Informatica

Informatica® Cloud Data Integration for PowerCenter

April 2024

Administrator Guide

Informatica Cloud Data Integration for PowerCenter Administrator Guide
April 2024

Publication Date: 2024-04-21

Table of Contents

Preface

Use the *Administrator Guide* to learn how to log into the Administrator tool and understand the user interface. Read on how to configure, manage, and monitor the Cloud Data Integration for PowerCenter (CDI-PC) domain. Learn about CDI-PC domain architecture and its components, including CDI-PC nodes, services, high availability, connections, and monitoring.

CHAPTER 1

Understanding Domains

This chapter includes the following topics:

Understanding Domains Overview

Informatica has a service-oriented architecture that provides the ability to scale services and share resources across multiple machines. High availability functionality helps minimize service downtime due to unexpected failures or scheduled maintenance in the Informatica environment.

The Informatica domain is the fundamental administrative unit in Informatica. The domain supports the administration of the distributed services. A domain is a collection of nodes and services that you can group in folders based on administration ownership.

A node is the logical representation of a machine in a domain. One node in the domain acts as a gateway to receive service requests from clients and route them to the appropriate service and node. Services and processes run on nodes in a domain. The availability of a service or process on a node depends on how you configure the service and the node.

Services for the domain include the Service Manager and a set of application services:

- Service Manager. A service that runs on each node in the domain to manage all domain operations. The Service Manager performs domain functions such as authentication, authorization, and logging. The Service Manager also starts the application services configured to run on the node.
- Application Services. Services that represent server-based functionality. The application services that run on a node depend on the way you configure the services.

The Service Manager and application services control security. The Service Manager manages users and groups that can log in to application clients and authenticates the users who log in to the application clients. The Service Manager and application services authorize user requests from application clients.

Informatica Administrator (the Administrator tool), consolidates the administrative tasks for domain objects such as services, nodes, licenses, and grids. You manage the domain and the security of the domain through the Administrator tool.

If you have the high availability option, you can scale services and eliminate single points of failure for services. Services can continue running despite temporary network or hardware failures.

Nodes

A node is a logical representation of a machine in a domain. During installation, you add the installation machine to the domain as a node. You can add multiple nodes to a domain.

Each node in the domain runs the Service Manager that manages domain functions on that node. The Service Manager also supports the application services that run on the node. The domain functions that the node performs and the services that the node runs depend on the following node configurations:

Node type

The node type determines whether the node can serve as a gateway or worker node and determines the domain functions that the node performs. One gateway node serves as the master gateway node for the domain. The master gateway node receives service requests from clients and routes them to the appropriate service and node. A worker node is any node not configured to serve as a gateway. The first time that you install the Informatica services, you create a gateway node and the Informatica domain. When you install the Informatica services on other machines, you create additional gateway nodes or worker nodes that you join to the domain.

Node role

The node role defines the purpose of the node. A node with the service role can run application services. A node with the compute role can perform computations requested by remote application services. A node with both roles can run application services and locally perform computations for those services. By default, each gateway and worker node has both the service and compute roles enabled.

You can subscribe to alerts to receive notification about node events such as node failure or a master gateway election. You can also generate and upload node diagnostics to the Configuration Support Manager and review information such as available EBFs and Informatica recommendations.

Service Manager

The Service Manager is a service that manages all domain operations. It runs within Informatica services. It runs as a service on Windows and as a daemon on UNIX. When you start Informatica services, you start the Service Manager.

The Service Manager runs on each node in the domain. If the Service Manager is not running, the node is not available.

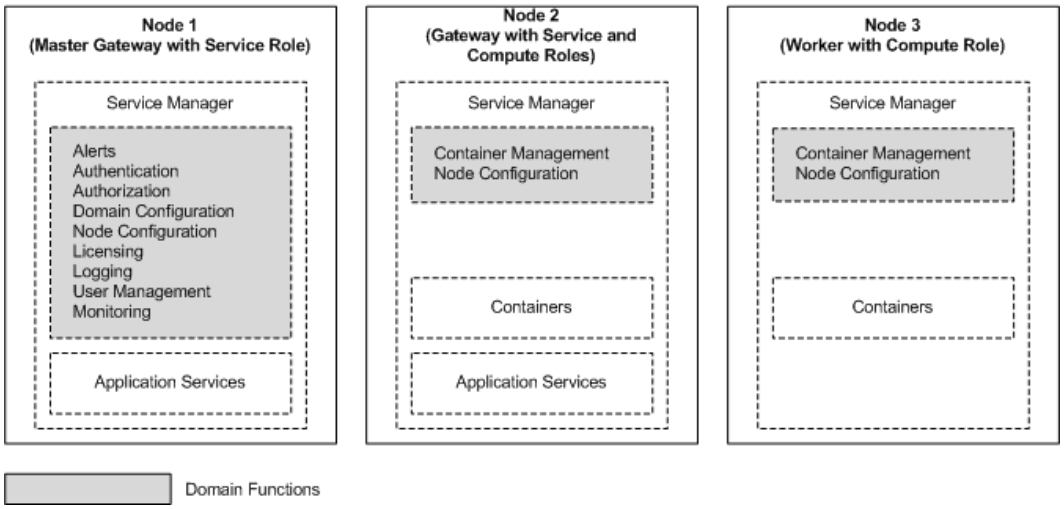
The Service Manager runs on all nodes in the domain to support the domain and application services:

- Domain support. The Service Manager performs functions on each node to support the domain. The functions that the Service Manager performs on a node depend on the type and role of the node. For example, the Service Manager running on the master gateway node performs all domain functions on that node. The Service Manager running on any other type of node performs limited domain functions on that node.
- Application service support. When a node has the service role, the Service Manager starts application services configured to run on that node. It starts and stops services and service processes based on requests from clients. It also directs service requests to application services. The Service Manager uses TCP/IP to communicate with the application services.

The following table describes the domain functions that the Service Manager performs:

Function	Description
Authentication	The Service Manager authenticates users who log in to application clients. Authentication occurs on the master gateway node.
Authorization	The Service Manager authorizes user requests for domain objects based on the privileges, roles, and permissions assigned to the user. Requests for domain objects can come from the Administrator tool. Domain authorization occurs on the master gateway node.
Container Management	When a node has the compute role, the Service Manager manages the containers on the node. A container is an allocation of memory and CPU resources. An application service uses the container to remotely perform computations on the node. Container management occurs on any node with the compute role.
Domain Configuration	The Service Manager manages the domain configuration metadata. Domain configuration occurs on the master gateway node.
Node Configuration	The Service Manager manages node configuration metadata in the domain. Node configuration occurs on all nodes in the domain.
Licensing	The Service Manager registers license information and verifies license information when you run application services. Licensing occurs on the master gateway node.
Logging	The Service Manager provides accumulated log events from each service in the domain. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent. The Log Manager runs on the master gateway node. The Log Agent runs on all nodes where CDI-PC Integration Service sessions and workflows run.
User Management	The Service Manager manages the native and LDAP users and groups that can log in to application clients. It also manages the creation of roles and the assignment of roles and privileges to native and LDAP users and groups. User management occurs on the master gateway node.

The following image shows where the Service Manager performs domain functions:



Application Services

Application services represent server-based functionality.

Application services include services that you create and system services that are created for you when you create the domain. A system service can have a single instance in the domain.

Note: You can't use the system services in the current release as the Model Repository Service is not available.

Application services include the following services:

- CDI-PC Repository Service
- CDI-PC Integration Service
- PowerExchange® Listener Service
- PowerExchange Logger Service
- SAP BW Service
- Web Services Hub

When you configure an application service, you designate a node to run the service process. When a service process runs, the Service Manager assigns a port number from the range of port numbers assigned to the node.

The service process is the runtime representation of a service running on a node. The service type determines how many service processes can run at a time. For example, the CDI-PC Integration Service can run multiple service processes at a time when you run it on a grid.

If you have the high availability option, you can run a service on multiple nodes. Designate the primary node to run the service. All other nodes are back-up nodes for the service. If the primary node is not available, the service runs on a back-up node. You can subscribe to alerts to receive notification in the event of a service process failover.

If you do not have the high availability option, configure a service to run on one node. If you assign the service to multiple nodes, then the service will not start.

CDI-PC Repository Service

The CDI-PC Repository Service manages the CDI-PC repository. It retrieves, inserts, and updates metadata in the repository database tables. If the service process fails or the node becomes unavailable, then the service becomes unavailable.

If you have the high availability option, you can configure the service to run on primary and backup nodes. By default, the service process runs on the primary node. If the service process fails, a new process starts on the same node. If the node becomes unavailable, a service process starts on one of the backup nodes.

CDI-PC Integration Service

The CDI-PC Integration Service runs CDI-PC sessions and workflows. When you configure the CDI-PC Integration Service, you can specify where you want it to run:

- On a grid. When you configure the service to run on a grid, it can run on multiple nodes at a time. The CDI-PC Integration Service dispatches tasks to available nodes assigned to the grid. If you do not have the high availability option, the task fails if any service process or node becomes unavailable. If you have the high availability option, failover and recovery is available if a service process or node becomes unavailable.

- On nodes. If you have the high availability option, you can configure the service to run on multiple nodes. By default, it runs on the primary node. If the primary node is not available, it runs on a backup node. If the service process fails or the node becomes unavailable, the service fails over to another node. If you do not have the high availability option, you can configure the service to run on one node.

PowerExchange Listener Service

The PowerExchange Listener Service is an application service that manages the PowerExchange Listener. The PowerExchange Listener manages communication between a CDI-PC or PowerExchange client and a data source for bulk data movement and change data capture. The CDI-PC Integration Service connects to the PowerExchange Listener through the Listener Service. Use the Administrator tool to manage the service and view service logs.

If you have the CDI-PC high availability option, you can run the Listener Service on multiple nodes. If the Listener Service process fails on the primary node, it fails over to a backup node.

PowerExchange Logger Service

The Logger Service is an application service that manages the PowerExchange Logger for Linux, UNIX, and Windows. The PowerExchange Logger captures change data from a data source and writes the data to PowerExchange Logger log files. Use the Admnistrator tool to manage the service and view service logs.

If you have the CDI-PC high availability option, you can run the Logger Service on multiple nodes. If the Logger Service process fails on the primary node, it fails over to a backup node.

SAP BW Service

The SAP BW Service listens for RFC requests from SAP NetWeaver BI and initiates workflows to extract from or load to SAP NetWeaver BI. The SAP BW Service is not highly available. You can configure it to run on one node.

Web Services Hub

The Web Services Hub receives requests from web service clients and exposes CDI-PC workflows as services. The Web Services Hub does not run an associated service process. It runs within the Service Manager.

High Availability

High availability is an option that eliminates a single point of failure in a domain and provides minimal service interruption in the event of failure. High availability consists of the following components:

- Resilience. The ability of application services to tolerate transient network failures until either the resilience timeout expires or the external system failure is fixed.
- Failover. The migration of an application service or task to another node when the node running the service process becomes unavailable.
- Recovery. The automatic completion of tasks after a service is interrupted. Automatic recovery is available for CDI-PC Integration Service and CDI-PC Repository Service tasks. You can also manually recover CDI-PC Integration Service workflows and sessions. Manual recovery is not part of high availability.

CHAPTER 2

Managing Your Account

This chapter includes the following topics:

Managing Your Account Overview

Manage your account to change your password or edit user preferences.

If you have a native user account, you can change your password at any time with the Change Password application. If someone else created your user account, change your password the first time you log in to the Administrator tool.

User preferences control the options that appear in the Administrator tool when you log in. User preferences do not affect the options that appear when another user logs in to the Administrator tool.

You can configure Informatica Network credentials for your account so that you can access the Informatica Knowledge Base from the Administrator tool.

Password Management

You can change the password through the Change Password application.

You can open the Change Password application from the Administrator tool or with the following URL:
`http://<fully qualified host name>:<port>/passwordchange/`

The Service Manager uses the user password associated with a worker node to authenticate the domain user. If you change a user password that is associated with one or more worker nodes, the Service Manager updates the password for each worker node. The Service Manager cannot update nodes that are not running. For nodes that are not running, the Service Manager updates the password when the nodes restart.

Note: For an LDAP user account, change the password in the LDAP directory service.

For a user account in the domain that uses native authentication, if you enable password complexity, use the following guidelines when you create or change a password:

- The length of the password must be at least eight characters.
- It must be a combination of an alphabet character, a numeric character and a non-alphanumeric character, such as:
  ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

When you use special characters in a password, the shell sometimes interprets them differently. For example, $ is interpreted as a variable. In this case, use an escape character to escape the special character.

Changing Your Password

Change the password for a native user account at any time. For a user account created by someone else, change the password the first time you log in to the Administrator tool.

1. In the Administrator tool header area, click **Manage** > **Change Password**.

   The Change Password application opens in a new browser window.
2. Enter the current password in the **Password** box, and the new password in the **New Password** and **Confirm Password** boxes.
3. Click **Update**.

Preferences

Your preferences determine the options that appear in the Administrator tool when you log in. Your preferences do not affect the options that appear when another user logs in to the Administrator tool.

The following table describes the options that you can configure for your preferences:

Option	Description
Subscribe for Alerts	Subscribes you to domain and service alerts. You must have a valid email address configured for your user account. Default is No.
Show Custom Properties	Displays custom properties in the contents panel when you click an object in the Navigator. You use custom properties to configure Informatica behavior for special cases or to increase performance. Hide the custom properties to avoid inadvertently changing the values. Use custom properties only if Informatica Global Customer Support instructs you to.

To edit your preferences, click **Manage** > **Preferences** in the Administrator tool header area.

Informatica Network Credentials

You can enter your Informatica Network credentials in the Administrator tool to access the Informatica Knowledge Base from the Administrator tool.

You can also view the search results for an error message in the Informatica Knowledge Base by clicking the error message code in the Administrator tool.

Enter Informatica Network Credentials

Enter your Informatica Network credentials to access the Informatica Knowledge Base from the Administrator tool.

1. Click **Manage** > **Support Portal Credentials**.

   The **Informatica Network Login Credentials** window appears.
2. Enter your Informatica Network credentials and the customer project ID.
3. Click **OK.**

Searching Informatica Knowledge Base

You can search for terms in the Informatica Knowledge Base directly from the Administrator tool.

1. Click **Help** > **Search Knowledge Base**.

   The **Search Knowledge Base** window appears.
2. Enter the term that you want to search in the text box.
3. Click **OK**.

   The search results appear in a different browser window.

CHAPTER 3

Using Informatica Administrator

This chapter includes the following topics:

Using Informatica Administrator Overview

Informatica Administrator is the tool that you use to manage the Informatica domain and Informatica security.

The Administrator tool has the following tabs:

- **Manage**. View and edit the properties of the domain and objects within the domain.
- **Logs**. View log events for the domain and services within the domain.
- **Reports**. Run a Web Services Report or License Management Report.
- **Security**. Manage users, groups, roles, and privileges.
- **Cloud**. View information about your Informatica Cloud® organization.

The Administrator tool has the following header items:

- **Log out**. Log out of the Administrator tool.
- **Manage**. Manage your account.
- **Help**. Access help for the current tab and determine the Informatica version.

Log in to Informatica Administrator

You must have a user account to log in to the Informatica Administrator web application.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:

   ```
   https://<fully qualified hostname>:<https port>/administrator/
   ```

   Host name and port in the URL represent the host name and port number of the master gateway node.
3. If you do not use Kerberos authentication, enter the user name, password, and security domain for your user account, and then click **Login**.

   The **Security Domain** field appears when the CDI-PC domain contains an LDAP security domain. If you do not know the security domain that your user account belongs to, contact the CDI-PC domain administrator.

   If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

   Note: If this is the first time you log in with the user name and password provided by the domain administrator, change your password to maintain security.

Informatica Administrator URL

In the Administrator tool URL, `<host>:<port>` represents the host name of the master gateway node and the Administrator tool port number.

You configure the Administrator tool port when you define the domain. You can define the domain during installation. If you enter the domain port instead of the Administrator tool port in the URL, the browser is directed to the Administrator tool port.

Troubleshooting the Login to Informatica Administrator

If the CDI-PC domain uses Kerberos authentication, you might encounter the following issues when logging in to the Administrator tool:

I cannot log in to the Administrator tool from the same machine where I created the domain gateway node.

After installation, if you cannot log in to the Administrator tool from the same machine where you created the domain gateway node, clear the browser cache. When you initially log in to the Administrator tool after installation, you can only log in with the Administrator user account created during installation. If a different user credential is stored in the browser cache, the login can fail.

A blank page appears after I log in to the Administrator tool.

If a blank page appears after you log in to the Administrator tool, verify that you enabled delegation for all user accounts with service principals used in the CDI-PC domain. To enable delegation, in the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

Manage Tab

On the **Manage** tab, you can view and manage the domain and the objects that it contains.

The contents that appear and the tasks you can complete on the **Manage** tab vary based on the view that you select. You can select the following views:

- **Domain**. View and manage domain status, resource consumption, and events.
- **Services and Nodes**. View and manage application services and nodes.

Manage Tab - Domain View

The **Domain** view displays an overview of the domain and its contents. You can use the domain view to monitor the domain status, resource consumption, and events. You can also perform domain actions, such as enabling and disabling services.

The **Domain** view has the following components:

Domain Actions menu

Use the **Domain Actions** menu to view more information about the domain or shut down the domain.

Use the **Domain Actions** menu to perform the following tasks:

- View Properties. Open the **Services and Nodes** view and display the properties for the domain.
- View Logs. Open the **Logs** tab and display **Service Manager** log events from the last day.
- View Command History. Open the **Command History** panel and display the 50 most recent service lifecycle commands that were issued from the Administrator tool.
- Shut Down Domain.

Contents panel

Displays domain objects and their states. Domain objects include services, nodes, and grids.

The following table describes the methods that you can use to view objects in the contents panel:

Method	Description
Service State	Filter services by the following states: - All states - Available - Unavailable - Disabled
Service Type	Filter some or all services in the domain.
Navigate by	Group objects by node, type, or folder.
Search	Search for an object by name. You can use an asterisk (*) as a wildcard character in this field.
Show Legend	View a list of state icons and descriptions.

Object Actions menus

Objects in the contents panel have Actions menus. Use the Actions menus to view information about domain objects or perform common tasks. The information you can view and the tasks that you can perform vary depending on which object you select.

Use the service Actions menu to perform the following tasks:

- View Properties. Open the Services and Nodes view and display the properties for the service.
- View Logs. Open the Logs tab and display service log events from the last day.
- View Dependencies. Open the Dependency graph and display direct dependencies for the service.
- Recycle Service.
- Enable or Disable Service.

Use the node Actions menu to perform the following tasks:

- View Properties. Open the Services and Nodes view and display properties for the node.
- View Dependencies. Open the Dependency graph and display direct dependencies for the node.
- Shut Down Node

Use the grid Actions menu to perform the following tasks:

- View Properties. Open the Services and Nodes view and display properties for the grid.
- View Dependencies. Open the Dependency graph and display direct dependencies for the grid.

Service State Summary

Doughnut chart that shows the number and state of the services in the domain. When you click a state in the chart, the contents panel displays services with that state.

Resource usage indicators

Bar charts that compare resource usage of a domain process to resource usage of all processes on the machine. The Domain view contains a memory usage indicator and a CPU usage indicator.

Manage tab Actions menu

Access help for the Domain view.

Details Panel

When you select a domain object, the **Details** panel displays information about the object. The information that you can view varies depending on which object you select.

The following table describes the details that display depending on the object that you select in the contents panel:

Object	Details Panel Content
Node	Node name and state. Click the node name to view the node properties.
Service	The Details panel displays the following content for a service: - Service name and state. Click the service name to view the service properties. - Node on which the service process runs. Click the node name to view the node properties. - State of the node on which the service process runs. - State of the service process.

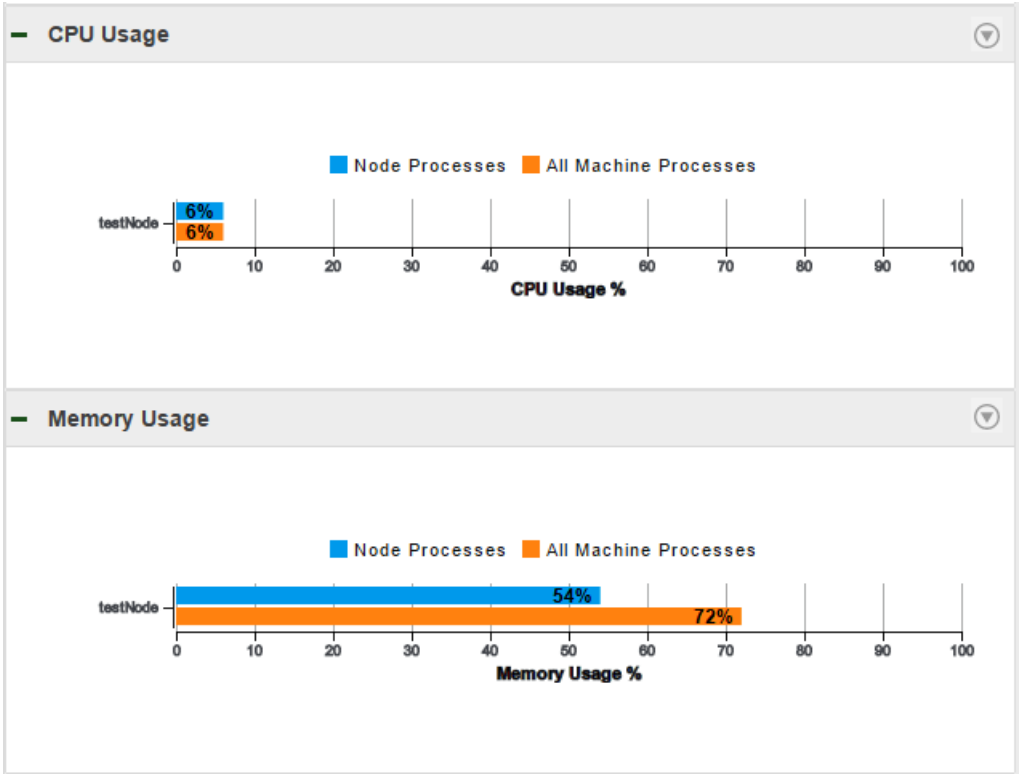
Object	Details Panel Content
Service running on a grid	The Details panel displays the following content for a service that runs on a grid: - Service name and state. Click the service name to view the service properties. - Nodes in the grid. Click a node name to view the node properties. - State of the nodes on which the service processes run. - State of the service processes.
Service in high availability mode	The Details panel displays the following content for a service that is highly available: - Service name and state. Click the service name to view the service properties. - Nodes on which the service is configured to run. Click a node name to view the node properties. - State of the nodes on which the service processes run. - State of the service process on the nodes.
Grid	The Details panel displays the following content for a grid: - Grid name and state. Click the grid name to view the grid properties. - Nodes in the grid. Click a node name to view the node properties. - State of nodes running in the grid.

Resource Usage Indicators

The resource usage indicators are bar charts and graphs that compare resource usage for a domain process to resource usage of all processes on the machine. Select a domain process to compare with all processes. You can view current usage statistics or statistics for the previous 60 minutes.

You can view usage statistics for memory and CPU. Choose whether to view current statistics or to view graphs of usage for the past 60 minutes. Click the selection arrow and choose **Current**.

The following image shows the current resource usage in a domain that contains one node:



The information that the graphs display varies based on which domain object you select.

The following table describes the information that you can view when you select the domain or a domain object:

Domain Object	Usage Indicator Content
Domain	The usage indicators display the following content: - Nodes in the domain. - Resource usage of all processes running on each node in the domain. - Resource usage of all processes running on the machine.
Node	The usage indicators display the following content: - The node. - Resource usage of processes running on the node. - Resource usage of all processes running on the machine.
Service	The usage indicators display the following content: - The node on which the service process runs. - Resource usage of the service process that is running on the node. - Resource usage of all processes running on the machine.
Service in high availability mode	The usage indicators display the following content: - The node on which the service process is running. - Resource usage of the service process that is running on the node. - Resource usage of all processes running on the machine.
Service running on a grid	The usage indicators display the following content: - All nodes on which the service process runs. - Resource usage of the service process that is running on each node. - Resource usage of all processes running on the machine.
Grid	The usage indicators display the following content: - All available nodes in the grid. - Resource usage of all processes running on each node in the domain. - Resource usage of all processes running on the machine.

If a **See More...** link appears in the indicator, you can click it to view the complete list of nodes in the domain. You can sort the list by node name, process usage on the nodes, or process usage on the machine. You can also search the list for a particular node.

Manage Tab - Services and Nodes View

The **Services and Nodes** view shows all application services and nodes defined in the domain.

The **Services and Nodes** view has the following components:

Navigator

Appears in the left pane of the **Manage** tab. The Navigator displays the following types of objects:

- Domain. You can view one domain, which is the highest object in the Navigator hierarchy.
- Folders. Use folders to organize domain objects in the Navigator. Select a folder to view information about the folder and the objects in the folder.
- Application services. An application service represents server-based functionality. Select an application service to view information about the service and its processes.

- System services. A system service is an application service that can have a single instance in the domain. Select a system service to view information about the service and its processes.
- Nodes. A node represents a machine in the domain. You configure service processes to run on nodes with the service role.
- Grids. Create a grid to run the CDI-PC Integration Service on multiple nodes. Select a grid to view nodes assigned to the grid.
- Licenses. Create a license on the **Manage** tab based on a license key file provided by Informatica. Select a license to view services assigned to the license.

You can search for nodes, services, and grids in the Navigator.

Contents panel

Appears in the right pane of the **Manage** tab and displays information about the domain or domain object that you select in the Navigator.

Actions menu in the Navigator

When you select the domain in the Navigator, you can create a folder, service, node, grid, or license.

When you select a domain object in the Navigator, you can delete the object, refresh the object, or move it to a folder.

Actions menu on the Manage tab

When you select the domain in the Navigator, you can shut down the domain or view logs for the domain.

When you select a node in the Navigator, you can remove a node association, recalculate the CPU profile benchmark, or shut down the node.

When you select a service in the Navigator, you can recycle or disable the service and configure properties for the service.

When you select a license in the Navigator, you can add an incremental key to the license.

Navigator Search

You can search for and filter nodes, application services, and grids in the Navigator.

You can perform the following tasks in the Navigator search section:

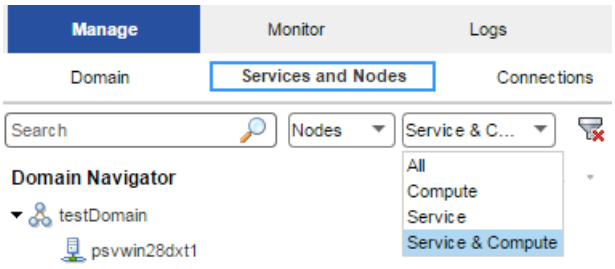
Search by object name.

In the search text box, enter the name or partial name of the object to search for. The Navigator displays the search results.

Filter by object type.

Click **Filters**, and then select the object type to filter by. If you filter by nodes, you can filter further by node role. If you filter by services, you can filter further by service type. The Navigator displays the filtered results.

The following image displays the Navigator search section filtered by nodes with the service and compute roles:



Reset filters.

Click **Reset Filters** to clear any filters or entered search text.

Domain

You can view one domain in the **Services and Nodes** view on the **Manage** tab. It is the highest object in the Navigator hierarchy.

When you select the domain in the Navigator, the contents panel shows the following views and buttons:

- **Properties** view. View or edit domain resilience properties.
- **Resources** view. View available resources for each node in the domain.
- **Permissions** view. View or edit group and user permissions on the domain.
- **Plug-ins** view. View plug-ins registered in the domain.
- **View Domain Logs** button. View logs for the domain and services in the domain.

In the **Actions** menu in the Navigator, you can add a folder, node, grid, application service, or license to the domain.

In the **Actions** menu on the **Manage** tab, you can shut down the domain, view logs, or access help for the current view.

Folders

You can use folders in the domain to organize objects and to manage security.

Folders can contain nodes, services, grids, licenses, and other folders.

When you select a folder in the Navigator, the Navigator opens to display the objects in the folder. The contents panel displays the following information:

- **Properties** view. Displays the name and description of the folder.
- **Permissions** view. View or edit group and user permissions on the folder.

In the **Actions** menu in the Navigator, you can delete the folder, move the folder into another folder, refresh the contents on the **Manage** tab, or access help for the current tab.

Note: The System_Services folder is created for you when you create the domain, and contains all of the system services. A system service is an application service that can have a single instance in the domain. You cannot delete, move, or edit the properties or contents of the System_Services folder.

Application Services

Application services are a group of services that represent Informatica server-based functionality.

In the **Services and Nodes** view on the **Manage** tab, you can create and manage the following application services:

CDI-PC Repository Service

Manages the CDI-PC repository. It retrieves, inserts, and updates metadata in the repository database tables. Select a CDI-PC Repository Service in the Navigator to access information about the service.

When you select a CDI-PC Repository Service in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state and operating mode of the service. Manage general and advanced properties, node assignments, and database properties.
- **Processes** view. View the state of the service process on each node. View and edit service process properties on each assigned node.
- **Connections and Locks** view. View and terminate repository connections and object locks.
- **Plug-ins** view. View and manage registered plug-ins.
- **Permissions** view. View or edit group and user permissions on the CDI-PC Repository Service.
- **Actions** menu. Manage the contents of the repository and perform other administrative tasks.

CDI-PC Integration Service

Runs CDI-PC sessions and workflows. Select a CDI-PC Integration Service in the Navigator to access information about the service.

When you select a CDI-PC Integration Service in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state of the service. View or edit Integration Service properties.
- **Associated Repository** view. View or edit the repository associated with the Integration Service.
- **Processes** view. View the state of the service process on each node. View or edit the service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Integration Service.
- **Actions** menu. Manage the service.

PowerExchange Listener Service

Runs the PowerExchange Listener.

When you select a Listener Service in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state of the service and the URL of the PowerExchange Listener instance. View or edit Listener Service properties.
- **Actions** menu. Contains actions that you can perform on the Listener Service, such as viewing logs or enabling and disabling the service.

PowerExchange Logger Service

Runs the PowerExchange Logger for Linux, UNIX, and Windows.

When you select a Logger Service in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state of the service and the URL of the PowerExchange Logger instance. View or edit Logger Service properties.
- **Actions** menu. Contains actions that you can perform on the Logger Service, such as viewing logs or enabling and disabling the service.

SAP BW Service

Listens for RFC requests from SAP BW and initiates workflows to extract from or load to SAP BW. Select an SAP BW Service in the Navigator to access properties and other information about the service.

When you select an SAP BW Service in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state of the service. Manage general properties and node assignments.
- **Associated Integration Service** view. View or edit the Integration Service associated with the SAP BW Service.
- **Processes** view. View the state of the service process on each node. View or edit the directory of the BWParam parameter file.
- **Permissions** view. View or edit group and user permissions on the SAP BW Service.
- **Actions** menu. Manage the service.

Web Services Hub

A web service gateway for external clients. It processes SOAP requests from web service clients that want to access CDI-PC functionality through web services. Web service clients access the CDI-PC Integration Service and CDI-PC Repository Service through the Web Services Hub.

When you select a Web Services Hub in the Navigator, the contents panel displays the following information:

- **Properties** view. View the state of the service. View or edit Web Services Hub properties.
- **Associated Repository** view. View the CDI-PC Repository Service associated with the Web Services Hub.
- **Permissions** view. View or edit group and user permissions on the Web Services Hub.
- **Actions** menu. Manage the service.

Nodes

A node is a logical representation of a physical machine in the domain. On the Services and Nodes view on the Manage tab, you assign resources to nodes and configure service processes to run on nodes that have the service role.

When you select a node in the Navigator, the contents panel displays the following information:

- **Properties** view. View the status of the node. View or edit node properties, such as the repository backup directory or range of port numbers for the processes that run on the node.
- **Processes** view. View the status of processes configured to run on the node. Service processes run on nodes that have the service role.
- **Resources** view. View or edit resources assigned to the node.
- **Permissions** view. View or edit group and user permissions on the node.

In the **Actions** menu in the Navigator, you can delete the node, move the node to a folder, refresh the contents on the **Manage** tab, or access help on the current tab.

In the **Actions** menu on the **Manage** tab, you can remove the node association, recalculate the CPU profile benchmark, or shut down the node.

Grids

A grid is an alias assigned to a group of nodes that run CDI-PC Integration Service jobs.

When you run a job on a grid, the Integration Service distributes the processing across multiple nodes in the grid. You assign nodes to the grid in the **Services and Nodes** view on the **Manage** tab.

When you select a grid in the Navigator, the contents panel displays the following information:

- **Properties** view. View or edit node assignments to a grid.
- **Permissions** view. View or edit group and user permissions on the grid.

In the **Actions** menu in the Navigator, you can delete the grid, move the grid to a folder, refresh the contents on the **Manage** tab, or access help for the current tab.

Licenses

You create a license object on the **Manage** tab based on a license key file provided by Informatica.

After you create the license, you can assign services to the license.

When you select a license in the Navigator, the contents panel displays the following information:

- **Properties** view. View license properties, such as supported platforms, repositories, and licensed options. You can also edit the license description.
- **Assigned Services** view. View or edit the services assigned to the license.
- **Options** view. View the licensed CDI-PC options.
- **Permissions** view. View or edit user permissions on the license.

In the **Actions** menu in the Navigator, you can delete the license, move the license to a folder, refresh the contents on the **Manage** tab, or access help on the current tab.

In the **Actions** menu on the **Manage** tab, you can add an incremental key to a license.

Logs Tab

The **Logs** tab shows logs.

On the **Logs** tab, you can view the following types of logs:

- Domain log. Domain log events are log events generated from the domain functions that the Service Manager performs.
- Service log. Service log events are log events generated by each application service.
- User Activity log. User Activity log events monitor user activity in the domain.

The **Logs** tab displays the following components for each type of log:

- Filter. Configure filter options for the logs.

- Log viewer. Displays log events based on the filter criteria.
- Reset filter. Reset the filter criteria.
- Copy rows. Copy the log text of the selected rows.
- **Actions** menu. Contains options to save, purge, and manage logs. It also contains filter options.

Reports Tab

The **Reports** tab shows domain reports.

On the **Reports** tab, you can run the following domain reports:

- License Management Report. Run a report to monitor the number of software options purchased for a license and the number of times a license exceeds usage limits. Run a report to monitor the usage of logical CPUs and CDI-PC Repository Service. You run the report for a license.
- Web Services Report. Run a report to analyze the performance of web services running on a Web Services Hub. You run the report for a time interval.

Security Tab

You administer Informatica security on the Security tab of the Administrator tool.

The Security tab has the following components:

- Search section. Search for users, groups, or roles by name.
- Navigator. The Navigator appears in the left pane and displays groups, users, and roles.
- Contents panel. The contents panel displays properties and options based on the object selected in the Navigator and the tab selected in the contents panel.
- Security Actions menu. Contains options to create or delete a group, user, or role. You can manage LDAP configurations and operating system profiles. You can also view users that have privileges for a service.

Using the Search Section

Use the Search section to search for users, groups, and roles by name. Search is not case sensitive.

1. In the Search section, select whether you want to search for users, groups, or roles.
2. Enter the name or partial name to search for.

   You can include an asterisk (*) in a name to use a wildcard character in the search. For example, enter “ad*” to search for all objects starting with “ad”. Enter “*ad” to search for all objects ending with “ad”.
3. Click Go.

   The Search Results section appears and displays a maximum of 100 objects. If your search returns more than 100 objects, narrow your search criteria to refine the search results.
4. Select an object in the Search Results section to display information about the object in the contents panel.

Using the Security Navigator

The Navigator appears in the contents panel of the Security tab. When you select an object in the Navigator, the contents panel displays information about the object.

The Navigator on the Security tab displays one of the following sections based on what you are viewing:

- Groups section. Select a group to view the properties of the group, the users assigned to the group, and the roles and privileges assigned to the group.
- Users section. Select a user to view the properties of the user, the groups the user belongs to, and the roles and privileges assigned to the user.
- Roles section. Select a role to view the properties of the role, the users and groups that have the role assigned to them, and the privileges assigned to the role.
- Operating Profiles section. Select an operating profile to view the properties of the operating system profile, and the permissions assigned to users and groups that use the operating system profile.
- LDAP Configuration section. Select a configuration to view the LDAP server connection details, the LDAP security domain that contains users and groups imported from the LDAP directory service, and the LDAP synchronization schedule.

The Navigator provides different ways to complete a task. You can use any of the following methods to manage groups, users, and roles:

- Click the **Actions** menu. Each section of the Navigator includes an Actions menu to manage groups, users, roles, operating system profiles, or LDAP configurations.
- Right-click an object. Right-click an object in the Navigator to display the options available in the Actions menu.
- Use keyboard shortcuts. Use keyboard shortcuts to move to different sections of the Navigator.

Groups

A group is a collection of users and groups that can have the same privileges, roles, and permissions.

The Groups section of the Navigator organizes groups into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Groups section of the Navigator, the contents panel displays all groups belonging to the security domain.

When you select a group in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the group and users assigned to the group.
- Privileges. Displays the privileges and roles assigned to the group for the domain and for application services in the domain.
- Permissions. Displays the level of access that users within the group have perform tasks on domain objects, including nodes, grids and application services . Also displays the level of access that users within the group have to perform tasks on connection objects and operating system profiles.

Users

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator

- CDI-PC Client

The Users section of the Navigator organizes users into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Users section of the Navigator, the contents panel displays all users belonging to the security domain.

When you select a user in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the user and all groups to which the user belongs.
- Privileges. Displays the privileges and roles assigned to the user for the domain and for application services in the domain.
- Permissions. Displays the level of access that the user has to perform tasks on domain objects, including nodes, grids and application services . Also displays the level of access that the user has to perform tasks on connection objects and operating system profiles.

Roles

A role is a collection of privileges that you assign to a user or group. Privileges determine the actions that users can perform. You assign a role to users and groups for the domain and for application services in the domain.

The Roles section of the Navigator organizes roles into the following folders:

- System-defined Roles. Contains roles that you cannot edit or delete. The Administrator role is a system-defined role.
- Custom Roles. Contains roles that you can create, edit, and delete. The Administrator tool includes some custom roles that you can edit and assign to users and groups.

When you select a folder in the Roles section of the Navigator, the contents panel displays all roles belonging to the folder.

When you select a role in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the role and the users and groups that have the role assigned for the domain and application services.
- Privileges. Displays the privileges assigned to the role for the domain and application services.

Operating System Profiles

An operating system profile is a security mechanism that the CDI-PC Integration Service use to run mappings, workflows, and profiling jobs.

The Operating System Profiles section of the Navigator lists the operating system profiles configured in the domain.

When you select an operating system profile in the Navigator, the contents panel displays the following tabs:

- Properties. Displays general properties of the operating system profile configured for the CDI-PC Integration Service.
- Permissions. Displays the permissions assigned to users and groups that use the operating system profile. Also indicates whether the operating system profile is the default profile assigned to a user or group.

LDAP Configuration

You can configure an Informatica domain to enable users and groups imported from one or more LDAP directory services to log in to Informatica nodes, services, and application clients.

The LDAP Configuration section of the Navigator lists the LDAP configurations the domain uses.

When you select an LDAP configuration, the following tabs appear under the LDAP Configuration tab:

- Overview. Lists the connection details for the LDAP server that contains the directory service from which you want to import users and groups.
- Security Domains. Lists the details for the LDAP security domain that contains users and groups imported from the LDAP directory service.
- Schedule. Lists the details for the synchronization schedule specifying when the Service Manager updates the security domain with the users and groups in the LDAP directory service.

Account Management

To improve security in the Informatica domain, you can enforce lockout of user and administrator accounts after a specified number of failed login attempts.

The Account Lockout Configuration section of the Account Management page displays whether account lockout is enabled for user accounts and administrator accounts. The section also indicates the maximum number of failed login attempts allowed.

The Locked Out Native Users section of the page lists locked out user accounts in the native security domain. You can unlock a user account in the native security domain.

The Locked Out LDAP Users section of the page lists locked out user accounts in an LDAP security domain. You can unlock a user account in the Informatica domain. However, the LDAP administrator must unlock the user account in the LDAP server. The user cannot log in to the Informatica domain until the LDAP administrator unlocks the user account.

Audit Reports

Audit reports provide information about users and groups in the Informatica domain, and about the privileges, roles, and permissions assigned to each user or group.

You select the audit report to generate from the Select Report Type menu. You can generate the following audit reports:

User Personal Information

Displays contact information and status details of user accounts in the domain. You can select the users or groups for which you want to generate the report.

User Group Association

Displays information about users and the groups to which they belong. You can select the users or groups for which you want to generate the report.

Privileges

Displays information about privileges assigned to the users and groups in the domain. You can select the users or groups for which you want to generate the report.

Roles

Displays information about the roles assigned to the users and groups in the domain. You can select the roles for which you want to generate the report.

Domain Object Permissions

Displays information about the domain objects for which users and groups have permission. You can select the users or groups for which you want to generate the report.

Service States

You can identify the state of an application service by the icon that displays in the Administrator tool.

The following table describes the icons that indicate service states:

State	Icon
Available	
Disabled	
Unavailable	

Process States

You can identify the state of a CDI-PC Integration Service process by the icon that displays in the Administrator tool.

The state icons also indicate the type of node on which the process runs. If the primary node has high availability, a yellow diamond is superimposed on the process state icon. If the process runs on a grid, a grid icon is superimposed on the process state icon.

The following table describes the icons that indicate process states:

State	Icon
Aborted	
Aborted (with high availability)	
Aborted (Grid)	
Disabled	
Disabled (with high availability)	

State	Icon
Disabled (Grid)	
Failed	
Failed (with high availability)	
Failed (Grid)	
Running	
Running (with high availability)	
Running (Grid)	
Standing by or Delayed	
Standing by or Delayed (with high availability)	
Standing by or Delayed (Grid)	
Starting	
Starting (with high availability)	
Starting (Grid)	
Stopped	
Stopped (with high availability)	
Stopped (Grid)	
Stopping	
Stopping (with high availability)	
Stopping (Grid)	

Job States

You can identify the state of a job by the icon that displays in the Administrator tool.

The following table describes the icons associated with each job state:

State	Icon
Aborted	
Canceled	
Completed	
Failed	
Queued or Pending	
Running	
Starting	
Stopped	
Stopping	
Terminated	
Unknown	

Informatica Administrator Accessibility Overview

You can use a screen reader and keyboard shortcuts to navigate and work with the Administrator tool interface.

To turn the JAWS Virtual PC cursor on and off, use the keyboard shortcut **Insert+Z**.

Note: To use the JAWS screen reader with the Administrator tool, you must use Internet Explorer 11.

Keyboard Shortcuts

You can use keyboard shortcuts to navigate and work with the Administrator tool interface.

You can add, edit, and change values in the Administrator tool. Keyboard focus in the Administrator tool is indicated by a blue border around the interface label. A dotted line appears around a selected object indicating that the object is in focus. Tooltips appear when the label item receives keyboard focus or on mouse-over. The navigation order of objects in the editor is from top to bottom and left to right.

You can perform the following tasks with keyboard shortcuts:

Navigate among elements and select an element

Press **Tab**.

Select the previous object

Press **Shift+Tab**.

Navigate among perspective tabs

Press the **Left** or **Right** arrow key.

Select or clear a check box or radio button

Press the **Space** bar.

Upload files using the File Upload button

Press the **Space** bar.

Navigate through records in a dialog box

Press the **Up** or **Down** arrow key.

Select and open a drop-down menu item with sub-menus

Press the **Space** arrow key. To go back to the main menu, press **Esc**.

Edit the value of grid content such as the Access and Revoke fields in the Assign Permission and Edit Direct Permissions dialog box

Press the **Space** bar.

Note: You must enter appropriate values for all the form elements marked with an asterisk (*).

Move focus from Update Frequency drop-down menu to Time Range check box in the Statistics and Reports list grid in the Report and Statistic Settings dialog box of the Monitor tab or Monitoring tool

Press **Esc**.

You cannot access the split bars in the Administrator tool and increase or decrease the size of the panels using the keyboard. You cannot select multiple items with the **Ctrl** key in the Audit Reports tab under Security.

CHAPTER 4

Using the Domain View

This chapter includes the following topics:

About the Domain View

The Domain view displays an overview of the status of the domain and the objects it contains. You can use the Domain view to review current and historical information about the domain.

Use the Domain view to perform the following tasks:

- View current status, resource usage, and details for the domain and objects in the domain.
- View dependencies among objects in the domain.
- Perform domain actions such as shutting down the domain, enabling and disabling services, and shutting down nodes.
- View recent service commands that users issued from the Administrator tool.
- View historical information about status, resource usage, and events in the domain.

Dependency Graph

The **Dependency** graph displays dependencies among services, nodes, and grids in the Informatica domain.

You can use the **Dependency** graph to perform the following tasks:

- View dependencies among nodes, services, and grids.
- Shut down a node.
- Enable, disable, or recycle a service.
- Disable or recycle services that depend on other services.

When you view dependencies for an object, the **Dependency** graph displays the upstream and downstream dependencies. Upstream dependencies are objects on which the selected object depends. Downstream dependencies are objects that depend on the selected object.

When you enable, disable, or recycle services from the **Dependency** graph, the actions appear in the **Command History** panel.

Viewing Dependencies for Application Services, Nodes, and Grids

You can view dependencies among application services, nodes, and grids in the Informatica domain.

1. In the Administrator tool, click the **Manage** tab.
2. In the contents panel, click the **Actions** menu for a domain object, and then select **View Dependencies**.

   The **Dependency** graph opens and displays the object and its direct dependencies.
   The **Dependency** graph displays domain objects connected by blue and orange lines, as follows:

   - Blue lines indicate service-to-node and service-to-grid dependencies.
   - Dashed blue lines indicate backup node-to-service dependencies.
   - Orange lines indicate service-to-service dependencies.

   The following table describes the information that appears in the **Dependency** graph based on the object:

Domain Object	Upstream Dependencies	Downstream Dependencies
Node	N/A	Services that run on the node.
Node running in a grid	N/A	The node has the following downstream dependencies: - Grid in which the node runs. - Service process that runs on the grid. - Service processes that run on the node, but not in the grid.
Service	Node on which the service process runs.	Services that depend on the service.
Service running on a grid	The service has the following upstream dependencies: - Nodes on which the service process runs. - The grid on which the service processes run.	Services that depend on the service.
Service running in HA mode	Primary and backup nodes on which the service processes can run.	Services that depend on the service.
Grid	Nodes assigned to the grid.	Services that are running on the grid.

3. In the **Dependency** graph, you can optionally complete the following tasks:
   - Select **Show Legend** to view information about the icons and lines used in the graph.
   - Click and drag to view different parts of the graph.
   - Zoom in or zoom out of the graph.
   - To exit the **Dependency** graph, click **Close**.

Recycling or Disabling Downstream Services

You can recycle or disable downstream services in the **Dependency** graph.

Downstream services are services that depend on other services. You recycle or disable downstream services using the Actions menu for the service on which they depend. When you disable downstream services, the service processes abort.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Actions** menu for a domain object, and then select **View Dependencies**.

   The **Dependency** graph opens and displays the object and its direct dependencies.
3. Click **Actions** > **Recycle Downstream Dependents** or **Actions** > **Disable Downstream Dependents**.

   The Recycle Downstream Dependents or Disable Downstream Dependents window appears.
4. Optionally, choose whether the action is **Planned** or **Unplanned**.
5. Optionally, enter comments about the action.
6. Select the services that you would like to recycle or disable.
7. Click **Recycle Services** or **Disable Services**.

Command History

The **Command History** panel on the **Domain** view displays recent service lifecycle commands that users issued from the Administrator tool. Service lifecycle commands include enable, disable, and recycle.

To view the command history, click **Domain Actions** > **View Command History**.

You can view the following information about the commands in the **Command History** panel:

- Service Name. Name of the service for which the command was issued.
- Service Type.
- Command.
- Status. Can be Failed, Success, or Queued.
- Status Updated
- Comments. Comments that users entered when they recycled or disabled the service.
- Message. Log messages associated with the command.

Optionally, you can show or hide columns in the command history. To change the columns, right-click the column header, and then select or clear columns.

Note: The command history is erased when you shut down or restart the master gateway node.

CHAPTER 5

Domain Management

This chapter includes the following topics:

Domain Management Overview

An Informatica domain is a collection of nodes and services that define the Informatica environment. To manage the domain, you manage the nodes and services within the domain.

Use the Administrator tool to complete the following tasks:

- Manage alerts. Configure, enable, and disable domain and service alerts for users.
- Create folders. Create folders to organize domain objects and manage security by setting permission on folders.
- Manage domain security. Configure secure communication between domain components.
- Manage user security. Assign privileges and permissions to users and groups.
- Manage application services. Enable, disable, recycle, and remove application services. Enable and disable service processes.
- Manage nodes. Configure node properties, such as the backup directory and resources, and shut down nodes.
- Configure gateway nodes. Configure nodes to serve as a gateway.
- Shut down the domain. Shut down the domain to complete administrative tasks on the domain.

- Manage domain configuration. Back up the domain configuration on a regular basis. You might need to restore the domain configuration from a backup to migrate the configuration to another database user account. You might also need to reset the database information for the domain configuration if it changes.
- Complete domain tasks. You can monitor the statuses of all application services and nodes, view dependencies among application services and nodes, and shut down the domain.
- Configure domain properties. For example, you can change the database properties, SMTP properties for alerts, and domain resiliency properties.

To manage nodes and services through a single interface, all nodes and services must be in the same domain. You cannot access multiple Informatica domains in the same Administrator tool window. You can share metadata between domains when you register or unregister a local repository in the local Informatica domain with a global repository in another Informatica domain.

Alert Management

Alerts provide users with domain and service alerts. Domain alerts provide notification about node failure and master gateway election. Service alerts provide notification about service process failover.

To use the alerts, complete the following tasks:

- Configure the SMTP settings for the outgoing email server.
- Subscribe to alerts.

After you configure the SMTP settings, users can subscribe to domain and service alerts.

Configuring SMTP Settings

You configure the SMTP settings for the outgoing mail server to enable alerts.

Configure SMTP settings on the domain **Properties** view.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.
4. In the contents panel, click the **Properties** view.
5. In the SMTP Configuration section, click **Edit**.
6. Edit the SMTP settings.

Property	Description
Host Name	The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook.
Port	Port used by the outgoing mail server. Valid values are from 1 to 65535. Default is 25.
User name	The user name for authentication upon sending if required by the outbound mail server.

Property	Description
Password	The user password for authentication upon sending if required by the outbound mail server.
Sender Email Address	The email address that the Service Manager uses in the From field when sending notification emails. If you leave this field blank, the Service Manager uses `Administrator@<host name>` as the sender.

7. Click **OK**.

Subscribing to Alerts

After you complete the SMTP configuration, you can subscribe to alerts.

1. Verify that the domain administrator has entered a valid email address for your user account on the **Security** page.

   If the email address or the SMTP configuration is not valid, the Service Manager cannot deliver the alert notification.
2. In the Administrator tool header area, click **Manage** > **Preferences**.

   The **Preferences** page appears.
3. In the User Preferences section, click **Edit**.

   The **Edit Preferences** dialog box appears.
4. Select **Subscribe for Alerts**.
5. Click **OK**.
6. Click **OK**.

The Service Manager sends alert notification emails based on your domain privileges and permissions.

The following table lists the alert types and events for notification emails:

Alert Type	Event
Domain	Node Failure Master Gateway Election
Service	Service Process Failover

Viewing Alerts

When you subscribe to alerts, you can receive domain and service notification emails for certain events. When a domain or service event occurs that triggers a notification, you can track the alert status in the following ways:

- The Service Manager sends an alert notification email to all subscribers with the appropriate privilege and permission on the domain or service.
- The Log Manager logs alert notification delivery success or failure in the domain or service log.

For example, the Service Manager sends the following notification email to all alert subscribers with the appropriate privilege and permission on the service that failed:

```
From: Administrator@<database host>
To: Jon Smith
```

```
Subject: Alert message of type [Service] for object [HR_811].
The service process on node [node01] for service [HR_811] terminated unexpectedly.
```

In addition, the Log Manager writes the following message to the service log:

```
ALERT_10009 Alert message [service process failover] of type [service] for object
[HR_811] was successfully sent.
```

You can review the domain or service logs for undeliverable alert notification emails. In the domain log, filter by Alerts as the category. In the service logs, search on the message code ALERT. When the Service Manager cannot send an alert notification email, the following message appears in the related domain or service log:

```
ALERT_10004: Unable to send alert of type [alert type] for object [object name], alert
message [alert message], with error [error].
```

Folder Management

Use folders in the domain to organize objects and to manage security.

Folders can contain nodes, services, grids, licenses, and other folders. You might want to use folders to group services by type. For example, you can create a folder called IntegrationServices and move all Integration Services to the folder. Or, you might want to create folders to group all services for a functional area, such as Sales or Finance.

When you assign a user permission on the folder, the user inherits permission on all objects in the folder.

You can perform the following tasks with folders:

- View services and nodes. View all services in the folder and the nodes where they run. Click a node or service name to access the properties for that node or service.
- Create folders. Create folders to group objects in the domain.
- Move objects to folders. When you move an object to a folder, folder users inherit permission on the object in the folder. When you move a folder to another folder, the other folder becomes a parent of the moved folder.
- Remove folders. When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

Note: The System_Services folder is created for you when you create the domain, and contains all of the system services. A system service is an application service that can have a single instance in the domain. You cannot delete, move, or edit the properties or contents of the System_Services folder.

Creating a Folder

You can create a folder in the domain or in another folder.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select the domain or folder in which you want to create a folder.
3. On the Navigator Actions menu, click New > Folder.

4. Edit the following properties:

Node Property	Description
Name	Name of the folder. The name is not case sensitive and must be unique within the domain. It cannot exceed 80 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the folder. The description cannot exceed 765 characters.
Path	Location in the Navigator.

5. Click OK.

Moving Objects to a Folder

When you move an object to a folder, folder users inherit permission on the object. When you move a folder to another folder, the moved folder becomes a child object of the folder where it resides.

Note: The domain serves as a folder when you move objects in and out of folders.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select an object.
3. On the Navigator Actions menu, select Move to Folder.
4. In the Select Folder dialog box, select a folder, and click OK.

Removing a Folder

When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select a folder.
3. On the Navigator Actions menu, select Delete.
4. Confirm that you want to delete the folder.

   You can delete the contents only if you have the appropriate privileges and permissions on all objects in the folder.
5. Choose to wait until all processes complete or to abort all processes.
6. Click OK.

Domain Security Management

You can configure Informatica domain components to use the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to encrypt connections with other components. When you enable SSL or TLS for domain components, you ensure secure communication.

You can configure secure communication in the following ways:

Between services within the domain

You can configure secure communication between services within the domain.

Between the domain and external components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

Each method of configuring secure communication is independent of the other methods. When you configure secure communication for one set of components, you do not need to configure secure communication for any other set.

Note: If you change a non-secure domain to a secure domain, you must delete the domain configuration in the CDI-PC Client tools and configure the domain again in the client.

User Security Management

You manage user security within the domain with privileges and permissions.

Privileges determine the actions that users can complete on domain objects. Permissions define the level of access a user has to a domain object. Domain objects include the domain, folders, nodes, grids, licenses, database connections, operating system profiles, and application services.

Even if a user has the domain privilege to complete certain actions, the user might also require permission to complete the action on a particular object. For example, a user has the Manage Services domain privilege which grants the user the ability to edit application services. However, the user also must have permission on the application service. A user with the Manage Services domain privilege and permission on the Development Repository Service but not on the Production Repository Service can edit the Development Repository Service but not the Production Repository Service.

To log in to the Administrator tool, a user must have the Access Informatica Administrator domain privilege. If a user has the Access Informatica Administrator privilege and permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can view the object. For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties but cannot configure, shut down, or remove the node.

If a user does not have permission on a selected object in the Navigator, the contents panel displays a message indicating that permission on the object is denied.

Application Service Management

You can perform the following common administration tasks for application services:

- Enable and disable services and service processes.
- Configure the domain to restart service processes.
- Remove an application service.
- Troubleshoot problems with an application service.

Note: You can perform all of the common administration tasks for system services, except for removing the system service.

Enabling and Disabling Services and Service Processes

You can enable and disable application services and service processes in the Administrator tool. When a service is enabled, there must be at least one service process enabled and running for the service to be available. By default, all service processes are enabled.

The behavior of a service when it starts service processes depends on how it is configured:

- If the service is configured for high availability, then the service starts the service process on the primary node. The service processes on the backup nodes are in Standing By state.
- If the service is configured to run on a grid, then the service starts service processes on all nodes that have the service role.

A service does not start a disabled service process in any situation.

The state of a service depends on the state of its processes. A service can have the following states:

- Available. You have enabled the service and at least one service process is running. The service is available to process requests.
- Unavailable. You have enabled the service and none of its processes are running. This can be because the service processes are disabled or failed to start. The service is not available to process requests.
- Disabled. You have disabled the service.

You can disable a service to perform a management task, such as changing the data movement mode for a CDI-PC Integration Service. You might want to disable the service process on a node if you need to shut down the node for maintenance. When you disable a service, all associated service processes stop, but they remain enabled.

The following table describes the different states of a service and its processes:

Service Process Configuration	Service Process State	Description
Enabled	Running	The service process is running on the node.
Enabled	Standing By	The service process is enabled but is not running because another service process is running as the primary service process. It is on standby to run in case of service failover.
Disabled	Disabled	The service is enabled but the service process is not running on the node.
Enabled	Stopped	The service is unavailable.
Enabled	Failed	The service and service process are enabled, but the service process could not start.

Viewing Service Processes

You can view the state of a service process on the Processes view of a service. You can view the state of all service processes on the Overview view of the domain.
To view the state of a service process:

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select a service.
3. In the contents panel, select the Processes view.

   The Processes view displays the state of the processes.

Configuring Restart for Service Processes

If an application service process becomes unavailable while a node is running, the domain tries to restart the process on the same node based on the restart options configured in the domain properties.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select the domain.
3. In the Properties view, configure the following restart properties:

Domain Property	Description
Maximum Restart Attempts	Number of times within a specified period that the domain attempts to restart an application service process when it fails. The value must be greater than or equal to 1. Default is 3.
Within Restart Period (sec)	Maximum period of time that the domain spends attempting to restart an application service process when it fails. If a service fails to start after the specified number of attempts within this period of time, the service does not restart. Default is 900.

Removing Application Services

You can remove an application service using the Administrator tool. Before removing an application service, you must disable it.

Note: You cannot remove a system service.

Disable the service before you delete the service to ensure that the service is not running any processes. If you do not disable the service, you may have to choose to wait until all processes complete or abort all processes when you delete the service.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select the application service.
3. In the **Manage** tab Actions menu, select **Delete**.
4. In the warning message that appears, click **Yes** to stop other services that depend on the application service.
5. If the **Disable Service** dialog box appears, choose to wait until all processes complete or abort all processes, and then click **OK**.

Troubleshooting Application Services

I think that a service is using incorrect environment variable values. How can I find out which environment variable values are used by a service.

Set the error severity level for the node to debug. When the service starts on the node, the Domain log will display the environment variables that the service is using.

Gateway Configuration

A domain requires at least one node configured as a gateway node. You can configure multiple gateway nodes as backups.

One gateway node in the domain serves as the master gateway node for the domain. The Service Manager on the master gateway node accepts service requests and manages the domain and services in the domain. If the domain has one gateway node and it becomes unavailable, the domain cannot accept service requests. If the domain has multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect a new master gateway node. The new master gateway node accepts service requests. Only one gateway node can be the master gateway node at any particular time.

You can make the following changes to the gateway configuration for the domain:

Convert a worker node to serve as a gateway node.

You can convert a worker node to serve as a gateway node if the worker node is running and has the service role enabled. When you convert a worker node to a gateway node, you must specify the log directory for the node. If you have multiple gateway nodes, configure all gateway nodes to write log files to the same directory on a shared disk.

After you convert a worker node to a gateway node, the Service Manager on the master gateway node writes the domain configuration database connection to the nodemeta.xml file of the new gateway node.

Convert a gateway node to serve as a worker node.

You can convert a gateway node to serve as a worker node if another node in the domain is configured as a gateway node.

If you convert a master gateway node to serve as a worker node, you must restart the node to make the Service Managers elect a new master gateway node. If you do not restart the node, the node continues as the master gateway node until you restart the node or the node becomes unavailable.

Configuring the Gateway and Worker Nodes

You can convert an existing worker node to a gateway node. Or, you can convert an existing gateway node to a worker node.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select the domain.
3. In the contents panel, select the **Properties** view.
4. In the **Properties** view, click **Edit** in the **Gateway Configuration Properties** section.
5. To convert a worker node to a gateway node, complete the following steps:
   a. Select the check box next to the node.
   b. If the domain uses a secure domain configuration database, specify the truststore file and password for the database.
   c. Configure the directory path for the log files for each node that you convert to a gateway node.

      If you have multiple gateway nodes, configure all gateway nodes to write log files to the same directory on a shared disk.

      Note: You must use the infacmd isp SwitchToWorkerNode command to convert a a worker node to a gateway node in a domain configured to use SAML authentication. See the *Informatica Command Reference* for instructions on using the infacmd isp SwitchToWorkerNode command.
6. To convert a gateway node to a worker node, clear the check box next to the node.

7. Click **OK**.

Domain Configuration Management

The Service Manager on the master gateway node manages the domain configuration. The domain configuration is a set of metadata tables stored in a relational database that is accessible by all gateway nodes in the domain. Each time you make a change to the domain, the Service Manager writes the change to the domain configuration. For example, when you add a node to the domain, the Service Manager adds the node information to the domain configuration. The gateway nodes use a JDBC connection to access the domain configuration database.

You can perform the following domain configuration management tasks:

- Back up the domain configuration. Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup if the domain configuration in the database becomes corrupt.
- Restore the domain configuration. You may need to restore the domain configuration if you migrate the domain configuration to another database user account. Or, you may need to restore the backup domain configuration to a database user account.
- Migrate the domain configuration. You may need to migrate the domain configuration to another database user account.
- Configure the connection to the domain configuration database. Each gateway node must have access to the domain configuration database. You configure the database connection when you create a domain. If you change the database connection information or migrate the domain configuration to a new database, you must update the database connection information for each gateway node.
- Configure custom properties. Configure domain properties that are unique to your environment or that apply in special cases. Use custom properties only if Informatica Global Customer Support instructs you to do so.

Backing Up the Domain Configuration

Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup file if the domain configuration in the database becomes corrupt.

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Note: If the infasetup BackupDomain command fails with a Java memory error, increase the system memory available for infasetup. To increase system memory, set the -Xmx value in the INFA_JAVA_COMD_OPTS environment variable.

When you run this command, infasetup backs up the domain configuration database tables. To restore the domain to another database, you must back up the ISP_RUN_LOG table contents manually to get the previous workflow and session logs.

Additionally, use the database backup utility to manually back up additional repository tables that the infasetup command does not back up.

Restoring the Domain Configuration

You can restore domain configuration from a backup file. You may need to restore the domain configuration if the domain configuration in the database becomes inconsistent or if you want to migrate the domain configuration to another database.

Informatica restores the domain configuration from the current version. If you have a backup file from an earlier product version, you must use the earlier version to restore the domain configuration.

You can restore the domain configuration to the same or a different database user account. If you restore the domain configuration to a database user account with existing domain configuration, you must configure the command to overwrite the existing domain configuration. If you do not configure the command to overwrite the existing domain configuration, the command fails.

Each node in a domain has a host name and port number. When you restore the domain configuration, you can disassociate the host names and port numbers for all nodes in the domain. You might do this if you want to run the nodes on different machines. After you restore the domain configuration, you can assign new host names and port numbers to the nodes. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.

If you restore the domain configuration to another database, you must reset the database connections for all gateway nodes.

Important: You lose all data in the summary tables when you restore the domain configuration.

Complete the following tasks to restore the domain:

1. Disable the application services. Disable the application services in complete mode to ensure that you do not abort any running service process. You must disable the application services to ensure that no service process is running when you shut down the domain.
2. Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.
3. Assign new host names and port numbers to the nodes in the domain if you disassociated the previous host names and port numbers when you restored the domain configuration. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.
4. Reset the database connections for all gateway nodes if you restored the domain configuration to another database. All gateway nodes must have a valid connection to the domain configuration database.

Migrating the Domain Configuration

You can migrate the domain configuration to another database user account. You may need to migrate the domain configuration if you no longer support the existing database user account. For example, if your company requires all departments to migrate to a new database type, you must migrate the domain configuration.

1. Shut down all application services in the domain.
2. Shut down the domain.
3. Back up the domain configuration.
4. Create the database user account where you want to restore the domain configuration.
5. Restore the domain configuration backup to the database user account.
6. Update the database connection for each gateway node.

7. Start all nodes in the domain.
8. Enable all application services in the domain.

Important: Summary tables are lost when you restore the domain configuration.

Step 1. Disable All Application Services

You must disable all application services to disable all service processes. If you do not disable an application service and a user starts a service process while you are backing up and restoring the domain, the service process changes may be lost and data may become corrupt.

Disable application services in complete mode to ensure that you do not abort running service processes.

Disable the application services in the following order:

1. Web Services Hub
2. SAP BW Service
3. CDI-PC Integration Service
4. CDI-PC Repository Service

Step 2. Shut Down the Domain

You must shut down the domain to ensure that users do not modify the domain while you are migrating the domain configuration. For example, if the domain is running when you are backing up the domain configuration, users can create new services and objects. Also, if you do not shut down the domain and you restore the domain configuration to a different database, the domain becomes inoperative. The connections between the gateway nodes and the domain configuration database become invalid. The gateway nodes shut down because they cannot connect to the domain configuration database. A domain is inoperative if it has no running gateway node.

Step 3. Back Up the Domain Configuration

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Step 4. Create a Database User Account

Create a database user account if you want to restore the domain configuration to a new database user account.

Step 5. Restore the Domain Configuration

Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.

Step 6. Update the Database Connection

If you restore the domain configuration to a different database user account, you must update the database connection information for each gateway node in the domain. Gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration.

Step 7. Start All Nodes in the Domain

Start all nodes in the domain. You must start the nodes to enable services to run.

1. Shut down the gateway node that you want to update.
2. Run the *infasetup* UpdateGatewayNode command to update the gateway node.
3. Start the gateway node.
4. Repeat this process for each gateway node.

Step 8. Enable All Application Services

Enable all application services that you previously shut down. Application services must be enabled to run service processes.

Updating the Domain Configuration Database Connection

All gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration. When you create a gateway node or configure a node to serve as a gateway, you specify the database connection, including the database user name and password. If you migrate the domain configuration to a different database or change the database user name or password, you must update the database connection for each gateway node. For example, as part of a security policy, your company may require you to change the password for the domain configuration database every three months.

To update the node with the new database connection information, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the user or password, you must update the node.

To update the node after you change the user or password, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the host name or port number, you must redefine the node.

To redefine the node after you change the host name or port number, complete the following steps:

1. Shut down the gateway node.
2. In the Administrator tool, remove the node association.
3. Run the *infasetup* DefineGatewayNode command.

Rename the Domain

You can change the domain name and update nodes to reference the updated domain name.

If the Informatica domain uses Kerberos authentication, all service and node SPNs have the same Kerberos realm name. After you change the Informatica domain name, you must generate SPNs and keytab files with the new Informatica domain name.

To rename the domain, complete the following tasks:

1. If the domain contains a CDI-PC global repository, you must unregister all local repositories from the global repository.
2. Shut down the domain. Shut down the domain through the Administrator tool, ensuring that all nodes are shut down.
3. Back up the domain with the infasetup BackupDomain command.
4. Back up the sitekey and keytab files. By default, the files are in the following location:

   ```
   <Informatica installation directory>/isp/config/keys
   ```
5. Update the domain and nodes.

   To update the domain name, run the infasetup updateDomainName command from any gateway node.

   Run the updateGatewayNode and updateWorkerNode commands with the updated domain name for all the gateway and worker nodes.
6. On CDI-PC, register the local repository with a connected global repository with the updated domain name with the pmrep Register command.
7. You can create SPN and keytab files with the updated domain name for Kerberos authentication. Copy the keytab files in the keys directory. You can continue to use the older site key file. If you need to regenerate the site key when it is missing or corrupted, you must provide the older domain name.
8. Optionally, you can run the License Management Report in the Administrator tool to review the updated domain name.
9. You must configure the Informatica clients to use the updated domain name.

Shutting Down a Domain

To run administrative tasks on a domain, you might need to shut down the domain. For example, to back up and restore a domain configuration, you must first shut down the domain.

When you shut down a domain, the Service Manager on the master gateway node stops all application services and Informatica services in the domain. Any service processes running on nodes in the domain are aborted. To avoid possible loss of data or metadata and allow running processes to complete, you can shut down each node from the Administrator tool or from the operating system.

Before you shut down a domain, verify that all processes, including workflows, have completed and no users are logged in to repositories in the domain.

1. Click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.
4. Click **Manage tab Actions** > **Shut Down Domain** .

   The **Shut Down Domain** dialog box lists the processes that are running in the domain.
5. Click **Shut down**.

   The **Shutdown Down Domain** dialog box displays a warning message.
6. Click **Shut down**.

   The Service Manager on the master gateway node shuts down the application services and Informatica services on each node in the domain.
7. To restart the domain, restart Informatica services on the gateway and worker nodes in the domain.

Domain Properties

On the **Manage** tab, you can configure domain properties including database properties, gateway configuration, and service levels.

To view and edit properties, click the **Manage** tab. In the Navigator, select a domain. Then click the **Properties** view in the contents panel. The contents panel shows the properties for the domain.

You can configure the properties to change the domain. You cannot change the database properties in the Admin Console. You need to change these properties using the Command UpdateGatewayNode. You can change SMTP properties for alerts, and the domain resiliency properties.

You can configure the following domain properties:

- General properties. Edit general properties, such as service resilience and dispatch mode.
- Database properties. View the database properties, such as database name and database host.
- Gateway configuration properties. Configure a node to serve as gateway and specify the location to write log events.
- Service level management. Create and configure service levels.
- SMTP configuration. Edit the SMTP settings for the outgoing mail server to enable alerts.
- Custom properties. Edit custom properties that are unique to the Informatica environment or that apply in special cases. When you create a domain, it has no custom properties. Use custom properties only at the request of Informatica Global Customer Support.

General Properties

In the General Properties area, you can configure general properties for the domain.

To edit general properties, click **Edit**.

The following table describes the properties that you can edit in the General Properties area:

Property	Description
Name	Read-only. The name of the domain.
Resilience Timeout	The number of seconds that an application service tries to connect or reconnect to the CDI-PC Repository Service or the CDI-PC Integration Service. Valid values are from 0 to 1000000. Default is 30 seconds.
Limit on Resilience Timeout	The maximum number of seconds that application clients or application services can try to connect or reconnect to the CDI-PC Repository Service or the CDI-PC Integration Service. Default is 180 seconds.
Restart Period	The maximum amount of time in seconds that the domain spends trying to restart an application service process. Valid values are from 0 to 1000000.
Maximum Restart Attempts within Restart Period	The number of times that the domain tries to restart an application service process. Valid values are from 0 to 1000. If you set the value as 0, the domain does not try to restart the service process.

Property	Description
Dispatch Mode	The mode that the Load Balancer uses to dispatch CDI-PC Integration Service tasks to nodes in a grid. Select one of the following dispatch modes: - MetricBased - RoundRobin - Adaptive
Enable Secure Communication	Configures services to use the TLS protocol to transfer data securely within the domain. When you enable secure communication for the domain, services use secure connections to communicate with other Informatica application services and clients. Verify that all domain nodes are available before you enable secure communication for the domain. If a node is not available, the secure communication changes cannot be applied to the Service Manager of the node. To apply changes, restart the domain. Set this property to True or False.

Database Properties

In the Database Properties area, you can view the database properties for the domain, such as database name and database host. You cannot edit these properties in the Admin Console. You need to update these properties using the command UpdateGatewayNode.

The following table describes the Database properties :

Property	Description
Database Type	The type of database that stores the domain configuration metadata.
Database Host	The name of the machine hosting the database.
Database Port	The port number used by the database.
Database Name	The name of the database.
Database User	The user account for the database containing the domain configuration information.
Database TLS enabled	Indicates whether the database for the domain configuration repository is a secure database. True if the domain configuration repository database is secure. You can use a secure domain configuration repository if secure communication is enabled for the Informatica domain.

Note: The service manager uses the DataDirect drivers included with the Informatica installation. Informatica does not support the use of any other database driver.

Gateway Configuration Properties

In the Gateway Configuration Properties area, you can configure a node to serve as gateway for a domain and specify the directory where the Service Manager on this node writes the log event files.

If you edit gateway configuration properties, previous logs do not appear. Also, the changed properties apply to restart and failover scenarios only.

To edit gateway configuration properties, click **Edit**.

To sort gateway configuration properties, click the header of the column by which you want to sort.

The following table describes the properties that you can edit in the Gateway Configuration Properties area:

Property	Description
Node Name	Read-only. The name of the node.
Status	The status of the node.
Gateway	To configure the node as a gateway node, select this option. If the domain uses a secure domain configuration database, you must specify the truststore file and password for the database. To configure the node as a worker node, clear this option.
Log Directory Path	The directory path for the log event files. If the Log Manager cannot write to the directory path, it writes log events to the node.log file on the master gateway node.

Secure Domain Configuration Repository

If you configure a node as a gateway node and the domain uses a secure domain configuration database, you must specify the truststore file and password for the secure database.

If you configure multiple gateway nodes for the domain, set the database truststore file and password for all gateway nodes.

The following table describes the database truststore properties:

Property	Description
Database Truststore Password	Password for the truststore file.
Database Truststore Location	Path and file name of the truststore file for the secure database.

Note: To use a secure domain configuration repository database, the secure communication option must be enabled for the domain.

Service Level Management

In the Service Level Management area, you can view, add, and edit service levels.

Service levels set priorities among tasks that are waiting to be dispatched. When the Load Balancer has more tasks to dispatch than the CDI-PC Integration Service can run at the time, the Load Balancer places those tasks in the dispatch queue. When multiple tasks are in the dispatch queue, the Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

Because service levels are domain properties, you can use the same service levels for all repositories in a domain. You create and edit service levels in the domain properties or by using infacmd.

You can edit but you cannot delete the Default service level, which has a dispatch priority of 5 and a maximum dispatch wait time of 1800 seconds.

To add a service level, click **Add**.

To edit a service level, click the link for the service level.

To delete a service level, select the service level and click the Delete button.

The following table describes the properties that you can edit in the Service Level Management area:

Property	Description
Name	The name of the service level. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : / ? . < > | ! ( )] [After you add a service level, you cannot change its name.
Dispatch Priority	A number that sets the dispatch priority for the service level. The Load Balancer dispatches high priority tasks before low priority tasks. Dispatch priority 1 is the highest priority. Valid values are from 1 to 10. Default is 5.
Maximum Dispatch Wait Time (seconds)	The amount of time in seconds that the Load Balancer waits before it changes the dispatch priority for a task to the highest priority. Setting this property ensures that no task waits forever in the dispatch queue. Valid values are from 1 to 86400. Default is 1800.

SMTP Configuration

Use the SMTP Configuration properties to configure SMTP settings for the domain. The outgoing mail server uses the SMTP settings to send alerts and scorecard notifications.

The following table describes the properties that you can edit in the SMTP Configuration area:

Property	Description
Host Name	The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook.
Port	Port used by the outgoing mail server. Valid values are from 1 to 65535. Default is 25.
User name	The user name for authentication upon sending if required by the outbound mail server.
Password	The user password for authentication upon sending if required by the outbound mail server.
Sender Email Address	The email address that the Service Manager uses in the From field when sending notification emails. If you leave this field blank, the Service Manager uses `Administrator@<host name>` as the sender.

Custom Properties for the Domain

Configure custom properties that are unique to specific environments.

You might need to apply custom properties in special cases. When you define a custom property, enter the property name and an initial value. Define custom properties only at the request of Informatica Global Customer Support.

Configure a Catalog Service URL for Email Notifications

Configure a custom Catalog Service URL to access the Catalog Service from email notifications.

1. In the Navigator, select a domain.

2. Then click the Properties view in the contents panel.

   The contents panel shows the properties for the domain.

3. Click **Edit Custom Properties** > **New**.

   The New Custom Property window appears.

4. In the Name field, enter `LdmCustomOptions.change.notification.ldm.catalog.custom.url`. In the Value field, enter a URL based on your requirements. For example, `http://hostname.informatica.com:9085/`.

5. Click **OK**. Restart the Catalog Service.

CHAPTER 6

Nodes

This chapter includes the following topics:

Nodes Overview

A node is the logical representation of a machine in the domain. When you configure a domain with multiple nodes, you can scale service processing across multiple machines. The Service Manager runs on all nodes in the domain to support the domain and application services. If the Service Manager is not running, the node is not available.

An installation on multiple machines consists of a master gateway node, which hosts the domain, and additional gateway nodes and worker nodes that run Informatica application services. The node type determines whether the node can serve as a gateway or a worker node and determines the domain functions that the node performs. You define the node type when you install Informatica services and join the node to the domain. You can use the Administrator tool to change the node type after installation.

By default, each node in the domain can run application services and computational processes. The node role determines whether a node can run application services, computational processes, or both. If the node has the service role, you can view the application service processes running on the node. Before you remove or shut down a node, verify that all running processes are stopped. You might need to shut down the node if you need to perform maintenance on the machine or to ensure that domain configuration changes take effect.

Use the Manage tab of the Administrator tool to manage nodes, including configuring node properties, updating a node role, and removing nodes from a domain. The properties that you can configure depend on the node role.

If your license includes grid, you can configure the CDI-PC Integration Service to run on a grid. A grid is an alias assigned to a group of nodes. When you run jobs on a grid of nodes, you improve scalability and performance by distributing jobs to processes running on multiple nodes in the grid. When the CDI-PC

Integration Service runs on a grid, you can configure it to check the resources available on each node. Assign connection resources and define custom and file/directory resources on a node that is assigned to a CDI-PC Integration Service grid.

Node Types

The node type determines whether the node can serve as a gateway or worker node and determines the domain functions that the node performs.

You define the node type when you install Informatica services and join the node to the domain. You can use the Administrator tool to change the node type after installation. You change the node type in the gateway configuration properties for the domain.

Related Topics:

- "Gateway Configuration" on page 50

Gateway Nodes

A gateway node is any node that you configure to serve as a gateway for the domain. A gateway node can run application services and perform computations, and it can serve as a master gateway node. One gateway node acts as the master gateway at any given time. The master gateway node is the entry point to the domain.

The Service Manager on the master gateway node performs all domain functions on the master gateway node. The Service Managers running on other gateway nodes perform limited domain functions on those nodes.

You can configure more than one node to serve as a gateway. If the master gateway node becomes unavailable, the Service Managers on other gateway nodes elect another master gateway node. If you configure only one node to serve as the gateway and the node becomes unavailable, the domain cannot accept service requests.

Worker Nodes

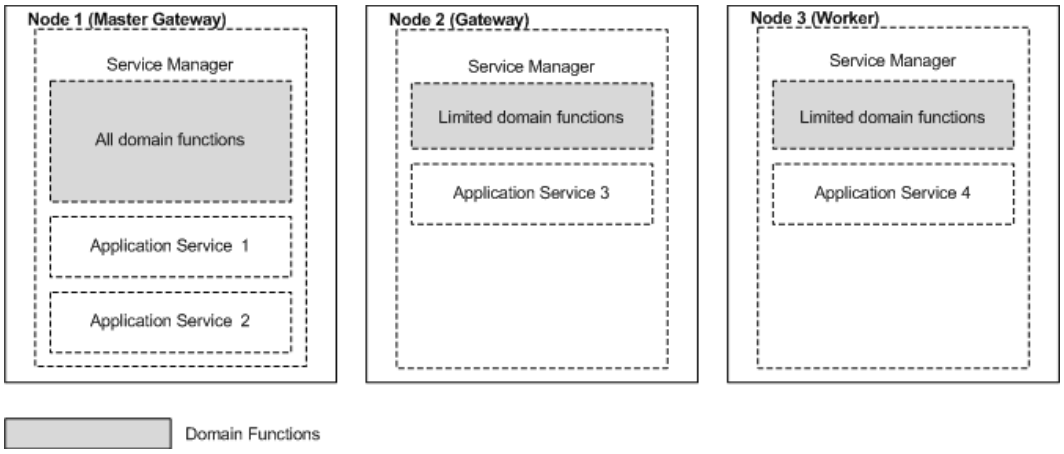
A worker node is any node that you do not configure to serve as a gateway for the domain. A worker node can run application services and perform computations, but it cannot serve as a gateway. The Service Manager performs limited domain functions on a worker node.

Example Domain with Multiple Nodes

This example domain contains three nodes. Each node has both the service and compute roles enabled.

All nodes run the Service Manager. Node 1 is the master gateway node and runs two application services. Node 2 is a back-up gateway node and runs one application service. Node 3 is a worker node and runs one application service. If Node 1 becomes unavailable, Node 2 is elected as the new master gateway node. The Service Manager on Node 2 then performs all domain functions. When Node 1 restarts, it becomes a back-up gateway node and the Service Manager performs limited domain functions.

The following image shows a domain with two gateway nodes and one worker node:



Node Roles

The node role defines the purpose of the node. A node with the service role can run application services. A node with the compute role can perform computations requested by remote application services. A node with both roles can run application services and locally perform computations for those services.

By default, each gateway and worker node has both the service and compute roles enabled. Each node must have at least one role enabled.

Service Role

A node with the service role can run application services.

When you enable the service role on a node, the Service Manager supports application services configured to run on that node.

A node requires the service role in the following situations:

- The node is a gateway node.
- The node is configured as a primary or back-up node for an application service.
- The node is assigned to a CDI-PC Integration Service grid and a service process is running on the node.

Compute Role

A node with the compute role can perform computations requested by remote application services.

When a node has the compute role, the Service Manager manages the containers on the node. A container is an allocation of memory and CPU resources. An application service uses the container to remotely perform computations on the node.

When you disable the compute role on a node, you must specify whether to stop, complete, or abort computations that might be running on the node.

Viewing Processes on a Node with the Service Role

You can view the status of all application service processes configured to run on a node with the service role. Before you shut down or remove a node, you can view the status of each application service process to determine which service processes you need to disable.

When a node does not have the service role, no application service processes run on the node.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select a node with the service role.
3. In the contents panel, select the **Processes** view.

   The view displays the status of each application service process configured to run on the node.

Define and Add Nodes

To create a node, you define the node as a gateway or worker node and then add the node to the domain.

Use either of the following programs to define a node:

Informatica installer

Run the installer on each machine you want to define as a node.

infasetup command line program

Run the infasetup DefineGatewayNode or infasetup DefineWorkerNode command on each machine that you want to define as a node. You might use infasetup to define a node if you decide to move a node from one domain to another domain.

When the Informatica installer or infasetup defines a node, the program creates `nodemeta.xml`. This file is the node configuration file for the node. A gateway node uses information in `nodemeta.xml` to connect to the domain configuration database. A worker node uses the information in `nodemeta.xml` to connect to the domain. The file is stored in the following directory on each node:

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

When you define a node using the Informatica installer, the installer adds the node to the domain with both the service and compute roles enabled. When you log in to the Administrator tool, the node appears in the Navigator.

When you define a node with infasetup, you must manually add the node to the domain. You can add a node to the domain in the Administrator tool or with the infacmd isp AddDomainNode command. When you add the node, you specify the roles to enable on the node.

You can use the Administrator tool to add a node to the domain before you define the node. In this case, the Administrator tool displays a message saying that you need to run the Informatica installer to associate the node with a physical host name and port number. The name that you enter for the node must be the same name that you use when you define the node.

Adding Nodes to the Domain

You can use the Administrator tool to add a node to the domain.

Use the Administrator tool to add a node to the domain in the following situations:

- After you run the infasetup DefineGatewayNode or infasetup DefineWorkerNode command.

- When you decide to add the node before running the Informatica installer or infasetup command line program to define the node.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select the folder where you want to add the node. If you do not want the node to appear in a folder, select the domain.
3. On the Navigator Actions menu, click **New** > **Node**.

   The **Create Node** dialog box appears.
4. Enter the node name.

   The name must be the same node name that you use when you define the node.
5. If you want to change the folder for the node, click **Browse** and choose a new folder or the domain.
6. Optionally update the node role.

   By default, each node has both the service and compute roles.
7. Click **OK**.

   If you add a node to the domain before you define the node using the Informatica installer or infasetup, the Administrator tool displays a message saying that you need to run the installer to associate the node with a physical host name and port number.

Related Topics:

- "Node Roles" on page 63

Configuring Node Properties

You configure node properties on the Properties view for the node. You can configure properties such as the node roles, error severity level, and minimum and maximum port numbers.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select a node.
3. Click the **Properties** view.

   The Properties view displays the node properties in separate sections.
4. In the **Properties** view, click **Edit** for the section that contains the property you want to set.
5. Edit the following properties:

Node Property	Description
Name	Name of the node. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the node. The description cannot exceed 765 characters.
Host Name	Host name of the machine represented by the node.

Node Property	Description
Port	Port number used by the node.
Gateway Node	Indicates whether the node can serve as a gateway. If this property is disabled, then the node is a worker node.
Service Role	Indicates whether the node has the service role. If enabled, application services can run on the node. If disabled, application services cannot run on the node. Default is enabled.
Compute Role	Indicates whether the node has the compute role. If enabled, the node can perform computations. If disabled, the node cannot perform computations. Default is enabled.
Backup Directory	Directory to store repository backup files. The directory must be accessible by the node.
Error Severity Level	Level of error logging for the node. These messages are written to the Log Manager application service and Service Manager log files. Set one of the following message levels: - **ERROR**. Writes ERROR code messages to the log. - **WARNING**. Writes WARNING and ERROR code messages to the log. - **INFO**. Writes INFO, WARNING, and ERROR code messages to the log. - **TRACING**. Writes TRACE, INFO, WARNING, and ERROR code messages to the log. - **DEBUG**. Writes DEBUG, TRACE, INFO, WARNING, and ERROR code messages to the log. Default is **WARNING**.
Minimum Port Number	Minimum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
Maximum Port Number	Maximum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
CPU Profile Benchmark	Ranks the node's CPU performance against a baseline system. Used by the Load Balancer component of the CDI-PC Integration Service. For example, if the CPU is running 1.5 times as fast as the baseline machine, the value of this property is 1.5. You can calculate the benchmark by clicking **Actions** > **Recalculate CPU Profile Benchmark**. The calculation takes approximately five minutes and uses 100% of one CPU on the machine. Or, you can update the value manually. Default is 1.0. Minimum is 0.001. Maximum is 1,000,000. Used in adaptive dispatch mode. Ignored in round-robin and metric-based dispatch modes.
Maximum Processes	Maximum number of running session tasks or command tasks allowed for each CDI-PC Integration Service process running on the node. Used by the Load Balancer component of the CDI-PC Integration Service. For example, if you set the value to 5, up to 5 command tasks and 5 session tasks can run at the same time. Set this threshold to a high number, such as 200, to cause the Load Balancer to ignore it. To prevent the Load Balancer from dispatching tasks to this node, set this threshold to 0. Default is 10. Minimum is 0. Maximum is 1,000,000,000. Used in all dispatch modes.

Node Property	Description
Maximum CPU Run Queue Length	Maximum number of runnable threads waiting for CPU resources on the node. Used by the Load Balancer component of the CDI-PC Integration Service. Set this threshold to a low number to preserve computing resources for other applications. Set this threshold to a high value, such as 200, to cause the Load Balancer to ignore it. Default is 10. Minimum is 0. Maximum is 1,000,000,000. Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.
Maximum Memory %	Maximum percentage of virtual memory allocated on the node relative to the total physical memory size. Used by the Load Balancer component of the CDI-PC Integration Service. Set this threshold to a value greater than 100% to allow the allocation of virtual memory to exceed the physical memory size when dispatching tasks. Set this threshold to a high value, such as 1,000, if you want the Load Balancer to ignore it. Default is 150. Minimum is 0. Maximum is 1,000,000,000. Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.
Log Collection Directory	The directory that stores the logs for the application service when you run the log aggregator. The directory must be accessible from all the nodes in the domain. If the log collection directory is not accessible by other nodes, the aggregated logs do not appear in the aggregated logs listgrid. The users who run node processes must have read-write permissions on the directory. Configure the log collection directory for the master gateway node in the domain.
Core Dump Directory	The directory that stores the core dump files for the domain processes when you run the log aggregator. Configure the core dump directory for all the nodes in the domain.

6. Click **OK**.

Shutting Down and Restarting the Node

Some administrative tasks might require you to shut down a node. For example, you might need to perform maintenance or benchmarking on a machine. You might also need to shut down and restart a node for some configuration changes to take effect. For example, if you change the shared directory for the Log Manager or domain, you must shut down the node and restart it to update the configuration files.

You can shut down a node from the Administrator tool or from the operating system. When you shut down a node, you stop Informatica services and abort all application service processes and computations running on the node.

To restart a node, start Informatica services on the node.

Warning: To avoid loss of data or metadata when you shut down a node, disable all running application service processes in complete mode.

Shutting Down a Node from the Administrator Tool

When you shut down a node from the Administrator tool, you can view all application service processes running on the node.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.

2. In the Domain Navigator, select a node.
3. In the Navigator **Actions** menu, select **Shutdown Node**.

   If the node has the service role, the Administrator tool displays the list of application service processes running on that node.
4. Optionally, choose whether the shutdown is planned or unplanned.
5. Optionally, enter comments about the shutdown.
6. Click **OK** to stop all service processes and shut down the node, or click **Cancel** to cancel the operation.

Starting or Stopping a Node on UNIX

On UNIX, run infaservice.sh to start and stop the Informatica daemon. By default, infaservice.sh is installed in the following directory:

```
<InformaticaInstallationDir>/tomcat/bin
```

1. Go to the directory where infaservice.sh is located.
2. At the command prompt, enter the following command to start the daemon:

   ```
   infaservice.sh startup
   ```

   Enter the following command to stop the daemon:

   ```
   infaservice.sh shutdown
   ```

   Note: Always start Informatica nodes with a non-root user. If you use a softlink to specify the location of infaservice.sh, set the INFA_HOME environment variable to the location of the Informatica installation directory.

Removing the Node Association

You can remove the host name and port number associated with a node. When you remove the node association, the node remains in the domain, but it is not associated with a host machine.

To associate a different host machine with the node, you must run the installation program or infasetup DefineGatewayNode or infasetup DefineWorkerNode command on the new host machine, and then restart the node on the new host machine.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Navigator, select a node.
3. In the **Services and Nodes** view **Actions** menu, select **Remove Node Association**.

Removing a Node

When you remove a node from a domain, it is no longer visible in the Navigator. If the node is running when you remove it, the node shuts down and aborts all application service processes.

Note: To avoid loss of data or metadata when you remove a node, disable all running application service processes in complete mode.

1. In the Administrator tool, click the **Manage** tab > **Services and Nodes** view.
2. In the Domain Navigator, select a node.
3. In the Navigator **Actions** menu, select **Delete**.
4. In the warning message that appears, click **OK**.

CHAPTER 7

High Availability

This chapter includes the following topics:

High Availability Overview

High availability refers to the uninterrupted availability of computer system resources. In an Informatica domain, high availability eliminates a single point of failure and provides minimal service interruption in the event of failure. When you configure high availability for a domain, the domain can continue running despite temporary network, hardware, or service failures.

The following high availability components make services highly available in an Informatica domain:

- Resilience. An Informatica domain can tolerate temporary connection failures until either the resilience timeout expires or the failure is fixed.
- Restart and failover. A process can restart on the same node or on a backup node after the process becomes unavailable.
- Recovery. Operations can complete after a service is interrupted. After a service process restarts or fails over, it restores the service state and recovers operations.

When you plan a highly available Informatica environment, configure high availability for both the internal Informatica components and systems that are external to Informatica. Internal components include the domain, application services, application clients, and command line programs. External systems include the network, hardware, database management systems, FTP servers, message queues, and shared storage.

High availability features for the Informatica environment are available based on your license.

Example

As you open a mapping in the CDI-PC Designer workspace, the CDI-PC Repository Service becomes unavailable and the request fails. The domain contains multiple nodes for failover and the CDI-PC Designer is resilient to temporary failures.

The CDI-PC Designer tries to establish a connection to the CDI-PC Repository Service within the resilience timeout period. The CDI-PC Repository Service fails over to another node because it cannot restart on the same node.

The CDI-PC Repository Service restarts within the resilience timeout period, and the CDI-PC Designer reestablishes the connection.

After the CDI-PC Designer reestablishes the connection, the CDI-PC Repository Service recovers from the failed operation and fetches the mapping into the CDI-PC Designer workspace.

Resilience

The domain tolerates temporary connection failures between application clients, application services, and nodes.

A temporary connection failure might occur because an application service process fails or because of a network failure. When a temporary connection failure occurs, the Service Manager tries to reestablish connections between the application clients, application services, and nodes.

Application Client Resilience

The application clients try to reconnect to application services when a temporary connection failure occurs.

Based on your license, the following application clients are resilient to the services that they connect to:

CDI-PC Client

The CDI-PC Client tries to reconnect to the CDI-PC Repository Service and the CDI-PC Integration Service when a temporary network failure occurs.

If you perform a CDI-PC Client action that requires connection to the repository while the CDI-PC Client is trying to reestablish the connection, the CDI-PC Client prompts you to try the operation again after the CDI-PC Client reestablishes the connection. If the CDI-PC Client is unable to reestablish the connection during the resilience timeout period, the CDI-PC Client prompts you to reconnect to the repository manually.

Command line programs

Command line programs try to reconnect to the domain or an application service when a temporary network failure occurs while a command line program is running.

Example CDI-PC Client Resilience to Application Services

There is a network connection loss of 120 seconds between the CDI-PC Workflow Monitor and the CDI-PC Repository Service when a developer is monitoring a workflow. The CDI-PC Client, Workflow Monitor has a 60 second resilience timeout and the CDI-PC Repository Service has a resilience timeout of 180 seconds.

The Developer does not notice the loss of connection and he is unaffected by the 120 seconds connection loss. However, the following messages appear in the **Notifications** tab on the CDI-PC Repository Service Workflow Monitor:

```
Repository Service notifications are enabled.
DATE TIME-[REP_55101] Connection to the Repository Service [Repository_Service_Name] is
broken.
DATE TIME-[REP_55114] Reconnecting to the Repository Service [Repository_Service_Name].
The resilience time is 180 seconds.
DATE TIME-Reconnected to Repository Service [Repository_Service_Name] successfully.
```

Application Service Resilience

Some application services try to reconnect to application services, application clients, and external components when a temporary connection failure occurs.

Based on your license, the following application services are resilient to the temporary connection failure of their clients:

CDI-PC Integration Service

The CDI-PC Integration Service is resilient to temporary connection failures to other services, the CDI-PC Client, and external components such databases and FTP servers.

CDI-PC Repository Service

The CDI-PC Repository Service is resilient to temporary connection failures to other services, such as the CDI-PC Integration Service. It is also resilient to the temporary connection failures to the repository database.

Node Resilience

When a domain contains multiple nodes, the nodes are resilient to temporary failures in communication from other nodes in the domain.

Nodes are resilient to the following temporary connection failures:

A non-master gateway node becomes unavailable.

Every node in the domain sends a communication signal to the master gateway node at periodic intervals of 15 seconds. For nodes with the service role, the communication includes a list of application services running on the node.

All nodes have a resilience timeout of 90 seconds. If a node fails to connect to the master gateway node within the resilience timeout period, the master gateway node marks the node unavailable. If the node that fails to connect has the service role, the master gateway node also reassigns its application services to a back-up node. This ensures that services on a node continue to run despite node failures.

The master gateway node becomes unavailable.

You can configure more than one node to serve as a gateway. If the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect another master gateway node.

If you configure one node to serve as the gateway and the node becomes unavailable, all other nodes shut down.

Example Resilience Timeout Configuration

Some resilience timeout values are default and others can be configured or overwritten.

You can use the resilience timeout and limit on resilience timeout configured for the domain for CDI-PC application services if you do not set it for the application service. Command line programs use the service resilience timeout. If the service limit on resilience timeout is smaller than the resilience timeout for the connecting client, the client uses the services limit as the resilience timeout.

The following table describes the resilience timeout and the limits shown in the figure above:

	Connect From	Connect To	Description
A	CDI-PC Integration Service	CDI-PC Repository Service	The CDI-PC Integration Service can spend up to 30 seconds to connect to the CDI-PC Repository Service, based on the domain resilience timeout. It is not bound by the CDI-PC Repository Service limit on resilience timeout of 60 seconds.
B	*pmcmd*	CDI-PC Integration Service	*pmcmd* is bound by the CDI-PC Integration Service limit on resilience timeout of 180 seconds, and it cannot use the 200 second resilience timeout configured in INFA_CLIENT_RESILIENCE_TIMEOUT.
C	CDI-PC Client	CDI-PC Repository Service	The CDI-PC Client is bound by the CDI-PC Repository Service limit on resilience timeout of 60 seconds. It cannot use the default resilience timeout of 180 seconds.
D	Node A	Node B	Node A can spend up to 90 seconds to connect to Node B. The Service Managers on Node A and Node B use the default node resilience timeout of 90 seconds.

Restart and Failover

To maximize operation time in the event of a failure, the Informatica domain can restart or fail over processes to another node.

The Service Manager on the master gateway node accepts application service request and manages the domain. If a master gateway node is not available, the domain shuts down. Configure the domain to failover to another node by configuring multiple gateway nodes.

Based on your license, you can also configure backup nodes for application services. The Service Manager can restart or failover the following application services if a failure occurs:

- CDI-PC Integration Service
- CDI-PC Repository Service
- PowerExchange Listener Service
- PowerExchange Logger Service

Domain Failover

The Service Manager on the master gateway node accepts service requests and manages the domain and services in the domain. The domain can failover to another node when the domain has multiple gateway nodes. Configure multiple gateway nodes to prevent domain shutdown when the master gateway node is unavailable.

The master gateway node maintains a connection to the domain configuration repository. If the domain configuration repository becomes unavailable, the master gateway node tries to reconnect when a user performs an operation. If the master gateway node cannot connect to the domain configuration repository, the master gateway node may shut down.

If the domain has multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect another master gateway node. The domain tries to connect to

the domain configuration repository with each gateway node. If none of the gateway nodes can connect, the domain shuts down and all domain operations fail. When a master gateway fails over, the client tools retrieve information about the alternate domain gateways from the domains.infa file.

Note: Application services running on the master gateway node will not fail over when another master gateway node is elected unless the application service has a backup node configured.

Application Service Restart and Failover

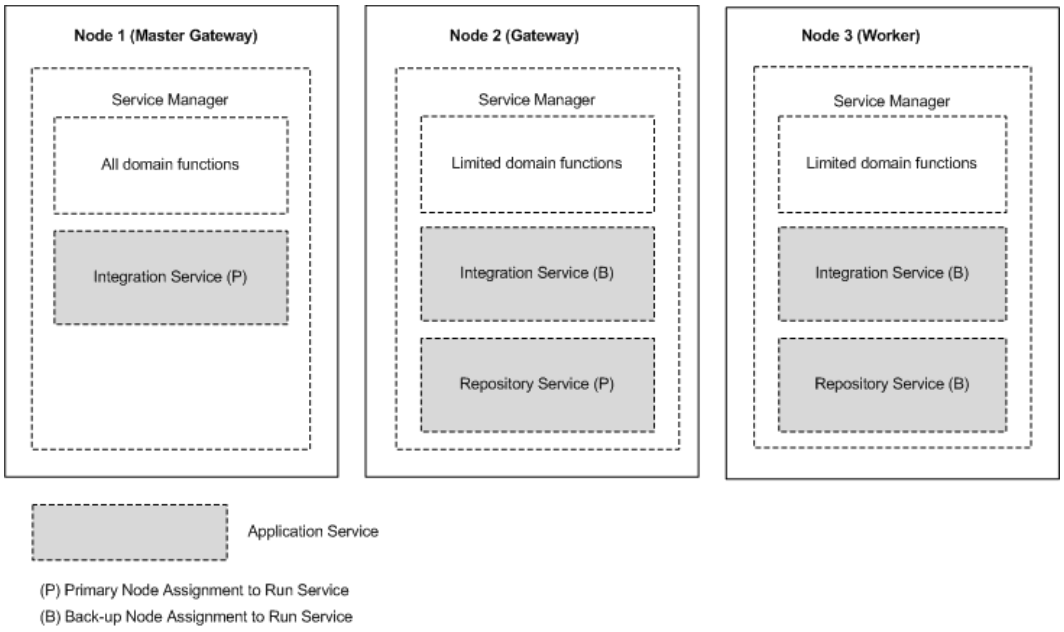
If an application service process becomes unavailable, the Service Manager can restart the application service or fail it over to a back-up node. When the Service Manager fails over an application service, it starts the service on another node that the service is configured to run on.

The following situations describe how the Service Manager restarts or fails over an application service:

- If the primary node running the service process becomes unavailable, the service fails over to a back-up node. The primary node might be unavailable if it shuts down or if the connection to the node becomes unavailable.
- If the primary node running the service process is available, the domain tries to restart the process based on the restart options configured in the domain properties. If the process does not restart, the Service Manager may mark the process as failed. The service then fails over to a back-up node and starts another process. If the Service Manager marks the process as failed, the administrator must enable the process after addressing any configuration problem.

If a service process fails over to a back-up node, it does not fail back to the primary node when the node becomes available. You can disable the service process on the back-up node to cause it to fail back to the primary node.

The following image shows how you can configure primary and back-up nodes for an application service:



Recovery

Recovery is the completion of operations after an interrupted service is restored. The state of operation for a service contains information about the service process.

Based on your license, the following components can recover after an interrupted service is restored:

Service Manager

The Service Manager for each node in the domain maintains the state of service processes running on that node. If the master gateway shuts down, the newly elected master gateway collects the state information from each node to restore the state of the domain.

CDI-PC Repository Service

The CDI-PC Repository Service maintains the state of operation in the CDI-PC repository. The state of operation includes information about repository locks, requests in progress, and connected clients. After restart or failover, the CDI-PC Repository Service can recover operations from the point of interruption.

CDI-PC Integration Service

The CDI-PC Integration Service maintains the state of operation in the shared storage configured for the service. The state of operation includes information about scheduled, running, and completed tasks for the service.

The CDI-PC Integration Service maintains CDI-PC session and workflow state of operation based on the recovery strategy you configure for the session and workflow. When the CDI-PC Integration Service restarts or fails over a service process, it can automatically recover interrupted workflows that are configured for recovery.

Configuration for a Highly Available Domain

To minimize system downtime, configure Informatica domain components to be highly available.

You can configure the following Informatica domain components to be highly available:

Domain

One node in the domain acts as a gateway to receive service requests from clients and routes them to the appropriate service and node. To prevent domain shutdown when the master gateway node is unavailable, configure more than one gateway node.

Nodes

Informatica services are processes that run on each node. You can configure Informatica services to restart automatically if it terminates unexpectedly.

Application Services

The application services run on nodes in the Informatica domain.

Based on your license, you can configure the following high availability features for application services:

- To minimize the application service downtime, configure backup nodes for application services.
- To specify the resilience period for application services, review default settings and configure resilience timeout periods for application services.
- To ensure CDI-PC Integration Service failover and recovery, configure the CDI-PC Integration Service to store process state information on a POSIX compliant shared file system or in a database.

Application Clients

Application clients provide access to Informatica functionality, and they run on user machines. Application clients send requests to the Service Manager or application services.

You can configure resilience timeout periods for command line programs. You cannot configure a CDI-PC Client resilience timeout.

External Systems

Use highly available versions of external systems such as source and target databases, message queues, and FTP servers.

Network

Make the network highly available by configuring redundant components such as routers, cables, and network adapters.

Application Service Resilience Configuration

When a temporary network failure occurs, application services try to reconnect to other application services for the duration of the resilience timeout. You can configure the resilience timeout for application services.

When an application service connects to another application service in the domain, the service that initiates the connection is a client of the other service.

You can configure application service resilience timeouts for the following application services:

CDI-PC Application Services

You can configure the resilience timeout and resilience timeout limits in the advanced properties of the CDI-PC Integration Service and CDI-PC Repository Service. The resilience timeout for application services that connects to a CDI-PC Integration Service or CDI-PC Repository Service is determined by one of the following values:

- The service **Resilience Timeout** property. You can configure the resilience timeout for the service in the service properties. To disable resilience for a service, set the resilience timeout to 0.
- The domain **Resilience Timeout** property. To use the resilience timeout configured for the domain, set the resilience timeout for the service to blank.
- The service **Limit on Resilience Timeout** property. If the service limit on resilience timeout is smaller than the resilience timeout for the connecting client, the client uses the limit as the resilience timeout. To use the limit on resilience timeout configured for the domain, set the service resilience limit to blank.
- The domain **Limit on Resilience Timeout** property. To use the resilience timeout configured for the domain, set the limit on resilience timeout for the service to blank.

You can configure the resilience timeout for the SAP BW Service in the general properties for the service. The SAP BW Service resilience timeout property is called the **Retry Period**.

Note: A client cannot be resilient to service interruptions if you disable the service in the Administrator tool. If you disable the service process, the client is resilient to the interruption in service.

Application Service Failover Configuration

Based on your license, you can configure backup nodes so that application services can failover to another node when the primary node fails. Configure backup nodes when you create or update an application service.

When you configure a backup node, verify that the node has access to run-time files that each application service requires to process data integration tasks such as workflows and mappings. For example, a workflow might require parameter files, input files, or output files.

CDI-PC Integration Service Failover and Recovery Configuration

During failover and recovery, the CDI-PC Integration Service needs to access state of operation files and process state information.

The state of operation files store the state of each workflow and session operation. The CDI-PC Integration Service always stores the state of each workflow and session operation in files in the $PMStorageDir directory of the CDI-PC Integration Service process.

Process state information includes information about which node was running the master CDI-PC Integration Service process and which node was running each session. You can configure the CDI-PC Integration Service to store process state information on a cluster file system or in the CDI-PC repository database.

Store High Availability Persistence on a Cluster File System

By default, the CDI-PC Integration Service stores process state information along with the state of operation files in the $PMStorageDir directory of the Integration Service process. You must configure the $PMStorageDir directory for each CDI-PC Integration Service process to use the same directory on a cluster file system.

Nodes that run the CDI-PC Integration Service must be on the same cluster file system so that they can share resources. Also, nodes within a cluster must be on the cluster file system's heartbeat network. Use a highly available cluster file system that is configured for I/O fencing. The hardware requirements and configuration of an I/O fencing solution are different for each file system.

The following cluster file systems are certified by Informatica for use for CDI-PC Integration Service failover and session recovery:

Storage Array Network

Veritas Cluster Files System (VxFS)

IBM General Parallel File System (GPFS)

Network Attached Storage using NFS v3 protocol

EMC UxFS hosted on an EMV Celerra NAS appliance

NetApp WAFL hosted on a NetApp NAS appliance

Contact the file system vendors directly to evaluate which file system matches your requirements.

Store High Availability Persistence in a Database

You can configure the CDI-PC Integration Service to store process state information in database tables. When you configure the CDI-PC Integration Service to store process state information in a database, the service still stores the state of each workflow and session operation in files in the $PMStorageDir directory. You can configure the $PMStorageDir directory to use a POSIX compliant shared file system. You do not need to use a cluster file system.

Configure the CDI-PC Integration Service to store process state information in database tables in the advanced properties. The CDI-PC Integration Service stores process state information in persistent database tables in the associated CDI-PC repository database.

During failover, automatic recovery of workflows resume when the service process can access the database tables.

Command Line Program Resilience Configuration

You can configure the resilience timeout that command line programs use to perform domain and service operations.

When you use the infacmd , pmcmd, or pmrep command line programs to connect to the domain or an application service the resilience timeout is determined by the command line option, an environment variable, or the default resilience timeout.

Use the following guidelines when you configure command line program resilience:

Command line option

You can set the resilience timeout for infacmd by using the -ResilienceTimeout command line option each time you run a command. You can set the resilience timeout for pmcmd by using the -timeout command line option each time you run a command. When you use pmrep connect to connect to a repository, you can use the -t command line option to set the resilience timeout for pmrep commands that use the connection.

Environment variable.

If you do not set the timeout option in the infacmd and pmcmd command line syntax, the infacmd and pmcmd command line programs use the value of the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT that is configured on the client machine. If you do not set the timeout option when you use pmrep connect to connect to the repository, pmrep commands use the value of the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT that is configured on the client machine.

Default value

If you do not use the command line option or the environment variable, the pmcmd and pmrep command line program uses the default resilience timeout of 180 seconds. If you do not use the command line option or the environment variable, the infacmd command line program uses the value of the domain **Service Level Timeout** property as the default resilience timeout.

Limit on timeout

If the limit on resilience timeout for the CDI-PC Integration Service or the CDI-PC Repository Service is smaller than the command line resilience timeout, the command line program uses the limit as the resilience timeout.

Note: CDI-PC does not provide resilience for a repository client when the CDI-PC Repository Service is running in exclusive mode.

Domain Failover Configuration

You can define multiple gateway nodes to prevent domain shutdown when the master gateway node is unavailable.

The first time that you install Informatica services, you create one gateway node. After you install Informatica, you can define additional gateway nodes. To define a gateway node, add a gateway node to the domain or configure a worker node to serve as a gateway node.

Node Restart Configuration

The Informatica services run the Service Manager on all nodes in the domain. You can configure the Informatica services to start automatically when a node terminates unexpectedly and restarts.

To restart the Informatica services when a node restarts, complete the following steps:

- In a UNIX environment, you can create a script to automatically start the Informatica services when the node starts.

You can configure restart for all nodes, regardless of node type or node role.

Oracle RAC Database Failover

You can use Oracle Real Application Cluster (RAC) to specify a connection to an Oracle service that is enabled with load balancing and high availability. Oracle RAC distributes the workload among all available nodes in the cluster. If a node fails, the workload of the unavailable node fails over to an available node. Use Oracle RAC load-balanced connections in a fail-safe environment to ensure a database connection is available even when one or more RAC nodes fail.

The following operations in the CDI-PC Repository Service are resilient to the database failover in Oracle RAC setup:

- ExecuteQuery
- ObjectExport
- ObjectImport
- PurgeVersion
- RollbackDeployment

You cannot perform any administrator operations with Oracle RAC database failover for Informatica domain.

Troubleshooting High Availability

The solutions to the following situations might help you with high availability.

I am not sure where to look for status information regarding client connections to the CDI-PC repository.

In CDI-PC Client applications such as the CDI-PC Designer and the CDI-PC Workflow Manager, an error message appears if the connection cannot be established during the timeout period. Detailed information about the connection failure appears in the Output window. If you are using *pmrep*, the connection error information appears at the command line. If the CDI-PC Integration Service cannot establish a connection to the repository, the error appears in the CDI-PC Integration Service log, the workflow log, and the session log.

I entered the wrong connection string for an Oracle database. Now I cannot enable the CDI-PC Repository Service even though I edited the CDI-PC Repository Service properties to use the right connection string.

You need to wait for the database resilience timeout to expire before you can enable the CDI-PC Repository Service with the updated connection string.

I have the high availability option, but my FTP server is not resilient when the network connection fails.

The FTP server is an external system. To achieve high availability for FTP transmissions, you must use a highly available FTP server. For example, Microsoft IIS 6.0 does not natively support the restart of file uploads or file downloads. File restarts must be managed by the client connecting to the IIS server. If the transfer of a file to or from the IIS 6.0 server is interrupted and then reestablished within the client resilience timeout period, the transfer does not necessarily continue as expected. If the write process is more than half complete, the target file may be rejected.

I have the high availability option, but the Informatica domain is not resilient when machines are connected through a network switch.

If you are using a network switch to connect machines in the domain, use the auto-select option for the switch.

CHAPTER 8

Connections

This chapter includes the following topics:

Connections Overview

A connection is a repository object that defines a connection in the domain configuration repository.

You can create and manage connections in the Administrator tool.

The tasks that you can perform in each tool depend on the tool that you use.

Note: These connections are independent of the connections that you create in the CDI-PC Workflow Manager.

Pass-through Security

Pass-through security is the capability to connect to an SQL data service or an external source with the client user credentials instead of the credentials from a connection object.

Users might have access to different sets of data based on the job in the organization. Client systems restrict access to databases by the user name and the password. When you create an SQL data service, you might combine data from different systems to create one view of the data. However, when you define the connection to the SQL data service, the connection has one user name and password.

A web service operation mapping might need to use a connection object to access data. If you configure pass-through security and the web service uses WS-Security, the web service operation mapping connects to a source using the user name and password provided in the web service SOAP request.

Configure pass-through security for a connection in the connection properties of the Administrator tool or with infacmd dis UpdateServiceOptions. You can set pass-through security for connections to deployed applications. Only SQL data services and web services recognize the pass-through security configuration.

CHAPTER 9

Connection Properties

This chapter includes the following topics:

Connection Properties Overview

Connection properties enable the Informatica client to connect to data sources.

This chapter contains connection properties for each of the connections you can create and manage through Informatica clients.

Greenplum Connection Properties

Use a Greenplum connection to connect to a Greenplum database. The Greenplum connection is a relational type connection. You can create and manage a Greenplum connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

When you create a Greenplum connection, you enter information for metadata and data access.

The following table describes Greenplum connection properties:

Property	Description
Name	Name of the Greenplum relational connection.
Description	Description of the connection. The description cannot exceed 765 characters.
Location	Domain on which you want to create the connection.
Type	Type of connection.

The user name, password, driver name, and connection string are required to import the metadata. The following table describes the properties for metadata access:

Property	Description
User Name	User name with permissions to access the Greenplum database.
Password	Password to connect to the Greenplum database.
Driver Name	The name of the Greenplum JDBC driver. For example: `com.pivotal.jdbc.GreenplumDriver` For more information about the driver, see the Greenplum documentation.
Connection String	Use the following connection URL: `jdbc:pivotal:greenplum://<hostname>:<port>;DatabaseName=<database_name>` For more information about the connection URL, see the Greenplum documentation.

PowerExchange for Greenplum uses the host name, port number, and database name to create a control file to provide load specifications to the Greenplum gpload bulk loading utility. It uses the Enable SSL option and the certificate path to establish secure communication to the Greenplum server over SSL.

The following table describes the connection properties for data access:

Property	Description
Host Name	Host name or IP address of the Greenplum server.
Port Number	Greenplum server port number. If you enter 0, the gpload utility reads from the environment variable $PGPORT. Default is 5432.
Database Name	Name of the database.
Enable SSL	Select this option to establish secure communication between the gpload utility and the Greenplum server over SSL.
Certificate Path	Path where the SSL certificates for the Greenplum server are stored. For information about the files that need to be present in the certificates path, see the gpload documentation.

IBM DB2 Connection Properties

Use an IBM DB2 connection to access IBM DB2. An IBM DB2 connection is a relational database connection. You can create and manage an IBM DB2 connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	The description of the connection. The description cannot exceed 765 characters.
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Connection String for data access	The DB2 connection URL used to access metadata from the database. `dbname` Where `dbname` is the alias configured in the DB2 client.

Property	Description

Metadata Access Properties: Connection String	Use the following metadata connection string URL:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>`
	When you import a table, by default, all tables are displayed under the default schema name. To view tables under a specific schema instead of the default schema, you can specify the schema name from which you want to import the table. Include the ischemaname parameter in the URL to specify the schema name. For example, use the following syntax to import a table from a specific schema:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>;ischemaname=<schema_name>`
	To search for a table in multiple schemas and import it, you can specify multiple schema names in the ischemaname parameter. The schema name is case sensitive. You cannot use special characters when you specify multiple schema names. Use the pipe (|) character to separate multiple schema names. For example, use the following syntax to search for a table in three schemas and import it:
	`jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>;ischemaname=<schema_name1>|<schema_name2>|<schema_name3>`
	When you specify multiple schema names, you must clear the **Show Default Schema Only** option to view the tables under the specified schema names.

AdvancedJDBCSecurityOptions	Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - cryptoProtocolVersion. Optional. If you enable TLS for the IBM DB2 instance, set the cryptoProtocolVersion parameter as follows: cryptoProtocolVersion=TLSv<version number>. For example, cryptoProtocolVersion=TLSv1.2 **Note:** The version number must be the same as the TLS version you configured for the server. - TrustStore. Required. Path and file name of the truststore file. **Note:** If you configure SSL or TLS and specify only the file name, you must copy the truststore file to the following directory to test the connection: `<Informatica server installation directory>/tomcat/bin` - TrustStorePassword. Required. Password for the truststore file for the secure database. **Note:** Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.

Property	Description
Data Access Properties: Connection String	The connection string used to access data from the database. For IBM DB2 this is `<database name>`
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database.
Retry Period	This property is reserved for future use.
Tablespace	The tablespace name of the database.
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type.
ODBC Provider	ODBC. The type of database to which ODBC connects. The options are: - Other - Sybase - Microsoft_SQL_Server Default is Other.

IBM DB2 for i5/OS Connection Properties

Use an IBM DB2 for i5/OS connection to access tables in IBM DB2 for i5/OS. An IBM DB2 for i5/OS connection is a relational database connection. You can create and manage an IBM DB2 for i5/OS connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 for i5/OS connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	The description of the connection. The description cannot exceed 255 characters.
Connection Type	The connection type (DB2I).
Username	A database user name.

Property	Description
Password	A password for the specified user name or a valid PowerExchange passphrase. A PowerExchange passphrase can be from 9 to 31 characters in length and can contain the following characters: - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: `' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ?` **Note:** The first character is an apostrophe. Passphrases cannot include single quotation marks (‘), double quotation marks (“), or currency symbols. To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the *PowerExchange Reference Manual*.
Pass-through security enabled	Enables pass-through security for the connection.
Database name	The database instance name.
Location	Node name for the location of the PowerExchange Listener that connects to DB2. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Database file overrides	Specifies the i5/OS database file override in the following format: `from_file/to_library/to_file/to_member` Where: - *from_file* is the file to be overridden. - *to_library* is the new library to use. - *to_file* is the file in the new library to use. - *to_member* is optional and is the member in the new library and file to use. *FIRST is used if nothing is specified. You can specify up to eight unique file overrides on a single connection. A single override applies to a single source or target. When you specify more than one file override, enclose the string of file overrides in double quotes (") and include a space between each file override. **Note:** If you specify both **Library List** and **Database File Overrides** and a table exists in both, the **Database File Overrides** value takes precedence.
Library list	List of libraries that PowerExchange searches to qualify the table name for Select, Insert, Delete, or Update statements. PowerExchange searches the list if the table name is unqualified. Separate libraries with commas. **Note:** If you specify both **Library List** and **Database File Overrides** and a table exists in both, the **Database File Overrides** value takes precedence.
Code Page	The code page used to read from a source database or write to a target database or file.

Property	Description
SQL Identifier character to use	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type.
Isolation level	Commit scope of the transaction. Select one of the following options: - **None** - **CS**. Cursor stability. - **RR**. Repeatable Read. - **CHG**. Change. - **ALL** Default is CS.
Pacing size	Optional. Amount of data that the source system can pass to the PowerExchange Listener. Use lower values for faster performance. The minimum value and default value is 0. A value of 0 provides the best performance.
Interpret as rows	Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Array size	Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the **Worker Threads** option to a value greater than 0. Valid values are 25 to 5000. Default is 25.
Write mode	Optional. Select one of the following write modes: - **CONFIRMWRITEON**. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - **CONFIRMWRITEOFF**. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - **ASYNCHRONOUSWITHFAULTTOLERANCE**. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. Default is CONFIRMWRITEON.
Reject file	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is ASYNCHRONOUSWITHFAULTTOLERANCE. Enter PWXDISABLE to prevent the creation of the reject files.

IBM DB2 for z/OS Connection Properties

Use an IBM DB2 for z/OS connection to access tables in IBM DB2 for z/OS. An IBM DB2 for z/OS connection is a relational database connection. You can create and manage an IBM DB2 for z/OS connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 for z/OS connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
Description	Description of the connection. The description cannot exceed 255 characters.
Connection Type	Connection type (DB2Z).
Username	Database user name.
Password	Password for the specified user name or a valid PowerExchange passphrase. A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters: - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * ( ) _ + { } : @ | < > ? **Note:** The first character is an apostrophe. Passphrases cannot include single quotation marks (‘), double quotation marks (“), or currency symbols. To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the *PowerExchange Reference Manual*. The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases. **Note:** A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.
Pass-through security enabled	Enables pass-through security for the connection.
DB2 Subsystem ID	Name of the DB2 subsystem.
Location	Node name for the location of the PowerExchange Listener that connects to DB2. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Correlation ID	Value to be concatenated to prefix PWX to form the DB2 correlation ID for DB2 requests.

Property	Description
Code Page	Code page used to read from a source database or write to a target database or file.
SQL identifier character to use	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type.
Pacing size	Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, or the database node is a bottleneck. User lower values for faster performance. The minimum value and default value is 0. A value of 0 provides the best performance.
Interpret as rows	Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Array size	Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the **Worker Threads** option to a value greater than 0. Valid values are 1 to 5000. Default is 25.
Reject file	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is ASYNCHRONOUSWITHFAULTTOLERANCE. Enter PWXDISABLE to prevent the creation of reject files.

JD Edwards EnterpriseOne Connection Properties

Use a JD Edwards EnterpriseOne connection to connect to a JD Edwards EnterpriseOne object.

The following table describes the JD Edwards EnterpriseOne connection properties:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	The connection type. Select JD Edwards EnterpriseOne.
Host Name	JD Edwards EnterpriseOne server host name.
Enterprise Port	JD Edwards EnterpriseOne server port number. Default is 6016.

Property	Description
User Name	The JD Edwards EnterpriseOne database user name.
Password	The password for the JD Edwards EnterpriseOne database user.
Environment	Name of the JD Edwards EnterpriseOne environment you want to connect to.
Role	Role of the JD Edwards EnterpriseOne user. Default is *ALL.
User Name	The JD Edwards EnterpriseOne database user name.
Password	Password for the database user.
Driver Class Name	The following list provides the driver class name that you can enter for the applicable database type: - DataDirect JDBC driver class name for Oracle: `com.informatica.jdbc.oracle.OracleDriver` - DataDirect JDBC driver class name for IBM DB2: `com.informatica.jdbc.db2.DB2Driver` - DataDirect JDBC driver class name for Microsoft SQL Server: `com.informatica.jdbc.sqlserver.SQLServerDriver` For more information about which driver class to use with specific databases, see the vendor documentation.
Connection String	The connection string to connect to the database. Use the following connection string: The JDBC connection string uses the following syntax: - For Oracle: `jdbc:informatica:oracle://<host name>:<port>,ServiceName=<db service name>` - For DB2: `jdbc:informatica:db2://<host name>:<port>;databaseName=<db name>` - For Microsoft SQL: `jdbc:informatica:sqlserver://<host name>:<port>;databaseName=<db name>`

MS SQL Server Connection Properties

Use a Microsoft SQL Server connection to access Microsoft SQL Server. A Microsoft SQL Server connection is a connection to a Microsoft SQL Server relational database. You can create and manage a Microsoft SQL Server connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes MS SQL Server connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
Description	The description of the connection. The description cannot exceed 765 characters.
Use trusted connection	Enables the application service to use Windows authentication to access the database. The user name that starts the application service must be a valid Windows user with access to the database. By default, this option is cleared. **Note:** Windows and NTLM authentication is not certified for a Microsoft SQL Server 2017 version hosted on Linux.
User Name	The database user name. Required if Microsoft SQL Server uses NTLMv1 or NTLMv2 authentication.
Password	The password for the database user name. Required if Microsoft SQL Server uses NTLMv1 or NTLMv2 authentication.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.

Metadata Access Properties: Connection String	Connection string used to access metadata from the database.
	Use the following connection string:
	`jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name>`
	To test the connection with NTLM authentication, include the following parameters in the connection string:
	- AuthenticationMethod. The NTLM authentication version to use.
	Note: UNIX supports NTLMv1 and NTLMv2 but not NTLM.
	- Domain. The domain that the SQL server belongs to.
	The following example shows the connection string for a SQL server that uses NTLMv2 authentication in a NT domain named Informatica.com:
	`jdbc:informatica:sqlserver://host01:1433;DatabaseName=SQL1;AuthenticationMethod=ntlm2java;Domain=Informatica.com`
	If you connect with NTLM authentication, you can enable the **Use trusted connection** option in the MS SQL Server connection properties. If you connect with NTLMv1 or NTLMv2 authentication, you must provide the user name and password in the connection properties.

Property	Description
AdvancedJDBCSecurityOptions	Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - cryptoProtocolVersion. Optional. If you enable TLS for the Microsoft SQL Server instance, set the cryptoProtocolVersion parameter as follows: cryptoProtocolVersion=TLSv<version number>. For example, cryptoProtocolVersion=TLSv1.2 **Note:** The version number must be the same as the TLS version you configured for the server. - TrustStore. Required. Path and file name of the truststore file. **Note:** If you configure SSL or TLS and specify only the file name, you must copy the truststore file to the following directory to test the connection: `<Informatica server installation directory>/tomcat/bin` - TrustStorePassword. Required. Password for the truststore file for the secure database. Not applicable for ODBC. **Note:** Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.
Data Access Properties: Provider Type	The connection provider that you want to use to connect to the Microsoft SQL Server database. You can select the following provider types: - ODBC - Oldeb(Deprecated) Default is ODBC. **Note:** Although the Microsoft SQL Server connection user interface shows the OLEDB provider type as deprecated, Informatica supports the OLEDB provider type. For more information about the OLEDB provider type support statement, see the following Knowledge Base article KB 522895.
Use DSN	If you do not select the Use DSN option, you must provide the database and server names.

Property	Description

Connection String	Use the following connection string if you do not enable DSN mode:
	`<server name>@<database name>`
	If you enable DSN mode, use the following connection strings:
	`<DSN Name>`

Code Page	The code page used to read from a source database or to write to a target database or file.
Domain Name	The name of the domain.
Packet Size	The packet size used to transmit data. Used to optimize the native drivers for Microsoft SQL Server.
Owner Name	The name of the owner of the schema. **Note:** When you generate a table DDL through a dynamic mapping or through the **Generate and Execute DDL** option, the DDL metadata does not include schema name and owner name properties.
Schema Name	The name of the schema in the database. You must specify the schema name for the Profiling Warehouse if the schema name is different from the database user name. You must specify the schema name for the data object cache database if the schema name is different from the database user name and if you configure user-managed cache tables. **Note:** When you generate a table DDL through a dynamic mapping or through the **Generate and Execute DDL** option, the DDL metadata does not include schema name and owner name properties.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database.
Retry Period	This property is reserved for future use.
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select (None) if the database uses regular identifiers. Select a character if the database uses delimited identifiers.
Support Mixed-case Identifiers	Enable if the database uses case-sensitive identifiers. When the **SQL Identifier Character** property is set to none, the **Support Mixed-case Identifiers** property is disabled.
ODBC Provider	ODBC. The type of database to which ODBC connects. The options are: - Other - Sybase - Microsoft_SQL_Server Default is Other.

Netezza Connection Properties

Use a Netezza connection to access a Netezza database. The Netezza connection is a database connection. You can create and manage a Netezza connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes the Netezza connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	Description of the connection. The description cannot exceed 765 characters.
Location	Domain where you want to create the connection.
Type	Connection type. Select **Netezza**.
User name	User name with the appropriate permissions to access the Netezza database.
Password	Password for the database user name.
JDBC Url	Use the following format: `jdbc:netezza://<hostname>:<port>/<database name>`
Connection String	Name of the ODBC data source that you want to use to connect to the Netezza database.

ODBC Connection Properties

Use an ODBC connection to access ODBC data. An ODBC connection is a relational database connection. You can create and manage an ODBC connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes ODBC connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	The description of the connection. The description cannot exceed 765 characters.

Property	Description
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Data Access Properties: Connection String	The ODBC connection URL used to access metadata from the database. `<data source name>`
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database.
Retry Period	This property is reserved for future use.
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select (None) if the database uses regular identifiers. Select a character if the database uses delimited identifiers.
Support Mixed-case Identifiers	Enable if the database uses case-sensitive identifiers. When the **SQL Identifier Character** property is set to none, the **Support Mixed-case Identifiers** property is disabled.
ODBC Provider	The type of database to which ODBC connects. The options are: - Other - Sybase - Microsoft_SQL_Server - Snowflake Default is Other.

Oracle Connection Properties

Use an Oracle connection to connect to an Oracle database. The Oracle connection is a relational connection type. You can create and manage an Oracle connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Oracle connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
Description	The description of the connection. The description cannot exceed 765 characters.
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.

Metadata Access Properties: Connection String	Connection string used to access metadata from the database.
	Use the following connection string:
	`jdbc:informatica:oracle://<host_name>:<port>;SID=<database name>`
	Use the following connection string to connect to Oracle database through Oracle Connection Manager:
	`jdbc:informatica:oracle:TNSNamesFile=<fully qualified path to the tnsnames.ora file>;TNSServerName=<TNS server name>;`

Property	Description
AdvancedJDBCSecurityOptions	Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted. To connect to a secure database, include the following parameters: - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - cryptoProtocolVersion. Optional. If you enable TLS for the Oracle instance, set the cryptoProtocolVersion parameter as follows: cryptoProtocolVersion=TLSv<version number>. For example, cryptoProtocolVersion=TLSv1.2 **Note:** The version number must be the same as the TLS version you configured for the server. - TrustStore. Required. Path and file name of the truststore file. **Note:** If you configure SSL or TLS and specify only the file name, you must copy the truststore file to the following directory to test the connection: `<Informatica server installation directory>/tomcat/bin` - TrustStorePassword. Required. Password for the truststore file for the secure database. - KeyStore. Required. Path and file name of the keystore file. - KeyStorePassword. Required. Password for the keystore file for the secure database. **Note:** Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.
Data Access Properties: Connection String	Use the following connection string: `<database name>.world`
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database.
Retry Period	This property is reserved for future use.
Enable Parallel Mode	Enables parallel processing when loading data into a table in bulk mode. By default, this option is cleared.

Property	Description
SQL Identifier Character	Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type. Select (None) if the database uses regular identifiers. Select a character if the database uses delimited identifiers.
Support Mixed-case Identifiers	Enable if the database uses case-sensitive identifiers. When the **SQL Identifier Character** property is set to none, the **Support Mixed-case Identifiers** property is disabled.

Salesforce Connection Properties

Use a Salesforce connection to connect to a Salesforce object. The Salesforce connection is an application connection type. You can create and manage a Salesforce connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Salesforce connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	The connection type. You can select the Standard connection type or OAuth connection type.
User Name	Applicable for Standard connection type. Salesforce user name.
User Password	Applicable for Standard connection type. Password for the Salesforce user name. To access Salesforce outside the trusted network of your organization, you must append a security token to your password to log in to the API or a desktop client. To receive or reset your security token, log in to Salesforce and click **Setup** > **My Personal Information** > **Reset My Security Token**. Password is case sensitive.

Property	Description
Service URL	URL of the Salesforce service you want to access. For example, `https://login.salesforce.com/services/Soap/u/57.0` In a test or development environment, you might want to access the Salesforce Sandbox testing environment. For more information about the Salesforce Sandbox, see the Salesforce documentation.
Refresh Token	Applicable for OAuth connection type. Refresh Token of Salesforce.
Consumer Key	Applicable for OAuth connection type. The Consumer Key obtained from Salesforce, required to generate the Refresh Token. For more information about how to generate the Consumer Key, see the Salesforce documentation.
Consumer Secret	Applicable for OAuth connection type. The Consumer Secret obtained from Salesforce, required to generate the Refresh Token. For more information about how to generate the Consumer Secret, see the Salesforce documentation.

SAP Connection Properties

Use an SAP connection to access an SAP table or an SAP BW object. The SAP connection is an enterprise application connection. You can create and manage an SAP connection in the Administrator tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes the SAP connection properties:

Property	Description
Username	Required. User name for the SAP source system that you want to access.
Password	Required. Password for the user name.
Connection type	Required. Type of connection that you want to create. Select one of the following values: - Application. Create an application connection when you want to connect to a specific SAP application server. - Load balancing. Create a load balancing connection when you want to use SAP load balancing. Default is Application. Based on the connection type you select, the corresponding connection property fields become available in the **Connection Details** dialog box. The Developer tool greys out the connection property fields that are not applicable for a particular connection type.
Host name	Required when you create an SAP application connection. Host name or IP address of the SAP server that you want to connect to.
System number	Required when you create an SAP application connection. SAP system number.

Property	Description
Message host name	Required when you create an SAP load balancing connection. Host name of the SAP message server.
R3 name/SysID	Required when you create an SAP load balancing connection. Name of the SAP system.
Group	Required when you create an SAP load balancing connection. Group name of the SAP application server.
Client	Required. SAP client number.
Language	Optional. Language that you want to use for mappings and workflows. Must be compatible with the Developer tool code page. If you leave this option blank, the Developer tool uses the default language of the SAP system.
Trace	Optional. Use this option to track the JCo calls that the SAP system makes. SAP stores the information about the JCo calls in a trace file. Specify one of the following values: - 0. Off - 1. Full Default is 0. You can access the trace files from the following directories: - `<Informatica installation directory>/tomcat/bin` directory on the machine where you installed the Informatica services - `<Informatica installation directory>/clients/DeveloperClient` directory on the machine where you installed the Developer tool
Additional parameters	Optional. Enter any other connection parameter that you want to use. Use the following format: `<parameter name>=<value>`
Staging directory	Path in the SAP system where the stage file will be created.
Source directory	Path that contains the source file.
Use FTP	Enables FTP access to SAP.
FTP user	Required when you use FTP. User name to connect to the FTP server.
FTP password	Required when you use FTP. Password for the FTP user.

Property	Description
FTP host	Required when you use FTP. Host name or IP address of the FTP server. Optionally, you can specify a port number from 1 through 65535, inclusive. Default for FTP is 21. Use one of the following syntax to specify the host name: - `hostname:port_number` - `IP address:port_number` When you specify a port number, enable that port number for FTP on the host machine. If you enable SFTP, specify a host name or port number for an SFTP server. Default for SFTP is 22.
Use SFTP	Enables SFTP access to SAP.
Public key file name	Required when you enable SFTP and the SFTP server uses public key authentication. Public key file path and file name.
Private key file name	Required when you enable SFTP and the SFTP server uses public key authentication. Private key file path and file name.
Private key file name password	Required when you enable SFTP, and the SFTP server uses public key authentication and the private key is encrypted. Password to decrypt the private key file.
Use HTTPS	Select this option to enable HTTPS streaming when you read data from SAP tables. By default, the **Use HTTPS** check box is not selected. For more information about configuring HTTPS for table reader mappings in streaming mode, see the article "HTTPS Configuration for Table Reader Mappings in Streaming Mode for PowerExchange for SAP NetWeaver" on the Informatica Documentation Portal.
Key store file path	Required when you use HTTPS. Path to the keystore file that contains the private or public key pairs and the associated certificates.
Key store password	Required when you use HTTPS. Password for the keystore file.
Private key password	Required when you use HTTPS. Password to decrypt the private key file.

Teradata Parallel Transporter Connection Properties

Use a Teradata PT connection to access Teradata tables. The Teradata PT connection is a database type connection. You can create and manage a Teradata PT connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Teradata PT connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 765 characters.
Location	Domain where you want to create the connection.
Type	Connection type. Select Teradata PT.
User Name	Teradata database user name with the appropriate read and write permissions to access the database.
Password	Password for the Teradata database user name.
Driver Name	Name of the Teradata JDBC driver.
Connection String	Connection string used to access metadata from the database. Use the following connection string: jdbc:teradata://<hostname>/database=<database name>,tmode=ANSI,charset=UTF8

The following table describes the properties for data access:

Property	Description
TDPID	Name or IP address of the Teradata database machine.
Database Name	Teradata database name. If you do not enter a database name, Teradata PT API uses the default login database name.
Data Code Page	Code page associated with the database. When you run a mapping that writes data to a Teradata target, the code page of the Teradata PT connection must be the same as the code page of the Teradata target. Default is UTF-8.
Tenacity	Number of hours that Teradata PT API continues trying to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 4.
Max Sessions	Maximum number of sessions that Teradata PT API establishes with the Teradata database. Must be a positive, non-zero integer. Default is 4.
Min Sessions	Minimum number of Teradata PT API sessions required for the Teradata PT API job to continue. Must be a positive integer between 1 and the **Max Sessions** value. Default is 1.

Property	Description
Sleep	Number of minutes that Teradata PT API pauses before it retries to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 6.
Use Metadata JDBC URL for TDCH	Indicates that the Teradata Connector for Hadoop (TDCH) must use the JDBC URL that you specified in the connection string under the metadata access properties. Default is selected. Clear this option to enter a different JDBC URL that TDCH must use when it runs the mapping.
TDCH JDBC Url	Enter the JDBC URL that TDCH must use when it runs a Teradata mapping. Use the following format: `jdbc:teradata://<hostname>/database=<database name>,tmode=ANSI,charset=UTF8` This field is available only when you clear the **Use Metadata JDBC URL for TDCH** option.
Data Encryption	Enables full security encryption of SQL requests, responses, and data on Windows. Default is disabled.
Additional Sqoop Arguments	This property is applicable if you use a Hortonworks or Cloudera cluster, and run a Teradata mapping on the Blaze or Spark engine through Sqoop. Enter the arguments that Sqoop must use to process the data. For example, enter `--method split.by.amp`. Separate multiple arguments with a space. See the Hortonworks for Teradata Connector and Cloudera Connector Powered by Teradata documentation for a list of arguments that you can specify. **Note:** If you use Hortonworks for Teradata Connector, the --split-by argument is required if you add two or more source tables in the read operation. If you use Cloudera Connector Powered by Teradata, the --split-by argument is required in the source connection if the source table does not have a primary key defined.
Authentication Type	Method to authenticate the user. Select one of the following authentication types: - Native. Authenticates your user name and password against the Teradata database specified in the connection. - LDAP. Authenticates user credentials against the external LDAP directory service. Default is Native.

Tableau Connection Properties

Use a Tableau connection to connect to Tableau. When you create a Tableau connection, you enter information to access Tableau.

The following table describes the Tableau connection properties:

Property	Description
Name	Name of the Tableau connection.
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	Type of connection. Select Tableau.

The following table describes the properties to connect to Tableau:

Connection Property	Description
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the TDE or TWBX file: - Tableau Desktop. Creates a TDE file in the Data Integration Service machine. You can then manually import the TDE file to Tableau Desktop. - Tableau Server. Publishes the generated TDE or TWBX file to Tableau Server. - Tableau Online. Publishes the generated TDE or TWBX file to Tableau Online.
Connection URL	URL of Tableau Server or Tableau Online to which you want to publish the TDE or TWBX file. The URL has the following format: `http://<Host name of Tableau Server or Tableau Online>:<port>`
User Name	User name of the Tableau Server or Tableau Online account.
Password	Password for the Tableau Server or Tableau Online account.
Content URL	The name of the site on Tableau Server or Tableau Online where you want to publish the TDE or TWBX file. Contact the Tableau administrator to provide the site name.

Tableau V3 Connection Properties

When you set up a Tableau V3 connection, you must configure the connection properties.

The following table describes the Tableau V3 connection properties:

Property	Description
Name	Name of the Tableau V3 connection.
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	Type of connection. Select Tableau V3.

The following table describes the properties to connect to Tableau:

Connection Property	Description
Tableau Product	The name of the Tableau product to which you want to connect. You can choose one of the following Tableau products to publish the `.hyper` or TWBX file: **Tableau Desktop** Creates a `.hyper` file in the Data Integration Service machine. You can then manually import the `.hyper` file to Tableau Desktop. **Tableau Server** Publishes the generated `.hyper` or TWBX file to Tableau Server. **Tableau Online** Publishes the generated `.hyper` or TWBX file to Tableau Online.
Connection URL	The URL of Tableau Server or Tableau Online to which you want to publish the `.hyper` or TWBX file. Enter the URL in the following format: `http://<Host name of Tableau Server or Tableau Online>:<port>`
User Name	The user name of the Tableau Server or Tableau Online account.
Password	The password for the Tableau Server or Tableau Online account.

Connection Property	Description
Site ID	The ID of the site on Tableau Server or Tableau Online where you want to publish the or TWBX file. **Note:** Contact the Tableau administrator to provide the site ID.
Schema File Path	The path to a sample `.hyper` file from where the Data Integration Service imports the Tableau metadata. Enter one of the following options for the schema file path: - Absolute path to the `.hyper` file. - Directory path for the `.hyper` files. - Empty directory path. The path you specify for the schema file becomes the default path for the target `.hyper` file. If you do not specify a file path, the Data Integration Service uses the following default file path for the target `.hyper` file: `<Data Integration Service installation directory>/apps/Data_Integration_Server/<latest version>/bin/rtdm`

Identifier Properties in Database Connections

When you create most relational database connections, you must configure database identifier properties.

A database identifier is a database object name. Tables, views, columns, indexes, triggers, procedures, constraints, and rules can have identifiers. You use the identifier to reference the object in SQL queries. A database can have regular identifiers or delimited identifiers that must be enclosed within delimited characters.

Regular Identifiers

Regular identifiers comply with the format rules for identifiers. Regular identifiers do not require delimited characters when they are used in SQL queries.

For example, the following SQL statement uses the regular identifiers *MYTABLE* and *MYCOLUMN*:

```
SELECT * FROM MYTABLE
WHERE MYCOLUMN = 10
```

Delimited Identifiers

Delimited identifiers must be enclosed within delimited characters because they do not comply with the format rules for identifiers.

Databases can use the following types of delimited identifiers:

Identifiers that use reserved keywords

If an identifier uses a reserved keyword, you must enclose the identifier within delimited characters in an SQL query. For example, the following SQL statement accesses a table named *ORDER*:

```
SELECT * FROM "ORDER"
WHERE MYCOLUMN = 10
```

Identifiers that use special characters

If an identifier uses special characters, you must enclose the identifier within delimited characters in an SQL query. For example, the following SQL statement accesses a table named *MYTABLE$@*:

```
SELECT * FROM "MYTABLE$@"
WHERE MYCOLUMN = 10
```

Case-sensitive identifiers

By default, identifiers in IBM DB2, Microsoft SQL Server, and Oracle databases are not case sensitive. Database object names are stored in uppercase, but SQL queries can use any case to refer to them. For example, the following SQL statements access the table named *MYTABLE*:

```
SELECT * FROM mytable
SELECT * FROM MyTable
SELECT * FROM MYTABLE
```

To use case-sensitive identifiers, you must enclose the identifier within delimited characters in an SQL query. For example, the following SQL statement accesses a table named *MyTable*:

```
SELECT * FROM "MyTable"
WHERE MYCOLUMN = 10
```

Identifier Properties

When you create most database connections, you must configure database identifier properties. The identifier properties that you configure depend on whether the database uses regular identifiers, uses keywords or special characters in identifiers, or uses case-sensitive identifiers.

Configure the following identifier properties in a database connection:

SQL Identifier Character

Type of character that the database uses to enclose delimited identifiers in SQL queries. The available characters depend on the database type.

Select (None) if the database uses regular identifiers.

Select a character if the database uses delimited identifiers.

Support Mixed-case Identifiers

Enable if the database uses case-sensitive identifiers.

In the Informatica client tools, you must refer to the identifiers with the correct case. For example, when you create the database connection, you must enter the database user name with the correct case.

When the **SQL Identifier Character** property is set to none, the **Support Mixed-case Identifiers** property is disabled.

Example: Database Uses Regular Identifiers

In this example, the database uses regular identifiers. No identifiers contain a reserved keyword or a special character. The database uses identifiers that are not case sensitive.

In the database connection, set the **SQL Identifier Character** property to (None). When **SQL Identifier Character** is set to none, the **Support Mixed-case Identifiers** property is disabled.

Example: Database Uses Keywords or Special Characters in Identifiers

In this example, the database uses keywords or special characters in some identifiers. The database uses identifiers that are not case sensitive.

In the database connection, configure the identifier properties as follows:

1. Set the **SQL Identifier Character** property to the character that the database uses for delimited identifiers.

   This example sets the property to *"" (quotes)*.
2. Clear the **Support Mixed-case Identifiers** property.

Example: Database Uses Case-Sensitive Identifiers

In this example, the database uses case-sensitive identifiers. The database might use keywords or special characters in some identifiers, or it might not.

In the database connection, configure the identifier properties as follows:

1. Set the **SQL Identifier Character** property to the character that the database uses for delimited identifiers.

   This example sets the property to *"" (quotes)*.
2. Select the **Support Mixed-case Identifiers** property.

PowerExchange for PostgreSQL Connection Properties

When you configure a PowerExchange for PostgreSQL connection, you define the connection attributes that the CDI-PC Integration Service uses to connect to the PostgreSQL database.

The following table describes the PostgreSQL connection properties:

Connection Property	Description
Host Name	Host name of the PostgreSQL server to which you want to connect.
Port	Port number for the PostgreSQL server to which you want to connect. Default is 5432.
Database	The PostgresSQL database name.
User Name	User name to access the PostgreSQL database.
Password	Password for the PostgreSQL database user name.

Connection Property	Description
Encryption Method	Determines whether the data exchanged between the CDI-PC Integration Service and the PostgreSQL database server is encrypted: Select one of the following encryption methods: - noEncryption. Establishes a connection without using SSL. Data is not encrypted. - SSL. Establishes a connection using SSL. Data is encrypted using SSL. If the PostgreSQL database server does not support SSL, the connection fails. - requestSSL. Attempts to establish a connection using SSL. If the PostgreSQL database server does not support SSL, the CDI-PC Integration Service establishes an unencrypted connection. Default is noEncryption.
Validate Server Certificate	Applicable if you enable the encryption method to SSL or requestSSL. Select the **Validate Server Certificate** option so that the CDI-PC Integration Service validates the server certificate that is sent by the PostgreSQL database server. If you specify the **Hostname In Certificate** parameter, the CDI-PC Integration Service also validates the host name in the certificate.
TrustStore	Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts.
TrustStore Password	Applicable if you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. The password to access the truststore file that contains the SSL certificate.
Host Name In Certificate	Optional when you select SSL or requestSSL as the encryption method and the Validate Server Certificate option. Specifying a host name ensures additional security and the CDI-PC Integration Service validates the host name included in the connection with the host name in the SSL certificate.
KeyStore	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. The path and the file name of the key store. The keystore file contains the certificates that the PostgreSQL client sends to the PostgreSQL server in response to the server's certificate request.
KeyStore Password	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. The password for the keystore file required for secure communication.
Key Password	Applicable if you select SSL as the encryption method and when client authentication is enabled on the PostgreSQL database server. Required when individual keys in the keystore file have a different password than the keystore file.

Connection Property	Description
Additional Connection Properties	Additional connection parameters that you want to use. You must provide the connection parameters as semicolon-separated key-value pairs. For example, `ConnectionRetryCount=2; ConnectionRetryDelay=5`
Crypto Protocol Versions	Required if you enable the encryption method to SSL or requestSSL. Specifies a cryptographic protocol or a list of cryptographic protocols when you use an encrypted connection. You can select from the following protocols: - SSLv3 - TLSv1 - TLSv1_1 - TLSv1_2

Microsoft Dynamics 365 for Sales Connection Properties

When you configure a Microsoft Dynamics 365 for Sales connection, you define the connection attributes that the CDI-PC Integration Service uses to connect to the Microsoft Dynamics 365 for Sales database.

to be conreffed

The following table describes the Microsoft Dynamics 365 for Sales connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Authentication Type	The authentication method that the connector must use to login to the web application. Select one of the following authentication types: **OAuth 2.0 Password Grant.** It requires you to use the ADFS configuration. Specify the web API URL, username, password, and application ID. You additionally need the security token service URL to access Microsoft Dynamics 365 for Sales on-premises. Applies to Microsoft Dynamics 365 for Sales on-premise. **OAuth 2.0 Client Certificate Grant.** Requires you to specify the web API URL, application ID, tenant ID, keystore file, keystore password, key alias, and key password. Applies to Microsoft Dynamics 365 for Sales online. **OAuth 2.0 Client Secret.**Requires you to specify the application ID and client secret. Applies to Microsoft Dynamics 365 for Sales online. For more information on how to configure OAuth with IFD(ADFS) configuration, see the knowledge base article: Configuration of on-premise endpoint
Web API URL	The URL of the Microsoft Dynamics 365 for Sales endpoint.
Username	The user name to connect to the Microsoft Dynamics 365 for Sales account.
Password	The password to connect to the Microsoft Dynamics 365 for Sales account.

Property	Description
Application ID	The Azure application ID for Microsoft Dynamics 365 for Sales.
Tenant ID	The directory ID for Azure Active Directory.
Keystore File	The location and the file name of the key store. Not applicable when you use the Hosted Agent.
Keystore Password	The password for the keystore file required for secure communication.
Key Alias	The alias name for the individual key.
Key Password	The password for the individual keys in the keystore file required for secure communication. Not applicable when you use the Hosted Agent.
Retry Error Codes	The comma-separated http error codes for which the retries are made.
Retry Count	The number of retries to get the response from an endpoint based on the retry interval. Default is 5.
Retry Interval	The time in seconds to wait before Microsoft Dynamics 365 for Sales Connector retries for a response. Default is 60.
Client Secret	The client secret key to connect to Microsoft Dynamics 365 for Sales account.
Server Type	The Microsoft Dynamics 365 for Sales server that you want to access. You can select the server type from the following list: - **Microsoft Dynamics Online.** Select this option to connect to Microsoft Dynamics 365 for Sales deployed online. Requires you to enter the Web API URL, client secret, and certificate password. - **Microsoft Dynamics On-premise.** Select this option to connect to Microsoft Dynamics 365 for Sales deployed on-premises. Requires you to enter the ADFS client ID as Application ID and certificate password.
Security Token Service URL	The service URL with the security token. For example, `http://<customer_STS_URL>/adfs/oauth2/token`.

PowerExchange for Oracle E-Business Suite Connection Properties

When you configure an Oracle E-Business Suite connection, you define the connection attributes that the CDI-PC Integration Service uses to connect to the Oracle E-Business Suite.

The following table describes the connection properties:

Property	Description
User Name	User name to connect to Oracle E-Business Suite. If you are configuring a connection for an E-Business Suite target, the user name must be apps for the CDI-PC Integration Service to be able to execute the concurrent program.
Password	Password for the user name. You cannot use a parameter to specify the password.
Connect String	ODBC data source name. Use Informatica-certified ODBC drivers for ODBC data source connections.
Apps Schema Name	Name of the application schema that contains metadata for Oracle E-Business Suite. Default is apps.

Siebel Application Connections for Sources, Targets, and EIM Invoker Transformations

The Siebel Sources, Targets, and EIM Invoker transformations use the Siebel connection application connection to connect to the Siebel repository. When you configure an application connection, you must specify the connection attributes for the Siebel repository.

The following table describes the application connection properties:

Connection Parameter	Description
Protocol	Protocol used to connect to Siebel. Specify the following protocol parameters: - Transport. Enter HTTP or TCP/IP. Default is TCP/IP. - Encryption. Enter NONE or RSA. Default is NONE. - Compression. Enter NONE or ZLIB. Default is ZLIB. Specify the parameters in the following format: `siebel[[.transport][.[encryption][.[compression]]]]`
User Name	User name to connect to Siebel.
Password	Password for the user name.
Siebel Server Host	Host name or IP address of the Siebel server. If you configure native load balancing, specify the virtual host name.

Connection Parameter	Description
SCBroker Port	Siebel Connection Broker port number.
Enterprise Server	Enterprise Server name.
Application Object Manager	Siebel application business object manager.
Encoding	Encoding defined in the code page the CDI-PC Integration Service uses to communicate with the Siebel Server. Default is UTF-8.

Microsoft Dynamics CRM Connection

A Microsoft Dynamics CRM connection extracts data from and loads data to the Microsoft Dynamics CRM. PowerExchange for Microsoft Dynamics CRM uses SOAP to connect to Microsoft Dynamics CRM.

The following table describes the Microsoft Dynamics CRM connection properties:

Property	Description
Service Type	Type of Web service for passport authentication. Select Organizational service. **Note:** You can select Discovery service for active directory and claim-based authentication.
Application Server	Name of the server that hosts Microsoft Dynamics CRM. For active directory and claims-based authentication, provide the fully qualified domain name. The fully-qualified domain name must be the same as in the SSL certificate file. For passport authentication, specify the CRM Organization web service URL.
Port	Port in which Microsoft Dynamics CRM is configured. Configure for active directory, claims-based, and passport authentication.
Use SSL/TLS	Secure method to connect to the application server by using SSL or TLS security protocols. Configure for active directory and claims-based authentication.
Organization Name	Name of the organization that you want to connect to. Use one of the following options: - Name of the organization that appears when you log in to Microsoft Dynamics CRM. - Name that appears in the Deployment Manager. - The unique organization name. To find the unique organization name, log in to Microsoft Dynamics account and click **Settings** > **Customizations** > **Developer Resources**. Configure for active directory and claims-based authentication only.
Domain	Domain to which the user belongs. You must provide the complete domain name. Configure for active directory and claims-based authentication.

Property	Description
Authentication Type	Authentication type for the connection. Select one of the following authentication types based on the Microsoft Dynamics CRM deployment: - Passport. To connect to an online deployment of Microsoft Dynamics CRM using OAuth authentication. - Claims-based. To connect to an on-premise and Internet-facing deployment of Microsoft Dynamics CRM. - Active directory. To connect to on-premise deployment of Microsoft Dynamics CRM.
Security Token Service	Microsoft Dynamics CRM security token service URL. For example, https://sts1.company.com. Configure for claims-based authentication.

PowerExchange for Essbase Connections

When you configure a Essbase connection, you define the connection attributes that the CDI-PC Integration Service uses to connect to Essbase.

The following table describes the Essbase connection properties that you must configure:

Connection Attribute	Description
User Name	User name to connect to Essbase.
Password	Password to connect to Essbase.
ServerHost	Essbase server name.
Application	Name of the application. Default is none. **Note:** For a Unicode application, specify the name of the Unicode application.
Database	Name of the database. Default is none.

Vertica Relational Connection Properties

The following table describes the properties that you must configure for a Vertica relational connection:

Property	Description
Name	Enter a name for the connection.
Type	The connection type is set by default. You cannot edit this value.

Property	Description
User Name	Enter the user name to connect to the Vertica database. The user must have read permissions on the schema where the Vertica source table resides. Similarly, the user must have write permissions on the schema where the Vertica target table resides.
Password	Enter the password to connect to the Vertica database.
Use Parameter in Password	Indicates that the password for the repository user name is a session parameter, $Param*Name*. Define the password in the workflow or session parameter file, and encrypt it by using the *pmpasswd* CRYPT_DATA option. Default is disabled.
Connect String	Enter the name of the ODBC data source that you created for the Vertica database.
Code Page	Select the code page that the CDI-PC Integration Service Service must use to read or write data.
Connection Environment SQL	Runs an SQL command with each database connection. Default is disabled.
Transaction Environment SQL	Runs an SQL command before the initiation of each transaction. Default is disabled.
Connection Retry Period	The number of seconds that the CDI-PC Integration Service attempts to reconnect to the database if the connection fails. If the CDI-PC Integration Service cannot connect to the database in the retry period, the session fails. Default value is 0.
Load Balance	Select this option to enable load balancing on the Vertica database. When you enable load balancing, the CDI-PC Integration Service requests a load balanced connection with the Vertica database. Default is enabled. For more information on load balancing, see the Vertica database documentation.

PowerExchange for Db2 Warehouse Connections

The following table describes the Db2 Warehouse connection properties that you must configure:

Property	Description
User Name	Database user name with the appropriate read and write database permissions to access Db2 Warehouse.
Use Parameter in Password	Indicates the password for the database user name is a session parameter, $Param*Name*. Define the password in the workflow or session parameter file, and encrypt it by using the *pmpasswd* CRYPT_DATA option. Default is disabled.
Password	Password for the database user name.

Property	Description
Connect String	ODBC data source to connect to Db2 Warehouse.
Database Name	Database name of Db2 Warehouse that you want to connect to.
Schema Name	The schema name in Db2 Warehouse from where you want to fetch the metadata.
Server Name	Host name of Db2 Warehouse.
Port Number	Network port number used to connect to the Db2 Warehouse server.
Driver Name	Specify the name of the IBM Data Server driver that you configured in the `odbcinst.ini` file. For example, IBM DB2 ODBC DRIVER - IBMDBCL1.
Advanced connection properties	Optional. Additional connection parameters that you want to use. Specify the connection parameters as key-value pairs in the following format, and separate each key-value pair with a semicolon: `<param1>=<value>;<param2>=<value>;<param3>=<value>....`

PowerExchange for HANA Connections

You must configure a HANA ODBC data source before you can import HANA sources.

The following table describes the HANA ODBC connection properties:

Property	Decription
Name	Name you want to use for this connection. The connection name cannot contain spaces or other special characters, except for the underscore.
Type	Read-only. Type of database. For SAP HANA, this property is set to ODBC.
User Name	Database user name with the appropriate read and write database permissions to access the database. To define the user name in the parameter file, enter session parameter $ParamName as the user name, and define the value in the session or workflow parameter file. The Integration Service interprets user names that start with $Param as session parameters.
Use Parameter in Password	Indicates that the password for the database user name is a session parameter, $ParamName. Define the password in the workflow or session parameter file, and encrypt it by using the pmpasswd CRYPT_DATA option. Default is disabled.
Password	Password for the database user name. Must be in 7-bit ASCII.
Connect String	Connect string used to communicate with the SAP HANA database.

Property	Decription
Code Page	Code page the Integration Service uses to read from a source database or write to a target database.
Connection Environment SQL	Runs an SQL command with each database connection. Default is disabled.
Transaction Environment SQL	Runs an SQL command before the initiation of each transaction. Default is disabled.
Connection Retry Period	Number of seconds the Integration Service attempts to reconnect to the database if the connection fails. If the Integration Service cannot connect to the database in the retry period, the session fails. Default value is 0.
ODBC Subtype	Type of database to which ODBC connects. Select **SAP HANA**.

CHAPTER 10

Domain Object Export and Import

This chapter includes the following topics:

Domain Object Export and Import Overview

You can use the command line to migrate objects between two different domains of the same version.

You might migrate domain objects from a development environment to a test or production environment.

To export and import domain objects, use the following infacmd isp commands:

ExportDomainObjects

Exports native users, native groups, roles, and connections to an XML file.

ImportDomainObjects

Imports native users, native groups, roles, and connections into an Informatica domain.

You can use an infacmd control file to filter the objects during the export or import.

You can also use the infacmd xrf generateReadableViewXML command to generate a readable XML file from an export file. You can review the readable XML file to determine if you need to filter the objects that you import.

Export Process

You can use the command line to export domain objects from a domain.

Perform the following tasks to export domain objects:

1. Determine the domain objects that you want to export.
2. If you do not want to export all domain objects, create an export control file to filter the objects that are exported.
3. Run the infacmd isp exportDomainObjects command to export the domain objects.

The command exports the domain objects to an export file. You can use this file to import the objects into another domain.

Rules and Guidelines for Exporting Domain Objects

Review the following rules and guidelines before you export domain objects:

- When you export a user, by default, you do not export the user password. If you do not export the password, the administrator must reset the password for the user after the user is imported into the domain. However, when you run the infacmd isp exportDomainObjects command, you can choose to export an encrypted version of the password.
- When you export a user, you do not export the associated groups of the user. If applicable, assign the user to the group after you import the user and group.
- When you export a group, you export all sub-groups and users in the group.
- You cannot export the Administrator user, the Administrator role, the Everyone group, or LDAP users or groups. To replicate LDAP users and groups in an Informatica domain, import the LDAP users and groups directly from the LDAP directory service.
- To export native users and groups from domains of different versions, use the infacmd isp exportUsersAndGroups command.
- When you export a connection, by default, you do not export the connection password. If you do not export the password, the administrator must reset the password for the connection after the connection is imported into the domain. However, when you run the infacmd isp exportDomainObjects command, you can choose to export an encrypted version of the password.

View Domain Objects

You can view domain object names and properties in the export XML file.

Run infacmd xrf generateReadableViewXML command, to create a readable XML from the export file.

The following section provides a sample readable XML file:

```
<global:View xmlns:global="http://global" xmlns:connection="http://connection"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
  http://connection connection.xsd http://global globalSchemaDomain.xsd http://global
  globalSchema.xsd">
  <NativeUser isAdmin="false" name="admin" securityDomain="Native" viewId="0">
    <UserInfo email="" fullName="admin" phone="" viewId="1"/>
  </NativeUser>
  <User isAdmin="false" name="User1" securityDomain="Native" viewId="15">
    <UserInfo email="" fullName="NewUSer" phone="" viewId="16"/>
  </User>
  <Group name="TestGroup1" securityDomain="Native" viewId="182">
    <UserRef name="User1" securityDomain="Native" viewId="183"/>
    <UserRef name="User6" securityDomain="Native" viewId="188"/>
  </Group>
  <Role customRole="false" name="Administrator" viewId="242">
    <Description viewId="243">Provides all privilege and permission access to an
Informatica service.</Description>
    <ServicePrivilegeDefinition name="PwxListenerService" viewId="244">
      <Privilege category="" isEnabled="true" name="close" viewId="245"/>
      <Privilege category="" isEnabled="true" name="closeforce" viewId="246"/>
      <Privilege category="" isEnabled="false" name="Management Commands" viewId="249"/>
      <Privilege category="" isEnabled="false" name="Informational Commands"
viewId="250"/>
    </ServicePrivilegeDefinition>
  </Role>
```

```
  <Connection connectionString="inqa85sql25@qa90"
connectionType="SQLServerNativeConnection"
    domainName="" environmentSQL="" name="conn4" ownerName=""
    schemaName="" transactionSQL="" userName="dummy" viewId="7512">
    <ConnectionPool maxIdleTime="120" minConnections="0" usePool="true" viewId="7514"/>
  </Connection>
 </global:View>
```

Viewable Domain Object Names

You can view the following domain object names in the readable XML file:

- User
- UserInfo
- Role
- ServicePrivilegeDef
- Privilege
- Group
- GroupRef
- UserRef
- ConnectInfo
- ConnectionPoolAttributes

Supported Connection Types

- DB2iNativeConnection
- DB2NativeConnection
- DB2zNativeConnection
- JDBCConnection
- ODBCNativeConnection
- OracleNativeConnection
- PWXMetaConnection
- SAPConnection

Import Process

You can use the command line to import domain objects from an export file into a domain.

Perform the following tasks to import domain objects:

1. Run the infacmd xrf generateReadableViewXML command to generate a readable XML file from an export file. Review the domain objects in the readable XML file and determine the objects that you want to import.
2. If you do not want to import all domain objects in the export file, create an import control file to filter the objects that are imported.
3. Run the infacmd isp importDomainObjects command to import the domain objects into the specified domain.

4. After you import the objects, you may still have to create other domain objects such as application services and folders.

Rules and Guidelines for Importing Domain Objects

Review the following rules and guidelines before you import domain objects:

- When you import a group, you import all sub-groups and users in the group.
- To import native users and groups from domains of different versions, use the infacmd isp importUsersAndGroups command.
- After you import a user or group, you cannot rename the user or group.
- You import roles independently of users and groups. Assign roles to users and groups after you import the roles, users, and groups.
- You cannot import the Administrator group, the Administrator user, the Administrator role, the Everyone group, or LDAP users or groups.

Conflict Resolution

A conflict occurs when you try to import an object with a name that exists for an object in the target domain. Configure the conflict resolution to determine how to handle conflicts during the import.

You can define a conflict resolution strategy through the command line or control file when you import the objects. The control file takes precedence if you define conflict resolution in the command line and control file. The import fails if there is a conflict and you did not define a conflict resolution strategy.

You can configure one of the following conflict resolution strategies:

Reuse

Reuses the object in the target domain.

Rename

Renames the source object. You can provide a name in the control file, or else the name is generated. A generated name has a number appended to the end of the name.

Replace

Replaces the target object with the source object.

Merge

Merges the source and target objects into one group. For example, if you merge groups with the same name, users and sub-groups from both groups are merged into the group in the target domain.

You cannot define the merge conflict resolution strategy through the command line. Use a control file to define the merge conflict resolution strategy. You must include the group object type section with merge as the conflict resolution policy with reuse, replace, or rename for all conflicting users in the control file.

For example, specify the merge conflict resolution strategy for the following groups:

- Group A with users a1, a2, b1, b2 in the source domain.
- Group A with users a1, a2, a3 b1, b2 in the target domain

You get the following results in the group after merge in the target domain:

- a1, a2, b1, b2 if you choose reuse or replace
- a1, a2, a3, b1, b2 if you choose rename.

CHAPTER 11

License Management

This chapter includes the following topics:

License Management Overview

The Service Manager on the master gateway node manages Informatica licenses.

A license enables you to perform the following tasks:

- Run application services, such as the CDI-PC Repository Service.
- Use add-on options, such as partitioning for CDI-PC, grid, and high availability.
- Access particular types of connections, such as Oracle, Teradata, Microsoft SQL Server, and IBM MQ Series.

When you install Informatica, the installation program creates a license object in the domain based on the license key that you used during installation.

You assign a license object to each application service to enable the service. For example, you must assign a license to the CDI-PC Integration Service before you can use the CDI-PC Integration Service to run a workflow.

You can create additional license objects in the domain. Based on your project requirements, you may need multiple license objects. For example, you may have two license objects, where each license object allows you to run services on a different operating system. You might also use multiple license objects to manage multiple projects in the same domain. One project may require access to particular database types, while the other project does not.

License Validation

The Service Manager validates application service processes when they start. The Service Manager validates the following information for each service process:

- Product version. Verifies that you are running the appropriate version of the Informatica services.
- Platform. Verifies that the Informatica services are running on a licensed operating system.

- Expiration date. Verifies that the license is not expired. If the license expires, no application service assigned to the license can start. You must assign a valid license to the Informatica services to start them.
- CDI-PC options. Determines the options that the Informatica services have permission to use. For example, the Service Manager verifies if the CDI-PC Integration Service can use the Session on Grid option.
- Connectivity. Verifies connections that the Informatica services have permission to use. For example, the Service Manager verifies that CDI-PC can connect to a IBM DB2 database.

Licensing Log Events

The Service Manager generates log events and writes them to the Log Manager. It generates log events for the following actions:

- You create or delete a license.
- You apply an incremental license key to a license.
- You assign an application service to a license.
- You unassign a license from an application service.
- The license expires.
- The Service Manager encounters an error, such as a validation error.

The log events include the user name and the time associated with the event.

You must have permission on the domain to view the logs for Licensing events.

The Licensing events appear in the domain logs.

License Management Tasks

You can perform the following tasks to manage the licenses:

- Create the license in the Administrator tool. You use a license key to create a license in the Administrator tool.
- Assign a license to each application service. Assign a license to each application service to enable the service.
- Remove the license. Remove a license if it is obsolete.
- Configure user permissions on a license.
- View license details. You may need to review the licenses to determine details, such as expiration date and the maximum number of licensed CPUs. You may want to review these details to ensure you are in compliance with the license. Use the Administrator tool to determine the details for each license.
- Monitor license usage and licensed options. You can monitor the usage of logical CPUs and CDI-PC Repository Service. You can monitor the number of software options purchased for a license and the number of times a license exceeds usage limits in the License Management Report.

You can perform all of these tasks in the Administrator tool or by using *infacmd isp* commands.

Creating a License Object

You can create a license object in a domain and assign the license to application services. You can create the license in the Administrator tool using a license key file. The license key file contains an encrypted original key. You use the original key to create the license.

You can also use the *infacmd isp* AddLicense command to add a license to the domain.

Use the following guidelines to create a license:

- Use a valid license key file. The license key file must contain an original license key. The license key file must not be expired.
- You cannot use the same license key file for multiple licenses. Each license must have a unique original key.
- Enter a unique name for each license. You create a name for the license when you create the license. The name must be unique among all objects in the domain.
- Put the license key file in a location that is accessible by the Administrator tool computer. When you create the license object, you must specify the location of the license key file.

After you create the license, you can change the description. To change the description of a license, select the license in Navigator of the Administrator tool, and then click Edit.

1. In the Administrator tool, click **Actions** > **New** > **License**.

   The **Create License** window appears.

2. Enter the following options:

Option	Description
Name	Name of the license. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the license. The description cannot exceed 765 characters.
Path	Path of the domain in which you create the license. Read-only field. Optionally, click **Browse** and select a domain in the **Select Folder** window. Optionally, click **Create Folder** to create a folder for the domain.
License File	File containing the original key. Click **Browse** to locate the file.

   If you try to create a license using an incremental key, a message appears that states you cannot apply an incremental key before you add an original key.

   You must use an original key to create a license.

3. Click **Create**.

Assigning a License to a Service

Assign a license to an application service before you can enable the service. When you assign a license to a service, the Service Manager updates the license metadata. You can also use the *infacmd isp* AssignLicense command to assign a license to a service.

1. Select the license in the **Domain Navigator** of the Administrator tool.
2. Click the **Assigned Services** tab.
3. In the **License** tab, click **Actions** > **Edit Assigned Services.**

   The **Assign or Unassign this license to the services** window appears.
4. Select the services under **Unassigned Services**, and click Add.

   Use Ctrl-click to select multiple services. Use Shift-click to select a range of services. Optionally, click **Add all** to assign all services.
5. Click **OK**.

Rules and Guidelines for Assigning a License to a Service

Use the following rules and guidelines when you assign licenses:

- You can assign licenses to disabled services.
- If you want to assign a license to a service that has a license assigned to it, you must first unassign the existing license from the service.
- To start a service with backup nodes, you must assign it to a license with high availability.
- To restart a service automatically, you must assign the service to a license with high availability.

License Properties

You can view license details using the Administrator tool or the *infacmd isp* ShowLicense command.

The license details are based on all license keys applied to the license. The Service Manager updates the existing license details when you add a new incremental key to the license.

You might review license details to determine options that are available for use. You may also review the license details and license usage logs when monitoring licenses.

For example, you can determine the number of CPUs your company is licensed to use for each operating system.

To view license details, select the license in the **Domain Navigator**.

The Administrator tool displays the license properties in the following sections:

- License Details. View license details on the **Properties** tab. Shows license attributes, such as the license object name, description, and expiration date.
- Assigned Services. View application services that are assigned to the license on the **Assigned Services** tab.
- CDI-PC Options. View the CDI-PC options on the **Options** tab. Shows all licensed CDI-PC options, such as session on grid, high availability, and pushdown optimization.

- Connections. View the licensed connections on the **Options** tab. Shows all licensed connections. The license enables you to use connections, such as DB2 and Oracle database connections.

License Details

You can use the license details to view high-level information about the license. Use this license information when you audit the licensing usage.

The general properties for the license appear in the **License Details** section of the **Properties** tab.

The following table describes the general properties for a license:

Property	Description
Name	Name of the license.
Description	Description of the license.
Location	Path to the license in the Navigator.
Edition	CDI-PC Advanced edition.
License Version	Version of license.
Distributed By	Distributor of the product.
Issued On	Date when the license was issued to the customer.
Expires On	Date when the license expires.
Validity Period	Period for which the license is valid.
Serial Number	Serial number of the license. The serial number identifies the customer or project. If you have multiple CDI-PC installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are "Development" and "Production."

You can also use the license event logs to view audit summary reports. You must have permission on the domain to view the logs for license events.

Service Options

The license enables you to use Informatica Service options such as data cleansing, data federation, and pushdown optimization.

The options for the license appear in the Service Options section of the **Options** tab.

Connections

The license enables you to use connections such as DB2 and Oracle database connections. The license also enables you to use connections for PowerExchange adapters such as PowerExchange for Facebook.

The connections for the license appear in the Connections section of the **Options** tab.

CHAPTER 12

Log Management

This chapter includes the following topics:

Log Management Overview

The Service Manager accumulates log events for the domain, application services, users, and CDI-PC sessions and workflows. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent.

The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations, application services, and user activity. The log events contain operational and error messages for a domain. The Service Manager and the application services send log events to the Log Manager. When the Log Manager receives log events, it generates log event files. You can view service log events in the Administrator tool based on criteria that you provide.

The Log Agent runs on all nodes in the domain. The Log Agent retrieves the workflow and session log events that the CDI-PC Integration Service writes and displays them in the Workflow Monitor. Workflow log events include information about workflow processing, workflow errors, and tasks that the CDI-PC Integration Service performs. Session log events include information about the tasks performed by the CDI-PC Integration Service, session errors, and load summary and transformation statistics for the session. You can view log events for the last workflow run with the Log Events window in the Workflow Monitor.

Log event files are binary files that the Administrator tool Logs Viewer uses to display log events. When you view log events in the Administrator tool, the Log Manager uses the log event files to display the log events for the domain, application services, and user activity.

Domain logs include domain, application service, and user activity logs. You can view them in the Administrator tool. System logs are for use only by Informatica Support to address open support issues.

You can use the Administrator tool to perform the following tasks with the Log Manager:

- Configure the log location. Configure the node that runs the Log Manager, the directory path for log event files, purge options, and time zone for log events.
- Configure log management. Configure the Log Manager to purge logs or purge logs manually. Save log events to XML, text, or binary files. Configure the time zone for the time stamp in the log event files.
- View log events. View domain function, application service, and user activity log events on the Logs tab. Filter log events by domain, application service type, and user.

Log Manager Architecture

The Service Manager on the master gateway node controls the Log Manager. The Log Manager starts when you start the Informatica services. After the Log Manager starts, it listens for log events from the Service Manager and application services. When the Log Manager receives log events, it generates log event files.

The Log Manager creates the following types of log files:

- Log event files. Stores log events in binary format. The Log Manager creates log event files to display log events in the Logs tab. When you view events in the Administrator tool, the Log Manager retrieves the log events from the event nodes.

  The Log Manager stores the files by date and by node. Set the directory path with the infasetup tools defineDomain command -ld option.
- Guaranteed Message Delivery files. Stores domain, application service, and user activity log events. The Service Manager writes the log events to temporary Guaranteed Message Delivery files and sends the log events to the Log Manager.

  If the Log Manager becomes unavailable, the Guaranteed Message Delivery files stay in the default log directory on the node where the service runs. By default, the directory path is `<Informatica_installation_directory>/logs/<Node_Name>`. When the Log Manager becomes available, the Service Manager for the node reads the log events in the temporary files, sends the log events to the Log Manager, and deletes the temporary files.

CDI-PC Session and Workflow Log Events

CDI-PC session and workflow logs are stored in a separate location from the domain, application service, and user activity logs. The CDI-PC Integration Service writes session and workflow log events to binary files on the node where the CDI-PC Integration Service runs.

The Log Manager performs the following tasks to process CDI-PC session and workflow log events:

1. During a session or workflow, the CDI-PC Integration Service writes binary log files on the node. It sends information about the logs to the Log Manager.
2. The Log Manager stores information about workflow and session logs in the domain database. The domain database stores information such as the path to the log file location, the node that contains the log, and the CDI-PC Integration Service that created the log.
3. When you view a session or workflow in the Log Events window of the Workflow Monitor, the Log Manager retrieves the information from the domain database. The Log Manager uses the information to determine the location of the logs.
4. The Log Manager dispatches a Log Agent to retrieve the log events on each node to display in the Log Events window.

Log Manager Recovery

When a service generates log events, it sends them to the Log Manager on the master gateway node. When you have the high availability option and the master gateway node becomes unavailable, the application services send log events to the Log Manager on a new master gateway node.

The Service Manager, the application services, and the Log Manager perform the following tasks:

1. An application service process writes log events to a Guaranteed Message Delivery file.
2. The application service process sends the log events to the Service Manager on the gateway node for the domain.
3. The Log Manager processes the log events and writes log event files. The application service process deletes the temporary file.
4. If the Log Manager is unavailable, the Guaranteed Message Delivery files stay on the node running the service process. The Service Manager for the node sends the log events in the Guaranteed Message Delivery files when the Log Manager becomes available, and the Log Manager writes log event files.

Troubleshooting the Log Manager

Domain and application services write log events to Service Manager log files when the Log Manager cannot process log events. The Service Manager log files are located in the default logs directory. The Service Manager log files include catalina.out, localhost_<date>.txt, and node.log. Services write log events to different log files depending on the type of error.

Use the Service Manager log files to troubleshoot issues when the Log Manager cannot process log events. You will also need to use these files to troubleshoot issues when you contact Informatica Global Customer Support.

Note: You can troubleshoot an Informatica installation by reviewing the log files generated during installation. You can use the installation summary log file to find out which components failed during installation.

Log Location

The Service Manager on the master gateway node writes log event files to the log file directory. When you configure a node to serve as a gateway, you must configure the directory where the Service Manager on this node writes the log event files. Each gateway node must have access to the directory path.

You configure the log location in the Properties view for the domain. Configure a directory location that is accessible to the gateway node during installation or when you define the domain. Store the logs on a shared disk when you have more than one gateway node. If the Log Manager is unable to write to the directory path, it writes log events to node.log on the master gateway node.

When you configure the log location, the Administrator tool validates the directory as you update the configuration. If the directory is invalid, the update fails. The Log Manager verifies that the log directory has read/write permissions on startup. Log files might contain inconsistencies if the log directory is not shared in a highly available environment.

You can change the directory path for domain logs in the Administrator tool or with the log service directory parameter, -ld. You can use the -ld parameter with any of the following commands:

- infacmd isp SwitchToGatewayNode
- infasetup DefineDomain

- infasetup DefineGatewayNode
- infasetup UpdateGatewayNode

System Logs

System logs contain information that Informatica Support views to help solve issues that you raise with Support. Ordinarily, you have no need to view these logs.

By default, the directory path is `<Informatica_installation_directory>/logs/<Node_Name>/`.. You can change the default directory path for logs with the System Log Directory parameter, -sld. You can use the -sld parameter with any of the following commands:

- infasetup DefineDomain
- infasetup DefineGatewayNode
- infasetup DefineWorkerNode
- infasetup UpdateGatewayNode
- infasetup UpdateWorkerNode

When you create a custom location, you can use a local location or a location that all domain nodes share. The Service Manager adds the node name to the path and creates separate log directories for each node.

When you update the gateway node or worker node with a new default location for system logs, existing logs remain intact. The server creates future logs at the new location, and abandons logs at the old location.

If you specify a node name when you change the default path, the Service Manager adds it to the path. For example, if you specify C:/logs/node1/ as the system log directory, the Service Manager creates logs in directories under C:/logs/node1/node1/.

If you have multiple Informatica domains, you must configure a different directory path for the Log Manager in each domain. Multiple domains cannot use the same shared directory path.

Note: When you change the directory path, you must restart Informatica services on the node you changed.

Log Management Configuration

The Service Manager and the application services continually send log events to the Log Manager. As a result, the directory location for the logs can grow to contain a large number of log events.

You can purge logs events periodically to manage the amount of log events stored by the Log Manager. You can export logs before you purge them to keep a backup of the log events.

Purging Log Events

You can automatically or manually purge log events. The Service Manager purges log events from the log directory according to the purge properties you configure in the Log Management dialog box. You can manually purge log events to override the automatic purge properties.

Purging Log Events Automatically

The Service Manager purges log events from the log directory according to the purge properties.

When the number of days or the size of the log directory exceeds the limit, the Log Manager deletes the log event files, starting with the oldest log events. The Log Manager periodically verifies the purge options and purges log events. The Log Manager does not purge the current day log event files and folder.

The following table lists purge properties:

Option	Description
Preserve logs for number of days	Number of days to preserve logs. Default is 30.
Maximum size for logs in MB	Number of megabytes of disk space to store logs. Default is 200.

Note: The Log Manager does not purge CDI-PC session and workflow log files.

Purging Log Events Manually

You can purge log events for the domain, application services, or user activity. When you purge log events, the Log Manager removes the log event files from the log directory. The Log Manager does not remove log event files currently being written to the logs.

Optionally, you can use the *infacmd* PurgeLog command to purge log events.

The following table lists the purge log options:

Option	Description
Log Type	Type of log events to purge. You can purge domain, service, user activity or all log events.
Service Type	When you purge application service log events, you can purge log events for a particular application service type or all application service types.
Purge Entries	Date range of log events you want to purge. You can select the following options: - All Entries. Purges all log events. - Before Date. Purges log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.

Time Zone

When the Log Manager creates log event files, it generates a time stamp based on the time zone for each log event. The log event time stamp includes date, time, and time zone information. When the Log Manager creates log folders, it labels folders according to a time stamp. When you export or purge log event files, the Log Manager uses this property to calculate which log event files to purge or export. Set the time zone to the location of the machine that stores the log event files.

Verify that you do not lose log event files when you configure the time zone for the Log Manager. If the application service that sends log events to the Log Manager is in a different time zone than the master gateway node, you may lose log event files you did not intend to delete. Configure the same time zone for each gateway node.

Note: When you change the time zone, you must restart Informatica Services on the node that you changed.

Configuring Log Management Properties

Configure the log management properties in the **Log Management** dialog box in Informatica Administrator.

1. In the Administrator console, click the **Logs** tab.
2. Select **Log Actions** > **Log Management**.
3. Enter the number of days for the Log Manager to preserve log events.
4. Enter the maximum disk size for the directory that contains the log event files.
5. Enter the time zone in the following format:

   ```
   GMT(+|-)<hours>:<minutes>
   ```

   For example: GMT+08:00
6. Click **OK**.

Using the Logs Tab

You can view domain, application service, and user activity log events in the Logs tab of the Administrator tool. When you view log events in the Logs tab, the Log Manager displays the generated log event files in the log directory. When an error message appears in the Administrator tool, the error provides a link to the Logs tab.

You can use the Logs tab to perform the following tasks:

- View log events and the Administrator tool operational errors. View log events for the domain, an application service, or user activity.
- Filter log event results. After you display the log events, you can display log events that match filter criteria.
- Configure columns. Configure the columns you want the Logs tab to display.
- Save log events. You can save log events in XML, text, and binary format.
- Purge log events. You can manually purge log events.
- Copy log event rows. You can copy log event rows.

Viewing Log Events

To view log events in the Logs tab of the Administrator tool, select the Domain, Service, or User Activity view. Next, configure the filter options. You can filter log events based on attributes such as log type, domain function category, application service type, application service name, user, message code, activity code, timestamp, and severity level. The available options depend on whether you choose to view domain, application service, or user activity log events.

To view more information about a log event, click the log event in the search results.

On AIX and Linux, if the Log Manager receives an internal error message from the CDI-PC Integration Service, it writes a stack trace to the log event window.

You can view logs to get more information about errors that you receive while working in the Administrator tool.

1. In the Administrator Tool, click the Logs tab.
2. In the contents panel, select Domain, Service, or User Activity view.

3. Configure the filter criteria to view a specific type of log event.

   The following table lists the query options:

Log Type	Option	Description
Domain	Category	Category of domain service you want to view.
Service	Service Type	Application service you want to view.
Service	Service Name	Name of the application service for which you want to view log events. You can choose a single application service name or all application services.
Domain, Service	Severity	The Log Manager returns log events with this severity level.
User Activity	User	User name for the Administrator tool user.
User Activity	Security Domain	Security domain to which the user belongs.
Domain, Service, User Activity	Timestamp	Date range for the log events that you want to view. You can choose the following options: - Blank. View all log events. - Within Last Day - Within Last Month - Custom. Specify the start and end date. Default is Within Last Day.
Domain, Service	Thread	Filter criteria for text that appears in the thread data. You can use wildcards (*) in this text field.
Domain, Service	Message Code	Filter criteria for text that appears in the message code. You can also use wildcards (*) in this text field.
Domain, Service	Message	Filter criteria for text that appears in the message. You can also use wildcards (*) in this text field.
Domain, Service	Node	Name of the node for which you want to view log events.
Domain, Service	Process	Process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.
User Activity	Activity Code	Filter criteria for text that appears in the activity code. You can also use wildcards (*) in this text field.
User Activity	Activity	Filter criteria for text that appears in the activity. You can also use wildcards (*) in this text field.

4. Click the Filter button.

   The Log Manager retrieves the log events and displays them in the Logs tab with the most recent log events first.

5. Click the Reset Filter button to view a different set of log events.

   Tip: To search for logs related to an error or fatal log event, note the timestamp of the log event. Then, reset the filter and use a custom filter to search for log events during the timestamp of the event.

Configuring Log Columns

You can configure the Logs tab to display the following columns:

- Category
- Service Type
- Service Name
- Severity
- User
- Security Domain
- Timestamp
- Thread
- Message Code
- Message
- Node
- Process
- Activity Code
- Activity

Note: The columns appear based on the query options that you choose. For example, when you display a service type, the service name appears in the Logs tab.

1. In the Administrator Tool, click the **Logs** tab.
2. Select the **Domain**, **Service**, or **User Activity** view.
3. To add a column, right-click a column name, select **Columns**, and then the name of the column you want to add.
4. To remove a column, right-click a column name, select **Columns**, and then clear the checkmark next to the name of the column you want to remove.
5. To move a column, select the column name, and then drag it to the location where you want it to appear.

   The Log Manager updates the Logs tab columns with your selections.

Saving Log Events

You can save the log events that you filter and view in the Log Viewer. When you save log events, the Log Manager saves whatever logs that you are viewing based on the filter criteria. To save log events to a file, click Save Logs on the Log Actions menu.

The Log Manager does not delete the log events when you save them. The Administrator Tool prompts you to save or open the saved log events file.

Optionally, you can use the *infacmd* isp GetLog command to retrieve log events.

The format you choose to save log events to depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

Exporting Log Events

You can export the log events to an XML, text, or binary file. To export log events to a file, click Export Logs on the Log Actions menu.

When you export log events, you can choose which logs you want to save. When you choose Service logs, you can export logs for a particular service type. You can choose the sort order of the log events in the export file.

The Log Manager does not delete the log events when you export them. The Administrator tool prompts you to save or open the exported log events file.

Optionally, you can use the *infacmd* GetLog command to retrieve log events.

The format you choose to export log events depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

The following table describes the export log options for each log type:

Option	Log Type	Description
Type	Domain, Service, User Activity	Type of logs you want to export.
Service Type	Service	Type of application service for which to export log events. You can also export log events for all service types.
Export Entries	Domain, Service, User Activity	Date range of log events you want to export. You can select the following options: - All Entries. Exports all log events. - Before Date. Exports log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.
Export logs in descending chronological order	Domain, Service, User Activity	Exports log events starting with the most recent log events.

XML Format

When you export log events to an XML file, the Log Manager exports each log event as a separate element in the XML file. The following example shows an excerpt from a log events XML file:

```
<log xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:common="http://
www.informatica.com/pcsf/common" xmlns:metadata="http://www.informatica.com/pcsf/
metadata" xmlns:domainservice="http://www.informatica.com/pcsf/domainservice"
xmlns:logservice="http://www.informatica.com/pcsf/logservice" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098642698"
severity="3" messageCode="AUTHEN_USER_LOGIN_SUCCEEDED" message="User Admin successfully
logged in." user="Admin" stacktrace="" service="authenticationservice"
serviceType="PCSF" clientNode="sapphire" pid="0" threadName="http-8080-Processor24"
context="" />
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098517000"
severity="3" messageCode="LM_36854" message="Connected to node [garnet] on outbound
connection [id = 2]." user="" stacktrace="" service="Copper" serviceType="IS"
clientNode="sapphire" pid="4484" threadName="4528" context="" />
```

Text Format

When you export log events to a text file, the Log Manager exports the log events in Information and Content Exchange (ICE) Protocol. The following example shows an excerpt from a log events text file:

```
2006-02-27 12:29:41 : INFO : (2628 | 2768) : (IS | Copper) : sapphire : LM_36522 :
Started process [pid = 2852] for task instance Session task instance
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master.
2006-02-27 12:29:41 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor -
Master].
2006-02-27 12:29:36 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : LM_36522 :
Started process [pid = 2632] for task instance Session task instance
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer.
2006-02-27 12:29:35 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer].
```

Binary Format

When you export log events to a binary file, the Log Manager exports the log events to a file that Informatica Global Customer Support can import. You cannot view the file unless you convert it to text. You can use the *infacmd* ConvertLogFile command to convert binary log files to text files, XML files, or readable text on the screen.

Viewing Administrator Tool Log Errors

If you receive an error while starting, updating, or removing services in the Administrator tool, an error message in the contents panel of the service provides a link to the Logs tab. Click the link in the error message to access detail information about the error in the Logs tab.

Log Events

The Service Manager and application services send log events to the Log Manager. The Log Manager generates log events for each service type.

Log events include a timestamp, in milliseconds, and a thread name that identifies the event.

You can view the following log event types on the Logs tab:

- Domain log events. Log events generated from the Service Manager functions.
- CDI-PC Integration Service log events. Log events about each CDI-PC Integration Service running in the domain.
- CDI-PC Repository Service log events. Log events from each CDI-PC Repository Service running in the domain.
- Resource Manager Service log events. Log events about the Resource Manager Service running in the domain.
- SAP BW Service log events. Log events about the interaction between the CDI-PC and the SAP NetWeaver BI system.
- Web Services Hub log events. Log events about the interaction between applications and the Web Services Hub.
- User activity log events. Log events about domain and security management tasks that a user completes.

Log Event Components

The Log Manager uses a common format to store and display log events. You can use the components of the log events to troubleshoot Informatica.

Each log event contains the following components:

- Service type, category, or user. The Logs tab categorizes events by domain category, service type, or user. If you view application service logs, the Logs tab displays the application service names. When you view domain logs, the Logs tab displays the domain categories in the log. When you view user activity logs, the Logs tab displays the users in the log.
- Message or activity. Message or activity text for the log event. Use the message text to get more information about the log events for domain and application services. Use the activity text to get more information about log events for user activity. Some log events contain embedded log event in the message texts. For example, the following log events contains an embedded log event:

  ```
  Client application [PmDTM], connection [59]: recv failed.
  ```

  In this log event, the following log event is the embedded log event:

  ```
  [PmDTM], connection [59]: recv failed.
  ```

  When the Log Manager displays the log event, the Log Manager displays the severity level for the embedded log event.
- Security domain. When you view user activity logs, the Logs tab displays the security domain for each user.
- Message or activity code. Log event code. If the message type is error or fatal, click on the message code to open the Informatica Knowledge Base search for the message. You must configure the support portal credentials in the user account to do the search.
- Process. The process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.
- Node. Name of the node running the process that generated the log event.
- Thread. Identification number or name of a thread started by a service process.
- Time stamp. Date, time, and time zone of the log event that occurred.
- Severity. The severity level for the log event. When you view log events, you can configure the Logs tab to display log events for a specific severity level.

Domain Log Events

Domain log events are log events generated from the domain functions the Service Manager performs.

Use the domain log events to view information about the domain and troubleshoot issues. You can use the domain log events to troubleshoot issues related to the startup and initialization of nodes and application services for the domain.

Domain log events include log events from the following functions:

- Authorization. Log events that occur when the Service Manager authorizes user requests for services. Requests can come from the Administrator tool.

  Note: Sensitive information might not appear in the domain log. For example, in case of a user authentication failure, the user and security domain for failed login attempts do not appear. The User Activity log contains full information.
- Container Management. Log events that occur when the Service Manager manages containers on nodes with the compute role.
- Domain Configuration. Log events that occur when the Service Manager manages the domain configuration metadata.
- Licensing. Log events that occur when the Service Manager registers license information.
- License Usage. Log events that occur when the Service Manager verifies license information from application services.
- Log Manager. Log events from the Log Manager. The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations and application services.
- Log Agent. Log events from the Log Agent.
- Monitoring. Log events about Domain Functions.
- Node Configuration. Log events that occur as the Service Manager manages node configuration metadata in the domain.
- User Management. Log events that occur when the Service Manager manages users, groups, roles, and privileges.
- Service Manager. Log events from the Service Manager and signal exceptions from DTM processes. The Service Manager manages all domain operations. If the error severity level of a node is set to Debug, when a service starts the log events include the environment variables used by the service.

Listener Service Log Events

The PowerExchange Listener logs contain information about the application service that manages the PowerExchange Listener.

The Listener Service logs contain the following information:

- Client communication. Log events for communication between a CDI-PC or PowerExchange client and a data source.
- Listener service. Log events about the Listener service, including configuring, enabling, and disabling the service.
- Listener service operations. Log events for operations such as managing bulk data movement and change data capture.

Logger Service Log Events

The PowerExchange Logger Service writes logs about the application service that manages the PowerExchange Logger.

The Logger Service logs contain the following information:

- Connections. Log events about connections between the Logger Service and the source databases.
- Logger service. Log events about the Logger Service, including configuring, enabling, and disabling the service.
- Logger service operations. Log events for operations such as capturing changed data and writing the data to PowerExchange Logger files.

CDI-PC Integration Service Log Events

The CDI-PC Integration Service log events contain information about each CDI-PC Integration Service running in the domain.

CDI-PC Integration Service log events contain the following information:

- CDI-PC Integration Service processes. Log events about the CDI-PC Integration Service processes, including service ports, code page, operating mode, service name, and the associated repository and CDI-PC Integration Service status.
- Licensing. Log events for license verification for the CDI-PC Integration Service by the Service Manager.

CDI-PC Repository Service Log Events

The CDI-PC Repository Service log events contain information about each CDI-PC Repository Service running in the domain.

CDI-PC Repository Service log events contain the following information:

- CDI-PC repository connections. Log events for connections to the repository from CDI-PC Client applications, including user name and the host name and port number for the client application.
- CDI-PC repository objects. Log events for repository objects locked, fetched, inserted, or updated by the CDI-PC Repository Service.
- CDI-PC Repository Service processes. Log events about CDI-PC Repository Service processes, including starting and stopping the CDI-PC Repository Service and information about repository databases used by the CDI-PC Repository Service processes. Also includes repository operating mode, the nodes where the CDI-PC Repository Service process runs, initialization information, and internal functions used.
- Repository operations. Log events for repository operations, including creating, deleting, restoring, and upgrading repository content, copying repository contents, and registering and unregistering local repositories.
- Licensing. Log events about CDI-PC Repository Service license verification.

Resource Manager Service Log Events

Resource Manager Service log events contain the following information:

- Resource Manager Service. Log events about the Resource Manager Service, including enabling, disabling, starting, and stopping the service.
- Compute nodes. Log events about nodes with the compute role registering with the Resource Manager Service.

SAP BW Service Log Events

The SAP BW Service log events contain information about the interaction between CDI-PC and the SAP NetWeaver BI system.

SAP NetWeaver BI log events contain the following log events for an SAP BW Service:

- SAP NetWeaver BI system log events. Requests from the SAP NetWeaver BI system to start a workflow and status information from the ZPMSENDSTATUS ABAP program in the process chain.
- CDI-PC Integration Service log events. Session and workflow status for sessions and workflows that use a CDI-PC Integration Service process to load data to or extract data from SAP NetWeaver BI.

To view log events about how the CDI-PC Integration Service processes an SAP NetWeaver BI workflow, you must view the session or workflow log.

Web Services Hub Log Events

The Web Services Hub log events contain information about the interaction between applications and the Web Services Hub.

Web Services Hub log events contain the following log events:

- Web Services processes. Log events about web service processes, including starting and stopping Web Services Hub, web services requests, the status of the requests, and error messages for web service calls. Log events include information about which service workflows are fetched from the repository.
- CDI-PC Integration Service log events. Workflow and session status for service workflows including invalid workflow errors.

User Activity Log Events

User activity log events describe all domain and security management tasks that a user completes.

Use the user activity log events to determine when a user created, updated, or removed services, nodes, users, groups, or roles.

The Service Manager writes user activity log events when the Service Manager needs to authorize a user to perform one of the following domain actions:

- Enable or disable a service process.
- Start, stop, enable, or disable a service.
- Add, update, or shut down a node.
- Modify the domain properties.
- Move a folder in the domain.

The Service Manager also writes user activity log events each time a user adds, updates, or removes a user, group, operating system profile, or role.

The user activity log displays information about the user who performed the security action or who failed to log in. When the Service Manager logs an unsuccessful login attempt, the logs display an error message that contains the following information:

- User ID whose login attempt failed
- Security domain that rejected the login attempt
- Application and version that the user attempted to log in to. For example: `application [Informatica Administrator] version [10.5.2]`

- Client IP address from which the login attempt originated
- Reason for the rejection. For example: `[<error code>] The user [<user ID>] in security domain [Native] does not exist in the domain.]`

The user activity logs also displays information about security audit trails and log events for changes to users, groups, and permissions.

The Service Manager writes a user activity log event each time a user account is locked or unlocked. The Service Manager also writes a user activity log event each time a user tries to log in to the domain with a client application.

To include security audit trails in the user activity log events, you must enable the SecurityAuditTrail property for the CDI-PC Repository Service in the Administrator tool.

When you import one or more repository objects, you can generate audit logs.

The audit logs contain the following information about the .xml file imported:

- Host name and IP address of the client machine from which the .xml file was imported
- Full local path of the .xml import file
- The file name
- The file size in bytes
- Logged in user name
- Number of objects imported
- Time stamp of the import operation

CHAPTER 13

Domain Reports

This chapter includes the following topics:

Domain Reports Overview

You can run the following domain reports from the Reports tab in the Administrator tool:

- License Management Report. Monitors the number of software options purchased for a license and the number of times a license exceeds usage limits. The License Management Report displays the license usage information such as CPU and repository usage and the node configuration details.
- Web Services Report. Monitors activities of the web services running on a Web Services Hub. The Web Services Report displays run-time information such as the number of successful or failed requests and average service time. You can also view historical statistics for a specific period of time.

Note: If the master gateway node runs on a UNIX machine and the UNIX machine does not have a graphics display server, you must install X Virtual Frame Buffer on the UNIX machine to view the report charts in the License Report or the Web Services Report. If you have multiple gateway nodes running on UNIX machines, install X Virtual Frame Buffer on each UNIX machine.

License Management Report

You can monitor the list of software options purchased with a license and the number of times a license exceeds usage limits. The License Management Report displays the general properties, CPU and repository usage, user details, hardware and node configuration details, and the options purchased for each license.

You can save the License Management Report as a PDF on your local machine. You can also email a PDF version of the report to someone.

Run the License Management Report to monitor the following license usage information:

- Licensing details. Shows general properties for every license assigned in the domain.
- CPU usage. Shows the number of logical CPUs used to run application services in the domain. The License Management Report counts logical CPUs instead of physical CPUs for license enforcement. If the

number of logical CPUs exceeds the number of authorized CPUs, then the License Management Report shows that the domain exceeded the CPU limit.

- Repository usage. Shows the number of CDI-PC Repository Service in the domain.
- User information. Shows information about users in the domain.
- Hardware configuration. Shows details about the machines used in the domain.
- Node configuration. Shows details about each node in the domain.
- Licensed options. Shows a list of CDI-PC and other Informatica options purchased for each license.

Licensing

The Licensing section of the License Management Report shows information about each license in the domain.

The following table describes the licensing information in the License Management Report:

Property	Description
Name	Name of the license.
Edition	CDI-PC edition.
Version	Version of Informatica platform.
Expiration Date	Date when the license expires.
Serial Number	Serial number of the license. The serial number identifies the customer or project. If the customer has multiple CDI-PC installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are Development and Production.
Operating System / BitMode	Operating system and bitmode for the license. Indicates whether the license is installed on a 32-bit or 64-bit operating system.
CPU	Maximum number of authorized logical CPUs.
Repository	Maximum number of authorized CDI-PC repositories.
Product Bitmode	Bitmode of the server binaries that are installed. Values are 32-bit or 64-bit.

CPU Summary

The CPU Summary section of the License Management Report shows the maximum number of logical CPUs used to run application services in the domain. Use the CPU summary information to determine if the CPU usage exceeded the license limits. If the number of logical CPUs is greater than the total number of CPUs authorized by the license, the License Management Report indicates that the CPU limit is exceeded.

The License Management Report determines the number of logical CPUs based on the number of processors, cores, and threads. Use the following formula to calculate the number of logical CPUs:

`N*C*T`, where

N is the number of processors.

C is the number of cores in each processor.

T is the number of threads in each core.

For example, a machine contains 4 processors. Each processor has 2 cores. The machine contains 8 (4*2) physical cores. Hyperthreading is enabled, where each core contains 3 threads. The number of logical CPUs is 24 (4*2*3).

Note: Although the License Management Report includes threads in the calculation of logical CPUs, Informatica license compliance is based on the number of physical cores, not threads. To be compliant, the number of physical cores must be less than or equal to the maximum number of licensed CPUs. If the License Management Report shows that you have exceeded the license limit but the number of physical cores is less than or equal to the maximum number of licensed CPUs, you can ignore the message. If you have a concern about license compliance, contact your Informatica account manager.

The following table describes the CPU summary information in the License Management Report:

Property	Description
Domain	Name of the domain on which the report runs.
Current Usage	Maximum number of logical CPUs used concurrently on the day the report runs.
Peak Usage	Maximum number of logical CPUs used concurrently during the last 12 months.
Peak Usage Date	Date when the maximum number of logical CPUs were used concurrently during the last 12 months.
Days Exceeded License Limit	Number of days that the CPU usage exceeded the license limits. The domain exceeds the CPU license limit when the number of concurrent logical CPUs exceeds the number of authorized CPUs.

CPU Detail

The CPU Detail section of the License Management Report provides CPU usage information for each host in the domain. The CPU Detail section shows the maximum number of logical CPUs used each day in a selected time period.

The report counts the number of logical CPUs on each host that runs application services in the domain. The report groups logical CPU totals by node.

The following table describes the CPU detail information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Current Usage	Maximum number of logical CPUs that the host used concurrently on the day the report runs.
Peak Usage	Maximum number of logical CPUs that the host used concurrently during the last 12 months.
Peak Usage Date	Date in the last 12 months when the host concurrently used the maximum number of logical CPUs.
Assigned Licenses	Name of all licenses assigned to services that run on the node.

Repository Summary

The Repository Summary section of the License Management Report provides repository usage information for the domain. Use the repository summary information to determine if the repository usage exceeded the license limits.

The following table describes the repository summary information in the License Management Report:

Property	Description
Current Usage	Maximum number of repositories used concurrently in the domain on the day the report runs.
Peak Usage	Maximum number of repositories used concurrently in the domain during the last 12 months.
Peak Usage Date	Date in the last 12 months when the maximum number of repositories were used concurrently.
Days Exceeded License Limit	Number of days that the repository usage exceeded the license limits.

Hardware Configuration

The Hardware Configuration section of the License Management Report provides details about machines used in the domain.

The following table describes the hardware configuration information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Logical CPUs	Number of logical CPUs used to run application services in the domain.
Sockets	Number of sockets on the machine.
Consumed cores	Number of cores on the machine.
Cores per socket	Number of cores for each socket on the machine.
CPU Model	Model of the CPU.
Hyperthreading Enabled	Indicates whether hyperthreading is enabled.
Virtual Machine	Indicates whether the machine is a virtual machine.

Node Configuration

The Node Configuration section of the License Management Report provides details about each node in the domain.

The following table describes the node configuration information in the License Management Report:

Property	Description
Node Name	Name of the node or nodes assigned to a machine for a license.
Host Name	Host name of the machine.
IP Address	IP address of the node.
Operating System	Operating system of the machine on which the node runs.
Status	Status of the node.
Gateway	Indicates whether the node is a gateway node.
Service Type	Type of the application service configured to run on the node.
Service Name	Name of the application service configured to run on the node.
Service Status	Status of the application service.
Assigned License	License assigned to the application service.

Licensed Options

The Licensed Options section of the License Management Report provides details about each option for every license assigned to the domain.

The following table describes the licensed option information in the License Management Report:

Property	Description
License Name	Name of the license.
Description	Name of the license option.
Status	Status of the license option.
Issued On	Date when the license option was issued.
Expires On	Date when the license option expires.

Running the License Management Report

Run the License Management Report from the **Reports** tab in the Administrator tool.

1. Click the **Reports** tab in the Administrator tool.
2. Click the **License Management Report** view.

   The License Management Report appears.
3. Click **Save** to save the License Management Report as a PDF.

   If a License Management Report contains multibyte characters, you must configure the Service Manager to use a Unicode font.

4. Click **Email** to send a copy of the License Management Report in an email.

   The **Send License Management Report** page appears.

Configuring a Unicode Font for the Report

Before you can save a License Management Report that contains multibyte characters or non-English characters, configure the Service Manager to use a Unicode font when generating the PDF file.

1. Install a Unicode font on the master gateway node.
2. Use a text editor to create a file named AcUtil.properties.
3. Add the following properties to the file:

   ```
   PDF.Font.Default=Unicode_font_name
   PDF.Font.MultibyteList=Unicode_font_name
   ```

   Unicode_font_name is the name of the Unicode font installed on the master gateway node.

   You might also need to add the following property if the font file is not available in the locale:

   ```
   Unicode_font_name_path=Unicode_font_file_location
   ```

   For example:

   ```
   PDF.Font.Default=Arial Unicode MS
   PDF.Font.MultibyteList=Arial Unicode MS
   Arial Unicode MS_path=/usr/lib/X11/fonts/TrueType
   ```

4. Save the AcUtil.properties file to the following location:

   ```
   InformaticaInstallationDir\services\AdministratorConsole\administrator
   ```

5. Use a text editor to open the licenseUtility.css file in the following location:

   ```
   InformaticaInstallationDir\services\AdministratorConsole\administrator\css
   ```

6. Append the Unicode font name to the value of each font-family property.

   For example:

   ```
   font-family: Arial Unicode MS, Verdana, Arial, Helvetica, sans-serif;
   ```

7. Restart Informatica services on each node in the domain.

Sending the License Management Report in an Email

You must configure the SMTP settings for the domain before you can send the License Management Report in an email.

The domain administrator can send the License Management Report in an email from Send License Management Report page in the Administrator tool.

1. Enter the following information:

Property	Description
To Email	Email address to which you send the License Management Report.
Subject	Subject of the email.
Customer Name	Name of the organization that purchased the license.

Property	Description
Request ID	Request ID that identifies the project for which the license was purchased.
Contact Name	Name of the contact person in the organization.
Contact Phone Number	Phone number of the contact person.
Contact Email	Email address of the contact person at the customer site.

2. Click OK.

   The Administrator tool sends the License Management Report in an email.

Web Services Report

To analyze the performance of web services running on a Web Services Hub, you can run a report for the Web Services Hub or for a web service running on the Web Services Hub.

The Web Services Report provides run-time and historical information on the web service requests handled by the Web Services Hub. The report displays aggregated information for all web services in the Web Services Hub and information for each web service running on the Web Services Hub. The Web Services Report also provides historical information.

Understanding the Web Services Report

You can run the Web Services Report for a time interval that you choose. The Web Services Hub collects information on web services activities and caches 24 hours of information for use in the Web Services Report. It also writes the information to a history file.

Time Interval

By default, the Web Services Report displays activity information for a five-minute interval. You can select one of the following time intervals to display activity information for a web service or Web Services Hub:

- 5 seconds
- 1 minute
- 5 minutes
- 1 hour
- 24 hours

The Web Services Report displays activity information for the interval ending at the time you run the report. For example, if you run the Web Services Report at 8:05 a.m. for an interval of one hour, the Web Services Report displays the Web Services Hub activity from 7:05 a.m. and 8:05 a.m.

Caching

The Web Services Hub caches 24 hours of activity data. The cache is reinitialized every time the Web Services Hub is restarted. The Web Services Report displays statistics from the cache for the time interval that you run the report.

History File

The Web Services Hub writes the cached activity data to a history file. The Web Services Hub stores data in the history file for the number of days that you set in the MaxStatsHistory property of the Web Services Hub. For example, if the value of the MaxStatsHistory property is 5, the Web Services Hub keeps five days of data in the history file.

Contents of the Web Services Report

The Web Services Report view contains information about the web services in the domain. When you select a web services hub in the Navigator, you can view the following information about the web services it contains:

- Properties view. Displays General Properties, Web Services Hub Summary, and Historical Statistics for the web services hub.
- Web Services view. Lists the web services in the web services hub. When you select a web service, you can view Properties, Top IP Addresses, and Historical Statistics for the web service.

General Properties and Web Services Hub Summary

To view the general properties and summary information for the Web Services Hub, select the Properties view in the content panel.

The following table describes the general properties:

Property	Description
Name	Name of the Web Services Hub.
Description	Short description of the Web Services Hub.
Service type	Type of Service. For a Web Services Hub, the service type is ServiceWSHubService.

The following table describes the Web Services Hub Summary properties:

Property	Description
# of Successful Message	Number of requests that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by web services in the Web Services Hub. The fault responses could be due to any error.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Tme	Date and time when the Web Services Hub was last started.
Avg. # of Service Partitions	Average number of partitions allocated for all web services in the Web Services Hub.
% of Partitions in Use	Percentage of web service partitions that are in use for all web services in the Web Services Hub.
Avg. # of Run Instances	Average number of instances running for all web services in the Web Services Hub.

Web Services Historical Statistics

To view historical statistics for the web services in the Web Services Hub, select the Properties view in the content panel. The detail panel displays data from the Web Services Hub history file for the date that you specify.

The following table describes the historical statistics:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed. When you click the name of a web service, the Web Services Report displays the Service Statistics window.
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of fault responses sent by the web service.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Max Service Time	The largest amount of time taken by the web service to process a request.
Min Service Time	The smallest amount of time taken by the web service to process a request.
Avg. DTM Time	Average number of seconds it takes the CDI-PC Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg Run Instances	Average number of instances running for the web service.

Web Services Run-time Statistics

To view run-time statistics for each web service in the Web Services Hub, select the Web Services view in the content panel. The Web Services view lists the statistics for each web service.

The report provides the following information for each web service for the selected time interval:

Property	Description
Service name	Name of the web service for which the information is displayed.
Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Avg. Service Time	Average time it takes to process a service request received by the web service.

Property	Description
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Avg. Run Instances	Average number of instances of the web service running during the interval.

Web Service Properties

To view the properties of a web service, select the web service in the Web Services view of the content panel. In the details panel, the Properties view displays the properties for the web service.

The report provides the following information for the selected web service:

Property	Description
# of Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Time	Date and time when the Web Services Hub was last started
Last Service Time	Number of seconds it took to process the most recent service request
Average Service Time	Average time it takes to process a service request received by the web service.
Avg.# of Service Partitions	Average number of session partitions allocated for the web service.
Avg. # of Run Instances	Average number of instances of the web service running during the interval.

Web Service Top IP Addresses

To view the top IP addresses for a web service, select a web service in the Web Services view of the content panel and select the Top IP Addresses view in the details panel. The Top IP Addresses displays the most active IP addresses for the web service, listed in the order of longest to shortest service times.

The report provides the following information for each of the most active IP addresses:

Property	Description
Top 10 Client IP Addresses	The list of client IP addresses and the longest time taken by the web service to process a request from the client. The client IP addresses are listed in the order of longest to shortest service times. Use the *Click here* link to display the list of IP addresses and service times.

Web Service Historical Statistics Table

To view a table of historical statistics for a web service, select a web service in the Web Services view of the content panel and select the Table view in the details panel. The details panel displays a table of historical statistics for the web service.

The table provides the following information for the selected web service:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed.
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of requests received for the web service that could not be processed and generated fault responses.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Min. Service Time	The smallest amount of time taken by the web service to process a request.
Max. Service Time	The largest amount of time taken by the web service to process a request.
Avg. DTM Time	Average time it takes the CDI-PC Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg. Run Instances	Average number of instances running for the web service.

Running the Web Services Report

Run the Web Services Report from the Reports tab in the Administrator tool.

Before you run the Web Services Report for a Web Services Hub, verify that the Web Services Hub is enabled. You cannot run the Web Services Report for a disabled Web Services Hub.

1. In the Administrator tool, click the Reports tab.
2. Click Web Services.
3. In the Navigator, select the Web Services Hub for which to run the report.

   In the content panel, the Properties view displays the properties of the Web Services Hub. The details view displays historical statistics for the services in the Web Services Hub.
4. To specify a date for historical statistics, click the date filter icon in the details panel, and select the date.
5. To view information about each service, select the Web Services view in the content panel.

   The Web Services view displays summary statistics for each service for the Web Services Hub.
6. To view additional information about a service, select the service from the list.

   In the details panel, the Properties view displays the properties for the service.
7. To view top IP addresses for the service, select the Top IP Addresses view in the details panel.
8. To view table attributes for the service, select the Table view in the detail panel.

Running the Web Services Report for a Secure Web Services Hub

To run a Web Services Hub on HTTPS, you must have an SSL certificate file for authentication of message transfers. When you create a Web Services Hub to run on HTTPS, you must specify the location of the keystore file that contains the certificate for the Web Services Hub. To run the Web Services Report in the Administrator tool for a secure Web Services Hub, you must import the SSL certificate into the Java certificate file. The Java certificate file is named *cacerts* and is located in the /lib/security directory of the Java directory. The Administrator tool uses the cacerts certificate file to determine whether to trust an SSL certificate.

In a domain that contains multiple nodes, the node where you generate the SSL certificate affects how you access the Web Services Report for a secure Web Services Hub.

Use the following rules and guidelines to run the Web Services Report for a secure Web Services Hub in a domain with multiple nodes:

- For each secure Web Services Hub running in a domain, generate an SSL certificate and import it to a Java certificate file.
- The Administrator tool searches for SSL certificates in the certificate file of a gateway node. The SSL certificate for a Web Services Hub running on worker node must be generated on a gateway node and imported into the certificate file of the same gateway node.
- To view the Web Services Report for a secure Web Services Hub, log in to the Administrator tool from the gateway node that has the certificate file containing the SSL certificate of the Web Services Hub for which you want to view reports.
- If a secure Web Services Hub runs on a worker node, the SSL certificate must be generated and imported into the certificate file of the gateway node. If a secure Web Services Hub runs on a gateway and a worker node, the SSL certificate of both nodes must be generated and imported into the certificate file of the gateway node. To view reports for the secure Web Services Hub, log in to the Administrator tool from the gateway node.
- If the domain has two gateway nodes and a secure Web Services Hub runs on each gateway node, access to the Web Services Reports depends on where the SSL certificate is located.

  For example, gateway node GWN01 runs Web Services Hub WSH01 and gateway node GWN02 runs Web Services Hub WSH02. You can view the reports for the Web Services Hubs based on the location of the SSL certificates:

  - If the SSL certificate for WSH01 is in the certificate file of GWN01 but not GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01. You cannot view the reports for WSH01 if you log in to the Administrator tool through GWN02. If GWN01 fails, you cannot view reports for WSH01.
  - If the SSL certificate for WSH01 is in the certificate files of GWN01 and GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01 or GWN02. If GWN01 fails, you can view the reports for WSH01 if you log in to the Administrator tool through GWN02.
- To ensure successful failover when a gateway node fails, generate and import the SSL certificates of all Web Services Hubs in the domain into the certificates files of all gateway nodes in the domain.

CHAPTER 14

Understanding Globalization

This chapter includes the following topics:

Globalization Overview

Informatica can process data in different languages. Some languages require single-byte data, while other languages require multibyte data. To process data correctly in Informatica, you must set up the following items:

- Locale. Informatica requires that the locale settings on machines that access Informatica applications are compatible with code pages in the domain. You may need to change the locale settings. The locale specifies the language, territory, encoding of character set, and collation order.
- Data movement mode. The CDI-PC Integration Service can process single-byte or multibyte data and write it to targets. Use the ASCII data movement mode to process single-byte data. Use the Unicode data movement mode for multibyte data.
- Code pages. Code pages contain the encoding to specify characters in a set of one or more languages. You select a code page based on the type of character data you want to process. To ensure accurate data movement, you must ensure compatibility among code pages for Informatica and environment components. You use code pages to distinguish between US-ASCII (7-bit ASCII), ISO 8859-1 (8-bit ASCII), and multibyte characters.

To ensure data passes accurately through your environment, the following components must work together:

- Domain configuration database code page
- Administrator tool locale settings and code page
- CDI-PC Integration Service data movement mode

- Code page for each CDI-PC Integration Service process
- CDI-PC Client code page
- CDI-PC repository code page
- Source and target database code pages

You can configure the CDI-PC Integration Service for relaxed code page validation. Relaxed validation removes restrictions on source and target code pages.

Unicode

The Unicode Standard is the work of the Unicode Consortium, an international body that promotes the interchange of data in all languages. The Unicode Standard is designed to support any language, no matter how many bytes each character in that language may require. Currently, it supports all common languages and provides limited support for other less common languages. The Unicode Consortium is continually enhancing the Unicode Standard with new character encodings. For more information about the Unicode Standard, see http://www.unicode.org.

The Unicode Standard includes multiple character sets. Informatica uses the following Unicode standards:

- UCS-2 (Universal Character Set, double-byte). A character set in which each character uses two bytes.
- UTF-8 (Unicode Transformation Format). An encoding format in which each character can use between one to four bytes.
- UTF-16 (Unicode Transformation Format). An encoding format in which each character uses two or four bytes.
- UTF-32 (Unicode Transformation Format). An encoding format in which each character uses four bytes.
- GB18030. A Unicode encoding format defined by the Chinese government in which each character can use between one to four bytes.

Informatica is a Unicode application. The CDI-PC Client and CDI-PC Integration Service use UCS-2 internally. The CDI-PC Client converts user input from any language to UCS-2 and converts it from UCS-2 before writing to the CDI-PC repository. The CDI-PC Integration Service converts source data to UCS-2 before processing and converts it from UCS-2 after processing. The CDI-PC repository, and CDI-PC Integration Service support UTF-8. You can use Informatica to process data in any language.

Working with a Unicode CDI-PC repository

The CDI-PC repository code page is the code page of the data in the CDI-PC repository. You choose the CDI-PC repository code page when you create or upgrade a CDI-PC repository. When the CDI-PC repository database code page is UTF-8, you can create a CDI-PC repository using the UTF-8 code page.

The domain configuration database uses the UTF-8 code page. If you need to store metadata in multiple languages, such as Chinese, Japanese, and Arabic, you must use the UTF-8 code page for all services in that domain.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user in the domain has characters that the code page of the application services does not recognize, characters do not convert correctly and inconsistencies occur.

Use the following guidelines when you use UTF-8 as the CDI-PC repository code page:

- The CDI-PC repository database code page must be UTF-8.
- The CDI-PC repository code page must be a superset of the CDI-PC Client and CDI-PC Integration Service process code pages.

- You can input any character in the UCS-2 character set. For example, you can store German, Chinese, and English metadata in a UTF-8 enabled CDI-PC repository.
- Install languages and fonts on the CDI-PC Client machine. If you are using a UTF-8 PCDI-PC repository, you may want to enable the CDI-PC Client machines to display multiple languages. By default, the CDI-PC Clients display text in the language set in the system locale. Use the Regional Options tool in the Control Panel to add language groups to the CDI-PC Client machines.
- You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language.
- Choose a code page for a CDI-PC Integration Service process that can process all CDI-PC repository metadata correctly. The code page of the CDI-PC Integration Service process must be a subset of the CDI-PC repository code page. If the CDI-PC Integration Service has multiple service processes, ensure that the code pages for all CDI-PC Integration Service processes are subsets of the CDI-PC repository code page. If you are running the CDI-PC Integration Service process on Windows, the code page for the CDI-PC Integration Service process must be the same as the code page for the system or user locale. If you are running the CDI-PC Integration Service process on UNIX, use the UTF-8 code page for the CDI-PC Integration Service process.

Locales

Every machine has a locale. A locale is a set of preferences related to the user environment, including the input language, keyboard layout, how data is sorted, and the format for currency and dates. Informatica uses locale settings on each machine.

You can set the following locale settings on Windows:

- System locale. Determines the language, code pages, and associated bitmap font files that are used as defaults for the system.
- User locale. Determines the default formats to display date, time, currency, and number formats.
- Input locale. Describes the input method, such as the keyboard, of the system language.

For more information about configuring the locale settings on Windows, consult the Windows documentation.

System Locale

The system locale is also referred to as the system default locale. It determines which ANSI and OEM code pages, as well as bitmap font files, are used as defaults for the system. The system locale contains the language setting, which determines the language in which text appears in the user interface, including in dialog boxes and error messages. A message catalog file defines the language in which messages display. By default, the machine uses the language specified for the system locale for all processes, unless you override the language for a specific process.

The system locale is already set on your system and you may not need to change settings to run Informatica. If you do need to configure the system locale, you configure the locale on a Windows machine in the Regional Options dialog box. On UNIX, you specify the locale in the LANG environment variable.

User Locale

The user locale displays date, time, currency, and number formats for each user. You can specify different user locales on a single machine. Create a user locale if you are working with data on a machine that is in a

different language than the operating system. For example, you might be an English user working in Hong Kong on a Chinese operating system. You can set English as the user locale to use English standards in your work in Hong Kong. When you create a new user account, the machine uses a default user locale. You can change this default setting once the account is created.

Input Locale

An input locale specifies the keyboard layout of a particular language. You can set an input locale on a Windows machine to type characters of a specific language.

You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language. For example, if you are working on an English operating system and need to enter text in Chinese, you can use IME to set the input locale to Chinese without having to install the Chinese version of Windows. You might want to use an input method editor to enter multibyte characters into a CDI-PC repository that uses UTF-8.

Data Movement Modes

The data movement mode is a CDI-PC Integration Service option you choose based on the type of data you want to move, single-byte or multibyte data. The data movement mode you select depends the following factors:

- Requirements to store single-byte or multibyte metadata in the CDI-PC repository
- Requirements to access source data containing single-byte or multibyte character data
- Future needs for single-byte and multibyte data

The data movement mode affects how the CDI-PC Integration Service enforces session code page relationships and code page validation. It can also affect performance. Applications can process single-byte characters faster than multibyte characters.

Character Data Movement Modes

The CDI-PC Integration Service runs in the following modes:

- ASCII (American Standard Code for Information Interchange). The US-ASCII code page contains a set of 7-bit ASCII characters and is a subset of other character sets. When the CDI-PC Integration Service runs in ASCII data movement mode, each character requires one byte.
- Unicode. The universal character-encoding standard that supports all languages. When the CDI-PC Integration Service runs in Unicode data movement mode, it allots up to two bytes for each character. Run the CDI-PC Integration Service in Unicode mode when the source contains multibyte data.

  Tip: You can also use ASCII or Unicode data movement mode if the source has 8-bit ASCII data. The CDI-PC Integration Service allots an extra byte when processing data in Unicode data movement mode. To increase performance, use the ASCII data movement mode. For example, if the source contains characters from the ISO 8859-1 code page, use the ASCII data movement.

The data movement you choose affects the requirements for code pages. Ensure the code pages are compatible.

ASCII Data Movement Mode

In ASCII mode, the CDI-PC Integration Service processes single-byte characters and does not perform code page conversions. When you run the CDI-PC Integration Servicein ASCII mode, it does not enforce session code page relationships.

Unicode Data Movement Mode

In Unicode mode, the CDI-PC Integration Service recognizes multibyte character data and allocates up to two bytes for every character. The CDI-PC Integration Service performs code page conversions from sources to targets. When you set the CDI-PC Integration Service to Unicode data movement mode, it uses a Unicode character set to process characters in a specified code page, such as Shift-JIS or UTF-8.

When you run the CDI-PC Integration Service in Unicode mode, it enforces session code page relationships.

Changing Data Movement Modes

You can change the data movement mode in the CDI-PC Integration Service properties in the Administrator tool. After you change the data movement mode, the CDI-PC Integration Service runs in the new data movement mode the next time you start the CDI-PC Integration Service. When the data movement mode changes, the CDI-PC Integration Service handles character data differently. To avoid creating data inconsistencies in your target tables, the CDI-PC Integration Service performs additional checks for sessions that reuse session caches and files.

The following table describes how the CDI-PC Integration Service handles session files and caches after you change the data movement mode:

Session File or Cache	Time of Creation or Use	CDI-PC Integration Service Behavior After Data Movement Mode Change
Session Log File (*.log)	Each session.	No change in behavior. Creates a new session log for each session using the code page of the CDI-PC Integration Service process.
Workflow Log	Each workflow.	No change in behavior. Creates a new workflow log file for each workflow using the code page of the CDI-PC Integration Service process.
Reject File (*.bad)	Each session.	No change in behavior. Appends rejected data to the existing reject file using the code page of the CDI-PC Integration Service process.
Output File (*.out)	Sessions writing to flat file.	No change in behavior. Creates a new output file for each session using the target code page.
Indicator File (*.in)	Sessions writing to flat file.	No change in behavior. Creates a new indicator file for each session.
Incremental Aggregation Files (*.idx, *.dat)	Sessions with Incremental Aggregation enabled.	When files are removed or deleted, the CDI-PC Integration Service creates new files. When files are not moved or deleted, the CDI-PC Integration Service fails the session with the following error message: `SM_7038 Aggregate Error: ServerMode: [server data movement mode] and CachedMode: [data movement mode that created the files] mismatch.` Move or delete files created using a different code page.

Session File or Cache	Time of Creation or Use	CDI-PC Integration Service Behavior After Data Movement Mode Change
Unnamed Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for an unnamed persistent lookup cache.	Rebuilds the persistent lookup cache.
Named Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for a named persistent lookup cache.	When files are removed or deleted, the CDI-PC Integration Service creates new files. When files are not moved or deleted, the CDI-PC Integration Service fails the session. Move or delete files created using a different code page.

Code Page Overview

A code page contains the encoding to specify characters in a set of one or more languages. An encoding is the assignment of a number to a character in the character set. You use code pages to identify data that might be in different languages. For example, if you create a mapping to process Japanese data, you must select a Japanese code page for the source data.

When you choose a code page, the program or application for which you set the code page refers to a specific set of data that describes the characters the application recognizes. This influences the way that application stores, receives, and sends character data.

Most machines use one of the following code pages:

- US-ASCII (7-bit ASCII)
- MS Latin1 (MS 1252) for Windows operating systems
- Latin1 (ISO 8859-1) for UNIX operating systems
- IBM EBCDIC US English (IBM037) for mainframe systems

The US-ASCII code page contains all 7-bit ASCII characters and is the most basic of all code pages with support for United States English. The US-ASCII code page is not compatible with any other code page. When you install either the CDI-PC Client, CDI-PC Integration Service, or CDI-PC repository on a US-ASCII system, you must install all components on US-ASCII systems and run the CDI-PC Integration Service in ASCII mode.

MS Latin1 and Latin1 both support English and most Western European languages and are compatible with each other. When you install the CDI-PC Client, CDI-PC Integration Service, or CDI-PC repository on a system using one of these code pages, you can install the rest of the components on any machine using the MS Latin1 or Latin1 code pages.

You can use the IBM EBCDIC code page for the CDI-PC Integration Service process when you install it on a mainframe system. You cannot install the CDI-PC Client or CDI-PC repository on mainframe systems, so you cannot use the IBM EBCDIC code page for CDI-PC Client or CDI-PC repository installations.

UNIX Code Pages

In the United States, most UNIX operating systems have more than one code page installed and use the ASCII code page by default. If you want to run CDI-PC in an ASCII-only environment, you can use the ASCII code page and run the CDI-PC Integration Service in ASCII mode.

UNIX systems allow you to change the code page by changing the LANG, LC_CTYPE or LC_ALL environment variable. For example, you want to change the code page an AIX machine uses. Use the following command in the C shell to view your environment:

```
locale
```

This results in the following output, in which “C” implies “ASCII”:

```
LANG="C"
LC_CTYPE="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_ALL="C"
```

To change the language to English and require the system to use the Latin1 code page, you can use the following command:

```
setenv LANG en_US.iso88591
```

When you check the locale again, it has been changed to use Latin1 (ISO 8859-1):

```
LANG="en_US.iso88591"
LC_CTYPE="en_US.iso88591"
LC_NUMERIC="en_US.iso88591"
LC_TIME="en_US.iso88591"
LC_ALL="en_US.iso88591"
```

For more information about changing the locale or code page of a UNIX system, see the UNIX documentation.

Choosing a Code Page

Choose code pages based on the character data you use in mappings. Character data can be represented by character modes based on the character size. Character size is the storage space a character requires in the database. Different character sizes can be defined as follows:

- Single-byte. A character represented as a unique number between 0 and 255. One byte is eight bits. ASCII characters are single-byte characters.
- Double-byte. A character two bytes or 16 bits in size represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have double-byte characters.
- Multibyte. A character two or more bytes in size is represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have multibyte characters.

Code Page Compatibility

Compatibility between code pages is essential for accurate data movement when the CDI-PC Integration Service runs in the Unicode data movement mode.

A code page can be compatible with another code page, or it can be a subset or a superset of another:

- Compatible. Two code pages are compatible when the characters encoded in the two code pages are virtually identical. For example, JapanEUC and JIPSE code pages contain identical characters and are compatible with each other. The CDI-PC repository and CDI-PC Integration Service process can each use one of these code pages and can pass data back and forth without data loss.
- Superset. A code page is a superset of another code page when it contains all the characters encoded in the other code page and additional characters not encoded in the other code page. For example, MS Latin1 is a superset of US-ASCII because it contains all characters in the US-ASCII code page.

Note: Informatica considers a code page to be a superset of itself and all other compatible code pages.

- Subset. A code page is a subset of another code page when all characters in the code page are also encoded in the other code page. For example, US-ASCII is a subset of MS Latin1 because all characters in the US-ASCII code page are also encoded in the MS Latin1 code page.

For accurate data movement, the target code page must be a superset of the source code page. If the target code page is not a superset of the source code page, the CDI-PC Integration Service may not process all characters, resulting in incorrect or missing data. For example, Latin1 is a superset of US-ASCII. If you select Latin1 as the source code page and US-ASCII as the target code page, you might lose character data if the source contains characters that are not included in US-ASCII.

When you install or upgrade a CDI-PC Integration Service to run in Unicode mode, you must ensure code page compatibility among the domain configuration database, the Administrator tool, CDI-PC Client, CDI-PC Integration Service process nodes, the CDI-PC repository and the machines hosting *pmrep* and *pmcmd*. In Unicode mode, the CDI-PC Integration Service enforces code page compatibility between the CDI-PC Client and the CDI-PC repository, and between the CDI-PC Integration Service process and the CDI-PC repository. In addition, when you run the CDI-PC Integration Service in Unicode mode, code pages associated with sessions must have the appropriate relationships:

- For each source in the session, the source code page must be a subset of the target code page. The CDI-PC Integration Service does not require code page compatibility between the source and the CDI-PC Integration Service process or between the CDI-PC Integration Service process and the target.
- If the session contains a Lookup or Stored Procedure transformation, the database or file code page must be a subset of the target that receives data from the Lookup or Stored Procedure transformation and a superset of the source that provides data to the Lookup or Stored Procedure transformation.
- If the session contains an External Procedure or Custom transformation, the procedure must pass data in a code page that is a subset of the target code page for targets that receive data from the External Procedure or Custom transformation.

Informatica uses code pages for the following components:

- Domain configuration database. The domain configuration database must be compatible with the code pages of the CDI-PC repository.
- Administrator tool. You can enter data in any language in the Administrator tool.
- CDI-PC Client. You can enter metadata in any language in the CDI-PC Client.
- CDI-PC Integration Service process. The CDI-PC Integration Service can move data in ASCII mode and Unicode mode. The default data movement mode is ASCII, which passes 7-bit ASCII or 8-bit ASCII character data. To pass multibyte character data from sources to targets, use the Unicode data movement mode. When you run the CDI-PC Integration Service in Unicode mode, it uses up to three bytes for each character to move data and performs additional checks at the session level to ensure data integrity.
- CDI-PC repository. The CDI-PC repository can store data in any language. You can use the UTF-8 code page for the CDI-PC repository to store multibyte data in the CDI-PC repository. The code page for the CDI-PC repository is the same as the database code page.
- Sources and targets. The sources and targets store data in one or more languages. You use code pages to specify the type of characters in the sources and targets.
- CDI-PC command line programs. You must also ensure that the code page for *pmrep* is a subset of the CDI-PC repository code page and the code page for *pmcmd* is a subset of the CDI-PC Integration Service process code page.

Most database servers use two code pages, a client code page to receive data from client applications and a server code page to store the data. When the database server is running, it converts data between the two code pages if they are different. In this type of database configuration, the CDI-PC Integration Service

process interacts with the database client code page. Thus, code pages used by the CDI-PC Integration Service process, such as the CDI-PC repository, source, or target code pages, must be identical to the database client code page. The database client code page is usually identical to the operating system code page on which the CDI-PC Integration Service process runs. The database client code page is a subset of the database server code page.

For more information about specific database client and server code pages, see your database documentation.

Domain Configuration Database Code Page

The domain configuration database must be compatible with the code pages of the CDI-PC repository.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user name in the domain has characters that the code page of the application service does not recognize, characters do not convert correctly and inconsistencies occur.

Administrator Tool Code Page

The Administrator tool can run on any node in a Informatica domain. The Administrator tool code page is the code page of the operating system of the node. Each node in the domain must use the same code page.

The Administrator tool code page must be:

- A subset of the CDI-PC repository code page

CDI-PC Client Code Page

The CDI-PC Client code page is the code page of the operating system of the CDI-PC Client. To communicate with the CDI-PC repository, the CDI-PC Client code page must be a subset of the CDI-PC repository code page.

CDI-PC Integration Service Process Code Page

The code page of a CDI-PC Integration Service process is the code page of the node that runs the CDI-PC Integration Service process. Define the code page for each CDI-PC Integration Service process in the Administrator tool on the Processes tab.

However, on UNIX, you can change the code page of the CDI-PC Integration Service process by changing the LANG, LC_CTYPE or LC_ALL environment variable for the user that starts the process.

The code page of the CDI-PC Integration Service process must be:

- A subset of the CDI-PC repository code page
- A superset of the machine hosting *pmcmd* or a superset of the code page specified in the INFA_CODEPAGENAME environment variable

The code pages of all CDI-PC Integration Service processes must be compatible with each other. For example, you can use MS Windows Latin1 for a node on Windows and ISO-8859-1 for a node on UNIX.

CDI-PC Integration Services configured for Unicode mode validate code pages when you start a session to ensure accurate data movement. It uses session code pages to convert character data. When the CDI-PC Integration Service runs in ASCII mode, it does not validate session code pages. It reads all character data as ASCII characters and does not perform code page conversions.

Each code page has associated sort orders. When you configure a session, you can select one of the sort orders associated with the code page of the CDI-PC Integration Service process. When you run the CDI-PC

Integration Service in Unicode mode, it uses the selected session sort order to sort character data. When you run the CDI-PC Integration Service in ASCII mode, it sorts all character data using a binary sort order.

If you run the CDI-PC Integration Service in the United States on Windows, consider using MS Windows Latin1 (ANSI) as the code page of the CDI-PC Integration Service process.

If you run the CDI-PC Integration Service in the United States on UNIX, consider using ISO 8859-1 as the code page for the CDI-PC Integration Service process.

If you use *pmcmd* to communicate with the CDI-PC Integration Service, the code page of the operating system hosting *pmcmd* must be identical to the code page of the CDI-PC Integration Service process.

The CDI-PC Integration Service generates the names of session log files, reject files, caches and cache files, and performance detail files based on the code page of the CDI-PC Integration Service process.

CDI-PC repository Code Page

The CDI-PC repository code page is the code page of the data in the repository. The CDI-PC Repository Service uses the CDI-PC repository code page to save metadata in and retrieve metadata from the CDI-PC repository database. Choose the CDI-PC repository code page when you create or upgrade a CDI-PC repository. When the CDI-PC repository database code page is UTF-8, you can create a CDI-PC repository using UTF-8 as its code page.

The CDI-PC repository code page must be:

- Compatible with the domain configuration database code page
- A superset of the Administrator tool code page
- A superset of the CDI-PC Client code page
- A superset of the code page for the CDI-PC Integration Service process
- A superset of the machine hosting *pmrep* or a superset of the code page specified in the INFA_CODEPAGENAME environment variable

A global CDI-PC repository code page must be a subset of the localCDI-PC repository code page if you want to create shortcuts in the local CDI-PC repository that reference an object in a global CDI-PC repository.

If you copy objects from one CDI-PC repository to another CDI-PC repository, the code page for the target CDI-PC repository must be a superset of the code page for the source CDI-PC repository.

CDI-PC Source Code Page

The source code page depends on the type of source:

- Flat files and VSAM files. The code page of the data in the file. When you configure the flat file or COBOL source definition, choose a code page that matches the code page of the data in the file.
- XML files. The CDI-PC Integration Service converts XML to Unicode when it parses an XML source. When you create an XML source definition, the CDI-PC Designer assigns a default code page. You cannot change the code page.
- Relational databases. The code page of the database client. When you configure the relational connection in the CDI-PC Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is identical to the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang, data may become inconsistent, or you might receive a database error, such as:

```
ORA-00911: Invalid character specified.
```

Regardless of the type of source, the source code page must be a subset of the code page of transformations and targets that receive data from the source. The source code page does not need to be a subset of transformations or targets that do not receive data from the source.

Note: Select IBM EBCDIC as the source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

CDI-PC Target Code Page

The target code page depends on the type of target:

- Flat files. When you configure the flat file target definition, choose a code page that matches the code page of the data in the flat file.
- XML files. Configure the XML target code page after you create the XML target definition. The XML Wizard assigns a default code page to the XML target. The CDI-PC Designer does not apply the code page that appears in the XML schema.
- Relational databases. When you configure the relational connection in the CDI-PC Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is compatible with the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang or you might receive a database error, such as:

  ```
  ORA-00911: Invalid character specified.
  ```

The target code page must be a superset of the code page of transformations and sources that provide data to the target. The target code page does not need to be a superset of transformations or sources that do not provide data to the target.

The CDI-PC Integration Service creates session indicator files, session output files, and external loader control and data files using the target flat file code page.

Note: Select IBM EBCDIC as the target database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

Command Line Program Code Pages

The *pmcmd* and *pmrep* command line programs require code page compatibility. *pmcmd* and *pmrep* use code pages when sending commands in Unicode. Other command line programs do not require code pages.

The code page compatibility for *pmcmd* and *pmrep* depends on whether you configured the code page environment variable INFA_CODEPAGENAME for *pmcmd* or *pmrep*. You can set this variable for either command line program or for both.

If you did not set this variable for a command line program, ensure the following requirements are met:

- If you did not set the variable for *pmcmd*, then the code page of the machine hosting *pmcmd* must be a subset of the code page for the CDI-PC Integration Service process.
- If you did not set the variable for *pmrep*, then the code page of the machine hosting *pmrep* must be a subset of the CDI-PC repository code page.

If you set the code page environment variable INFA_CODEPAGENAME for *pmcmd* or *pmrep*, ensure the following requirements are met:

- If you set INFA_CODEPAGENAME for *pmcmd,* the code page defined for the variable must be a subset of the code page for the CDI-PC Integration Service process.

- If you set INFA_CODEPAGENAME for *pmrep*, the code page defined for the variable must be a subset of the CDI-PC repository code page.
- If you run *pmcmd and pmrep* from the same machine and you set the INFA_CODEPAGENAME variable, the code page defined for the variable must be subsets of the code pages for the CDI-PC Integration Service process and the CDI-PC repository.

If the code pages are not compatible, the CDI-PC Integration Service process may not fetch the workflow, session, or task from the CDI-PC repository.

Code Page Validation

The machines hosting the CDI-PC Client, CDI-PC Integration Service process, and CDI-PC repository database must use appropriate code pages. This eliminates the risk of data or repository inconsistencies. When the CDI-PC Integration Service runs in Unicode data movement mode, it enforces session code page relationships. When the CDI-PC Integration Service runs in ASCII mode, it does not enforce session code page relationships.

To ensure compatibility, the CDI-PC Client and CDI-PC Integration Service perform the following code page validations:

- CDI-PC restricts the use of EBCDIC-based code pages for repositories. Since you cannot install the CDI-PC Client or CDI-PC repository on mainframe systems, you cannot select EBCDIC-based code pages, like IBM EBCDIC, as the CDI-PC repository code page.
- CDI-PC Client can connect to the CDI-PC repository when its code page is a subset of the CDI-PC repository code page. If the CDI-PC Client code page is not a subset of the CDI-PC repository code page, the CDI-PC Client fails to connect to the CDI-PC repository code page with the following error:

  ```
  REP_61082 <CDI-PC Client>'s code page <CDI-PC Client code page> is not one-way
  compatible to repository <CDI-PC repository name>'s code page <CDI-PC repository code
  page>.
  ```

- After you set the CDI-PC repository code page, you cannot change it. After you create or upgrade a CDI-PC repository, you cannot change the CDI-PC repository code page. This prevents data loss and inconsistencies in the CDI-PC repository.
- The CDI-PC Integration Service process can start if its code page is a subset of the CDI-PC repository code page. The code page of the CDI-PC Integration Service process must be a subset of the CDI-PC repository code page to prevent data loss or inconsistencies. If it is not a subset of the CDI-PC repository code page, the CDI-PC Integration Service writes the following message to the log files:

  ```
  REP_61082 <CDI-PC Integration Service>'s code page <CDI-PC Integration Service code
  page> is not one-way compatible to repository <CDI-PC repository name>'s code page
  <CDI-PC repository code page>.
  ```

- When in Unicode data movement mode, the CDI-PC Integration Service starts workflows with the appropriate source and target code page relationships for each session. When the CDI-PC Integration Service runs in Unicode mode, the code page for every source in a session must be a subset of the target code page. This prevents data loss during a session.

  If the source and target code pages do not have the appropriate relationships with each other, the CDI-PC Integration Service fails the session and writes the following message to the session log:

  ```
  TM_6227 Error: Code page incompatible in session <session name>. <Additional details>.
  ```

- The CDI-PC Workflow Manager validates source, target, lookup, and stored procedure code page relationships for each session. The CDI-PC Workflow Manager checks code page relationships when you save a session, regardless of the CDI-PC Integration Service data movement mode. If you configure a

session with invalid source, target, lookup, or stored procedure code page relationships, the CDI-PC Workflow Manager issues a warning similar to the following when you save the session:

```
CMN_1933 Code page <code page name> for data from file or connection associated with
transformation <name of source, target, or transformation> needs to be one-way
compatible with code page <code page name> for transformation <source or target or
transformation name>.
```

If you want to run the session in ASCII mode, you can save the session as configured. If you want to run the session in Unicode mode, edit the session to use appropriate code pages.

Relaxed Code Page Validation

Your environment may require you to process data from different sources using character sets from different languages. For example, you may need to process data from English and Japanese sources using the same CDI-PC repository, or you may want to extract source data encoded in a Unicode encoding such as UTF-8. You can configure the CDI-PC Integration Service for relaxed code page validation. Relaxed code page validation enables you to process data using sources and targets with incompatible code pages.

Although relaxed code page validation removes source and target code page restrictions, it still enforces code page compatibility between the CDI-PC Integration Service and CDI-PC repository.

Note: Relaxed code page validation does not safeguard against possible data inconsistencies when you move data between incompatible code pages. You must verify that the characters the CDI-PC Integration Service reads from the source are included in the target code page.

Informatica removes the following restrictions when you relax code page validation:

- Source and target code pages. You can use any code page supported by Informatica for your source and target data.
- Session sort order. You can use any sort order supported by Informatica when you configure a session.

When you run a session with relaxed code page validation, the CDI-PC Integration Service writes the following message to the session log:

```
TM_6185 WARNING! Data code page validation is disabled in this session.
```

When you relax code page validation, the CDI-PC Integration Service writes descriptions of the database connection code pages to the session log.

The following text shows sample code page messages in the session log:

```
TM_6187 Repository code page: [MS Windows Latin 1 (ANSI), superset of Latin 1]
WRT_8222 Target file [$PMTargetFileDir\passthru.out] code page: [MS Windows Traditional
Chinese, superset of Big 5]
WRT_8221 Target database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
TM_6189 Source database connection [Japanese Oracle] code page: [MS Windows Japanese,
superset of Shift-JIS]
CMN_1716 Lookup [LKP_sjis_lookup] uses database connection [Japanese Oracle] in code
page [MS Windows Japanese, superset of Shift-JIS]
CMN_1717 Stored procedure [J_SP_INCREMENT] uses database connection [Japanese Oracle] in
code page [MS Windows Japanese, superset of Shift-JIS]
```

If the CDI-PC Integration Service cannot correctly convert data, it writes an error message to the session log.

Configuring the CDI-PC Integration Service

To configure the CDI-PC Integration Service for code page relaxation, complete the following tasks in the Administrator tool:

- Disable code page validation. Disable the ValidateDataCodePages option in the CDI-PC Integration Service properties.
- Configure the CDI-PC Integration Service for Unicode data movement mode. Select Unicode for the Data Movement Mode option in the CDI-PC Integration Service properties.
- Configure the CDI-PC Integration Service to write to the logs using the UTF-8 character set. If you configure sessions or workflows to write to log files, enable the LogsInUTF8 option in the CDI-PC Integration Service properties. The CDI-PC Integration Service writes all logs in UTF-8 when you enable the LogsInUTF8 option. The CDI-PC Integration Service writes to the Log Manager in UTF-8 by default.

Selecting Compatible Source and Target Code Pages

Although CDI-PC allows you to use any supported code page, there are risks associated with using incompatible code pages for sources and targets. If your target code page is not a superset of your source code page, you risk inconsistencies in the target data because the source data may contain characters not encoded in the target code page.

When the CDI-PC Integration Service reads characters that are not included in the target code page, you risk transformation errors, inconsistent data, or failed sessions.

Note: If you relax code page validation, it is your responsibility to ensure that data converts from the source to target properly.

Troubleshooting for Code Page Relaxation

The CDI-PC Integration Service failed a session and wrote the following message to the session log:

```
TM_6188 The specified sort order is incompatible with the CDI-PC Integration Service
code page.
```

If you want to validate code pages, select a sort order compatible with the CDI-PC Integration Service code page. If you want to relax code page validation, configure the CDI-PC Integration Service to relax code page validation in Unicode data movement mode.

I tried to view the session or workflow log, but it contains garbage characters.

The CDI-PC Integration Service is not configured to write session or workflow logs using the UTF-8 character set.

Enable the LogsInUTF8 option in the CDI-PC Integration Service properties.

CDI-PC Code Page Conversion

When in data movement mode is set to Unicode, the CDI-PC Client accepts input in any language and converts it to UCS-2. The CDI-PC Integration Service converts source data to UCS-2 before processing and converts the processed data from UCS-2 to the target code page before loading.

When you run a session, the CDI-PC Integration Service converts source, target, and lookup queries from the CDI-PC repository code page to the source, target, or lookup code page. The CDI-PC Integration Service also converts the name and call text of stored procedures from the CDI-PC repository code page to the stored procedure database code page.

At run time, the CDI-PC Integration Service verifies that it can convert the following queries and procedure text from the CDI-PC repository code page without data loss:

- Source query. Must convert to source database code page.
- Lookup query. Must convert to lookup database code page.
- Target SQL query. Must convert to target database code page.
- Name and call text of stored procedures. Must convert to stored procedure database code page.

Choosing Characters for CDI-PC repository Metadata

You can use any character in the CDI-PC repository code page when inputting CDI-PC repository metadata. If the CDI-PC repository uses UTF-8, you can input any Unicode character. For example, you can store German, Japanese, and English metadata in a UTF-8 enabled CDI-PC repository. However, you must ensure that the CDI-PC Integration Service can successfully perform SQL transactions with source, target, lookup, and stored procedure databases. You must also ensure that the CDI-PC Integration Service can read from source and lookup files and write to target and lookup files. Therefore, when you run a session, you must ensure that the CDI-PC repository metadata characters are encoded in the source, target, lookup, and stored procedure code pages.

Example

The CDI-PC Integration Service, CDI-PC repository, and CDI-PC Client use the ISO 8859-1 Latin1 code page, and the source database contains Japanese data encoded using the Shift-JIS code page. Each code page contains characters not encoded in the other. Using characters other than 7-bit ASCII for the CDI-PC repository and source database metadata can cause the sessions to fail or load no rows to the target in the following situations:

- You create a mapping that contains a string literal with characters specific to the German language range of ISO 8859-1 in a query. The source database may reject the query or return inconsistent results.
- You use the CDI-PC Client to generate SQL queries containing characters specific to the German language range of ISO 8859-1. The source database cannot convert the German-specific characters from the ISO 8859-1 code page into the Shift-JIS code page.
- The source database has a table name that contains Japanese characters. The CDI-PC Designer cannot convert the Japanese characters from the source database code page to the CDI-PC Client code page. Instead, the CDI-PC Designer imports the Japanese characters as question marks (?), changing the name of the table. The CDI-PC Repository Service saves the source table name in the CDI-PC repository as question marks. If the CDI-PC Integration Service sends a query to the source database using the changed table name, the source database cannot find the correct table, and returns no rows or an error to the CDI-PC Integration Service, causing the session to fail.

Because the US-ASCII code page is a subset of both the ISO 8859-1 and Shift-JIS code pages, you can avoid these data inconsistencies if you use 7-bit ASCII characters for all of your metadata.

Case Study: Processing ISO 8859-1 Data

This case study describes how you might set up an environment to process ISO 8859-1 multibyte data. You might want to configure your environment this way if you need to process data from different Western European languages with character sets contained in the ISO 8859-1 code page. This example describes an environment that processes English and German language data.

For this case study, the ISO 8859-1 environment consists of the following elements:

- The CDI-PC Integration Service on a UNIX system
- CDI-PC Client on a Windows system, purchased in the United States
- The CDI-PC repository stored on an Oracle database on UNIX
- A source database containing English language data
- Another source database containing German and English language data
- A target database containing German and English language data
- A lookup database containing English language data

  The data environment must process English and German character data.

Configuring the ISO 8859-1 Environment

Use the following guidelines when you configure an environment similar to this case study for ISO 8859-1 data processing:

1. Verify code page compatibility between the CDI-PC repository database client and the database server.
2. Verify code page compatibility between the CDI-PC Client and the CDI-PC repository, and between the CDI-PC Integration Service process and the CDI-PC repository.
3. Set the CDI-PC Integration Service data movement mode to ASCII.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify CDI-PC repository Database Client and Server Compatibility

The database client and server hosting the CDI-PC repository must be able to communicate without data loss.

The CDI-PC repository resides in an Oracle database. Use NLS_LANG to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures NLS_LANG for the U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write ISO 8859-1 data to the CDI-PC repository using the Oracle WE8ISO8859P1 code page. For example:

```
NLS_LANG = AMERICAN_AMERICA.WE8ISO8859P1
```

For more information about verifying and changing the CDI-PC repository database code page, see your database documentation.

Step 2. Verify CDI-PC Code Page Compatibility

The CDI-PC Integration Service and CDI-PC Client code pages must be subsets of the CDI-PC repository code page. Because the CDI-PC Client and CDI-PC Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the CDI-PC repository code page.

In this case, the CDI-PC Client on Windows systems were purchased in the United States. Thus the system code pages for the CDI-PC Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel. For systems purchased in the United States, the Regional Settings and Input Locale must be configured for English (United States).

The CDI-PC Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, change the UNIX system code page to ISO 8859-1 Western European so that it is a subset of the CDI-PC repository code page.

Step 3. Configure the CDI-PC Integration Service for ASCII Data Movement Mode

Configure the CDI-PC Integration Service to process ISO 8859-1 data. In the Administrator tool, set the Data Movement Mode to ASCII for the CDI-PC Integration Service.

Step 4. Verify Session Code Page Compatibility

When you run a workflow in ASCII data movement mode, the CDI-PC Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains source databases containing German and English data. When you configure a source database connection in the CDI-PC Workflow Manager, the code page for the connection must be identical to the source database code page and must be a subset of the target code page. Since both the MS Windows Latin1 and the ISO 8859-1 Western European code pages contain German characters, you would most likely use one of these code pages for source database connections.

Because the target code page must be a superset of the source code page, use either MS Windows Latin1, ISO 8859-1 Western European, or UTF-8 for target database connection or flat file code pages. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the CDI-PC Integration Service for relaxed code page validation, the CDI-PC Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages. In this case, all data processed by the External Procedure or Custom transformations must be in the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 7. Configure Session Sort Order

When you run the CDI-PC Integration Service in ASCII mode, it uses a binary sort order for all sessions. In the session properties, the CDI-PC Workflow Manager lists all sort orders associated with the CDI-PC Integration Service code page. You can select a sort order for the session.

Case Study: Processing Unicode UTF-8 Data

This case study describes how you might set up an environment that processes Unicode UTF-8 multibyte data. You might want to configure your environment this way if you need to process data from Western European, Middle Eastern, Asian, or any other language with characters encoded in the UTF-8 character set. This example describes an environment that processes German and Japanese language data.

For this case study, the UTF-8 environment consists of the following elements:

- The CDI-PC Integration Service on a UNIX machine
- The CDI-PC Client on Windows systems
- The CDI-PC repository stored on an Oracle database on UNIX
- A source database contains German language data
- A source database contains German and Japanese language data
- A target database contains German and Japanese language data
- A lookup database contains German language data

  The data environment must process German and Japanese character data.

Configuring the UTF-8 Environment

Use the following guidelines when you configure an environment similar to this case study for UTF-8 data processing:

1. Verify code page compatibility between the CDI-PC repository database client and the database server.
2. Verify code page compatibility between the CDI-PC Client and the CDI-PC repository, and between the CDI-PC Integration Service and the CDI-PC repository.
3. Configure the CDI-PC Integration Service for Unicode data movement mode.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify CDI-PC repository Database Client and Server Code Page Compatibility

The database client and server hosting the CDI-PC repository must be able to communicate without data loss.

The CDI-PC repository resides in an Oracle database. With Oracle, you can use NLS_LANG to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures NLS_LANG for U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write UTF-8 data to the CDI-PC repository using the Oracle UTF8 character set. For example:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

For more information about verifying and changing the CDI-PC repository database code page, see your database documentation.

Step 2. Verify CDI-PC Code Page Compatibility

The CDI-PC Integration Service and CDI-PC Client code pages must be subsets of the CDI-PC repository code page. Because the CDI-PC Client and CDI-PC Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the CDI-PC repository code page.

In this case, the CDI-PC Client on Windows systems were purchased in Switzerland. Thus, the system code pages for the CDI-PC Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel.

The CDI-PC Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, the UNIX system character set must be changed to UTF-8.

Step 3. Configure the CDI-PC Integration Service for Unicode Data Movement Mode

You must configure the CDI-PC Integration Service to process UTF-8 data. In the Administrator tool, set the Data Movement Mode to Unicode for the CDI-PC Integration Service. The CDI-PC Integration Service allots an extra byte for each character when processing multibyte data.

Step 4. Verify Session Code Page Compatibility

When you run a CDI-PC workflow in Unicode data movement mode, the CDI-PC Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains a source database containing German and Japanese data. When you configure a source database connection in the CDI-PC Workflow Manager, the code page for the connection must be identical to the source database code page. You can use any code page for the source database.

Because the target code page must be a superset of the source code pages, you must use UTF-8 for the target database connections or flat files. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the CDI-PC Integration Service for relaxed code page validation, the CDI-PC Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with UTF-8.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages.

In this case, the External Procedure or Custom transformations must be able to process the German and Japanese data from the sources. However, the CDI-PC Integration Service passes data to procedures in UCS-2. Therefore, all data processed by the External Procedure or Custom transformations must be in the UCS-2 character set.

Step 7. Configure Session Sort Order

When you run the CDI-PC Integration Service in Unicode mode, it sorts session data using the sort order configured for the session. By default, sessions are configured for a binary sort order.

To sort German and Japanese data when the CDI-PC Integration Service uses UTF-8, you most likely want to use the default binary sort order.

APPENDIX A

Code Pages

This appendix includes the following topics:

Supported Code Pages for Application Services

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see http://demo.icu-project.org/icu-bin/convexp.

When you assign an application service code page in the Administrator tool, you select the code page description.

The following table lists the name, description, and ID for supported code pages for the CDI-PC Repository Service and for each CDI-PC Integration Service process:

Name	Description	ID
IBM037	IBM EBCDIC US English	2028
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM273	IBM EBCDIC German	2030
IBM280	IBM EBCDIC Italian	2035
IBM285	IBM EBCDIC UK English	2038
IBM297	IBM EBCDIC French	2040
IBM500	IBM EBCDIC International Latin-1	2044
IBM930	IBM EBCDIC Japanese	930
IBM935	IBM EBCDIC Simplified Chinese	935
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939

Name	Description	ID
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
Latin1	ISO 8859-1 Western European	4
MS1250	MS Windows Latin 2 (Central Europe)	2250
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950

Name	Description	ID
US-ASCII	7-bit ASCII	1
UTF-8	UTF-8 encoding of Unicode	106

Supported Code Pages for Sources and Targets

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see http://demo.icu-project.org/icu-bin/convexp.

When you assign a source or target code page in the CDI-PC Client, you select the code page description. When you assign a code page using the *pmrep* CreateConnection command or define a code page in a parameter file, you enter the code page name. The following table lists the name, description, and ID for supported code pages for sources and targets:

Name	Description	ID
Adobe-Standard-Encoding	Adobe Standard Encoding	10073
BOCU-1	Binary Ordered Compression for Unicode (BOCU-1)	10010
CESU-8	ICompatibility Encoding Scheme for UTF-16 (CESU-8)	10011
cp1006	ISO Urdu	10075
cp1098	PC Farsi	10076
cp1124	ISO Cyrillic Ukraine	10077
cp1125	PC Cyrillic Ukraine	10078
cp1131	PC Cyrillic Belarus	10080
cp1381	PC Chinese GB (S-Ch Data mixed)	10082
cp850	PC Latin1	10036
cp851	PC DOS Greek (without euro)	10037
cp856	PC Hebrew (old)	10040
cp857	PC Latin5 (without euro update)	10041
cp858	PC Latin1 (with euro update)	10042
cp860	PC Portugal	10043
cp861	PC Iceland	10044

Name	Description	ID
cp862	PC Hebrew (without euro update)	10045
cp863	PC Canadian French	10046
cp864	PC Arabic (without euro update)	10047
cp865	PC Nordic	10048
cp866	PC Russian (without euro update)	10049
cp868	PC Urdu	10051
cp869	PC Greek (without euro update)	10052
cp922	IPC Estonian (without euro update)	10056
cp949c	PC Korea - KS	10028
ebcdic-xml-us	EBCDIC US (with euro) - Extension for XML4C(Xerces)	10180
EUC-KR	EUC Korean	10029
GB_2312-80	Simplified Chinese (GB2312-80)	10025
gb18030	GB 18030 MBCS codepage	1392
GB2312	Chinese EUC	10024
HKSCS	Hong Kong Supplementary Character Set	9200
hp-roman8	HP Latin1	10072
HZ-GB-2312	Simplified Chinese (HZ GB2312)	10092
IBM037	IBM EBCDIC US English	2028
IBM-1025	EBCDIC Cyrillic	10127
IBM1026	EBCDIC Turkey	10128
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM-1047-s390	EBCDIC IBM-1047 for S/390 (lf and nl swapped)	10167
IBM-1097	EBCDIC Farsi	10129
IBM-1112	EBCDIC Baltic	10130
IBM-1122	EBCDIC Estonia	10131
IBM-1123	EBCDIC Cyrillic Ukraine	10132
IBM-1129	ISO Vietnamese	10079

Name	Description	ID
IBM-1130	EBCDIC Vietnamese	10133
IBM-1132	EBCDIC Lao	10134
IBM-1133	ISO Lao	10081
IBM-1137	EBCDIC Devanagari	10163
IBM-1140	EBCDIC US (with euro update)	10135
IBM-1140-s390	EBCDIC IBM-1140 for S/390 (lf and nl swapped)	10168
IBM-1141	EBCDIC Germany, Austria (with euro update)	10136
IBM-1142	EBCDIC Denmark, Norway (with euro update)	10137
IBM-1142-s390	EBCDIC IBM-1142 for S/390 (lf and nl swapped)	10169
IBM-1143	EBCDIC Finland, Sweden (with euro update)	10138
IBM-1143-s390	EBCDIC IBM-1143 for S/390 (lf and nl swapped)	10170
IBM-1144	EBCDIC Italy (with euro update)	10139
IBM-1144-s390	EBCDIC IBM-1144 for S/390 (lf and nl swapped)	10171
IBM-1145	EBCDIC Spain, Latin America (with euro update)	10140
IBM-1145-s390	EBCDIC IBM-1145 for S/390 (lf and nl swapped)	10172
IBM-1146	EBCDIC UK, Ireland (with euro update)	10141
IBM-1146-s390	EBCDIC IBM-1146 for S/390 (lf and nl swapped)	10173
IBM-1147	EBCDIC French (with euro update)	10142
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (lf and nl swapped)	10174
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (lf and nl swapped)	10174
IBM-1148	EBCDIC International Latin1 (with euro update)	10143
IBM-1148-s390	EBCDIC IBM-1148 for S/390 (lf and nl swapped)	10175
IBM-1149	EBCDIC Iceland (with euro update)	10144
IBM-1149-s390	IEBCDIC IBM-1149 for S/390 (lf and nl swapped)	10176
IBM-1153	EBCDIC Latin2 (with euro update)	10145
IBM-1153-s390	EBCDIC IBM-1153 for S/390 (lf and nl swapped)	10177
IBM-1154	EBCDIC Cyrillic Multilingual (with euro update)	10146

Name	Description	ID
IBM-1155	EBCDIC Turkey (with euro update)	10147
IBM-1156	EBCDIC Baltic Multilingual (with euro update)	10148
IBM-1157	EBCDIC Estonia (with euro update)	10149
IBM-1158	EBCDIC Cyrillic Ukraine (with euro update)	10150
IBM1159	IBM EBCDIC Taiwan, Traditional Chinese	11001
IBM-1160	EBCDIC Thai (with euro update)	10151
IBM-1162	Thai (with euro update)	10033
IBM-1164	EBCDIC Vietnamese (with euro update)	10152
IBM-1250	MS Windows Latin2 (without euro update)	10058
IBM-1251	MS Windows Cyrillic (without euro update)	10059
IBM-1255	MS Windows Hebrew (without euro update)	10060
IBM-1256	MS Windows Arabic (without euro update)	10062
IBM-1257	MS Windows Baltic (without euro update)	10064
IBM-1258	MS Windows Vietnamese (without euro update)	10066
IBM-12712	EBCDIC Hebrew (updated with euro and new sheqel, control characters)	10161
IBM-12712-s390	EBCDIC IBM-12712 for S/390 (If and nl swapped)	10178
IBM-1277	Adobe Latin1 Encoding	10074
IBM13121	IBM EBCDIC Korean Extended CP13121	11002
IBM13124	IBM EBCDIC Simplified Chinese CP13124	11003
IBM-1363	PC Korean KSC MBCS Extended (with \ <-> Won mapping)	10032
IBM-1364	EBCDIC Korean Extended (SBCS IBM-13121 combined with DBCS IBM-4930)	10153
IBM-1371	EBCDIC Taiwan Extended (SBCS IBM-1159 combined with DBCS IBM-9027)	10154
IBM-1373	Taiwan Big-5 (with euro update)	10019
IBM-1375	MS Taiwan Big-5 with HKSCS extensions	10022
IBM-1386	PC Chinese GBK (IBM-1386)	10023
IBM-1388	EBCDIC Chinese GB (S-Ch DBCS-Host Data)	10155
IBM-1390	EBCDIC Japanese Katakana (with euro)	10156

Name	Description	ID
IBM-1399	EBCDIC Japanese Latin-Kanji (with euro)	10157
IBM-16684	EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399)	10158
IBM-16804	EBCDIC Arabic (with euro update)	10162
IBM-16804-s390	EBCDIC IBM-16804 for S/390 (lf and nl swapped)	10179
IBM-25546	ISO-2022 encoding for Korean (extension 1)	10089
IBM273	IBM EBCDIC German	2030
IBM277	EBCDIC Denmark, Norway	10115
IBM278	EBCDIC Finland, Sweden	10116
IBM280	IBM EBCDIC Italian	2035
IBM284	EBCDIC Spain, Latin America	10117
IBM285	IBM EBCDIC UK English	2038
IBM290	EBCDIC Japanese Katakana SBCS	10118
IBM297	IBM EBCDIC French	2040
IBM-33722	Japanese EUC (with \ <-> Yen mapping)	10017
IBM367	IBM367	10012
IBM-37-s390	EBCDIC IBM-37 for S/390 (lf and nl swapped)	10166
IBM420	EBCDIC Arabic	10119
IBM424	EBCDIC Hebrew (updated with new sheqel, control characters)	10120
IBM437	PC United States	10035
IBM-4899	EBCDIC Hebrew (with euro)	10159
IBM-4909	ISO Greek (with euro update)	10057
IBM4933	IBM Simplified Chinese CP4933	11004
IBM-4971	EBCDIC Greek (with euro update)	10160
IBM500	IBM EBCDIC International Latin-1	2044
IBM-5050	Japanese EUC (Packed Format)	10018
IBM-5123	EBCDIC Japanese Latin (with euro update)	10164
IBM-5351	MS Windows Hebrew (older version)	10061

Name	Description	ID
IBM-5352	MS Windows Arabic (older version)	10063
IBM-5353	MS Windows Baltic (older version)	10065
IBM-803	EBCDIC Hebrew	10121
IBM833	IBM EBCDIC Korean CP833	833
IBM834	IBM EBCDIC Korean CP834	834
IBM835	IBM Taiwan, Traditional Chinese CP835	11005
IBM836	IBM EBCDIC Simplified Chinese Extended	11006
IBM837	IBM Simplified Chinese CP837	11007
IBM-838	EBCDIC Thai	10122
IBM-8482	EBCDIC Japanese Katakana SBCS (with euro update)	10165
IBM852	PC Latin2 (without euro update)	10038
IBM855	PC Cyrillic (without euro update)	10039
IBM-867	PC Hebrew (with euro update)	10050
IBM870	EBCDIC Latin2	10123
IBM871	EBCDIC Iceland	10124
IBM-874	PC Thai (without euro update)	10034
IBM-875	EBCDIC Greek	10125
IBM-901	PC Baltic (with euro update)	10054
IBM-902	PC Estonian (with euro update)	10055
IBM918	EBCDIC Urdu	10126
IBM930	IBM EBCDIC Japanese	930
IBM933	IBM EBCDIC Korean CP933	933
IBM935	IBM EBCDIC Simplified Chinese	935
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939
IBM-942	PC Japanese SJIS-78 syntax (IBM-942)	10015
IBM-943	PC Japanese SJIS-90 (IBM-943)	10016

Name	Description	ID
IBM-949	PC Korea - KS (default)	10027
IBM-950	Taiwan Big-5 (without euro update)	10020
IBM-964	EUC Taiwan	10026
IBM-971	EUC Korean (DBCS-only)	10030
IMAP-mailbox-name	IMAP Mailbox Name	10008
is-960	Israeli Standard 960 (7-bit Hebrew encoding)	11000
ISO-2022-CN	ISO-2022 encoding for Chinese	10090
ISO-2022-CN-EXT	ISO-2022 encoding for Chinese (extension 1)	10091
ISO-2022-JP	ISO-2022 encoding for Japanese	10083
ISO-2022-JP-2	ISO-2022 encoding for Japanese (extension 2)	10085
ISO-2022-KR	ISO-2022 encoding for Korean	10088
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-13	ISO 8859-13 PC Baltic (without euro update)	10014
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
JEF	Japanese EBCDIC Fujitsu	9000
JEF-K	Japanese EBCDIC-Kana Fujitsu	9005
JIPSE	NEC ACOS JIPSE Japanese	9002
JIPSE-K	NEC ACOS JIPSE-Kana Japanese	9007

Name	Description	ID
JIS_Encoding	ISO-2022 encoding for Japanese (extension 1)	10084
JIS_X0201	ISO-2022 encoding for Japanese (JIS_X0201)	10093
JIS7	ISO-2022 encoding for Japanese (extension 3)	10086
JIS8	ISO-2022 encoding for Japanese (extension 4)	10087
JP-EBCDIC	EBCDIC Japanese	9010
JP-EBCDIK	EBCDIK Japanese	9011
KEIS	HITACHI KEIS Japanese	9001
KEIS-K	HITACHI KEIS-Kana Japanese	9006
KOI8-R	IRussian Internet	10053
KSC_5601	PC Korean KSC MBCS Extended (KSC_5601)	10031
Latin1	ISO 8859-1 Western European	4
LMBCS-1	Lotus MBCS encoding for PC Latin1	10103
LMBCS-11	Lotus MBCS encoding for MS-DOS Thai	10110
LMBCS-16	Lotus MBCS encoding for Windows Japanese	10111
LMBCS-17	Lotus MBCS encoding for Windows Korean	10112
LMBCS-18	Lotus MBCS encoding for Windows Chinese (Traditional)	10113
LMBCS-19	Lotus MBCS encoding for Windows Chinese (Simplified)	10114
LMBCS-2	Lotus MBCS encoding for PC DOS Greek	10104
LMBCS-3	Lotus MBCS encoding for Windows Hebrew	10105
LMBCS-4	Lotus MBCS encoding for Windows Arabic	10106
LMBCS-5	Lotus MBCS encoding for Windows Cyrillic	10107
LMBCS-6	Lotus MBCS encoding for PC Latin2	10108
LMBCS-8	Lotus MBCS encoding for Windows Turkish	10109
macintosh	Apple Latin 1	10067
MELCOM	MITSUBISHI MELCOM Japanese	9004
MELCOM-K	MITSUBISHI MELCOM-Kana Japanese	9009
MS1250	MS Windows Latin 2 (Central Europe)	2250

Name	Description	ID
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950
SCSU	Standard Compression Scheme for Unicode (SCSU)	10009
UNISYS	UNISYS Japanese	9003
UNISYS-K	UNISYS-Kana Japanese	9008
US-ASCII	7-bit ASCII	1
UTF-16_OppositeEndian	UTF-16 encoding of Unicode (Opposite Platform Endian)	10004
UTF-16_PlatformEndian	UTF-16 encoding of Unicode (Platform Endian)	10003
UTF-16BE	UTF-16 encoding of Unicode (Big Endian)	1200
UTF-16LE	UTF-16 encoding of Unicode (Lower Endian)	1201
UTF-32_OppositeEndian	UTF-32 encoding of Unicode (Opposite Platform Endian)	10006
UTF-32_PlatformEndian	UTF-32 encoding of Unicode (Platform Endian)	10005
UTF-32BE	UTF-32 encoding of Unicode (Big Endian)	10001
UTF-32LE	UTF-32 encoding of Unicode (Lower Endian)	10002
UTF-7	UTF-7 encoding of Unicode	10007

Name	Description	ID
UTF-8	UTF-8 encoding of Unicode	106
windows-57002	Indian Script Code for Information Interchange - Devanagari	10094
windows-57003	Indian Script Code for Information Interchange - Bengali	10095
windows-57004	Indian Script Code for Information Interchange - Tamil	10099
windows-57005	Indian Script Code for Information Interchange - Telugu	10100
windows-57007	Indian Script Code for Information Interchange - Oriya	10098
windows-57008	Indian Script Code for Information Interchange - Kannada	10101
windows-57009	Indian Script Code for Information Interchange - Malayalam	10102
windows-57010	Indian Script Code for Information Interchange - Gujarati	10097
windows-57011	Indian Script Code for Information Interchange - Gurumukhi	10096
x-mac-centraleurroman	Apple Central Europe	10070
x-mac-cyrillic	Apple Cyrillic	10069
x-mac-greek	Apple Greek	10068
x-mac-turkish	Apple Turkish	10071

Restrictions for Code Pages for Sources and Targets

Consider the following restrictions when you assign a source or target code page:

- Select IBM EBCDIC as your source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.
- The following code pages are not supported for database or relational connections:
  - UTF-16 encoding of Unicode (Opposite Platform Endian)
  - UTF-16 encoding of Unicode (Platform Endian)
  - UTF-16 encoding of Unicode (Big Endian)
  - UTF-16 encoding of Unicode (Lower Endian)

APPENDIX B

Custom Roles

This appendix includes the following topic:

CDI-PC Repository Service Custom Roles

The CDI-PC Repository Service custom roles include the CDI-PC Connection Administrator, CDI-PC Operator, and CDI-PC repository Folder Administrator.

CDI-PC Connection Administrator

The following table lists the default privileges assigned to the CDI-PC Connection Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Manager
Global Objects	Create Connections

CDI-PC Operator

The following table lists the default privileges assigned to the CDI-PC Operator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Monitor
Run-time Objects	- Execute - Manage Execution - Monitor

CDI-PC repository Folder Administrator

The following table lists the default privileges assigned to the CDI-PC repository Folder Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Repository Manager
Folders	- Copy - Create - Manage Versions
Global Objects	- Manage Deployment Groups - Execute Deployment Groups - Create Labels - Create Queries

APPENDIX C

Informatica Platform Connectivity

This appendix includes the following topics:

Informatica Platform Connectivity Overview

The Informatica platform uses the following types of connectivity to communicate among clients, services, and other components in the domain:

TCP/IP network protocol

Application services and the Service Managers in a domain use TCP/IP network protocol to communicate with other nodes and services. The clients also use TCP/IP to communicate with application services. You can configure the host name and port number for TCP/IP communication on a node when you install the Informatica services. You can configure the port numbers used for services on a node during installation or in Informatica Administrator.

Native drivers

The CDI-PC Integration Service and the CDI-PC Repository Service use native drivers to communicate with databases. Native drivers are packaged with the database server and client software. Install and configure the native database client software on the machines where the services run.

ODBC

The ODBC drivers are installed with the Informatica services and the Informatica clients. The integration services use ODBC drivers to communicate with databases.

CDI-PC Connectivity

CDI-PC uses the TCP/IP network protocol, native database drivers, and ODBC for communication between the following CDI-PC components:

- **CDI-PC Repository Service.** The CDI-PC Repository Service uses native database drivers to communicate with the CDI-PC repository. The CDI-PC Repository Service uses TCP/IP to communicate with other CDI-PC components.

- **CDI-PC Integration Service.** The CDI-PC Integration Service uses native database connectivity and ODBC to connect to source and target databases. The CDI-PC Integration Service uses TCP/IP to communicate with other CDI-PC components.
- **CDI-PC Client.** CDI-PC Client uses ODBC to connect to source and target databases. CDI-PC Client uses TCP/IP to communicate with the CDI-PC Repository Service and CDI-PC Integration Service.

The following table lists the drivers used by CDI-PC components:

Component	Database	Driver
CDI-PC Repository Service	CDI-PC repository	Native
CDI-PC Integration Service	Source Target Stored Procedure Lookup	Native ODBC
CDI-PC Client	CDI-PC repository	Native
CDI-PC Client	Source Target Stored Procedure Lookup	ODBC

Repository Service Connectivity

The CDI-PC Repository Service manages the metadata in the CDI-PC repository database. All applications that connect to the repository must connect to the CDI-PC Repository Service. The CDI-PC Repository Service uses native drivers to communicate with the repository database.

The following table describes the connectivity required to connect the CDI-PC Repository Service to the repository and source and target databases:

CDI-PC Repository Service Connection	Connectivity Requirement
CDI-PC Client	TCP/IP
CDI-PC Integration Service	TCP/IP
CDI-PC repository database	Native database drivers

The CDI-PC Integration Service connects to the Repository Service to retrieve metadata when it runs workflows.

Connecting from CDI-PC Client

To connect to the CDI-PC Repository Service from CDI-PC Client, add a domain and repository in the CDI-PC Client tool. When you connect to the repository from a CDI-PC Client tool, the client tool sends a connection request to the Service Manager on the gateway node. The Service Manager returns the host name and port number of the node where the CDI-PC Repository Service runs. CDI-PC Client uses TCP/IP to connect to the CDI-PC Repository Service.

Connecting to Databases

To set up a connection from the CDI-PC Repository Service to the repository database, configure the database properties in Informatica Administrator. You must install and configure the native database drivers for the repository database on the machine where the CDI-PC Repository Service runs.

Integration Service Connectivity

The CDI-PC Integration Service connects to the repository to read repository objects. The CDI-PC Integration Service connects to the repository through the CDI-PC Repository Service. Use Informatica Administrator to configure an associated repository for the Integration Service.

The following table describes the connectivity required to connect the CDI-PC Integration Service to the platform components, source databases, and target databases:

CDI-PC Integration ServiceConnection	Connectivity Requirement
CDI-PC Client	TCP/IP
Other CDI-PC Integration Service Processes	TCP/IP
Repository Service	TCP/IP
Source and target databases	Native database drivers or ODBC **Note:** The CDI-PC Integration Service on Windows and UNIX can use ODBC drivers to connect to databases. You can use native drivers to improve performance.

The CDI-PC Integration Service includes ODBC libraries that you can use to connect to other ODBC sources. The Informatica installation includes ODBC drivers.

For flat file, XML, or COBOL sources, you can either access data with network connections, such as NFS, or transfer data to the CDI-PC Integration Service node through FTP software. For information about connectivity software for other ODBC sources, refer to your database documentation.

Connecting from the CDI-PC Client

The Workflow Manager communicates with a CDI-PC Integration Service process over a TCP/IP connection. The Workflow Manager communicates with the CDI-PC Integration Service process each time you start a workflow or display workflow details.

Connecting to the CDI-PC Repository Service

When you create a CDI-PC Integration Service, you specify the CDI-PC Repository Service to associate with the CDI-PC Integration Service. When the CDI-PC Integration Service runs a workflow, it uses TCP/IP to connect to the associated CDI-PC Repository Service and retrieve metadata.

Connecting to Databases

Use the Workflow Manager to create connections to databases. You can create connections using native database drivers or ODBC. If you use native drivers, specify the database user name, password, and native connection string for each connection. The CDI-PC Integration Service uses this information to connect to the database when it runs the session.

Note: CDI-PC supports ODBC drivers, such as ISG Navigator, that do not need user names and passwords to connect. To avoid using empty strings or nulls, use the reserved words PmNullUser and PmNullPasswd for the user name and password when you configure a database connection. The CDI-PC Integration Service treats PmNullUser and PmNullPasswd as no user and no password.

CDI-PC Client Connectivity

The CDI-PC Client uses ODBC drivers and native database client connectivity software to communicate with databases. It uses TCP/IP to communicate with the Integration Service and with the repository.

The following table describes the connectivity types required to connect the CDI-PC Client to the Integration Service, repository, and source and target databases:

CDI-PC Client Connection	Connectivity Requirement
Integration Service	TCP/IP
Repository Service	TCP/IP
Databases	ODBC connection for each database

Connecting to the Repository

You can connect to the repository using the CDI-PC Client tools. All CDI-PC Client tools use TCP/IP to connect to the repository through the Repository Service each time you access the repository to perform tasks such as connecting to the repository, creating repository objects, and running object queries.

Connecting to Databases

To connect to databases from the Designer, use the Windows ODBC Data Source Administrator to create a data source for each database you want to access. Select the data source names in the Designer when you perform the following tasks:

- **Import a table or a stored procedure definition from a database.** Use the Source Analyzer or Target Designer to import the table from a database. Use the Transformation Developer, Mapplet Designer, or Mapping Designer to import a stored procedure or a table for a Lookup transformation.

  To connect to the database, you must also provide your database user name, password, and table or stored procedure owner name.
- **Preview data.** You can select the data source name when you preview data in the Source Analyzer or Target Designer. You must also provide your database user name, password, and table owner name.

Connecting to the Integration Service

The Workflow Manager and Workflow Monitor communicate directly with the Integration Service over TCP/IP each time you perform session and workflow-related tasks, such as running a workflow. When you log in to a repository through the Workflow Manager or Workflow Monitor, the client application lists the Integration Services that are configured for that repository in Informatica Administrator.

Native Connectivity

To establish native connectivity between an application service and a database, you must install the database client software on the machine where the service runs.

The following table describes the syntax for the native connection string for each supported database system:

Database	Connect String Syntax	Example
IBM DB2	*dbname*	mydatabase
Microsoft SQL Server	*servername@dbname*	sqlserver@mydatabase
Oracle	*dbname*.world (same as TNSNAMES entry)	oracle.world
Sybase ASE	*servername@dbname*	sambrown@mydatabase **Note:** Sybase ASE servername is the name of the Adaptive Server from the interfaces file.
Teradata	*ODBC_data_source_name* or *ODBC_data_source_name@db_name* or *ODBC_data_source_name@db_user_name*	TeradataODBC TeradataODBC@mydatabase TeradataODBC@sambrown **Note:** Use Teradata ODBC drivers to connect to source and target databases.

ODBC Connectivity

Open Database Connectivity (ODBC) provides a common way to communicate with different database systems.

To use ODBC connectivity, you must install the following components on the machine hosting the Informatica service or client tool:

- **Database client software.** Install the client software for the database system. This installs the client libraries needed to connect to the database.

  Note: Some ODBC drivers contain wire protocols and do not require the database client software.

- **ODBC drivers.** The DataDirect closed 32-bit or 64-bit ODBC drivers are installed when you install the Informatica services. The DataDirect closed 32-bit ODBC drivers are installed when you install the Informatica clients. The database server can also include an ODBC driver.

After you install the necessary components you must configure an ODBC data source for each database that you want to connect to. A data source contains information that you need to locate and access the database, such as database name, user name, and database password. On Windows, you use the ODBC Data Source Administrator to create a data source name. On UNIX, you add data source entries to the odbc.ini file found in the system $ODBCHOME directory.

When you create an ODBC data source, you must also specify the driver that the ODBC driver manager sends database calls to.

The following table shows the recommended ODBC drivers to use with each database:

Database	ODBC Driver	Requires Database Client Software
Informix	DataDirect Informix Wire Protocol	No
Microsoft Access	Microsoft Access driver	No
Microsoft Excel	Microsoft Excel driver	No
Microsoft SQL Server	DataDirect SQL Server Wire Protocol	No
Netezza	Netezza SQL	Yes
Teradata	Teradata ODBC driver	Yes
SAP HANA	SAP HANA ODBC driver	Yes

APPENDIX D

Configure the Web Browser

This appendix includes the following topic:

Configure the Web Browser

You can run the Administrator tool in the Microsoft Internet Explorer, Microsoft Edge, Google Chrome, or Safari web browser.

To use the Administrator tool, configure the following options in the browser:

Scripting and ActiveX

Enable the following controls on Microsoft Internet Explorer:

- Active scripting
- Allow programmatic clipboard access
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

To configure the controls, click **Tools** > **Internet options** > **Security** > **Custom level**.

Trusted sites

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer, Microsoft Edge, and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. In Safari, add the certificate of the Informatica web application to the keychain. If you are using Chrome version 86.0.42x or later on Windows, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

INDEX

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X