Informatica®
10.2

Metadata Manager Command Reference

Informatica Metadata Manager Command Reference
10.2
September 2017

Publication Date: 2018-06-18

Table of Contents

Preface

The *Metadata Manager Command Reference* provides information about Metadata Manager command line programs. This guide is written for Metadata Manager administrators who use command line programs to load and manage resources, back up and restore the repository, and migrate resources across Metadata Manager versions.

Informatica Resources

Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit https://network.informatica.com.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- 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 search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.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

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

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

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access 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. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access 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 augment, extend, or enhance your Informatica implementations. By leveraging any of the hundreds of solutions from Informatica developers and partners, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.

CHAPTER 1

mmcmd

This chapter includes the following topics:

mmcmd Overview

mmcmd is a command line program that loads and manages resources, imports and exports models and custom resources, creates and deletes Metadata Manager repository contents, and restores PowerCenter® repository contents.

mmcmd is installed when you run the Informatica services installer or the Informatica client installer. You can also install mmcmd on any machine when you install Informatica utilities. mmcmd is installed as a batch file on Windows and as a shell script on UNIX.

mmcmd is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\mmcmd`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\mmcmd`
- `<Informatica utilities installation directory>\MetadataManager\utilities\mmcmd`

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

Use mmcmd in the following modes:

Command Line Mode

You invoke and exit mmcmd each time you issue a command. You can write scripts with the command line syntax. Each command that you write in command line mode must include connection information to the Metadata Manager Service.

Interactive Mode

You establish and maintain an active connection to the Metadata Manager Service. In interactive mode, you can issue a series of commands. To start interactive mode, enter `mmcmd` at the command line. To exit interactive mode, use the exit command.

Certificate Validation for mmcmd

If you configure a secure connection between the Metadata Manager web application and the Metadata Manager Service, you must configure mmcmd to use the truststore file. mmcmd uses the truststore file to validate the security certificates. mmcmd does not accept a security certificate that has errors.

To configure mmcmd to use the truststore file, edit the MMCmdConfig.properties file. Set the TrustStore.Path property to the path and file name of the truststore file.

If you do not configure a secure connection for the Metadata Manager web application, do not specify a truststore file. Leave the TrustStore.Path property in the MMCmdConfig.properties file empty.

MMCmdConfig.properties File

Use the MMCmdConfig.properties file to configure mmcmd properties such as the truststore file, server polling interval, and server connection timeout period.

MMCmdConfig.properties is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\mmcmd\config`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\mmcmd\config`
- `<Informatica utilities installation directory>\MetadataManager\utilities\mmcmd\config`

Note: There are separate copies of the MMCmdConfig.properties file for mmcmd and for mmRepoCmd.

You can configure the following properties:

TrustStore.Path

Required if you configure a secure connection for the Metadata Manager web application. Path and file name of the truststore file that contains the public key.

If you do not configure a secure connection for the Metadata Manager web application, leave this property empty.

Server.PollInterval

Amount of time in milliseconds that the command line program waits before querying the Metadata Manager application. The program queries for the status of the last command when you run a command in wait mode. Default is 6000.

Server.ConnectionTimeOut

Number of milliseconds after which the remote connection to the Metadata Manager Service times out. Default is 86,400,000 (24 hours).

Running Commands

When you run mmcmd, 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 starts a resource load for the Oracle_DB resource:

```
mmcmd load -url http://localhost:10250 -r Oracle_DB -u dave -pw ******
```

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

1. At the command prompt, switch to the directory where mmcmd is located.
2. Enter `mmcmd` on Windows or `mmcmd.sh` on UNIX followed by the command name and its required options and arguments.

   For example:

   ```
   mmcmd(.sh) command_name [-option1] argument_1 [-option2] argument_2...
   ```

   The command names are not case sensitive.

mmcmd Commands

The following table describes the mmcmd commands:

Command Name	Description
assignConnection	Configures connection assignments for a resource based on the properties in the specified resource configuration file.
assignParameterFile	Assigns parameter files to PowerCenter workflows for a PowerCenter resource based on the properties in the specified resource configuration file.
backupConfiguration	Backs up the resource configurations, source files associated with resources, linking rules associated with resources, and custom models for a Metadata Manager instance.
cancel	Cancels a resource load.
connect	Connects the mmcmd program to the Metadata Manager Service in the interactive mode.
createLinkRuleSet	Creates a linking rule set for a pair of resources, a rule set definition for a pair of models, or a rule set parameter definition for a pair of resources in the Metadata Manager repository.
createLoadTemplate	Creates a load template file.

Command Name	Description
createResource	Creates a resource based on the properties in the specified resource configuration file.
deleteLinkRuleSet	Removes a linking rule set for a pair of resources or a rule set definition for a pair of models from the Metadata Manager repository.
deleteLoadTemplate	Deletes a load template.
deleteResource	Deletes the resource and all metadata for the resource from the Metadata Manager repository.
encrypt	Encrypts the text you specify. You can specify the encrypted text when you use the -ep option in a command or in a resource configuration file.
exit	In interactive mode, disconnects mmcmd from the Metadata Manager Service and closes the mmcmd program
export	Exports a custom resource from the Metadata Manager repository to an XML file. You can import it into another Metadata Manager repository.
exportLinkRuleSetDefs	Exports all linking rule set definitions for a model to XML files.
exportLinkRuleSets	Exports all linking rule sets for a resource to XML files.
exportLoadLog	Exports the load details for a resource to a Microsoft Excel file.
exportModel	Exports a model from the Metadata Manager repository. You can import it into another Metadata Manager repository.
exportObject	Exports a metadata catalog object from the Metadata Manager repository. You can export metadata objects to the Adobe PDF, HTML, or Microsoft Excel file types.
generateDefaultLoadTemplate	Generates a default load template to load all top level classes for the specified model.
getLinkReport	Exports the link report. The link summary report contains the resource, connection, assigned database, and assigned schema details.
geLoadTemplate	Exports a load template file.
getResource	Writes properties for the specified resource to a resource configuration file.
getResourceFiles	Retrieves all the source files associated with a resource, including rule sets. Metadata Manager retrieves parameter files for PowerCenter resources and retrieves model files for data modeling resources.
getServiceLog	Exports the service log file from Metadata Manager for a specified date.
help	Returns help for an mmcmd command.
import	Imports the metadata for a custom resource from an XML file into the Metadata Manager repository.
importLinkRuleSets	Imports all linking rule sets from XML files in the specified path into the Metadata Manager repository.

Command Name	Description
importModel	Imports a model from a file into the Metadata Manager repository.
link	Creates the links between resources to run data lineage analysis across metadata sources. Before you create links for a resource, you must configure connection assignments or linking rules for the resource.
listLoadTemplates	Lists all the load template files for a custom resource.
listModels	Lists all models in Metadata Manager.
listResources	Lists all resources in the Metadata Manager repository.
load	Starts a resource load. Metadata Manager adds the resource load to the load queue.
migrateBGLinks	Restores the related catalog objects for a business glossary after you upgrade from version 9.5.x.
purgeMetadata	Deletes metadata for a resource from the Metadata Manager repository. You cannot recover the purged metadata. Back up the Metadata Manager repository database before you purge metadata.
restoreConfiguration	Restores the resource configurations, source files associated with resources, linking rules associated with resources, and custom models from a back-up file.
resume	Resume a failed resource load. If a resource load fails when PowerCenter runs the workflows that load the metadata into the warehouse, you can resume the resource load.
search	Searches for objects in the Metadata Manager repository using a keyword search.
status	View the status of a running or completed resource load.
testSourceConnection	Tests connection to the source system of a resource.
updateLinkRuleSet	Updates a linking rule set for a pair of resources or a rule set definition for a pair of models in the Metadata Manager repository.
updateLoadTemplate	Updates a load template file.
updateResource	Updates a resource based on the properties in the specified resource configuration file.
version	Displays the current version of Metadata Manager.

assignConnection

Configures connection assignments for a resource based on the properties in the specified resource configuration file. Connection assignments are connections between two metadata sources. Metadata Manager uses connections to run data lineage across metadata sources.

Use the assignConnection command when you move resources from a development to a production environment. After you create a resource based on a resource configuration file, you might need to change

the connection assignments in the resource configuration file. You then use the assignConnection command to update the resource with the modified connection assignments.

assignConnection Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-rcf|--resourceConfigurationFile> resourceConfigurationFile>
[-s|--skipConFetch]
[<-pdir> paramFileDir]
```

assignConnection Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to configure connections. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

XML file name and path for the resource configuration file that contains the modified connection assignments. If you do not include a path, mmcmd looks for the XML file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify the path, mmcmd looks for the sources files in the mmcmd directory.

[-s | --skipConFetch]

During refresh, skips retrieving the connection objects you specify in the resource configuration file.

Before you use this option, verify that the connection object is available so that the connection assignment does not fail.

[<-pdir>]

Directory where the source files of the Metadata Manager resources are stored.

assignParameterFile

Assigns parameter files to PowerCenter workflows for a PowerCenter resource based on the properties in the specified resource configuration file.

Use the assignParameterFile command when you move PowerCenter resources from a development to a production environment. After you create a PowerCenter resource based on a resource configuration file, you might need to change the PowerCenter parameter file assignments in the resource configuration file. You

then use the assignParameterFile command to update the resource with the modified parameter file assignments.

assignParameterFile Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-rcf|--resourceConfigurationFile> resourceConfigurationFile>
[<-pdir> paramFileDir]
```

assignParameterFile Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the PowerCenter resource for which you want to configure PowerCenter parameter files. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

XML file name and path for the resource configuration file that contains the modified PowerCenter parameter file assignments. If you do not include a path, mmcmd looks for the XML file in the mmcmd directory.

The parameter files must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If not specified, mmcmd looks for the parameter files in the mmcmd directory.

[<-pdir>]

Directory where the parameter files of the PowerCenter resource are stored.

backupConfiguration

Backs up the resource configurations, source files associated with resources, linking rules associated with resources, and custom models for a Metadata Manager instance.

backupConfiguration Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
```

```
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-file> .cbkp File>
```

backupConfiguration Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>

Path and file name of the back-up file. If you do not specify a .cbkp extension, mmcmd appends ".cbkp" to the file name. If you do not include a path, mmcmd saves the back-up file in the mmcmd directory.

cancel

Cancels a resource load.

cancel Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

cancel Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the resource for which you want to cancel the load. If the resource name contains spaces, enclose the resource name in quotes.

connect

Connects the mmcmd program to the Metadata Manager Service in the interactive mode. After mmcmd successfully connects, you can issue commands without reentering the connection information.

connect Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
```

connect Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

createLinkRuleSet

Creates a linking rule set for a pair of resources, a rule set definition for a pair of models, or a rule set parameter definition for a pair of resources in the Metadata Manager repository. Creates the rule set, rule set definition, or rule set parameter definition based on a linking rules file.

createLinkRuleSet Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-file> rule set xml|rule set definition xml|rule set parameter xml>
```

createLinkRuleSet Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>

XML file name and path for the linking rules file that you use to create the rule set, the rule set definition, or the rule set parameter definition.

If you specify a rule set file, this command creates a rule set for the resources named in the file. If you specify a rule set definition file, this command creates a rule set definition for the models named in the file. If you specify a rule set parameter file, this command creates a rule set for the resources named in the file when a rule set definition exists for the models.

Default path is the mmcmd directory.

createLoadTemplate

Creates a load template file.

createLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-f|--File> File>
```

createLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --file>>

Name of the load template file.

createResource

Creates a resource based on the properties in the specified resource configuration file. Use the createResource command when you move resources from a development to a production environment.

createResource Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
```

```
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-rcf|--resourceConfigurationFile> resourceConfigurationFile>
[<-pdir> paramFileDir]
[<-rpw|--resourcePassword> resourcePassword]
[<-sjp|--secureJDBCParameters> secureJDBCParameters]
```

createResource Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource that you want to create. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

File name and path for the resource configuration file that contains the resource properties. You can import a resource configuration file (.rcf file). Alternatively, you can import a resource configuration file that also contains all the rule sets and rule set parameter definitions associated with the resource (.rcz file). If you do not include a path, mmcmd looks for the file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify a path, mmcmd looks for the source files in the mmcmd directory.

[<-pdir>]

Directory where Metadata Manager stores the source files for the resources.

[<-rpw | --resourcePassword>]

Required if the resource uses a password and the resource configuration file does not contain the resource password. Resource password in plain text.

[<-sjp | --secureJDBCParameters>]

Secure JDBC parameters that you want to append to the JDBC connection URL. Use this option with database management resources to specify secure connection parameters such as passwords. Metadata Manager does not display secure parameters or parameter values in the resource configuration properties. Enter the parameters as name=value pairs separated by the delimiter character that the database driver requires.

If secure communication is enabled for the metadata source database, enter the secure JDBC parameters in this option.

deleteLinkRuleSet

Removes a linking rule set for a pair of resources or a rule set definition for a pair of models from the Metadata Manager repository.

deleteLinkRuleSet Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-rn|--rule set id|rule set definition id|rule set parameter id> string>
[-force]
```

deleteLinkRuleSet Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-rn | --rule set id|rule set definition id|rule set parameter id>>

Name of the rule set or rule set definition that you want to delete. If you delete a rule set for a resource by removing the rule set parameter definition, this option specifies the ID of the rule set parameter definition.

[-force]

Deletes the rule set definition and all parameters associated with it. If you delete a rule set definition that has parameters associated with it, specify this option to delete the rule set definition.

deleteLoadTemplate

Deletes a load template file.

deleteLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-na|--Name> Name>
```

deleteLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-na | --Name>>

Name of the load template file.

deleteResource

Deletes the resource and all metadata for the resource from the Metadata Manager repository.

deleteResource Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[-f]
```

deleteResource Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource that you want to delete. If the resource name contains spaces, enclose the resource name in quotes.

[-f]

Delete the resource without confirmation. If you omit this option, the command prompts you for confirmation before it deletes the resource.

encrypt

Encrypts the text that you specify. Specify text to encrypt when you use the --encryptedPassword (-ep) option in a command and when you use the password parameter in a resource configuration file.

The command generates and displays the encrypted data. The command uses the Informatica default encryption key to encrypt data.

encrypt Syntax

The command uses the following syntax:

```
<<-data> data>
```

encrypt Options

The command uses the following options:

<<-data>>

Text that you want to encrypt.

exit

Disconnects mmcmd from the Metadata Manager Service and closes the mmcmd program.

Note: Use this command in the mmcmd interactive mode only.

export

Exports a custom resource from the Metadata Manager repository to an XML file. You can import it into another Metadata Manager repository.

export Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-f|--file> file>
```

export Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the custom resource that you want to export. If the name contains spaces, enclose the name in quotes.

<<-f | --file>>

XML file name and path for the exported custom resource. If you do not include a path, mmcmd exports the custom resource to an XML file in the mmcmd directory.

exportLinkRuleSetDefs

Exports all linking rule set definitions for a model to XML files. You can import the rule set definitions into another Metadata Manager repository.

exportLinkRuleSetDefs Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-m|--model> Model Name>
<<-d|--dir> Export Directory>
[-o|--overwrite]
```

exportLinkRuleSetDefs Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-m | --model>>

Name of the model that uses the rule set definitions you want to export.

<<-d | --dir>>

Directory to which you want to export the rule set definition files.

[-o | --overwrite]

Overwrites existing rule set definition files during export.

exportLinkRuleSets

Exports all linking rule sets for a resource to XML files. Optionally exports the rule set parameter definitions associated with the resource. You can import the rule sets and rule set parameter definitions into another Metadata Manager repository.

exportLinkRuleSets Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> Resource Name>
<<-d|--dir> Export Directory>
[-o|--overwrite]
[-includeDefs]
```

exportLinkRuleSets Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the resource that uses the rule sets you want to export.

<<-d | --dir>>

Directory to which you want to export the rule set files.

[-o | --overwrite]

Overwrites existing rule set files during export.

[-includeDefs]

Exports the rule set parameter definitions in addition to the rule set definitions.

exportLoadLog

Exports the load details for a resource to a Microsoft Excel file.

exportLoadLog Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-s|--severity> info|warn|error>
<<-f|--file> file>
```

exportLoadLog Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the resource for which you want to export the load log information.

<<-s | --severity>>

Error severity level.

Specify one of the following levels:

- info. Metadata Manager writes informational, warning, and error messages to the log file.
- warn. Metadata Manager writes warning and error messages to the log file.
- error. Metadata Manager writes error messages to the log file.

<<-f | --file>>

File name and path of the Microsoft Excel file to which you want to export the load details. You must specify a file with the .xlsx extension. If you do not specify a path, Metadata Manager creates the file in the mmcmd directory.

exportModel

Exports a model from the Metadata Manager repository to a file. You can import the file into another Metadata Manager repository.

Note: You cannot export the Business Glossary model from Metadata Manager. To export business glossary assets and templates, use the Analyst tool.

exportModel Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-m|--modelName> modelName>
<<-f|--file> file>
[-includeRuleSets]
```

exportModel Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-m | --modelName>>

Name of the model you want to export. If the model name contains spaces, enclose the model name in quotes.

You can export a packaged model, a universal model, a custom model, or multiple custom models to one export file. You cannot export a packaged model and a custom model to one export file. Similarly, you cannot export a universal model and a custom model to one export file.

<<-f | --file>>

File name and path for the model export file. If you do not include a path, mmcmd exports the model to a file in the mmcmd directory.

[-includeRuleSets]

Exports all rule set definitions associated with the model. If you specify this option, the exportModel command creates a zip file that contains the model export XML file plus an XML file for each rule set definition. If you do not specify this option, the exportModel command creates an XML file.

exportObject

Exports a metadata catalog object from the Metadata Manager repository.

You can export the metadata object to the following file types:

- Adobe PDF
- HTML
- Microsoft Excel

Note: The include options are not applicable for all metadata catalog objects. If you use an include option that is not applicable for the selected metadata object, mmcmd ignores the option.

exportObject Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-l|--location> location>
<<-f|--file> file>
[-includeChildren]
[-includeBasicProperties]
[-includeAdvancedProperties]
[-includeComments]
[-includeAssociations]
[-includeLinks]
[-includeBusinessTerms]
[-includeCategories]
```

```
[-includeImpactUpstream]
[-includeImpactDownstream]
```

exportObject Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-l | --location>>

Name and location of the metadata object in the catalog hierarchy that you want to export.

<<-f | --file>>

PDF, HTML, or XLS file name and path for the exported metadata object. If you do not include a path, mmcmd exports the metadata object to a file in the mmcmd directory.

[-includeChildren]

Includes the object you selected and its child objects in the exported file.

[-includeBasicProperties]

Includes basic object properties in the exported file.

[-includeAdvancedProperties]

Includes advanced object properties in the exported file.

[-includeComments]

Includes comments on the object in the exported file.

[-includeAssociations]

Includes related catalog objects for the object in the exported file.

[-includeLinks]

Includes links for the object in the exported file.

[-includeBusinessTerms]

Includes related business terms for the object in the exported file.

[-includeCategories]

Includes related categories for the object in the exported file.

[-includeImpactUpstream]

Includes objects that the selected metadata object is impacted by in the exported file.

[-includeImpactDownstream]

Includes objects that the selected metadata object impacts in the exported file.

generateDefaultLoadTemplate

Generates a default load template to load all top level classes for the specified model.

generateDefaultLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-m|--modelName> Name>
<<-out|--outputDirectory> Name>
```

generateDefaultLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-m | --modelName>>

Name of the model associated with the custom resource.

<<-out | --outputDirectory>>

Directory where the default load template file is saved.

getLinkReport

Exports the link summary report. The link summary report contains the resource, connection, assigned database, and assigned schema details.

getLinkReport Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-f|--file> file>
```

getLinkReport Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to the get link report.

<<-f | --file>>

Name of the file to which you want to export the link details.

getLoadTemplate

Exports a load template file.

getLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-na|--Name> Name>
<<-f|--File> File>
```

getLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-na | --Name>>

Name of the model associated with the custom resource.

<<-f | --File>>

Name of the file to which you want to export the load template details.

getResource

Writes properties for the specified resource to a resource configuration file. Use the getResource command when you move resources from a development to a production environment.

By default, the command writes all properties except the resource password to the resource configuration file. Optionally, you can include the resource password in the file.

getResource Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-rcf|--resourceConfigurationFile> resourceConfigurationFile>
[-includeRuleSets]
[-includeFiles]
[-includePassword]
```

getResource Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource whose properties you want to write to a configuration file. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

XML file name and path to which Metadata Manager writes the resource properties. Creates a file with the .rcf extension. If you do not include a path, mmcmd writes the XML file in the mmcmd directory.

[-includeRuleSets]

Exports the resource configuration file with all rule sets and rule set parameter definitions associated with the resource. Creates a file with the .rcz extension instead of the .rcf extension.

[-includeFiles]

Exports the resource configuration file with PowerCenter parameter files and all other files that you upload and associate with the resource except for rule sets.

[-includePassword]

Includes the encrypted resource password in the resource configuration file.

getResourceFiles

Retrieves all the source files associated with a resource, including rule sets. Metadata Manager retrieves parameter files for PowerCenter resources and retrieves model files for data modeling resources.

getResourceFiles Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[<-destDir> destDir]
```

getResourceFiles Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to retrieve the source files.

[<-destDir>]

Directory where the source files of the resource are stored. If not specified, the source files are saved in the current directory.

getServiceLog

Exports the service log file from Metadata Manager for a specified date.

getServiceLog Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-dt|--date> yyyy-mm-dd]
<<-f|--file> file>
```

getServiceLog Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<-dt | --date>]

Date of the service log details that you want to export. Format must be yyyy-mm-dd.

<<-f | --file>>

Name of the file to which you want to export the service log details.

help

Returns help for an mmcmd command.

help Syntax

The command uses the following syntax:

```
help [Operation]
```

help Options

The command uses the following options:

[Operation]

Name of the command for which you want to view the syntax. If you omit the operation, mmcmd returns the syntax for all mmcmd commands.

import

Imports the metadata for a custom resource from an XML file into the Metadata Manager repository.

Use import to import a custom resource into the Metadata Manager repository that you exported from another Metadata Manager repository. The import command imports the custom resource metadata, but it does not create the resource.

import Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-f|--file> file>
```

import Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --file>>

XML file name and path for the custom resource that you want to import. If you do not include a path, mmcmd assumes the file is in the mmcmd directory.

importLinkRuleSets

Imports all linking rule sets from XML files in the specified path into the Metadata Manager repository. Use importlinkrulesets to import rule sets into the Metadata Manager repository that you exported from another Metadata Manager repository.

importLinkRuleSets Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-d|--dir> Import Directory>
[-up|--update]
```

importLinkRuleSets Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-d | --dir>>

Directory from which you want to import the rule set files.

[-up | --update]

Updates an existing rule set during import.

importModel

Imports a model from a file into the Metadata Manager repository. Use importModel to import a model into the Metadata Manager repository that you exported from another Metadata Manager repository.

Note: You cannot import a Business Glossary model in Metadata Manager. To import business glossary assets and templates, use the Analyst tool.

importModel Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[<-m|--modelName> modelName]
<<-f|--file> file>
```

importModel Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[<-m | --modelName>]

Name of the model in the XML file that you want to import. If the model name contains spaces, enclose the model name in quotes. For example, "My Model." If you do not include a model name, mmcmd imports all models in the XML file.

<<-f | --file>>

File name and path for the model export file that you want to import. The file can be a model export XML file or a zip file that contains the model XML file plus the associated rule set definitions. If you do not include a path, mmcmd assumes the file is located in the mmcmd directory.

link

Creates the links between resources that share a connection assignment to run data lineage analysis across metadata sources.

Before you create links for a resource, you must configure connection assignments for the resource.

link Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[-wait]
[-sf|--skipFilter]
```

link Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to create links. If the resource name contains spaces, enclose the resource name in quotes.

[-wait]

Causes mmcmd to wait for the command to complete before returning the command prompt.

[-sf | --skipFilter]

Skips filtering of connection assignments during linking.

listLoadTemplates

Lists all of the load template files for a model.

listLoadTemplates Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-m|--modelName> Name>
```

listLoadTemplates Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-m | --modelName>>

Name of the model for which you want to list load templates.

listModels

Lists all models in Metadata Manager.

listModels Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[-c|--custom]
```

listModels Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-c | --custom]

Lists all custom models. If you do not specify this option, Metadata Manager lists all models.

listResources

Lists all resources in the Metadata Manager repository.

listResources Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
```

```
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
```

listResources Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

load

Starts a resource load.

Metadata Manager adds the resource load to the load queue. You can view the status of the resource load using the mmcmd status command or in the Metadata Manager **Load** tab. When you run the load command, mmcmd returns the current status of the load and the time that the load started.

load Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[-wait]
```

load Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource that you want to load. If the resource name contains spaces, enclose the resource name in quotes.

[-wait]

Causes mmcmd to wait for the command to complete before returning the command prompt.

migrateBGLinks

Restores the related catalog objects for a business glossary after you upgrade from version 9.5.x.

When you upgrade business glossaries, you perform the following tasks:

1. Export a business glossary from the previous version of Metadata Manager.
2. Import the business glossary into the Analyst tool.
3. Create and load the Business Glossary resource in the current version of Metadata Manager.

This command runs automatically when you load a Business Glossary resource. When this command runs, the load details show the following messages:

```
<date, time>: Task started: Linking and BG links migration
    <date, time>: BG links migration started…
    <date, time>: BG links migration succeeded
    <date, time>: Task handled successfully: Linking and BG links migration
```

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

For more information about upgrading business glossaries, see the *Upgrading from Version 9.5.0* or *Upgrading from Version 9.5.1* guide.

migrateBGLinks Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-g|--Glossary> Glossary>
```

migrateBGLinks Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-g | --Glossary>>

Name of the business glossary for which you want to restore related catalog objects after upgrade.

purgeMetadata

Deletes metadata for a resource from the Metadata Manager repository. You cannot recover the purged metadata. Back up the Metadata Manager repository database before you purge metadata.

After you purge a resource, you can optimize the index to free disk space used by the indexing files.

purgeMetadata Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
[-wait]
```

purgeMetadata Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to purge metadata. If the resource name contains spaces, enclose the resource name in quotes.

[-wait]

Causes mmcmd to wait for the command to complete before returning the command prompt.

restoreConfiguration

Restores the resource configurations, source files associated with resources, linking rules associated with resources, and custom models from a back-up file.

restoreConfiguration Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-file> file>
[<-pdir> paramFileDir]
```

restoreConfiguration Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>

File name and path of the back-up file.

[<-pdir>]

Directory where the source files of the Metadata Manager resources are stored. If not specified, the source files that are saved in the backup are used.

resume

Resumes a failed resource load.

If a resource load fails when PowerCenter runs the workflows that load the metadata into the warehouse, you can resume the resource load. When you run the resume command, mmcmd returns the current status of the load and the time that the load resumed.

resume Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

resume Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to resume the load. If the resource name contains spaces, enclose the resource name in quotes.

search

Searches for objects in the Metadata Manager repository using a keyword search.

Perform a keyword search to search all properties of objects that match the keyword. mmcmd displays the results of the search in the command prompt. The search results list the locations of all objects that match the search criteria.

search Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-arg|--argument> argument>
```

search Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-arg | --argument>>

Keyword to search for. You can use search operators and wildcard characters in a keyword search.

status

Displays the status of a running or completed resource load. When you run the status command, mmcmd returns the current status of the load and the time that you ran the command.

status Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

status Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to view the status. If the resource name contains spaces, enclose the resource name in quotes.

testSourceConnection

Tests connection to the source system of a resource.

testSourceConnection Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
```

testSourceConnection Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource for which you want to test source connections.

updateLinkRuleSet

Updates a linking rule set for a pair of resources or a rule set definition for a pair of models in the Metadata Manager repository. Updates the rule set or rule set definition based on a linking rules file. If the rule set or rule set definition does not exist, this command creates it.

updateLinkRuleSet Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-file> rule set xml|rule set definition xml|rule set parameter xml>
```

updateLinkRuleSet Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-file>>

XML file name and path for the linking rules file that you use to update the rule set, the rule set definition, or the rule set parameter definition.

If you specify a rule set file, this command updates the rule set for the resources named in the file. If you specify a rule set definition file, this command updates the rule set definition for the models named in the file. If you specify a rule set parameter file, this command updates the rule set for the resources named in the file when a rule set definition exists for the models.

Default path is the mmcmd directory.

updateLoadTemplate

Updates a load template file.

updateLoadTemplate Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-f|--File> File>
```

updateLoadTemplate Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --File>>

Name of the load template file that you want to update.

updateResource

Updates a resource based on the properties in the specified resource configuration file.

Use the updateResource command when you move resources from a development to a production environment. After you create a resource based on a resource configuration file, you might need to change the properties in the resource configuration file. Use the updateResource command to update the resource with the modified properties.

updateResource Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-r|--resource> resource>
<<-rcf|--resourceConfigurationFile> resourceConfigurationFile>
[<-pdir> paramFileDir]
[<-rpw|--resourcePassword> resourcePassword]
[<-sjp|--secureJDBCParameters> secureJDBCParameters]
```

updateResource Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-r | --resource>>

Name of the Metadata Manager resource that you want to update. If the resource name contains spaces, enclose the resource name in quotes.

<<-rcf | --resourceConfigurationFile>>

File name and path for the resource configuration file that contains the modified resource properties. You can import a resource configuration file (.rcf file). Alternatively, you can import a resource configuration file that also contains all the rule sets and rule set parameter definitions associated with the resource (.rcz file). If you do not include a path, mmcmd looks for the file in the mmcmd directory.

The source files of the resource must be in the directory specified in the resource configuration file or in the directory specified using the -pdir option. If you do not specify a path, mmcmd looks for the source files in the mmcmd directory.

[<-pdir>]

Directory where the source files of the Metadata Manager resources are stored.

[<-rpw | --resourcePassword>]

Required if the resource uses a password and the resource configuration file does not contain the resource password. Resource password in plain text.

[<-sjp | --secureJDBCParameters>]

Secure JDBC parameters that you want to append to the JDBC connection URL. Use this option with database management resources to specify secure connection parameters such as passwords. Metadata Manager does not display secure parameters or parameter values in the resource configuration properties. Enter the parameters as name=value pairs separated by the delimiter character that the database driver requires.

If secure communication is enabled for the metadata source database, enter the secure JDBC parameters in this option.

version

Displays the current version of Metadata Manager.

CHAPTER 2

mmLineageMigrator

This chapter includes the following topics:

mmLineageMigrator Overview

mmLineageMigrator is a command line program that migrates data lineage linking information after you upgrade from Metadata Manager 9.6.x to the current version. mmLineageMigrator migrates data lineage linking information from the Metadata Manager repository to the data lineage graph database.

mmLineageMigrator reads data lineage linking information from the Metadata Manager repository, creates a file-based graph database to store the information, and then copies the information to the graph database. The program creates the graph database files in the Metadata Manager lineage graph location that you specify. mmLineageMigrator does not change any table or view in the Metadata Manager repository.

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.

Running mmLineageMigrator

You run mmLineageMigrator from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, mmLineageMigrator is a batch file with a .bat extension. On UNIX, mmLineageMigrator is a script file with a .sh extension.

mmLineageMigrator is located in the following directory:

```
<Informatica services installation directory>\services\MetadataManagerService\utilities
\mmLineageMigrator
```

mmLineageMigrator is not installed with the Informatica client or with the Informatica command line utilities.

1. Disable the Metadata Manager Service.
2. At a command prompt, navigate to the directory where mmLineageMigrator is located.

3. Enter `mmLineageMigrator` on Windows or `mmLineageMigrator.sh` on UNIX followed by the required options and arguments.
4. When the migration finishes, restart the Metadata Manager Service.

mmLineageMigrator Syntax

mmLineageMigrator options and arguments specify connection information for the Metadata Manager repository database and the Metadata Manager lineage graph location.

mmLineageMigrator uses the following syntax:

```
mmLineageMigrator.bat
 <<-dt|--DatabaseType> databaseType>
 <<-du|--DatabaseUserName> databaseUserName>
 <<-gd|--GraphDir> graphDirectory>
 <<-dp|--DatabasePassword> databasePassword>
 <<-url|--DbUrl> databaseURL>
 [-h|--help]
```

mmLineageMigrator Options

mmLineageMigrator uses the following options:

<<-dt>>

Database type for the Metadata Manager repository database.

Specify one of the following types:

- `DB2`
- `ORACLE`
- `SQLSERVER`

<<-du>>

Database user name for the Metadata Manager repository database.

<<-gd>>

Directory where the program creates the graph database files. Must match the Metadata Manager lineage graph location that you configure for the Metadata Manager Service in the Administrator tool. If the directory contains spaces, enclose it in double quotes.

<<-dp>>

Password for the Metadata Manager repository database user.

<<-url>>

JDBC URL for the Metadata Manager repository database.

The syntax depends on the repository database type:

- For IBM DB2, use the following syntax:

  ```
  "jdbc:informatica:db2://[host name]:[port];DatabaseName=[database name]"
  ```

- For Microsoft SQL Server, use the following syntax:

  ```
  "jdbc:informatica:sqlserver://[host name]:
  [port];SelectMethod=cursor;DatabaseName=[database name]"
  ```

  To authenticate the database user credentials using Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, append `;AuthenticationMethod=ntlm` to the URL.

  When you use a trusted connection to connect to a Microsoft SQL Server database, the Metadata Manager Service connects to the repository with the credentials of the user logged in to the machine on which the service is running.

  If you run the program from a machine on which Informatica is not installed, configure the PATH variable to point to the location of the DDJDBCAuth04.dll file.

- For Oracle, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host name]:[port];SID=[sid]"
  ```

  You can enter the SID or use the full service name. For example:

  ```
  "jdbc:informatica:oracle://[host name]:[port];ServiceName=[service name]"
  ```

  If the Oracle database is clustered, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host1]:[port];ServiceName=[service
  name];AlternateServers = ([host2]:[port]);LoadBalancing=true"
  ```

  If the Oracle database uses the Advanced Security Option, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host name]:
  [port];SID=[SID];EncryptionLevel=[encryption level];EncryptionTypes=[encryption
  types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data
  integrity types]"
  ```

Note: If secure communication is enabled for the Metadata Manager repository database, you must append additional JDBC parameters to the JDBC URL.

[-h]

Displays help for the mmLineageMigrator command line program. The help option lists the mmLineageMigrator options and arguments.

JDBC Parameters for Secure Databases

If the Metadata Manager repository database uses a secure connection to communicate with external components, you must append additional parameters to the JDBC URL.

Append the following parameters to the URL:

```
;EncryptionMethod=SSL;TrustStore=<truststore
location>;TrustStorePassword=<password>;HostNameInCertificate=<host
name>;ValidateServerCertificate=<true|false>;KeyStore=<keystore
location>;keyStorePassword=<password>
```

Configure the parameters as follows:

EncryptionMethod

Encryption method for data transfer between Metadata Manager and the database server. Must be set to SSL.

TrustStore

Path and file name of the truststore file that contains the security certificate of the database server.

TrustStorePassword

Password used to access the truststore file.

HostNameInCertificate

Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the security certificate.

ValidateServerCertificate

Indicates whether the Metadata Manager Service validates the certificate that the database server presents. If you set this parameter to true, the Metadata Manager Service validates the certificate. If you specify the HostNameInCertificate parameter, the Metadata Manager Service also validates the host name in the certificate.

If you set this parameter to false, the Metadata Manager Service does not validate the certificate that the database server presents. The Metadata Manager Service ignores any truststore information that you specify.

KeyStore

Path and file name of the keystore file that contains the security certificates that the Metadata Manager Service presents to the database server.

KeyStorePassword

Password used to access the keystore file.

CHAPTER 3

mmRepoCmd

This chapter includes the following topics:

mmRepoCmd Overview

mmRepoCmd is a command line program that creates, deletes, backs up, and restores Metadata Manager repository contents. It also restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database.

mmRepoCmd is installed when you run the Informatica services installer or the Informatica client installer. You can also install mmRepoCmd on any machine when you install Informatica utilities. mmRepoCmd is installed as a batch file on Windows and as a shell script on UNIX.

mmRepoCmd is located in the following directories:

- `<Informatica services installation directory>/services/MetadataManagerService/utilities/mmrepocmd`
- `<Informatica client installation directory>/clients/PowerCenterClient/CommandLineUtilities/MM/mmrepocmd`
- `<Informatica utilities installation directory>/MetadataManager/utilities/mmrepocmd`

mmRepoCmd writes log events to the mmRepoCmd.log file. If you run mmRepoCmd from the command line, it creates the log file in the directory where the program is installed.

If the Metadata Manager Service calls this program, the program creates the log file in the following directory:

<Informatica services installation directory>/logs/<node name>/services/MetadataManagerService/<Metadata Manager Service name>

Certificate Validation for mmRepoCmd

If you configure a secure connection between the Metadata Manager web application and the Metadata Manager Service, you must configure mmRepoCmd to use the truststore file. mmRepoCmd uses the truststore file to validate the security certificates. mmRepoCmd does not accept a security certificate that has errors.

To configure mmRepoCmd to use the truststore file, edit the MMCmdConfig.properties file. Set the TrustStore.Path property to the path and file name of the truststore file.

If you do not configure a secure connection for the Metadata Manager web application, do not specify a truststore file. Leave the TrustStore.Path property in the MMCmdConfig.properties file empty.

MMCmdConfig.properties File

Use the MMCmdConfig.properties file to configure mmRepoCmd properties such as the truststore file, server polling interval, and server connection timeout period.

MMCmdConfig.properties is located in the following directories:

- <Informatica services installation directory>\services\MetadataManagerService\utilities\mmrepocmd\config
- <Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\mmrepocmd\config
- <Informatica utilities installation directory>\MetadataManager\utilities\mmrepocmd\config

Note: There are separate copies of the MMCmdConfig.properties file for mmcmd and for mmRepoCmd.

You can configure the following properties:

TrustStore.Path

Required if you configure a secure connection for the Metadata Manager web application. Path and file name of the truststore file that contains the public key.

If you do not configure a secure connection for the Metadata Manager web application, leave this property empty.

Server.PollInterval

Amount of time in milliseconds that the command line program waits before querying the Metadata Manager application. The program queries for the status of the last command when you run a command in wait mode. Default is 6000.

Server.ConnectionTimeOut

Number of milliseconds after which the remote connection to the Metadata Manager Service times out. Default is 86,400,000 (24 hours).

mmRepoCmd Rules and Guidelines

Use the following rules and guidelines with mmRepoCmd:

- To run mmRepoCmd commands, the Metadata Manager Service must be enabled and available.
- When you back up repository contents, mmRepoCmd uses the default encryption key to encrypt sensitive data in the binary back-up file. For maximum security, limit users that can access the back-up file directory.
- When you restore repository contents, mmRepoCmd uses the encryption key for the Informatica domain to encrypt sensitive data in the Metadata Manager repository.
- mmRepoCmd does not back up index files for a loaded resource. You must manually create the index for resources after you restore a Metadata Manager repository.
- To restore the Metadata Manager repository for a Metadata Manager Service in a different Informatica domain, you must first migrate the Metadata Manager users and groups. Before you restore the Metadata Manager repository, export the users and groups from the original domain and import them into the new domain.

  To export and import users and groups, use the infacmd command line program.
- After you restore repository contents, recycle the Metadata Manager Service. Recycle the Metadata Manager Service so that it drops and recreates the caches that store model and resource information.
- Back up and restore the Metadata Manager repository with the same Metadata Manager version. You cannot restore a back-up file from a different version.

mmRepoCmd Commands

The following table describes the mmRepoCmd commands:

Command Name	Description
backupRepository	Backs up the Metadata Manager repository to a back-up file.
createRepository	Creates the Metadata Manager warehouse tables and imports models for metadata sources into the Metadata Manager repository.
deleteRepository	Deletes Metadata Manager repository contents, including all metadata and repository database tables.
restorePCRepository	Restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database.
restoreRepository	Restores Metadata Manager repository contents from a back-up file.

backupRepository

Backs up the Metadata Manager repository to a back-up file. Backs up all tables in the Metadata Manager repository except staging tables and temporary tables.

Back up repository contents so that you can recover them after a hardware or software problem or to migrate a repository across domains or Metadata Manager Services. You can restore repository contents to the same database, to a different database, or to a different database type. To migrate a repository, back up repository contents, change the repository database, and restore the contents to the new database.

The backupRepository command creates a binary back-up file. It creates the back-up file in the `backup` subdirectory of the Metadata Manager file location that you set for the Metadata Manager Service.

By default, the backupRepository command creates the back-up file in the following directory:

```
<Informatica services installation directory>\services\MetadataManagerService\mm_files
\<Metadata Manager Service name>\backup
```

backupRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-f|--file> file>
[<-nt|--numThreads> numThreads]
```

backupRepository Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --file>>

Name of the file to which you want to back up the Metadata Manager repository database.

mmRepoCmd stores the back-up file in the `backup` subdirectory of the Metadata Manager file location that is set for the Metadata Manager Service. The back-up file name must be unique in the directory.

[<-nt | --numThreads>]

Number of processing threads that the Metadata Manager Service uses when it reads data from the Metadata Manager repository database. Must be a positive integer. Default is 5.

createRepository

Creates the Metadata Manager warehouse tables and imports models for metadata sources into the Metadata Manager repository.

Create repository contents after you create the Metadata Manager Service or if you deleted the repository contents. You cannot create contents for a repository that already includes contents.

createRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
```

createRepository Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

deleteRepository

Deletes Metadata Manager repository contents, including all metadata and repository database tables.

Delete the repository contents if the metadata is obsolete. If the repository contains information that you want to save, back up the repository before you delete it. Use the database client or mmRepoCmd to back up the database before you delete contents.

deleteRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
[-f]
```

deleteRepository Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

[-f]

Forces the delete operation and deletes the repository contents without confirmation. If you omit this option, the command prompts you for confirmation before it deletes the repository contents.

restorePCRepository

Restores a PowerCenter repository back-up file that contains Metadata Manager objects to the PowerCenter repository database. This command restores different contents to the PowerCenter repository based on the operating mode of the PowerCenter Repository Service.

The PowerCenter repository back-up file includes the metadata objects that Metadata Manager uses to load metadata into the Metadata Manager warehouse. These metadata objects include sources, targets, sessions, and workflows. In the PowerCenter repository, the metadata objects used by Metadata Manager are stored in the Metadata Load folder.

The restorePCRepository command restores different contents based on the following PowerCenter Repository Service operating modes:

Exclusive mode

If the PowerCenter Repository Service is running in exclusive mode, this command replaces all contents in the PowerCenter repository database. If the PowerCenter repository database contains contents, this command overwrites all contents.

Run this command when the PowerCenter Repository Service is running in exclusive mode if either of the following conditions are true:

- The PowerCenter repository has no content associated with it.
- The repository contains content that has not been upgraded.

Normal mode

If the PowerCenter Repository Service is running in normal mode, this command creates the Metadata Load folder and restores the folder contents. If the Metadata Load folder contains contents, this command overwrites all contents of the Metadata Load folder. It does not overwrite other PowerCenter repository database contents.

Run this command when the PowerCenter Repository Service is running in normal mode if the following conditions are true:

- The PowerCenter repository database contains contents.
- You only want to restore the contents of the Metadata Load folder.

Note: You must run this command from an mmRepoCmd instance that is installed with the Informatica services. You cannot run this command from an mmRepoCmd instance that is installed with Informatica utilities or with the Informatica client.

restorePCRepository Syntax

The command uses the following syntax:

```
<<-dn|--domainName> domainName>
[<-sdn|--securityDomain> security_domain]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
<<-du|--domainUser> domainUser>
[<-dp|--domainPassword> domainPassword]
<<-mm|--mmServiceName> mmServiceName>
[<-kt|--keyTab> keyTab]
<<-pcRepositoryName> pcRepositoryName>
<<-pcRepositoryUser> pcRepositoryUser>
[<-pcRepositoryNamespace> pcRepositoryNamespace]
<<-pcRepositoryPassword> pcRepositoryPassword>
```

restorePCRepository Options

The command uses the following options:

<<-dn | --domainName>>

Name of the Informatica domain.

[<-sdn | --securityDomain>]

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 Informatica domain user belongs. The security domain name is case sensitive.

[<-hp | --gateway>]

Required if the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain. If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

<<-du | --domainUser>>

User name used to connect to the Informatica domain.

[<-dp | --domainPassword>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option for the domain user. Password for the Informatica domain user.

<<-mm | --mmServiceName>>

Name of the Metadata Manager Service for which you want to restore the PowerCenter repository.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a domain user password. Path and file name of the keytab file for the domain user.

<<-pcRepositoryName>>

Name of the PowerCenter repository that you want to restore.

<<-pcRepositoryUser>>

User account for the PowerCenter repository. Use the repository user account you configured for the Repository Service.

[<-pcRepositoryNamespace>]

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.

<<-pcRepositoryPassword>>

Password for the PowerCenter repository user.

restoreRepository

Restores Metadata Manager repository contents from a back-up file. You can restore repository contents to the same database, to a different database, or to a different database type. You can restore repository contents to an empty repository.

When you restore a Metadata Manager repository, mmRepoCmd creates the repository tables in the Metadata Manager repository and then restores the contents. If the repository contains a table with the same name as a table that mmRepoCmd is trying to restore, mmRepoCmd drops the existing table, creates a new table, and restores the contents to the new table.

restoreRepository Syntax

The command uses the following syntax:

```
[<-dn|--domainName> domainName]
[<-hp|--gateway> gateway_host1:port gateway_host2:port...]
[<-mm|--mmServiceName> mmServiceName]
<<-url> http(s)://<host>:<port>>
<<-u|--user> user>
[-ep|--encryptedPassword]
[<-pw|--password> password]
[<-n|--namespace> namespace]
[<-kt|--keyTab> keyTab]
<<-f|--file> file>
[<-nt|--numThreads> numThreads]
[<-ci|--commitInt> commitInt]
```

restoreRepository Options

The command uses the following options:

[<-dn | --domainName>]

Required if the domain uses Kerberos authentication and you do not specify the --gateway option. Name of the Informatica domain.

This option uses the gateway connectivity information in the domains.infa file. If the domains.infa file is missing or contains connectivity information that is out of date, you must use the --gateway option instead.

[<-hp | --gateway>]

Required if the domain uses Kerberos authentication and you do not specify the --domainName option. Also required if the domain uses Kerberos authentication and the domains.infa file is missing or contains connectivity information that is out of date. Host names and port numbers of the gateway nodes in the domain.

If there are multiple gateway nodes, separate the gateways with a space. For example:

```
-hp host1:6001 host2:6002
```

Note: If you run the command from a machine where the Informatica client or the Informatica utilities are installed, the host name must be fully qualified.

[<-mm | --mmServiceName>]

Required if the domain uses Kerberos authentication. Name of the Metadata Manager Service.

<<-url>>

Host name and port number of the Metadata Manager Service that runs the Metadata Manager application. Use the following format: `http(s)://<host>:<port>`.

If a secure connection is configured for the Metadata Manager web application, the host name must match the common name (CN) used to generate the keystore that you use for the HTTPS connection to the Metadata Manager Service.

<<-u | --user>>

Metadata Manager user name.

[-ep | --encryptedPassword]

Required if you specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the Metadata Manager user is encrypted. For example:

```
-ep -pw WP+qtfYwB2KYLXID9jgC+6WHbMOg/94AO8R1nOC1vd0=
```

[<-pw | --password>]

Required if the domain does not use Kerberos authentication. Also required if the domain uses Kerberos authentication and you do not specify the --keyTab option. Password for the Metadata Manager user. For example:

```
-pw Administrator
```

Note: To specify an encrypted password, you must specify the --encryptedPassword option in addition to this option.

[<-n | --namespace>]

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 Metadata Manager user belongs. The security domain name is case sensitive.

[<-kt | --keyTab>]

Required if the domain uses Kerberos authentication and you do not specify a password. Path and file name of the keytab file for the Metadata Manager user.

<<-f | --file>>

Name of the file from which you want to restore Metadata Manager repository database contents.

The back-up file must exist in the `backup` subdirectory of the Metadata Manager file location that is set for the Metadata Manager Service.

[<-nt | --numThreads>]

Number of processing threads that the Metadata Manager Service uses when it writes data to the Metadata Manager repository database. Must be a positive integer. Default is 5.

[<-ci | --commitInt>]

Number of rows after which the Metadata Manager Service commits the data into the Metadata Manager repository. The restoreRepository command uses a batch commit each time it writes this number of rows. Using a batch commit reduces the size of the undo tablespace required if the command fails and mmRepoCmd rolls back the restore operation.

If set to 0, the command commits all rows at the end of the restore operation. Default is 10,000.

CHAPTER 4

mmXConPluginUtil

This chapter includes the following topics:

mmXConPluginUtil Overview

mmXConPluginUtil is a command line program that generates the image mapping information or the plug-in for a universal XConnect.

mmXConPluginUtil is installed when you run the Informatica services installer. mmXConPluginUtil is installed as a batch file on Windows and as a shell script on UNIX.

mmXConPluginUtil is located in the following directory:

```
<Informatica services installation directory>\services\MetadataManagerService\utilities
\mmxconpluginutil
```

mmXConPluginUtil writes log events to the following log file:

```
<Informatica services installation directory>\services\MetadataManagerService\utilities
\mmxconpluginutil\mmxconnectpluginutil.log
```

You run mmXConPluginUtil from the command line. The program creates the image mapping file or the plug-in in the following directory, where the owner and name are defined in the plug-in definition file:

```
<Informatica services installation directory>\services\MetadataManagerService\utilities
\mmxconpluginutil\<owner>.<name>
```

For more information about creating universal XConnects, see the *Metadata Manager Administrator Guide*.

Running Commands

When you run mmXConPluginUtil, you enter options for each command, followed by the required options and arguments. Command names are not case sensitive. Command options are preceded by a hyphen and are not case sensitive. Arguments follow the option.

For example, the following command generates the plug-in for a universal XConnect for QlikView:

```
mmXConPluginUtil generatePlugin -x C:\MMPlugInDefs\HypoStores_QlikViewDef.xml
```

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

1. At the command prompt, switch to the directory where mmXConPluginUtil is located.
2. Enter mmXConPluginUtil on Windows or mmXConPluginUtil.sh on UNIX followed by the command name and its required options and arguments.

   For example:

   ```
   mmXConPluginUtil(.sh) command_name -option argument
   ```

mmXConPluginUtil Commands

The following table describes the mmXConPluginUtil commands:

Command Name	Description
generateImageMapping	Generates the image mapping information for a universal XConnect.
generatePlugin	Generates the plug-in for a universal XConnect.

generateImageMapping

Generates the image mapping information for a universal XConnect. You need the image mapping information if you want to use custom icons for the groups and classes in the model. The image mapping information is a CSV file that lists each group and class in the model with the corresponding icon file.

The command uses the name and owner elements in the XML definition file to generate the image mapping file name in the following format:

```
mm-<owner>.<name>-xconnect.txt
```

generateImageMapping Syntax

The command uses the following syntax:

```
<<-x> xconnect definition file>
```

generateImageMapping Options

The command uses the following options:

<<-x>>

File path and file name of the plug-in definition XML file. If the file path or file name contains spaces, enclose the entire file path, including the file name, in double quotes.

generatePlugin

Generates the plug-in for a universal XConnect. The generatePlugin command generates the plug-in as an XConnect archive (XAR) file.

The command uses the name and owner elements in the XML definition file to generate the plug-in name in the following format:

```
mm-<owner>.<name>-xconnect.xar
```

After you create the plug-in, you can create the model. To create the model, copy the plug-in to the following directory, and then restart the Metadata Manager Service:

```
<Informatica services installation directory>\services\MetadataManagerService\mm-plugins
\xconnect\<Metadata Manager Service name>
```

generatePlugin Syntax

The command uses the following syntax:

```
<<-x> xconnect definition file>
```

generatePlugin Options

The command uses the following options:

<<-x>>

File path and file name of the plug-in definition XML file. If the file path or file name contains spaces, enclose the entire file path, including the file name, in double quotes.

CHAPTER 5

rcfmu

This chapter includes the following topics:

rcfmu Overview

rcfmu is a command line program that migrates a resource configuration file from a previous version of Metadata Manager to the current version.

rcfmu creates a new resource configuration file in the directory where you run it or in a directory that you specify. It does not replace the original resource configuration file.

rcfmu writes migration errors to the migration log file. If rcfmu cannot migrate the resource configuration file, check the log file, fix the errors, and rerun rcfmu. The migration log file is `<Informatica Installation Directory>\services\MetadataManagerService\utilities\rcfmuUtil\resourcemigration.log`.

After you migrate a resource configuration file, you can upload it into the repository.

rcfmu Migration Rules for Resource Properties

To reflect model changes, rcfmu might create or remove resource properties for some resource types. It might also update the names, values, and value sets of some resource properties.

rcfmu applies different migration rules to the following types of properties:

Unchanged Properties

If a property is unchanged between versions, rcfmu copies the property from the original resource configuration file to the new resource configuration file.

New Properties

If a property exists in the new resource but not in the original resource, rcfmu creates the property in the new resource configuration file. It applies one of the following rules to determine the value of the property in the new resource configuration file:

- If the property is required, rcfmu assigns the model-provided default value to the property.
- If the property is optional and the model provides a default value, rcfmu assigns the model-provided default value to the property.
- If the property is optional and the model provides no default value, rcfmu assigns a null value to the property.

Renamed Properties

If the property has a different name, rcfmu copies the property value from the original resource configuration file to the corresponding property in the new resource configuration file.

Properties with Value Set Changes

If the property has a different set of values, rcfmu maps the original set of values to the new set of values.

Deleted Properties

If a property exists in the original resource but not in the new resource, rcfmu omits the resource property from the new resource configuration file.

To view the renamed properties, properties with value set changes, and deleted properties for different resource types, see the *Informatica Release Guide*.

Running rcfmu

You invoke rcfmu from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, rcfmu is a batch file with a .bat extension. On UNIX, rcfmu is a script file with a .sh extension.

rcfmu is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\rcfmuUtil`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\rcfmuUtil`
- `<Informatica utilities installation directory>\MetadataManager\utilities\rcfmuUtil`

1. At a command prompt, navigate to the directory where rcfmu is located.
2. Enter `rcfmu` on Windows or `rcfmu.sh` on UNIX followed by the required arguments.

rcfmu Syntax

rcfmu options and arguments specify connection information for the original repository database.

rcfmu uses the following syntax:

```
rcfmu.bat
 <<-dt> databaseType>
 <<-u> userName>
 <<-rn> resourceNewName>
 [<-ep> encryptedPasswordFlag]
 <<-smv> sourceMMVersion>
 <<-rcf> resourceConfigurationFile>
 [<-src> sourceFilesDirectoryPath]
 <<-pw> password>
 <<-durl> databaseURL>
 <<-connection_assignment> Retain|Discard>
 [<-nrd> newRCFDirectoryPath]
```

rcfmu Options

rcfmu uses the following options:

<<-dt>>

Database type for the original Metadata Manager repository database.

Specify one of the following types:

- `DB2`
- `Oracle`
- `"Microsoft SQL Server"`

<<-u>>

Database user name for the original Metadata Manager repository database.

<<-rn>>

Name of the new resource. If the name contains spaces, enclose it in double quotes.

[<-ep>]

Required to specify an encrypted password. Encrypted password flag. Use with the password option to indicate that the password for the database user name is encrypted.

<<-smv>>

Metadata Manager source version.

Specify one of the following versions:

- `9.1.0`
- `9.1.0.HF1-SNAPSHOT`
- `9.1.0.HF2-SNAPSHOT`
- `9.1.0.HF3-SNAPSHOT`
- `9.1.0.HF4-SNAPSHOT`
- `9.1.0.HF5-SNAPSHOT`

- 9.1.0.HF6-SNAPSHOT
- 9.5.0
- 9.5.1
- 9.5.1.HF1
- 9.5.1.HF2
- 9.5.1.HF3
- 9.5.1.HF4
- 9.6.0
- 9.6.1
- 9.6.1.HF1
- 9.6.1.HF2
- 9.6.1.HF3
- 9.6.1.HF4
- 10.0.0
- 10.1.0

Tip: To get the Metadata Manager source version number, run the mmcmd version command in the original Metadata Manager version.

<<-rcf>>

File path and file name of the resource configuration file that you want to migrate.

[<-src>]

File path of metadata source files for the original resource. Required for Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources.

<<-pw>>

Password for the database user name.

<<-durl>>

JDBC URL for the original Metadata Manager repository database.

The syntax depends on the repository database type:

- For IBM DB2, use the following syntax:

```
"jdbc:informatica:db2://[host name]:[port];DatabaseName=[database name]"
```

- For Microsoft SQL Server, use the following syntax:

```
"jdbc:informatica:sqlserver://[host name]:
[port];SelectMethod=cursor;DatabaseName=[database name]"
```

To authenticate the database user credentials using Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, append `;AuthenticationMethod=ntlm` to the URL.

When you use a trusted connection to connect to a Microsoft SQL Server database, the Metadata Manager Service connects to the repository with the credentials of the user logged in to the machine on which the service is running.

If you run the program from a machine on which Informatica is not installed, configure the PATH variable to point to the location of the DDJDBCAuth04.dll file.

- For Oracle, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host name]:[port];SID=[sid]"
  ```

  You can enter the SID or use the full service name. For example:

  ```
  "jdbc:informatica:oracle://[host name]:[port];ServiceName=[service name]"
  ```

  If the Oracle database is clustered, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host1]:[port];ServiceName=[service
  name];AlternateServers = ([host2]:[port]);LoadBalancing=true"
  ```

  If the Oracle database uses the Advanced Security Option, use the following syntax:

  ```
  "jdbc:informatica:oracle://[host name]:
  [port];SID=[SID];EncryptionLevel=[encryption level];EncryptionTypes=[encryption
  types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data
  integrity types]"
  ```

Note: If secure communication is enabled for the Metadata Manager repository database, you must append additional JDBC parameters to the JDBC URL.

<<-connection_assignment>>

Specifies whether to retain connection assignments in the new resource configuration file.

Enter one of the following arguments:

- `Retain`. rcfmu migrates connection assignments to the new resource configuration file. If a connection name changed, you must reassign the connection in the new resource.
- `Discard`. rcfmu does not migrate any connection assignment. However, Metadata Manager automatically configures connection assignments for the new resource when you load it.

[<-nrd>]

File path for the new resource configuration file. If you do not specify a file path, rcfmu creates the new resource configuration file in the directory where you run it.

JDBC Parameters for Secure Databases

If the original Metadata Manager repository database uses a secure connection to communicate with external components, you must append additional parameters to the JDBC URL.

Append the following parameters to the URL:

```
;EncryptionMethod=SSL;TrustStore=<truststore
location>;TrustStorePassword=<password>;HostNameInCertificate=<host
name>;ValidateServerCertificate=<true|false>;KeyStore=<keystore
location>;keyStorePassword=<password>
```

Configure the parameters as follows:

EncryptionMethod

Encryption method for data transfer between Metadata Manager and the database server. Must be set to SSL.

TrustStore

Path and file name of the truststore file that contains the security certificate of the database server.

TrustStorePassword

Password used to access the truststore file.

HostNameInCertificate

Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the security certificate.

ValidateServerCertificate

Indicates whether the Metadata Manager Service validates the certificate that the database server presents. If you set this parameter to true, the Metadata Manager Service validates the certificate. If you specify the HostNameInCertificate parameter, the Metadata Manager Service also validates the host name in the certificate.

If you set this parameter to false, the Metadata Manager Service does not validate the certificate that the database server presents. The Metadata Manager Service ignores any truststore information that you specify.

KeyStore

Path and file name of the keystore file that contains the security certificates that the Metadata Manager Service presents to the database server.

KeyStorePassword

Password used to access the keystore file.

CHAPTER 6

rmu

This chapter includes the following topics:

rmu Overview

rmu is a command line program that migrates resources from a previous version of Metadata Manager to the current version. rmu migrates deprecated resources and creates new resources that you can use in the current version of Metadata Manager.

You can migrate one resource or all resources in a repository. If you migrate individual resources, migrate and reload JDBC and data management resources before you migrate and reload other types of resources. If you do not migrate and reload resources in this order, you might lose connection information for business intelligence and data modeling resources.

If you migrate one resource, you can specify a name for the new resource. If you do not specify a name for the new resource or you migrate all resources, rmu generates the new resource names. If you migrate an Embarcadero ERStudio, MicroStrategy, or SAP PowerDesigner resource, rmu creates one new resource for each metadata source file.

rmu takes an XML configuration file as an argument. The configuration file specifies connection information for the original repository database. It also specifies authentication information for the original resource and the new resource.

When you migrate a resource, rmu first creates a new resource configuration file and then creates a new resource from the resource configuration file. If errors occur during the migration process, check the migration log file to determine the cause of the errors, and then rerun rmu. The migration log file is `<Informatica Installation Directory>\services\MetadataManagerService\utilities\rcfmuUtil\resourcemigration.log`.

After you run rmu, you can view the new resource on the **Load** tab or the **Browse** tab.

Metadata Manager displays one of the following statuses for the new resource:

Not loaded

rmu successfully created the new resource from the original resource. The new resource is valid and ready to load.

Invalidated

rmu encountered errors during resource creation. The new resource is not valid. Check the mm.log file to determine the cause of the errors, and then update the resource. For example, you might have to reconfigure parameters or connection assignments for the resource.

After migration, load the new resource. Then re-create the shortcuts, comments, links, and relationships from the original resource. You must also update any schedule that the original resource is assigned to.

rmu cannot convert Business Objects universe names to universe IDs. Therefore, after you migrate and load a Business Objects resource, you might need to update the universe ID.

rmu Migration Rules for Resource Properties

To reflect model changes, rmu might create or remove resource properties for some resource types. It might also update the names, values, and value sets of some resource properties.

rmu applies different migration rules to the following types of properties:

Unchanged Properties

If a property is unchanged between versions, rmu copies the property from the original resource to the new resource.

New Properties

If a property exists in the new resource but not in the original resource, rmu creates the property in the new resource. It applies one of the following rules to determine the value of the property in the new resource:

- If the property is required, rmu assigns the model-provided default value to the property.
- If the property is optional and the model provides a default value, rmu assigns the model-provided default value to the property.
- If the property is optional and the model provides no default value, rmu assigns a null value to the property.

Renamed Properties

If the property has a different name, rmu copies the property value from the original resource to the corresponding property in the new resource.

Properties with Value Set Changes

If the property has a different set of values, rmu maps the original set of values to the new set of values.

Deleted Properties

If a property exists in the original resource but not in the new resource, rmu omits the resource property from the new resource.

To view the renamed properties, properties with value set changes, and deleted properties for different resource types, see the *Informatica Release Guide*.

Running rmu

You invoke rmu from the command line. You can issue commands directly or from a script, batch file, or other program. On Windows, rmu is a batch file with a .bat extension. On UNIX, rmu is a script file with a .sh extension.

rmu is located in the following directories:

- `<Informatica services installation directory>\services\MetadataManagerService\utilities\rcfmuUtil`
- `<Informatica client installation directory>\clients\PowerCenterClient\CommandLineUtilities\MM\rcfmuUtil`
- `<Informatica utilities installation directory>\MetadataManager\utilities\rcfmuUtil`

1. At a command prompt, navigate to the directory where rmu is located.
2. Enter `rmu` on Windows or `rmu.sh` on UNIX followed by the required arguments.

rmu Syntax

rmu uses the following syntax:

```
rmu.bat
 [<-mr> newMigratedResourceName]
 <<-r> oldResourceName|ALL>
 <<-cf> configurationFile>
 <<-connection_assignment> Retain|Discard>
```

rmu Options

rmu uses the following options:

[<-mr>]

Name of the new resource. rmu appends the metadata source file name to Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources.

If you do not enter a value for this option, rmu generates the new resource name as follows:

- Embarcadero ERStudio, MicroStrategy, and SAP PowerDesigner resources. rmu names each new resource `<original name>_new_<file name>`, where `<file name>` is the first 15 characters of the metadata source file name. If the source file names exceed 15 characters, rmu uses sequential numbers for the last character in each resource name.
- Other resources. rmu names the new resource `<original name>_new`.

<<-r>>

Name of the resource that you want to migrate. To migrate all resources in a repository, enter `-r all`.

<<-cf>>

Name of the XML configuration file.

<<-connection_assignment>>

Specifies whether to retain connection assignments in the new resource.

Enter one of the following arguments:

- `Retain`. rmu migrates connection assignments to the new resource. If a connection name changed, you must reassign the connection in the new resource.
- `Discard`. rmu does not migrate any connection assignment. However, Metadata Manager automatically configures connection assignments for the new resource when you load it.

rmu Configuration File Format

rmu requires an XML configuration file that specifies connection information for the original Metadata Manager repository and authentication information for the original and new resources. Use a text editor to create and update the rmu configuration file.

The rmu configuration file contains the following elements:

configurations

Root element for the configuration file.

sourceService

Defines the original resource.

targetService

Defines the new resource.

MMService

Defines authentication information for the Metadata Manager service.

database

Defines database information for the original Metadata Manager repository database.

user

In the MMService element, defines the Metadata Manager user name.

In the database element, defines the database user name for the original Metadata Manager repository database.

password

Defines the password for the Metadata Manager user. If the domain uses Kerberos authentication, specify either the password or the keytab file.

encryptFlag

Defines whether the password for the Metadata Manager user is encrypted.

url

In the MMService element, defines the Metadata Manager URL.

In the database element, defines the URL for the original Metadata Manager repository database.

namespace

If the domain uses Kerberos authentication or LDAP authentication, defines the name of the security domain to which the Metadata Manager user belongs. If the domain uses native authentication, leave this element empty or set the value to `Native`.

domainName

Defines the name of the Informatica domain. If the domain uses Kerberos authentication, specify either the domain name or the gateway host name and port number. If the domain does not use Kerberos authentication, leave this element empty or omit it.

gateway

Defines the host name and port number of the gateway node in the Informatica domain in the format `<host>:<port>`. If the domain uses Kerberos authentication, specify either the domain name or the gateway host name and port number. If the domain contains multiple gateway nodes, specify the domain name. If the domain does not use Kerberos authentication, leave this element empty or omit it.

keyTab

Defines the path and file name of the keytab file for the Metadata Manager user. If the domain uses Kerberos authentication, specify either the password or the keytab file. If the domain does not use Kerberos authentication, leave this element empty or omit it.

type

Defines the database type for the original Metadata Manager repository database.

Specify one of the following types:

- DB2
- Oracle
- Microsoft SQL Server

mmcmdDirPath

Defines the file path for the mmcmd.bat file. Required for both the original and new resources. rmu uses mmcmd to determine the version of the original resource.

filesDirPath

Defines the file path for the original resource configuration file and the metadata source files for the original resource.

rmu Sample Configuration File

The rmu resource migration utility takes an XML configuration file that specifies connection information and authentication information.

The following example shows a typical rmu configuration file:

```
<configurations>
    <sourceService>
        <MMService>
            <user>Administrator</user>
            <password>4/mnaeiVbXqC44SZBaQtjH7G/y1yOGBmpF0NC34kHxU=</password>
            <encryptFlag>true</encryptFlag>
            <url>http://mminst01:10250</url>
            <namespace></namespace>
        </MMService>
        <database>
            <user>DBUser01</user>
            <password>Ev+EEMdYjri3FeGK1R9Ez+kIDaamMUMRTznGHx6bvpc=</password>
            <encryptFlag>true</encryptFlag>
```

```
            <url>jdbc:informatica:oracle://10.65.40.60:1521;SID=goldwing</url>
            <type>Oracle</type>
        </database>
        <mmcmdDirPath>C:\Informatica\9.1.0\mmcmc\mmcmd</mmcmdDirPath>
    </sourceService>
    <targetService>
        <MMService>
            <user>Administrator</user>
            <password>QoZG3OqekSjdr97ceGB4f5PJ3ofiF52ZQTtWOxfOV8s=</password>
            <url>http://mminst02:10250</url>
            <encryptFlag>true</encryptFlag>
            <namespace></namespace>
        </MMService>
        <mmcmdDirPath>C:\Informatica\9.6.1\source\services\MetadataManagerService
\utilities\mmcmd\</mmcmdDirPath>
    </targetService>
    <filesDirPath>c:\users\jsmith\desktop\RCF</filesDirPath>
</configurations>
```

INDEX

H

I

L

M

P

R

S

T

U

V