberos|-krb> true|false
[<-mitKerberosDirectory|-mkd> kerberos_library_directory]
```

The following table describes the infasetup updateMitKerberosLinkage options and arguments:

Option	Argument	Description
-useKeberos -krb	true|false	Required. Boolean value. Set this value to true if the Informatica domain uses Kerberos authentication. If true, Informatica processes make Kerberos calls with the default Kerberos libraries or the libraries in the directory specified with the -mkd option. Set this value to false if the Informatica domain does not use Kerberos. If false, Informatica does not load Kerberos libraries. Third-party clients, such as database clients, perform Kerberos calls with the libraries specified in the directory specified with the -mkd option.
-mitKerberosDirectory -mkd	kerberos_library_directory_node_spn	Optional. The directory that contains the custom MIT Kerberos libraries. The directory must contain the library files. You cannot use symbolic links. If the -krb option is true, ensure that the custom Kerberos libraries that you want to use are the same version number as the Kerberos libraries that Informatica uses by default. If there are multiple versions of the same library, all versions must be the same size and have the same checksum. For instance, if the directory contains two versions of libkrb5, such as libkr5.so.3 and libkrb5.so, then both libraries should have the same file size and checksum value. If the specified directory is empty, the command removes all custom Kerberos libraries from the Informatica domain.

UpdatePasswordConfig

Updates the password complexity rules for the domain.

The infasetup UpdatePasswordConfig command uses the following syntax:

```
UpdatePasswordConfig
[<-EnablePasswordComplexity|-pc> enable_password_complexity]
[<-PasswordLength|-pl> password_length]
[<-DigitCharacterCount|-dc> digit_character_count]
[<-SpecialCharacterCount|-scc> special_character_count]
[<-AlphabetCount|-ac> alphabet_count]
[<-maxPasswordValidDuration|-pvd> max_password_valid_duration_in_days]
[<-NotAllowedPreviousPasswordsCount|-ppc> not_allowed_previous_passwords_count]
```

The following table describes infasetup UpdatePasswordConfig options and arguments:

Option	Description
-EnablePasswordComplexity -pc	Optional. Enable password complexity to validate the password strength. By default this option is disabled. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~ When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.
-PasswordLength -pl	Required if you enable the complexity of the password. The minimum number of characters required in a password. Enter a value between 8 and 255. Default is 8 characters.
-DigitCharacterCount -dc	Required if you enable the complexity of the password. The minimum number of numeric characters required in a password. Enter a value between 0 and 255. Default is 1 numeric character.
-SpecialCharacterCount -scc	Required if you enable the complexity of the password. The minimum number of special characters required in a password. Enter a value between 0 and 255. Default is 1 special character. You can use the following special characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~
-AlphabetCount -ac	Required if you enable the complexity of the password. The minimum number of alphabetic characters required in a password. Enter a value between 0 and 255. Default is 1 alphabetic character.
-maxPasswordValidDuration -pvd	Required if you enable the complexity of the password. The duration of password validity. If you don't want passwords to expire, set to 0. Default is 0.
-NotAllowedPreviousPasswordsCount -ppc	Required if you enable the complexity of the password. The number of consecutive previous passwords that can't be reused. Enter a value between 0 and 12. Default is 0.

updateDomainSamlConfig

Enables or disables Secure Assertion Markup Language (SAML) authentication for Informatica web applications in an Informatica domain. You can also use the command to update the identity provider URL and specify allowed time difference between the identity provider host system clock and the system clock on the master gateway node.

Run the command on each gateway node within the Informatica domain. Shut down the domain before you run the command.

The infasetup updateDomainSamlConfig command uses the following syntax:

```
updateDomainSamlConfig
[<-EnableSaml|-saml> enable_saml]
[<-IdpUrl|-iu> idp_url]
[<-ServiceProviderId|-spid> service_provider_id]
[<-ClockSkewTolerance|-cst> clock_skew_tolerance_in_seconds]
[<-SamlAssertionSigned|-sas> sign_saml_assertion]
[<-AssertionSigningCertificateAlias|-asca> idp_assertion_signing_certificate_alias]
[<-AuthnContextComparsion|-acc> saml_requested_authn_context_comparsion_type]
[<-AuthnContextClassRef|-accr> saml_requested_authn_context_class_reference]
[<-SignSamlRequest|-ssr> sign_saml_request]
[<-RequestSigningPrivateKeyAlias|-rspa> saml_request_signing_private_key_alias]
[<-RequestSigningPrivateKeyPassword|-rspp> saml_request_signing_private_key_password]
[<-RequestSigningAlgorithm|-rsa> saml_request_signing_algorithm]
[<-SamlResponseSigned|-srs> saml_response_signed]
[<-ResponseSigningCertificateAlias|-rsca> idp_response_signing_certificate_alias]
[<-SamlAssertionEncrypted|-sae> saml_assertion_encrypted]
[<-EncryptedAssertionPrivateKeyAlias|-eapa> saml_encrypt_assertion_private_key_alias]
[<-EncryptedAssertionPrivateKeyPassword|-eapp>
saml_encrypt_assertion_private_key_password]
```

The following table describes the infasetup updateDomainSamlConfig options and arguments:

Option	Description
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-idpUrl -iu	Required if the -saml option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	Optional. The relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you specified "Informatica" as the relying party trust name in AD FS, you do not need to specify a value.
-ClockSkewTolerance -cst	Optional. The allowed time difference between the identity provider host system clock and the system clock on the master gateway node. The lifetime of SAML tokens issued by the identity provider by is set according to the identity provider host system clock. The lifetime of a SAML token issued by the identity provider is valid if the start time or end time set in the token is within the specified number seconds of the system clock on the master gateway node. Values must be from 0 to 600 seconds. Default is 120 seconds.
-SamlAssertionSigned -sas	Optional. Set to TRUE to enable assertion signing by the identity provider. Default is FALSE.
-AssertionSigningCertificateAlias -asca	Required if SamlAssertionSigned is set to TRUE. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.

Option	Description
-AuthnContextComparsion -acc	Specifies the comparison method used to evaluate the requested authorization statement. One of the following: - MINIMUM. The authentication context in the authentication statement must be the exact match of at least one of the authentication contexts specified. - MAXIMUM. The authentication context in the authentication statement must be at least as strong (as deemed by the responder) as one of the authentication contexts specified. - BETTER. The authentication context in the authentication statement must be stronger (as deemed by the responder) than any one of the authentication contexts specified. - EXACT. The authentication context in the authentication statement must be as strong as possible (as deemed by the responder) without exceeding the strength of at least one of the authentication contexts specified Default is Exact.
-AuthnContextClassRef -accr	The authentication context class. One of the following: - PASSWORD - PASSWORDPROTECTEDTRANSPORT
-SignSamlRequest -ssr	Set to true to enable request signing Default is False.
-RequestSigningPrivateKeyAlias -rspa	Required if you enable signed request. Alias name of the private key that Informatica uses to sign the request. This private key resides in the keystore in the gateway node. The corresponding public key (usually a certificate) should be imported to the identity provider.
-RequestSigningPrivateKeyPassword -rspp	Plaintext password of the private key that Informatica uses to sign the request. Default is the password of private key present in the keystore file `<Informatica home>\services\shared\security\infa_keystore.jks` with the alias "Informatica LLC".
-RequestSigningAlgorithm -rsa	Required if you enable signed request. Algorithm used to sign the request. One of the following: - RSA_SHA256 - DSA_SHA1 - DSA_SHA256 - RSA_SHA1 - RSA_SHA224 - RSA_SHA384 - RSA_SHA512 - ECDSA_SHA1 - ECDSA_SHA224 - ECDSA_SHA256 - ECDSA_SHA384 - ECDSA_SHA512 - RIPEMD160 - RSA_MD5
-SamlResponseSigned -srs	Set to true to specify whether the IDP signs the SAML response. **Note:** When set to TRUE, requires the IDP administrator to configure the identify provider to sign the response. Default is False.

Option	Description
-ResponseSigningCertificateAlias -rsca	Required if you enable signed response. Alias name of the certificate in the gateway node SAML truststore to use to verify the signature.
-SamlAssertionEncrypted -sae	Set to true to specify that the IDP encrypts the assertion. **Note:** When set to TRUE, requires the IDP administrator to configure the identify provider to encrypt the assertion. Default is False.
-EncyptedAssertionPrivateKeyAlias -eapa	Alias name of the private key present in the gateway node SAML keystore. The private key is used for encrypting the assertion. The IDP administrator must import the corresponding public key (usually a certificate).
-EncyptedAssertionPrivateKeyPassword -eapp	Plaintext password. Default is the password of private key present in the keystore file `<Informatica home>\services\shared\security\infa_keystore.jks` with the alias "Informatica LLC".

UpdateWorkerNode

Updates connectivity information for a worker node on the current machine. Before you update the worker node, run the infacmd isp ShutDownNode command to shut down the node.

The UpdateWorkerNode command uses the following syntax:

```
UpdateWorkerNode
[<-DomainName|-dn> domain_name]
[<-NodeName|-nn> node_name]
[<-NodeAddress|-na> node_host:port]
[<-ServiceManagerPort|-sp> service_manager_port]
[<-EnableTLS|-tls> enable_tls]
[<-NodeKeystore|-nk> node_keystore_directory]
[<-NodeKeystorePass|-nkp> node_keystore_password]
[<-NodeTruststore|-nt> node_truststore_directory]
[<-NodeTruststorePass|-ntp> node_truststore_password]
[<-CipherWhiteList|-cwl> comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackList|-cbl> comma_separated_black_list_jsse_cipher_names]
[<-CipherWhiteListFile|-cwlf>
absolute_filename_containing_comma_separated_white_list_jsse_cipher_names]
[<-CipherBlackListFile|-cblf>
absolute_filename_containing_comma_separated_black_list_jsse_cipher_names]
[<-EnableKerberos|-krb> enable_kerberos]
[<-ServiceRealmName|-srn> realm_name_of_node_spn]
[<-UserRealmName|-urn> realm_name_of_user_spn]
[<-KeysDirectory|-kd> Infa_keys_directory_location]
[<-HttpsPort|-hs> admin_tool_https_port]
[<-KeystoreFile|-kf> admin_tool_keystore_file_location]
[<-KeystorePass|-kp> admin_tool_keystore_password]
[<-GatewayAddress|-dg> domain_gateway_host:port]
[<-UserName|-un> user_name]
[<-SecurityDomain|-sdn> security domain]
[<-Password|-pd> password]
[<-ServerPort|-sv> server_shutdown_port]
[<-resetHostPort|-rst> resetHostPort]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-EnableSaml|-saml> enable_saml]
[<-SamlKeyStoreDir|-skd> saml_keystore_directory]
[<-SamlKeyStorePassword|-skp> saml_keystore_password]
```

The following table describes *infasetup* UpdateWorkerNode options and arguments:

Option	Description
-DomainName -dn	Optional. Name of the domain.
-NodeName -nn	Optional. Name of the node. Node names must be between 1 and 79 characters and cannot contain spaces or the following characters: \ / * ? < > " |
-NodeAddress -na	Optional. Host name and port number for the machine hosting the node. Choose an available port number.
-ServiceManagerPort -sp	Optional. Port number used by the Service Manager to listen for incoming connection requests.
-EnableTLS -tls	Optional. Configures secure communication among the services in the Informatica domain. If you use the default SSL certificates provided by Informatica, you do not need to specify the keystore and truststore options. If you do not use the default SSL certificate, you must specify the keystore and truststore options. Valid values are true or false. Default is false. If you specify the -tls option without a value, the Informatica domain uses secure communication among the services. To enable secure communication for the associated services or web applications, such as Administrator tool, Analyst tool, or Web Services Hub, configure the secure communication separately within the applications.
-NodeKeystore- -nk	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Directory that contains the keystore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain keystore files in PEM and JKS formats. The keystore files must be named infa_keystore.jks and infa_keystore.pem. If the keystore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_keystore.jks and infa_keystore.pem. You must use the same keystore file for all the nodes in the domain.
-NodeKeystorePass -nkp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the keystore infa_keystore.jks file.
-NodeTruststore -nt	Optional if you use the default SSL certificates from Informatica. Directory that contains the truststore files. The Informatica domain requires the SSL certificates in PEM format and in Java Keystore (JKS) files. The directory must contain truststore files in PEM and JKS formats. The truststore files must be named infa_truststore.jks and infa_truststore.pem. If the truststore file that you receive from the certificate authority (CA) has a different name, you must rename it to infa_truststore.jks and infa_truststore.pem.
-NodeTruststorePass -ntp	Optional if you use the default SSL certificates from Informatica. Required if you use your SSL certificates. Password for the infa_truststore.jks file.
-CipherWhiteList -cwl	Optional. Comma-separated list of JSSE cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackList -cbl	Optional. Comma-separated list of JSSE cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.

Option	Description
-CipherWhiteListFile -cwlf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to add to the effective list. **Note:** The list must contain at least one valid JRE or OpenSSL cipher suite.
-CipherBlackListFile -cblf	Optional. Absolute file name of the plain text file that contains a comma-separated list of cipher suites that you want to remove from the effective list. **Note:** The effective list must contain at least one valid JRE or OpenSSL cipher suite.
-EnableKerberos -krb	Optional. Configures the Informatica domain to use Kerberos authentication. Valid values are true or false. If true, the domain uses Kerberos authentication, and you cannot later change the authentication mode. After you enable Kerberos authentication, you cannot disable it. Default is false. If you specify the -krb option without a value, the Informatica domain uses Kerberos authentication.
-ServiceRealmName -srn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-UserRealmName -urn	Optional. Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example, specify the following value to include all realms that include the EAST.COMPANY.COM name: *EAST.COMPANY.COM
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-HttpsPort -hs	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-GatewayAddress -dg	Required. Gateway host machine name and port number.

Option	Description
-UserName -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-SecurityDomain -sdn	Name of the security domain that you want to create to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-MinProcessPort -mi	Required. Minimum port number for application service processes that run on the node.
-MaxProcessPort -ma	Required. Maximum port number for application service processes that run on the node.
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from domain components on this port. Set this port number if you have multiple nodes on one machine or if the default port number is in use. Default is the node port number plus one.
-BackupDirectory -bd	Optional. Directory to store repository backup files. The directory must be accessible by the node.
-ErrorLogLevel -el	Optional. Severity level for log events in the domain log. Default is info.
-ResourceFile -rf	Required. File that contains the list of available resources for the node. Use the file, nodeoptions.xml, located in the following location: `<Informatica installation directory>/isp/bin`
-EnableSaml -saml	Optional. Enables or disables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the Informatica domain. Default is false.
-SamlKeyStoreDir -skd	Optional. The directory containing the custom keystore file required to use SAML authentication on the gateway node. Specify the directory only, not the full path to the file.

Option	Description
-SamlKeyStorePassword -skp	Required if you use a custom keystore for SAML authentication. Password to the SAML keystore. *
-GatewayAddress -dg	Required. Gateway host machine name and port number.
-UserName -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence. Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-SecurityDomain -sdn	Name of the security domain that you want to create to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. You can specify a value for -sdn or use the default based on the authentication mode: - Required if the domain uses LDAP authentication. Default is Native. To work with LDAP authentication, you need to specify the value for -sdn. - Optional if the domain uses native authentication or Kerberos authentication. Default is native for native authentication. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServerPort -sv	Optional. TCP/IP port number used by the Service Manager. The Service Manager listens for shutdown commands from PowerCenter components on this port. Set this port number if you have multiple nodes on one machine or if the default port number is in use.
-resetHostPort -rst	Required if you specify the NodeAddress or ServiceManager option. Resets the host port number.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Default is <INFA_home>/logs.
* Note: If you currently run scripts that use this command to enable a custom keystore for SAML authentication, you must update them to include this option.	

upgradeDomainMetadata

Updates metadata for the domain. Before you update the domain, run the infacmd isp ShutDownNode command to shut down the node.

The upgradeDomainMetadata command uses the following syntax:

```
upgradeDomainMetadata
<-PreviousInfaHome|-ph> previous_infa_home
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
[<-SingletonServiceParameters|-ssp> option_name=value ...(SystemServicesFolderName,
SchedulerService, ResourceManager, EmailService)]
```

The following table describes *infasetup* upgradeDomainMetadata options and arguments:

Option	Description
-PreviousInfaHome -ph	Required. Path to the previous Informatica home directory.
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.

Option	Description
-SchemaName -sc	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.
-DatabaseTruststoreLocation -dbtl	Optional. Path and file name of the truststore file for the gateway node.
-SingletonServiceParameters -ssp	Optional. Upgrade service parameters using any of the following options: - SystemServicesFolderName - SchedulerService - ResourceManager - EmailService Syntax: `infasetup upgradeDomainMetadata -ssp <option>=<value>`

UpgradeGatewayNodeMetadata

Updates metadata for a gateway node on the current machine. Before you update the gateway node, run the infacmd isp ShutDownNode command to shut down the node.

The UpgradeGatewayNodeMetadata command uses the following syntax:

```
UpdateGatewayNode
[<-LogServiceDirectory|-ld> log_service_directory (used for GatewayNode only)]
[<-SystemLogDirectory|-sld> system_log_directory]
[<-HttpsPort|-hs> https_port]
[<-KeystoreFile|-kf> keystore_file_location]
[<-KeystorePass|-kp> keystore_password]
<<-DatabaseAddress|-da> database_hostname:database_port|<-DatabaseConnectionString|-cs>
database_connection_string>
[<-DatabaseUserName|-du> database_user_name]
[<-DatabasePassword|-dp> database_password]
<-DatabaseType|-dt> database_type ORACLE|DB2|MSSQLSERVER|SYBASE|POSTGRESQL
[<-DatabaseServiceName|-ds> database_service_name]
[<-Tablespace|-ts> tablespace_name]
[<-SchemaName|-sc> schema_name (used for MSSQLServer and PostgreSQL only)]
[<-TrustedConnection|-tc> trusted_connection (used for MSSQLServer only)]
<-PreviousInfaHome|-ph> previous_infa_home
[<-KeysDirectory|-kd> Infa_secrets_directory_location]
[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]
```

```
[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]
[<-DatabaseTruststoreLocation|-dbtl> database_truststore_location]
```

The following table describes *infasetup* UpgradeGatewayNodeMetadata options and arguments:

Option	Description
-LogServiceDirectory -ld	Required. Shared directory path used by the Log Manager to store log event files. Verify that -ld does not match or contain the specified -sld value.
-SystemLogDirectory -sld	Optional. Directory path to store system log files. Verify that -ld does not match or contain the specified -sld value. Default is <INFA_home>/logs.
-HttpsPort -hs	Optional. Port number that the node uses for communication between the Administrator tool and the Service Manager. Set this port number if you want to configure HTTPS for a node. To disable HTTPS support for a node, set this port number to zero.
-KeystoreFile -kf	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol.
-KeystorePass -kp	Optional. A plain-text password for the keystore file. You can set a password with the -kp option or the environment variable INFA_PASSWORD. If you set a password with both methods, the password set with the -kp option takes precedence.
-DatabaseAddress -da	Required if you do not use -DatabaseConnectionString (-cs) option. Name and port number of the machine hosting the domain configuration database.
-DatabaseConnectionString -cs	Required if you do not use -DatabaseAddress (-da) and -DatabaseServiceName (-ds) options. Connection string used to connect to the domain configuration database. Specify the database host, database port, and the database service name as part of the connection string. Enclose the connection string in quotes.
-DatabaseUserName -du	Required if you do not use -TrustedConnection (-tc) option. Account for the database containing the domain configuration information.
-DatabasePassword -dp	Domain configuration database password corresponding to the database user. If you omit this option, *infasetup* uses the password specified in the INFA_DEFAULT_DATABASE_PASSWORD environment variable. If no value is specified in the environment variable, you must enter a password using this option.
-DatabaseType -dt	Required. Type of database that stores the domain configuration metadata. Database types include: - db2 - oracle - mssqlserver - sybase - postgresql
-DatabaseServiceName -ds	Required if you do not use -DatabaseConnectionString (-cs) option. The database service name. Required for Oracle, IBM DB2, and Microsoft SQL Server databases. Enter the SID for Oracle, the service name for IBM DB2, or the database name for Microsoft SQL Server.

Option	Description
-Tablespace -ts	Required for an IBM DB2 database. Name of the tablespace where the domain configuration database tables reside.
-SchemaName -sc	Optional. Name of the Microsoft SQL Server schema. Enter a schema name if you are not using the default schema.
-TrustedConnection -tc	Optional. Connect to the Microsoft SQL Server database through a trusted connection. Trusted authentication uses the Windows security credentials of the current user to connect to Microsoft SQL Server.
-PreviousInfaHome -ph	Required. Path to the previous Informatica home directory.
-KeysDirectory -kd	Optional. Directory where all keytab files and the encryption key for the Informatica domain are stored. Default is `<InformaticaInstallationDir>/isp/config/keys`.
-DatabaseTlsEnabled -dbtls	Optional. Indicates whether the Informatica domain database is secure with TLS or SSL. Set this option to True for the secure database. Default is false. If you specify the -dbtls option without a value, the Informatica domain uses secure communication to the Informatica domain database.
-DatabaseTruststorePassword -dbtp	Optional. Password for the database truststore file for the secure database.
-DatabaseTruststoreLocation -dbtl	Optional. Path and file name of the truststore file for the gateway node.

UnlockUser

Unlocks a native or an LDAP user account. When you unlock a native user account, you can also provide a new password for the account.

You can unlock a user account after you shut down the domain from the gateway node.

The infasetup UnlockUser command uses the following syntax:

```
UnlockUser
<-UserName|-un> user_name
[<-SecurityDomain|-sdn] security domain]
[<-NewPassword|-np] new_password]
```

The following table describes the infasetup UnlockUser options and arguments:

Option	Argument	Description
-UserName -un	user_name	Required. User name of the locked account. The value is case sensitive.
-SecurityDomain -sdn	security domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-NewPassword -np	new_password	Optional. New password for the locked native account. For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password: - The length of the password must be at least eight characters. - It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as: `! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~` When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

ValidateandRegisterFeature

Validates and registers the feature in the domain.

The ValidateandRegisterFeature command uses the following syntax:

```
ValidateandRegisterFeature

<-FeatureFilename|-ff> feature_filename

<-IsUpgrade|-up> is_upgrade
```

The following table describes *infasetup* ValidateandRegisterFeature options and arguments:

Option	Argument	Description
-FeatureFilename -ff	feature_filename	Required. Location of the xml file for the plugin.
-IsUpgrade -up	is_upgrade	Required. Indicates whether to upgrade the plug-in to the specified version in the feature file. Valid values are true and false. Default is true.

CHAPTER 43

pmcmd Command Reference

This chapter includes the following topics:

Using pmcmd

pmcmd is a program you use to communicate with the Integration Service. With *pmcmd,* you can perform some of the tasks that you can also perform in the Workflow Manager, such as starting and stopping workflows and sessions.

Use *pmcmd* in the following modes:

- **Command line mode.** You invoke and exit *pmcmd* each time you issue a command. You can write scripts to schedule workflows with the command line syntax. Each command you write in command line mode must include connection information to the Integration Service.
- **Interactive mode.** You establish and maintain an active connection to the Integration Service. This lets you issue a series of commands.

You can use environment variables for user names and passwords with *pmcmd*. You can also use environment variables to customize the way *pmcmd* displays the date and time on the machine running the Integration Service process. Before you use *pmcmd*, configure these variables on the machine running the Integration Service process. The environment variables apply to *pmcmd* commands that run on the node.

Note: If the domain is a mixed-version domain, run *pmcmd* from the installation directory of the Integration Service version.

Running Commands in Command Line Mode

Command line mode invokes and exits *pmcmd* each time you issue a command. Command line mode is useful if you want to run *pmcmd* commands through batch files, scripts, or other programs.

Use *pmcmd* commands with operating system scheduling tools like *cron,* or you can embed *pmcmd* commands into shell or Perl scripts.

When you run *pmcmd* in command line mode, you enter connection information such as domain name, Integration Service name, user name and password in each command. For example, to start the workflow "wf_SalesAvg" in folder "SalesEast," use the following syntax:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesAvg
```

The user, seller3, with the password "jackson" sends the request to start the workflow.

If you omit or incorrectly enter one of the required options, the command fails, and *pmcmd* returns a non-zero return code. For more information about all the return codes, see "pmcmd Return Codes" on page 1235.

To run pmcmd commands in command line mode:

1. At the command prompt, switch to the directory where the *pmcmd* executable is located.

   By default, the PowerCenter installer installs *pmcmd* in the \server\bin directory.

2. Enter `pmcmd` followed by the command name and its required options and arguments:

   `pmcmd command_name [-option1] argument_1 [-option2] argument_2...`

pmcmd Return Codes

In command line mode, *pmcmd* indicates the success or failure of a command with a return code. Return code "0" indicates that the command succeeded. Any other return code indicates that the command failed.

Use the DOS or UNIX echo command immediately after running a *pmcmd* command to see the return code for the command:

- In a DOS shell: `echo %ERRORLEVEL%`

- In a UNIX Bourne or Korn shell: `echo $?`
- In a UNIX C shell: `echo $status`

The following table describes the return codes for *pmcmd:*

Code	Description
0	For all commands, a return value of zero indicates that the command ran successfully. You can issue the following commands in the wait or nowait mode: starttask, startworkflow, aborttask, and abortworkflow. If you issue a command in the wait mode, a return value of zero indicates the command ran successfully. If you issue a command in the nowait mode, a return value of zero indicates that the request was successfully transmitted to the Integration Service, and it acknowledged the request.
1	Integration Service is not available, or *pmcmd* cannot connect to the Integration Service. There is a problem with the TCP/IP host name or port number or with the network.
2	Task name, workflow name, or folder name does not exist.
3	An error occurred starting or running the workflow or task.
4	Usage error. You passed the wrong options to *pmcmd*.
5	An internal *pmcmd* error occurred. Contact Informatica Global Customer Support.
7	You used an invalid user name or password.
8	You do not have the appropriate permissions or privileges to perform this task.
9	Connection to the Integration Service timed out while sending the request.
12	Integration Service cannot start recovery because the session or workflow is scheduled, waiting for an event, waiting, initializing, aborting, stopping, disabled, or running.
13	User name environment variable is set to an empty value.
14	Password environment variable is set to an empty value.
15	User name environment variable is missing.
16	Password environment variable is missing.
17	Parameter file does not exist.
18	Integration Service found the parameter file, but it did not have the initial values for the session parameters, such as $input or $output.
19	Integration Service cannot resume the session because the workflow is configured to run continuously.
20	A repository error has occurred. Make sure that the Repository Service and the database are running and the number of connections to the database is not exceeded.
21	Integration Service is shutting down and it is not accepting new requests.
22	Integration Service cannot find a unique instance of the workflow/session you specified. Enter the command again with the folder name and workflow name.
23	There is no data available for the request.

Code	Description
24	Out of memory.
25	Command is cancelled.

Running Commands in Interactive Mode

Use *pmcmd* in interactive mode to start and stop workflows and sessions without writing a script. When you use the interactive mode, you enter connection information such as domain name, Integration Service name, user name, and password. You can run subsequent commands without entering the connection information for each command.

For example, the following commands invoke the interactive mode, establish a connection to Integration Service "MyIntService," and start workflows "wf_SalesAvg" and "wf_SalesTotal" in folder "SalesEast":

```
pmcmd
pmcmd> connect -sv MyIntService -d MyDomain -u seller3 -p jackson
pmcmd> setfolder SalesEast
pmcmd> startworkflow wf_SalesAvg
pmcmd> startworkflow wf_SalesTotal
```

To run pmcmd commands in interactive mode:

1. At the command prompt, switch to the directory where the *pmcmd* executable is located.

   By default, the PowerCenter *installer installs pmcmd* in the \server\bin directory.

2. At the command prompt, type `pmcmd`.

   This starts *pmcmd* in interactive mode and displays the `pmcmd>` prompt. You do not have to type `pmcmd` before each command in interactive mode.

3. Enter connection information for the domain and Integration Service. For example:

   ```
   connect -sv MyIntService -d MyDomain -u seller3 -p jackson
   ```

4. Type a command and its options and arguments in the following format:

   command_name [-option1] *argument_1* [-option2] *argument_2*...

   pmcmd runs the command and displays the prompt again.

5. Type `exit` to end an interactive session.

Setting Defaults

After you connect to an Integration Service using *pmcmd*, you can designate default folders or conditions to use each time the Integration Service executes a command. For example, if you want to issue a series of commands or tasks in the same folder, specify the name of the folder with the setfolder command. All subsequent commands use that folder as the default.

The following table describes the commands that you use to set defaults for subsequent commands:

Command	Description
setfolder	Designates a folder as the default folder in which to execute all subsequent commands.
setnowait	Executes subsequent commands in the nowait mode. The *pmcmd* prompt is available after the Integration Service receives the previous command. The nowait mode is the default mode.

Command	Description
setwait	Executes subsequent commands in the wait mode. The *pmcmd* prompt is available after the Integration Service completes the previous command.
unsetfolder	Reverses the setfolder command.

You can use *pmcmd* ShowSettings command to display the default settings.

Running in Wait Mode

You can run *pmcmd* in wait or nowait mode. In wait mode, *pmcmd* returns to the shell or command prompt after the command completes. You cannot run subsequent commands until the previous command completes.

For example, if you enter the following command, *pmcmd* starts the workflow “wf_SalesAvg” and does not return to the prompt until the workflow completes:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast -
wait wf_SalesAvg
```

In nowait mode, *pmcmd* returns to the shell or command prompt immediately. You do not have to wait for one command to complete before running the next command.

For example, if you enter the following commands, *pmcmd* starts workflow “wf_SalesTotal” even if workflow “wf_SalesAvg” is still running:

```
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesAvg
pmcmd startworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f SalesEast
wf_SalesTotal
```

By default, *pmcmd* executes commands in nowait mode.

You can configure the wait mode when you run in command line or interactive mode. In command line mode, use the -wait option to run a command in wait mode. In interactive mode, use the setwait or setnowait command before entering subsequent commands.

Scripting pmcmd Commands

When you use *pmcmd*, you might use some commands with specific options and arguments on a regular basis. For example, you might use *pmcmd* to check the status of the Integration Service. In this case, you can create a script or batch file to call one or more *pmcmd* commands including its options and arguments.

You can run scripts in command line mode. You cannot run *pmcmd* scripts in interactive mode.

For example, the following UNIX shell script checks the status of Integration Service “testService,” and if it is running, gets details for session “s_testSessionTask”:

```
#!/usr/bin/bash
# Sample pmcmd script
# Check if the service is alive

pmcmd pingservice -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not ping service"

    exit
```

```
fi
# Get service properties

pmcmd getserviceproperties  -sv testService -d testDomain
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get service properties"

    exit

fi
# Get task details for session task "s_testSessionTask" of workflow

# "wf_test_workflow" in folder "testFolder"

pmcmd gettaskdetails -sv testService -d testDomain -u Administrator -p adminPass -folder
testFolder -workflow wf_test_workflow s_testSessionTask
if [ "$?" != 0 ]; then

    # handle error

    echo "Could not get details for task s_testSessionTask"

    exit

fi
```

Entering Command Options

pmcmd provides multiple ways to enter some of the command options and arguments. For example, to enter a password, use the following syntax:

<<-password|-p> password**|**<-passwordvar|-pv> passwordEnvVar**>**

To enter a password, precede the password with the -password or -p option:

```
-password ThePassword
or
-p ThePassword
```

If you use a password environment variable, precede the variable name with the -pv or -passwordvar option:

```
-passwordvar PASSWORD
or
-pv PASSWORD
```

If a command option contains spaces, use single or double quotation marks to enclose the option. For example, use single quotes in the following syntax to enclose the folder name:

```
abortworkflow -sv MyIntService -d MyDomain -u seller3 -p jackson -f 'quarterly sales' -
wait wf_MyWorkflow
```

To denote an empty string, use two single quotes ('') or two double quotes ("").

aborttask

Aborts a task. Issue this command only if the Integration Service fails to stop the task when you issue the stoptask command.

The pmcmd aborttask command uses the following syntax in the command line mode:

```
pmcmd aborttask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

The pmcmd aborttask command uses the following syntax in the interactive mode:

```
aborttask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

The following table describes pmcmd aborttask options and arguments:

Option	Argument	Description
-service -sv	service	Required in command line mode. Integration Service name. Not used in interactive mode.
-domain -d	domain	Optional in command line mode. Domain name. Not used in interactive mode.
-timeout -t	timeout	Optional in command line mode. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. Not used in interactive mode. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.

Option	Argument	Description
-uservar -uv	userEnvVar	Required in command line mode if you do not specify the user name. Specifies the user name environment variable. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the task name is not unique in the repository. Name of the folder containing the task.
-workflow -w	workflow	Required. Name of the workflow.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task you want to abort. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance that contains the task you want to abort. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	taskInstancePath	Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

abortworkflow

Aborts a workflow. Issue this command only if the Integration Service fails to stop the workflow when you issue the stopworkflow command.

The abortworkflow command uses the following syntax in the command line mode:

```
pmcmd abortworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The abortworkflow command uses the following syntax in the interactive mode:

```
abortworkflow

[<-folder|-f> folder]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The following table describes *pmcmd* abortworkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required in command line mode. Integration Service name. Not used in interactive mode.
-domain -d	domain	Optional in command line mode. Domain name. Not used in interactive mode.
-timeout -t	timeout	Optional in command line mode. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. Not used in interactive mode. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.

Option	Argument	Description
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-runinsname -rin	runInsName	Name of the workflow run instance you want to abort. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance you want to abort. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	workflow	Required. Name of the workflow.

Connect

Connects the *pmcmd* program to the Integration Service in the interactive mode. If you omit connection information, *pmcmd* prompts you to enter the correct information. Once *pmcmd* successfully connects, you can issue commands without reentering the connection information.

```
Connect

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

Note: Use this command in the *pmcmd* interactive mode only.

The following table describes *pmcmd* Connect options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.

Disconnect

Disconnects *pmcmd* from the Integration Service. It does not close the *pmcmd* program. Use this command when you want to disconnect from an Integration Service and connect to another in the interactive mode.

The Disconnect command uses the following syntax in the interactive mode:

```
Disconnect
```

Note: Use this command in the *pmcmd* interactive mode only.

Exit

Disconnects *pmcmd* from the Integration Service and closes the *pmcmd* program.

The Exit command uses the following syntax in the interactive mode:

```
Exit
```

Note: Use this command in the *pmcmd* interactive mode only.

getrunningsessionsdetails

Returns the following details for all sessions currently running on an Integration Service:

- Integration Service status, startup time, and current time
- Folder and workflow name
- Worklet and session instance
- For each running session: task type, start time, run status, first error code, associated Integration Service, run mode, and node name
- For the mapping in a running session: mapping name, session log file, first error code and error message, number of source and target success and failed rows, and number of transformation error messages
- Number of sessions running on the Integration Service

The pmcmd getrunningsessionsdetails command uses the following syntax in the command line mode:

```
pmcmd getrunningsessionsdetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

The pmcmd getrunningsessionsdetails command uses the following syntax in the interactive mode:

```
getrunningsessionsdetails
```

The following table describes pmcmd getrunningsessionsdetails options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.

Option	Argument	Description
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.

GetServiceDetails

Returns the following details about an Integration Service:

- Integration Service name, status, startup time, and current time
- For each active workflow: folder name, workflow name, version, run status, first error code, start time, log file, run type, user that runs the workflow
- For each active task: folder name, workflow name and version, task instance name and version, task type, start and end time, run status, first error code, error message, associated Integration Service, run mode, names of nodes where the task runs
- Number of scheduled, active, and waiting workflows and sessions

The GetServiceDetails command uses the following syntax in the command line mode:

```
pmcmd GetServiceDetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>
```

```
[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[-all|-running|-scheduled]
```

The GetServiceDetails command uses the following syntax in the interactive mode:

```
GetServiceDetails

[-all|-running|-scheduled]
```

The following table describes *pmcmd* GetServiceDetails options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-all -running -scheduled	-	Optional. Specifies the workflows to return details for: - all. Returns status details on the scheduled and running workflows. - running. Returns status details on active workflows. Active workflows include running, suspending, and suspended workflows. - scheduled. Returns status details on the scheduled workflows. Default is all.

getserviceproperties

Returns the following information about the PowerCenter Integration Service:

- Domain in which the PowerCenter Integration Service runs
- PowerCenter Integration Service name and version
- Whether the PowerCenter Integration Service allows running debug mappings
- Data movement mode
- Associated repository service
- Current timestamp and startup time
- Grid name
- Names, nodes, and code pages for the associated PowerCenter Integration Service processes
- Operating mode for the PowerCenter Integration Service

The pmcmd getserviceproperties command uses the following syntax in the command line mode:

```
pmcmd getserviceproperties

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

The pmcmd getserviceproperties command uses the following syntax in the interactive mode:

```
getserviceproperties
```

The following table describes pmcmd getserviceproperties options and arguments:

Option	Argument	Description
-service -sv	service	Required. PowerCenter Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the PowerCenter Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.

getsessionstatistics

Returns session details and statistics. The command returns the following information:

- Folder name, workflow name, worklet or session instance, and mapping name
- Session log file name and location
- Number of source and target success and failure rows
- Number of transformation errors
- First error code and error message
- Task run status
- Name of associated Integration Service
- Grid and node names where the session runs

The command also returns the following information for each partition:

- Partition name
- For each transformation within a partition: transformation instance, transformation name, number of applied, affected, and rejected rows, throughput, last error code, start and end time

The getsessionstatistics command uses the following syntax in the command line mode:

```
pmcmd getsessionstatistics

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]
```

```
<-workflow|-w> workflow

taskInstancePath
```

The getsessionstatistics command uses the following syntax in the interactive mode:

```
getsessionstatistics

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

<-workflow|-w> workflow

taskInstancePath
```

The following table describes *pmcmd* getsessionstatistics options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Required if you use LDAP authentication. Optional in command line mode. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.

Option	Argument	Description
-folder -f	folder	Required if the task name is not unique in the repository. Name of the folder containing the task.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance that contains the task. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-workflow -w	workflow	Required. Name of the workflow.
-	taskInstancePath	Required. Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

gettaskdetails

Returns the following information about a task:

- Folder name, workflow name, task instance name, and task type
- Last execution start and complete time
- Task run status, first error code, and error message
- Grid and node names where the task runs
- Name of associated Integration Service
- Task run mode

If the task is a session, the command also returns the following details:

- Mapping and session log file name
- First error code and message
- Source and target success and failed rows
- Number of transformation errors

The pmcmd gettaskdetails command uses the following syntax in the command line mode:

```
pmcmd gettaskdetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]> <<-user|-u>
username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]
```

```
[<-folder|-f> folder]
<-workflow|-w> workflow
[<-runinsname|-rin> runInsName]
taskInstancePath
```

The pmcmd gettaskdetails command uses the following syntax in the interactive mode:

```
gettaskdetails
[<-folder|-f> folder]
<-workflow|-w> workflow
[<-runinsname|-rin> runInsName]
taskInstancePath
```

The following table describes pmcmd gettaskdetails options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.

Option	Argument	Description
-folder -f	folder	Required if the task name is not unique in the repository. Name of the folder containing the task.
-workflow -w	workflow	Required if the task name is not unique in the repository. Name of the folder containing the task.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task. Use this option if you are running concurrent workflows.
-	taskInstancePath	Required. Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

getworkflowdetails

Returns the following information about a workflow:

- Folder and workflow names
- Workflow run status
- First error code and error message
- Start and end times
- Log file name
- Workflow run type
- Name of user that last ran the workflow
- Name of associated Integration Service

The getworkflowdetails command uses the following syntax in the command line mode:

```
pmcmd getworkflowdetails

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The getworkflowdetails command uses the following syntax in the interactive mode:

```
getworkflowdetails
```

```
[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The following table describes *pmcmd* getworkflowdetails options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-runinsname -rin	runInsName	Name of the workflow run instance. Use this option if you are running concurrent workflows.

Option	Argument	Description
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	workflow	Name of the workflow.

The following table describes the different statuses for workflows:

Status Name	Description
Aborted	You choose to abort the workflow or task in the Workflow Monitor or through *pmcmd*. The Integration Service kills the DTM process and aborts the task. You can recover an aborted workflow if you enable the workflow for recovery.
Aborting	The Integration Service is in the process of aborting the workflow.
Disabled	You select the Disabled option in the workflow properties. The Integration Service does not run the disabled workflow until you clear the Disabled option.
Failed	The Integration Service fails the workflow because it encountered errors. You cannot recover a failed workflow.
Preparing to Run	The Integration Service is waiting for an execution lock for the workflow.
Running	The Integration Service is running the workflow.
Scheduled	You schedule the workflow to run at a future date. The Integration Service runs the workflow for the duration of the schedule.
Stopped	You choose to stop the workflow or task in the Workflow Monitor or through *pmcmd*. The Integration Service stops processing the task and all other tasks in its path. The Integration Service continues running concurrent tasks. You can recover a stopped workflow if you enable the workflow for recovery.
Stopping	The Integration Service is in the process of stopping the workflow.
Succeeded	The Integration Service successfully completes the workflow.
Suspended	The Integration Service suspends the workflow because a task failed and no other tasks are running in the workflow. This status is available when you select the Suspend on Error option. You can recover a suspended workflow.
Suspending	A task fails in the workflow when other tasks are still running. The Integration Service stops running the failed task and continues running tasks in other paths. This status is available when you select the Suspend on Error option.
Terminated	The Integration Service shuts down unexpectedly when running this workflow or task. You can recover a terminated workflow if you enable the workflow for recovery.
Terminating	The Integration Service is in the process of terminating the workflow or task.

Status Name	Description
Unknown Status	This status displays in the following situations: - The Integration Service cannot determine the status of the workflow or task. - The Integration Service does not respond to a ping from the Workflow Monitor. - The Workflow Monitor cannot connect to the Integration Service within the resilience timeout period.
Unscheduled	You remove a workflow from the schedule.
Waiting	The Integration Service is waiting for available resources so it can run the workflow or task. For example, you may set the maximum number of running Session and Command tasks allowed for each Integration Service process on the node to 10. If the Integration Service is already running 10 concurrent sessions, all other workflows and tasks have the Waiting status until the Integration Service is free to run more tasks.

The getworkflowdetails command displays the last workflow run type details. Workflow run types refers to the method used to start the workflow.

The following table describes the different workflow run types with the getworkflowdetails command:

Workflow Run Types	Description
User Request	Manually started a workflow.
Schedule	Workflow runs at the scheduled time.

help

Returns the syntax for the command you specify. If you omit the command name, *pmcmd* lists all commands and their syntax.

The pmcmd help command uses the following syntax in the command line mode:

```
pmcmd help [command]
```

The pmcmd help command uses the following syntax in the interactive mode:

```
help [command]
```

The following table describes the pmcmd help option and argument:

Option	Argument	Description
-	command	Optional. Name of command. If you omit the command name, *pmcmd* lists all commands and their syntax.

pingservice

Verifies that the Integration Service is running.

The pmcmd pingservice command uses the following syntax in the command line mode:

```
pmcmd pingservice

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>
```

The pmcmd pingservice command uses the following syntax in the interactive mode:

```
pingservice
```

The following table describes pmcmd pingservice options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.

recoverworkflow

Recovers suspended workflows. To recover a workflow, specify the folder and workflow name. The Integration Service recovers the workflow from all suspended and failed worklets and all suspended and failed Command, Email, and Session tasks.

The pmcmd recoverworkflow command uses the following syntax in the command line mode:

```
pmcmd recoverworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[-wait|-nowait]
```

```
[<-runinsname|-rin> runInsName]
[-wfrunid workflowRunId]
workflow
```

The pmcmd recoverworkflow command uses the following syntax in the interactive mode:

```
recoverworkflow
[<-folder|-f> folder]
[<-paramfile> paramfile]
[<-localparamfile|-lpf> localparamfile]
[-wait|-nowait]
[<-runinsname|-rin> runInsName]
[-wfrunid workflowRunId]
workflow
```

The following table describes pmcmd recoverworkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.

Option	Argument	Description
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-paramfile	paramfile	Optional. Determines which parameter file to use when a task or workflow runs. It overrides the configured parameter file for the workflow or task.
-localparamfile -lpf	localparamfile	Optional. Specifies the parameter file on a local machine that *pmcmd* uses when you start a workflow.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-runinsname -rin	runInsName	Name of the workflow run instance you want to recover. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance you want to recover. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	workflow	Required. Name of the workflow.

scheduleworkflow

Instructs the Integration Service to schedule a workflow. Use this command to reschedule a workflow that has been removed from the schedule.

The pmcmd scheduleworkflow command uses the following syntax in the command line mode:

```
pmcmd scheduleworkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

workflow
```

The pmcmd scheduleworkflow command uses the following syntax in the interactive mode:

```
scheduleworkflow

[<-folder|-f> folder]

workflow
```

The following table describes pmcmd scheduleworkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-	workflow	Required. Name of the workflow.

SetFolder

Designates a folder as the default folder in which to execute all subsequent commands. After issuing this command, you do not need to enter a folder name for workflow, task, and session commands. If you enter a folder name in a command after the SetFolder command, that folder name overrides the default folder name for that command only.

The SetFolder command uses the following syntax in the interactive mode:

```
SetFolder folder
```

Note: Use this command in the *pmcmd* interactive mode only.

The following table describes *pmcmd* SetFolder option and argument:

Option	Argument	Description
-	folder	Required. Name of the folder.

SetNoWait

You can run *pmcmd* in wait or nowait mode. In wait mode, *pmcmd* returns to the shell or command prompt after the command completes. You cannot run subsequent commands until the previous command completes. In nowait mode, *pmcmd* returns to the shell or command prompt immediately. You do not have to wait for one command to complete before running the next command.

The SetNoWait command runs *pmcmd* in nowait mode. The nowait mode is the default mode.

The SetNoWait command uses the following syntax in the interactive mode:

```
SetNoWait
```

When you set nowait mode, use the *pmcmd* prompt after the Integration Service executes the previous command.

Note: Use this command in the *pmcmd* interactive mode only.

SetWait

You can run *pmcmd* in wait or nowait mode. In wait mode, *pmcmd* returns to the shell or command prompt after the command completes. You cannot run subsequent commands until the previous command completes. In nowait mode, *pmcmd* returns to the shell or command prompt immediately. You do not have to wait for one command to complete before running the next command.

The SetWait command runs *pmcmd* in wait mode. The *pmcmd* prompt is available after the Integration Service completes the previous command.

The SetWait command uses the following syntax in the interactive mode:

```
SetWait
```

Note: Use this command in the *pmcmd* interactive mode only.

ShowSettings

Returns the name of the domain, Integration Service, and repository to which *pmcmd* is connected. It displays the user name, wait mode, and default folder.

The ShowSettings command uses the following syntax in the interactive mode:

```
ShowSettings
```

Note: Use this command in the *pmcmd* interactive mode only.

StartTask

Starts a task.

The StartTask command uses the following syntax in the command line mode:

```
pmcmd StartTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]

taskInstancePath
```

The StartTask command uses the following syntax in the interactive mode:

```
pmcmd StartTask

[<-folder|-f> folder]

<-workflow|-w> workflow

<-paramfile> paramfile]

[-wait|-nowait]

[<-recovery|-norecovery>]

[<-runinsname|-rin> runInsName]

taskInstancePath
```

The following table describes *pmcmd* StartTask options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-workflow -w	workflow	Required. Name of the workflow.
-paramfile	paramfile	Optional. Determines which parameter file to use when a task or workflow runs. It overrides the configured parameter file for the workflow or task.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.

Option	Argument	Description
-recovery -norecovery	-	Optional. If the task is a session, the Integration Service runs the session based on the configured recovery strategy. - recovery. For real-time sessions that are enabled for recovery, the Integration Service recovers the failed session and stops running the rest of the tasks in the workflow. The recovery option is the same as the Recover Task option in the Workflow Manager. This option is not applicable for sessions that do not have recovery enabled. - norecovery. For real-time sessions that are enabled for recovery, the Integration Service does not process recovery data. The Integration Service clears the state of operation and the recovery file or table before it restarts the task. For the sessions that do not have recovery enabled, the Integration Service clears the state of operation and restarts the task. The norecovery option is the same as the Cold Start Task option in the Workflow Manager. If you do not provide any option for recovery enabled sessions, the Integration Service runs the session in recovery mode. If you do not provide any option for the sessions that do not have recovery enabled, the Integration Service runs the session in norecovery mode.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task you want to start. Use this option if you are running concurrent workflows.
-	taskInstancePath	Required. Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

Using Parameter Files with starttask

When you start a task, you can optionally enter the directory and name of a parameter file. The Integration Service runs the task using the parameters in the file you specify.

For UNIX shell users, enclose the parameter file name in single quotes:

```
-paramfile '$PMRootDir/myfile.txt'
```

For Windows command prompt users, the parameter file name cannot have beginning or trailing spaces. If the name includes spaces, enclose the file name in double quotes:

```
-paramfile "$PMRootDir\my file.txt"
```

When you write a *pmcmd* command that includes a parameter file located on another machine, use the backslash (\) with the dollar sign ($). This ensures that the machine where the variable is defined expands the process variable.

```
pmcmd starttask -sv MyIntService -d MyDomain -uv USERNAME -pv PASSWORD -f east -w
wSalesAvg -paramfile '\$PMRootDir/myfile.txt' taskA
```

StartWorkflow

Starts a workflow.

The StartWorkflow command uses the following syntax in the command line mode:

```
pmcmd StartWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-startfrom> taskInstancePath]

[<-recovery|-norecovery>]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> OSUser]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

The StartWorkflow command uses the following syntax in the interactive mode:

```
pmcmd StartWorkflow

[<-folder|-f> folder]

[<-startfrom> taskInstancePath [<-recovery|-norecovery>]]

[<-paramfile> paramfile]

[<-localparamfile|-lpf> localparamfile]

[<-osprofile|-o> osProfile]

[-wait|-nowait]

[<-runinsname|-rin> runInsName]

workflow
```

The following table describes *pmcmd* StartWorkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.

Option	Argument	Description
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnv Var	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-startfrom	taskInstancePath	Optional. Starts a workflow from a specified task, taskInstancePath. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string. If you do not specify a starting point, the workflow starts at the Start task. If the task is a session, specify -recovery or -norecovery option to run the session based on the configured recovery strategy.
-paramfile	paramfile	Optional. Determines which parameter file to use when a task or workflow runs. It overrides the configured parameter file for the workflow or task.

Option	Argument	Description
-recovery -norecovery	-	Optional. The Integration Service runs the session based on the configured recovery strategy. - recovery. For real-time sessions that are enabled for recovery, the Integration Service recovers the failed session and stops running the rest of the tasks in the workflow. The recovery option is the same as the Recover Workflow option in the Workflow Manager. This option is not applicable for sessions that do not have recovery enabled. - norecovery. For real-time sessions that are enabled for recovery, the Integration Service does not process recovery data. The Integration Service clears the state of operation and the recovery file or table before it restarts the task. For the sessions that do not have recovery enabled, the Integration Service clears the state of operation and restarts the task. The norecovery option is the same as the Cold Start Workflow option in the Workflow Manager. If you do not provide any option for recovery enabled sessions, the Integration Service runs the session in recovery mode. If you do not provide any option for the sessions that do not have recovery enabled, the Integration Service runs the session in norecovery mode.
-localparamfile -lpf	localparamfile	Optional. Specifies the parameter file on a local machine that *pmcmd* uses when you start a workflow.
-osprofile -o	osProfile	Optional. Specifies the operating system profile assigned to the workflow.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-runinsname -rin	runInsName	Name of the workflow run instance you want to start. Use this option if you are running concurrent workflows.
-	workflow	Required. Name of the workflow.

Using Parameter Files with startworkflow

When you start a workflow, you can optionally enter the directory and name of a parameter file. The Integration Service runs the workflow using the parameters in the file you specify. For UNIX shell users, enclose the parameter file name in single quotes. For Windows command prompt users, the parameter file name cannot have beginning or trailing spaces. If the name includes spaces, enclose the file name in double quotes.

Use parameter files on the following machines:

- **Node running the Integration Service.** When you use a parameter file located on the Integration Service machine, use the -paramfile option to indicate the location and name of the parameter file.

  On UNIX, use the following syntax:

  ```
  -paramfile '$PMRootDir/myfile.txt'
  ```

  On Windows, use the following syntax:

  ```
  -paramfile "$PMRootDir\my file.txt"
  ```

- **Local machine.** When you use a parameter file located on the machine where *pmcmd* is invoked, *pmcmd* passes variables and values in the file to the Integration Service. When you list a local parameter file, specify the absolute path or relative path to the file. Use the -localparamfile or -lpf option to indicate the location and name of the local parameter file.

  On UNIX, use the following syntax:

  ```
  -lpf 'param_file.txt'

  -lpf 'c:\Informatica\parameterfiles\param file.txt'

  -localparamfile 'c:\Informatica\parameterfiles\param file.txt'
  ```

  On Windows, use the following syntax:

  ```
  -lpf param_file.txt

  -lpf "c:\Informatica\parameterfiles\param file.txt”

  -localparamfile param_file.txt
  ```

- **Shared network drives.** When you use a parameter file located on another machine, use the backslash (\) with the dollar sign ($). This ensures that the machine where the variable is defined expands the process variable.

  ```
  -paramfile '\$PMRootDir/myfile.txt'
  ```

StopTask

Stops a task.

The StopTask command uses the following syntax in the command line mode:

```
pmcmd StopTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

taskInstancePath
```

The StopTask command uses the following syntax in the interactive mode:

```
pmcmd StopTask
[<-folder|-f> folder]
<-workflow|-w> workflow
[<-runinsname|-rin> runInsName]
[-wfrunid workflowRunId]
[-wait|-nowait]
taskInstancePath
```

The following table describes *pmcmd* StopTask options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.

Option	Argument	Description
-workflow -w	workflow	Required. Name of the workflow.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task you want to stop. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance that contains the task you want to stop. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-	taskInstancePath	Required. Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

StopWorkflow

Stops a workflow.

The StopWorkflow command uses the following syntax in the command line mode:

```
pmcmd StopWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

The StopWorkflow command uses the following syntax in the interactive mode:

```
pmcmd StopWorkflow
```

```
[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

[-wait|-nowait]

workflow
```

The following table describes *pmcmd* StopWorkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-runinsname -rin	runInsName	Name of the workflow run instance you want to stop. Use this option if you are running concurrent workflows.

Option	Argument	Description
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance you want to stop. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-wait -nowait	-	Optional. Configures the wait mode: - wait. You can enter a new *pmcmd* command only after the Integration Service completes the previous command. - nowait. You can enter a new *pmcmd* command after the Integration Service receives the previous command. Default is nowait.
-	workflow	Required. Name of the workflow.

UnscheduleWorkflow

Removes a workflow from a schedule.

The UnscheduleWorkflow command uses the following syntax in the command line mode:

```
pmcmd UnscheduleWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

workflow
```

The UnscheduleWorkflow command uses the following syntax in the interactive mode:

```
UnscheduleWorkflow

[<-folder|-f> folder]

workflow
```

The following table describes *pmcmd* UnscheduleWorkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.

Option	Argument	Description
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-	workflow	Required. Name of the workflow.

UnsetFolder

Removes the designation of a default folder. After you issue this command, you must specify a folder name each time you enter a command for a session, workflow, or task.

The UnsetFolder command uses the following syntax in the interactive mode:

```
UnsetFolder
```

Note: Use this command in the *pmcmd* interactive mode only.

Version

Displays the PowerCenter version and Informatica trademark and copyright information.

The Version command uses the following syntax in the command line mode:

```
pmcmd Version
```

The Version command uses the following syntax in the interactive mode:

```
Version
```

WaitTask

Instructs the Integration Service to complete the task before returning the *pmcmd* prompt to the command prompt or shell.

The WaitTask command uses the following syntax in the command line mode:

```
pmcmd WaitTask

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

The WaitTask command uses the following syntax in the interactive mode:

```
WaitTask

[<-folder|-f> folder]

<-workflow|-w> workflow

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

taskInstancePath
```

The following table describes *pmcmd* WaitTask options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the task name is not unique in the repository. Name of the folder containing the task.
-workflow -w	workflow	Required. Name of the workflow.
-runinsname -rn	runInsName	Name of the workflow run instance that contains the task. Use this option if you are running concurrent workflows.

Option	Argument	Description
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance that contains the task. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	taskInstancePath	Required. Specifies a task name and where it appears within the workflow. If the task is within a workflow, enter the task name alone. If the task is within a worklet, enter WorkletName.TaskName. Enter the taskInstancePath as a fully qualified string.

WaitWorkflow

Causes *pmcmd* to wait for a workflow to complete before it executes subsequent commands. Use this command in conjunction with the return code when you run *pmcmd* from a script. For example, you may want to check the status of a critical workflow before starting another workflow. Use the WaitWorkflow command to wait for the critical workflow to complete, and then check the *pmcmd* return code. If the return code is 0 (successful), start the next workflow.

The WaitWorkflow command returns the prompt when a workflow completes.

The WaitWorkflow command uses the following syntax in the command line mode:

```
pmcmd WaitWorkflow

<<-service|-sv> service [<-domain|-d> domain] [<-timeout|-t> timeout]>

<<-user|-u> username|<-uservar|-uv> userEnvVar>

<<-password|-p> password|<-passwordvar|-pv> passwordEnvVar>

[<<-usersecuritydomain|-usd> usersecuritydomain|<-usersecuritydomainvar|-usdv>
userSecuritydomainEnvVar>]

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The WaitWorkflow command uses the following syntax in the interactive mode:

```
WaitWorkflow

[<-folder|-f> folder]

[<-runinsname|-rin> runInsName]

[-wfrunid workflowRunId]

workflow
```

The following table describes *pmcmd* WaitWorkflow options and arguments:

Option	Argument	Description
-service -sv	service	Required. Integration Service name.
-domain -d	domain	Optional. Domain name.
-timeout -t	timeout	Optional. Amount of time, in seconds, *pmcmd* attempts to connect to the Integration Service. If the -timeout option is omitted, *pmcmd* uses the timeout value specified in the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If the environment variable is not set, *pmcmd* uses the default timeout value. Default is 180.
-user -u	username	Required in command line mode if you do not specify the user name environment variable. User name. Not used in interactive mode.
-uservar -uv	userEnvVar	Specifies the user name environment variable. Required in command line mode if you do not specify the user name. Not used in interactive mode.
-password -p	password	Required in command line mode if you do not specify the password environment variable. Password. Not used in interactive mode.
-passwordvar -pv	passwordEnvVar	Required in command line mode if you do not specify the password. Password environment variable. Not used in interactive mode.
-usersecuritydomain -usd	usersecuritydomain	Optional in command line mode. Required if you use LDAP authentication. Name of the security domain that the user belongs to. Not used in interactive mode. Default is Native.
-usersecuritydomainvar -usdv	userSecuritydomainEnvVar	Optional in command line mode. Security domain environment variable. Not used in interactive mode.
-folder -f	folder	Required if the workflow name is not unique in the repository. Name of the folder containing the workflow.
-runinsname -rin	runInsName	Name of the workflow run instance. Use this option if you are running concurrent workflows.
-wfrunid	workflowRunId	Run identifier number (Run ID) of the workflow run instance. Use this option if you are running concurrent workflows. **Note:** Use this option if the workflow does not have a unique run instance name.
-	workflow	Required. Name of the workflow.

CHAPTER 44

pmrep Command Reference

This chapter includes the following topics:

Using pmrep

pmrep is a command line program that you use to update repository information and perform repository functions. *pmrep* is installed in the PowerCenter Client and PowerCenter Services bin directories.

Use *pmrep* to perform repository administration tasks such as listing repository objects, creating and editing groups, restoring and deleting repositories, and updating session-related parameters and security information in the PowerCenter repository.

When you use *pmrep*, you can enter commands in the following modes:

- **Command line mode.** You can issue *pmrep* commands directly from the system command line. Use command line mode to script *pmrep* commands.
- **Interactive mode.** You can issue *pmrep* commands from an interactive prompt. *pmrep* does not exit after it completes a command.

You can use environment variables to set user names and passwords for *pmrep*. Before you use *pmrep*, configure these variables. The environment variables apply to *pmrep* commands that run on the node.

All *pmrep* commands require a connection to the repository except for the following commands:

- Help
- ListAllPrivileges

Use the *pmrep* Connect command to connect to the repository before using other *pmrep* commands.

Note: If the domain is a mixed-version domain, run *pmrep* from the installation directory of the Repository Service version.

Running Commands in Command Line Mode

Command line mode invokes and exits *pmrep* each time you issue a command. Command line mode is useful if you want to run *pmrep* commands through batch files, scripts, or other programs.

To run pmrep commands in command line mode:

1. At the command prompt, change to the directory where the *pmrep* executable is located.
2. Enter `pmrep` followed by the command name and its options and arguments:

```
pmrep command_name [-option1] argument_1 [-option2] argument_2...
```

Running Commands in Interactive Mode

Interactive mode invokes *pmrep*. You can issue a series of commands from a *pmrep* prompt without exiting after each command.

To run pmrep commands in interactive mode:

1. At the command prompt, enter `pmrep` to invoke interactive mode.

   This starts *pmrep* in interactive mode and displays a `pmrep>` prompt. You do not have to type `pmrep` before each command in interactive mode.
2. Enter a command and its options and arguments.

   At the prompt, enter:

```
command_name [-option1] argument_1 [-option2] argument_2...
```

   pmrep runs the command and displays the prompt again.
3. Type `exit` to end an interactive session.

Running Commands in Normal Mode and Exclusive Mode

The Repository Service runs in normal or exclusive mode. Run the Repository Service in exclusive mode to perform tasks that permit only one user connection to the repository.

Run the Repository Service in exclusive mode to use the following *pmrep* commands:

- Create
- Delete
- Register
- RegisterPlugin
- Unregister
- UnregisterPlugin

You can use the Administrator tool or *infacmd* to run the Repository Service in exclusive mode.

pmrep Return Codes

pmrep indicates the success or failure of a command with a return code. Return code "0" indicates that the command succeeded. Return code "1" indicates that the command failed. Some commands perform multiple operations. For example, AddToDeploymentgroup adds multiple objects to a deployment group. In these cases, a Return code "0" indicates that the command was executed successfully even if only some of the objects were deployed successfully.

Enter one of the following DOS or UNIX echo commands immediately after running the *pmrep* command:

- In a DOS shell, enter `echo %ERRORLEVEL%`
- In a UNIX Bourne or Korn shell, enter `echo $?`
- In a UNIX C shell, enter `echo $status`

Using Native Connect Strings

Some *pmrep* commands, such as CreateConnection and Restore, require a native connect string.

The following table describes the native connect string syntax for each supported repository database:

Database	Connect String Syntax	Example
IBM DB2	*dbname*	mydatabase
Microsoft SQL Server	*servername*@*dbname*	sqlserver@mydatabase
Oracle	*dbname*.world (same as TNSNAMES entry)	oracle.world
Sybase ASE	servername@dbname	sambrown@mydatabase

Scripting pmrep Commands

When you use *pmrep*, you might use some commands with specific options and arguments on a regular basis. For example, you might use *pmrep* to perform a daily backup of a production repository. In this case, you can create a script file to call one or more *pmrep* commands including its options and arguments.

For example, the following Windows batch file, `backupproduction.bat`, connects to and backs up a repository called Production:

```
backupproduction.bat
REM This batch file uses pmrep to connect to and back up the repository Production on
the server ServerName
@echo off
echo Connecting to repository Production...
c:\PowerCenter\pmrep\pmrep connect -r Production -n Administrator -x Adminpwd -d
MyDomain -h Machine -o 8080
echo Backing up repository Production...
c:\PowerCenter\pmrep\pmrep backup -o c:\backup\Production_backup.rep
```

You can run script files from the command interface. You cannot run *pmrep* batch files in interactive mode.

Tips for Scripting pmrep Commands

Use the following tips when you create and run *pmrep* scripts:

- Include a Connect command as the first command called by the script file. This helps ensure that you perform tasks on the correct repository.
- To run *pmrep* scripts that connect to different repositories simultaneously, set the INFA_REPCNX_INFO environment variable in each environment to store the name and file path for the repository connection file. This prevents a script from overwriting the connection information used by another script.

Connection Subtypes

When you list or update a connection, you can specify the connection subtypes based on the associated connection type. Based on the repository plugins, the pmrep command lists the connection subtypes in the repository, by default.

The following table shows the list of connection subtypes for the associated type of connection:

Type of Connection	Connection Subtype
Relational	Sybase
Relational	Informix (Obsolete)
Relational	Microsoft SQL Server
Relational	DB2
Relational	ODBC
Relational	Teradata
Relational	Netezza
Relational	Vertica
Relational	PowerChannel for DB2
Relational	PowerChannel for Oracle
Relational	PowerChannel for MS SQL Server
Relational	PowerChannel for ODBC

Type of Connection	Connection Subtype
Relational	PWX DB2zOS
Relational	PWX DB2i5OS
Relational	PWX DB2LUW
Relational	PWX Oracle
Relational	PWX MSSQLServer
Relational	PWX NRDB Lookup
Relational	Teradata PT Connection
Application	SAP BW
Application	SAP R3
Application	PeopleSoft Oracle
Application	PeopleSoft Sybase
Application	PeopleSoft Informix
Application	PeopleSoft MsSqlserver
Application	PeopleSoft Db2
Application	Siebel Oracle
Application	Siebel Sybase
Application	Siebel Informix
Application	Siebel MsSqlserver
Application	Siebel Db2
Application	SAP_ALE_IDoc_Reader
Application	SAP Type A
Application	SAP_BWOHS_READER
Application	SAP_ALE_IDoc_Writer
Application	SAP RFC/BAPI Interface
Application	JNDI Connection
Application	JMS Connection
Application	webMethods Broker

Type of Connection	Connection Subtype
Application	webMethods Integration Server
Application	Web Services Consumer
Application	PWX NRDB Batch
Application	PWX NRDB CDC Change
Application	PWX NRDB CDC Real Time
Application	PWX DB2zOS CDC Change
Application	PWX DB2zOS CDC Real Time
Application	PWX DB2i5OS CDC Change
Application	PWX DB2i5OS CDC Real Time
Application	Http Transformation
Application	PWX Oracle CDC Change
Application	PWX Oracle CDC Real Time
Application	LMAPITarget
Application	Teradata FastExport Connection
Application	PWX MSSQL CDC Change
Application	PWX MSSQL CDC Real Time
Application	PWX DB2LUW CDC Change
Application	PWX DB2LUW CDC Real Time
Application	Salesforce Connection
Application	Hadoop HDFS Connection
FTP	FTP
External Loader	Teradata Mload External Loader
External Loader	Teradata Tpump External Loader
External Loader	DB2 EE External Loader
External Loader	DB2 EEE External Loader
External Loader	Teradata FastLoad External Loader
External Loader	Teradata Warehouse Builder External Loader

Type of Connection	Connection Subtype
External Loader	HP NeoView Java Transporter
Queue	Message Queue
Queue	MSMQ

AddToDeploymentGroup

Adds objects to a deployment group. Use AddToDeploymentGroup to add source, target, transformation, mapping, session, worklet, workflow, scheduler, session configuration, and task objects.

You cannot add checked out objects to a deployment group. You can specify objects using command options or you can use a persistent input file. If you use a persistent input file, you can enter the deployment group name option.

Use AddToDeploymentGroup to add reusable input objects. If you want to add non-reusable input objects, you must use a persistent input file that contains encoded object IDs.

If AddToDeploymentGroup runs successfully, it either sends back no status information, or it returns a list of objects that are already in the deployment group. If the command fails, it displays the reason for failure.

The AddToDeploymentGroup command uses the following syntax:

```
addtodeploymentgroup
-p <deployment_group_name>
{{-n <object_name>
  -o <object_type>
  -t <object_subtype>]
  [-v <version_number>]
  [-f <folder_name>]} |
  [-i <persistent_input_file>]}
[-d <dependency_types (all, "non-reusable", or none)>]
[-s dbd_separator]
```

The following table describes *pmrep* AddToDeploymentGroup options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the deployment group to add objects to.
-n	object_name	Required when you add a specific object. Name of the object you are adding to the deployment group. You cannot enter the name of a checked out object. You cannot use the -n option if you use the -i option.

Option	Argument	Description
-o	object_type	Required when adding a specific object. Type of object you are adding. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session configuration, task, cube, and dimension.
-t	object_subtype	Required when using valid subtypes. Type of task or transformation you are adding. For more information about valid subtypes, see "Listing Object Types" on page 1330.
-v	version_number	Optional. Version of the object to add. Default is the latest version of the object. The command fails if you specify a version number for a non-versioned repository.
-f	folder_name	Required when you enter an object name. Folder that contains the object you are adding.
-i	persistent_input_file	A text file generated from ExecuteQuery, Validate, or ListObjectDependencies that contains a list of object records with encoded IDs. If you use this parameter, *pmrep* does not allow the -n, -o, and -f options.
-d	dependency_types	Optional. Dependent objects to add to the deployment group with the object. Enter one of the following: - all. *pmrep* adds the objects and all dependent objects, reusable and non-reusable, to the deployment group. - "non-reusable". *pmrep* adds the objects and the corresponding non-reusable dependent objects to the deployment group. - none. *pmrep* does not add dependent objects to the deployment group. If you omit this parameter, *pmrep* adds the objects and all dependent objects to the deployment group. **Note:** Use double quotes around arguments that contain spaces or non-alphanumeric characters.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

ApplyLabel

Applies a label to an object or a set of objects in a folder. If you enter a folder name, all the objects in the folder receive the label. You can apply the label to dependent objects. If you use the `dependency_object_types` option, *pmrep* labels all dependent objects. To apply a label to selected dependent objects, separate each object type name by a comma with no spaces between them on the command line.

Use ApplyLabel to label reusable input objects. If you want to label non-reusable input objects, you must use a persistent input file that contains encoded object IDs.

If ApplyLabel succeeds, *pmrep* displays either no status information or a list of objects that already have the label. If the command fails, *pmrep* displays the reason for the failure.

The ApplyLabel command uses the following syntax:

```
applylabel
-a <label_name>
{{-n <object_name>
  -o <object_type>
  [-t <object_subtype>]
  [-v <version_number>]
  [-f <folder_name>] } |
  -i <persistent_input_file>}
[-d <dependency_object_types>]
[-p <dependency_direction (children, parents, or both)>]
[-s (include pk-fk dependency)]
[-g (across repositories)]
[-m (move label)]
[-c <comments>]
[-e dbd_separator]
```

The following table describes *pmrep* ApplyLabel options and arguments:

Option	Argument	Description
-a	label_name	Required. Label name to apply to the object.
-n	object_name	Required if you are updating a specific object. Name of the object to receive the label. You cannot enter object names if you use the -i option.
-o	object_type	Type of object to apply the label to. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session config, task, cube, or dimension. Required when applying a label to a specific object.
-t	object_subtype	Required. Type of task or transformation you are labeling. *pmrep* ignores other object types. For more information about valid subtypes, see "Listing Object Types" on page 1330.
-v	version_number	Optional. Version of the object to apply the label to. The command fails if the version is checked out. Applies the label to the latest version of the object by default.
-f	folder_name	Optional. Folder that contains the objects. If you enter a folder name but no object name, *pmrep* applies the label to all objects in the folder. If you enter a folder name with an object name, *pmrep* searches the folder for the object. You cannot use the -f option if you use the -i option.

Option	Argument	Description
-i	persistent_input_file	Optional. Name of a text file generated from ExecuteQuery, ListObjectDependency, or Validate. Contains a list of objects to receive the label. If you use this option, do not use the object name, object type, or folder name to specify objects.
-d	dependency_object_types	Optional. Dependent object types to label. Valid dependent object types include shortcuts, mappings, mapplets, sessions, workflows, worklets, target definitions, source definitions, and foreign key dependencies. Use this option with option -p. If you enter an object type, the label applies to dependent objects of that object type.
-p	dependency_direction	Optional. Dependent parents or children to apply the label to. You can specify parents, children, or both. If you do not enter option -d, all dependent objects receive the label. If you do not enter this option, the label applies to the specified object.
-s	-	Optional. Include the primary key-foreign key dependency objects regardless of the direction of the dependency.
-g	-	Optional. Find object dependencies across repositories.
-m	-	Optional. Move a label from the current version to the latest version of an object. Use this argument when the label type is one_per_object.
-c	comments	Optional. Comments about the label.
-e	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

AssignIntegrationService

Assigns the PowerCenter Integration Service to the specified workflow.

If you run the workflow from the Workflow Manager and you associated a PowerCenter Integration Service with the workflow in the *pmrep AssignIntegrationService* command, the workflow runs on the PowerCenter Integration Service specified with the -i option.

If you run the workflow from the command line, the workflow runs on the PowerCenter Integration Service specified in the *pmcmd StartWorkflow* command. The workflow does not run on the PowerCenter Integration Service that you specified in the *pmrep AssignIntegrationService* command.

The AssignIntegrationService command uses the following syntax:

```
assignintegrationservice
-f <folder_name>
-n <workflow_name>
-i <integration_service_name>
```

The following table describes *pmrep* AssignIntegrationService options and arguments:

Option	Argument	Description
-f	folder_name	Required. Name of the folder that contains the workflow. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-n	workflow_name	Required. Name of the workflow.
-i	integration_service_name	Required. Name of the PowerCenter Integration Service associated with the workflow.

AssignPermission

Allows you to add, remove, or update permissions on a global object for a user, group, or the Others default group.

Note: Only the administrator or the current owner of the object can manage permissions on the object.

The AssignPermission command uses the following syntax:

```
AssignPermission
-o <object_type>
[-t <object_subtype>]
-n <object_name>
{-u <user_name> | -g <group_name>}
[-s <security_domain>]
-p <permission>
```

The following table describes *pmrep* AssignPermission options and arguments:

Option	Argument	Description
-o	object_type	Required. Type of the object for which you want to manage permissions. You can specify folder, label, deploymentgroup, query, or connection.
-t	object_subtype	Optional. Type of connection object or query. Not required for other object types. For more information about valid subtypes, see "AssignPermission" on page 1289.
-n	object_name	Required. Name of the object for which you want to manage permissions. You can use special characters for the object name.
-u	user_name	Required if you do not use the -g option. Name of the user for whom you want to add, remove, or update permissions. Use the -u or -g option, not both.

Option	Argument	Description
-g	group_name	Name of the group for which you want to add, remove, or update permissions. Specify “Others” as the group name to change permissions for the Others default group. Use the -u or -g option, but not both. You can use special characters for the group name.
-s	security_domain	Required if you use LDAP authentication. Name of the security domain that the user or group belongs to. Default is Native.
-p	permission	Required. Permissions you want to add, remove, or update. You assign read, write and execute permission on a global object. Use the characters r, w, and x to assign read, write, and execute permissions.

The following table describes the object types and values to use with *pmrep* commands:

Object Type	Object Subtype
Query	Shared
Query	Personal
Connection	Application
Connection	FTP
Connection	Loader
Connection	Queue
Connection	Relational

Example

You can add, remove, or update permissions with the -p option.

For example, to add read and write permissions on a folder, enter the following text at the prompt:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

You can also update permissions on an object. For example, you assigned permission to read on a folder and need to include permission to write. To update permissions, enter the following text at the prompt:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p rw
```

To remove all permissions, enter the following text at the prompt:

```
pmrep AssignPermission -o folder -n Sales -u Admin -p ""
```

BackUp

Backs up the repository to the file specified with the -o option. You must provide the backup file name. Use this command when the repository is running. You must be connected to a repository to use this command.

The BackUp command uses the following syntax:

```
backup
-o <output_file_name>
[-d <description>]
[-f (overwrite existing output file)]
[-b (skip workflow and session logs)]
[-j (skip deploy group history)]
[-q (skip MX data)]
[-v (skip task statistics)]
```

The following table describes *pmrep* BackUp options and arguments:

Option	Argument	Description
-o	output_file_name	Required. Name and path of the file for the repository backup. When you view the list of repository backup files in the Administrator tool, you can see only files with an extension of .rep.
-d	description	Optional. Creates a description of the backup file based on the string that follows the option. The backup process truncates any character beyond 2,000.
-f	-	Optional. Overwrites an existing file with the same name.
-b	-	Optional. Skips tables related to workflow and session logs during backup.
-j	-	Optional. Skips deployment group history during backup.
-q	-	Optional. Skips tables related to MX data during backup.
-v	-	Optional. Skips task statistics during backup.

To restore the backup file, use the Administrator tool, or use the *pmrep* Restore command.

ChangeOwner

Changes the owner name for a global object.

Note: Only the administrator or current owner of the object have the permission to change ownership for an object.

The ChangeOwner command uses the following syntax:

```
ChangeOwner
-o <object_type>
```

```
[-t <object_subtype>]
-n <object_name>
-u <new_owner_name>
[-s <security_domain>]
```

The following table describes *pmrep* ChangeOwner options and arguments:

Option	Argument	Description
-o	object_type	Required. Type of the object. You can specify folder, label, deploymentgroup, query, or connection.
-t	object_subtype	Optional. Type of object query or connection object. Not required for other object types. For more information about valid subtypes, see "AssignPermission" on page 1289.
-n	object_name	Required. Name of the object. You can use special characters for the object name.
-u	new_owner_name	Required. Name of the changed owner. The changed owner name must be a valid user account in the domain.
-s	security_domain	Required if you use LDAP authentication. Name of the security domain that the new owner belongs to. Default is Native.

CheckIn

Checks in an object that you have checked out. When you check in an object, the repository creates a new version of the object and assigns it a version number. The version number is one number greater than the version number of the last checked-in version.

The CheckIn command uses the following syntax:

```
checkin
-o <object_type>
[-t <object_subtype>]
-n <object_name>
-f <folder_name>
[-c <comments>]
[-s dbd_separator]
```

The following table describes *pmrep* CheckIn options and arguments:

Option	Argument	Description
-o	object_type	Required. Type of object you are checking in: source, target, transformation, mapping, session, worklet, workflow, scheduler, session config, task, cube, or dimension.
-t	object_subtype	Optional. Type of task or transformation to check in. Not required for other object types. For more information about valid subtypes, see "Listing Object Types" on page 1330.
-n	object_name	Required. Name of the object that you are checking in.
-f	folder_name	Required. Folder to contain the new object version.
-c	comments	Optional. Comments about the check in.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name \source_name, and define the dbd_separator as backslash (\).

CleanUp

Cleans up any persistent resource created by *pmrep*. This command also cleans up any connection information from previous sessions of *pmrep*. Calling CleanUp as the first command in a session always returns an error.

If you call CleanUp in the interactive mode, *pmrep* disconnects any repository you are connected to.

The CleanUp command uses the following syntax:

```
cleanup
```

ClearDeploymentGroup

Clears all objects from a deployment group. Use this command to retain the deployment group but remove the objects.

The ClearDeploymentGroup command uses the following syntax:

```
cleardeploymentgroup

-p <deployment_group_name>

[-f (force clear)]
```

The following table describes *pmrep* ClearDeploymentGroup options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the deployment group that you want to clear.
-f	-	Optional. Remove objects without confirmation. If you omit this argument, the command prompts you for a confirmation before it clears the objects.

Connect

Connects to a repository. The first time you use pmrep in either command line or interactive mode, you must use the Connect command. All commands require a connection to the repository except for the following commands:

- Exit
- Help
- ListAllPrivileges

In the command line mode, pmrep uses the information specified by the last call to connect to the repository. If pmrep is called without a successful connection, it returns an error. In command line mode, pmrep connects to and disconnects from the repository with every command.

To use pmrep to perform tasks in multiple repositories in a single session, you must issue the Connect command each time you want to switch to a different repository. In the interactive mode, pmrep retains the connection until you exit pmrep or connect again. If you call Connect again, pmrep disconnects from the first repository and then connects to the second repository. If the second connection fails, the previous connection remains disconnected and you will not be connected to any repository. If you issue a command that requires a connection to the repository, and you are not connected to that repository, pmrep uses the connection information specified in the last successful connection made to the repository from any previous session of pmrep. pmrep retains information from the last successful connection until you use the Cleanup command.

The Connect command uses the following syntax:

```
connect

-r <repository_name>

{-d <domain_name> |

 {-h <portal_host_name>

  -o <portal_port_number>}}

[{-n <user_name>

[-s <user_security_domain>]

[-x <password> |

 -X <password_environment_variable>]} |

-u <connect_without_user_in_kerberos_mode>]

[-t <client_resilience>]
```

The following table describes pmrep Connect options and arguments:

Option	Argument	Description
-r	repository_name	Required. Name of the repository you want to connect to.
-d	domain_name	Required if you do not use -h and -o. Name of the domain for the repository. If you use the -d option, do not use the -h and -o options.
-h	portal_host_name	Required if you do not use -d. If you use the -h option, then you must also use the -o option. Gateway host name.
-o	portal_port_number	Required if you do not use -d. If you use the -o option, then you must also use the -h option. Gateway port number.
-n	user_name	Optional. User name used to connect to the repository.
-s	user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.
-x	password	Required if you use the -n option and you do not use the -X option. Password for the user name. The password is case sensitive. Use the -x or -X option, but not both.
-X	password_ environment_variable	Required if you use the -n option and you do not use the -x option. Password environment variable. Use the -x or -X option, but not both.
-u	connect_without _user_ in_kerberos_mode	Required. Connects to a Repository Service without a user name and password when the Informatica domain uses Kerberos authentication. Use the -u option to connect to the Repository Service if the repository has no content.
-t	client_resilience	Optional. Amount of time in seconds that pmrep attempts to establish or reestablish a connection to the repository. If you omit the -t option, pmrep uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

Create

Creates the repository tables in the database. Before you can create the repository tables, you must complete these tasks:

- Create and configure the database to contain the repository.
- Create the Repository Service in either the Administrator tool or *infacmd*.
- Run the Repository Service in exclusive mode in either the Administrator tool or *infacmd*.
- Connect to the repository in *pmrep*.

You cannot use the Create command if the repository database already contains repository tables.

To use the Create command, you must have permission on the Repository Service in the domain.

The Create command uses the following syntax:

```
create
-u <domain_user_name>
[-s <domain_user_security_domain>]
[-p <domain_password> |
 -P <domain_password_environment_variable>]
[-g (create global repository)]
[-v (enable object versioning)]
```

The following table describes *pmrep* Create options and arguments:

Option	Argument	Description
-u	domain_user_name	Required. User name.
-s	domain_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.
-p	domain_password	Optional. Password. Use either the -p or -P option, but not both. If you do not use either the -p or -P option, *pmrep* prompts you to enter the password.
-P	domain_password_ environment_variable	Optional. Password environment variable. Use either the -p or -P option, but not both. If you do not use either the -p or -P option, *pmrep* prompts you to enter the password.
-g	-	Optional. Promotes the repository to a global repository.
-v	-	Optional Enables object versioning for the repository.

CreateConnection

Creates a source or target connection in the repository. The connection can be a relational, application, or an FTP connection. Relational database connections for each relational subtype require a subset of all

CreateConnection options and arguments. For example, Oracle connections do not accept the -z, -d, or -t options. Use the -k option to specify attributes for application connections.

The CreateConnection command uses the following syntax:

```
createconnection

-s <connection_subtype>

-n <connection_name>

[{-u <user_name>

[{-p <password> |

-P <password_environment_variable>

[-w (use parameter in password)]}]}]|

-K <connection_to_the_Kerberos_server>]

[-c <connect_string> (required for Oracle, Informix, DB2, Microsoft SQL Server, ODBC,
and NetezzaRelational)]

[-l <code_page>]

[-r <rollback_segment> (valid for Oracle connection only)]

[-e <connection_environment_SQL>]

[-f <transaction_environment_SQL>]

[-z <packet_size> (valid for Sybase ASE and MS SQL Server connection)]

[-b <database_name> (valid for Sybase ASE, Teradata and MS SQL Server connection)]

[-v <server_name> (valid for Sybase ASE and MS SQL Server connection)]

[-d <domain_name> (valid for MS SQL Server connection only)]

[-t (enable trusted connection, valid for MS SQL Server connection only)]

[-a <data_source_name> (valid for Teradata connection only)]

[-x (enable advanced security, lets users give Read, Write and Execute permissions only
for themselves.)]

[-k <connection_attributes> (attributes have the format name=value;name=value; and so
on)]

[-y (Provider Type (1 for ODBC and 2 for OLEDB), valid for MS SQL Server connection
only)]

[-m (UseDSN, valid for MS SQL Server connection only)]

[-S <odbc_subtype> (valid for ODBC connection only, default is None)]
```

The following table describes *pmrep* CreateConnection options and arguments:

Option	Argument	Description
-s	connection_subtype	Required. Displays the connection subtype. A connection can be one of the following types: - Application - FTP - Relational For example, for a Relational connection, connection subtypes include Oracle, Sybase, and Microsoft SQL Server. For FTP connections, the valid subtype is FTP.
-n	connection_name	Required. Name of the connection.
-u	user_name	Required for some connection types. User name used for authentication.
-p	password	Required for some connection types. Password used for authentication when you connect to the relational database. Use the -p or -P option, but not both. If you specify a user name and you do not specify -p or -P, pmrep prompts you for the password. To specify a parameter in the password, add the $Param prefix for the -p option and ensure that you use the -w option. Do not use a dollar sign ($) anywhere else in the -p option, and enter the parameter password without spaces. For example, `-p '$Param_abc' -w`
-P	password_ environment_variable	Optional. Password environment variable used for authentication when you connect to the relational database. Use the -p or -P option, but not both. If you do not use the -p or -P option, *pmrep* prompts you for the password.
-w	-	Optional. Enables you to use a parameter in the password option. *pmrep* uses the password specified with the -p or -P option as the name of the session parameter at run time. Valid only if you use the -p or -P option. If you do not use a parameter in the password option, *pmrep* uses the user password specified with the -p or -P option.
-K	connection_to_the_Kerberos_server	Optional. Indicates that the database that you are connecting to runs on a network that uses Kerberos authentication.
-c	connect_string	Connect string the Integration Service uses to connect to the relational database.
-l	code_page	Required for some connection types. Code page associated with the connection.
-r	rollback_segment	Optional. Valid for Oracle connections. The name of the rollback segment. A rollback segment records database transactions that allow you to undo the transaction.
-e	connection_ environment_sql	Optional. Enter SQL commands to set the database environment when you connect to the database. The Integration Service executes the connection environment SQL each time it connects to the database.

Option	Argument	Description
-f	transaction_ environment_sql	Optional. Enter SQL commands to set the database environment when you connect to the database. The Integration Service executes the transaction environment SQL at the beginning of each transaction.
-z	packet_size	Optional. Valid for Sybase ASE and Microsoft SQL Server connections. Optimizes the ODBC connection to Sybase ASE and Microsoft SQL Server.
-b	database_name	Optional. Name of the database. Valid for Sybase ASE and Microsoft SQL Server connections.
-v	server_name	Optional Name of the database server. Valid for Sybase ASE and Microsoft SQL Server connections.
-d	domain_name	Optional Valid for Microsoft SQL Server connections. The name of the domain. Used for Microsoft SQL Server.
-t	-	Optional. Valid for Microsoft SQL Server connections. If enabled, the Integration Service uses Windows authentication to access the Microsoft SQL Server database. The user name that starts the Integration Service must be a valid Windows user with access to the Microsoft SQL Server database.
-a	data_source_name	Optional Teradata ODBC data source name. Valid for Teradata connections.
-x	-	Enables enhanced security. Grants you read, write, and execute permissions. Public and world groups are not granted any permissions. If this option is not enabled, all groups and users are granted read, write, and execute permissions.
-k	connection_attributes	Enables user-defined connection attributes. Attributes have the format <name>=<value>;<name>=<value>. **Note:** Do not add a space before the attribute name.
-y	-	Enables the provider type value. You can specify the following provider types: - 1 for ODBC - 2 for Oledb(Deprecated)
-m	-	Enables the Use DSN attribute. The PowerCenter Integration Service retrieves the database and server names from the DSN.
-S	odbc_subtype	Optional. Enables the ODBC subtype for an ODBC connection. An ODBC connection can be one of the following ODBC subtypes: - AWS Redshift - Azure DW - Greenplum - Google Big Query - PostgreSQL - Snowflake - SAP HANA - None Default is None.

For more information about connection subtypes, see "Connection Subtypes" on page 1282.

Specifying the Database Code Page

The -l option specifies the code page for the database connection. Enter the code page name you want to assign to the database connection. For example, to assign the US-ASCII code page to the database connection, enter the code page name "US-ASCII."

Changing the database connection code page can cause data inconsistencies if the new code page is not compatible with the source or target database connection code pages. Also, if you configure the Integration Service for data code page validation, changing the database connection code page can cause sessions to fail if the source database connection code page is not a subset of the target database connection code page.

CreateDeploymentGroup

Creates a deployment group. You can create a dynamic or static deployment group. To create a dynamic deployment group, you must supply a query name, and indicate whether the query is private or public.

The CreateDeploymentGroup command uses the following syntax:

```
createdeploymentgroup
-p <deployment_group_name>
[-t <deployment_group_type (static or dynamic)>]
[-q <query_name>]
[-u <query_type (shared or personal)>]
[-c <comments>]
```

The following table describes *pmrep* CreateDeploymentGroup options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the deployment group to create.
-t	deployment_group_type	Optional. Create a static group or use a query to dynamically create the group. You can specify static or dynamic. Default is static.
-q	query_name	Required if the deployment group is dynamic, but ignored if the group is static. Name of the query associated with the deployment group.
-u	query_type	Required if the deployment group is dynamic, but ignored if the group is static. Type of query to create a deployment group. You can specify shared or personal.
-c	comments	Optional. Comments about the new deployment group.

CreateFolder

Creates a folder in the repository.

The CreateFolder command uses the following syntax:

```
createfolder
-n <folder_name>
[-d <folder_description>]
[-o <owner_name>]
[-a <owner_security_domain>]
[-s (shared_folder)]
[-p <permissions>]
[-f <active | frozendeploy | frozennodeploy>]
```

The following table describes *pmrepCreateFolder* options and arguments:

Option	Argument	Description
-n	folder_name	Required. Folder name.
-d	folder_description	Optional. Description of the folder that appears in the Repository Manager. If the folder description contains spaces or other non-alphanumeric characters, enclose it in quotation marks.
-o	owner_name	Optional. Owner of the folder. Any user in the repository can be the folder owner. Default owner is the user creating the folder.
-a	owner_security_domain	Required if you use LDAP authentication. Name of the security domain that the owner belongs to. Default is Native.
-s	-	Optional. Makes the folder shared.
-p	permissions	Optional. Access rights for the folder. If omitted, the Repository Service assigns default permissions.
-f	active frozendeploy frozennodeploy	Optional. Changes the folder status to one of the following statuses: - active. This status allows users to check out versioned objects in the folder. - frozendeploy (Frozen, Allow Deploy to Replace). This status prevents users from checking out objects in the folder. Deployment into the folder creates new versions of the objects. - frozennodeploy (Frozen, Do Not Allow Deploy to Replace). This status prevents users from checking out objects in the folder. You cannot deploy objects into this folder.

Note: You can add, remove, or update permissions on a folder by using the AssignPermission command.

Assigning Permissions

You can assign repository permissions by entering a digit when you use the -p option.

Enter one number for each set of permissions. Designate 4 for read permission, 2 for write permission, and 1 for execute permission. To assign permissions, you enter 4, 2, 1, or the sum of any of those numbers.

For example, if you want to assign default permissions, use the following command syntax:

```
-p 764
```

This gives the folder owner read, write, and execute permissions (7 = 4+2+1). The owner's group has read and write permissions (6 = 4+2). All others have read permission.

Note: By default, the folder owner is always granted read, write, and execute permissions, and the group is always granted default permissions from the third correspondents. You cannot update the folder owner and group permissions for a shared folder.

The command returns "createfolder successfully completed" or returns "createfolder failed" message. The creation might fail for the following reasons:

- The folder already exists.
- The owner does not exist or does not belong to the group.

CreateLabel

Creates a label that you use to associate groups of objects during development. You can associate a label with any versioned object or group of objects in a repository.

The CreateLabel command uses the following syntax:

```
createlabel

-a <label_name>

[-c <comments>]
```

The following table describes *pmrep* CreateLabel options and arguments:

Option	Argument	Description
-a	label_name	Required. Name of the label you are creating.
-c	comments	Optional. Comments about the label.

CreateQuery

Creates an object query in the repository. You must configure the query conditions to create an object query. A query condition consists of a parameter, an operator, and a value. You can enter the expression in a file or at the command prompt.

The CreateQuery command uses the following syntax:

```
createquery

-n <query_name>

-t <query_type (shared or personal)>
```

```
{-e <expression> |
-f <file_name>}
[-u (UTF-8 encoded input file)]
[-c <comments>]
```

The following table describes *pmrep* CreateQuery options and arguments:

Option	Argument	Description
-n	query_name	Required. Name of the query that you want to create.
-t	query_type	Required. The type of query. You can specify shared or personal.
-e	expression	Required if you do not use the -f option. Expression of the query.
-f	file_name	Required if you do not use the -e option. Name and path of the file that contains the expression of a query. You must use the -e or -f option, but not both.
-u	-	Optional. Encodes the file in the UTF-8 format. **Note:**If you do not specify the -u option, the default system encoding encodes the file.
-c	comments	Optional. Comments about the query.

The following table describes the query parameters and the valid operators and values for each parameter that you can use in an expression:

Parameter	Description	Valid Operator	Accepted Values
BusinessName	Displays sources and targets based on their business names. For example, the query Business Name is Equal to Informatica, returns sources and targets that contain the Informatica business name and filters out all other objects.	Contains, EndsWith, Equals, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	String
CheckinTime	Displays checked in versioned objects for a specified time, before or after a specified time, or within a specified number of days. You can specify this parameter for versioned repositories only.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric

Parameter	Description	Valid Operator	Accepted Values
CheckoutTime	Displays checked out versioned objects for a specified time, before or after a specified time, or within a specified number of days. You can specify this parameter for versioned repositories only.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
Comments	Displays comments associated with a source, target, mapping, or workflow.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not In, Not StartsWith, StartsWith	String
DeploymentDispatchHistory	Displays versioned objects deployed to another folder or repository through deployment groups in a given time period.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
DeploymentReceiveHistory	Displays versioned objects deployed from another folder or repository using deployment groups in a given time period.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric
Folder	Displays objects in a specified folder.	Equals, In, Not Equals, Not In	Folder name

Parameter	Description	Valid Operator	Accepted Values
IncludeChildren	Displays child dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.
IncludeChildrenAndParents	Displays child and parent dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.

Parameter	Description	Valid Operator	Accepted Values
IncludeParents	Displays parent dependent objects.	Where (Value 1) depends on (Value 2), (Value 3)	For value 1 and value 2, use: Any, Source Definition, Target Definition, Transformation, Mapplet, Mapping, Cube, Dimension, Task, Session, Worklet, Workflow, Scheduler, SessionConfig For value 3 use: Non-reusable dependency, Reusable dependency.
IncludePKFKDependencies	Displays primary key-foreign key dependencies.	-	-
ImpactedStatus	Displays objects based on impacted status. Objects can be marked as impacted when a child object changes in such a way that the parent object may not be able to run.	Equals	Impacted, Not Impacted
Label	Displays versioned objects associated with a label or group of labels. You can specify this parameter for versioned repositories only.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, In, Not StartsWith, Not In, StartsWith	String
LastSavedTime	Displays objects saved at a particular time or within a particular time range.	Between, GreaterThan, LessThan, Not Between, WithinLastDays	Date/time, Numeric

Parameter	Description	Valid Operator	Accepted Values
LatestStatus	Displays versioned objects based on the object history. The query can return local objects that are checked out, the latest version of checked-in objects, or a collection of all older versions of objects. You can specify this parameter for versioned repositories only.	Equals, Not Equals, In	Checked-out Latest, Checked-in Older
MetadataExtension	Displays objects based on an extension name or value pair. Use this query parameter to find non-reusable metadata extensions. The query does not return user-defined reusable metadata extensions.	Equals, Not Equals	Vendor-defined metadata domain
ObjectName	Displays objects based on the object name.	Contains, Equals, EndsWith, In, Not Contains, Not Equals, Not EndsWith, Not StartsWith, Not In, StartsWith	String
ObjectType	Displays objects based on the object type. For example, you can find all workflows in a specified folder.	Equals, In, Not Equals, Not In	Cube, Dimension, Mapping, Mapplet, Scheduler, Session, Session Config, Source Definition, Target Definition, Task, Transformation, User-Defined Function, Workflow, Worklet

Parameter	Description	Valid Operator	Accepted Values
ObjectUsedStatus	Displays objects that are used by other objects. For example, you can find mappings that are not used in any session. If any version of an object is used by another object, the query returns the most recent version of the object. This occurs even when the most recent version of the object is unused. The query does not return workflows or cubes because these objects cannot be used by other objects.	Equals	Unused, Used
ShortcutStatus	Displays objects based on shortcut status. If you select this option, the query returns local and global shortcut objects. Shortcut objects are considered valid regardless of whether the objects they reference are valid.	Equals	Is Not Shortcut, Is Shortcut
Reusable Status	Displays reusable or non-reusable objects.	Equals, In	Non-reusable, Reusable
User	Displays objects checked in or checked out by the specified user.	Equals, In, Not Equals, Not In	Users in specified repository
ValidStatus	Displays valid or invalid objects. The Repository Service validates an object when you run validation or save an object to the repository.	Equals	Invalid, Valid
VersionStatus	Displays objects based on deleted or non-deleted status. You can specify this parameter for versioned repositories only.	Equals, In	Deleted, Not deleted

Examples

Review the following samples to correctly use the pmrep CreateQuery command:

Session as the object type

Set the query in either single or double quotes.

Example:

```
pmrep createQuery -n <TEST1> -t <shared> -e "ObjectType Equals Session"
```

Source definition as the object type

Set the expression between double quotes and set the source definition string within single quotes.

Example:

```
pmrep createQuery -n <TEST2> -t <shared> -e "ObjectType Equals 'Source Definition'"
```

Set the folder name and set the object type to session

Enclose the folder name in parenthesis and the object type in another parenthesis and use the AND operator.

Example:

```
pmrep createquery -n "T_Query17" -t shared -e "(Folder=Folder1) AND (ObjectType=Session)"
```

Setting the status as reusable

Specify the reusable status in single quotes without spaces.

Example:

```
pmrep createQuery -n <TEST5> -t <shared> -e "'ReusableStatus' Equals Reusable"
```

Set the status to include the reusable and non reusable values

Enclose the list of expected values between parenthesis and separate the values with a comma.

For instance:

```
pmrep createQuery -n <TEST5.1> -t <shared> -e "ReusableStatus In '(Non-
reusable,Reusable)'"
```

Delete

Deletes the repository tables from the repository database.

Before you use the Delete command, you must connect to the repository and provide a user name and password or password environment variable.

When you use the Delete command, the Repository Service must be running in exclusive mode. You can configure the Repository Service to run in exclusive mode in the Administrator tool or you can use the *infacmd* UpdateRepositoryService command.

The Delete command uses the following syntax:

```
delete
[-x <repository_password_for_confirmation> |
 -X <repository_password_environment_variable_for_confirmation>]
[-f (forceful delete: unregisters local repositories and deletes)]
```

The following table describes *pmrep* Delete options and arguments:

Option	Argument	Description
-x	repository_password_for_ confirmation	Optional. Password. You can use the -x or -X option, but not both. If you do not use the -x or -X option, *pmrep* prompts you to enter the password for confirmation.
-X	repository_password_ environment_variable_for_ confirmation	Optional. Password environment variable. You can use the -x or -X option, but not both. If you do not use the -x or -X option, *pmrep* prompts you to enter the password for confirmation.
-f	-	Optional. Deletes a global repository and unregisters local repositories. All registered local repositories must be running.

DeleteConnection

Deletes a relational connection from the repository.

The DeleteConnection command uses the following syntax:

```
deleteconnection
-n <connection_name>
[-f (force delete)]
[-s <connection type application, relational, ftp, loader or queue>]
```

The following table describes *pmrep* DeleteConnection options and arguments:

Option	Argument	Description
-n	connection_name	Required. Name of the connection to delete.
-f	-	Optional. Connection will be deleted without further confirmation.
-s	connection type application, relational, ftp, loader or queue	Optional. Type of connection. A connection can be one of the following types: - Application - FTP - Loader - Queue - Relational Default is relational.

DeleteDeploymentGroup

Deletes a deployment group. If you delete a static deployment group, you also remove all objects from the deployment group.

The DeleteDeploymentGroup command uses the following syntax:

```
deletedeploymentgroup
-p <deployment_group_name>
[-f (force delete)]
```

The following table describes *pmrep* DeleteDeploymentGroup options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the deployment group to delete.
-f	-	Optional. Deletes the deployment group without confirmation. If you omit this argument, *pmrep* prompts you for a confirmation before it deletes the deployment group.

DeleteFolder

Deletes a folder from the repository.

The DeleteFolder command uses the following syntax:

```
deletefolder
-n <folder_name>
```

The following table describes *pmrep* DeleteFolder option and argument:

Option	Argument	Description
-n	folder_name	Required. Name of the folder.

DeleteLabel

Deletes a label and removes the label from all objects that use it. If the label is locked, the delete fails.

The DeleteLabel command uses the following syntax:

```
deletelabel
-a <label_name>
[-f (force delete)]
```

The following table describes *pmrep* DeleteLabel options and arguments:

Option	Argument	Description
-a	label_name	Required. Name of the label to delete.
-f	-	Optional. Delete the label without confirmation. If you omit this argument, the command prompts you for a confirmation before it deletes the label.

DeleteObject

Deletes an object. Use DeleteObject to delete a source, target, user-defined function, mapplet, mapping, session, worklet or workflow.

The DeleteObject command uses the following syntax:

```
DeleteObject
-o <object_type>
-f <folder_name>
-n <object_name>
[-s dbd_separator]
```

The following table describes *pmrep* DeleteObject options and arguments:

Option	Argument	Description
-o	object_type	Required Type of the object you are deleting: source, target, mapplet, mapping, session, “user defined function”, worklet, workflow.
-f	folder_name	Required Name of the folder that contains the object.
-n	object_name	Required. Name of the object you are deleting. If you delete a source definition you must prepend the database name. For example, DBD.sourcename.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name \source_name, and define the dbd_separator as backslash (\).

Note: You can run the DeleteObject command against a non-versioned repository. If you run the DeleteObject command against a versioned repository, *pmrep* returns the following error:

```
This command is not supported because the versioning is on for the repository
<Repository name>.
Failed to execute DeleteObject
```

DeleteQuery

Deletes an object query from the repository. You cannot delete an object query associated with a deployment group.

The DeleteQuery command uses the following syntax:

```
deletequery
-n <query_name>
-t <query_type (shared or personal)>
[-f (force delete)]
```

The following table describes *pmrep* DeleteQuery options and arguments:

Option	Argument	Description
-n	query_name	Required. Name of the query that you want to delete.
-t	query_type	Required. The type of query. You can specify shared or personal.
-f	-	Optional. Delete the query without confirmation. If you omit this argument, the command prompts for a confirmation before it deletes the query.

DeployDeploymentGroup

Deploys a deployment group. You can use this command to copy a deployment group within a repository or to a different repository.

To use this command, you must create a control file with all the specifications that the Copy Wizard requires. The control file is an XML file defined by the depcntl.dtd file.

If *pmrep* cannot immediately acquire object locks in the target repository, by default it waits indefinitely to acquire the locks.

You can use the deployment control file parameters to specify a deployment timeout. The deployment timeout is the period of time (in seconds) that *pmrep* waits to acquire locks. A value of 0 fails the deployment if *pmrep* cannot immediately acquire locks. The default value is -1, which instructs *pmrep* to wait indefinitely to acquire the locks.

Press Ctrl+C to cancel the deployment during the deployment operation or while *pmrep* is waiting to acquire object locks.

The DeployDeploymentGroup command uses the following syntax:

```
deploydeploymentgroup
-p <deployment_group_name>
-c <control_file_name>
-r <target_repository_name>
[-n <target_repository_user_name>
[-s <target_repository_user_security_domain>]
```

```
    [-x <target_repository_password> |
     -X <target_repository_password_environment_variable>]
    [-d <target_domain_name> |
     {-h <target_portal_host_name>
      -o <target_portal_port_number>}]] (only if target is in a different domain)
  [-l <log_file_name>]
```

The following table describes *pmrep* DeployDeploymentGroup options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the group to deploy.
-c	control_file_name	Required. Name of the XML file containing the Copy Wizard specifications. The deployment control file is required.
-r	target_repository_name	Required. Name of the target repository where you are copying the deployment group.
-n	target_repository_user_name	Required if you copy the deployment group to a different repository. Login user name for the target repository.
-s	target_repository_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.
-x	target_repository_password	Optional. Login password for the target repository. You use the -x or -X option, but not both. If you copy the deployment group to a different repository and you do not use the -x or -X option, *pmrep* prompts you for the password.
-X	target_repository_password_environment_variable	Optional. Login password environment variable for the target repository. You use the -x or -X option, but not both. If you copy the deployment group to a different repository and you do not use the -x or -X option, *pmrep* prompts you for the password.
-d	target_domain_name	Required if you copy the deployment group to a different repository and you do not use the -h and -o options. Name of the domain for repository.
-h	target_portal_host_name	Required if you copy the deployment group to a different repository and you do not use the -d option. Machine name for the node that hosts the domain of the target repository.
-o	target_portal_port_number	Required if you copy the deployment group to a different repository and you do not use the -d option. Port number for the node that hosts the domain of the target repository.
-l	log_file_name	Optional. Log file that records each deployment step. If you omit this option, *pmrep* outputs the deployment steps to the command line window.

DeployFolder

Deploys a folder. You can use this command to copy a folder within a repository or to a different repository.

To use this command, you must create a control file with all the specifications that the Copy Wizard requires. The control file is an XML file defined by the depcntl.dtd file.

If *pmrep* cannot immediately acquire object locks in the target repository, by default it waits indefinitely to acquire the locks.

You can use the deployment control file parameters to specify a deployment timeout. The deployment timeout is the period of time (in seconds) that *pmrep* waits to acquire locks. A value of 0 fails the deployment if *pmrep* cannot immediately acquire locks. The default value is -1, which instructs *pmrep* to wait indefinitely to acquire the locks.

Press Ctrl+C to cancel the deployment during the deployment operation or while *pmrep* is waiting to acquire object locks.

The DeployFolder command uses the following syntax:

```
deployfolder
-f <folder_name>
-c <control_file_name>
-r <target_repository_name>
[-n <target_repository_user_name>
[-s <target_repository_user_security_domain>]
 [-x <target_repository_password> |
  -X <target_repository_password_environment_variable>]
 [-d <target_domain_name> |
   {-h <target_portal_host_name>
    -o <target_portal_port_number>}]] (only if target is in a different domain)
[-l <log_file_name>]
```

The following table describes *pmrep* DeployFolder options and arguments:

Option	Argument	Description
-f	folder_name	Required. Name of the folder to deploy.
-c	control_file_name	Required. Name of the XML file containing the Copy Wizard specifications.
-r	target_repository_name	Required. Name of the target repository you are copying the folder to.
-n	target_repository_user_name	Required if you copy the folder to another repository. Login user name for the target repository.
-s	target_repository_user_ security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.

Option	Argument	Description
-x	target_repository_user_password	Optional. Login password for the target repository. Use the -x or -X option, but not both. If you copy the folder to a different repository and you do not use the -x or -X option, *pmrep* prompt you for the password.
-X	target_repository_password_environment_variable	Optional. Login password environment variable for the target repository. Use the -x or -X option, but not both. If you copy the folder to a different repository and you do not use the -x or -X option, *pmrep* prompt you for the password.
-d	target_domain_name	Required if you copy the folder to a different repository and you do not use the -h and -o options. Name of the domain for the repository.
-h	target_portal_host_name	Required if you copy the folder to a different repository and you do not use the -d option. Machine name for the node that hosts the domain of the target repository.
-o	target_portal_port_number	Required if you copy the folder to a different repository and you do not use the -d option. Port number for the node that hosts the domain of the target repository.
-l	log_file_name	Optional. Log file that records each deployment step. If you omit this option, *pmrep* outputs the deployment steps to the command line window.

ExecuteQuery

Runs a query. You can choose to display the result or write the result to a persistent input file. If the query is successful, it returns the total number of qualifying records.

Use the persistent input file with the ApplyLabel, AddToDeploymentGroup, MassUpdate, and Validate commands.

The ExecuteQuery command uses the following syntax:

```
executequery
-q <query_name>
[-t <query_type (shared or personal)>]
[-u <output_persistent_file_name>]
[-a (append)]
[-c <column_separator]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
[-n (do not include parent path)]
```

```
[-s <dbd_separator>]
```

The following table describes *pmrep* ExecuteQuery options and arguments:

Option	Argument	Description
-q	query_name	Required. Name of the query to run.
-t	query_type	Optional. Type of query to run. You can specify public or private. If not specified, *pmrep* searches all the private queries first to find the matching query name. Then it searches the public queries.
-u	persistent_output_file_name	Optional. Send the query result to a text file. If you do not enter a file name, the query result goes to stdout.
-a	-	Optional. Appends the query results to the persistent output file. If you do not enter this option, *pmrep* overwrites the file content.
-c	column_separator	Optional. Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. If you omit this option, *pmrep* uses a single space.
-r	end-of-record_separator	Optional. Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a new line.
-l	end-of-listing_indicator	Optional. Character or set of characters used to specify the end of the object list. Enter a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a period.
-b	-	Optional. Verbose. Displays more than the minimum information about the objects. If you omit this option, *pmrep* prints a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the object status, version number, folder name, and checked out information. The short format for global objects, such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the label type, query type, deployment group type, creator name, and creation time.
-y	-	Optional. Displays the database type of sources and targets.

Option	Argument	Description
-n	-	Optional. Does not include the full parent path of non-reusable objects in the query result. For example, if you use this option and the result includes a non-reusable transformation, *pmrep* prints transformation_name instead of mapping_name.transformation_name. This option can improve *pmrep* performance.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

Exit

Exits from the *pmrep* interactive mode.

The command line mode invokes and exits *pmrep* each time you issue a command.

The Exit command uses the following syntax:

```
exit
```

FindCheckout

Displays a list of checked out objects in the repository. The listing contains the checked-out items unless you enter “all users.”

If you choose an object type, then you can list checked-out objects in a specific folder or across all folders. If you do not specify an object type, *pmrep* returns all the checked-out objects in the repository.

The FindCheckout command uses the following syntax:

```
findcheckout

[-o <object_type>]

[-f <folder_name>]

[-u (all_users)]

[-c <column_separator>]

[-r <end-of-record_separator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]

[-s <dbd_separator>]
```

The following table describes *pmrep* FindCheckout options and arguments:

Option	Argument	Description
-o	object_type	Object type you want to list. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session config, task, cube, or dimension. If you do not use this option, *pmrep* ignores the -f and -u options and the command returns all checked-out objects in the repository.
-f	folder_name	Optional if you specify an object type. Return a list of checked out objects for the object type in the specified folder. The default is to list objects for the object type across folders.
-u	-	Optional. List the checked out objects by all users. The default is to list checked out objects by the current user.
-c	column_separator	Optional. Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. If you omit this option, *pmrep* uses a single space.
-r	end-of-record_separator	Optional. Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. Default is newline /n.
-l	end-of-listing_indicator	Optional. Character or set of characters used to specify the end of the object list. Use a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a period.
-b	-	Optional. Verbose. Displays more than the minimum information about the objects. If you omit this option, *pmrep* prints a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the version number and folder name. The short format for global objects such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the creator name and creation time.
-y	-	Optional. Displays the database type of sources and targets.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

GetConnectionDetails

Lists the properties and attributes of a connection object as name-value pairs.

To use the GetConnectionDetails command, you need read permission on the connection object.

The GetConnectionDetails command uses the following syntax:

```
getconnectiondetails
-n <connection_name>
-t <connection_type>
```

The following table describes *pmrep* GetConnectionDetails options and arguments:

Option	Argument	Description
-n	connection_name	Required. Name of the connection to list details for.
-t	connection_type	Required. Type of connection. A connection can be one of the following types: - Application - FTP - Loader - Queue - Relational

GenerateAbapProgramToFile

Generates the ABAP program for a mapping with SAP table as the source and saves the program as a file. The GenerateAbapProgramToFile command generates the ABAP program for a mapping in the PowerCenter repository. The generated program is saved as a file. You can use the GenerateAbapProgramToFile command for mappings that use SAP tables as the source.

The naming convention for the file is *mappingname_<version>_<program_mode>.ab4*. You must enclose the path and the file name in double quotes. After you generate the ABAP program and save it to a file, use the InstallAbapProgram command to install it on an SAP system.

The GenerateAbapProgramToFile command uses the following syntax:

```
generateabapprogramtofile
-s <folder_name>
-m <mapping_name>
[-v <version_number>]
[-l <log_filename>]
-u <user_name>
-x <password>
-c <connect_string>
-t <client>
[-y <language>]
-p <program_mode (file, stream)>
-f <output_file_location>
{-e (enable override)
```

```
-o <override_name> }
[-a (authority check)]
[-n (use namespace)]
```

The following table describes pmrep GenerateAbapProgramToFile options and arguments:

Option	Argument	Description
-s	folder_name	Required. The name of the folder that contains the mapping for which the ABAP program needs to be generated.
-m	mapping_name	Required. Name of the mapping.
-v	version_number	Optional. Version number of the mapping. Default is the latest version.
-l	log_filename	Optional. Name of the log file where the information or error messages are written. By default, the log file is created in the directory where you run the command.
-u	user_name	Required. SAP source system connection user name. Must be a user for which you have created a source system connection.
-x	password	Required. Password for the user name. Use the command line program pmpasswd to encrypt the user password.
-c	connect_string	Required. DEST entry defined in the `sapnwrfc.ini` file for a connection to a specific SAP application server or for a connection that uses SAP load balancing.
-t	client	Required. SAP client number.
-y	language	Optional. SAP Logon language. Must be compatible with the PowerCenter Client code page. Default is the language of the SAP system.
-p	program_mode (file, stream)	Required. Mode in which the PowerCenter Integration Service extracts data from the SAP system. Select file or stream.
-f	output_file_location	Required. Location in the local machine where you want to save the ABAP program file.
-e	-	Optional. Overrides the default ABAP program file name.
-o	override_name	Required if you enable override. ABAP program file name.
-a	-	Optional. Adds authority checks to the ABAP program.
-n	-	Optional. Appends a namespace that you registered with SAP to the ABAP program name.

Example

The following example generates an ABAP program and saves it to a file:

```
generateabapprogramtofile -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream -e -o program_name -n -a -f
"C:\<informatica_installation_dir>\ABAP_prog"
```

Help

Returns the syntax for the command you specify. If you do not specify a command, then syntax for all of the *pmrep* commands is displayed.

For the Help command, use one of the following syntax structures:

```
help [command]
-help [command]
```

InstallAbapProgram

Installs an ABAP program in the SAP system. Use the InstallAbapProgram command to generate and install the ABAP program directly onto the SAP system. You can use this command to install an ABAP program from a file onto the SAP system. You can use the InstallAbapProgram command for mappings that use SAP tables as the source.

The InstallAbapProgram command gets the mapping information from the PowerCenter repository for a mapping and generates the ABAP program. The command installs the generated ABAP program in the SAP system. The first time you install the ABAP program onto the SAP system, the command generates a program name. Subsequent installations uses the same program name if you are using the same program mode.

When you install an ABAP program to the SAP system from a file, you must provide the full path and file name of the ABAP program you want to install. Enclose the path and the file name in double quotes. You must provide the folder name and mapping information for which you generated the ABAP program. The InstallAbapProgram command gets the description of the mapping and appends it to the ABAP program when it is installed onto the SAP system.

The InstallAbapProgram command uses the following syntax:

```
installabapprogram

-s <folder_name>

-m <mapping_name>

[-v <version_number>]

[-l <log_filename>]

-u <user_name>

-x <password>

-c <connect_string>

-t <client>

[-y <language>]

{-f <input_file_name> |

-p <program_mode (file, stream)>

{-e (enable override)

-o <override_name> }

[-a (authority check)]
```

```
[-n (use namespace)]}
[-d <development_class_name>]
```

The following table describes pmrep InstallAbapProgram options and arguments:

Option	Argument	Description
-s	folder_name	Required. The name of the folder that contains the mapping for which the ABAP program needs to be generated. If you are installing from a file, the name of the folder that contains the mapping for which you generated the ABAP program.
-m	mapping_name	Required. Name of the mapping. If you are installing from a file, the name of the mapping for which you generated the ABAP program.
-v	version_number	Optional. Version number of the mapping. Default is the latest version. If you are installing from a file, the version of the mapping for which you generated the ABAP program.
-l	log_filename	Optional. Name of the log file where the information or error messages are written. By default, the log file is stored in the directory where you run the command.
-u	user_name	Required. SAP source system connection user name. Must be a user for which you have created a source system connection.
-x	password	Required. Password for the user name. Use the command line program pmpasswd to encrypt the user password.
-c	connect_string	Required. DEST entry defined in the `sapnwrfc.ini` file for a connection to a specific SAP application server or for a connection that uses SAP load balancing.
-t	client	Required. SAP client number.
-y	language	Optional. SAP Logon language. Must be compatible with the PowerCenter Client code page. Default is the language of the SAP system.
-f	input_file_name	Required if you are installing the ABAP program from a file. Name of the ABAP program file from where you want to install the ABAP program into the SAP system.
-p	program_mode (file, stream)	Required if you are generating and installing the ABAP program directly onto the SAP system. Optional if you are installing the ABAP program from a file. Mode in which the PowerCenter Integration Service extracts data from the SAP system. Select file or stream.
-e	-	Optional if you are generating and installing the ABAP program directly onto the SAP system. Overrides the default ABAP program file name.
-o	override_name	Required if you enable override. ABAP program file name.
-a	-	Optional if you are generating and installing the ABAP program directly onto the SAP system. Adds authority checks to the ABAP program.

Option	Argument	Description
-n	-	Optional if you are generating and installing the ABAP program directly onto the SAP system. Appends a namespace that you registered with SAP to the ABAP program name.
-d	development_class_name	Optional. Package or the development class name where the PowerCenter Repository Service installs the ABAP program. Default development class is $TMP.

Examples

The following example installs the ABAP program directly onto the SAP system:

```
installabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -e -o zabc -a -n -d development_class
```

The following example installs the ABAP program from a file onto the SAP system:

```
installabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p file -v 1 -f
"C:\mapping_name_version_file.ab4"
```

KillUserConnection

Terminates user connections to the repository. You can terminate user connections based on the user name or connection ID. You can also terminate all user connections to the repository.

The KillUserConnection command uses the following syntax:

```
killuserconnection

{-i <connection_id> |

-n <user_name> |

-a (kill all)}
```

The following table describes *pmrep* KillUserConnection options and arguments:

Option	Argument	Description
-i	connection_id	Repository connection ID.
-n	user_name	User name.
-a	-	Terminates all connections.

ListConnections

Lists all connection objects in the repository and their respective connection types. A connection can be one of the following types:

- Application
- FTP
- Loader
- Queue
- Relational

The ListConnections command uses the following syntax:

```
listconnections

[-t (output includes connection subtype)]
```

The following table describes the *pmrep* ListConnections option:

Option	Argument	Description
-t	-	Optional. Displays the connection subtype. For example, for a Relational connection, connection subtypes include Oracle, Sybase, and Microsoft SQL Server. You can only view the subtype for connections that you have read permission on.

For more information about connection subtypes, see "Connection Subtypes" on page 1282.

ListObjectDependencies

Lists dependency objects for reusable and non-reusable objects. If you want to list dependencies for non-reusable objects, you must use a persistent input file containing object IDs. You can create this file by running a query and choosing to create a text file.

ListObjectDependencies accepts a persistent input file and it can create a persistent output file. These files are the same format. If you create an output file, use it as input to the ApplyLabel, AddToDeployment Group, or Validate *pmrep* commands.

ListObjectDependencies returns the number of records if the command runs successfully.

The ListObjectDependencies command uses the following syntax:

```
listobjectdependencies

{{-n <object_name>

  -o <object_type>

  [-t <object_subtype>]

  [-v <version_number>]

  [-f <folder_name>] } |

   -i <persistent_input_file>}

[-d <dependency_object_types>]
```

```
[-p <dependency_direction (children, parents, or both)>]
[-s (include pk-fk dependency)]
[-g (across repositories)]
[-u <persistent_output_file_name>
  [-a (append)]]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
[-e <dbd_separator>]
```

The following table describes *pmrep* ListObjectDependencies options and arguments:

Option	Argument	Description
-n	object_name	Required. Name of a specific object to list dependencies for.
-o	object_type	Required. Object type to list dependencies for. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session, session config, task, cube, dimension, query and deploymentgroup.
-t	object_subtype	Type of transformation, task, or query. Ignored for other object types. For more information about valid subtypes, see "Listing Object Types" on page 1330.
-v	version_number	Optional. List dependent objects for an object version other than the latest version. You must use this option only for versioned repositories. It does not apply to non-versioned repositories.
-f	folder_name	Folder containing object name. Folder is required if you do not use the -i option.
-i	persistent_input_file	Optional. Text file of objects generated from ExecuteQuery or Validate commands. You must use this file if you want to list dependencies for non-reusable objects. If you use this option, then you cannot use the -n, -o, -f options to specify objects.
-d	dependency_object_types	Optional. Type of dependent objects to list. You can enter ALL or one or more object types. Default is ALL. If ALL, then *pmrep* lists all supported dependent objects. If you choose one or more objects, then *pmrep* lists dependent objects for these types. To enter multiple object types, separate them by commas without spaces.
-p	dependency_direction	Required if you do not use the -s option. Parents or children dependent objects to list. You can specify parents, children, or both. If you do not use the -p option, *pmrep* does not list parent or child dependencies.

Option	Argument	Description
-s	-	Required if you do not use the -p option. Include the primary key-foreign key dependency object regardless of the direction of the dependency. If you do not use the -s option, *pmrep* does not list primary-key/foreign-key dependencies.
-g	-	Optional. Find object dependencies across repositories.
-u	persistent_output_file_name	Send the dependency result to a text file. Use the text file as input to the ApplyLabel, AddToDeployment Group, or Validate *pmrep* commands. The default sends the query result to stdout. You cannot use the -b and -c options with this option.
-a	-	Append the result to the persistent output file instead of overwriting it.
-c	column_separator	Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. You cannot use this option with the -u option. If you omit this option, *pmrep* uses a single space.
-r	end-of-record_ separator	Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. Default is newline /n.
-l	end-of-listing_indicator	Character or set of characters used to specify the end of the object list. Enter a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a period.
-b	-	Verbose. Displays more than the minimum information about the objects. If you omit this option, *pmrep* displays a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the version number and folder name. The short format for global objects, such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the creator name and creation time. You cannot use this option with the -u option.
-y	-	Optional. Displays the database type of sources and targets.
-e	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

ListObjects

Returns a list of objects in the repository. When you list objects, *pmrep* returns object metadata. Use the following list operations:

- **List object types**. Define the objects you want to list.
- **List folders**. List all the folders in the repository.
- **List objects**. List reusable and non-reusable objects in the repository or in a folder.

Use ListObjects in a shell script to return the object metadata, parse the metadata, and then use the parsed data in another *pmrep* command.

For example, use ListObjects to list all Sequence Generator transformations in the repository. Create a shell script that uses ListObjects to return Sequence Generator transformation information, parse the data ListObjects returns, and use UpdateSeqGenVals to update the sequence values.

pmrep returns each object in a record and returns the metadata of each object in a column. It separates records by a new line by default. You can enter the characters to use to separate records and columns. You can also enter the characters to indicate the end of the listing.

Tip: When you enter characters to separate records and columns and to indicate the end of the listing, use characters that are not used in repository object names. This helps you use a shell script to parse the object metadata.

The ListObjects command uses the following syntax:

```
listobjects

-o <object_type>

[-t <object_subtype>]

[-f <folder_name>]

[-c <column_separator>]

[-r <end-of-record_indicator>]

[-l <end-of-listing_indicator>]

[-b (verbose)]

[-y (print database type)]

[-s <dbd_separator>]
```

The following table describes *pmrep* ListObjects options and arguments:

Option	Argument	Description
-o	object_type	Required. Type of object to list. - When you enter folder, you do not need to include any other option. *pmrep* ignores the -t and -f options. - When you enter objects other than folders, you must include the -f option. - When you enter transformation or task, you must include the -f option, and you can optionally include the -t option. For more information about object types to use with ListObjects, see "Listing Object Types" on page 1330.
-t	object_subtype	Optional. Type of transformation or task to list. When you enter transformation or task for the object type, you can include this option to return a specific type. For more information about object types to use with ListObjects, see "Listing Object Types" on page 1330.
-f	folder_name	Required if you list objects other than folders. Folder to search. Use this option for all object types except deployment group, folder, label, and query.
-c	column_separator	Optional. Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. If you omit this option, *pmrep* uses a single space.
-r	end-of-record_indicator	Optional. Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. Default is newline /n.
-l	end_of_listing_indicator	Optional. Character or set of characters used to specify the end of the object list. Enter a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a period.
-b	-	Optional. Verbose. Display more than the minimum information about the objects. If you omit this option, you display a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the object status, version number, and checked out information. The short format for global objects, such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the label type, query type, deployment group type, creator name, and creation time.
-y	-	Optional. Displays the database type of sources and targets.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

Listing Object Types

Use the object_type option to define the objects you want to list. The command lists the latest versions or checked out versions of objects, including shortcuts, but excluding objects according to the rules for object types.

The following table describes the object types and rules you use with ListObjects:

Object Type	Rule
Deploymentgroup	List deployment groups in the repository.
Folder	List folders in the repository.
Label	List labels in the repository.
Mapplet	List mapplets with latest or checked out version in a folder, including shortcuts but excluding instances of reusable mapplets.
Mapping	List mappings with latest or checked out version in a folder, including shortcuts but excluding instances of reusable mapplets.
Query	List queries in the repository.
Scheduler	List reusable and non-reusable schedulers with latest or checked out version in a folder.
Session	List reusable and non-reusable sessions with latest or checked out version in a folder, excluding instances of reusable sessions.
Sessionconfig	List the session configurations with latest or checked out version in a folder.
Source	List sources with latest or checked out version in a folder, including shortcuts but excluding source instances.
Target	List targets with latest or checked out version in a folder, including shortcuts but excluding target instances.
Task	List reusable and non-reusable tasks with latest or checked out version in a folder.
Transformation	List reusable and non-reusable transformations with latest or checked out version in a folder, including shortcuts and excluding instances of reusable transformations.
“User Defined Function”	List user-defined functions in the repository.
Workflow	List the workflows with latest version or checked out version in a folder.
Worklet	List reusable and non-reusable worklets with latest version or checked out version in a folder, excluding instances of reusable worklets.

The following table describes the object types and values to use with *pmrep* commands:

Object Type	Subtype Value	Description
Query	personal	Personal
Query	shared	Shared
Task	assignment	Assignment
Task	command	Command
Task	control	Control
Task	decision	Decision
Task	email	Email
Task	event_raise	Event-raise
Task	event_wait	Event-wait
Task	start	Start
Task	timer	Timer
Transformation	aggregator	Aggregator
Transformation	application_source_qualifier	Application Source Qualifier
Transformation	app_multi-group_source_qualifier	Application Multi-Group Source Qualifier
Transformation	custom_transformation	Custom
Transformation	custom_transformation	HTTP
Transformation	custom_transformation	SQL
Transformation	custom_transformation	Union
Transformation	custom_transformation	XML Generator
Transformation	custom_transformation	XML Parser
Transformation	expression	Expression
Transformation	external_procedure	External Procedure
Transformation	filter	Filter
Transformation	input_transformation	Input
Transformation	java	Java
Transformation	joiner	Joiner
Transformation	lookup_procedure	Lookup

Object Type	Subtype Value	Description
Transformation	mq_source_qualifier	MQ Source Qualifier
Transformation	normalizer	Normalizer
Transformation	output_transformation	Output
Transformation	rank	Rank
Transformation	router	Router
Transformation	sequence	Sequence Generator
Transformation	sorter	Sorter
Transformation	source_qualifier	Source Qualifier
Transformation	stored_procedure	Stored Procedure
Transformation	transaction_control	Transaction Control
Transformation	update_strategy	Update Strategy
Transformation	xml_source_qualifier	XML Source Qualifier

Listing Folders

Use ListObjects to return each folder in the repository. When you enter `folder` for the object type, *pmrep* ignores the subtype and folder name.

For example, to list all folders in the repository, use the following syntax:

```
listobjects -o folder
```

Alternatively, you can enter a different column separator and end of listing indicator:

```
ListObjects -o folder -c "**" -l #
```

Listing Objects

Use ListObjects to list reusable and non-reusable objects in the repository or in a folder. *pmrep* does not include instances of reusable objects. When you list objects, you must include the folder name for all objects that are associated with a folder.

pmrep returns the name of the object with the path when applicable. For example, when a transformation is in a mapping or mapplet, *pmrep* returns *mapping_name.transformation_name* or *mapplet_name.transformation_name*.

For more information about a list of transformation or task return values, see "Listing Object Types" on page 1330.

For example, to list all transformation types in a folder, enter the following text at the prompt:

```
listobjects -o transformation -f myfolder
```

pmrep returns the following information:

```
stored_procedure reusable sp_sproc1
expression reusable exp1
stored_procedure non-reusable mapping1.sp_nsproc
sequence non-reusable smallmapplet.seqgen_empid
.listobjects completed successfully.
```

To list all Stored Procedure transformations in a folder, enter the following text at the prompt:

```
listobjects -o transformation -t stored_procedure -f myfolder
```

pmrep returns the following information:

```
stored_procedure reusable sp_sproc1
stored_procedure non-reusable mapping1.sp_nsproc
.listobjects completed successfully.
```

To list all sessions in a folder, enter the following text at the prompt:

```
listobjects -o session -f myfolder
```

pmrep returns the following information:

```
session reusable s_sales_by_CUSTID
session non-reusable wf_sales.s_sales_Q3
session non-reusable wf_orders.wl_shirt_orders.s_shirt_orders
.listobjects completed successfully.
```

ListTablesBySess

Returns a list of sources or targets used in a session. When you list sources or targets, *pmrep* returns source or target instance names to the window. Use ListTablesBySess in a shell script with other *pmrep* commands. For example, you can create a shell script that uses ListTablesBySess to return source instance names and uses Updatesrcprefix to update the source owner name.

When you use ListTablesBySess, *pmrep* returns source and target instance names as they appear in the session properties. For example, if the mapping contains a mapplet with a source, *pmrep* returns the source instance name in the following format:

```
mapplet_name.source_name
```

The ListTablesBySess command uses the following syntax:

```
listtablesbysess

-f <folder_name>

-s [<qualifying_path>.]<session_name>

-t <object_type_listed> (source or target)
```

The following table describes *pmrep* ListTablesBySess options and arguments:

Option	Argument	Description
-f	folder_name	Required. Name of the folder containing the session.
-s	session_name	Required. Name of the session containing the sources or targets. You can enter a reusable or non-reusable session name. However, you cannot enter an instance of a reusable session name. To enter a non-reusable session name in a workflow, enter the workflow name and the session name as *workflow_name.session_name*.
-t	object_type_listed	Required. Enter source to list sources, or enter target to list targets.

For example, to list all sources in a reusable session, enter the following text at the prompt:

```
listtablesbysess -f myfolder -s s_reus_sess1 -t source
```

pmrep returns the following information:

```
ITEMS
mapplet1.ORDERS
Shortcut_To_ITEM_ID
listtablesbysess completed successfully.
```

When the mapping contains a mapplet with a source, *pmrep* includes the mapplet name with the source, such as mapplet1.ORDERS.

For example, you can list all targets in a non-reusable session in a workflow:

```
listtablesbysess -f myfolder -s wf_workkflow1.s_nrsess1 -t target
```

pmrep returns the following information:

```
target1_inst
ORDERS_BY_CUSTID
Shortcut_To_tgt2_inst
listtablesbysess completed successfully.
```

ListUserConnections

Lists information for each user connected to the repository.

The ListUserConnections command uses the following syntax:

```
listuserconnections
```

MassUpdate

Updates session properties for a set of sessions that meet specified conditions. You can update all sessions in a folder or a list of sessions. To update a list of sessions, create a persistent input file. The list can contain a specific list of sessions, or it can contain conditions such as a name pattern or a property value. Use ExecuteQuery to generate a persistent input file.

When you run MassUpdate, you can view information such as the folder name, the number of sessions that are successfully updated or failed, and the names of the sessions that are updated. You can view the status

of the update in the command line window or in a log file that the command generates. You specify the name and path for the log file when you run the command. By default, the log file is stored in the directory where you run the command.

Use MassUpdate to update a session property across multiple sessions when a PowerCenter version changes a default value.

Note: You cannot update dependent session properties.

Before you update the sessions, you can also run MassUpdate in a test mode to view changes. To view a sample log file, see "Sample Log File" on page 1340.

The MassUpdate command uses the following syntax:

```
pmrep massupdate

-t <session_property_type (session_property, session_config_property,
transformation_instance_attribute, session_instance_runtime_option)>

-n <session_property_name>

-v <session_property_value>

[-w <transformation_type>]

{-i <persistent_input_file> | -f <folder_name> }

[-o <condition_operator (equal, unequal, less, greater)>]

[-l <condition_value>]

[-g <update_session_instance_flag>]

[-m <test_mode>]

[-u <output_log_file_name>]
```

The following table describes *pmrep* MassUpdate options and arguments:

Option	Argument	Description
-t	session_property_type	Required. Session property type to update. Session properties are of the following types: - session_property - session_config_property - transformation_instance_attribute - session_instance_runtime_option
-n	session_property_name	Required. Name of the attribute or property to update.
-v	session_property_value	Required. Value that you want to assign to the property followed by a semicolon. For example, to assign a value to the property, use the following syntax: `-v "IgnoreNULLInExpressionComparison=Yes;"` **Note:** Enclose the session property value in double quotes.
-w	transformation_type	Required if you update a transformation instance attribute. Transformation type to update. You can update the following transformation types: aggregator, joiner, lookup procedure, rank, sorter, source definition, and target definition.

Option	Argument	Description
-i	persistent_input_file	Required if you do not use the -f option. Name of the file that contains the selected list of sessions to update. You can use the *pmrep* ExecuteQuery command to run a query and generate this file. MassUpdate returns an error if you specify an object that is not a session. You must use the -i option or the -f option, but not both.
-f	folder_name	Required if you do not use the -i option. Name of the folder. Use to update all sessions in a folder. You must use the -i option or the -f option, but not both.
-o	condition_operator	Required if you use condition_value. Part of the condition that defines the session set. The attribute of a session or session instance is updated when the condition is met. You can use the following condition operators to update a string: equal or unequal. You can use the following condition operators to update an integer: equal, unequal, less, or greater.
-l	condition_value	Required if you use a condition operator. Part of the condition. The condition appears as follows: <session_property_value> <condition operator> <condition_value>
-g	update_session_instance_flag	Required if you update a session instance run-time option. Optional for the following session property types: session property, session configuration attribute, and transformation instance attribute. Updates session instances. You can update an attribute in a session instance if the session instance overrides the attribute.
-m	test_mode	Optional. Runs MassUpdate in test mode. View sessions that will be impacted by the command before you commit changes. You can see the following details in the command line window: - Session name - Type of session: reusable or non-reusable - Current value of the session property - Sessions for which the attribute has the same value and are not affected by the command.
-u	output_log_file_name	Optional. Name of the log file that stores the status of the update and basic information about the sessions or session instances. Previous attribute values are also written to this file. If you do not use this option, the details appear in the command line window.

The MassUpdate command returns “massupdate successfully completed” or returns “failed to execute massupdate” message. The update might fail for the following reasons:

- You did not specify a valid attribute value pertaining to the attribute name.
- You specified the correct session property name and the wrong session property type along with it.
- You did not specify the -v option that ends with a semicolon while updating a session property value.
- You did not specify the -w option while updating a transformation instance attribute.
- You did not specify the -g option while updating a session instance run-time option.

- You do not have the Repository Services Administrator role.

Session Property Types

When you run MassUpdate, specify the session property type and the name. You specify the following session property types:

- Session properties
- Session configuration attributes
- Transformation instance attributes
- Session instance run time options

Note: You must enclose the session property in quotes.

The following table lists the session properties that you can update and the session property types:

Session Property	Session Property Type
$Source connection value	session_property
$Target connection value	session_property
Additional Concurrent Pipelines for Lookup Cache Creation	session_config_property
Aggregator Data Cache Size	transformation_instance_attribute The transformation_type argument must be aggregator.
Aggregator Index Cache Size	transformation_instance_attribute The transformation_type argument must be aggregator.
Allow Temporary Sequence for Pushdown	session_property
Allow Temporary View for Pushdown	session_property
Cache Directory	transformation_instance_attribute The transformation_type argument must be aggregator, joiner, or rank.
Cache LOOKUP( ) function	session_config_property
Collect performance data	session_property
Commit Interval	session_property
Commit Type	session_property
Constraint based load ordering	session_config_property
Custom Properties	session_config_property
DateTime Format String	session_config_property
Default buffer block size	session_config_property

Session Property	Session Property Type
Disable this task	session_instance_runtime_option
DTM buffer size	session_property
Enable high precision	session_property
Enable Test Load	session_property
Fail parent if this task does not run	session_instance_runtime_option
Fail parent if this task fails	session_instance_runtime_option
Incremental Aggregation	session_property
Is Enabled	session_config_property
Java Classpath	session_property
Joiner Data Cache Size	transformation_instance_attribute The transformation_type argument must be joiner.
Joiner Index Cache Size	transformation_instance_attribute The transformation_type argument must be joiner.
Line Sequential buffer length	session_config_property
Lookup cache directory name	transformation_instance_attribute The transformation_type argument must be lookup procedure.
Lookup Data Cache Size	transformation_instance_attribute The transformation_type argument must be lookup procedure.
Lookup Index Cache Size	transformation_instance_attribute The transformation_type argument must be lookup procedure.
Maximum Memory Allowed For Auto Memory Attributes	session_config_property
Maximum Percentage of Total Memory Allowed For Auto Memory Attributes	session_config_property
On Pre-Post SQL error	session_config_property
On Pre-session command task error	session_config_property
On Stored Procedure error	session_config_property
Output file directory	transformation_instance_attribute The transformation_type argument must be target definition.
Override tracing	session_config_property
Parameter Filename	session_property

Session Property	Session Property Type
Pre 85 Timestamp Compatibility	session_config_property
Pre-build lookup cache	session_config_property
Pushdown Optimization	session_property
Rank Data Cache Size	transformation_instance_attribute The transformation_type argument must be rank.
Rank Index Cache Size	transformation_instance_attribute The transformation_type argument must be rank.
Recovery Strategy	session_property
Reject file directory	transformation_instance_attribute The transformation_type argument must be target definition.
Rollback Transactions on Errors	session_property
Save session log by	session_config_property
Session Log File directory	session_property
Session retry on deadlock	session_property
Session Sort Order	session_property When the Integration Service runs in Unicode mode, you can choose the sort order to sort character data in the session. You can configure the following values for the sort order: - 0. BINARY - 2. SPANISH - 3. TRADITIONAL_SPANISH - 4. DANISH - 5. SWEDISH - 6. FINNISH
Sorter Cache Size	transformation_instance_attribute The transformation_type argument must be sorter.
Source file directory	transformation_instance_attribute The transformation_type argument must be source definition.
Stop on errors	session_config_property
Treat source rows as	session_property
Treat the input link as AND	session_instance_runtime_option
Write Backward Compatible Session Log File	session_property

Rules and Guidelines for MassUpdate

Use the following rules and guidelines when you run MassUpdate:

- If the node running the Repository Service process has limited memory, disable repository agent caching before you run MassUpdate or restart the Repository Service after you run MassUpdate.
- You can update reusable and non-reusable sessions.
- You can update the value of any supported session or session config property whether or not it is overridden.
- You cannot revert property values after you run MassUpdate.
- You cannot update sessions that are checked out.
- You cannot update sessions in frozen folders.

Sample Log File

The following text shows a sample log file generated by *pmrep* MassUpdate:

```
cases_auto,s_test_ff,reusable,0
s_test_ff was successfully checked out.

------------------------------------------------------------------------------
11/10/2008 11:12:55 ** Saving... Repository test_ver_MU, Folder cases_auto
------------------------------------------------------------------------------
Session s_test_ff updated.
Checking-in saved objects...done
------------------------------------------------------------------------------

cases_auto,wf_non_reusable_test_ff.s_test_ff_non_reusable,non-reusable,0
wf_non_reusable_test_ff was successfully checked out.

------------------------------------------------------------------------------
11/10/2008 11:12:57 ** Saving... Repository test_ver_MU, Folder cases_auto
------------------------------------------------------------------------------
Validating the flow semantics of Workflow wf_non_reusable_test_ff...
...flow semantics validation completed with no errors.

Validating tasks of Workflow wf_non_reusable_test_ff...
...Workflow wf_non_reusable_test_ff tasks validation completed with no errors.

Workflow wf_non_reusable_test_ff updated.
Checking-in saved objects...done
------------------------------------------------------------------------------

Massupdate Summary:
Number of reusable sessions that are successfully updated: 1.
Number of non-reusable sessions that are successfully updated: 1.
Number of session instances that are successfully updated: 0.
Number of reusable sessions that fail to be updated: 0.
Number of non-reusable sessions that fail to be updated: 0.
Number of session instances that fail to be updated: 0.
------------------------------------------------------------------------------
```

ModifyFolder

Modifies folder properties. You modify a folder in a non-versioned repository.

The command returns “ModifyFolder successfully completed” or returns “ModifyFolder Failed” message. The modification might fail for the following reasons:

- The folder does not exist.
- The new owner does not exist or does not belong to the group.
- A folder with the new folder name already exists.

The ModifyFolder command uses the following syntax:

```
modifyFolder
-n <folder_name>
[-d <folder_description>]
[-o <owner_name>]
[-a <owner_security_domain>]
[-s (shared folder)]
[-p <permissions>]
[-r <new_folder_name>]
[-f <folder_status> (active, frozendeploy, or frozennodeploy)]
[-u <os_profile>]
```

The following table describes the *pmrepModifyFolder* options and arguments:

Option	Argument	Description
-n	folder_name	Required. New folder name.
-d	folder_description	Optional. Description of the folder that displays in the Repository Manager.
-o	owner_name	Optional. Current owner of the folder. Any user in the repository can be the folder owner. Default owner is the current user.
-a	owner_security_domain	Required if you use LDAP authentication. Name of the security domain that the owner belongs to. Default is Native.
-s	shared_folder	Optional. Makes the folder shared.
-p	permissions	Optional. Access rights for the folder. If omitted, the Repository Service uses existing permissions.
-r	new_folder_name	Optional. New name of the folder.

Option	Argument	Description
-f	folder_status	Optional. Change the folder status to one of the following status: - active. This status allows users to check out versioned objects in the folder. - frozendeploy (Frozen, Allow Deploy to Replace). This status prevents users from checking out objects in the folder. Deployment into the folder creates new versions of the objects. - frozennodeploy (Frozen, Do Not Allow Deploy to Replace). This status prevents users from checking out objects in the folder. You cannot deploy objects into this folder.
-u	os_profile	Optional. Assigns an operating system profile to the folder.

Notify

Sends notification messages to users connected to a repository or users connected to all repositories managed by a Repository Service.

The Notify command uses the following syntax:

```
notify

-m <message>
```

The following table describes *pmrep* Notify option and argument:

Option	Argument	Description
-m	message	Required. Message you want to send.

The command returns “notify successfully completed” or returns “failed to execute notify” message. The notification might fail for the following reasons:

- The message you entered is invalid.
- You failed to connect to the Repository Service.
- The Repository Service failed to notify users.

ObjectExport

Exports objects to an XML file defined by the powrmart.dtd file. You export an object by name. If you enter an object, you must enter the name of the folder that contains it. If you do not enter a version number, you export the latest version of the object.

Use a persistent input file to specify different objects to export at one time. You can create this file by using the ExecuteQuery, Validate, or ListObjectDependencies *pmrep* commands. If you use the persistent input file, do not use the other parameters to specify objects.

If you export a mapping, by default PowerCenter exports the mapping and its instances. If you want to include dependent objects, you must add the appropriate *pmrep* options. You can optionally include reusable and non-reusable dependent objects, objects referenced by shortcuts, and related objects in a primary key-foreign key relationship.

To export mapping dependencies, you must use the -b and -r options.

The ObjectExport command uses the following syntax:

```
objectexport
{{-n <object_name>
 -o <object_type>
 [-t <object_subtype>]
 [-v <version_number>]
 [-f <folder_name>]} |
 -i <persistent_input_file>}
[-m (export pk-fk dependency)]
[-s (export objects referred by shortcut)]
[-b (export non-reusable dependents)]
[-r (export reusable dependents)]
-u <xml_output_file_name>
[-l <log_file_name>]
[-e dbd_separator]
```

The following table describes *pmrep* ObjectExport options and arguments:

Option	Argument	Description
-n	object_name	Required if you do not use the -i option. Name of a specific object to export. If you do not enter this option, *pmrep* exports all the latest or checked out objects in the folder. Use the -n option or the -i option, but not both.
-o	object_type	Object type of the object name. You can specify source, target, transformation, mapping, mapplet, session, worklet, workflow, scheduler, session config, or task. If you use this option, you cannot use the -i option.
-t	object_subtype	Type of transformation or task. This argument is ignored for other object types. For more information about valid subtypes, see "Listing Object Types" on page 1330.
-v	version_number	Optional. Exports the version of the object that you enter.
-f	folder_name	Name of the folder containing the object to export. If you do not enter an object name, *pmrep* exports all the objects in this folder. If you use this option, you cannot use the -i option.
-i	persistent_input_file	Required if you do not use the -n option. Text file list of objects generated from ExecuteQuery, Validate, or ListObjectDependencies. It contains object records with encoded IDs. If you use this parameter, you cannot use the -n, -o, or -f options.

Option	Argument	Description
-m	-	Required to export dependent objects. Exports primary key table definitions when you export sources or targets with foreign keys.
-s	-	Required to export dependent objects. Exports the original object referenced by the shortcut.
-b	-	Required to export dependent objects. Exports non-reusable objects used by the object.
-r	-	Required to export dependent objects. Exports reusable objects used by the object.
-u	xml_output_file_name	Required. Name of the XML file to contain the object information.
-l	log_file_name	Optional. Log file that records each export step. If you omit this option, status messages output to the window.
-e	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

Examples

The following example exports a mapping named “map,” which is located in folder1, to a file named map.xml:

```
objectexport  -n map -o mapping -f folder1 -u map.xml
```

The following example exports the objects identified in a persistent input file named persistent_input.xml to a file named map.xml:

```
objectexport  -i persistent_input.txt -u map.xml
```

Note: If you use a manually created persistent input file, since you enter “none” for the encoded ID, the following message appears: Ids are invalid. Trying with names for [none,folder1,map,mapping,none,1].

ObjectImport

Imports objects from an .xml file. This command requires a control file to specify the objects to import and how to resolve conflicts. The control file is an .xml file defined by the impcntl.dtd file.

The ObjectImport command uses the following syntax:

```
objectimport

-i <input_xml_file_name>

-c <control_file_name>

[-l <log_file_name>]

[-p (retain persistent value)]
```

The following table describes *pmrep* ObjectImport options and arguments:

Option	Argument	Description
-i	input_XML_file_name	Required. Name of the .xml file to import.
-c	control_file_name	Required. Name of the control file that defines import options.
-l	log_file_name	Optional. Log file that records each export step. If you omit this option, status messages output to the window.
-p	-	Optional. Retains persistent values for mapping variables.

Note: The ObjectImport command does not create a folder if the folder name you enter does not exist in the repository.

You can generate audit logs when you import an .xml file into the PowerCenter repository with the pmrep ObjectImport command. When you import one or more repository objects, you can generate audit logs. To include security audit trails in the user activity log events, enable the SecurityAuditTrail property for the PowerCenter Repository Service in the Administrator tool before you import an .xml file. The user activity logs captures all the audit messages.

The audit logs contain the following information about the .xml file imported:

- Host name and IP address of the client machine from which the .xml file was imported
- Full local path of the .xml import file
- The file name
- The file size in bytes
- Logged in user name
- Number of objects imported
- Time stamp of the import operation

PurgeVersion

Purges object versions from the repository database. You can purge versions of deleted objects and active objects. An object is a deleted object if the latest version is checked in and it has the version status Deleted. Other objects are active objects.

When you purge versions of deleted objects, you purge all versions. The deleted objects must be checked in. You can purge versions for all deleted objects or for objects deleted before a specified end time. You can specify the end time as a date and time, a date only, or a number of days before the current date.

When you purge versions of active objects, you can specify purge criteria. You can specify the number of versions to keep and purge the previous versions, and you can purge versions that are older than a specified purge cutoff time. You cannot purge a checked-out version or the latest checked-in version.

If you purge versions of a composite object, consider which versions of the dependent objects are purged.

You can use the -k option to display the objects that do not purge and the reason object versions do not purge. For example, you might not have permission to purge an object version. You cannot purge object versions that are part of a deployment group.

The PurgeVersion command uses the following syntax:

```
purgeversion
{-d <all | time_date | num_day> |
{-n <last_n_versions_to_keep> |
 -t <time_date | num_day>}}
[-f <folder_name>]
[-q <query_name>]
[-o <output_file_name>]
[-p (preview purged objects only)]
[-b (verbose)]
[-c (check deployment group reference)]
[-s dbd_separator]
[-k (log objects not purged)]
```

The following table describes *pmrep* PurgeVersion options and arguments:

Option	Argument	Description
-d	all time_date num_day	Required if you do not use -n or -t. Purges all versions of checked-in deleted objects. You can specify `all` for all deleted objects, or you can specify an end time to purge all versions of objects that were deleted before the end time. You specify the end time in MM/DD/YYYY HH24:MI:SS format, MM/DD/YYYY format, or as the number of days before the current date. If you specify a number of days, the value must be an integer greater than 0.
-n	last_n_versions_to_keep	Required if you do not use -d or -t. Number of latest checked-in object versions to keep for an active object. The value must be an integer greater than 0. For example, enter 6 to purge all versions except the last six checked-in versions. If the object is checked out, you also retain the checked-out version. **Note:** After you purge object versions, you cannot retrieve them. To ensure that you can revert to past versions, avoid purging all versions of an object.
-t	purge_cutoff_time	Required if you do not use -d or -n. Cutoff time for purging object versions of active objects. Purges versions that were checked in before the cutoff time. You can specify the purge cutoff time in MM/DD/YYYY HH24:MI:SS format, MM/DD/YYYY format, or as a number of days before the current date. If you specify a number of days, the value must be an integer greater than 0. When you use the -t option, you retain the latest checked-in version even if it was checked in after the purge cutoff time.
-f	folder_name	Optional. Folder from which object versions are purged. If you do not specify a folder, you purge object versions from all folders in the repository.
-q	query_name	Optional. Query used to purge object versions from a particular query result set. **Note:** If you use the -d option, you purge all versions of the deleted objects. To keep recent versions of deleted objects and purge older versions, you can define a query that returns the deleted objects and then use the -q option with -n, -t, or both.
-o	outputfile_name	Optional. Output file for saving information about purged object versions.
-p	-	Optional. Previews the PurgeVersion command. *pmrep* displays the purge results without actually purging object versions.

Option	Argument	Description
-b	-	Optional. Displays or saves purge information in verbose mode. Verbose mode provides detailed information about object versions, including repository name, folder name, version number, and status. You can use the -b option with -o and -p.
-c	-	Optional. Checks deployment groups in the repository for references to the object versions returned in a purge preview. If a purge preview contains an object version in a deployment group, *pmrep* displays a warning. When you use the -c option with the -p option, the command lists objects that purge, then lists which object versions are contained in deployment groups. When you use the -c option without the -p option, the command does not purge object versions that are part of deployment groups. **Note:** The -c option can have a negative impact on performance.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).
-k	-	Optional. Lists all the object names and versions that do not purge although they match the purge criteria. The -k option also lists the reason that the object versions do not purge. For example, an object version does not purge if you do not have sufficient privileges to purge the object. **Note:** An object version does not purge when it belongs to a deployment group. When an object is a member of more than one deployment group, the reason lists the first deployment group that causes the object not to purge.

Examples

The following example purges all versions of all deleted objects in the repository:

```
pmrep purgeversion -d all
```

Note: For optimal performance, purge at the folder level or use purge criteria to reduce the number of purged object versions. Avoid purging all deleted objects or all older versions at the repository level.

The following example purges all but the latest checked-in version of objects in the folder1 folder:

```
pmrep purgeversion -n 1 -f folder1
```

The following example previews a purge of all object versions that were checked in before noon on January 5, 2005, and outputs the results to the file named purge_output.txt:

```
pmrep purgeversion -t '01/05/2005 12:00:00' -o purge_output.txt -p
```

Register

Registers a local repository with a connected global repository. You must connect to the global repository before you register the local repository.

Also, you must run the Repository Service for the local repository in exclusive mode. You can configure the Repository Service to run in exclusive mode in the Administrator tool or you can use the *infacmd* UpdateRepositoryService command.

The command returns “register successfully completed” or returns “failed to execute register” message. The registration might fail for the following reasons:

- You failed to connect to the Repository Service.
- The local repository is not running in exclusive mode.
- The Repository Service failed to initialize information about the global repository.
- The Repository Service failed to register the local repository with the global repository.

The Register command uses the following syntax:

```
register
-r <local_repository_name>
-n <local_repository_user_name>
[-s <local_repository_user_security_domain>]
[-x <local_repository_password> |
-X <local_repository_password_environment_variable>]
[-d <local_repository_domain_name> |
{-h <local_repository_portal_host_name>
-o <local_repository_portal_port_number>}] (if local repository is in a different domain)
```

The following table describes *pmrep* Register options and arguments:

Option	Argument	Description
-r	local_repository_name	Required. Name of the local repository to register.
-n	local_repository_user_name	Required. Local user name.
-s	local_repository_user_security_ domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.
-x	local_repository_password	Optional. Login password for the local target repository. You use the -x or -X option, but not both. If you do not use the -x or -X option, *pmrep* prompts you for the password.
-X	repository_password_ environment_variable	Optional. Login password environment variable for the local target repository. You use the -x or -X option, but not both. If you do not use the -x or -X option, *pmrep* prompts you for the password.
-d	local_repository_domain_name	Required if the local repository is in a different domain and you do not use the -h and -o options. Name of the Informatica domain for the repository.

Option	Argument	Description
-h	local_repository_portal_host_name	Required if the local repository is in a different domain and you do not use -d. Machine name of the domain where the local repository is located. If you use this option, you must also use the -o option.
-o	local_repository_portal_port_number	Required if the local repository is in a different domain and you do not use -d. Port number for the domain where the local repository is located. If you use this option, you must also use the -h option.

RegisterPlugin

Registers an external plug-in to a repository. Registering a plug-in adds its functionality to the repository. Use the RegisterPlugin command to update existing plug-ins.

When you use this command, the Repository Service must be running in exclusive mode. You can configure the Repository Service to run in exclusive mode in the Administrator tool or you can use the *infacmd* UpdateRepositoryService command.

The RegisterPlugin command uses the following syntax:

```
registerplugin
-i <input_registration_file_name_or_path>
[-e (update plug-in)]
[-l <NIS_login>
  {-w <NIS_password> |
  -W <NIS_password_environment_variable>}
  [-k (CRC check on security library)]]
[-N (is native plug-in)]
```

The following table describes *pmrep* RegisterPlugin options and arguments:

Option	Argument	Description
-i	input_registration_file_name_or_path	Required. Name or path of the registration file for the plug-in.
-e	-	Optional. Update an existing plug-in. Not applicable for authentication modules.
-l	NIS login	Optional. Registers security module components. Provide the NIS login of the user registering an external security module. If the plug-in contains an authentication module, you must supply the external login name, or the registration fails. This login becomes the administrator user name in the repository. Do not use this option for other plug-ins.

Option	Argument	Description
-w	NIS password	Optional. Use to register authentication module components. External directory password of the user registering the module. If the plug-in contains an authentication module, you must supply the user password from the external directory or the registration fails. Do not use this option for other plug-ins. Use the -w or -W option, but not both. If you do not supply a password or password environment variable, *pmrep* prompts you for a password.
-W	NIS_password_environment_variable	Optional. Use to register authentication module components. External directory password environment variable of the user registering the module. If the plug-in contains an authentication module you must supply the user password from the external directory or the registration fails. Do not use this option for other plug-ins. Use the -w or -W option, but not both. If you do not supply a password or password environment variable, *pmrep* prompts you for a password.
-k	-	Optional. Stores the CRC of the plug-in library in the repository. When the Repository Service loads the module, it checks the library against the CRC.
-N	-	Registers a plug-in. Required when the following conditions are true: - You upgrade PowerCenter. - The PowerCenter upgrade does not have a new repository version. - The plug-in contains updated functionality. - The plug-in is registered by default with a new PowerCenter installation.

Registering a Security Module

If you want to use an external directory service to maintain users and passwords for a repository, you must register the security module with the repository. Use the Registerplugin command to register the security plug-in.

Example

You administer PowerCenter for an organization that has a centralized LDAP NIS for user authentication. When you upgrade PowerCenter, you decide to use the LDAP for user authentication. The upgrade installs the LDAP security module in the repository security folder. After connecting to the repository with the Connect command, the administrator runs the *pmrep* command to register the new external module with the repository:

```
pmrep registerplugin -i security/ldap_authen.xml -l adminuser -w admnpass
```

The -l login name and -w login password options contain the valid NIS login information for the user running the *pmrep* command. After registration, you must use this login name and password to access the repository.

Note: The login name and password must be valid in the external directory, or the administrator cannot access the repository using LDAP.

The -i option contains the XML file name that describes the security module.

Restore

Restores a repository backup file to a database. The target database must be empty.

The *pmrep* Restore command uses the following syntax:

```
restore
-u <domain_user_name>
[-s <domain_user_security_domain>]
[-p <domain_password> |
 -P <domain_password_environment_variable>]
-i <input_file_name>
[-g (create global repository)]
[-y (enable object versioning)]
[-b (skip workflow and session logs)]
[-j (skip deployment group history)]
[-q (skip MX data)]
[-f (skip task statistics)]
[-a (as new repository)]
[-e (exit if domain name in the binary file is different from current domain name)]
```

The following table describes *pmrep* Restore options and arguments:

Option	Argument	Description
-u	domain_user_name	Required. User name.
-s	domain_user_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.
-p	domain_password	Optional. Password. You can use the -p or -P option, but not both. If you do not use the -p or -P option, *pmrep* prompts you for the password.
-P	domain_password_ environment_variable	Optional. Password environment variable. You can use the -p or -P option, but not both. If you do not use the -p or -P option, *pmrep* prompts you for the password.
-i	input_file_name	Required. Name of the repository backup file. Use a file name and path local to the Repository Service.
-g	-	Optional. Promotes the repository to a global repository.
-y	-	Optional. Enables object versioning for the repository.

Option	Argument	Description
-b	-	Optional. Skips tables related to workflow and session logs during restore.
-j	-	Optional. Skips deployment group history during restore.
-q	-	Optional. Skips tables related to MX data during restore.
-f	-	Optional. Skips task statistics during restore.
-a	-	Optional. Creates new internal folder IDs for folders in the restored repository. This enables you to copy folders and deployment groups between the original repository and the restored repository. If you do not use -a, you cannot copy folders and deployment groups between the original and restored repositories.
-e	-	Optional. Exits if domain name in the binary file is different from current domain name

Example

The following example restores a repository as a versioned repository and specifies the administrator user name and password to retain the LDAP security module registration:

```
restore -u administrator -p password -i repository1_backup.rep -y
```

RollbackDeployment

Rolls back a deployment to purge deployed versions of objects from the target repository. Use this command to roll back all the objects in a deployment group that you deployed at a specific date and time.

You cannot roll back part of the deployment. To roll back, you must connect to the target repository. You cannot roll back a deployment from a non-versioned repository.

To initiate a rollback, you must roll back the latest version of each object.

The RollbackDeployment command uses the following syntax:

```
pmrep rollbackdeployment -p <deployment_group_name> -t <nth_latest_deploy_run> -r
<repository_name> -v <nth_latest_version_of_deployment_group>
```

The following table describes the *pmrep* RollbackDeployment options and arguments:

Option	Argument	Description
-p	deployment_group_name	Required. Name of the deployment group to roll back.
-t	nth_latest_deploy_run	Required. Version of the deployment you want to roll back.

Option	Argument	Description
-r	repository_name	Optional. Name of the source repository from where you deploy the deployment group.
-v	nth_latest_version_of_deployment_group	Optional. Version of the deployment group you want to roll back.

Example

You have a deployment with five versions and want to rollback the last two versions. To do this, you must first roll back the latest deployment. Enter the following text at the prompt to roll back once and purge the last deployment:

```
rollbackdeployment -p Deploy_sales -t 1
```

Next, enter the following text to roll back the next to last deployment:

```
rollbackdeployment -p Deploy_sales -t 2
```

Run

Opens a script file containing multiple *pmrep* commands, reads each command, and runs them. If the script file is UTF-8 encoded, you must use the -u option and the repository code page must be UTF-8. If you run a UTF-8 encoded script file that includes the Connect command against a repository that does not have a UTF-8 code page, the Run command will fail.

If the script file is not UTF-8 encoded, omit the -u option. If you use the -o option and the -u option, *pmrep* generates the output file in UTF-8. If you use the -o option and omit the -u option, *pmrep* generates the output file based on the system locale of the machine where you run *pmrep*.

The command returns “run successfully completed” or returns “run failed” message. The run might fail if the Repository Service cannot open the script file or output file.

The Run command uses the following syntax:

```
run

-f <script_file_name>

[-o <output_file_name>]

[-e (echo commands)]

[-s (stop at first error)]

[-u (UTF-8 encoded script file and output file)]
```

The following table describes *pmrep* Run options and arguments:

Option	Argument	Description
-f	script file name	Required. Name of the script file.
-o	output file name	Optional. Name of the output file. This option writes all messages generated by the commands in the script file into the output file. If you use the -u option and the -o option, *pmrep* generates a UTF-8 encoded output file. If you use the -o option without the -u option, *pmrep* encodes the output file based on the system locale of the machine running *pmrep*.
-e	-	Optional. Commands are echoed back to the script.
-s	-	Optional. Stops running the script after the first error.
-u	-	Optional. Encodes the output file in UTF-8 format. If you use the -u option and the -o option, *pmrep* also encodes the output file in UTF-8 format. Use this option only if the repository code page is UTF-8.

ShowConnectionInfo

Returns the repository name and user information for the current connection.

Use the ShowConnectionInfo command in interactive mode. When you connect to a repository in interactive mode, *pmrep* keeps the connection information in memory until you exit the repository or connect to a different repository.

When you use the ShowConnectionInfo command in command line mode, a message indicating failure to execute the command is given. *pmrep* does not keep connection information in command line mode. The ShowConnectionInfo command does not connect to the repository.

The ShowConnectionInfo command uses the following syntax:

```
showconnectioninfo
```

It returns information similar to the following:

```
Connected to Repository MyRepository in MyDomain as user MyUserName
```

SwitchConnection

Changes the name of an existing connection. When you use SwitchConnection, the Repository Service replaces the relational database connections for all sessions using the connection in one of the following locations:

- Source connection
- Target connection
- Connection Information property in Lookup transformations
- Connection Information property in Stored Procedure transformations
- $Source Connection Value session property

- $Target Connection Value session property

If the repository contains both relational and application connections with the same name and you specified the connection type as relational in *all* locations in the repository, the Repository Service replaces the relational connection.

For example, you have a relational and an application source, each called ITEMS. In a session, you specified the name ITEMS for a relational source connection instead of Relational:ITEMS. When you use SwitchConnection to replace the relational connection ITEMS with another relational connection, *pmrep* does not replace any relational connection in the repository because it cannot determine the connection type for the source connection entered as ITEMS.

The SwitchConnection command uses the following syntax:

```
switchconnection

-o <old_connection_name>

-n <new_connection_name>
```

The following table describes *pmrep* SwitchConnection options and arguments:

Option	Argument	Description
-o	old_connection_name	Required. Name of the connection you want to change.
-n	new_connection_name	Required. New connection name.

TruncateLog

Deletes details from the repository. You can delete all logs, or delete logs for a folder or workflow. You can also enter a date and delete all logs older than that date.

The command returns “truncatelog completed successfully” or returns a “Failed to execute truncatelog” message. The truncate operation might fail for the following reasons:

- The folder name is not valid.
- The workflow does not exist in the given folder.
- You specified a workflow, but no folder name.

The TruncateLog command uses the following syntax:

```
truncatelog

-t <logs_truncated (all or up to end time in MM/DD/YYYY HH24:MI:SS format or as number
of days before current date)>

[-f <folder_name>]

[-w <workflow_name>]
```

The following table describes pmrep TruncateLog options and arguments:

Option	Argument	Description
-t	logs_truncated	Required. Use “all” to delete all logs, or enter an end time. *pmrep* deletes all logs older than the end time. You can enter the end time with the format MM/DD/YYYY HH24:MI:SS, or you can specify the number of days before the current date. If you specify the number of days, the end time must be an integer greater than 0.
-f	folder_name	Optional. Deletes logs associated with the folder. If you do not give both the folder name and the workflow name, then *pmrep* deletes all logs from the repository.
-w	workflow_name	Optional. Deletes logs associated with the workflow. The Repository Service deletes all logs from the repository if you do not give both the folder name and the workflow name. If you give both the folder name and workflow name, the Repository Service deletes logs associated with the workflow. If you enter the workflow name, you must also provide the folder name.

UndoCheckout

Reverses the checkout of an object. When you undo a checkout, the repository releases the write-intent lock on the object and reverts to the most recently checked in version of the object. If you want to modify the object again, you must check it out.

The UndoCheckout command uses the following syntax:

```
undocheckout
-o <object_type>
[-t <object_subtype>]
-n <object_name>
-f <folder_name>
[-s dbd_separator]
```

The following table describes *pmrep* UndoCheckout options and arguments:

Option	Argument	Description
-o	object_type	Required. Type of object. You can specify source, target, transformation, mapping, session, worklet, workflow, scheduler, session config, task, cube, and dimension.
-t	object_subtype	Optional. Type of transformation or task. Ignored for other object types. For more information about valid subtypes, see “Listing Object Types” on page 1330.
-n	object_name	Required. Name of the checked out object.

Option	Argument	Description
-f	folder_name	Required. Name of the folder containing the object.
-s	dbd_separator	Optional. If an ODBC source has a period (.) in the name, define a different separator character when you define the source object. For example, instead of database_name.source_name, define the source object as database_name\source_name, and define the dbd_separator as backslash (\).

Unregister

Unregisters a local repository from a connected global repository.

To use this command, you must run the Repository Service for the local repository in exclusive mode. You can configure the Repository Service to run in exclusive mode in the Administrator tool or you can use the *infacmd* UpdateRepositoryService command.

The command returns “unregister successfully completed” or returns “failed to execute unregister” message. The registration might fail for the following reasons:

- The Repository Service for the local repository is not running in exclusive mode.
- The Repository Service failed to initialize information about the global repository.
- You failed to connect to the Repository Service.

The Unregister command uses the following syntax:

```
unregister
-r <local_repository_name>
-n <local_repository_user_name>
[-s <local_repository_user_security_domain>]
[-x <local_repository_password> |
 -X <repository_password_environment_variable>]
[-d <local_repository_domain_name> |
{-h <local_repository_portal_host_name>
-o <local_repository_portal_port_number>}] (if local repository is in a different domain)
```

The following table describes *pmrep* Unregister options and arguments:

Option	Argument	Description
-r	local_repository_name	Required. Name of the local repository to unregister.
-n	local_repository_user_name	Required. Local user name.
-s	local_repository_user_ security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Default is Native.

Option	Argument	Description
-x	local_repository_password	Required if you do not use the -X option. Login password for the local target repository. You must use the -x or -X option, but not both.
-X	local_repository_password_environment_variable	Required if you do not use the -x option. Login password environment variable for the local target repository. You must use the -x or -X option, but not both.
-d	local_repository_domain_name	Required if the local repository is in a different domain and you do not use the -h and -o options. Name of the Informatica domain for repository.
-h	local_repository_portal_host_name	Required if the local repository is in a different domain and you do not use the -d option. Machine name of the domain where the local repository is located. If you use this option, you must also use the -o option.
-o	local_repository_portal_port_number	Required if the local repository is in a different domain and you do not use the -d option. Port number for the domain where the local repository is located. If you use this option, you must also use the -h option.

UnregisterPlugin

Removes a plug-in from a repository. You can add and remove plug-ins to extend system functionality. A plug-in is a software module that introduces new repository metadata.

When you use this command, the Repository Service must be running in exclusive mode. You can configure the Repository Service to run in exclusive mode in the Administrator tool or you can use the *infacmd* UpdateRepositoryService command.

The UnregisterPlugin command uses the following syntax:

```
unregisterplugin
-v <vendor_id>
-l <plug-in_id>
[-s (is security module)
 [-g (remove user-name-login mapping)]
 {-w <new_password> |
  -W <new_password_environment_variable>}]
```

The following table describes *pmrep* UnregisterPlugin options and arguments:

Option	Argument	Description
-v	vendor_id	Required. Identifies the security plug-in by vendor identification number. You define this number when you register the plug-in.
-l	plug-in_id	Required. Identifies the plug-in by identification number. You define this identification number when you register the plug-in.
-s	-	Optional. Indicates whether the module is an external security module.
-g	-	Optional. Applicable when registering an external security module. Removes the association between user names and login names in the repository when you unregister an external security module. If you omit this option, you retain the association in the repository, but the Repository Manager does not display it anywhere. Use this option when you are unregistering a security module.
-w	new_password	Required when the plug-in contains a security module. Required if you do not use the -W option. You must use the -w or -W option, but not both. Specifies a new password for the user running the UnregisterPlugin command. When you unregister an external authentication module, all user passwords reset to the values in the repository. You must enter a new password to access the repository.
-W	new_password_environment_ variable	Required when the plug-in contains a security module. Required if you do not use the -w option. You must use the -w or -W option, but not both. Specifies a new password environment variable for the user running the unregister command. When you unregister an external authentication module, all user passwords reset to the values in the repository. You must enter a new password to access the repository.

Unregistering an External Security Module

Use the UnregisterPlugin command to discontinue using an external security module with a repository. If you unregister the external security module, PowerCenter switches to repository authentication mode. All user passwords reset to the values in the repository instead of the values in the external directory. When you unregister the security module, you do not lose the mapping between the user names and the external security login names unless you enter the -g option. Use the mapping again if you register a new security module.

Note: Although you can save the associations between external logins and user names, the Repository Manager does not display the external logins while running under user authentication.

You must use the -w or -W option to create a new password when you unregister the security module.

Example

As an administrator, you decide to switch from the LDAP security module back to repository authentication. You remove the user name-login mapping. Any users that you added to the system under repository

authentication can log in with their old user names and passwords. Any users you added to the repository under the LDAP security cannot log in until you enable their user names.

Note: You must provide the LDAP NIS login and password to use the UnregisterPlugin command. You must also provide a new password to use after you switch back to user authentication.

UpdateConnection

Updates the user name, password, connect string, and attributes for a database connection.

The command returns an “operation successfully completed” or returns “operation failed” message. A failure might occur for the following reasons:

- The database type is not supported.
- The connection object does not exist.
- *pmrep* cannot acquire a lock on the object.
- One of the required parameters is missing.

The UpdateConnection command uses the following syntax:

```
updateconnection

-t <connection_subtype>

-d <connection_name>

[{[-u <new_user_name>]

[{-p <new_password> |

-P <new_password_environment_variable>

[-w (use parameter in password) |

-x (do not use parameter in password)]}]} |

-K <connection_to_the_Kerberos_server>]

[-c <new_connection_string>]

[-a <attribute_name>

-v <new_attribute_value>]

[-s <connection type application, relational, ftp, loader or queue > ]

[-l <code page>]

[-S <odbc_subtype> (valid for ODBC connection only, default is None)]
```

The following table describes *pmrep* UpdateConnection options and arguments:

Option	Argument	Description
-t	connection_subtype	Required. Displays the connection subtype. For example, for a Relational connection, connection subtypes include Oracle, Sybase, and Microsoft SQL Server. For FTP connections, the valid subtype is FTP. For a list of predefined connection subtypes, see "Connection Subtypes" on page 1282. **Note:** The connection subtype in the -t option must be valid for the associated connection type specified with the -s option.
-d	connection_name	Required. Database connection name.
-u	new_user_name	Optional. User name used for authentication when you connect to the relational database.
-p	new_password	Optional. Password used for authentication when you connect to the relational database. Use the -p or -P option, but not both. To specify a parameter in the password, add the $Param prefix for the -p option and ensure that you use the -w option. Do not use a dollar sign ($) anywhere else in the -p option, and enter the parameter password without spaces. For example, `-p '$Param_abc' -w`
-P	new_password_ environment_variable	Optional. Password environment variable used for authentication when you connect to the relational database. Use the -p or -P option, but not both.
-w	-	Optional. Enables you to use a parameter in the password option. *pmrep* uses the password specified with the -p or -P option as the name of the session parameter at run time. Valid only if you use the -p or -P option. If you do not use a parameter in the password option, *pmrep* uses the user password specified with the -p or -P option.
-x	-	Optional. Disables the use of password parameters if you use the parameter in password. *pmrep* uses the password specified with the -p or -P option.
-K	-	Optional. Indicates that the database that you are connecting to runs on a network that uses Kerberos authentication.
-c	new_connection_string	Optional. Connect string the Integration Service uses to connect to the relational database.
-a	attribute_name	Optional. Name of the attribute.
-v	new_attribute_value	Required if you use the -a option. New attribute value of the connection. Enter "yes" to enable new attributes, and "no" to disable new attributes.

Option	Argument	Description
-s	connection type application, relational, ftp, loader or queue	Optional. Type of connection. A connection can be one of the following types: - Application - FTP - Loader - Queue - Relational Default is relational. **Note:** The connection subtype in the -t option must be valid for the associated connection type specified with the -s option.
-l	code page	Optional. Code page associated with the connection.
-S	odbc_subtype	Optional. Enables the ODBC subtype for an ODBC connection. An ODBC connection can be one of the following ODBC subtypes: - AWS Redshift - Azure DW - Greenplum - Google Big Query - PostgreSQL - Snowflake - SAP HANA - None Default is None.

For more information about connection subtypes, see "Connection Subtypes" on page 1282.

UpdateEmailAddr

Updates the session notification email addresses associated with the Email tasks assigned to the session. If you did not previously enter a success or failure Email task for the session, the command does not update the email addresses. You can update the email notification addresses for a non-reusable session with a unique name in the folder. You can enter different addresses to receive either success or failure notifications. This command requires you to connect to a repository.

The UpdateEmailAddr command uses the following syntax:

```
updateemailaddr
-d <folder_name>
-s <session_name>
-u <success_email_address>
-f <failure_email_address>
```

The following table describes *pmrep* UpdateEmailAddr options and arguments:

Option	Argument	Description
-d	folder_name	Required. Name of the session folder.
-s	session_name	Required. Name of the session.
-u	success_email_address	Required. Email address to send session success notifications.
-f	failure_email_address	Required. Email address to send session failure notifications.

UpdateSeqGenVals

Updates one or more of the following properties for the specified Sequence Generator transformation:

- Start Value
- End Value
- Increment By
- Current Value

You might want to update sequence values when you move a mapping from a development environment to a production environment. Use the UpdateSeqGenVals command to update reusable and non-reusable Sequence Generator transformations. However, you cannot update values for instances of reusable Sequence Generator transformations or shortcuts to Sequence Generator transformations.

The UpdateSeqGenVals command uses the following syntax:

```
updateseqgenvals
-f <folder_name>
[-m <mapping_name>]
-t <sequence_generator_name>
[-s <start_value>]
[-e <end_value>]
[-i <increment_by>]
[-c <current_value>]
```

The following table describes *pmrep* UpdateSeqGenVals options and arguments:

Option	Argument	Description
-f	folder_name	Required. Folder name.
-m	mapping_name	Mapping name. When you update values for a non-reusable Sequence Generator transformation, you must include the mapping name.
-t	sequence_generator_name	Required. Sequence Generator transformation name.

Option	Argument	Description
-s	start_value	Optional. Start value of the generated sequence you want the Integration Service to use if the Sequence Generator transformation uses the Cycle property. If you select Cycle in the transformation properties, the Integration Service cycles back to this value when it reaches the end value. If you designate an invalid value, *pmrep* gives an error message and does not update the Sequence Generator transformation.
-e	end_value	Optional. Maximum value the Integration Service generates. If the Integration Service reaches this value during the session and the sequence is not configured to cycle, it fails the session. If you designate an invalid value, *pmrep* displays an error message and does not update the Sequence Generator transformation.
-i	increment_by	Optional. Difference between two consecutive values from the NEXTVAL port. If you designate an invalid value, *pmrep* displays an error message and does not update the Sequence Generator transformation.
-c	current_value	Optional. Current value of the sequence. Enter the value you want the Integration Service to use as the first value in the sequence. If you want to cycle through a series of values, the current value must be greater than or equal to the start value and less than the end value. If you designate an invalid value, *pmrep* gives an error message and does not update the Sequence Generator transformation.

UpdateSrcPrefix

Updates the owner name for session source tables. You can update the owner name for one or all sources in a session. Updatesrcprefix updates the owner name for source tables at the session level.

pmrep updates source table owner names if you previously edited the source table name in the session properties.

The UpdateSrcPrefix command uses the following syntax:

```
updatesrcprefix
-f <folder_name>
-s [<qualifying_path>.]<session_name>
[-t <source_name>]
-p <prefix_name>
[-n (use source instance name; not using -n gives old, deprecated behavior)]
```

The following table describes the *pmrep* UpdateSrcPrefix options and arguments:

Option	Argument	Description
-f	folder_name	Required. Name of the folder containing the session.
-s	session_name	Required. Name of the session containing the sources to update. For reusable sessions, enter the session name. For non-reusable sessions, you must also enter the session path, such as *worklet_name.session_name* or *workflow_name.session_name*.
-t	source_name	Optional. Name of the source to update. If you omit this option, *pmrep* updates all source table owner names in the session. When you include the -n option, you enter the name of the source instance as displayed in the session properties or as output by the ListTablesBySess command. Although the UpdateSrcPrefix command will run without the -n option, include the -n option to use the source instance name. If you omit the -n option, you must enter the dbd name and the source table name as *dbd_name.source_name*. You can find the source dbd name in the Designer Navigator. The Designer generates the dbd name from the source type or data source name when you create a source definition in the repository.
-p	prefix_name	Required. Owner name you want to update in the source table.
-n	-	Optional. Matches the source_name argument with source instance names. Although the UpdateSrcPrefix command will run without the -n option, include the -n option to use the source instance name. When you do not include this option, *pmrep* matches the source_name argument with the source table names.

UpdateStatistics

Updates statistics for repository tables and indexes.

The command returns “updatestatistics completed successfully” or returns “updatestatistics failed."

The UpdateStatistics command uses the following syntax:

```
updatestatistics
```

UpdateTargPrefix

Updates the table name prefix for session target tables. The table name prefix specifies the owner of the table in the database. You can update the owner name for one or all targets specified in a session. UpdateTargPrefix updates the target table name prefix at the session level.

pmrep updates table name prefixes if you previously edited the table name prefix at the session level.

The UpdateTargPrefix command uses the following syntax:

```
updatetargprefix
-f <folder_name>
-s [<qualifying_path>.]<session_name>
[-t <target_name>]
-p <prefix_name>
[-n (use target instance name; not using -n gives old, deprecated behavior)]
```

The following table describes the *pmrep* UpdateTargPrefix options and arguments:

Option	Argument	Description
-f	folder_name	Required. Name of the folder containing the session.
-s	session_name	Required. Name of the session containing the targets to update. For reusable sessions, enter the session name. For non-reusable sessions, enter the session name and session path, such as *worklet_name.session_name* or *workflow_name.session_name*.
-t	target_name	Optional. Name of the target to update. If you omit this option, *pmrep* updates all target table name prefixes in the session. When you include the -n option, you can enter the name of the target instance as displayed in the session properties or as output by the ListTablesBySess command. Although the UpdateTargPrefix command will run without the -n option, include the -n option to use the target instance name. When you omit the -n option, you must enter the target table name instead of the target instance name.
-p	prefix_name	Required. Table name prefix you want to update in the target table.
-n	-	Optional. Matches the target name argument with target instance names. Although the UpdateTargPrefix command will run without the -n option, include the -n option to use the target instance name. When you omit this option, *pmrep* matches the target name argument with the target table names.

Upgrade

Upgrades a repository to the latest version.

The Upgrade command uses the following syntax:

```
upgrade
[-x <repository_password_for_confirmation> |
```

```
-X <repository_password_environment_variable_for_confirmation>]
```

The following table describes *pmrep* Upgrade options and arguments:

Option	Argument	Description
-x	repository_ password_for_ confirmation	Optional. Password. You can use the -x or -X option, but not both. If you do not use the -x or -X option, pmrep prompts you to enter the password for confirmation.
-X	repository_password_ environment_variable_for_ confirmation	Required if you do not use the -x option. Password environment variable. You must use the -x or -X option, but not both.

UninstallAbapProgram

Uninstalls the ABAP program. Uninstall an ABAP program when you no longer want to associate the program with a mapping. The command uninstalls the programs from the SAP system and removes the corresponding program information from the PowerCenter repository.

The UninstallAbapProgram command uses the following syntax:

```
uninstallabapprogram
-s <folder_name>
-m <mapping_name>
[-v <version_number>]
[-l <log_filename>]
-u <user_name>
-x <password>
-c <connect_string>
-t <client>
[-y <language>]
-p <program_mode (file, stream)>
```

The following table describes pmrep UninstallAbapProgram options and arguments:

Option	Argument	Description
-s	folder_name	Required. The name of the folder that contains the mapping of the ABAP program that you want to uninstall.
-m	mapping_name	Required. Name of the mapping.
-v	version_number	Optional. Version number of the mapping. Default is the latest version.

Option	Argument	Description
-l	log_filename	Optional. Name of the log file where the command writes the information or error messages. By default, the log file is stored in the directory where you run the command.
-u	user_name	Required. SAP source system connection user name. Must be a user for which you have created a source system connection.
-x	password	Required. Password for the user name. Use the command line program pmpasswd to encrypt the user password.
-c	connect_string	Required. DEST entry defined in the `sapnwrfc.ini` file for a connection to a specific SAP application server or for a connection that uses SAP load balancing.
-t	client	Required. SAP client number.
-y	language	Optional. SAP Logon language. Must be compatible with the PowerCenter Client code page. Default is the language of the SAP system.
-p	program_mode (file, stream)	Required. Mode in which the PowerCenter Integration Service extracts data from the SAP system. Select file or stream.

Example

The following example uninstalls the ABAP program:

```
uninstallabapprogram -s folder_name -m mapping_name -l logfile_name -u user_name -x
password -c connect_string -t 800 -y EN -p stream
```

Validate

Validates objects. You can output the results to a persistent output file or standard output.

It also displays a validation summary to stdout. The summary includes the number of valid objects, invalid objects, and skipped objects. The persistent output file contains standard information, encoded IDs, and a CRC check. You can save and check in the objects that change from invalid to valid.

You can validate the following types of objects:

- Mappings
- Mapplets
- Sessions
- Workflows
- Worklet objects

If you use another type of object in the input parameter, *pmrep* returns an error. If you use the wrong type of object in a persistent input file, *pmrep* reports an error and skips the object.

Note: The *pmrep* Validate command does not validate shortcuts.

When you run Validate, you can output information about object status:

- **valid.** Objects successfully validated.

- **saved.** Objects saved after validation.
- **skipped.** Shortcuts and object types that do not require validation.
- **save_failed.** Objects that did not save because of lock conflicts or they were checked out by another user.
- **invalid_before.** Objects invalid before the validation check.
- **invalid_after.** Objects invalid after the validation check.

It is not possible to save a non-reusable object unless you save the reusable parent of the object. When you use the -s option, the command does not save validated non-reusable objects unless, as part of the same command, you list reusable objects that are the parents of the non-reusable objects.

The Validate command uses the following syntax:

```
validate
{{-n <object_name>
-o <object_type (mapplet, mapping, session, worklet, workflow)>
[-v <version_number>]
[-f <folder_name>]} |
-i <persistent_input_file>}
[-s (save upon valid)
[-k (check in upon valid)
[-m <check_in_comments>]]]
[-p <output_option_types (valid, saved, skipped, save_failed, invalid_before,
invalid_after, or all)>]
[-u <persistent_output_file_name>
[-a (append)]]
[-c <column_separator>]
[-r <end-of-record_separator>]
[-l <end-of-listing_indicator>]
[-b (verbose)]
[-y (print database type)]
```

The following table describes *pmrep* Validate options and arguments:

Option	Argument	Description
-n	object_name	Required. Name of the object to validate. Do not use this option if you use the -i argument. When you validate a non-reusable session, include the workflow name. Enter the workflow name and the session name in the following format: <workflow name>.<session instance name> When you validate a non-reusable session in a non-reusable worklet, enter the workflow name, worklet name, and session name in the following format: <workflow name>.<worklet name>.<session instance name>
-o	object_type	Required if you are not using a persistent input file. Type of object to validate. You can specify mapplet, mapping, session, worklet, and workflow.
-v	version_number	Optional. Version of the object to validate. Default is the latest or checked out version of the object.
-f	folder_name	Required. Name of the folder containing the object.
-i	persistent_input_file	Optional. Text file from ExecuteQuery, Validate, or ListObjectDependencies commands. Contains a list of object records. You cannot use this file if you specify objects using the -n, -o, or -f arguments.

Option	Argument	Description
-s	-	Optional. Save objects that change from invalid to valid to the repository.
-k	-	Required if you use -s. Check in saved objects.
-m	check_in_comments	Required if you use the -k option, and the current repository requires checkin comments. Add comments when you check in an object.
-p	output_option_types	Required if you use the -u argument. Type of object you want to output to the persistent output file or stdout after validation. You can specify valid, saved, skipped, save_failed, invalid_before, or invalid_after. To enter one or more options, separate them by commas.
-u	persistent_output_file_name	Required if you use the - p argument. Name of an output text file. If you enter a file name, the query writes the results to a file.
-a	append	Optional. Append the results to the persistent output file instead of overwriting it.
-c	column_separator	Optional. Character or set of characters used to separate object metadata columns. Use a character or set of characters that is not used in repository object names. If any repository object name contains spaces, you might want to avoid using a space as a column separator. If you omit this option, *pmrep* uses a single space.
-r	end-of-record_separator	Optional. Character or set of characters used to specify the end of the object metadata. Use a character or set of characters that is not used in repository object names. Default is newline /n.
-l	end-of-listing_indicator	Optional. Character or set of characters used to specify the end of the object list. Enter a character or set of characters that is not used in repository object names. If you omit this option, *pmrep* uses a period.
-b	-	Optional. Verbose. Displays more than the minimum information about the objects. If you omit this option, *pmrep* displays a shorter format including the object type, the word reusable or non-reusable, the object name and path. Verbose format includes the version number and folder name. The short format for global objects such as label, query, deployment group, and connection, includes the object type and object name. Verbose format includes the creator name and creation time.
-y	-	Optional. Displays the database type of sources and targets.

Version

Displays the PowerCenter version and Informatica trademark and copyright information.

The Version command uses the following syntax:

```
version
```

CHAPTER 45

Working with filemanager

This chapter includes the following topics:

filemanager Overview

The filemanager utility administers preprocessing and file-watching capabilities for a cloud ecosystem such as Amazon AWS or Microsoft Azure.

You can use the filemanager utility for the following preprocessing capabilities:

- List files on a cloud ecosystem.
- Copy files on a cloud ecosystem.
- Copy files from a local system to a cloud ecosystem.
- Move files on a cloud ecosystem.
- Rename files on a cloud ecosystem.
- Delete files from a cloud ecosystem.

You can use the filemanager utility for the following file-watching capabilities:

- Trigger a file-processing event.
- Trigger a workflow or mapping.

You can use the filemanager utility from one of the following locations:

- Client directory. Available under `<Infa home>/clients/tools/filemanager`
- Server directory. Available under `<Infa home>/tools/filemanager`

Logging Options

The filemanager utility provides the following log severity levels for debugging purposes:

- FINE. Writes severe, info, and warning messages to the log. The fine or debug messages are user-request logs.
- SEVERE. Writes severe, warning, and error messages to the log. The severe messages include non-recoverable system failures, connection failures, and service errors.
- WARNING. Writes severe, warning, and error messages to the log. The warning errors include recoverable system failures and warnings.
- INFO. Writes severe, info, warning, and error messages to the log. The info messages include system and service change messages.

Default Behavior

The filemanager utility exhibits the following default behavior:

- The filemanager utility treats `\` as an escape character and not a separator in cloud paths.
- The filemanager utility creates a target directory if you do not specify a target directory for move, copy, or rename operations in Amazon AWS cloud ecosystem.
- The filemanager utility creates a target directory if you do not specify a target directory for a copy operation in ADLS Gen2 storage. For other file operations, the filemanager utility displays an error.
- The filemanager utility deletes the target directory if you move or rename a file to a target directory that does not exist and then try to move the file back to the source directory.
- The filemanager utility displays a file name in the logs when you move, copy, rename, or remove a file.
- The filemanager utility does not display a file name in the logs when you remove a file stored in ADLS Gen2 storage.
- The list command does not specify whether a listed object is a file or a folder.
- The watch command triggers the mapping before a file gets copied in Microsoft Azure cloud ecosystem. This action applies to ADLS Gen1 storage and when you use external tools to copy a file.
- The copy and list commands do not work if you specify a folder path in the parameter `-bn<-bucketname>`.

Guidelines

Use the following guidelines when you use the filemanager utility:

- You must have connection, read, and execute permissions to run the filewatcher utility.
- You cannot copy an empty folder.
- Do not use multiple `/` to specify cloud paths.
- Do not use a file path in a pattern search.
- Do not use a symbolic link that points to the same directory recursively.
- Set the environment variables INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD if the domain is enabled with a custom SSL.
- Set the environment variable INFA_TRUSTSTORE if the domain is SSL enabled.
- Set the first three parameters in a command as: filemanager <cloud ecosystem> <command>. For example, `filemanager aws list`
- Use the absolute path for file names.

- Use the parameter -dn<domainname|optional> for multiple domains configured in Informatica Administrator.
- When yo use the watch command, place the parameter -op<other parameters|optional> at the end of the syntax.
- Use only the following wildcard characters to specify patterns:

  - .

  - ?

  - ""

  - *

copy

Use the copy command to copy files on an Amazon AWS cloud ecosystem.

The filemanager copy command uses the following syntax:

```
copy
[<-bucketname|-bn> bucket_name]
<-old_filename|-fn> old_filename
<-new_foldername|-nfn> new_foldername
<-new_bucketname|-nbn> new_bucketname
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager copy command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files.
-old filename -fn	The name of the source file or folder that you want to copy.
-new_foldername -nfn	The name of the target folder where you want to copy the files.
-new_bucketname -nbn	The name of the bucket where you want to copy the files.

Option	Description
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

copyfromlocal

Use the copyfromlocal command to copy files from a local system to a cloud ecosystem.

The filemanager copyfromlocal command uses the following syntax:

```
copyfromlocal
[<-bucketname|-bn> bucket_name]
[<-cloudpath|-cp> cloud_path]
<-localpath|-lp> local_path
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
[<-folderpath|-fp> folder_path
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager copyfromlocal command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files or folder. This option applies to Amazon AWS.
-cloudpath -cp	Path to the cloud files where you want to copy. This option applies to Microsoft Azure.
-localpath -lp	Path to the source files or folder on a local system that you want to copy.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-folderpath -fp	Optional. Path to the files on cloud where you want to copy. This option applies to Amazon AWS.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

list

Use the list command to list files on a cloud ecosystem.

The filemanager list command uses the following syntax:

```
list
[<-bucketname|-bn> bucket_name]
[<-cloudpath|-cp> cloud_path]
<-pattern|-ptn> pattern
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
```

```
<-folderpath|-fp> folder_path
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager list command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files. This option applies to Amazon AWS.
-cloudpath -cp	Path to the cloud files where you want to copy. This option applies to Microsoft Azure.
-pattern -ptn	A wildcard pattern to match and list filenames or patterns.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-folderpath -fp	Optional. Path to list the files on cloud. This option applies to Amazon AWS.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

move

Use the move command to move files on a cloud ecosystem.

In Microsoft Azure cloud ecosystem, the command move does not support the move operation if the target directory is not present.

The filemanager move command uses the following syntax:

```
move
[<-bucketname|-bn> bucket_name]
<source_cloudpath|-scp> source_cloudpath
```

```
<destination_cloudpath|-dcp> destination_cloudpath
<-old_filename|-fn> old_filename]
<-new_folder|-nfn> new_folder]
<-new_bucketname|-nbn> new_bucketname
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager move command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files. This option applies to Amazon AWS.
-old_filename -fn	Path of the source file name from where you want to move the file. This option applies to Amazon AWS.
-new_folder -nfn	Path to the target folder location where you want to move the file. This option applies to Amazon AWS.
-new_bucketname -nbn	Path to the target bucket name where you want to move the file. This option applies to Amazon AWS.
-source_cloudpath -scp	Path of the source file location on Microsoft Azure cloud ecosystem from where you want to move the file. This option applies to Microsoft Azure.
-destination_cloudpath -dcp	Path to the target folder location on Microsoft Azure cloud ecosystem to where you want to move the file. This option applies to Microsoft Azure.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

remove

Use the remove command to delete files from a cloud ecosystem.

The filemanager remove command uses the following syntax:

```
remove
[<-bucketname|-bn> bucket_name]
<cloudpath|-cp> source_cloudpath
<-filename|-fn> old_filename]
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domain]
<-connection|-cn> connection
<-folderpath|-fp> folder_path
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager remove command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files. This option applies to Amazon AWS.
-filename -fn	Name of the file or folder that you want to delete. This option applies to Amazon AWS.
-cloudpath -cp	Path of file or folder location on Microsoft Azure cloud ecosystem from where you want to delete the file. This option applies to Microsoft Azure.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs.The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.

Option	Description
-folderpath -fp	Optional. Path to the files on cloud from where you want to delete the file. This option applies to Amazon AWS.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

rename

Use the rename command to rename files on a cloud ecosystem.

The filemanager rename command uses the following syntax:

```
rename
[<-bucketname|-bn> bucket_name]
<-old_filename|-fn> old_filename
<-new_filename|-nfn> new_filename
[<-cloudpath|-cp> cloud_path]
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domainname]
<-connection|-cn> connection
[<-domainname|-dn> domain_name]
```

The following table describes the options for the filemanager rename command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files. This option applies to Amazon AWS.
-old filename -fn	Path to the source or old file name that you want to rename. This option applies to Amazon AWS.
-new_filename -nfn	Path to the target file or new file name.
-cloudpath -cp	Path to the cloud file from where you want to rename the file. This option applies to Microsoft Azure.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.

Option	Description
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-domainname -dn	Optional. Name of the Informatica domain. Required only if there are multiple domains configured in the Informatica Administrator.

watch

Use the watch command to watch files that trigger a file processing event, mapping, or workflow on a cloud ecosystem.

The filemanager watch command uses the following syntax:

```
watch
[<-bucketname|-bn> bucket_name]
[<-cloudpath|-cp> cloud_path]
<-pattern|-ptn> pattern
<-username|-un> user_name
<-password|-pd> password
[<-security_domainname|-sdn> security_domainname]
<-connection|-cn> connection
<-Domainname|-dn> domain_name of the DIS
<-DIS|-sn> Data Integration Service
<-applicationname|-a> application_name
<-mappingname|-m> mapping_name
<-workflowname|-w> workflow_name
[<-watchtime|-wt> watch_time]
[<-folderpath|-fp> folder_path
[<-other_parameters|-op> custom_infacmd_mapping_parameters
```

The following table describes the options for the filemanager watch command:

Option	Description
-bucketname -bn	Optional. The name of the bucket containing files or folder. This option applies to Amazon AWS.
-cloudpath -cp	Path to the cloud files that you want to watch. This option applies to Microsoft Azure.
-pattern -ptn	A wildcard pattern to match and list filenames or patterns.
-username -un	Required if the domain uses Native or LDAP authentication. User name to connect to the domain.
-password -pd	Required if you specify the user name. Password for the user name. The password is case sensitive.
security_domainname -sdn	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication. Name of the security domain to which the domain user belongs. The security domain name is case sensitive.If the domain uses native or LDAP authentication, the default is Native. The name of the security domain is the same as the user realm specified during installation.
-connection -cn	Name of the connection in the Informatica Administrator.
-Domainname -dn	Required. Name of the domain that runs the Data Integration Service.
-DIS -sn	Name of the Data Integration Service that runs a mapping or workflow.
-applicationname -a	Name of the application that contains a workflow or mapping.
-mappingname -m	Required if you want to watch a mapping. Name of the mapping that you want to watch.
-workflowname -w	Required if you want to watch a workflow. Name of the workflow that you want to watch.
-watchtime -wt	Optional. The duration of time in minutes to watch the file.
-folderpath -fp	Optional. Path to the files on cloud where you want to copy. This option applies to Amazon AWS.
-other_parameters -op	Optional. Custom parameters that you want to use from infacmd utility.

CHAPTER 46

Working with pmrep Files

This chapter includes the following topics:

Working with pmrep Files Overview

pmrep includes a set of control files that you use to define how to import objects into the repository. The control file parameters use the same parameters in the control file that you use in the PowerCenter Client. You can use the following control files:

- **Persistent input file**. Use a persistent input file to specify repository objects that you want to process.
- **Object import control file**. Use the object import control file and specify a set of questions to help define how objects are imported.
- **Deployment control file**. You can copy the objects in a dynamic or static deployment group to multiple target folders in the target repository.

Using the Persistent Input File

When you run *pmrep* with some tasks, use a persistent input file to specify repository objects that you want to process. The persistent input file represents objects already in the repository. You can create a persistent input file manually or by using *pmrep*.

Use a persistent input file with the following *pmrep* commands:

- **AddToDeploymentGroup**. Add objects to a deployment group.
- **ApplyLabel**. Label objects.
- **ExecuteQuery.** Run a query to create a persistent input file. Use the file for other *pmrep* commands.

- **ListObjectDependencies**. List dependency objects. This command can use a persistent input file for processing, and it can create one.
- **MassUpdate.** Updates session properties for a set of sessions.
- **ObjectExport**. Export objects to an XML file.
- **Validate**. Validate objects. This command can use a persistent input file for processing, and it can create one.

The persistent input file uses the following format:

```
encoded ID, foldername, object_name, object_type, object_subtype, version_number,
reusable|non-reusable
```

Creating a Persistent Input File with pmrep

You can create a persistent input file using the *pmrep* ExecuteQuery, Validate, or ListObjectDependencies commands. These commands create files that contain a list of objects with encoded IDs and a cyclic redundancy check (CRC) value. It also contains an encrypted repository GID. This ID identifies which repository the record comes from.

The *pmrep* commands that use a persistent input file get object information from the encoded IDs. The encoded IDs enable *pmrep* to process the input file quickly.

When you create a persistent input file with *pmrep*, it creates the file in the *pmrep* installation directory. You can specify a different path.

The following text shows a sample persistent input file:

```
2072670638:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944199885:138608640183285:1376256153425:131072168215:65536142655:0288235
:088154:65536122855,EXPORT,M_ITEMS,mapping,none,2
1995857227:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944135065:13867417666804:1376256233835:19660880104:65536271545:0319425:0
17154:6553644164,EXPORT,M_ITEMS_2,mapping,none,3
1828891977:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:3538944279765:138739712184505:137625613474:65536221345:65536133675:091734:09
053:65536156675,EXPORT,M_NIELSEN,mapping,none,1
3267622055:57bfc2ff-df64-40fc-9cd4-
a15cb489bab8:353894462954:138805248300075:1376256151365:6553675414:65536174015:0273455:02
41435:65536261685,EXPORT,M_OS1,mapping,none,1
```

Example

You can use the ExecuteQuery command to create a persistent input file of objects to process in another *pmrep* command. For example, you want to export all logically deleted objects from the repository. You might create a query called find_deleted_objects. When you run the query with *pmrep*, as shown here, it finds all the deleted objects in the repository and outputs the results to a persistent input file:

```
ExecuteQuery -q find_deleted_objects -t private -u deletes_workfile
```

You can then use deletes_workfile as the persistent input file to ObjectExport:

```
ObjectExport -i deletes_workfile -u exported_del_file
```

ObjectExport exports all the referenced objects to an XML file called exported_del_file.

Creating a Persistent Input File Manually

If you want to run *pmrep* commands against a set of objects that you cannot identify through commands such as ExecuteQuery, you can manually create an input file.

Use the following rules and guidelines when you create a persistent input file:

- Enter “none” for the encoded ID. The *pmrep* commands get the object information from the other arguments in the records.
- For source objects, enter the object name as <DBD_name>.<source_name>.
- For objects, such as mappings, that do not have a sub_type, enter “none” as object_subtype, or leave it blank. For more information about valid transformations and task types, see “Listing Object Types” on page 1330.
- For versioned repositories, enter the version number of the object you want, or enter “LATEST” to use the latest version of the object.
- For non-versioned repositories, leave the version_number argument blank.
- For object types, such as targets, that are not reusable or non-reusable, drop the argument.
- You cannot include non-reusable objects. You can specify the reusable parent of the non-reusable object.

  For example, you want to list the object dependencies for a non-reusable Filter transformation. You can specify the mapping that is the parent object of the transformation:

  ```
  none,CAPO,m_seqgen_map,mapping,none,1,reusable
  ```

  The mapping m_seqgen_map is the reusable parent of the Filter transformation. The command runs successfully when you specify the reusable parent.

Note: When you use a manually created persistent input file, the Repository Service returns a message indicating that the ID is not valid. This is an informational message. The Repository Service recognizes that this is a manually created input file and can process the command with “none” as the ID.

Example

The following example shows a manually created persistent input file:

```
none,EXPORT,CustTgt,target,none,2
none,EXPORT,S_Orders,session,,2,reusable
none,EXPORT,EXP_CalcTot,transformation,expression,LATEST,reusable
```

In the first record, CustTgt is a target definition. Targets have no subtype, so you enter “none” for the object_subtype argument. A target cannot be reusable or non-reusable, so you drop the reusable argument. Note that the record has six arguments instead of seven.

In the second record, S_Orders is a session. Sessions have no subtype, so you leave the argument blank.

In the third record, you want the latest version of the transformation, so you enter “LATEST” for the version_number argument.

Using the Object Import Control File

When you use the *pmrep* ObjectImport command, you can supply a control file to answer questions that you normally address when you import objects with the Import Wizard. To create a control file, you must create an XML file defined by impcntl.dtd. The import control file is installed with the PowerCenter Client, and you must include its location in the input XML file.

The following is a sample of the impcntl.dtd file:

```
<!-- Informatica Object Import Control DTD Grammar - >

<!--IMPORTPARAMS This inputs the options and inputs required for import operation -->
<!--CHECKIN_AFTER_IMPORT Check in objects on successful import operation -->
```

```
<!--CHECKIN_COMMENTS Check in comments -->
<!--APPLY_LABEL_NAME Apply the given label name on imported objects -->
<!--RETAIN_GENERATED_VALUE Retain existing sequence generator, normalizer and XML DSQ
current values in the destination -->
<!--COPY_SAP_PROGRAM Copy SAP program information into the target repository -->
<!--APPLY_DEFAULT_CONNECTION Apply the default connection when a connection used by a
session does not exist in the target repository -->
<!ELEMENT IMPORTPARAMS (FOLDERMAP*, TYPEFILTER*, RESOLVECONFLICT?)>
<!ATTLIST IMPORTPARAMS
        CHECKIN_AFTER_IMPORT                                    (YES | NO) "NO"
        CHECKIN_COMMENTS          CDATA      #IMPLIED
        APPLY_LABEL_NAME          CDATA      #IMPLIED
        RETAIN_GENERATED_VALUE    (YES | NO) "NO"
        COPY_SAP_PROGRAM          (YES | NO) "YES"
        APPLY_DEFAULT_CONNECTION  (YES | NO) "NO"
>

<!--FOLDERMAP matches the folders in the imported file with the folders in the target
repository -->
<!ELEMENT FOLDERMAP EMPTY>
<!ATTLIST FOLDERMAP
        SOURCEFOLDERNAME     CDATA    #REQUIRED
            SOURCEREPOSITORYNAME CDATA    #REQUIRED
        TARGETFOLDERNAME     CDATA    #REQUIRED
        TARGETREPOSITORYNAME CDATA    #REQUIRED
>

<!--Import will only import the objects in the selected types in TYPEFILTER node -->
<!--TYPENAME type name to import. This should comforming to the element name in
powermart.dtd, e.g. SOURCE, TARGET and etc.-->
<!ELEMENT TYPEFILTER EMPTY>
<!ATTLIST TYPEFILTER
        TYPENAME    CDATA    #REQUIRED
>

<!--RESOLVECONFLICT allows to specify resolution for conflicting objects during import.
The combination of specified child nodes can be supplied -->
<!ELEMENT RESOLVECONFLICT (LABELOBJECT | QUERYOBJECT | TYPEOBJECT | SPECIFICOBJECT)*>

<!--LABELOBJECT allows objects in the target with label name to apply replace/reuse upon
conflict -->
<!ELEMENT LABELOBJECT EMPTY>
<!ATTLIST LABELOBJECT
        LABELNAME            CDATA                        #REQUIRED
        RESOLUTION          (REPLACE | REUSE | RENAME)    #REQUIRED
>

<!--QUERYOBJECT allows objects result from a query to apply replace/reuse upon conflict
-->
<!ELEMENT QUERYOBJECT EMPTY>
<!ATTLIST QUERYOBJECT
        QUERYNAME             CDATA                         #REQUIRED
        RESOLUTION            (REPLACE | REUSE | RENAME)    #REQUIRED
>

<!--TYPEOBJECT allows objects of certain type to apply replace/reuse upon conflict-->
<!ELEMENT TYPEOBJECT EMPTY>
<!ATTLIST TYPEOBJECT
OBJECTTYPENAME            CDATA                        #REQUIRED
RESOLUTION                REPLACE | REUSE | RENAME)    #REQUIRED
>

<!--SPECIFICOBJECT allows a particular object(name, typename etc.) to apply replace/
reuse upon conflict -->
<!--NAME Object name-->
<!--EXTRANAME Source DBD name - required for source object to identify uniquely-->
<!--OBJECTTYPENAME Object type name-->
<!--FOLDERNAME Folder which the object belongs to-->
<!--REPOSITORYNAME Repository name that this object belongs to-->
<!--RESOLUTION Resolution to apply for the object in case of conflict-->
<!ELEMENT SPECIFICOBJECT EMPTY>
```

```
<!ATTLIST SPECIFICOBJECT
        NAME           CDATA    #REQUIRED
        DBDNAME        CDATA    #IMPLIED
        OBJECTTYPENAME CDATA    #REQUIRED
        FOLDERNAME     CDATA    #REQUIRED
        REPOSITORYNAME CDATA    #REQUIRED
        RESOLUTION
(REPLACE | REUSE | RENAME)    #REQUIRED>
```

Object Import Control File Parameters

The following table lists *pmrep* Object Import control file parameters:

Element	Attribute Name	Attribute Description
IMPORTPARAMS	CHECKIN_AFTER_IMPORT	Required if versioning is enabled.Checks in objects when they successfully import.
IMPORTPARAMS	CHECKIN_COMMENTS	Optional. Applies the comments to the checked in objects.
IMPORTPARAMS	APPLY_LABEL_NAME	Optional. Applies the label name on the imported objects.
IMPORTPARAMS	RETAIN_GENERATED_VALUE	Required if you use Sequence Generator, Normalizer, or XML Source Qualifier transformations. Retains existing Sequence Generator, Normalizer, and XML Source Qualifier transformation current values in the destination.
IMPORTPARAMS	COPY_SAP_PROGRAM	Optional. Copies SAP program information into the target repository.
IMPORTPARAMS	APPLY_DEFAULT_CONNECTION	Optional. Applies the default connection when a connection used by a session does not exist in the target repository. The default connection is the first connection from the sorted list of available connections. Finds the list of connections in the Workflow Manager.
FOLDERMAP	SOURCEFOLDERNAME	Required. Import folder name to match to a folder in the target repository.
FOLDERMAP	SOURCEREPOSITORYNAME	Required. Repository containing the source folder.
FOLDERMAP	TARGETFOLDERNAME	Required. Target folder name for matching.
FOLDERMAP	TARGETREPOSITORYNAME	Required. Repository containing the target folder.

Element	Attribute Name	Attribute Description
TYPEFILTER	TYPENAME	Optional. Imports the objects from a specific node, such as sources, targets, or mappings.
RESOLVECONFLICT	LABELOBJECT, QUERYOBJECT, TYPEOBJECT, AND SPECIFICOBJECT elements.	You can specify conflict resolutions for objects.
LABELOBJECT	LABELNAME	Required. Identifies objects by label name for conflict resolution specification.
LABELOBJECT	RESOLUTION	Required. Replace, Reuse, Rename.
QUERYOBJECT	QUERYNAME	Required. Identifies objects from this query for conflict resolution specification.
QUERYOBJECT	RESOLUTION	Required. Replace, Reuse, or Rename.
TYPEOBJECT	OBJECTTYPENAME	Required. Object type for this conflict resolution. For a list of object types, see "Object Import Control File Parameters" on page 1387.
TYPEOBJECT	RESOLUTION	Required. Replace, Reuse, or Rename.
SPECIFICOBJECT	NAME	Required. Specific object name for this conflict resolution.
SPECIFICOBJECT	DBDNAME	Optional. Source DBD to identify source object.
SPECIFICOBJECT	OBJECTTYPENAME	Required. Object type for this conflict resolution. For a list of object types, see "Object Import Control File Parameters" on page 1387.
SPECIFICOBJECT	FOLDERNAME	Required. Source folder the containing object.
SPECIFICOBJECT	REPOSITORYNAME	Required. Source repository containing the object.
SPECIFICOBJECT	RESOLUTION	Required. Replace, Reuse, or Rename.

You can use the following object types with the OBJECTTYPENAME attribute:

- All
- Aggregator
- App Multi-Group Source Qualifier
- Application Source Qualifier

- Assignment
- Command
- Control
- Custom Transformation
- Decision
- Email
- Event-raise
- Event-wait
- Expression
- External Procedure
- Filter
- Input transformation
- Joiner
- Lookup Procedure
- Mapping
- Mapplet
- MQ Source Qualifier
- Normalizer
- Output Transformation
- Rank
- Router
- Scheduler
- Session
- Sequence
- SessionConfig
- Sorter
- Source Definition
- Source Qualifier
- Start
- Target Definition
- Timer
- Transaction Control
- Update Strategy
- User Defined Function
- Workflow
- Worklet
- XML Source Qualifier

Note: Use the object type “All” to reuse or replace all objects.

Object Import Control File Examples

The parameters you specify in the control file code determine the actions that take place when you run the ObjectImport command in *pmrep*. The following examples discuss instances in which you use the ObjectImport command with a control file to import repository objects. The elements and attribute names that are key to performing the described tasks are designated with comments in the code.

The following table provides a description of sample object import control files:

Function	Description
Import source objects.	Use the TYPEFILTER element to import only source objects.
Import multiple objects into a folder.	Use the IMPORTPARAMS and FOLDERMAP elements to import multiple objects.
Check in and label imported objects.	Use the CHECKIN_AFTER_IMPORT and APPLY_LABEL_NAME attributes of the IMPORTPARAMS element to label imported objects.
Retain Sequence Generator and Normalizer transformation values.	Use the RETAIN_GENERATED_VALUE attribute of the IMPORTPARAMS element to retain Sequence Generator and Normalizer values when you import objects.
Import objects and local shortcut objects to the same repository.	Use all attributes of the FOLDERMAP element to import objects and local shortcut objects that reference the objects.
Import shortcut objects from another repository.	Use all attributes of the FOLDERMAP element to import shortcut objects from another repository.
Import objects to multiple folders.	Use all attributes of the FOLDERMAP element to import objects to multiple folders.
Import specific objects.	Use the TYPEFILTER element to import specific objects.
Reuse and replace dependent objects.	Use the OBJECTTYPENAME and RESOLUTION attributes of the TYPEOBJECT element to reuse and replace dependent objects.
Replace invalid mappings.	Use the QUERYOBJECT element to replace invalid mappings.
Rename objects.	Use the RESOLUTION attribute of the SPECIFICOBJECT element to rename objects.
Copy SAP mappings and SAP program information.	Use the COPY_SAP_PROGRAM attribute of the IMPORTPARAMS element to copy SAP mappings and SAP program information.
Apply default connection attributes.	Use the APPLY_DEFAULT_CONNECTION attribute of the IMPORTPARAMS element to apply default connection attributes.
Resolve object conflicts.	Use the RESOLVECONFLICT element to resolve object conflicts.

Importing Source Objects

You can import source objects. For example, you want to replace all the duplicate objects labeled “Monthend” in the target folder. However, you want to rename conflicting source objects that contain “Yr_End” in the object name. You have a query called “yr_end_qry” that finds these objects.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT ="NO">
<FOLDERMAP SOURCEFOLDERNAME ="OLD_ACCOUNTING"
   SOURCEREPOSITORYNAME ="OLD_REPOS"
   TARGETFOLDERNAME ="NEW_ACCOUNTING"
   TARGETREPOSITORYNAME ="NEW_REPOS"/>

<!-- use the TYPEFILTER element to import only source objects -->
<TYPEFILTER TYPENAME ="SOURCE"/>
<RESOLVECONFLICT>
     <LABELOBJECT LABELNAME ="Monthend"
    RESOLUTION = "REPLACE"/>
<QUERYOBJECT QUERYNAME ="yr_end_qry"
    RESOLUTION ="RENAME"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Importing Multiple Objects into a Folder

You can import multiple objects into a folder, check them in, and label them. For example, you want to import the objects to folder SRC_F1 and apply the label LABEL_IMPORT_NEW to the objects.

You might create a control file with the following attributes:

```
<xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--apply label name LABEL_IMPORT_NEW to imported objects-->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="NEWOBJECTS"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>
```

Checking In and Labeling Imported Objects

You can import objects into a folder, check them in, label them, and resolve the conflict between session configuration objects. For example, you want to export the objects from folder SRC_F1 and import them into folder TGT_F1. The Repository Service creates a session configuration in the target folder by default. You include the APPLY_LABEL_NAME attribute in the IMPORTPARAMS element to label the imported objects, and the RESOLVECONFLICT element in the control file to resolve the conflict.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter VERSION1 as the comment for the object you check in-->
<!--apply label name LABEL_IMPORT_NEW to imported objects-->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Retaining Sequence Generator and Normalizer Values

You can retain the values of Sequence Generator and Normalizer transformations when you import objects and replace all objects in the target folder.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<!--enter YES as the value for the RETAIN_GENERATED_VALUE attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="VERSION1"
APPLY_LABEL_NAME="LABEL_IMPORT_NEW" RETAIN_GENERATED_VALUE="YES">w
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME="ALL" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Importing Objects and Local Shortcut Objects to the Same Repository

You can import objects and their respective local shortcut objects to the same repository. For example, you have folders named SRC_SHARED_F1 and SRC_NONSHARED_F1. The SRC_NONSHARED_F1 folder is not shared and contains local shortcut objects that reference objects in the SRC_SHARED_F1 folder. You want to import the objects to different folders in the target repository, and you want the shortcut objects in folder TGT_NONSHARED_F1 to point to the objects in TGT_SHARED_F1.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO">

<!-- import objects from SRC_SHARED_F1 to TGT_SHARED_F1, and shortcut objects from
SRC_NONSHARED_F1 to TGT_NONSHARED_F1-->
<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC__REPO1"
TARGETFOLDERNAME="TGT_SHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="TGT_REPO1"/>
</IMPORTPARAMS>
```

Importing Shortcut Objects from Another Repository

You can import objects from other repositories. For example, you have folders in a local repository that contain shortcuts to objects in a global repository. You want to import the global shortcut objects to a repository that is registered to the global repository and maintain shortcuts to the original objects in the global repository.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="global objects"
APPLY_LABEL_NAME="LABEL_IMPORT_GLOBAL_SHORTCUT">

<!--import the shortcut objects from source folder SRC_SHARED_F1 in source repository
SRC_GDR_REPO1 to source folder SRC_SHARED_F1 in target repository SRC_GDR_REPO2 -->

<FOLDERMAP SOURCEFOLDERNAME="SRC_SHARED_F1" SOURCEREPOSITORYNAME="SRC_GDR_REPO1"
TARGETFOLDERNAME="SRC_SHARED_F1" TARGETREPOSITORYNAME="SRC_GDR_REPO2"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_NONSHARED_F1" SOURCEREPOSITORYNAME="SRC_LDR_REPO1"
TARGETFOLDERNAME="TGT_NONSHARED_F1" TARGETREPOSITORYNAME="SRC_LDR_REPO2"/>
</IMPORTPARAMS>
```

Importing Objects to Multiple Folders

You can import objects to multiple folders that were exported from multiple folders. For example, you exported objects from folders SRC_F1, SRC_F2, and SRC_F3, and you want to import them to target folders TGT_F1, TGT_F2, TGT_F3 in repository TGT_REPO1.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="mulfolders"
APPLY_LABEL_NAME="L1">

<!-- import objects from source folders SRC_F1, SRC_F2, and SRC_F3 to target folders
TGT_F1, TGT_F2, and TGT_F3 in repository TGT_REPO1 -->
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="SRC_REPO1"
TARGETFOLDERNAME="TGT_F1 TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_F2" SOURCEREPOSITORYNAME="SRC_REPO2"
TARGETFOLDERNAME="TGT_F2" TARGETREPOSITORYNAME="TGT_REPO1"/>
<FOLDERMAP SOURCEFOLDERNAME="SRC_F3" SOURCEREPOSITORYNAME="SRC_REPO3"
TARGETFOLDERNAME="TGT_F3" TARGETREPOSITORYNAME="TGT_REPO1"/>
   <RESOLVECONFLICT>
<TYPEOBJECT OBJECTTYPENAME = "SESSIONCONFIG" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>
```

Importing Specific Objects

You can choose the objects you want to import. For example, you exported multiple object types to an XML file. You want to import only mappings, and respective sources and targets, to a folder.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL_MAPPING_TYPEFILTER">
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX1_"/>

<!-- use the TYPENAME attribute to import only mappings -->
   <TYPEFILTER TYPENAME="MAPPING"/>
</IMPORTPARAMS>
```

Reusing and Replacing Dependent Objects

You can import sessions, replace the mappings, and reuse the existing sources and targets in the target folder. For example, you want to replace the mappings and reuse the source definitions, target definitions, and session configuration objects.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_TYPEFILTER"
APPLY_LABEL_NAME="LABEL_SESSION_TYPEFILTER">
<FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="PMREP_CHECKED_OUT_IMPORT_TYPEFILTER_SESSION"
TARGETREPOSITORYNAME="REPO_EX_1"/>
   <TYPEFILTER TYPENAME="SESSION"/>
   <RESOLVECONFLICT>
```

```
<!-- replace all mappings -->
      <TYPEOBJECT OBJECTTYPENAME = "MAPPING" RESOLUTION="REPLACE"/>

<!-- reuse source definitions, target definitions, and sessionconfigs -->
<TYPEOBJECT OBJECTTYPENAME = "SOURCE DEFINITION" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "TARGET DEFINITION" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "SESSIONCONFIG" RESOLUTION="REUSE"/>

<!-- replace some object types and reuse remaining objects-->
<TYPEOBJECT OBJECTTYPENAME = "ALL" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME = "SOURCE DEFINITION" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPENAME = "MAPPING" RESOLUTION="REPLACE"/>

</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Note: When you reuse or replace an object type, the resolution for that object type overrides the resolution for all object types. The preceding example replaces source definitions and mappings and reuses the remaining objects. Use the object type “All” to reuse or replace all objects. For more information about object types, see “Object Import Control File Parameters” on page 1387.

Replacing Invalid Mappings

You can replace invalid mappings and associated child objects that are returned by a query. For example, you want to replace objects returned by the query QUERY_PARENT_RENAME.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"

CHECKIN_COMMENTS="PMREP_IMPORT_QUERY_PARENT_REPLACE_CHILD_REUSE"
APPLY_LABEL_NAME="LABEL_QUERY_PARENT_RENAME_CHILD_REUSE">
   <FOLDERMAP SOURCEFOLDERNAME="PMREP_CHECKED_OUT" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="PMREP_CHECKED_OUT" TARGETREPOSITORYNAME="REPO_EX_1"/>
   <RESOLVECONFLICT>

<!--replace the objects returned by the query QUERY_PARENT_RENAME -->
<QUERYOBJECT QUERYNAME="QUERY_PARENT_RENAME" RESOLUTION="REPLACE"/>
</RESOLVECONFLICT>
</IMPORTPARAMS>
```

Renaming Objects

You can rename specific objects when object conflicts occur. For example, you want to the rename the objects ADDRESS, ADDRESS1, R_LKP, MAP_MLET, R_S3, WF_RS1. The Repository Service appends the object names with a number.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES"
CHECKIN_COMMENTS="PMREP_IMPORT_SPECIFICOBJECT_RENAME"
APPLY_LABEL_NAME="LABEL_IMPORT_SPECIFIC_OBJECT_RENAME">
<FOLDERMAP SOURCEFOLDERNAME="SRC_FOLDER1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_FOLDER1" TARGETREPOSITORYNAME="REPO_EX_1"/>

<RESOLVECONFLICT>

<!-- rename the objects ADDRESS, ADDRESS1, R_LKP, MAP_MLET, R_S3, WF_RS1 -->
```

```
<SPECIFICOBJECT NAME="ADDRESS" DBDNAME="sol805" OBJECTTYPENAME="Source Definition"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="ADDRESS1" OBJECTTYPENAME="Target Definition"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_LKP" OBJECTTYPENAME="Lookup Procedure"
FOLDERNAME="PMREP_CHECKED_OUT" REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="MAP_MLET" OBJECTTYPENAME="Mapping" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPENAME="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
<SPECIFICOBJECT NAME="WF_RS1" OBJECTTYPENAME="Workflow" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="RENAME"/>
</RESOLVECONFLICT></IMPORTPARAMS>
```

Copying SAP Mappings and SAP Program Information

You can copy SAP program information when you import SAP mappings. For example, you want to import the SAP mappings and copy the program information associated with the object you are importing to folder TGT_F1.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value for the COPY_SAP_PROGRAM attribute to copy SAP mappings and
SAP program information -->

<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="Version2 of objects"
APPLY_LABEL_NAME="LABEL71_REPLACE_FOLDER" COPY_SAP_PROGRAM="YES">
   <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
</IMPORTPARAMS>
```

Applying Default Connection Attributes

You can apply a default connection attribute to a session if a connection is not present in the target repository. For example, no connection exists in target repository REPO_EX_1.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">

<!-- enter YES as the value of the APPLY_DEFAULT_CONNECTION element to apply a default
connection attribute -->
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="NO" APPLY_DEFAULT_CONNECTION="YES">
   <FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>
<RESOLVECONFLICT>
<SPECIFICOBJECT NAME="R_S3" OBJECTTYPENAME="Session" FOLDERNAME="PMREP_CHECKED_OUT"
REPOSITORYNAME="REPO_EX_1" RESOLUTION="REPLACE"/>
<RESOLVECONFLICT>
</IMPORTPARAMS>
```

Resolving Object Conflicts

You can resolve object conflicts for labeled objects in the target repository. For example, you have mappings, mapplets, sources, and targets labeled LBL_MPNG_MPLTS_SRCS_TGTS. You want to replace these objects and label them REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS and reuse all transformations.

You might create a control file with the following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IMPORTPARAMS SYSTEM "impcntl.dtd">
<IMPORTPARAMS CHECKIN_AFTER_IMPORT="YES" CHECKIN_COMMENTS="PMREP_IMPORT_LABEL_REPLACE"
APPLY_LABEL_NAME="REPLACE_LBL_MPNG_MPLTS_SRCS_TGTS" >
<FOLDERMAP SOURCEFOLDERNAME="SRC_F1" SOURCEREPOSITORYNAME="REPO_EX_1"
TARGETFOLDERNAME="TGT_F1" TARGETREPOSITORYNAME="REPO_EX_1"/>

<!-- use the RESOLVECONFLICT element in conjunction with the RESOLUTION attribute of the
OBJECTTYPENAME element to resolve conflicts when you import objects -->
   <RESOLVECONFLICT>
<LABELOBJECT LABELNAME="LBL_MPNG_MPLTS_SRCS_TGTS" RESOLUTION="REPLACE"/>
<TYPEOBJECT OBJECTTYPENAME="Lookup Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Stored Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Expression" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Filter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Aggregator" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Rank" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Normalizer" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Router" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Sequence" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Sorter" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="update strategy" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Custom Transformation" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Transaction control" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="External Procedure" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="Joiner" RESOLUTION="REUSE"/>
<TYPEOBJECT OBJECTTYPENAME="SessionConfig" RESOLUTION="REUSE"/>
</RESOLVECONFLICT>

</IMPORTPARAMS>
```

Using the Deployment Control File

A deployment control file is an XML file that you use with the DeployFolder and DeployDeploymentGroup *pmrep* commands to deploy a folder or deployment group. You can create a deployment control file manually to provide parameters for deployment, or you can create a deployment control file with the Copy Wizard.

If you create the deployment control file manually, it must conform to the depcntl.dtd file that is installed with the PowerCenter Client. You include the location of the depcntl.dtd file in the deployment control file.

You can specify a deployment timeout in the deployment control file. The deployment timeout is the period of time that *pmrep* waits to acquire object locks in the target repository. By default, *pmrep* waits indefinitely until it acquires locks or you cancel the deployment. To cancel a deployment while *pmrep* is waiting to acquire locks, press Ctrl+C.

Note: You must create the deployment control file manually to use some deployment parameters such as DEPLOYTIMEOUT.

The following is a sample of the depcntl.dtd file:

```
<!ELEMENT DEPLOYPARAMS (DEPLOYFOLDER?, DEPLOYGROUP?)>
<!ATTLIST DEPLOYPARAMS
        DEFAULTSERVERNAME    CDATA      #IMPLIED
        COPYPROGRAMINFO      (YES | NO) "YES"
        COPYMAPVARPERVALS    (YES | NO) "NO"
        RETAINMAPVARPERVALS  (YES | NO) "NO"
        COPYWFLOWVARPERVALS  (YES | NO) "NO"
        COPYWFLOWSESSLOGS    (YES | NO) "NO"
        COPYDEPENDENCY       (YES | NO) "YES"
        LATESTVERSIONONLY    (YES | NO) "NO"
        CHECKIN_COMMENTS     CDATA      #IMPLIED
```

```
        DEPLOYTIMEOUT        CDATA      "-1"
        RETAINGENERATEDVAL   (YES | NO) "YES"
        RETAINSERVERNETVALS  (YES | NO) "YES"
        COPYDEPLOYMENTGROUP  (YES | NO) "NO"
        OVERRIDESERVER       (YES | No) "NO">

<!--criteria specific to deploying folder-->
<!ELEMENT DEPLOYFOLDER (REPLACEFOLDER?, DEPLOYEDFOLDEROWNER?, OVERRIDEFOLDER*)>
<!ATTLIST DEPLOYFOLDER
        NEWFOLDERNAME         CDATA      #IMPLIED>

<!--folder to replace-->
<!ELEMENT REPLACEFOLDER EMPTY>
<!ATTLIST REPLACEFOLDER
        FOLDERNAME            CDATA      #REQUIRED
        RETAINMAPVARPERVALS   (YES | NO) "NO"
        RETAINWFLOWVARPERVALS (YES | NO) "YES"
        RETAINWFLOWSESSLOGS   (YES | NO) "NO"
        MODIFIEDMANUALLY      (YES | NO) "NO"
        RETAINORIGFOLDEROWNER (YES | NO) "NO">

<!--shared folder to override-->
<!ELEMENT OVERRIDEFOLDER EMPTY>
<!ATTLIST OVERRIDEFOLDER
        SOURCEFOLDERNAME    CDATA            #REQUIRED
        SOURCEFOLDERTYPE    (LOCAL | GLOBAL) "LOCAL"
        TARGETFOLDERNAME    CDATA            #REQUIRED
        TARGETFOLDERTYPE    (LOCAL | GLOBAL) "LOCAL"
        MODIFIEDMANUALLY    (YES | NO)     "NO"

<!--criteria specific to deploy deployment group-->
<!ELEMENT DEPLOYGROUP (REPLACEDG?, TARGETDGOWNER?, OVERRIDEFOLDER*, APPLYLABEL?)>
<!ATTLIST DEPLOYGROUP
        CLEARSRCDEPLOYGROUP (YES | NO) "NO">
        NEWDEPLOYGROUPNAME   CDATA  #IMPLIED

<!--labels used to apply on the src objects and deployed objects-->
<!ELEMENT APPLYLABEL EMPTY>
<!ATTLIST APPLYLABEL
        SOURCELABELNAME     CDATA            #IMPLIED
        SOURCEMOVELABEL         (YES | NO)          "NO"
        TARGETLABELNAME     CDATA            #IMPLIED
        TARGETMOVELABEL             (YES | NO)          "NO">

<!-- new owners of deployed folders -->
<!ELEMENT DEPLOYEDFOLDEROWNER EMPTY>
<!ATTLIST DEPLOYEDFOLDEROWNER
        USERNAME         CDATA        #IMPLIED
                    SECURITYDOMAIN   CDATA        #IMPLIED
        GROUPNAME        CDATA #IMPLIED>

<!-- to indicate that a deployment group should be replaced-->
<!ELEMENT REPLACEDG EMPTY>
<!ATTLIST REPLACEDG
        DGNAME          CDATA        #REQUIRED
                    SECURITYDOMAIN   CDATA        #IMPLIED

<!-- new owner of copied deployment group-->
<!ELEMENT TARGETDGOWNER EMPTY>
<!ATTLIST TARGETDGOWNER
        USERNAME         CDATA        #IMPLIED
                    SECURITYDOMAIN   CDATA        #IMPLIED
```

Deployment Control File Parameters

The following table lists *pmrep* deployment control file parameters:

Element	Attribute Name	Attribute Description
DEPLOYPARAMS	DEFAULTSERVERNAME	Required if you use DeployFolder and DeployDeploymentGroup and set OVERRIDESERVER to Yes. Integration Service registered in the target repository to run the deployed workflows. For any deployment, you can specify one Integration Service.
-	COPYPROGRAMINFO	Optional. Copies SAP installed ABAP program.
-	COPYMAPVARPERVALS	Optional. Copies mapping variable persistent values based on the values set for RETAINMAPVARPERVALS. If you do not set COPYMAPVARPERVALS or set its value to No, the RETAINMAPVARPERVALS values are ignored. For more information, see "Persisted Mapping Variables" on page 1401.
-	RETAINMAPVARPERVALS	Optional. Retains mapping variable persistent values in the target based on the values set for COPYMAPVARPERVALS. If you do not set COPYMAPVARPERVALS or set its value to No, the RETAINMAPVARPERVALS values are ignored. For more information, see "Persisted Mapping Variables" on page 1401.
-	COPYWFLOWVARPERVALS	Optional. Copies workflow variable persistent values.
-	COPYWFLOWSESSLOGS	Optional. Copies workflow logs.
-	COPYDEPENDENCY	Optional. Copies dependency information for objects in mappings.
-	COPYDEPLOYMENTGROUP	Optional. Copies the deployment group along with the objects in the deployment group to the target repository.
-	VALIDATETARGETREPOSITORY	Optional. Validates objects in the target repository.
-	LATESTVERSIONONLY	Optional. Copies the latest version.
-	CHECKIN_COMMENTS	Optional. Overrides the default comment and adds a comment in the target repository when you copy or deploy an object. You must set LATESTVERSIONONLY to true to use this attribute.

Element	Attribute Name	Attribute Description
-	DEPLOYTIMEOUT	Optional. Period of time (in seconds) that *pmrep* attempts to acquire locks on objects in the target repository. A value of 0 fails the copy operation immediately if *pmrep* cannot obtain a lock. A value of -1 instructs *pmrep* to wait indefinitely until it acquires locks or the user cancels the operation. Default is -1.
-	RETAINGENERATEDVAL	Optional. Keeps the current value for Sequence Generator or Normalizer transformations.
-	RETAINSERVERNETVALS	Optional. Retains server-network-related values in tasks.
	OVERRIDESERVER	Optional. Use with DEFAULTSERVERNAME.If you set the OVERRIDESERVER value to Yes, the deployment operation assigns the Integration Service name that the DEFAULTSERVERNAME attribute specifies to run the deployed workflows. If the DEFAULTSERVERNAME is not specified or contains an Integration Service name that is not valid, the deployment operation does not assign an Integration Service to the deployed workflows. If you set the OVERRIDESERVER value to No, the deployment operation checks if it can assign an Integration Service to the workflows based on the Integration Service in the source and target repositories. If the same Integration Service name appears in the source and target repositories, the deployment operation assigns the Integration Service name to the deployed workflows. Otherwise, the deployed workflows are not assigned the Integration Service. Default is No.
DEPLOYFOLDER	NEWFOLDERNAME	Optional. Creates a folder with this name.
REPLACEFOLDER	FOLDERNAME	Required if you use DEPLOYFOLDER. Names the folder after replacing it.
-	RETAINMAPVARPERVALS	Optional. Retains mapping variable persistent values in the target.
-	RETAINWFLOWVARPERVALS	Optional. Retains workflow variable persistent values.
-	RETAINWFLOWSESSLOGS	Optional. Retains workflow session logs in the target.

Element	Attribute Name	Attribute Description
-	MODIFIEDMANUALLY	Optional. Compares folders if objects in the target folder have been created or modified since the previous deployment.
-	RETAINORIGFOLDEROWNER	Optional. Retains the existing folder owner. *pmrep* ignores any information provided in the DEPLOYEDFOLDEROWNER element.
OVERRIDEFOLDER	SOURCEFOLDERNAME	Required if you use DeployFolder and DeployDeploymentGroup. If deploying a folder, specifies the current folder that shortcuts point to. If deploying a deployment group, specifies the following folders: - Folder or folders that shortcuts point to - Folder or folders containing the deployment group objects
-	SOURCEFOLDERTYPE	Optional. If deploying a folder, specifies the type of folder that shortcuts point to. Use local or global shortcuts.
-	TARGETFOLDERNAME	Required. If deploying a folder, specifies the folder that shortcuts point to. If deploying a deployment group, specifies the following folders: - Folder or folders that shortcuts point to - Folder or folders containing the deployment group objects
-	TARGETFOLDERTYPE	Optional. If deploying a folder, specifies the type of folder that shortcuts point to. Use local or global shortcuts.
-	MODIFIEDMANUALLY	Optional. Compares folders if objects in the target folder have been created or modified since the previous deployment. Use this attribute only with the DeployDeploymentGroup command.
DEPLOYGROUP	CLEARSRCDEPLOYGROUP	Required if you use DeployDeploymentGroup. Removes objects from the source group after deploying.
-	NEWDEPLOYGROUPNAME	Optional. Creates a deployment group with this name. Ignored if REPLACEDG is specified. Default is the source deployment group name.
REPLACEDG	DGNAME	Optional. Name of the deployment group to be replaced.

Element	Attribute Name	Attribute Description
-	RETAINORIGDGOWNER	Optional. Specifies whether to retain the owner of the deployment group being replaced in the target repository.
TARGETDGOWNER	USERNAME	Optional. Owner of the copied deployment group. Default is the owner of the source deployment group.
-	SECURITYDOMAIN	Optional. Security domain of the target deployment group.
APPLYLABEL	SOURCELABELNAME	Required if you use DeployDeploymentGroup. Applies a label to all the objects in the source group.
-	SOURCEMOVELABEL	Optional. Moves the label from a different version of the object in the source group to the deployment group version of the object. If the Repository Agent detects the label is applied to another version of the same object, you can choose to move the label to the selected version of the object.
-	TARGETLABELNAME	Optional. Applies a label to all the objects deployed to the target repository.
-	TARGETMOVELABEL	Optional. Moves the label from a different version of the object in the target group to the deployment group version of the object. If the Repository Agent detects the label is applied to another version of the same object, you can choose to move the label to the latest version of the object.
DEPLOYEDFOLDEROWNER	USERNAME	Required if you use DeployFolder and DeployDeploymentGroup. Owner of the deployed folder or deployment group in the target repository.
-	SECURITYDOMAIN	Optional. Name of the security domain that the owner of the deployed folder or deployment group belongs to.
-	GROUPNAME	Optional. Group owner of the deployed folder or deployment group in the target repository.

Persisted Mapping Variables

When you deploy a folder or a group, you can copy the values of persisted mapping variables from the source repository to the target repository, retain the values from the target repository, or reset the values.

The following table describes how to configure COPYMAPVARPERVALS and RETAINMAPVARPERVALS to copy, retain, or reset the values of persisted mapping variables:

Deployment Behavior	Configuration
Reset the persisted mapping variable values in the target repository.	Set COPYMAPVARPERVALS to No.
Copies the mapping variable values from the source repository to the target repository.	Set the following parameter file options: - Set COPYMAPVARPERVALS to Yes. - Set RETAINMAPVARPERVALS to No.
Retains the existing persisted mapping variable values in the target repository.	Set the following parameter file options: - Set COPYMAPVARPERVALS to Yes. - Set RETAINMAPVARPERVALS to Yes.

Deployment Control File Examples

The parameters you specify in the deployment control file code determine the actions that occur when you execute the DeployFolder or DeployDeploymentGroup commands in *pmrep*. The following examples discuss instances in which you use the DeployFolder and DeployDeploymentGroup commands with a deployment control file.

Deploying the Latest Version of a Folder

You can deploy the latest version of a folder and include all dependencies. For example, you need to retain the current values in a Sequence Generator transformation, and you need to point the shortcuts from the sc_folder to the new_sc_folder. After you copy the folder, you want to rename it to “new_year.”

You might create a control file with following attributes:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME ="info7261"
  COPYPROGRAMINFO ="NO"
  COPYWFLOWVARPERVALS ="NO"
  COPYWFLOWSESSLOGS ="NO"
  COPYDEPENDENCY ="YES"
  LATESTVERSIONONLY = "NO">

<REPLACEFOLDER FOLDERNAME ="NEW_YEAR"
   RETAINMAPVARPERVALS ="YES"/>

<OVERRIDEFOLDER SOURCEFOLDERNAME ="SC_FOLDER"
   OVERRIDEFOLDERNAME ="NEW_SC_FOLDER"/>

</DEPLOYPARAMS>
```

Deploying the Latest Version of a Deployment Group

You can deploy the latest version of a deployment group and apply a label to the objects in the deployment group. For example, you want to apply the label NEW_SRC_LABEL_NAME to all objects in the source group, and NEW_TGT_LABEL_NAME to all objects in the target group. You might create a control file with following attributes:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.dtd">
```

```
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sunqa2_51880"
   COPYPROGRAMINFO="YES"
   COPYMAPVARPERVALS="YES"
   COPYWFLOWVARPERVALS="YES"
   COPYWFLOWSESSLOGS="NO"
   COPYDEPENDENCY="YES"
   LATESTVERSIONONLY="YES"
   RETAINGENERATEDVAL="YES"
   RETAINSERVERNETVALS="YES">
<DEPLOYGROUP CLEARSRCDEPLOYGROUP="NO">
<OVERRIDEFOLDER SOURCEFOLDERNAME="SRC_FOLDER1"
   SOURCEFOLDERTYPE="LOCAL"
   TARGETFOLDERNAME="TGT_FOLDER1"
   TARGETFOLDERTYPE="LOCAL"/>
               <APPLYLABEL SOURCELABELNAME="NEW_SRC_LABEL_NAME"
   SOURCEMOVELABEL="YES"
   TARGETLABELNAME="NEW_TGT_LABEL_NAME"
   TARGETMOVELABEL="YES" />
</DEPLOYGROUP>
</DEPLOYPARAMS>
```

Listing Multiple Source and Target Folders

Use the OVERRIDEFOLDER element in the control file to list multiple source and target folders. Use the SOURCEFOLDERNAME and TARGETFOLDERNAME attributes to specify the following folders in the source and target repositories:

- The folder or folders that shortcuts point to
- The folder or folders containing the deployment group objects

When you run the *pmrep* command, DeployDeploymentGroup, the deploy process picks the right target folder to use after checking the objects in the deployment group.

For example, if a deployment group contains objects in two folders with shortcuts to a third folder, you can create a control file with three occurrences of OVERRIDEFOLDER. The following sample control file deploys a deployment group that contains objects in the folders OBJECTFOLDER1 and OBJECTFOLDER2 that contain shortcuts pointing to the folder SHAREDSHORTCUT:

```
<!DOCTYPE DEPLOYPARAMS SYSTEM "depcntl.dtd">
<DEPLOYPARAMS DEFAULTSERVERNAME="dg_sun_71099"
   COPYPROGRAMINFO="YES"
   COPYMAPVARPERVALS="YES"
   COPYWFLOWVARPERVALS="YES"
   COPYWFLOWSESSLOGS="NO"
   COPYDEPENDENCY="YES"
   LATESTVERSIONONLY="YES"
   RETAINGENERATEDVAL="YES"
   RETAINSERVERNETVALS="YES">
<DEPLOYGROUP CLEARSRCDEPLOYGROUP="NO">
<OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER1"
   SOURCEFOLDERTYPE="LOCAL"
   TARGETFOLDERNAME="OBJECTFOLDER1"
   TARGETFOLDERTYPE="LOCAL"/>
<OVERRIDEFOLDER SOURCEFOLDERNAME="OBJECTFOLDER2"
   SOURCEFOLDERTYPE="LOCAL"
   TARGETFOLDERNAME="OBJECTFOLDER2"
   TARGETFOLDERTYPE="LOCAL"/>
<OVERRIDEFOLDER SOURCEFOLDERNAME="SHAREDSHORTCUTS"
   SOURCEFOLDERTYPE="GLOBAL"
   TARGETFOLDERNAME="SHAREDSHORTCUTS"
   TARGETFOLDERTYPE="GLOBAL"/>
</DEPLOYGROUP>
</DEPLOYPARAMS>
```

Tips for Working with pmrep Files

Use the -n option when you use the *pmrep* commands Updatesrcprefix or Updatetargprefix.

When you include the -n option, you must enter the name of the source or target instance for the -t option. The source or target instance name must match the name displayed in the session properties or the name output by the Listtablesbysess command.

Use the -n option to use the Listtablesbysess command with the Updatesrcprefix or Updatetargprefix commands in a shell script if the source and target instance names match. Also, use the -n option to update a source even if the session uses a shortcut to a mapping.

When using the *pmrep* command ListObjects, enter a character or set of characters that is not used in repository object names for the column separator, end of record indicator, and end of listing indicator.

When you enter characters to separate records and columns, and to indicate the end of the listing, use characters that are not included in repository object names. This helps you use a shell script to parse the object metadata.

In *pmrep*, use the -v option when restoring a repository that uses an external directory service for user management.

When you include the -v option with Restore, you can retain the external directory service registration for the repository. If you do not enter this option with the valid administrator user name and password, the restored repository defaults to repository authentication mode and you lose the association between login names and user names.

INDEX

A

B

C

D

E

F

G

H

I

M

N

O

P

Q

R

S

T

U

V

W

X