Informatica®
10.2 HotFix 2

Installation and Configuration Guide

Informatica Installation and Configuration Guide
10.2 HotFix 2

Publication Date: 2019-08-14

Table of Contents

Preface

The *Informatica Installation and Configuration Guide* is written for the system administrator who is responsible for installing the Informatica product. This guide assumes you have knowledge of operating systems, relational database concepts, and the database engines, flat files, or mainframe systems in your environment. This guide also assumes you are familiar with the interface requirements for your supporting applications.

Informatica Resources

Informatica Network

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

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- Review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

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

Informatica Documentation

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

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

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

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

If you are an Informatica Network member, you can access Informatica Velocity resources at http://velocity.informatica.com.

If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

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

Informatica Global Customer Support

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

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

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

Part I: Installation Overview

This part contains the following chapter:

CHAPTER 1

Installation Overview

This chapter includes the following topics:

Informatica Installation

Informatica provides separate installers to install the Informatica services and the Informatica clients. Download the Informatica installer files to install the Informatica services and clients for the Informatica domain.

The Informatica services consist of services to support the domain and application services to perform tasks and manage databases. The Informatica domain is the administrative unit for the Informatica environment. The domain is a collection of nodes that represent the machines on which the application services run. When you install the Informatica services on a machine, you install all files for all services. After you complete the installation, you can create application services based on the products and functionality that your organization purchased.

On Windows, you can use the Informatica services installer to install the Informatica services or the Data Transformation engine. On UNIX, you can use the Informatica services installer to install the Informatica services or the Data Transformation engine.

When you install the Informatica services, you are prompted to create a domain or to join a domain. The first time you run the installer, you must create the domain. If you install on a single machine, you create the Informatica domain and a gateway node on the machine. If you install on multiple machines, you create an Informatica domain and a gateway node during the first installation. During the installation on the additional machines, you create gateway or worker nodes that you join to the domain.

The Informatica clients consist of thick client applications and web client applications. You use the clients to access the services in the domain. When you run the client installer, you can install the thick client applications.

Installation Process

The installation of the Informatica services and Informatica clients consists of multiple phases.

The installation process consists of the following phases:

1. Before you install the Informatica services, perform the following tasks to plan and prepare for the services installation:
    a. Plan the Informatica domain. Consider the number of nodes in the domain, the application services that will run on each node, the system requirements, and the type of user authentication that the domain will use.
    b. Prepare the databases for the domain. Verify the database requirements and set up the databases.
    c. Set up the machines to meet either the Windows or UNIX requirements to ensure that you can successfully install and run the Informatica services.
2. Install the Informatica services.

    Use the server installer to install the Informatica services on one or more Windows or UNIX machines. The first time you run the installer, you must create the domain. During the installation on the additional machines, you create worker nodes that you join to the domain.
3. After you install the Informatica services, perform the following tasks to complete the services installation:
    a. Complete the domain configuration. Verify code page compatibility, complete tasks required by the type of user authentication used by the domain, and configure environment variables. Optionally, configure secure communication for the domain.
    b. Prepare to create the application services. Verify operating system requirements for application services and create the users and connections required by the application services.
    c. Create the application services in the required order.
4. Install the Informatica clients.

    Perform the following tasks to install the clients:
    a. Before you install the clients, verify the installation and third-party software requirements for the clients.
    b. Use the client installer to install the clients on Windows machines.
    c. After you install the clients, optionally install additional languages and configure the required environment variables for the clients.

Part II: Before You Install the Services

This part contains the following chapters:

CHAPTER 2

Plan the Domain

This chapter includes the following topics:

Introduction to the Informatica Domain

An Informatica domain is a collection of nodes and services. A node is the logical representation of a machine in a domain. Services for the domain include the Service Manager that manages all domain operations and a set of application services that represent server-based functionality.

The domain requires a relational database to store configuration information and user account privileges and permissions. The first time that you install the Informatica services, you must create the domain configuration repository in a relational database.

You use Informatica clients to access underlying Informatica functionality in the domain. The clients make requests to the Service Manager or to application services.

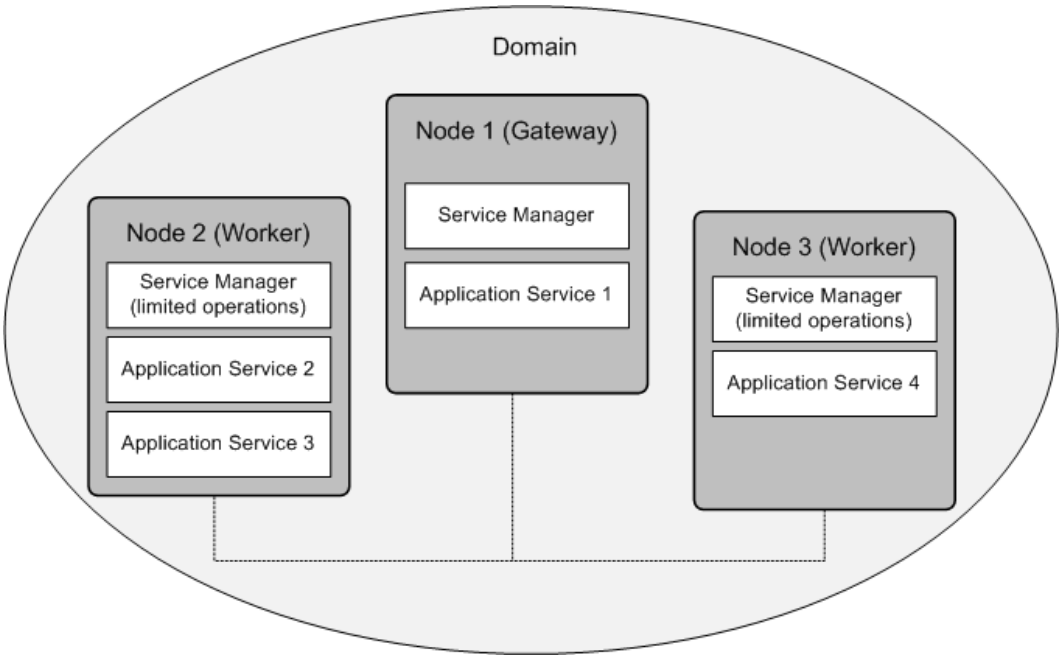
Single or Multiple Node Domain

When you install the Informatica services on a machine, you create a node and a domain. You can install the Informatica services on multiple machines to create additional nodes that you join to the domain.

A single node installation consists of a domain with one node. The node hosts the domain. The Service Manager and all Informatica application services run on the node.

An installation on multiple nodes consists of a gateway node, which hosts the domain, and additional nodes that run Informatica application services. The Service Manager runs on all nodes in the domain.

The following image shows an installation on multiple nodes:



Nodes

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 a node performs and the services that a 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. 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.

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

A worker node is any node not configured to serve as a gateway. A worker node can run application services, but it cannot serve as a gateway. The Service Manager performs limited domain operations on a worker node.

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.

If a node is assigned to a Data Integration Service grid, you might want to update the node role. Enable only the service role to dedicate the node to running the Data Integration Service process. Enable only the compute role to dedicate the node to running Data Integration Service mappings.

For more information about nodes, see the *Informatica Administrator Guide*.

For more information about Data Integration Service grids, see the *Informatica Application Service Guide*.

Service Manager

The Service Manager in the Informatica domain supports the domain and the application services. The Service Manager runs on each node in the domain.

The Service Manager runs on all nodes in the domain to support following areas:

Domain

The Service Manager performs functions on each node to support the domain. Domain functions include authentication, authorization, and logging. The domain 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 services

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 Informatica clients.

For more information about the Service Manager, see the *Informatica Administrator Guide*.

Application Services

Application services represent server-based functionality. Application services include services that can have multiple instances in the domain and system services that can have a single instance in the domain. System services are created for you when you create the domain. After you complete the installation, you create other application services based on the license key generated for your organization.

When you create an application service, you designate a node with the service role to run the service process. The service process is the run-time representation of a service running on a node. The service type determines how many service processes can run at a time.

If you have the high availability option, you can run an application service on multiple nodes. If you do not have the high availability option, configure each application service to run on one node.

Some application services require databases to store information processed by the application service. When you plan the Informatica domain, you also need to plan the databases required by each application service.

For more information about application services, see the *Informatica Application Service Guide*.

License Key

Informatica generates a license key based on the product and product options that your organization purchased. The license key controls the application services and the functionality that you can use.

When you install the Informatica services, you must enter the path and file name of the Informatica license key. The installer creates a license object in the domain based on the license key that you enter. When you create application services, you must assign the license object to each application service before you can run the service.

User Authentication

During installation, you can select the authentication to use for the Informatica domain.

The Informatica domain can use the following types of authentication to authenticate users in the Informatica domain:

- Native user authentication
- LDAP user authentication
- Kerberos network authentication

Native user accounts are stored in the Informatica domain and can only be used within the Informatica domain. Kerberos and LDAP user accounts are stored in an LDAP directory service and are shared by applications within the enterprise.

If you enable Kerberos authentication during installation, you must configure the Informatica domain to work with the Kerberos key distribution center (KDC). You must create the service principal names (SPN) required by the Informatica domain in the Kerberos principal database. The Kerberos principal database can be an LDAP directory service. You must also create keytab files for the SPNs and store it in the Informatica directory as required by the Informatica domain.

If you do not enable Kerberos authentication during installation, the installer configures the Informatica domain to use native authentication. After installation, you can set up a connection to an LDAP server and configure the Informatica domain to use LDAP authentication in addition to native authentication.

For more information about user authentication, see the *Informatica Security Guide*.

Encryption Key for Secure Data Storage

Informatica encrypts sensitive data, such as passwords and secure connection parameters, before it stores the data in the Informatica repositories. Informatica uses a keyword to create an encryption key with which to encrypt sensitive data.

When you install the Informatica services and create a domain, you must specify a keyword for the installer to use to generate the encryption key for the domain. Based on the keyword, the installer generates an encryption key file named *siteKey* and stores it in a directory you specify. If you do not specify a directory, the installer stores the *siteKey* file in the default directory: `<Informatica installation directory>/isp/config/keys`

All nodes in a domain must use the same encryption key. If you install on multiple nodes, the installer uses the same encryption key for all nodes in the domain. When you run the installer after you create the domain, you must specify the same encryption key for any node that you join to the domain.

You must specify a keyword even if you do not enable secure communication for the domain or use Kerberos authentication.

Important: You must keep the name of the domain, the keyword for the encryption key, and the encryption key file in a secure location. The encryption key is required when you change the encryption key of the domain or move a repository to another domain. If you do not have the encryption key, you must have the domain name and the keyword used to generate the encryption key.

Domain Security

When you install the Informatica services and create a domain, you can enable options to configure security in the domain.

You can configure the following security options for the domain:

Secure communication for services and the Service Manager

When you configure secure communication for the domain, you secure the connections between the Service Manager and the services in the domain. Informatica provides an SSL certificate that you can use to secure the domain. However, for better security for the domain, you can provide the SSL certificate during the installation. Provide the keystore and truststore files that contain the SSL certificates you want to use.

Secure domain configuration repository database

When you install the Informatica services and create a domain, you can create the domain configuration repository in a database secured with the SSL protocol. Access to the secure database requires a truststore that contains the SSL certificates for the database. During installation, you provide the truststore file that contains the SSL certificate you want to use.

Secure connection for the Administrator tool

Informatica Administrator (the Administrator tool) is the tool that you use to administer the Informatica domain. During installation, you can configure a secure HTTPS connection for the Administrator tool. You can provide the keystore file to use for the HTTPS connection.

For more information about domain security, see the *Informatica Security Guide*.

Informatica Clients

The Informatica clients are a group of clients that you use to access underlying Informatica functionality. The clients make requests to the Service Manager or to application services.

The Informatica clients consist of thick client applications and thin or web client applications. You use the clients to access the services in the domain. When you run the Informatica client installation, you can choose to install the thick client applications.

The clients that you use depend on the license key generated for your organization.

You can install the following thick client applications:

Informatica Developer

The Developer tool is a client application that you use to create and run data objects, mappings, profiles, workflows, and virtual databases. Objects that you create in the Developer tool are stored in a Model repository and are run by a Data Integration Service.

PowerCenter® Client

The PowerCenter Client is a client application that you use to define sources and targets, create transformations and build mappings, and create workflows to run mappings. Objects that you create in the PowerCenter Client are stored in a PowerCenter repository and run by a PowerCenter Integration Service.

You can create application services to run the following thin or web client applications:

Analyst tool

The Analyst tool is a web application that you use to analyze, cleanse, integrate, and standardize data in an enterprise. The Analyst Service runs the Analyst tool. Objects that you create in the Analyst tool are stored in a Model repository and are run by a Data Integration Service.

Metadata Manager

Metadata Manager is a web application that you use to browse and analyze metadata from disparate metadata repositories. The Metadata Manager Service runs the Metadata Manager application. Objects that you create in Metadata Manager are stored in a Metadata Manager repository.

Web Services Hub Console

The Web Services Hub Console is a web application that you use to manage the web services you create in PowerCenter. The Web Services Hub Service runs the Web Services Hub Console.

Informatica Administrator

Informatica Administrator (the Administrator tool) is the administration tool that you use to administer the Informatica domain and security. The Administrator tool is a thin or web client application.

You use the Administrator tool to perform the following tasks:

Domain administrative tasks

Manage logs, domain objects, and domain reports. Domain objects include application services, nodes, grids, folders, database connections, applications, and licenses.

Security administrative tasks

Manage users, groups, roles, privileges, and permissions.

On each node where you install the Informatica services, the installer creates a Windows service or UNIX daemon to run Informatica. When the installation completes successfully, the installer starts the Informatica service on Windows or the Informatica daemon on UNIX.

The Informatica service also runs the Administrator tool. Log in to the Administrator tool to create the user accounts for users of Informatica and to create and configure the application services in the domain.

Domain Planning Process

Before you install the Informatica services, you need to plan for all of the components in the Informatica domain.

When you plan the domain, you must consider the number of nodes needed in the domain, the types of application services that the domain requires, and the number of application services that run on each node. You must determine the database type and host name for the domain configuration repository and for the databases required by each application service. If you use Metadata Manager, you must also decide whether to create one domain or a split domain.

You must choose a keyword for the installer to use to generate the encryption key for the domain. Informatica uses the encryption key to encrypt sensitive data.

If you decide to configure SAML-based single sign-on (SSO) for the domain, you cannot configure the Kerberos authentication for the Informatica domain.

If you decide to configure security for the domain, you must know the location and password for the keystore and truststore files. If you decide to use Kerberos authentication for the Informatica domain, you must work with the Kerberos administrator to set up the user and service principals required by the domain.

As part of the planning process, you must also verify that each machine and database server in the domain meets the minimum system requirements.

Plan the Application Services

When you plan the Informatica domain, you also need to plan the application services that will run in the domain. You create application services based on the license key generated for your organization.

When you plan the application services, you must account for the associated services that connect to the application service. You also must plan the relational databases that are required to create the application service.

You create the application services after you complete the installation.

For more information about application services, see the *Informatica Application Service Guide*.

Application Services by Product

Each application service provides different functionality within the Informatica domain. You create application services based on the license key generated for your organization.

The following table lists the application services that you can create for each product:

Product	Application Services
Big Data Management	- Analyst Service - Data Integration Service - Model Repository Service - Search Service
Data Quality Standard Edition or Data Quality Advanced Edition	- Analyst Service - Content Management Service - Data Integration Service - Model Repository Service - Search Service
Data Quality Governance Edition	- Analyst Service - Content Management Service - Data Integration Service - Metadata Manager Service - Model Repository Service - PowerCenter Integration Service - PowerCenter Repository Service - Search Service
Data Services	- Analyst Service - Content Management Service - Data Integration Service - Model Repository Service - PowerCenter Integration Service - PowerCenter Repository Service - Search Service
Data Transformation	- Data Integration Service - Model Repository Service

Product	Application Services
PowerCenter Standard Edition	- Analyst Service - Content Management Service - Data Integration Service - Model Repository Service - PowerCenter Integration Service - PowerCenter Repository Service - Search Service - Web Services Hub (available with the real-time option)
PowerCenter Advanced Edition or PowerCenter Premium Edition	- Analyst Service - Content Management Service - Data Integration Service - Metadata Manager Service - Model Repository Service - PowerCenter Integration Service - PowerCenter Repository Service - Search Service - Web Services Hub (available with the real-time option)

Analyst Service

The Analyst Service is an application service that runs the Analyst tool in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to the Analyst tool.

When you run profiles, scorecards, or mapping specifications in the Analyst tool, the Analyst Service connects to the Data Integration Service to perform the data integration jobs. When you work on Human tasks in the Analyst tool, the Analyst Service connects to the Data Integration Service to retrieve the task metadata from the workflow database.

When you view, create, or delete a Model repository object in the Analyst tool, the Analyst Service connects to the Model Repository Service to access the metadata. When you view data lineage analysis on scorecards in the Analyst tool, the Analyst Service sends the request to the Metadata Manager Service to run data lineage.

Note: When you create the Analyst Service, you do not associate it with any relational databases.

Associated Services

The Analyst Service connects to other application services within the domain.

When you create the Analyst Service, you can associate it with the following application services:

Data Integration Services

You can associate up to two Data Integration Services with the Analyst Service. The Analyst Service manages the connection to the Data Integration Service that enables users to perform data preview, mapping specification, scorecard, and profile jobs in the Analyst tool. The Analyst Service also manages the connection to the Data Integration Service that you configure to run workflows. When you create the Analyst Service, you provide the name of the Data Integration Services. You can associate the Analyst Service with the same Data Integration Service for all operations.

Metadata Manager Service

The Analyst Service manages the connection to the Metadata Manager Service that runs data lineage for scorecards in the Analyst tool. When you create the Analyst Service, you can provide the name of the Metadata Manager Service.

Model Repository Service

The Analyst Service manages the connection to the Model Repository Service for the Analyst tool. The Analyst tool connects to the Model Repository Service to create, update, and delete Model repository objects in the Analyst tool. When you create the Analyst Service, you provide the name of the Model Repository Service.

Content Management Service

The Content Management Service is an application service that manages reference data. A reference data object contains a set of data values that you can search while performing data quality operations on source data. The Content Management Service also compiles rule specifications into mapplets. A rule specification object describes the data requirements of a business rule in logical terms.

The Content Management Service uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. The Content Management Service also provides transformations, mapping specifications, and rule specifications with the following types of reference data:

- Address reference data
- Identity populations
- Probabilistic models and classifier models
- Reference tables

Associated Services

The Content Management Service connects to other application services within the domain.

When you create the Content Management Service, you can associate it with the following application services:

Data Integration Service

The Content Management Service uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. When you create the Content Management Service, you provide the name of the Data Integration Service. You must create the Data Integration Service and Content Management Service on the same node.

Model Repository Service

The Content Management Service connects to the Model Repository Service to store metadata for reference data objects in the Model repository. When you create the Content Management Service, you provide the name of the Model Repository Service.

You can associate multiple Content Management Services with a Model Repository Service. The Model Repository Service identifies the first Content Management Service that you associate as the master Content Management Service. The master Content Management Service manages the data files for the probabilistic models and classifier models in the Model repository.

Required Databases

The Content Management Service requires a reference data warehouse in a relational database. When you create the Content Management Service, you must provide connection information to the reference data warehouse.

Create the following database before you create the Content Management Service:

Reference data warehouse

Stores data values for the reference table objects that you define in the Model repository. When you add data to a reference table, the Content Management Service writes the data values to a table in the reference data warehouse. You need a reference data warehouse to manage reference table data in the Analyst tool and the Developer tool.

Data Integration Service

The Data Integration Service is an application service that performs data integration jobs for the Analyst tool, the Developer tool, and external clients.

When you preview or run data profiles, SQL data services, and mappings in the Analyst tool or the Developer tool, the client tool sends requests to the Data Integration Service to perform the data integration jobs. When you run SQL data services, mappings, and workflows from the command line program or an external client, the command sends the request to the Data Integration Service.

Associated Services

The Data Integration Service connects to other application services within the domain.

When you create the Data Integration Service, you can associate it with the following application service:

Model Repository Service

The Data Integration Service connects to the Model Repository Service to perform jobs such as running mappings, workflows, and profiles. When you create the Data Integration Service, you provide the name of the Model Repository Service.

Required Databases

The Data Integration Service can connect to multiple relational databases. The databases that the service can connect to depend on the license key generated for your organization. When you create the Data Integration Service, you provide connection information to the databases.

Create the following databases before you create the Data Integration Service:

Data object cache database

Stores cached logical data objects and virtual tables. Data object caching enables the Data Integration Service to access pre-built logical data objects and virtual tables. You need a data object cache database to increase performance for mappings, SQL data service queries, and web service requests.

Profiling warehouse

Stores profiling information, such as profile results and scorecard results. You need a profiling warehouse to perform profiling and data discovery.

Workflow database

Stores all run-time metadata for workflows, including Human task metadata.

Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services.

When you access a Model repository object from the Developer tool, the Analyst tool, the Administrator tool, or the Data Integration Service, the client or service sends a request to the Model Repository Service. The

Model Repository Service process fetches, inserts, and updates the metadata in the Model repository database tables.

Configure a Model repository service to store monitoring statistics in the monitoring Model repository. When a Data Integration Service runs objects, it stores run-time statistics about the objects in the Model repository that you configure for monitoring. To optimize monitoring performance, create a Model Repository Service that is dedicated to storing monitoring data. This type of Model Repository Service is called a monitoring Model Repository Service.

Note: When you create the Model Repository Service, you do not associate it with other application services.

Required Databases

The Model Repository Service requires a Model repository in a relational database. When you create the Model Repository Service, you must provide connection information to the database.

Create the following database before you create the Model Repository Service:

Model repository

Stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services. You need a Model repository to store the design-time and run-time objects created by Informatica clients and application services.

Search Service

The Search Service is an application service that manages search in the Analyst tool and Business Glossary Desktop.

By default, the Search Service returns search results from a Model repository, such as data objects, mapping specifications, profiles, reference tables, rules, scorecards, and business glossary terms. The search results can also include column profile results and domain discovery results from a profiling warehouse.

Note: When you create the Search Service, you do not associate it with any relational databases.

Associated Services

The Search Service connects to other application services within the domain.

When you create the Search Service, you can associate it with the following application services:

Analyst Service

The Analyst Service manages the connection to the Search Service that enables and manages searches in the Analyst tool. The Analyst Service determines the associated Search Service based on the Model Repository Service associated with the Analyst Service.

Data Integration Service

The Search Service connects to the Data Integration Service to return column profile and domain discovery search results from the profiling warehouse associated with the Data Integration Service. The Search Service determines the associated Data Integration Service based on the Model Repository Service.

Model Repository Service

The Search Service connects to the Model Repository Service to return search results from a Model repository. The search results can include data objects, mapping specifications, profiles, reference tables, rules, and scorecards. When you create the Search Service, you provide the name of the Model Repository Service.

Verify System Requirements

Verify that your planned domain meets the minimum system requirements for the installation process, temporary disk space, port availability, databases, and application service hardware.

For more information about product requirements and supported platforms, see the Product Availability Matrix on Informatica Network:https://network.informatica.com/community/informatica-network/product-availability-matrices

Verify the Distributions

You can verify the distributions for the supported products in the Hadoop environment.

Hadoop Environment

Informatica products integrate with the non-native environment. The integration varies by product, as do the requirements at installation.

Big Data Management, Big Data Streaming, Big Data Quality, and PowerCenter supports the following Hadoop distributions:

- Amazon EMR
- Azure HDInsight
- Cloudera CDH
- Hortonworks HDP
- MapR

For the Informatica domain services, the non-native environment is not required at install time. Integrate the environments after installation.

In each release, Informatica adds, defers, and drops support for the non-native distribution versions. Informatica might reinstate support for deferred versions in a future release. To see a list of the latest supported versions, see the Product Availability Matrix on the Informatica Customer Portal: https://network.informatica.com/community/informatica-network/product-availability-matrices.

Verify Services Installation Requirements

Verify that your machine meets the minimum system requirements to install the Informatica services.

The following table lists the minimum memory and disk space required to install the Informatica services:

Operating System	RAM	Disk Space
Windows	6 GB	11 GB
AIX	6 GB	13 GB
Linux	6 GB	13 GB
Solaris	6 GB	13 GB

Verify Temporary Disk Space Requirements

The installer writes temporary files to the hard disk. Verify that you have enough available disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

The installer requires 1 GB of temporary disk space.

Verify Port Requirements

The installer sets up the ports for components in the Informatica domain, and it designates a range of dynamic ports to use for some application services.

You can specify the port numbers to use for the components and a range of dynamic port numbers to use for the application services. Or you can use the default port numbers provided by the installer. Verify that the port numbers are available on the machines where you install the Informatica services.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

Guidelines for Port Configuration

The installer validates the port numbers that you specify to ensure that there will be no port conflicts in the domain.

Use the following guidelines to determine the port numbers:

- The port number you specify for the domain and for each component in the domain must be unique.
- The port number for the domain and domain components cannot be within the range of the port numbers that you specify for the application service processes.

- The highest number in the range of port numbers that you specify for the application service processes must be at least three numbers higher than the lowest port number. For example, if the minimum port number in the range is 6400, the maximum port number must be at least 6403.
- The port numbers that you specify cannot be lower than 1025 or higher than 65535.

Verify Database Requirements

Verify that the database server has adequate disk space for the domain configuration repository and for the other databases required by the application services.

The following table describes the database requirements for the domain configuration repository and for the other databases required by the application services:

Database	Requirements
Informatica domain configuration repository	The domain configuration repository supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle - Sybase ASE Allow 200 MB of disk space for the database.
Data object cache database	The data object cache database supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 200 MB of disk space for the database. Allocate more space based on the amount of data you want to cache.
Metadata Manager repository	The Metadata Manager repository supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 1 GB of disk space for the database.
Model repository	The Model repository supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 3 GB of disk space for DB2. Allow 200 MB of disk space for all other database types. Allocate more space based on the amount of metadata you want to store.
PowerCenter repository	The PowerCenter repository supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle - Sybase ASE Allow 35 MB of disk space for the database. Allocate more space based on the amount of metadata you want to store.

Database	Requirements
Profiling warehouse	The profiling warehouse supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 10 GB of disk space for the database.
Reference data warehouse	The reference data warehouse supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 200 MB of disk space for the database.
Workflow database	The workflow database supports the following database types: - IBM DB2 UDB - Microsoft SQL Server - Microsoft Azure SQL Database - Oracle Allow 200 MB of disk space for the database. Allocate space based on the amount of metadata you want to store.

Verify Application Service Hardware Requirements

Verify that the nodes in the domain have adequate hardware for the Service Manager and the application services that run on the nodes.

You can create an Informatica domain with one node and run all application services on the same node. If you create an Informatica domain with multiple nodes, you can run the application services on separate nodes. When you plan the application services for the domain, consider system requirements based on the services that you run on a node.

Note: Based on workload and concurrency requirements, you might need to optimize performance by adding cores and memory on a node.

The following table lists the minimum system requirements for a node based on some common configuration scenarios. Use this information as a guideline for other configurations in your domain.

Services	Processor	Memory	Disk Space
One node runs the following services: - Analyst Service - Content Management Service - Data Integration Service - Metadata Manager Service - Model Repository Service - PowerCenter Integration Service - PowerCenter Repository Service - Search Service - Web Services Hub	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following services: - Analyst Service - Content Management Service - Data Integration Service - Model Repository Service - Search Service	2 CPUs with multiple cores	12 GB	20 GB
One node runs the following service: - Analyst Service	1 CPU with multiple cores	4 GB	n/a
One node runs the following service: - Search Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Analyst Service - Search Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Metadata Manager Service - PowerCenter Integration Service - PowerCenter Repository Service	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: - Metadata Manager Service - PowerCenter Integration Service - PowerCenter Repository Service	2 CPUs with multiple cores	8 GB	10 GB
One node runs the following services: - PowerCenter Integration Service - PowerCenter Repository Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Data Integration Service - Model Repository Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following services: - Data Integration Service - Content Management Service	1 CPU with multiple cores	4 GB	10 GB
One node runs the following service: - Metadata Manager Service	1 CPU with multiple cores	4 GB	10 GB

Services	Processor	Memory	Disk Space
One node runs the following service component: - Metadata Manager Agent	1 CPU with multiple cores	4 GB	400 MB
One node runs the following service: - Web Services Hub	1 CPU with multiple cores	4 GB	5 GB

Record the Informatica Domain and Node Information

When you install the Informatica services, you need to know information about the domain, nodes, application services, and databases that you plan to create. If you plan to install the Informatica services on a network that uses Kerberos authentication, you also need to know information about the Kerberos authentication server.

Use the tables in this section to record the information that you need.

Domain Object Naming Conventions

Choose a naming convention to use for the domain, nodes, and application services when you plan the domain.

You cannot change domain, node, and application service names. Use names that continue to work if you migrate a node to another machine or if you add additional nodes and services to the domain. In addition, use names that convey how the domain object is used.

For more information about domain object naming conventions, see the following Informatica Velocity Best Practice article available on the Informatica Network: http://velocity.informatica.com/index.php/best-practices-all/139-configuration-management-and-security/708-infa-nam-conv.

The following table lists recommended naming conventions for domain objects:

Object	Naming Convention	Examples
Domain	DMN, DOM, DOMAIN, _<ORG>_<ENV>	DOM_FIN_DEV (Finance Development) DOMAIN_ICC_PD (Integration Competency Center Production)
Node	Node<node##>_<ORG>_<optional distinguisher>_<ENV>	Node01_ICC_DEV Node07_FIN_REVENUE_DV
Analyst Service	AS_<ORG>_<ENV>	AS_FIN_DEV
Content Management Service	CMS_<ORG>_<ENV>	CMS_FIN_DEV

Object	Naming Convention	Examples
Data Integration Service	DIS_<ORG>_<ENV>	DIS_ICC_DEV
Metadata Manager Service	MM, MMS _<ORG>_<ENV>	MM_ICC_DEV
Model Repository Service	MRS_<ORG>_<ENV>	MRS_FIN_DEV
PowerCenter Integration Service	PCIS, IS _<ORG>_<ENV>	PCIS_FIN_DEV
PowerCenter Repository Service	PCRS, RS _<ORG>_<ENV>	PCRS_FIN_QA
Search Service	SCH_<ORG>_<ENV>	SCH_ORG_PROD
Web Services Hub	WS, WSH, WSHUB_<ORG>_<ENV>	WSH_ICC_PROD

Domain

The first time that you install the Informatica services, you create the master gateway node and the Informatica domain.

Use the following table to record the domain information that you need:

Domain Information	Description	Value
Domain name	Name of the domain that you plan to create. The name must not exceed 128 characters and must be 7-bit ASCII only. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /	
Master gateway node host name	Fully qualified host name of the machine on which to create the master gateway node. If the machine has a single network name, use the default host name. The node host name cannot contain the underscore (_) character. If the machine has multiple network names, you can modify the default host name to use an alternate network name. If the machine has a single network name, use the default host name. **Note:** Do not use localhost. The host name must explicitly identify the machine.	
Master gateway node name	Name of the master gateway node that you plan to create on this machine. The node name is not the host name for the machine.	

Nodes

When you install the Informatica services, you add the installation machine to the domain as a node. You can add multiple nodes to a domain.

Use the following table to record the node information that you need:

Node Information	Description	Value for Node1	Value for Node2	Value for Node3
Node host name	Fully qualified host name of the machine on which to create the node. If the machine has a single network name, use the default host name. The node host name cannot contain the underscore (_) character. If the machine has multiple network names, you can modify the default host name to use an alternate network name. If the machine has a single network name, use the default host name. **Note:** Do not use localhost. The host name must explicitly identify the machine.			
Node name	Name of the node that you plan to create on this machine. The node name is not the host name for the machine.			

Application Services

The application services that you create depend on the license key generated for your organization.

Important: If you plan to use Kerberos authentication, you must know the application service and node name before you create the keytab files.

Use the following table to record the application services that you need in the domain and to record the nodes that will run the application services:

Application Service	Service Name	Node Name
Analyst Service		
Content Management		
Data Integration Service		
Metadata Manager Service		
Model Repository Service		
PowerCenter Integration Service		
PowerCenter Repository Service		
Search Service		
Web Services Hub		

Databases

When you plan the Informatica domain, you also need to plan the required relational databases. The domain requires a database to store configuration information and user account privileges and permissions. Some application services require databases to store information processed by the application service.

Domain

Use the following table to record the database information that you need for the domain:

Database Information	Description	Value
Domain configuration database type	Database type for the domain configuration repository. The domain configuration repository supports IBM DB2 UDB, Microsoft SQL Server, Oracle, or Sybase ASE.	
Domain configuration database host name	The name of the machine hosting the database.	

Content Management Service

Use the following table to record the database information that you need for the Content Management Service:

Database Information	Description	Value
Reference data warehouse database type	Database type for the reference data warehouse. The reference data warehouse supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Reference data warehouse database host name	The name of the machine hosting the database.	

Data Integration Service

Use the following table to record the database information that you need for the Data Integration Service:

Database Information	Description	Value
Data object cache database type	Database type for the data object cache database. The data object cache database supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Data object cache database host name	The name of the machine hosting the database.	
Profiling warehouse database type	Database type for the profiling warehouse. The profiling warehouse supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Profiling warehouse database host name	The name of the machine hosting the database.	

Database Information	Description	Value
Workflow database type	Database type for the workflow database. The workflow database supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Workflow database host name	The name of the machine hosting the database.	

Metadata Manager Service

Use the following table to record the database information that you need for the Metadata Manager Service:

Database Information	Description	Value
Metadata Manager repository database type	Database type for the Metadata Manager repository. The Metadata Manager repository supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Metadata Manager repository database host name	The name of the machine hosting the database.	

Model Repository Service

Use the following table to record the database information that you need for the Model Repository Service:

Database Information	Description	Value
Model repository database type	Database type for the Model repository. The Model repository supports IBM DB2 UDB, Microsoft SQL Server, or Oracle.	
Model repository database host name	The name of the machine hosting the database.	

PowerCenter Repository Service

Use the following table to record the database information that you need for the PowerCenter Repository Service:

Database Information	Description	Value
PowerCenter repository database type	Database type for the PowerCenter repository. The PowerCenter repository supports IBM DB2 UDB, Microsoft SQL Server, Oracle, or Sybase ASE.	
PowerCenter repository database host name	The name of the machine hosting the database.	

Secure Data Storage

When you install the Informatica services, you must provide a keyword for the installer to use to generate the encryption key for the domain.

Use the following table to record the information that you need to configure secure data storage:

Encryption Key Information	Description	Value
Keyword	Keyword to use to create a custom encryption key to secure sensitive data in the domain. The keyword must meet the following criteria: - From 8 to 20 characters long - Includes at least one uppercase letter - Includes at least one lowercase letter - Includes at least one number - Does not contain spaces The encryption key is created based on the keyword that you provide when you create the Informatica domain.	
Encryption key directory	Directory in which to store the encryption key for the domain. The default location is the following directory: `<Informatica installation directory>/isp/config/keys`.	

Domain Security

When you install the Informatica services, you can enable options in the Informatica domain to configure security for the domain.

Secure Communication for Services and the Service Manager

You can optionally configure secure communication between services and the Service Manager.

Important: If you choose to use your SSL certificates instead of the default certificates, you must provide information about the SSL certificates during the installation. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain.

Use the following table to record information about the keystore and truststore files that contain the SSL certificates you want to use:

Security Information	Description	Value
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.	
Keystore password	Password for the keystore infa_keystore.jks.	
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.	
Truststore password	Password for the infa_truststore.jks file.	

Secure Domain Configuration Repository Database

You can optionally create the domain configuration repository in a database that is secured with the SSL protocol.

Important: Access to the secure database requires a truststore that contains the certificates for the database.

Use the following table to record the information about the truststore file for the secure database:

Security Information	Description	Value
Database truststore file	Path and file name of the truststore file for the secure database.	
Database truststore password	Password for the truststore file.	

Secure Connection for the Administrator Tool

You can optionally configure a secure HTTPS connection for the Administrator tool.

Important: If you choose to use a keystore file that you create instead of the default file, you must provide information about the file during installation.

Use the following table to record information about the keystore file that you want to use:

Security Information	Description	Value
Keystore password	A plain-text password for the keystore file.	
Keystore file directory	Location of the keystore file.	

Kerberos Authentication

To configure the Informatica domain to run on a network that uses Kerberos authentication, you need information about the Kerberos authentication server.

Use the following table to verify and record information about the Kerberos authentication server:

Domain Information	Description	Value
Service realm name	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.	
User realm name	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.	
Location of the Kerberos configuration file	Directory where the Kerberos configuration file named *krb5.conf* is stored. Informatica requires specific properties to be set in the configuration file. If you do not have permission to copy or update the Kerberos configuration file, you might have to request the Kerberos administrator to update the file.	

CHAPTER 3

Prepare Databases for the Informatica Domain

This chapter includes the following topics:

Prepare Databases for the Informatica Domain Overview

Informatica stores data and metadata in repositories in the domain. Before you create the domain and the application services, set up the databases and database user accounts for the repositories.

Set up a database and user account for the following repositories:

- Domain configuration repository
- Data object cache repository
- Exception management audit database
- Metadata Manager repository
- Model repository
- PowerCenter repository
- Profiling warehouse
- Reference data warehouse

- Workflow database

To prepare the databases, verify the database requirements and set up the database. The database requirements depend on the application services that you create in the domain and the number of data integration objects that you build and store in the repositories.

Set Up Database User Accounts

Set up a database and user account for the domain configuration repository and for the repository databases associated with the applications services.

Use the following rules and guidelines when you set up the user accounts:

- The database user account must have permissions to create and drop tables, indexes, and views, and to select, insert, update, and delete data from tables.
- Use 7-bit ASCII to create the password for the account.
- To prevent database errors in one repository from affecting any other repository, create each repository in a separate database schema with a different database user account. Do not create a repository in the same database schema as the domain configuration repository or any other repository in the domain.
- If you create more than one domain, each domain configuration repository must have a separate user account.

Domain Configuration Repository Database Requirements

Informatica components store metadata in relational database repositories. The domain stores configuration and user information in a domain configuration repository.

You must set up a database and user account for the domain configuration repository before you run the installation. The database must be accessible to all gateway nodes in the Informatica domain.

When you install Informatica, you provide the database and user account information for the domain configuration repository. The Informatica installer uses JDBC to communicate with the domain configuration repository.

The domain configuration repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- Sybase ASE

Allow 200 MB of disk space for the database.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- If the repository is in an IBM DB2 9.7 database, verify that IBM DB2 Version 9.7 Fix Pack 7 or a later fix pack is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- On the database, set the configuration parameters.

  The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

  In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

  In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

  The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

  For more information about updating the DynamicSections parameter, see Appendix D, “Updating the DynamicSections Parameter of a DB2 Database” on page 275.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
  To set the isolation level for the database, run the following commands:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following commands:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
  ```

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
  To set the isolation level for the database, run the following commands:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following commands:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
  ```

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the open_cursors parameter to 4000 or higher.
- Set the permissions on the view `$parameter` for the database user.
- Set the privileges for the database user to run *show parameter open_cursors* in the Oracle database. When you run the pre-installation (i10Pi) system check tool, i10Pi runs the command against the database to identify the OPEN_CURSORS parameter with the domain database user credentials.

  You can run the following query to determine the open cursors setting for the domain database user account:

  ```
  SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
  ```

- Verify that the database user has the following privileges:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Sybase ASE Database Requirements

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 16K or higher. You must set the page size to 16K as this is a one-time configuration and cannot be changed afterwards.
- Set the database locking configuration to use row-level locking.
  The following table describes the database locking configuration that you must set:

Database Configuration	Sybase System Procedure	Value
Lock scheme	sp_configure "lock scheme"	0, datarows

- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Turn ON the Sybase database option select into/bulkcopy/pllsort.
- Enable the "select" privilege for the sysobjects system table.
- Create the following login script to disable the default VARCHAR truncation:

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

  The login script is executed every time the user logs into the Sybase instance. The stored procedure sets the parameter at the session level. The sp_modifylogin system procedure updates "user_name" with the stored procedure as its "login script". The user must have permission to invoke the stored procedure.

- Verify that the database user has CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, and CREATE VIEW privileges.
- Set the database configurations to the recommended baseline values.
  The following table lists the database memory configuration parameters that you must set:

Database Configuration	Sybase System Procedure	Value
Maximum amount of total physical memory	sp_configure "max memory"	2097151
Procedure cache size	sp_configure "procedure cache size"	500000
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	5000
Heap memory per user	sp_configure "heap memory per user"	49152
Number of locks	sp_configure "number of locks"	100000

Data Object Cache Database Requirements

The data object cache database stores cached logical data objects and virtual tables for the Data Integration Service. You specify the data object cache database connection when you create the Data Integration Service.

The data object cache database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 200 MB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the Data Integration Service.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

  CREATE INDEX

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  INSERT INTO TABLE

  UPDATE TABLE

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Model Repository Database Requirements

Informatica services and clients store data and metadata in the Model repository. Configure a separate Model repository to store monitoring statistics. Before you create the Model Repository Service, set up a database and database user account for the Model repository.

The Model repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 3 GB of disk space for DB2. Allow 200 MB of disk space for all other database types.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- If the repository is in an IBM DB2 9.7 database, verify that IBM DB2 Version 9.7 Fix Pack 7 or a later fix pack is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

  In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

  In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

  The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

  For more information about updating the DynamicSections parameter, see Appendix D, “Updating the DynamicSections Parameter of a DB2 Database” on page 275.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
  To set the isolation level for the database, run the following commands:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following commands:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
  ```

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```
- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
  To set the isolation level for the database, run the following commands:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following commands:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
  ```

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the open_cursors parameter to 2000 or higher.
- Verify that the database user has the following privileges:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

PowerCenter Repository Database Requirements

A PowerCenter repository is a collection of database tables containing metadata. A PowerCenter Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

The PowerCenter repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- Sybase ASE

Allow 35 MB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the PowerCenter Repository Service.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- To optimize repository performance, set up the database with the tablespace on a single node. When the tablespace is on one node, PowerCenter Client and PowerCenter Integration Service access the repository faster than if the repository tables exist on different database nodes.

  Specify the single-node tablespace name when you create, copy, or restore a repository. If you do not specify the tablespace name, DB2 uses the default tablespace.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Verify that the database user account has the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Verify that the database user account has the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.

  The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY:

  ```
  ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS
  UNLIMITED PCTINCREASE 50 );
  ```

  Verify or change the storage parameter for a tablespace before you create the repository.
- Verify that the database user has the following privileges:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Sybase ASE Database Requirements

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.
- Set the database memory configuration requirements.
  The following table lists the memory configuration requirements and the recommended baseline values:

Database Configuration	Sybase System Procedure	Value
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	8000
Number of locks	sp_configure "number of locks"	100000

Profiling Warehouse Requirements

The profiling warehouse database stores profiling and scorecard results. You specify the profiling warehouse connection when you create the Data Integration Service.

The profiling warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 10 GB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the Data Integration Service. You can specify a JDBC connection or Hive connection as a profiling warehouse connection for IBM DB2 UDB, Microsoft SQL Server, and Oracle database types.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- The database user account must have the CREATETAB, CONNECT, CREATE VIEW, and CREATE FUNCTION privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

Note: Informatica does not support the partitioned database environment for IBM DB2 databases when you use a JDBC connection as the profiling warehouse connection.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- The database user account must have the CONNECT, CREATE TABLE, CREATE VIEW, and CREATE FUNCTION privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- The database user account must have the CONNECT, CREATE TABLE, CREATE VIEW, and CREATE FUNCTION privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

  ALTER TABLE

  CREATE ANY INDEX

  CREATE PROCEDURE

  CREATE SESSION

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  UPDATE TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the tablespace parameter.
- Set the following parameters to the Informatica recommended values:

Parameter	Recommended Value
open_cursors	3000
Sessions	1000
Processes	1000

Reference Data Warehouse Requirements

The reference data warehouse stores the data values for reference table objects that you define in a Model repository. You configure a Content Management Service to identify the reference data warehouse and the Model repository.

You associate a reference data warehouse with a single Model repository. You can select a common reference data warehouse on multiple Content Management Services if the Content Management Services identify a common Model repository. The reference data warehouse must support mixed-case column names.

The reference data warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 200 MB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the Content Management Service.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Verify that the database user has SELECT privileges on the SYSCAT.DBAUTH and SYSCAT.DBTABAUTH tables.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

Microsoft Azure SQL Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

  ALTER SEQUENCE

  ALTER TABLE

  CREATE SEQUENCE

  CREATE SESSION

  CREATE TABLE

  CREATE VIEW

  DROP SEQUENCE

  DROP TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Workflow Database Requirements

The Data Integration Service stores run-time metadata for workflows in the workflow database. Before you create the workflow database, set up a database and database user account for the workflow database.

You specify the workflow database connection when you create the Data Integration Service.

The workflow database supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 200 MB of disk space for the database.

Note: Ensure that you install the database client on the machine on which you want to run the Data Integration Service.

IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Verify that the database user account has CREATETAB and CONNECT privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Set the connection pooling parameters.

The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository on Microsoft SQL Server:

- Verify that the database user account has CONNECT and CREATE TABLE privileges.
- Enable JTA and XA datasource functionality on the database.
- Set the connection pooling parameters.

  The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

  ALTER TABLE

  ALTER VIEW

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW

  DROP TABLE

  DROP VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the connection pooling parameters.

The following table lists the connection pooling parameters that you must set:

Parameter	Value
Maximum Connection Pool Size	128
Minimum Connection Pool Size	0
Maximum Idle Time	120 seconds

Configure Native Connectivity on Service Machines

To establish native connectivity between an application service and a database, install the database client software for the database that you want to access.

Native drivers are packaged with the database server and client software. Configure connectivity on the machines that need to access the databases. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries.

The following services use native connectivity to connect to different databases:

Data Integration Service

The Data Integration Service uses native database drivers to connect to the following databases:

- Source and target databases. Reads data from source databases and writes data to target databases.
- Data object cache database. Stores the data object cache.
- Profiling source databases. Reads from relational source databases to run profiles against the sources.
- Profiling warehouse. Writes the profiling results to the profiling warehouse.
- Reference tables. Runs mappings to transfer data between the reference tables and the external data sources.

When the Data Integration Service runs on a single node or on primary and back-up nodes, install database client software and configure connectivity on the machines where the Data Integration Service runs.

When the Data Integration Service runs on a grid, install database client software and configure connectivity on each machine that represents a node with the compute role or a node with both the service and compute roles.

PowerCenter Repository Service

The PowerCenter Repository Service uses native database drivers to connect to the PowerCenter repository database.

Install database client software and configure connectivity on the machines where the PowerCenter Repository Service and the PowerCenter Repository Service processes run.

PowerCenter Integration Service

The PowerCenter Integration Service uses native database drivers to connect to the following databases:

- Source and target databases. Reads from the source databases and writes to the target databases.
- Metadata Manager source databases. Loads the relational data sources in Metadata Manager.

Install database client software associated with the relational data sources and the repository databases on the machines where the PowerCenter Integration Service runs.

Install Database Client Software

You must install the database clients on the required machines based on the types of databases that the application services access.

To ensure compatibility between the application service and the database, use the appropriate database client libraries and install a client software that is compatible with the database version.

Install the following database client software based on the type of database that the application service accesses:

IBM DB2 Client Application Enabler (CAE)

Configure connectivity on the required machines by logging in to the machine as the user who starts Informatica services.

Microsoft SQL Server 2012 Native Client

Download the client from the following Microsoft website:
http://www.microsoft.com/en-in/download/details.aspx?id=29065.

Oracle client

Install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Sybase Open Client (OCS)

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

Configure Database Client Environment Variables on UNIX

Configure database client environment variables on the machines that run the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes.

The database client path variable name and requirements depend on the UNIX platform and the database.

After you configure the database environment variables, you can test the connection to the database from the database client.

The following table lists the database environment variables you need to set in UNIX:

Database	Environment Variable Name	Database Utility	Value
Oracle	ORACLE_HOME PATH	sqlplus	Set to: <*DatabasePath*> Add: <*DatabasePath*>/bin
IBM DB2	DB2DIR DB2INSTANCE PATH	db2connect	Set to: <*DatabasePath*> Set to: <*DB2InstanceName*> Add: <*DatabasePath*>/bin
Sybase ASE	SYBASE15 SYBASE_ASE SYBASE_OCS PATH	isql	Set to: <*DatabasePath*>/sybase<*version*> Set to: ${SYBASE15}/ASE-<*version*> Set to: ${SYBASE15}/OCS-<*version*> Add: ${SYBASE_ASE}/bin:${SYBASE_OCS}/bin:$PATH

Connection String to a Secure Database

If you create a repository on a secure database, you must provide the truststore information for the database and a JDBC connection string that includes the security parameters for the database.

During installation, you can create the domain configuration repository in a secure database. You can also create the Model repository in a secure database.

You can configure a secure connection to the following databases:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Note: You cannot configure a secure connection to a Sybase database.

When you configure the connection to the secure database, you must specify the connection information in a JDBC connection string. In addition to the host name and port number for the database server, the connection string must include security parameters.

The following table describes the security parameters that you must include in the JDBC connection string:

Parameter	Description
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. If SSL encryption and validation is enabled and this property is not specified, the driver uses the server name specified in the connection URL or data source of the connection to validate the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server.

You can use the following syntax in the JDBC connection string to connect to a secure database:

IBM DB2

```
jdbc:Informatica:db2://
host_name:port_no;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificate=D
B_host_name;ValidateServerCertificate=true_or_false
```

Oracle

```
jdbc:Informatica:oracle://
host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertificate=DB_
host_name;ValidateServerCertificate=true_or_false
```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;EncryptionMethod=SSL;Hos
tNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializable=tru
e;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertifi
cate=false
```

Note: The installer does not validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

CHAPTER 4

Prepare for Kerberos Authentication Setup

This chapter includes the following topics:

Prepare for Kerberos Authentication Setup Overview

You can configure the Informatica domain to use Kerberos network authentication to authenticate users, services, and nodes.

Kerberos is a network authentication protocol which uses tickets to authenticate access to services and nodes in a network. Kerberos uses a Key Distribution Center (KDC) to validate the identities of users and services and to grant tickets to authenticated user and service accounts. In the Kerberos protocol, users and services are known as principals. The KDC has a database of principals and their associated secret keys that are used as proof of identity. Kerberos can use an LDAP directory service as a principal database.

To use Kerberos authentication, you must install and run the Informatica domain on a network that uses Kerberos network authentication. Informatica can run on a network that uses Kerberos authentication with Microsoft Active Directory service as the principal database.

The Informatica domain requires keytab files to authenticate nodes and services in the domain without transmitting passwords over the network. The keytab files contain the service principal names (SPN) and associated encrypted keys. Create the keytab files before you create nodes and services in the Informatica domain.

Before you configure Kerberos authentication for the domain, perform the following tasks:

- Set up the Kerberos configuration file.
- Generate the service principal and keytab file names in the Informatica format.
- Review the SPN and keytab format text file.
- Request the Kerberos administrator to add the SPN to the Kerberos principal database and create the keytab files.

Determine the Kerberos Service Principal Level

When you prepare to enable Kerberos authentication, you must determine the required service principal level. The required service principal level determines the procedures you must follow to prepare to enable Kerberos authentication in the domain.

You can enable Kerberos authentication at one of the following levels:

Node Level

If you use the domain for testing or development, and the domain does not require a high level of security, you can enable Kerberos at the node level. You can use a single service principal name and a single keytab file for the node and for all of the processes and services that run on the node. You must also create a an SPN and a keytab file for the HTTP processes that run on the node.

Process Level

If you use the domain for production, and the domain requires a high level of security, you can set the service principal at the process level. You create a unique SPN and keytab file for each node and each process on the node. You must also create a an SPN and a keytab file for the HTTP processes that run on the node.

Kerberos enabled at the process level provides the highest level of security, but might be difficult to manage in an Informatica domain that contains many nodes or has many services. In this scenario, you might want to enable Kerberos at the node level.

Configure the Kerberos Configuration File

Set the properties required by Informatica in the Kerberos configuration file, and then copy the file to each node in the Informatica domain.

Kerberos stores configuration information in a file named *krb5.conf*. You must set the properties in the krb5.conf configuration file and then copy the file to every node in the Informatica domain.

If the domain uses Kerberos cross realm authentication, enter the required properties for each Kerberos realm.

1. Configure the following Kerberos library properties in the *libdefaults* section of the file.

   The following table describes the properties to enter:

Property	Description
default_realm	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. If the domain uses a single Kerberos realm for authentication, the service realm name and the user realm name must be the same.
forwardable	Allows a service to delegate client user credentials to another service. The Informatica domain requires application services to authenticate the client user credentials with other services. Set to true.

Property	Description
default_tkt_enctypes	Encryption types for the session key included in ticket-granting tickets (TGT). Set this property only if session keys must use specific encryption types. Ensure that the Kerberos Key Distribution Center (KDC) supports the encryption type that you specify. Do not set this property to allow the Kerberos protocol to select the encryption type to use. If the node hosts or Informatica client hosts use 256-bit encryption, install the Java Cryptography Extension (JCE) unlimited strength policy files on all node hosts and Informatica client hosts to avoid authentication issues.
rdns	Determines whether reverse name lookup is used in addition to forward name lookup to canonicalize host names for use in service principal names. Set to false.
renew_lifetime	The default renewable lifetime for initial ticket requests.
ticket_lifetime	The default lifetime for initial ticket requests.
udp_preference_limit	Determines the protocol that Kerberos uses when it sends a message to the KDC. Set to 1 to use the TCP protocol if the domain experiences intermittent Kerberos authentication failures.

2. Define each Kerberos realm in the *realms* section of the file.

   The following example shows the entry for a Kerberos realm named COMPANY.COM:

   ```
   [realms]
   COMPANY.COM = {...}
   ```

3. Enter the following realm properties inside the brackets for each Kerberos realm in the *realms* section of the file.

   The following table describes the properties to enter:

Property	Description
admin_server	The name or IP address of the Kerberos administration server host. You can include an optional port number, separated from the host name by a colon. Default is 749.
kdc	The name or IP address of a host running the Key Distribution Center (KDC) for the realm. You can include an optional port number, separated from the host name by a colon. Default is 88.

   The following example shows the entries for each Kerberos realm in a Kerberos cross realm configuration:

   ```
   [realms]
   COMPANY.COM = {
   admin_server = KDC01.COMPANY.COM:749
   kdc = KDC01.COMPANY.COM:88
   }
   EAST.COMPANY.COM = {
   kdc = 10.75.141.193
   admin_server = 10.75.141.193
   }
   WEST.COMPANY.COM = {
   kdc = 10.78.140.111
   ```

```
admin_server = 10.78.140.111
}
```

4. Map the Windows domains to the Kerberos realms in the *domain_realm* section of the file. The Windows domain name must be all lowercase. The Kerberos realm name must be all uppercase.

   The following example maps the company.com Windows domain to the COMPANY.COM Kerberos realm in a single Kerberos realm configuration:

   ```
   [domain_realm]
   .company.com = COMPANY.COM
   company.com = COMPANY.COM
   ```

   The following example maps multiple Windows domains to the corresponding Kerberos realms in a Kerberos cross realm configuration:

   ```
   [domain_realm]
   .company.com = COMPANY.COM
   company.com = COMPANY.COM
   .east.company.com = EAST.COMPANY.COM
   east.company.com = EAST.COMPANY.COM
   .west.company.com = WEST.COMPANY.COM
   west.company.com = WEST.COMPANY.COM
   ```

5. Copy the configuration file to the following directory on every node in the domain:

   ```
   <Informatica installation directory>\services\shared\security
   ```

The following example shows the content of a Kerberos configuration file with the required properties for a single Kerberos realm configuration:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
```

The following example shows the content of a Kerberos configuration file with the required properties for a Kerberos cross realm configuration:

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
```

```
admin_server = 10.78.140.111

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM
```

For more information about the Kerberos configuration file, see the Kerberos network authentication documentation.

Create Kerberos Principal Accounts in Active Directory

Create LDAP user accounts for the Kerberos principals in Active Directory. A Kerberos principal is a process, service, or user within the Kerberos realm.

If you set the default_tkt_enctypes property in the krb5.conf configuration file to the 128-bit or 256-bit AES encryption types, configure each account to use the corresponding encryption type in Active Directory.

The accounts that you create depend on whether you enable Kerberos at the node level or at the process level.

Note: Account names can be a maximum of 20 characters in length.

Accounts Required at Node Level

Create the LDAP user accounts required to enable Kerberos authentication at the node level in Active Directory.

Create the following Kerberos principal accounts in Active Directory if you enable Kerberos at the node level:

Node processes

Create an account for each node that runs in the domain.

HTTP process

Create an account for the Informatica web applications that run on a node in the domain. Web applications that run on a node might include the Administrator tool, Informatica Analyst, and Catalog Administrator. Create a single account that is shared by all of the web applications that run on the node.

Bind User Distinguished Name (DN)

Create an LDAP bind user account that you use to synchronize the LDAP security domain that contains Kerberos user accounts with Active Directory.

Accounts Required at Process Level

Create the LDAP user accounts required to enable Kerberos authentication at the process level in Active Directory.

Create the following Kerberos principal accounts in Active Directory if you enable Kerberos at the process level:

Node processes

Create an account for each node that runs in the domain.

HTTP processes

Create an account for the Informatica web applications that run on a node in the domain. Web applications that run on a node might include Informatica Analyst and Catalog Administrator. Create a single account that is shared by all of the web applications that run on the node.

Informatica Administrator service

Create an account for the Administrator tool on each gateway node in the domain.

Informatica application services

Create an account for every Informatica application service that runs on each node in the domain.

Bind User Distinguished Name (DN)

Create an LDAP user account that you use to synchronize the LDAP security domain that contains Kerberos user accounts with Active Directory.

Generate the Service Principal Name and Keytab File Name Formats

Use the Informatica Kerberos SPN Format Generator utility to generate the service principal name (SPN) and keytab file name formats required to use Kerberos authentication. The Kerberos SPN Format Generator utility generates a text file named SPNKeytabFormat.txt that contains the correct format for the SPNs and keytab file names.

The SPN and keytab file name formats you generate depend on whether you enable Kerberos at the node level or at the process level.

Generate the Service Principal Name and Keytab File Name Formats at Node Level

Generate the formats for the SPNs and keytab file names required to enable Kerberos authentication at the node level.

The Informatica domain requires SPNs and keytab files for the following processes when you enable Kerberos authentication at the node level:

Node processes

Informatica requires an SPN and keytab file for every node in the domain. Kerberos uses the same service principal name and keytab to authenticate the Informatica application services that run on the node.

HTTP processes

Informatica requires an SPN and keytab file for the web applications that run on each node in the domain. Web applications that run on a node might include the Administrator tool, Informatica Analyst

and Catalog Administrator. Kerberos uses the same service principal name to authenticate all of the web applications that run on the node.

1. On a Windows Informatica node host, go to the directory that contains the SPNFormatGenerator.bat batch file:

   ```
   <Informatica installation directory>\tools\Kerberos
   ```

   On a UNIX Informatica node host, go to the directory that contains the SPNFormatGenerator.sh shell file:

   ```
   <Informatica installation directory>/tools/Kerberos
   ```

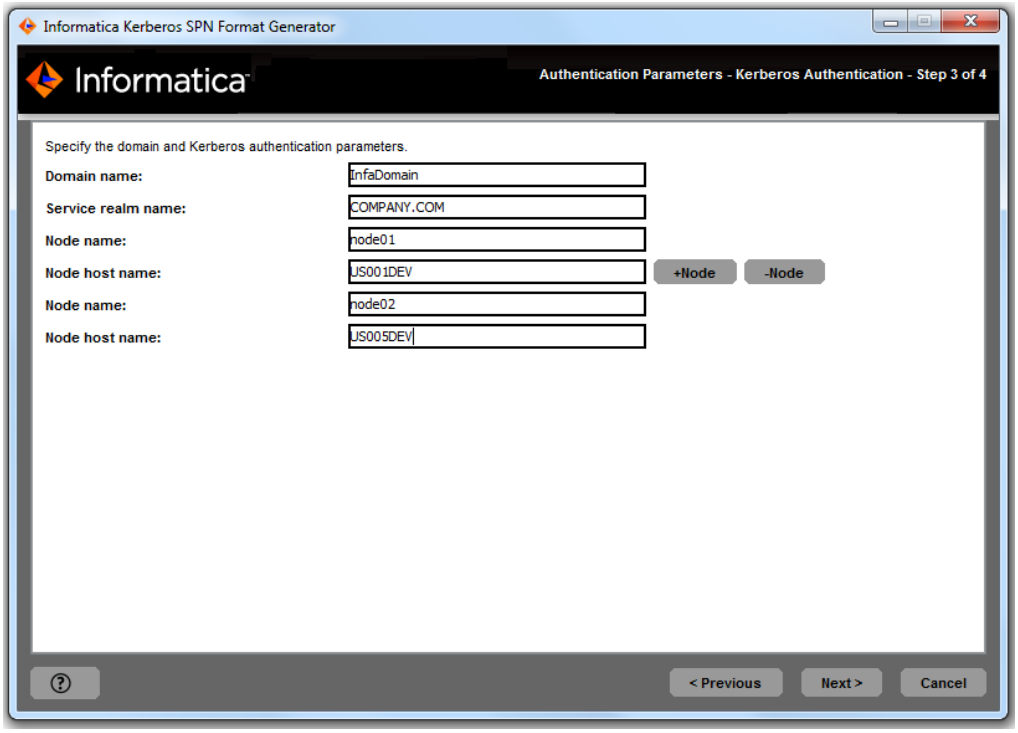
2. Run SPNFormatGenerator.bat or SPNFormatGenerator.sh.
3. Click **Next**.
4. Select **Node Level**.
5. Click **Next**.
6. Enter the properties required to generate the SPN and keytab file formats.

   The following table describes the properties:

Prompt	Description
Domain Name	Name of the Informatica domain. The name must not exceed 128 characters and must be 7-bit ASCII. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Service Realm Name	Name of the Kerberos realm. The realm name must be in uppercase.
Node Name	Name of the Informatica node.
Node Host Name	Fully qualified name of the node host. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the host.

7. To generate the SPN format for an additional node, click **+Node** and specify the node name and host name.

   The following image shows the entries for multiple nodes in the InfaDomain domain in the SPN Format Generator utility:



8. Click **Next**.

   The SPN Format Generator utility displays the path and file name of the file that contains the list of service principal names and keytab file names.

9. Click **Done** to exit the SPN Format Generator utility.

Generate the Service Principal Name and Keytab File Name Formats at Process Level

Generate the formats for the SPNs and keytab file names required to enable Kerberos authentication at the process level.

The Informatica domain requires SPNs and keytab files for the following processes and services when you enable Kerberos authentication at the process level:

Node processes

Informatica requires an SPN and keytab file for every node in the domain.

Informatica Administrator

Informatica requires an SPN and keytab file for the Administrator tool for every gateway node in the domain.

HTTP processes

Informatica requires an SPN and keytab file for the web applications that run on a node in the domain. Web applications that run on a node might include Informatica Analyst and Catalog Administrator.

Informatica application service processes

Informatica requires an SPN and keytab file for each Informatica application service that runs on every node in the domain.

1. On a Windows Informatica node host, go to the directory that contains the SPNFormatGenerator.bat batch file:

   ```
   <Informatica installation directory>\tools\Kerberos
   ```

   On a UNIX Informatica node host, go to the directory that contains the SPNFormatGenerator.sh shell file:

   ```
   <Informatica installation directory>/tools/Kerberos
   ```

2. Run SPNFormatGenerator.bat or SPNFormatGenerator.sh.
3. Click **Next**.
4. Select **Process Level**.
5. Click **Next**.
6. Enter the properties required to generate the SPN and keytab file formats.

   The following table describes the properties:

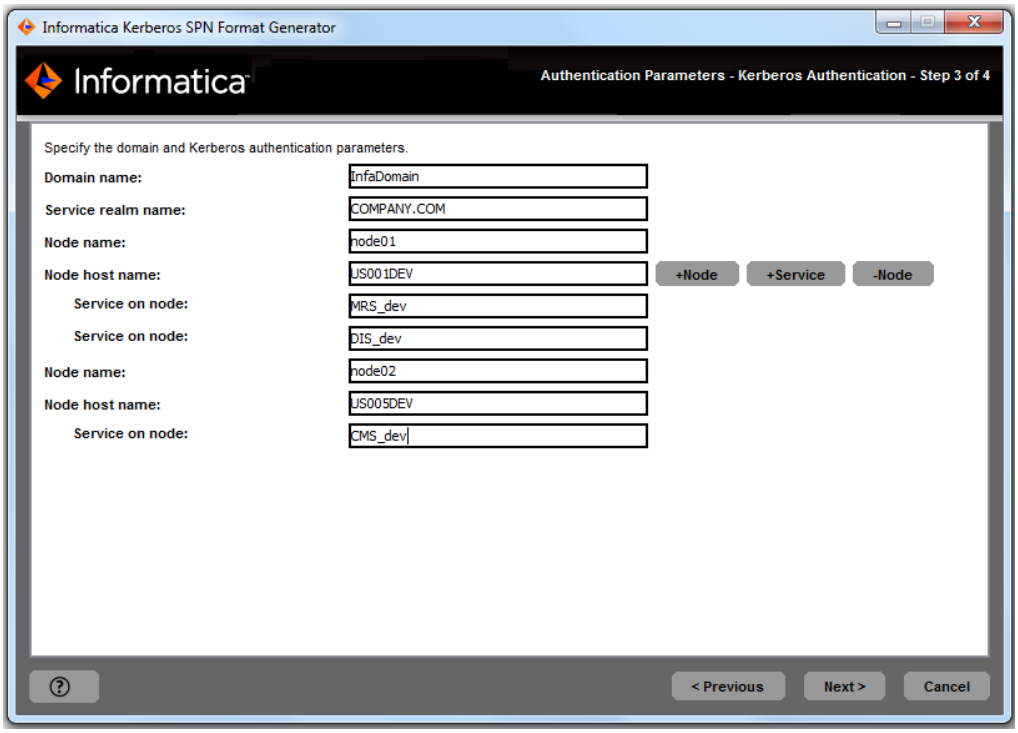
Prompt	Description
Domain Name	Name of the Informatica domain. The name must not exceed 128 characters and must be 7-bit ASCII. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Service Realm Name	Name of the Kerberos realm. The realm name must be in uppercase.
Node Name	Name of the Informatica node.
Node Host Name	Fully qualified name or the IP address of the node host. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the host.

7. To generate the SPN format for an Informatica application service that runs on a node, click **Service** after entering the node details.

   Enter the name of the Informatica application service as shown in the Administrator tool. Complete this step for each Informatica application service that runs on each node in the domain.

8. To generate the SPN format for an additional node, click **+Node** and specify the node name and host name.

   The following image shows the entries for multiple nodes and application services that run in the InfaDomain domain in the SPN Format Generator utility:



9. Click **Next**.

   The SPN Format Generator utility displays the path and file name of the file that contains the list of service principal names and keytab file names.

10. Click **Done** to exit the SPN Format Generator utility.

Review the Service Principal Name and Keytab File Name Format Text File

After you generate the SPNKeytabFormat.txt file, you can review the file.

You use the information in the file to generate the keytab files, and to associate each SPN with the corresponding principal user account in Active Directory.

The SPNKeytabFormat.txt file contains the following information:

Entity Name

Identifies the node or service associated with the process.

Service Principal Name

Format for the SPN. The SPN is case sensitive.

Note: If you enter a string containing multiple Kerberos domain names, or add an asterisk before a realm suffix to include all realms that include the suffix, the SPN format does not include the realm name.

The following table describes the SPN formats:

Keytab type	SPN Format
NODE_SPN	isp/<node name>/<domain name>@<REALM NAME>
NODE_AC_SPN	_AdminConsole/<node name>/<domain name>@<REALM NAME>
NODE_HTTP_SPN	HTTP/<node host name>@<REALM NAME> **Note:** The Kerberos SPN Format Generator validates the node host name. If the node host name is not valid, the utility does not generate an SPN. Instead, it displays the following message: Unable to resolve host name.
SERVICE_PROCESS_SPN	<application service name>/<node name>/<domain name>@<REALM NAME>

Keytab File Name

Format for the name of the keytab file to be created for the associated SPN. The keytab file name is case sensitive.

The following table describes the keytab file name formats:

Keytab Type	Keytab File Name
NODE_SPN	<node name>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<application service name>.keytab

Service Principals at Node Level

The following image shows the contents of the SPNKeytabFormat.txt file generated for service principals at the node level:

```
ENTITY_NAME     SPN                                          KEY_TAB_NAME          KEY_TAB_TYPE
node01          isp/node01/InfaDomain@COMPANY.COM            node01.keytab         NODE_SPN
node01          HTTP/US001DEV.company.com@COMPANY.COM        webapp_http.keytab    NODE_HTTP_SPN
node02          isp/node02/InfaDomain@COMPANY.COM            node02.keytab         NODE_SPN
node02          HTTP/US005DEV.company.com@COMPANY.COM        webapp_http.keytab    NODE_HTTP_SPN
```

Service Principals at Process Level

The following image shows the contents of the SPNKeytabFormat.txt file generated for service principals at the process level:

```
ENTITY_NAME     SPN                                          KEY_TAB_NAME          KEY_TAB_TYPE
node01          isp/node01/InfaDomain@COMPANY.COM            node01.keytab         NODE_SPN
node01          _AdminConsole/node01/InfaDomain@COMPANY.COM  _AdminConsole.keytab   NODE_AC_SPN
node01          HTTP/US001DEV.company.com@COMPANY.COM        webapp_http.keytab    NODE_HTTP_SPN
node02          isp/node02/InfaDomain@COMPANY.COM            node02.keytab         NODE_SPN
node02          _AdminConsole/node02/InfaDomain@COMPANY.COM  _AdminConsole.keytab   NODE_AC_SPN
node02          HTTP/US005DEV.company.com@COMPANY.COM        webapp_http.keytab    NODE_HTTP_SPN
MRS_dev:node01  MRS_dev/node01/InfaDomain@COMPANY.COM        MRS_dev.keytab        SERVICE_PROCESS_SPN
DIS_dev:node01  DIS_dev/node01/InfaDomain@COMPANY.COM        DIS_dev.keytab        SERVICE_PROCESS_SPN
CAT_dev:node02  CAT_dev/node02/InfaDomain@COMPANY.COM        CAT_dev.keytab        SERVICE_PROCESS_SPN
```

Generate the Keytab Files

Generate the keytab files used to authenticate Informatica users and services.

You use the Microsoft Windows Server ktpass utility to generate a keytab file for each user account you created in Active Directory. You must generate the keytab files on a member server or on a domain controller within the Active Directory domain. You cannot generate keytab files on a workstation operating system such as Microsoft Windows 7.

To use ktpass to generate a keytab file, run the following command:

```
ktpass.exe -out  <keytab filename> -princ <service principal name> -mapuser <user
account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-
target <realm name>]
```

The following table describes the command options:

Option	Description
-out	The file name of the Kerberos keytab file to generate as shown under the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file.
-princ	The service principal name displayed under the `SPN` column in the SPNKeytabFormat.txt file. If the domain uses Kerberos cross realm authentication, the service principal name must be unique across all Kerberos realms.
-mapuser	The Active Directory user account to associate with the SPN. The account name can be a maximum of 20 characters.
-pass	The password set in Active Directory for the Active Directory user account, if applicable.
-crypto	Specifies the key types generated in the keytab file. Set to all to use all supported cryptographic types.
-ptype	The principal type. Set to KRB5_NT_PRINCIPAL.
-target	The name of the realm to which the Active Directory server belongs. Include this option if the following error occurs when you run the utility: DsCrackNames returned 0x2 in the name

The keytab files you generate depends on whether you enable Kerberos at the node level or at the process level.

Generate the Keytab Files at Node Level

When you run ktpass to generate the keytab files at the node level, you associate each Kerberos principal user account with the corresponding SPN in Active Directory.

The following table shows the association between the Kerberos principal user accounts and the SPNs shown in the example SPNKeytabFormat.txt file:

User Account	Keytab Type	Service Principal Name
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

You also create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

1. Create a keytab file for the Kerberos principal user account that you created for each node in Active Directory.

   Copy the keytab file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named nodeuser0:

   ```
   ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser
   nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

2. Create a keytab file for each HTTP process Kerberos principal user account that you created in Active Directory.

   If the domain uses Kerberos cross realm authentication, the principal user account can exist in any Kerberos realm the domain uses.

   Copy the keytab file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named httpuser01:

   ```
   ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
   httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

3. Create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

   Structure the value for the -princ option as <principal name>@<KERBEROS REALM>. The file name of the keytab file must be infa_ldapuser.keytab.

   The following example creates a keytab file for a service principal user account named ldapuser:

   ```
   ktpass.exe -out infa_ldapuser.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -
   crypto all -ptype KRB5_NT_PRINCIPAL
   ```

Generate the Keytab Files at Process Level

When you run ktpass to generate the keytab files at the process level, you associate each Kerberos principal user account with the corresponding SPN in Active Directory.

The following table shows the association between the Kerberos principal user accounts and the SPNs shown in the example SPNKeytabFormat.txt file:

User Account	Keytab Type	Service Principal Name
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/InfaDomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/InfaDomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/InfaDomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/InfaDomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/InfaDomain@COMPANY.COM

You also create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

1. Create a keytab file for the Kerberos principal user account that you created for each node in Active Directory.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named nodeuser01:

   ```
   ktpass.exe -out node01.keytab -princ isp/node01/InfaDomain/COMPANY.COM -mapuser
   nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

2. Create a keytab file for each HTTP process Kerberos principal user account that you created.

   If the domain uses Kerberos cross realm authentication, the principal user account can exist in any Kerberos realm the domain uses.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a Kerberos principal user account named httpuser01:

   ```
   ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser
   httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

3. Create a keytab file for each Administrator tool Kerberos principal user account that you created.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

The following example creates a keytab file for a Kerberos principal user account named admintooluser01:

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/InfaDomain@COMPANY.COM -mapuser admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. Create a keytab file for each Informatica application service Kerberos principal user account that you created.

   Copy the file name from the `KEY_TAB_NAME` column in the SPNKeytabFormat.txt file. Copy the service principal name from the `SPN` column in the SPNKeytabFormat.txt file.

   The following example creates a keytab file for a service Kerberos principal user account named MRSdevuser01:

   ```
   ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

5. Create a keytab for the LDAP bind user account that is used to access and search Active Directory during LDAP synchronization.

   Structure the value for the -princ option as principal_name@<KERBEROS REALM>. The file name of the keytab file must be infa_ldapuser.keytab.

   The following example creates a keytab file for a service principal user account named ldapuser:

   ```
   ktpass.exe -out infa_ldapuser.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
   ```

Verify the Service Principal Names and Keytab Files

You can use Kerberos utilities to verify that the SPNs and the keytab files are valid. You can also use the utilities to determine the status of the Kerberos Key Distribution Center (KDC).

You can use Kerberos utilities such as *kinit* and *klist* to view and verify the SPNs and keytab files. To use the utilities, ensure that the KRB5_CONFIG environment variable contains the path and file name of the Kerberos configuration file. For more information about running the Kerberos utilities, see the Kerberos documentation.

Use the following utilities to verify the SPNs and keytab files:

kinit

You can use the *kinit* utility to request a ticket-granting ticket (TGT) from the KDC and verify that a keytab file can be used to establish a Kerberos connection. If the keytab and specified SPN are valid, the command obtains a ticket, and then caches the ticket in the specified cache.

The kinit utility is available in the following directory on an Informatica node:

```
<Informatica installation directory>\java\jre\bin
```

To request a ticket-granting ticket for an SPN, run the following command:

```
kinit -c <cache name> -k -t <keytab file name> <service principal name>
```

The following output example shows the ticket-granting ticket created in the default cache for a specified keytab file and SPN:

```
Cache: \temp\krb
Using principal: isp/node01/InfaDomain/COMPANY.COM
Using keytab: node01.keytab
Authenticated to Kerberos v5
```

klist

You can use the *klist* utility to list the Kerberos principals and keys in a keytab file. To list the keys in the keytab file and the time stamp for the keytab entry, run the following command:

```
klist -k -t <keytab file name>
```

The following output example shows the principals in a keytab file:

```
Keytab name: FILE:node01.keytab
KVNO Timestamp         Principal
---- ----------------- --------------------------------------------------------
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
   3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
```

CHAPTER 5

Before You Install the Services on Windows

This chapter includes the following topics:

Before You Install the Services on Windows Overview

Before you install the Informatica services, set up the machine to meet the requirements to install and run the Informatica platform. If the machine where you install the Informatica services is not configured correctly, the installation can fail.

Read the Release Notes

Read the Release Notes for updates to the installation and upgrade process. You can also find information about known and fixed limitations for the release.

Review the Patch Requirements

Before you install the Informatica services, verify that the machine has the required operating system patches and libraries.

The following table lists the patches and libraries that the Informatica services require on a Windows platform:

Platform	Operating System	Operating System Patch
Windows x64	2016 64-bit	None required
Windows x64	2012 R2 64-bit	None required

Back Up the Data Transformation Files

Before installation, you must back up the Data Transformation files that were created under previous versions. After you complete the installation, copy the files to the new installation directories to get the same repository and custom global components as in the previous version.

The following table lists the files or directories that you must back up:

File or Directory	Default Location
Repository	<Informatica installation directory>\DataTransformation\ServiceDB
Custom Global Components directory (TGP files)	<Informatica installation directory>\DataTransformation\autoInclude\user
Custom Global Components directory (DLL and JAR files)	<Informatica installation directory>\DataTransformation\externLibs\user
Configuration file	<Informatica installation directory>\DataTransformation\CMConfig.xml
License file	<Informatica installation directory>\DataTransformation\CDELicense.cfg

Do not copy the Data Transformation Library files. Instead, install the Data Transformation Libraries again.

Review the Environment Variables

Configure the environment variables to work with the Informatica installation.

The following table describes environment variables to review on Windows:

Variable	Description
%TEMP%	Location of the temporary files created during installation. Informatica requires 1 GB disk space for temporary files. Configure the environment variable if you do not want to create temporary files in the default drive.
PATH	The installer appends file paths required by Informatica to the PATH environment variable. Verify that the length of the PATH environment variable does not exceed the system limits.

Create a System User Account

Create a system user account to perform the installation and to run the Informatica service. Verify that the user account that you use to install the Informatica services has write permission on the installation directory.

You can install Informatica with the user account logged in to the machine and run it under another user account. You can create a local account or a domain account to install Informatica or run the Informatica Windows service.

Note: To access a repository on Microsoft SQL Server that uses a Windows trusted connection, create a domain account.

The user accounts require the following permissions to run the installer or to run the Informatica Windows service:

- **Logged in user account.** The user account must be a member of the Administrators group and have the *Log on as a service* permission. Log in with this user account before you install Informatica.
- **Another user account.** The user account must be a member of the Administrators group and have Log on as a service and Act as operating system permissions. You do not have to log in with this user account before you install Informatica. During installation, you can specify the user account to run the Informatica Windows service.

Set Up Keystore and Truststore Files

When you install the Informatica services, you can configure secure communication for the domain and set up a secure connection to Informatica Administrator (the Administrator tool). If you configure these security options, you must set up keystore and truststore files.

Before you install the Informatica services, set up the files for secure communication within the Informatica domain or for a secure connection to the Administrator tool. To create the required files, you can use the following programs:

keytool

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

For more information about using keytool, see the documentation on the following web site: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website: https://www.openssl.org/docs/

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Secure Communication Within the Informatica domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

Note: The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

You imported the certificate into truststores.

You must have a truststore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystores and truststores are in the correct directory.

The keystore and truststore must be in a directory that is accessible to the installer.

For more information about how to create a custom keystore and truststore, see the Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain": https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

Secure Connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

The keystore is in the correct directory.

The keystore must be in a directory that is accessible to the installer.

Extract the Installer Files

The installer files are compressed and distributed as a zip file.

Use a zip utility to extract the installer files to a directory on your machine. Verify the zip utility version is compatible with the Windows operating system version. When you unzip the file, verify that the zip utility also extracts empty folders.

You can extract the installer files through FTP download. Download the Informatica installation zip file from the Informatica Electronic Software Download site to a directory on your machine and then extract the installer files.

Note: Make sure that you download the file to a local directory or a shared network drive that is mapped on your machine. You can then extract the installer files. However, you cannot run the installer from a mapped file. Copy the extracted files to a local drive and then run the installer.

Verify the License Key

Before you install the software, verify that you have the license key available.

You can get the license key in the following ways:

- Installation DVD. If you receive the installation files in a DVD, the license key file is included in the Informatica License Key CD.
- HTTP download. If you download the installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

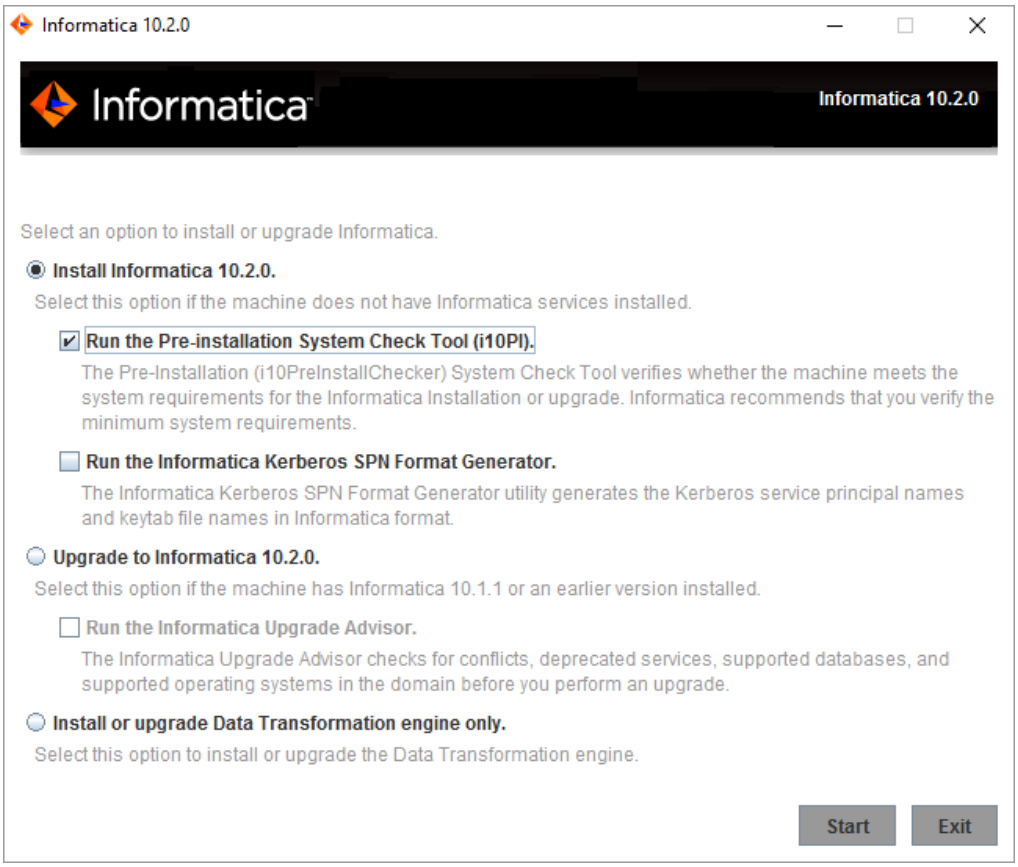
Contact Informatica Global Customer Support if you do not have a license key or if you have an incremental license key and you want to create a domain.

Run the Pre-Installation (i10Pi) System Check Tool

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation or upgrade.

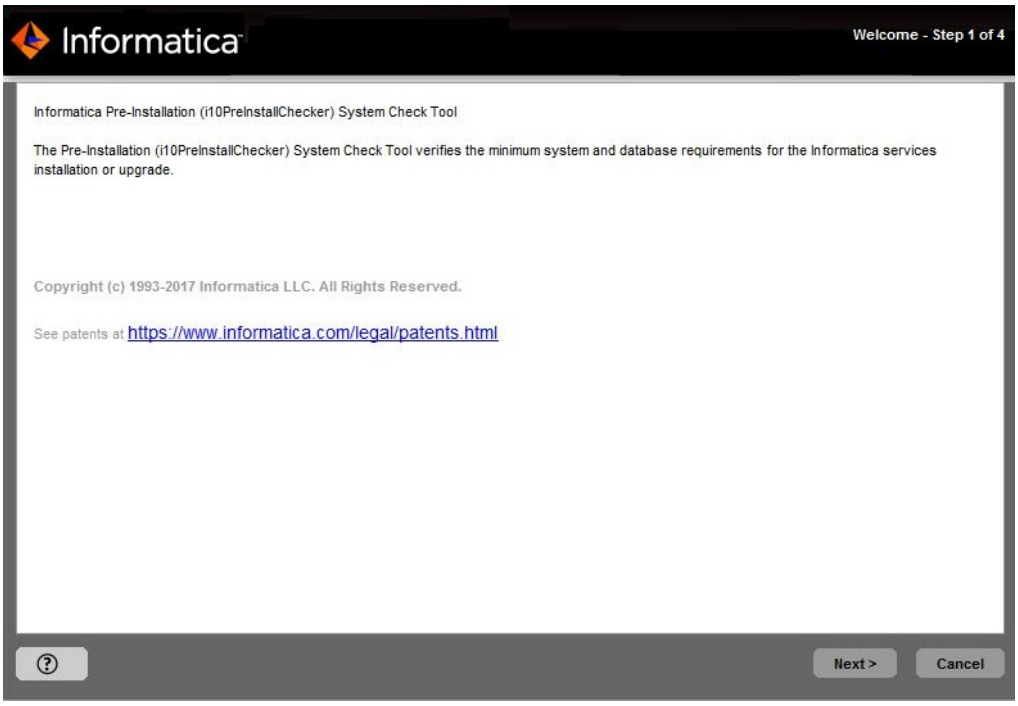
Ensure that you verified the system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Go to the root of the directory that contains the installation files and run install.bat as administrator.
4. Select **Install Informatica 10.2.0.**
5. Select **Run the Pre-Installation (i10Pi) System Check Tool** to verify whether the machine meets the system requirements for the installation or upgrade.



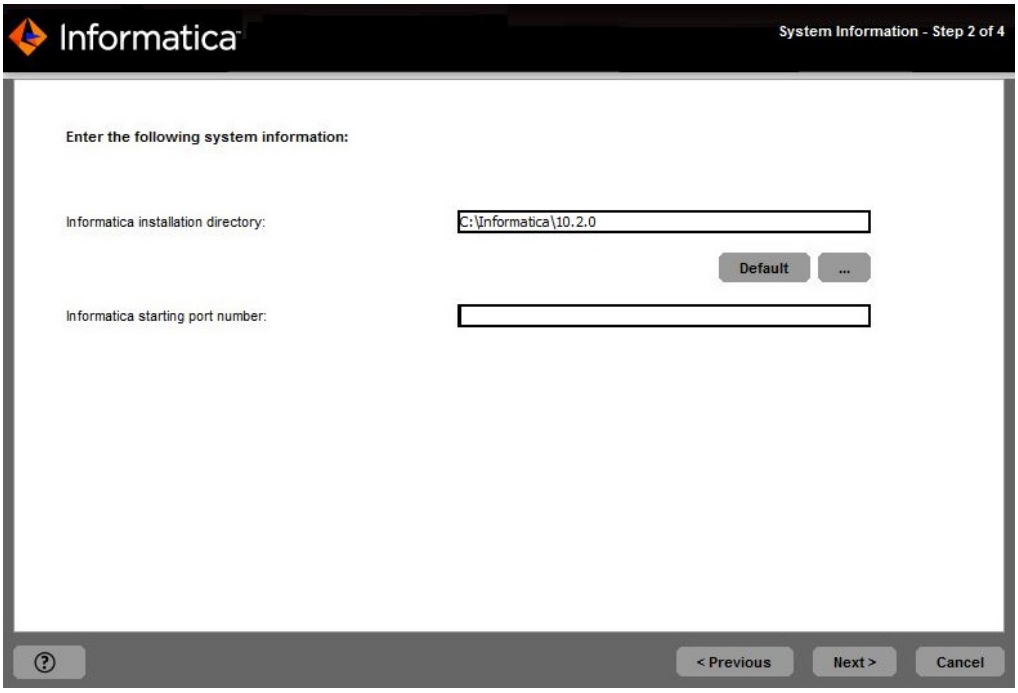
6. Click **Start**.

The Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** page appears.



7. Click **Next**.

   The **System Information** page appears.



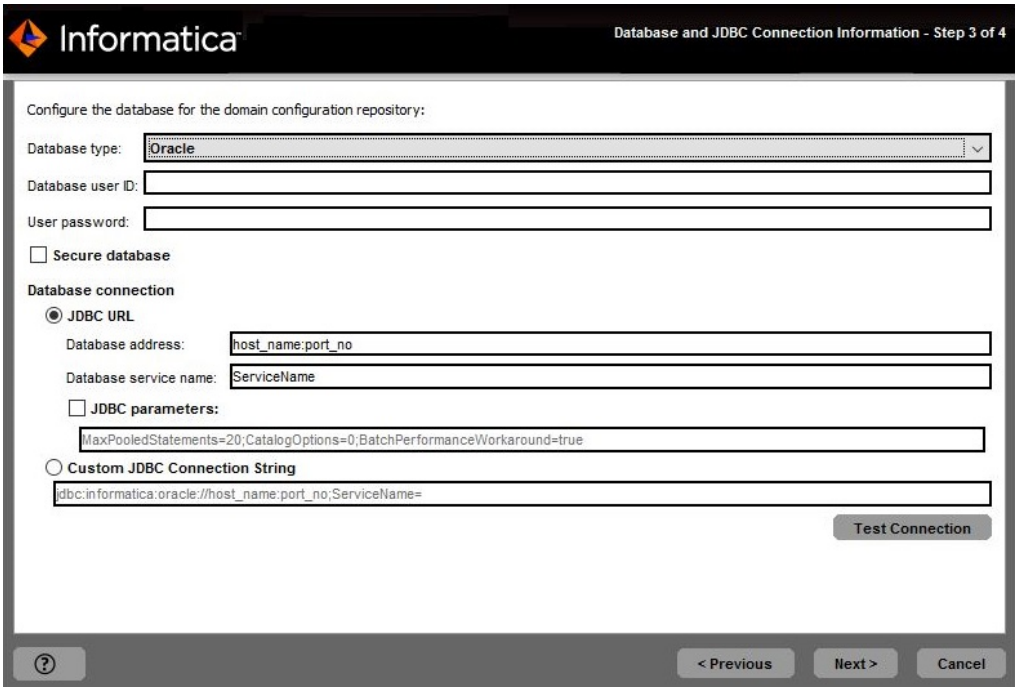
8. Enter the absolute path for the installation directory.

   The directory names in the path must not contain spaces or the following special characters: @ | * $ # ! % ( ) { } [ ] , ; '

Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

9. Enter the starting port number for the node that you will create or upgrade on the machine. The default port number for the node is 6005.
10. Click **Next**.

    The **Database and JDBC Connection Information** page appears.



11. Enter the information for the domain configuration repository database.

    The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Database user ID	User account for the repository database.
User password	Password for the database user account.

    The domain configuration repository must be accessible to all gateway nodes in the domain.

12. If you plan to use a secure database for the domain configuration repository, select the **Secure database** option.

13. Enter the database connection information.

- To enter the connection information using the JDBC URL information, select **JDBC URL** and specify the JDBC URL properties.
  The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format `host_name:port`.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL Database

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializa
  ble=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;Validat
  eServerCertificate=false
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.
- If you select the **Secure database** option, select **Custom JDBC connection string** and type the connection string.
  You must include the security parameters in addition to the connection parameters. For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

14. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
15. Click **Next** to start the system check.

The tool checks the settings of the hard drive, the availability of the ports, and the configuration of the database. After the system check is complete, the **System Check Summary** page appears, displaying the results of the system check.

16. Analyze the results of the system check.

    Each requirement is listed, along with one of the following check statuses:

    - [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
    - [Fail] - The requirement does not meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
    - [Information] - Verify the information and perform any additional tasks as outlined in the details.

    The results of the system check are saved to the following file: `.../Server/i10Pi/i10Pi/en/i10Pi_summary.txt`

17. Click **Done** to close the Pre-Installation (i10Pi) System Check Tool.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

Note: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

CHAPTER 6

Before You Install the Services on UNIX

This chapter includes the following topics:

Before You Install the Services on UNIX Overview

Before you install the Informatica services, set up the machine to meet the requirements to install and run the Informatica platform. If the machine where you install the Informatica services is not configured correctly, the installation can fail.

Read the Release Notes

Read the Release Notes for updates to the installation and upgrade process. You can also find information about known and fixed limitations for the release.

Review the Patch Requirements

Before you install the Informatica services, verify that the machine has the required operating system patches and libraries.

The following table lists the patches and libraries that the Informatica services require on a UNIX platform:

Platform	Operating System	Operating System Patch
AIX	7.1 TL4	OS level: 7100-04 bos.adt.debug Version 7.1.2.0
AIX	7.2 TL0	OS level: 7200-00 bos.adt.debug Version 7.2.0.0
Linux-x64	Red Hat Enterprise Linux 6.7	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el6 - keyutils-libs-<version>.el6 - libselinux-<version>.el6 - libsepol-<version>.el6
Linux-x64	Red Hat Enterprise Linux 7.3	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el7 - keyutils-libs-<version>.el7 - libselinux-<version>.el7 - libsepol-<version>.el7
Linux-x64	SUSE Linux Enterprise Server 11	Service Pack 4
Linux-x64	SUSE Linux Enterprise Server 12	Service Pack 2
Solaris	11	No patch required.
zLinux	Red Hat Enterprise Linux 6.9	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el6.s390 - keyutils-libs-<version>.el6.s390 - libselinux-<version>.el6.s390 - libsepol-<version>.el6.s390

Install the Java Runtime Environment

Informatica does not ship the Java libraries for AIX or zLinux. Before you install Informatica on AIX or zLinux, you must download and install the Java Runtime Environment (JRE). The required JRE version depends on the platform where you install Informatica.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or

implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Install the Java Runtime Environment for AIX

Informatica does not ship the Java libraries for AIX. Informatica services on AIX are certified on the following version:

Java(TM) SE Runtime Environment pap6480sr5fp30-20190207_01(SR5FP30)

Download the following file: `Java8_64.jre.8.0.0.530.tar`

If you have problems installing the JRE, contact the JRE vendor.

Note: You must install the Java Cryptography Extension (JCE) unlimited strength policy files on AIX machines that host Informatica services. Informatica does not ship the JCE policy files. For more information about downloading and installing the JCE policy files, see the JCE policy files at https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk.

Back Up the Data Transformation Files

Before installation, you must back up the Data Transformation files that were created under previous versions. After you complete the installation, copy the files to the new installation directories to get the same repository and custom global components as in the previous version.

The following table lists the files or directories that you must back up:

File or Directory	Default Location
Repository	<Informatica installation directory>\DataTransformation\ServiceDB
Custom Global Components directory (TGP files)	<Informatica installation directory>\DataTransformation\autoInclude\user
Custom Global Components directory (DLL and JAR files)	<Informatica installation directory>\DataTransformation\externLibs\user
Configuration file	<Informatica installation directory>\DataTransformation\CMConfig.xml
License file	<Informatica installation directory>\DataTransformation\CDELicense.cfg

Do not copy the Data Transformation Library files. Instead, install the Data Transformation Libraries again.

Review the Environment Variables

Configure the environment variables to work with the Informatica installation.

The following table describes the environment variables to review on UNIX:

Variable	Description
IATEMPDIR	Location of the temporary files created during installation. Informatica requires 1 GB disk space for temporary files. Configure the environment variable if you do not want to create temporary files in the /tmp directory.
INFA_JRE_HOME	Location of the folder containing the supported Java Runtime Environment (JRE).If you are installing Informatica on AIX, set the INFA_JRE_HOME environment variable. In the configuration file for your shell, for example the .bashrc file, set the INFA_JRE_HOME environment variable to the directory that contains the JRE. Verify that the login shell can access the INFA_JRE_HOME environment variable.
JRE_HOME	If you install the Informatica services on a UNIX machine, clear the JRE_HOME environment variable before you start the installation.
LANG and LC_ALL	Change the locale to set the appropriate character encoding for the terminal session. For example, set the encoding to `Latin1` or `ISO-8859-1` for French, `EUC-JP` or `Shift JIS` for Japanese, or `UTF-8` for Chinese or Korean. The character encoding determines the types of characters that appear in the UNIX terminal.
DISPLAY	Unset the DISPLAY environment before you run the installer. Installation might fail if the DISPLAY environment variable has some value.

Create a System User Account

Create a user account specifically to run the Informatica daemon.

Verify that the user account you use to install Informatica has write permission on the installation directory.

Set Up Keystore and Truststore Files

When you install the Informatica services, you can configure secure communication for the domain and set up a secure connection to Informatica Administrator (the Administrator tool). If you configure these security options, you must set up keystore and truststore files.

Before you install the Informatica services, set up the files for secure communication within the Informatica domain or for a secure connection to the Administrator tool. To create the required files, you can use the following programs:

keytool

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

For more information about using keytool, see the documentation on the following web site: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website: https://www.openssl.org/docs/

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Secure Communication Within the Informatica domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

Note: The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

You imported the certificate into truststores.

You must have a truststore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystores and truststores are in the correct directory.

The keystore and truststore must be in a directory that is accessible to the installer.

For more information about how to create a custom keystore and truststore, see the Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain": https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf

Secure Connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

The keystore is in the correct directory.

The keystore must be in a directory that is accessible to the installer.

Set the File Descriptor Limit

Verify that the operating system meets the file descriptor requirement.

Informatica service processes can use a large number of files. To prevent errors that result from the large number of files and processes, you can change system settings with the limit command if you use a C shell, or the ulimit command if you use a Bash shell.

To get a list of the operating system settings, including the file descriptor limit, run the following command:
C Shell

```
limit
```

Bash Shell

```
ulimit -a
```

Informatica service processes can use a large number of files. Set the file descriptor limit per process to 16,000 or higher. The recommended limit is 32,000 file descriptors per process.

To change system settings, run the limit or ulimit command with the pertinent flag and value. For example, to set the file descriptor limit, run the following command:
C Shell

```
limit -h filesize <value>
```

Bash Shell

```
ulimit -n <value>
```

Informatica services use a large number of user processes. Use the ulimit -u command to adjust the max user processes setting to a level that is high enough to account for all the processes required by Blaze. Depending on the number of mappings and transformations that might run concurrently, set the file descriptor limit per process to 16,000 or higher.

Run the following command to set the max user processes setting:
C Shell

```
limit -u processes <value>
```

Bash Shell

```
ulimit -u <value>
```

Configure POSIX Asynchronous I/O

If you install Informatica on IBM AIX, make POSIX Asynchronous I/O available on any node where you want to run a PowerCenter Integration Service. A PowerCenter Integration Service running on an IBM AIX machine can fail to start if POSIX Asynchronous I/O is not available.

Extract the Installer Files

The installer files are compressed and distributed as a tar file.

Use a native tar or GNU tar utility to extract the installer files to a directory on your machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on install.sh.

You can extract the installer files through FTP download. Download the Informatica installation tar file from the Informatica Electronic Software Download site to a directory on your machine and then extract the installer files.

Note: Make sure that you download the file to a local directory or a shared network drive that is mapped on your machine. You can then extract the installer files. However, you cannot run the installer from a mapped file. Copy the extracted files to a local drive and then run the installer.

Verify the License Key

Before you install the software, verify that you have the license key available.

You can get the license key in the following ways:

- Installation DVD. If you receive the installation files in a DVD, the license key file is included in the Informatica License Key CD.
- HTTP download. If you download the installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have a license key or if you have an incremental license key and you want to create a domain.

Run the Pre-Installation (i10Pi) System Check Tool

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation or upgrade.

Ensure that you verified the system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.

2. Close all other applications.
3. On a shell command line, run the install.sh file from the root directory.

   The installer displays the message to verify that the locale environment variables are set.
4. If the environment variables are not set, press **n** to exit the installer and set them as required.

   If the environment variables are set, press **y** to continue.
5. Press **1** to install or upgrade Informatica.
6. Press **1** to run the Pre-Installation (i10Pi) System Check Tool that verifies whether the machine meets the system requirements for the installation or upgrade.
7. From the Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** section, press **Enter**.

   The **System Information** section appears.
8. Type the absolute path for the installation directory.

   The directory names in the path must not contain spaces or the following special characters: @|* $ # ! % ( ) { } [ ] , ; '

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
9. Press **Enter**.
10. Enter the starting port number for the node that you will create or upgrade on the machine. The default port number for the node is 6005.
11. Press **Enter**.

    The **Database and Connection Information** section appears.
12. To enter the JDBC connection information using a custom JDBC connection string, press **1**. To enter the JDBC connection information using the JDBC URL information, press **2**.

    To connect to a secure database, you must enter the JDBC connection using a custom JDBC connection string.
13. Enter the JDBC connection information.
    - To enter the connection information using a custom JDBC connection string, type the connection string and specify the connection parameters.
      Use the following syntax in the JDBC connection string:
      IBM DB2

      ```
      jdbc:Informatica:db2://host_name:port_no;DatabaseName=
      ```

      Oracle

      ```
      jdbc:Informatica:oracle://host_name:port_no;ServiceName=
      ```

      Microsoft SQL Server

      ```
      jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
      ```

      Microsoft Azure SQL Database

      ```
      jdbc:Informatica:sqlserver://
      host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializa
      ble=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;Validat
      eServerCertificate=false
      ```

Sybase

```
jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.
  The following table describes the connection information:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following database types: - 1 - Oracle - 2 - Microsoft SQL Server - 3 - IBM DB2 - 4 - Sybase ASE
Database user ID	User ID for the database user account for the domain configuration repository.
Database user password	Password for the database user account.
Database host name	Host name for the database server.
Database port number	Port number for the database.
Database service name	Service name for Oracle and IBM DB2 databases or database name for Microsoft SQL Server and Sybase ASE.

- To connect to a secure database, select **1** to use a custom string and type the connection string. You must include the security parameters in addition to the connection parameters. For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

The tool checks the settings of the hard drive, the availability of the ports, and the configuration of the database. After the system check is complete, the **System Check Summary** section displays the results of the system check.

14. Analyze the results of the system check.

    Each requirement is listed, along with one of the following check statuses:

    - [Pass] - The requirement meets the criteria for the Informatica installation or upgrade.
    - [Fail] - The requirement does not meet the criteria for the Informatica installation or upgrade. Resolve the issue before you proceed with the installation or upgrade.
    - [Information] - Verify the information and perform any additional tasks as outlined in the details.

    The results of the system check are saved to the following file: `.../Server/i10Pi/i10Pi/en/i10Pi_summary.txt`

15. Press **Enter** to close the Pre-Installation (i10Pi) System Check Tool.

    You can continue to the Informatica service installation or upgrade immediately or end the system check and continue with the installation or upgrade later. If you continue to the installation or upgrade immediately, you do not have to restart the installer.

16. To continue to the Informatica service installation or upgrade immediately, press **y**.

    To end the system check and continue with the installation or upgrade later, press **n**.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again.

Note: If the Informatica Pre-Installation (i10Pi) System Check Tool check finishes with failed requirements, you can still perform the Informatica installation or upgrade. However, Informatica highly recommends that you resolve the failed requirements before you proceed.

Part III: Service Installation

This part contains the following chapters:

CHAPTER 7

Informatica Services Installation

This chapter includes the following topics:

Informatica Services Installation Overview

You can install the Informatica services on a Windows or UNIX machine. On Windows, you can run the installer in graphical or silent mode. On UNIX, you can run the installer in console or silent mode.

Complete the pre-installation tasks to prepare for the installation. You can install the Informatica services on multiple machines. The installation process creates a service named Informatica that runs as a service on Windows and as a daemon on UNIX. When you start the Informatica service, it starts the Service Manager, which manages all domain operations.

Optionally, you can create a Model Repository Service and a Data Integration Service during the installation process.

After installation, use Informatica Administrator to log in to the domain and create and configure the application services.

Create or Join a Domain

Create a domain if you are installing for the first time. Join a domain if you are installing on multiple machines and you have created a domain on another machine.

The Informatica domain is the fundamental administrative unit for services, users, and resources. A node is the logical representation of a single machine. A domain contains one or more nodes.

If you are installing on multiple machines, you can create multiple domains. If you create a domain, the node on the machine where you install becomes a gateway node in the domain. You can select the Enable Secure Communication option to set up secure communication between services within the domain.

When you install the Informatica services, you create a node on the machine. You can create a domain and add the node to the domain. If you do not create a domain, you can join the node to another domain.

If you join a domain, you can configure the node that you create to be a gateway node. When you create a gateway node, you can select enable a secure HTTPS connection to Informatica Administrator.

System Check Tool (i10Pi) and SPN Format Generator

Informatica provides utilities to facilitate the Informatica services installation process. You can use the Informatica installer to run the utilities.

Run the following utilities before you install Informatica services:

Pre-Installation (i10Pi) System Check Tool

The Pre-Installation (i10Pi) System Check Tool verifies whether a machine meets the system requirements for the Informatica installation. Informatica recommends that you verify the minimum system requirements before you start the installation.

Informatica Kerberos SPN Format Generator

The Informatica Kerberos SPN Format Generator generates a list of Kerberos service principal names (SPN) and keytab file names in the format required by Informatica. If you install Informatica on a network that uses Kerberos authentication, run this utility to generate the service principal and keytab file names in the informatica format. Then request the Kerberos administrator to add the SPNs to the Kerberos principal database and create the keytab files before you start the installation.

Secure Files and Directories

When you install or upgrade Informatica, the installer creates directories to store Informatica files that require restricted access, such as the domain encryption key file and the nodemeta.xml. On UNIX, the installer assigns different permissions for the directories and the files in the directories.

By default, the installer creates the following directories within the Informatica installation directory:

<Informatica installation directory>/isp/config

Contains the nodemeta.xml file. Also contains the /keys directory where the encryption key file is stored. If you configure the domain to use Kerberos authentication, the /keys directory also contains the Kerberos keytab files. You can specify a different directory in which to store the files. The installer assigns the same permissions to the specified directory as the default directory.

<Informatica installation directory>/services/shared/security

If you enable secure communication for the domain, the /security directory contains the keystore and truststore files for the default SSL certificates.

To maintain the security of the directories and files, the installer restricts access to the directories and the files in the directories. On UNIX, the installer assigns specific permissions to the group and user account that own the directories and files.

For more information about permissions assigned to the directories and files, see the *Informatica Security Guide*.

Installing the Informatica Services in Graphical Mode

You can install the Informatica services in graphical mode on Windows.

When you run the Pre-Installation (i10Pi) System Check Tool before you perform the installation, the installer sets the values for certain fields, such as the database connection and domain port numbers, based on the information you entered during the system check.

On Windows, if you encounter problems when you run the install.bat file from the root directory, run the following file: `<installer files directory>\server\install.exe`.

Important: If you install the Informatica services and the PowerCenter Client in the same install directory, the service binaries will be uninstalled when you uninstall the PowerCenter Client.

Creating a Domain

Create a domain if you are installing for the first time or if you want to administer nodes in separate domains.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Go to the root of the directory for the installation files and run install.bat as administrator.

   To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

   The **Informatica 10.2.0 HotFix 1** page appears.
4. Select **Install Informatica 10.2.0 HotFix 1**.

   Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

   - Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

     For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the Pre-Installation (i10Pi) System Check Tool" on page 82.
   - Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

     For more information about running the Informatica Kerberos SPN Format Generator, see GUID-D11D24A7-3CF3-4CFC-8B47-8A527CFA6F67.

   You can use the installer to run the utilities before you install informatica services. After you finish running a utility, restart the installer to run the next utility or install informatica services.
5. Click **Start**.
6. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

   Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.
7. Click **Next**.

   The **Installation Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.
8. Click **Next**.

   The **License and Installation Directory** page appears.
9. Enter the Informatica license key and the installation directory.

The following table describes the license key and directory that you specify for the informatica services installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: `@ | * $ # ! % ( ) { } [ ]` **Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

10. To configure the Informatica domain to run on a network with Kerberos authentication, select **Enable Kerberos Network Authentication**.
11. Click **Next**.

    If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** page appears.
    If you do not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Skip to 16.
12. On the **Network Security - Service Principal Level** page, select the level at which to set the Kerberos service principals for the domain.

    The following table describes the service principal levels that you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

13. Click **Next**.

    The **Network Security - Kerberos Authentication** page appears.
14. Enter the domain and keytab information required for Kerberos authentication.

The following table describes the Informatica domain and node information that you must provide:

Property	Description
Domain name	Name of the domain to create. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the node to create.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. **Note:** The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
User realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: *krb5.conf*

Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

15. Click **Next**.

    The **Pre-Installation Summary** page appears .

16. Review the installation information, and click **Install** to continue.

    The installer copies the Informatica files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

17. Select **Create a domain**.

    When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.

18. To set up secure communication between services in the domain, select **Enable secure communication for the domain**.

    By default, if you enable secure communication for the domain, the installer sets up an HTTPS connection for the Informatica Administrator. You can also create a domain configuration repository on a secure database.

19. To secure the connection to Informatica Administrator, select **Enable HTTPS for Informatica Administrator**.

    The following table describes the properties that you set for a secure connection to the Administrator tool:

Property	Description
Enable HTTPS for Informatica Administrator	Select this option to secure the connection to Informatica Administrator. To use an unsecure HTTP connection, clear the option. By default, if secure communication is enabled for the domain, the installer enables this option. You can also enable this option even if you do not enable secure communication for the domain.
Port	The port to use for communication between Informatica Administrator and the Service Manager.
Use a keystore file generated by the installer	Use a self-signed keystore file generated by the installer. The installer creates a keystore file named Default.keystore in the following location: `<Informatica installation directory>\tomcat\conf\`
Specify a keystore file and password	Use a keystore file that you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.
Keystore password	A plain-text password for the keystore file. Required if you use a keystore file that you create.
Keystore file	Path and file name of the keystore file. Required if you use a keystore file that you create.

20. To configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, **Enable SAML authentication**.

    Note: If you enabled Kerberos network authentication, you cannot configure SAML authentication.

21. Click **Next**.

    If you selected the **Enable SAML authentication** option, the **SAML Authentication** page appears.

22. Enter the Identity Provider URL for the domain.

23. Enter the identity provider assertion signing certificate alias name.

24. Specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

25. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore file:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.

26. Click **Next**.

    If you selected the **Enable secure communication for the domain** option, the **Domain Security - Secure Communication** page appears.
    If you did not enable secure communication for the domain, the **Domain Configuration Repository** page appears. Skip to step 30.

27. On the **Domain Security - Secure Communication** page, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. **Note:** If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Specify the location of the SSL certificate files	Use SSL certificates that you provide. You must specify the location of the keystore and truststore files. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

28. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

    The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

29. Click **Next**.

    The **Domain Configuration Repository** page appears.

30. On the **Domain Configuration Repository** page, enter the database and user account information for the domain configuration repository.

    The domain configuration repository stores metadata for domain operations and user authentication. The database must be accessible to all gateway nodes in the domain.

    The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Database user ID	User account for the repository database.
User password	Password for the database user account.

    If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enabled secure communication for the domain, you can create the domain configuration repository in a database secured with the SSL protocol. To create a secure domain configuration repository, select **Secure Database** and skip to step 32.

Note: You cannot configure a secure connection to a Sybase database.

31. Enter the database connection information.

    If you do not create a secure domain configuration repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

    - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.
      The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format `host_name:port`.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

    - To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string
      Use the following syntax in the JDBC connection string:
      IBM DB2

      ```
      jdbc:Informatica:db2://host_name:port_no;DatabaseName=
      ```

      Oracle

      ```
      jdbc:Informatica:oracle://host_name:port_no;ServiceName=
      ```

Microsoft SQL Server

```
jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
```

Microsoft Azure SQL Database

```
jdbc:Informatica:sqlserver://
host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializa
ble=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;Validat
eServerCertificate=false
```

Sybase

```
jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
```

Verify that the connection string contains all the connection parameters required by your database system.

.

32. If you selected the **Secure database** option to create a secure domain configuration repository, enter the connection information using a custom JDBC connection string.

    If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

    The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

    For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

33. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
34. Click **Next**.

    The **Domain Security - Encryption Key** page appears.
35. Enter the keyword and directory for the encryption key of the Informatica domain.

The following table describes the encryption key parameters that you must specify:

Property	Description
Keyword	Keyword to use to create a custom encryption key to secure sensitive data in the domain. The keyword must meet the following criteria: - From 8 to 20 characters long - Includes at least one uppercase letter - Includes at least one lowercase letter - Includes at least one number - Does not contain spaces The encryption key is created based on the keyword that you provide when you create the Informatica domain.
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: `<Informatica installation directory>/isp/config/keys`.

36. Click **Next**.

    The **Domain and Node Configuration** page appears.

37. Enter the information for the domain and the node that you want to create.

    The following table describes the properties that you set for the domain and gateway node:

Property	Description
Domain name	Name of the Informatica domain to create. The default domain name is Domain_<MachineName>. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: `` ` % * + ; " ? , < > \ / ``
Node name	Name of the node to create.
Node host name	Host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the a machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.
Node port number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.
Domain user name	User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines: - The name is not case sensitive and cannot exceed 128 characters. - The name cannot include a tab, newline character, or the following special characters: % * + / ? ; < > - The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.

Property	Description
Domain password	Password for the domain administrator. The password must be more than 2 characters and must not exceed 16 characters. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

38. To display the default ports for the domain and node components assigned by the installer, enable **Display advanced port configuration page**.

    If you display the port configuration page, the installer displays the default port numbers assigned to the domain and node. You can modify the port numbers or specify a different range of port numbers for the application service processes. If you do not select the display the port configuration page, the installer does not display the default port numbers and you cannot modify the assigned port numbers.

39. To create a Model Repository Service and a Data Integration Service during the installation, enable **Create Model Repository Service and Data Integration Service**.

    If you select to create the services, the installer creates a Model Repository Service and a Data Integration Service in the new domain. You must specify the database for the Model repository and configure the connection to the Data Integration Service. By default, the installer starts the services when the installation completes.

    If you do not configure the services, the installer does not create a Model Repository Service or a Data Integration Service in the new domain. You can create the services in the Administrator tool after installation.

    If you chose to create a Model Repository Service and a Data Integration Service, the **Model Repository Database** panel appears.

40. On the **Model Repository Service Database** page, enter the database and user account information for the Model repository.

    The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enabled secure communication for the domain, you can create the Model repository in a database secured with the SSL protocol. To create a secure Model repository, skip to step 42.

41. Enter the database connection information.

    If you do not create a secure Model repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

    - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.
      The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format `host_name:port`.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

42. To create a secure Model repository, enable **Secure database**.

    If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

    The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

    For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

43. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
44. To create a monitoring Model Repository Service, enable **Create monitoring Model Repository Service**.

    If you select to create the services, the installer creates a monitoring Model Repository Service in the new domain. You must specify the database for the monitoring Model repository. By default, the installer starts the services when the installation completes.

    If you do not configure the services, the installer does not create a monitoring Model Repository Service in the new domain. You can create the services in the Administrator tool after installation.

    If you chose to create a monitoring Model Repository Service, the **monitoring Model Repository Database** panel appears.
45. On the **monitoring Model Repository Service Database** page, enter the database and user account information for the Model repository.

The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enabled secure communication for the domain, you can create the Model repository in a database secured with the SSL protocol. To create a secure Model repository, skip to step 47.

46. Enter the database connection information.

    If you do not create a secure Model repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

    - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format `host_name:port`.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

47. To create a secure Model repository, enable **Secure database**.

    If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

    The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

    For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

48. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
49. Click **Next**.

If you selected to display the port configuration page, the installer displays the **Port Configuration** page appears.

If you did not select to display the port configuration page, the installer displays the **Windows Service Configuration** page. Skip to step 52.

50. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

    Verify that the port numbers you enter are not used by other applications.
    The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

51. Click **Next**.

    The installer displays the **Windows Service Configuration** page.

52. On the **Windows Service Configuration** page, select whether to run the Windows service under a different user account.

    The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

53. Click **Next**.

    If you selected to configure the Informatica application services, the installer displays the **Model Repository Service Database** page appears.

    If you did not select to create the services, the installer displays the **Post-Installation Summary** page. The **Post-Installation Summary** page indicates whether the installation completed successfully. Skip to step 62.

54. On the **Model Repository Service Database** page, enter the database and user account information for the Model repository.

    The following table describes the properties that you specify for the database and user account:

Property	Description
Database type	Database for the repository. Select one of the following databases: - Oracle - IBM DB2 - Microsoft SQL Server - Sybase ASE
Database user ID	User account for the repository database.
User password	Password for the database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multipartition database, select this option and specify the name of the tablespace that resides in the catalog partition of the database.

If you select Microsoft SQL Server, specify the schema for the repository tables and database connection:

Property	Description
Schema name	Name of the schema that will contain the repository tables. If not selected, the installer creates the tables in the default schema.
Trusted connection	Indicates whether to connect to Microsoft SQL Server through a trusted connection. Trusted authentication uses the security credentials of the current user to make the connection to Microsoft SQL Server. If not selected, the installer uses Microsoft SQL Server authentication.

If you enabled secure communication for the domain, you can create the Model repository in a database secured with the SSL protocol. To create a secure Model repository, skip to step 56.

55. Enter the database connection information.

    If you do not create a secure Model repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

    - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.
      The following table describes the JDBC URL properties that you specify:

Property	Description
Database address	Host name and port number for the database in the format `host_name:port`.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
JDBC parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

    - To enter the connection information using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

      IBM DB2

      ```
      jdbc:Informatica:db2://host_name:port_no;DatabaseName=
      ```

      Oracle

      ```
      jdbc:Informatica:oracle://host_name:port_no;ServiceName=
      ```

      Microsoft SQL Server

      ```
      jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=
      ```

      Verify that the connection string contains all the connection parameters required by your database system.

56. To create a secure Model repository, enable **Secure database**.

    If you create the repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

    The following table describes the properties you must set for a secure database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

    For information about the security parameters you must include in the JDBC connection for a secure database, see "Connection String to a Secure Database" on page 59.

57. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
58. Click **Next**.

    The **Application Service Parameters** page appears.

59. On the **Application Service Parameters** page, enter the name of the Model Repository Service and configure the Data Integration Service properties.

    The following table describes services parameters that you must set:

Port	Description
Model Repository Service name	Name of the Model Repository Service to create in the Informatica domain.
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: - HTTP. Requests to the service uses an HTTP connection. - HTTPS. Requests to the service uses a secure HTTP connection. - HTTP&HTTPS. Requests to the service can use either an HTTP or HTTPS connection.
HTTP port	Port number to used for the Data Integration Service. Default is 6030.

60. If you select an HTTPS connection, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure the connection to the Data Integration Service.

The following table describes the SSL certificate options for securing the Data Integration Service:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. **Note:** If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Enter the location of the SSL certificate files	Use SSL certificates that you provide. You must specify the location of the keystore and truststore files.

If you provide the certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file	Required. Path and file name of the keystore file that contains the private keys and SSL certificates for the database.
Keystore password	Required. Password for the keystore file for the secure database.
Truststore file	Required. Path and file name of the truststore file that contains the public key for the database.
Truststore password	Required. Password for the truststore file for the secure database.

61. Click **Next**.

    The installer creates the Model Repository Service and Data Integration Service and starts the services.

    The **Post-Installation Summary** page indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

62. Click **Done** to close the installer.

You can view the files to get more information about the tasks performed by the installer and to view configuration properties for the installed components.

Joining a Domain

You can join a domain if you are installing on multiple machines and you have created a domain on another machine.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Go to the root of the directory for the installation files and run install.bat as administrator.

   To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

   The **Informatica 10.2.0 HotFix 1** page appears.

4. Select **Install Informatica 10.2.0 HotFix 1**.

   Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

   - Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

     For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the Pre-Installation (i10Pi) System Check Tool" on page 82.

   - Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

     If you plan to join a domain that uses Kerberos authentication, you must generate the service principal names and keytab files for the node you create and service that will run on the node. For more information about running the Informatica Kerberos SPN Format Generator, see GUID-D11D24A7-3CF3-4CFC-8B47-8A527CFA6F67.

   You can use the installer to run the utilities before you install informatica services. After you finish running a utility, restart the installer to run the next utility or install informatica services.

5. Click **Start**.

6. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

   Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

7. Click **Next**.

   The **Installation Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.

8. Click **Next**.

   The **License and Installation Directory** page appears.

9. Enter the Informatica license key and the installation directory.

   The following table describes the license key and directory that you specify for the informatica services installation:

Property	Description
License key file	Path and file name of the Informatica license key.
Installation directory	Absolute path for the installation directory. The installation directory must be on the machine where you are installing Informatica. The directory names in the path must not contain spaces or the following special characters: `@ | * $ # ! % ( ) { } [ ]` **Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

10. To join an Informatica domain that runs on a network with Kerberos authentication, select **Enable Kerberos Network Authentication**.

11. Click **Next**.

If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** page appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Skip to step 16

12. On the **Network Security - Service Principal Level** page, select the service principal level of the domain that you plan to join.

    Note: All nodes in the domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

    The following table describes the service principal levels that you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

13. Click **Next**.

    The **Network Security - Kerberos Authentication** page appears.

14. Enter the domain and keytab information required for Kerberos authentication.

    The following table describes the information you must provide about the domain that you plan to join and the node to create during installation:

Property	Description
Domain name	Name of the domain to join. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the node to create.
Node host name	Fully qualified host name or IP address of the machine on which to create the node. **Note:** The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.

The following table describes the Kerberos realm and keytab information that you must provide:

Property	Description
Service realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
User realm name	Name of the Kerberos realm that the domain uses to authenticate users. The realm name must be in uppercase and is case-sensitive. To configure Kerberos cross realm authentication, specify the name of each Kerberos realm that the domain uses to authenticate users, separated by a comma. For example: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Use an asterisk as a wildcard character before a realm name to include all realms that include the name. For example: *EAST.COMPANY.COM
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: *krb5.conf*

15. Click **Next**.

    The **Pre-Installation Summary** page appears.

16. Review the installation information, and click **Install** to continue.

    The installer copies the Informatica files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

17. Select **Join a Domain**.

18. Specify whether the domain you want to join has secure communication enabled.

    To join a domain with secure communication enabled, select **Join a secure domain**. To join a domain that does not have secure communication enabled, clear the option.

19. Select the type of node that you want to create.

    To create a gateway node, select **Configure this node as a gateway**. To create a worker node, clear the option.

    If you configure the node as a gateway, you can enable a secure connection to the Informatica Administrator.

20. To secure the connection to Informatica Administrator, select **Enable HTTPS for Informatica Administrator**.

The following table describes the properties that you set for a secure connection to the Administrator tool:

Property	Description
Enable HTTPS for Informatica Administrator	Select this option to secure the connection to Informatica Administrator. To use an unsecure HTTP connection, clear the option. By default, if secure communication is enabled for the domain, the installer enables this option. You can also enable this option even if you do not enable secure communication for the domain.
Port	The port to use for communication between Informatica Administrator and the Service Manager.
Use a keystore file generated by the installer	Use a self-signed keystore file generated by the installer. The installer creates a keystore file named Default.keystore in the following location: `<Informatica installation directory>\tomcat\conf\`
Specify a keystore file and password	Use a keystore file that you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority.
Keystore password	A plain-text password for the keystore file. Required if you use a keystore file that you create.
Keystore file	Path and file name of the keystore file. Required if you use a keystore file that you create.

21. To configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, **Enable SAML authentication**.

    Note: If you enabled Kerberos network authentication, you cannot configure SAML authentication.

22. Click **Next**.

    If you selected the **Enable SAML authentication** option, the **SAML Authentication** page appears.

23. Enter the Identity Provider URL for the domain.
24. Enter the identity provider assertion signing certificate alias name.
25. Specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

26. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

The following table describes the location and password of the truststore file:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.

27. Click **Next**.

    If the domain you want to join is secure, the **Domain Security - Secure Communication** page appears. If the domain you want to join is not secure, the **Domain Configuration** page appears. Skip to step 29.

28. On the **Domain Security - Secure Communication** page, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    To use the default SSL certificates provided by Informatica, select **Use the default Informatica SSL certificate files**.

    To use your SSL certificate, select **Specify the location of the SSL certificate files** and specify the directories where the SSL certificate files are located.

    Note: All nodes in the domain must use the same SSL certificates. When you join a node to a domain, specify the same SSL certificates used by the gateway node in the domain.

    The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

    Click **Next**.

29. Enter the information for the domain that you want to join.

    The following table describes the properties that you specify for the domain:

Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.
Gateway node port	Port number of the gateway node.

Property	Description
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.

30. Click **Next**.

    The **Domain Security - Encryption Key** page appears.

31. Enter the encryption key information for the Informatica domain that you want to join.

    The following table describes the encryption key parameters that you must specify when you join a domain:

Property	Description
Select the encryption key	Path and file name of the encryption key for the Informatica domain that you want to join. All nodes in the Informatica domain use the same encryption key. You must specify the encryption key file created on the gateway node for the domain that you want to join. If you copied the encryption key file to a temporary directory to make it accessible to the nodes in the domain, specify the path and file name of the encryption key file in the temporary directory.
Encryption key directory	Directory in which to store the encryption key on the node created during this installation. The installer copies the encryption key file for the domain to the encryption key directory on the new node. By default, the encryption key is created in the following directory: `<Informatica installation directory>/isp/config/keys`.

32. Click **Next**.

    The **Join Domain Node Configuration** page appears.

33. Enter the information for the node you want to create.

    The following table describes the properties that you set for the node:

Property	Description
Node Host name	Host name for the node. The node host name cannot contain the underscore (_) character. **Note:** Do not use localhost. The host name must explicitly identify the machine.
Node name	Name of the Informatica node to create on this machine. The node name is not the host name for the machine.
Node port number	Port number for the node.

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database. Select the same database truststore file used by the master gateway node in the domain. Required if you join a gateway node to a domain that uses a secure domain configuration repository database.
Truststore password	Password for the database truststore file for the secure database. Required if you join a gateway node to a domain that uses a secure domain configuration repository database.

34. To display the default ports for the domain and node components assigned by the installer, select **Display advanced port configuration page**.

    If you display the port configuration page, the installer displays the default port numbers assigned to the domain and node. You can modify the port numbers or specify a different range of port numbers for the application service processes. If you do not select the display the port configuration page, the installer does not display the default port numbers and you cannot modify the assigned port numbers.

35. Click **Next**.

    If you selected to display the port configuration page, the installer displays the **Port Configuration** page.

    If you did not select to display the port configuration page, the installer displays the **Windows Service Configuration** page. Skip to step 38 .

36. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

    Verify that the port numbers you enter are not used by other applications.
    The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

37. Click **Next**.

38. On the **Windows Service Configuration** page, select whether to run the Windows service under a different user account.

    The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: <domain name>\<user account> This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

39. Click **Next**.

    The **Post-Installation Summary** page indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

40. Click **Done** to close the installer.

You can view the files to get more information about the tasks performed by the installer and to view configuration properties for the installed components.

Installing the Informatica Services in Console Mode

You can install the Informatica services in console mode on UNIX.

When you run the installer in console mode, the words Quit and Back are reserved words. Do not use them as input text.

When you run the Pre-Installation (i10Pi) System Check Tool before you perform the installation, the installer sets the values for certain fields, such as the database connection and domain port numbers, based on the information you entered during the system check.

Creating a Domain

Create a domain if you are installing for the first time or if you want to administer nodes in separate domains.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. On a shell command line, run the `install.sh` file from the root directory.

   The installer displays the message to verify that the locale environment variables are set.

4. If the environment variables are not set, press **n** to exit the installer and set them as required.

   If the environment variables are set, press **y** to continue.

5. Press **1** to install Informatica.

Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

- Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

  For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the Pre-Installation (i10Pi) System Check Tool" on page 82.

- Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

  For more information about running the Informatica Kerberos SPN Format Generator, see GUID-D11D24A7-3CF3-4CFC-8B47-8A527CFA6F67.

If you run the i10Pi System Check tool, you can run the Informatica Kerberos SPN Format Generator or run the Informatica services installation.

After you run the Informatica Kerberos SPN Format Generator, you can continue with the Informatica services installation. You cannot run the i10Pi System Check tool after you run the Informatica Kerberos SPN Format Generator.

6. Press **3** to run the Informatica service installation.

   The installer displays different options based on the platform you are installing on.

7. If you are installing on Linux, perform the following steps:

   a. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

      Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

   b. Press **1** to install Informatica services.

   c. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.

      Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.

      The **Installation Prerequisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

   d. Press **Enter** to continue.

   e. Enter the path and file name of the Informatica license key and press **Enter**.

   If you are installing on AIX and Solaris, perform the following steps:

   a. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

      Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

   b. The **Installation Prerequisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

   c. Press **Enter** to continue.

   d. Enter the path and file name of the Informatica license key and press **Enter**.

e. Enter the absolute path for the installation directory.

The directory names in the path must not contain spaces or the following special characters: @|* $ # ! % ( ) { } [ ] , ; ' Default is /home/toolinst.

Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

f. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.

Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.

8. Press **Enter**.

If you enabled Kerberos network authentication, the **Service Principal Level** section appears.
If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Skip to step 11.

9. On the **Service Principal Level** section, select the level at which to set the Kerberos service principals for the domain.

Note: All nodes in the domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

The following table describes the levels that you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

10. On the **Network Security - Kerberos Authentication** section, enter the parameters required for Kerberos authentication.

The following table describes the Kerberos authentication parameters that you must set:

Property	Description
Domain name	Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the Informatica node.

Property	Description
Node host name	Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the machine.
Service realm name	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
User realm name	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: *krb5.conf*

Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Informatica Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

11. Review the installation information and press **Enter** to continue.

    The installer copies the Informatica files to the installation directory.

12. Press **1** to create a domain.

    When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.

13. To enable secure communication for services in the domain, press **2**. To disable secure communication for the domain, press **1**.

    By default, if you enable secure communication for the domain, the installer sets up an HTTPS connection for the Informatica Administrator. You can also create a domain configuration repository on a secure database.

14. Specify the connection details for Informatica Administrator.

    a. If you do not enable secure communication for the domain, you can specify whether to set up a secure HTTPS connection for the Informatica Administrator.

The following table describes the options available to enable or disable a secure connection to Informatica Administrator:

Option	Description
Enable HTTPS for Informatica Administrator	Set up a secure connection to Informatica Administrator.
Disable HTTPS	Do not set up a secure connection to Informatica Administrator.

b. If you enable secure communication for the domain or if you enable HTTPS connection for the Informatica Administrator, enter the keystore file and port number for the HTTPS connection to Informatica Administrator.

The following table describes the connection information you must enter if you enable HTTPS:

Option	Description
Port	Port number for the HTTPS connection.
Keystore file	Select whether to use a keystore file generated by the installer or a keystore file you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority. 1 - Use a keystore generated by the installer 2 - Specify a keystore file and password If you select to use a keystore file generated by the installer, the installer creates a self-signed keystore file named Default.keystore in the following location: `<Informatica installation directory>/tomcat/conf/`

c. If you specify the keystore, enter the password and location of the keystore file.

If you enabled secure communication for the domain, the **Domain Security - Secure Communication** section appears. If you did not enable secure communication for the domain, the **Domain Configuration Repository** section appears. Skip to step 22.

15. Select whether to enable SAML authentication to configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain.

The following table describes the information you must enter to enable SAML authentication:

Prompt	Description
Enable SAML Authentication	Select whether to enable SAML Authentication: 1 - No 2 - Yes

16. Press **Enter**.
17. Enter the Identity Provider URL for the domain.
18. Enter the identity provider assertion signing certificate alias name.

19. Select whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

20. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore file:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.

21. In the Domain Security - Secure Communication section, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure domain communication.

    a. Select the type of SSL certificates to use.

       The following table describes the options for the SSL certificates that you can use to secure the Informatica domain:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. **Note:** If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Specify the location of the SSL certificate files	Use SSL certificates that you provide. You must specify the location of the keystore and truststore files. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

b. If you provide the SSL certificate, specify the location and passwords of the keystore and truststore files.

The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

The **Domain Configuration Repository** section appears.

22. Select the database to use for the domain configuration repository.

The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2 4 - Sybase ASE

The Informatica domain configuration repository stores metadata for domain operations and user authentication. The domain configuration repository must be accessible to all gateway nodes in the domain.

23. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the domain configuration database user account.
User password	Password for the domain configuration database user account.

24. Select whether to create a secure domain configuration repository.

You can create a domain configuration repository in a database secured with the SSL protocol. To create a domain configuration repository in a secure database, press 1 and skip to step 26.

To create a domain configuration repository in an unsecure database, press 2.

25. If you do not create a secure domain configuration repository, enter the parameters for the database.
    a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

       The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	Select whether to specify a tablespace: 1 - No 2 - Yes In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes.
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, if you select Yes to configure the tablespace, enter the name of the tablespace in which to create the tables. In a multi-partition database, specify the name of the tablespace that resides in the catalog partition of the database.

    b. If you select Microsoft SQL Server, enter the schema name for the database.

       The following table describes the properties that you must configure for the Microsoft SQL Server database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

    c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.
    d. Enter the JDBC connection information.
       - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.
         The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name. - Sybase ASE: Enter the database name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL Database

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSeria
  lizable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net
  ;ValidateServerCertificate=false
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

26. If you create a secure domain configuration repository, enter the parameters for the secure database.

    If you create the domain configuration repository on a secure database, you must provide the truststore information for the database. You must also provide a JDBC connection string that includes the security parameters for the database.

The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database truststore file	Path and file name of the truststore file for the secure database.
Database truststore password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

In addition to the host name and port number for the database server, you must include the following secure database parameters: You can use the following syntax for the connection strings:

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 the database server sends.

If this parameter is set to True, Informatica validates the certificate that the database server sends. 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 the database server sends. Informatica ignores any truststore information that you specify

Default is True.

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

Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server

- Oracle: `jdbc:Informatica:oracle://host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false`
- IBM DB2: `jdbc:Informatica:db2://host_name:port_no;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false`
- Microsoft SQL Server: `jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;EncryptionMethod=SSL;HostNameInCertificate=DB_host_name;ValidateServerCertificate=true_or_false`
- Microsoft Azure SQL Database: `jdbc:Informatica:sqlserver://host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSerializable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net;ValidateServerCertificate=false`

Note: The installer does not validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

27. If the database contains a domain configuration repository for a previous domain, select to overwrite the data or set up another database.

    The following table describes the options of overwriting the data or setting up another database when you create a domain configuration repository for a previous domain:

Option	Description
1 - OK	Enter the connection information for a new database.
2 - Continue	The installer overwrites the data in the database with new domain configuration.

28. In the **Domain Security - Encryption Key** section, enter the keyword and directory for the encryption key for the Informatica domain.

The following table describes the encryption key parameters that you must specify:

Property	Description
Keyword	Keyword to use to create a custom encryption key to secure sensitive data in the domain. The keyword must meet the following criteria: - From 8 to 20 characters long - Includes at least one uppercase letter - Includes at least one lowercase letter - Includes at least one number - Does not contain spaces The encryption key is created based on the keyword that you provide when you create the Informatica domain.
Encryption key directory	Directory in which to store the encryption key for the domain. By default, the encryption key is created in the following directory: `<Informatica installation directory>/isp/config/keys`.

The installer sets different permissions to the directory and the files in the directory. For more information about the permissions for the encryption key file and directory, see "Secure Files and Directories" on page 99.

29. Press **Enter** to select OK.

    The **Domain and Node Configuration** section appears.

30. Enter the information for the domain and the node that you want to create.

    The following table describes the properties that you set for the domain and gateway node.

Property	Description
Domain name	Name of the Informatica domain to create. The default domain name is Domain_<MachineName>. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: `` ` % * + ; " ? , < > \ / ``
Node name	Name of the node to create.
Node host name	Host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the a machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.
Node port number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.

Property	Description
Domain user name	User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines: - The name is not case sensitive and cannot exceed 128 characters. - The name cannot include a tab, newline character, or the following special characters: % * + / ? ; < >. - The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.
Domain password	Password for the domain administrator. The password must be more than 2 characters and must not exceed 16 characters. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.
Confirm password	Enter the password again to confirm. Not available if you configure the Informatica domain to run on a network with Kerberos authentication.

31. Select whether to display the default ports for the domain and node components assigned by the installer.

    The following table describes the advanced port configuration page:

Prompt	Description
Display advanced port configuration page	Select whether to display the port numbers for the domain and node components assigned by the installer: 1 - No 2 - Yes If you select Yes, the installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.

32. If you display the port configuration page, enter new port numbers at the prompt or press Enter to use the default port numbers.

    The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.

Port	Description
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

33. Select if you want to **Create the Model Repository Service and Data Integration Service**.

    The following table describes the option to configure the application services:

Prompt	Description
Create the Model Repository Service and Data Integration Service	Select whether you want to configure the Model Repository Service and Data Integration Service . 1 - Yes 2 - No If you select Yes, you can configure the application services. If you select No, you can configure the application services from the Administrator tool.

34. Select the database to configure Model repository.

    The following table lists the databases you can configure Model repository:

Prompt	Description
Database type	Type of database for the Model repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2

35. Enter the properties for the database user account.

    The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the Model repository database user account.
User password	Password for the domain configuration database user account.

36. Select whether to create a secure Model repository database.

    You can create a model repository service in a database secured with the SSL protocol. To create a model repository service in a secure database, press 1 and skip to step 3.

    To create a model repository service in an unsecured database, press 2.

37. If you chose not to create a secured Model repository, enter the parameters for the database.

    a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

    The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	Select whether to specify a tablespace: 1 - No 2 - Yes In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes.
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, if you select Yes to configure the tablespace, enter the name of the tablespace in which to create the tables. In a multi-partition database, specify the name of the tablespace that resides in the catalog partition of the database.

    b. If you select Microsoft SQL Server, enter the schema name for the database.

    The following table describes the properties that you must configure for the Microsoft SQL Server database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

    c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

    d. Enter the JDBC connection information.

    - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL Database

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSeria
  lizable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net
  ;ValidateServerCertificate=false
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

38. Select if you want to create a **monitoring Model Repository Service to monitor domain statistics**.

The following table describes the option to configure the monitoring Model repository:

Prompt	Description
Create a monitoring Model Repository Service	Select whether you want to create a monitoring Model Repository Service. 1 - Yes 2 - No If you select Yes, you can create a monitoring Model Repository Service. If you select No, you can create a monitoring Model Repository Service from the Administrator tool.

39. Select the database type for the monitoring Model repository.

    The following table lists the databases for the monitoring Model repository.

Prompt	Description
Database type	Type of database for the monitoring Model repository. Select from the following options: 1 - Oracle 2 - Microsoft SQL Server 3 - IBM DB2

40. Enter the properties for the database user account.

    The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the monitoring Model repository database user account.
User password	Password for the monitoring Model repository user account.

41. Select whether to create a secure monitoring Model repository database. You can create a monitoring Model repository in a database secured with the SSL protocol. To create a monitoring Model repository in a secure database, press 1 and skip to step 3.

    To create a monitoring Model repository in an unsecured database, press 2.

42. If you do not create a secure monitoring Model repository, enter the parameters for the database.

    a. If you select IBM DB2, select whether to configure a tablespace and enter the tablespace name.

The following table describes the properties that you must configure for the IBM DB2 database:

Property	Description
Configure tablespace	Select whether to specify a tablespace: 1 - No 2 - Yes In a single-partition database, if you select No, the installer creates the tables in the default tablespace. In a multi-partition database, you must select Yes.
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, if you select Yes to configure the tablespace, enter the name of the tablespace in which to create the tables. In a multi-partition database, specify the name of the tablespace that resides in the catalog partition of the database.

b. If you select Microsoft SQL Server, enter the schema name for the database.

The following table describes the properties that you must configure for the Microsoft SQL Server database:

Property	Description
Schema name	Name of the schema that will contain domain configuration tables. If this parameter is blank, the installer creates the tables in the default schema.

c. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

d. Enter the JDBC connection information.

- To enter the connection information using the JDBC URL information, specify the JDBC URL properties.
  The following table describes the database connection information:

Prompt	Description
Database host name	Host name for the database.
Database port number	Port number for the database.

Prompt	Description
Database service name	Service or database name : - Oracle: Enter the service name. - Microsoft SQL Server: Enter the database name. - IBM DB2: Enter the service name.
Configure JDBC Parameters	Select whether to add additional JDBC parameters to the connection string: 1 - Yes 2 - No If you select Yes, enter the parameters or press Enter to accept the default. If you select No, the installer creates the JDBC connection string without parameters.

- To enter the connection information using a custom JDBC connection string, type the connection string.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://host_name:port_no;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://host_name:port_no;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=
  ```

  Microsoft Azure SQL Database

  ```
  jdbc:Informatica:sqlserver://
  host_name:port_no;SelectMethod=cursor;DatabaseName=database_name;SnapshotSeria
  lizable=true;EncryptionMethod=SSL;HostNameInCertificate=*.database.windows.net
  ;ValidateServerCertificate=false
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://host_name:port_no;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

43. Press **Enter**.

    The **Service Parameters** section appears.

44. You can configure the service parameters for the application services.

Enter the following service parameter information:

Port	Description
Model Repository Service name	Name of the Model Repository Service to create in the Informatica domain.
Data Integration Service name	Name of the Data Integration Service to create in the Informatica domain.
monitoring Model Repository Service name	Name of the monitoring Model Repository Service to create in the Informatica domain.
HTTP protocol type	Type of connection to the Data Integration Service. Select one of the following options: - HTTP. Requests to the service uses an HTTP connection. - HTTPS. Requests to the service uses a secure HTTP connection. - HTTP&HTTPS. Requests to the service can use either an HTTP or HTTPS connection.
HTTP port	Port number to used for the Data Integration Service. Default is 9085.
HTTPS port	Port number to used for the Data Integration Service. Default is 9085.

45. Select the SSL certificates contained to secure the Data Integration Service.

Option	Description
Use the default Informatica SSL certificate files	Use the default Informatica SSL certificates contained in the default keystore and truststore. **Note:** If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Use custom SSL certificates	Use custom SSL certificates. You must specify the location of the keystore and truststore files. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

If you choose to use custom SSL certificates, enter the following information.

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

46. Select if you want to use the Spark engine to run Sqoop mappings or process a Java transformation.

Property	Description
Run Sqoop mappings or process a Java transformation	Select whether you want to use the Spark engine to run Sqoop mappings or process a Java transformation. 1 - Yes 2 - No If you select Yes, specify the the JDK home directory for the Data Integration Service. The JDK version that the Data Integration Service uses must be compatible with the JRE version on the cluster. If you select No, you can configure the JDK home directory property later when you want to use the Spark engine to run Sqoop mappings or process a Java transformation. For more information, see the *Informatica Big Data Management User Guide* and the *Informatica Big Data Management Hadoop Integration Guide*.

You can view the installation log files to get more information about the tasks performed by the installer and to view configuration properties for the installed components.

By default, the system services are disabled after the installation. You must enable them from the Administrator tool.

Joining a Domain

You can join a domain if you are installing on multiple machines and you have created a domain on another machine.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. On a shell command line, run the install.sh file from the root directory.

   The installer displays the message to verify that the locale environment variables are set.
4. If the environment variables are not set, press **n** to exit the installer and set them as required.

   If the environment variables are set, press **y** to continue.
5. Press **1** to install or upgrade Informatica.

Informatica provides utilities to facilitate the Informatica services installation process. Run the following utilities before you install Informatica services:

- Pre-Installation (i10Pi) System Check Tool. Verifies whether the machine on which you are installing Informatica services meets the system requirements for installation.

  For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the Pre-Installation (i10Pi) System Check Tool" on page 82.

- Informatica Kerberos SPN Format Generator. Creates a list of the Kerberos service principal names and keytab file names required to run Informatica services on a network with Kerberos authentication.

  For more information about running the Informatica Kerberos SPN Format Generator, see GUID-D11D24A7-3CF3-4CFC-8B47-8A527CFA6F67.

If you run the i10Pi System Check tool, you can run the Informatica Kerberos SPN Format Generator or run the Informatica services installation.

After you run the Informatica Kerberos SPN Format Generator, you can continue with the Informatica services installation. You cannot run the i10Pi System Check tool after you run the Informatica Kerberos SPN Format Generator.

6. Press **3** to run the Informatica services installation.
7. Press **1** to install Informatica services.

   The installer displays different options based on the platform you are installing on.
8. If you are installing on Linux, perform the following steps:
   a. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

      Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.

   b. Press **1** to install Informatica services.
   c. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.

      Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.

      The **Installation Prerequisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

   If you are installing on AIX, perform the following steps:

   a. Press **1** to configure the Informatica domain to run on a network that does not use Kerberos authentication.

      Press **2** to configure the Informatica domain to run on a network with Kerberos authentication.

      The **Installation Pre-Requisites** section displays the installation requirements. Verify that all requirements are met before you continue the installation.

   b. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.

      Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.
9. Press **Enter** to continue.

10. Type the path and file name of the Informatica license key and press **Enter**.
11. Type the absolute path for the installation directory.

    The directory names in the path must not contain spaces or the following special characters: @|* $ # ! % ( ) { } [ ] , ; ' Default is /home/toolinst.

    Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
12. Press **Enter**.

    If you enabled Kerberos network authentication, the **Service Principal Level** section appears.
    If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Skip to step 15.
13. On the **Service Principal Level** section, select the service principal level for the domain.

    Note: All nodes in the domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

    The following table describes the levels that you can select:

Level	Description
Process Level	Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
Node Level	Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

14. On the **Network Security - Kerberos Authentication** section, enter the parameters required for Kerberos authentication.

    The following table describes the Kerberos authentication parameters that you must set:

Property	Description
Domain name	Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
Node name	Name of the Informatica node.
Node host name	Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character. **Note:** Do not use *localhost*. The host name must explicitly identify the machine.

Property	Description
Service realm name	Name of the Kerberos realm to which the Informatica domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
User realm name	Name of the Kerberos realm to which the Informatica domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
Keytab directory	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
Kerberos configuration file	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: *krb5.conf*

15. Review the installation information and press **Enter** to continue.

    The installer copies the Informatica files to the installation directory.

16. Press **2** to join a domain.

    The installer creates a node on the machine where you install. You can specify the type of node to create and the domain to join.

17. Specify whether the domain you want to join has the secure communication option enabled.

    Press 1 to join an unsecure domain or press 2 to join a secure domain.

18. Select the type of node you want to create.

    The following table describes that types of nodes that you can create:

Property	Description
Configure this node as a gateway	Select whether to configure the node as a gateway or worker node. 1 - Yes 2 - No Select 1 to configure a gateway node or 2 to configure a worker node.

    If you configure the node as a gateway, you can enable a secure HTTPS connection to the Informatica Administrator.

19. Specify the connection details to Informatica Administrator.

    a. Specify whether to set up a secure HTTPS connection to the Informatica Administrator.

Option	Description
1 - Enable HTTPS for Informatica Administrator	Set up a secure connection to Informatica Administrator.
2 - Disable HTTPS	Do not set up a secure connection to Informatica Administrator.

b. If you enable HTTPS connection for the Informatica Administrator, enter the keystore file and port number to use to secure the connection.

Option	Description
Port	Port number for the HTTPS connection.
Keystore file	Select whether to use a keystore file generated by the installer or a keystore file you create. You can use a keystore file with a self-signed certificate or a certificate signed by a certification authority. 1 - Use a keystore generated by the installer 2 - Specify a keystore file and password If you select to use a keystore file generated by the installer, the installer creates a self-signed keystore file named Default.keystore in the following location: `<Informatica installation directory>/tomcat/conf/`

c. If you specify the keystore, enter the password and location of the keystore file.

If you enabled secure communication for the domain, the **Domain Security - Secure Communication** section appears. If you did not enable secure communication for the domain, the **Domain Configuration** section appears. Skip to step 27.

20. Select whether to enable SAML authentication to configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain.

    The following table describes the information you must enter to enable SAML authentication:

Prompt	Description
Enable SAML Authentication	Select whether to enable SAML Authentication: 1 - No 2 - Yes

21. Press **Enter**.
22. Enter the Identity Provider URL for the domain.
23. Enter the identity provider assertion signing certificate alias name.
24. Select whether to use the default Informatica SSL certificates or to use your SSL certificates to enable secure communication in the domain.

    The following table describes the SSL certificate options for SAML authentication:

Option	Description
Use the default Informatica SSL certificate file.	Select to use the default Informatica truststore file for SAML authentication.
Enter the location of the SSL certificate file.	Select to use a custom truststore file for SAML authentication. Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.

25. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore file:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.

26. In the Domain Security - Secure Communication section, specify whether to use the default Informatica SSL certificates or to use your SSL certificates to secure domain communication.

    a. Select the type of SSL certificates to use.

       The following table describes the SSL certificate options for securing the Informatica domain:

Option	Description
Use the default Informatica SSL certificate files	Use the default SSL certificates provided by Informatica. **Note:** If you do not provide an SSL certificate, Informatica uses the same default private key for all Informatica installations. If you use the default Informatica keystore and truststore files, the security of your domain could be compromised. To ensure a high level of security for the domain, select the option to specify the location of the SSL certificate files.
Specify the location of the SSL certificate files	Use SSL certificates that you provide. You must specify the location of the keystore and truststore files. You can provide a self-signed certificate or a certificate issued by a certificate authority (CA). You must provide SSL certificates in PEM format and in Java Keystore (JKS) files. Informatica requires specific names for the SSL certificate files for the Informatica domain. You must use the same SSL certificates for all nodes in the domain. Store the truststore and keystore files in a directory accessible to all the nodes in the domain and specify the same keystore file directory and truststore file directory for all nodes in the same domain.

    b. If you provide the SSL certificate, specify the location and passwords of the keystore and truststore files.

       The following table describes the parameters that you must enter for the SSL certificate files:

Property	Description
Keystore file directory	Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
Keystore password	Password for the keystore infa_keystore.jks.

Property	Description
Truststore file directory	Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
Truststore password	Password for the infa_truststore.jks file.

The Domain Configuration Repository section appears.

27. At the prompt, enter the information for the domain that you want to join.

    The following table describes the properties that you specify for the domain:

Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.
Gateway node port	Port number of the gateway node.
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.

The Domain Security - Encryption Key section appears.

28. Enter the encryption key information for the Informatica domain that you want to join.

    If the location of the encryption key in the gateway node is not accessible to the current node, copy the encryption key file to an accessible directory. You might need to assign read permission to the directory that contains the encryption key file on gateway node before you can copy the file. For more information about the permissions for the encryption key file and directory, see "Secure Files and Directories" on page 99.

    The following table describes the encryption key parameters that you must specify when you join a domain:

Property	Description
Select the encryption key	Path and file name of the encryption key for the Informatica domain that you want to join. All nodes in the Informatica domain use the same encryption key. You must specify the encryption key file created on the gateway node for the domain that you want to join. If you copied the encryption key file to a temporary directory to make it accessible to the nodes in the domain, specify the path and file name of the encryption key file in the temporary directory.
Encryption key directory	Directory in which to store the encryption key on the node created during this installation. The installer copies the encryption key file for the domain to the encryption key directory on the new node. By default, the encryption key is created in the following directory: `<Informatica installation directory>/isp/config/keys`.

29. On the Join Domain Node Configuration section, enter the information for the node you want to create.

    The following table describes the properties that you set for the node:

Property	Description
Node Host name	Host name for the node. The node host name cannot contain the underscore (_) character. **Note:** Do not use localhost. The host name must explicitly identify the machine.
Node name	Name of the Informatica node to create on this machine. The node name is not the host name for the machine.
Node port number	Port number for the node.
Database truststore file	Path and file name of the truststore file for the secure database. Select the same database truststore file used by the master gateway node in the domain. Required if you join a gateway node to a domain that uses a secure domain configuration repository database.
Truststore password	Password for the database truststore file for the secure database. Required if you join a gateway node to a domain that uses a secure domain configuration repository database.

30. Select whether to display the default ports for the domain and node components assigned by the installer.

    The following table describes the advanced port configuration page:

Prompt	Description
Display advanced port configuration page	Select whether to display the port numbers for the domain and node components assigned by the installer: 1 - No 2 - Yes If you select Yes, the installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.

31. If you display the port configuration page, enter new port numbers at the prompt or press **Enter** to use the default port numbers.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

The Post-installation Summary indicates whether the installation completed successfully. It also shows the status of the installed components and their configuration. You can view the installation log files to get more information about the tasks performed by the installer and to view configuration properties for the installed components.

By default, the system services are disabled after the installation. You must enable them from the Administrator tool.

Installing the Informatica Services in Silent Mode

To install the Informatica services without user interaction, install in silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the Informatica services on multiple machines on the network or to standardize the installation across machines.

Copy the Informatica installation files to the hard disk on the machine where you plan to install the Informatica. If you install on a remote machine, verify that you can access and create files on the remote machine.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.
3. Secure the passwords in the installation properties file.

Configuring the Properties File

Informatica provides a sample properties file that includes the parameters that are required by the installer. You can customize the sample properties file to specify the options for your installation. Then run the silent installation.

The sample SilentInput.properties file is stored in the root directory of the DVD or the installer download location. After you customize the file, re-save it with the file name SilentInput.properties.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the SilentInput.properties file.
4. Use a text editor to open the file and modify the values of the installation parameters.

   The following table describes the installation parameters that you can modify:

Property Name	Description
LICENSE_KEY_LOC	Absolute path and file name of the license key file.
USER_INSTALL_DIR	Directory in which to install Informatica.
INSTALL_TYPE	Indicates whether to install or upgrade Informatica. If the value is 0, the installer performs a fresh installation of Informatica. If the value is 1, the installer upgrades a previous version of Informatica.
UPGRADE_WITHOUT_BIGDATA	Informatica does not support big data products for version 10.1.1 HotFix 2. If you want to install or upgrade to this version, the big data functionality will not be available.Set the value to 1, to continue with the upgrade.Set the value to 0, to quit the upgrade
ENABLE_KERBEROS	Indicates whether to configure the Informatica domain to run on a network with Kerberos authentication. To configure the Informatica domain to run on a network with Kerberos authentication, set this parameter to 1.
SERVICE_REALM_NAME	Name of the Kerberos realm to which the Informatica domain services belong. The service realm name and the user realm name must be the same.
USER_REALM_NAME	Name of the Kerberos realm to which the Informatica domain users belong. The service realm name and the user realm name must be the same.
KEYTAB_LOCATION	Directory where all keytab files for the Informatica domain are stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
KRB5_FILE_LOCATION	Path and file name of the Kerberos configuration file. Informatica requires the following name for the Kerberos configuration file: krb5.conf

Property Name	Description
SPN_SHARE_LEVEL	Indicates the service principal level for the domain. Set the property to one of the following levels: - Process. The domain requires a unique service principal name (SPN) and keytab file for each node and each service on a node. The number of SPNs and keytab files required for each node depends on the number of service processes that run on the node. Recommended for production domains. - Node. The domain uses one SPN and keytab file for the node and all services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Recommended for test and development domains. Default is process.
HTTPS_ENABLED	Indicates whether to secure the connection to Informatica Administrator. If the value is 0, the installer sets up an unsecure HTTP connection to Informatica Administrator. If the value is 1, the installer sets up a secure HTTPS connection to Informatica Administrator.
DEFAULT_HTTPS_ENABLED	Indicates whether the installer creates a keystore file. If the value is 1, the installer creates a keystore and uses it for the HTTPS connection. If the value is 0, the installer uses a keystore file that you specify.
CUSTOM_HTTPS_ENABLED	Indicates whether the installer uses an existing keystore file. If the value is 1, the installer uses a keystore file that you specify. If DEFAULT_HTTPS_ENABLED=1, you must set this parameter to 0. If DEFAULT_HTTPS_ENABLED=0, you must set this parameter to 1.
KSTORE_PSSWD	Plain text password for the keystore file.
KSTORE_FILE_LOCATION	Absolute path and file name of the keystore file.
HTTPS_PORT	Port number to use for the secure connection to Informatica Administrator.
CREATE_DOMAIN	Indicates whether to create an Informatica domain. If the value is 1, the installer creates a node and an Informatica domain. If the value is 0, the installer creates a node and joins the node to another domain created in a previous installation.
KEY_DEST_LOCATION	Directory in which to store the encryption key on the node created during the installation.

Property Name	Description
PASS_PHRASE_PASSWD	Keyword to use to create an encryption key to secure sensitive data in the domain. The keyword must meet the following criteria: - From 8 to 20 characters long - Includes at least one uppercase letter - Includes at least one lowercase letter - Includes at least one number - Does not contain spaces
JOIN_DOMAIN	Indicates whether to join the node to another domain created in a previous installation. If the value is 1, the installer creates a node and joins the node to another domain. If CREATE_DOMAIN=1, you must set this parameter to 0. If CREATE_DOMAIN=0, you must set this parameter to 1.
KEY_SRC_LOCATION	Directory that contains the encryption key on the master gateway node of the Informatica domain that you want to join.
SSL_ENABLED	Enables or disables secure communication between services in the Informatica domain. Indicates whether to set up secure communication between services within the domain. If the value is true, secure communication between services within the domain is enabled. You can set this property to true if CREATE_DOMAIN=1. You must set this property to true if JOIN_DOMAIN=1.
SECURITY_DOMAIN_NAME	Name of the default security domain in the domain to which you join the node you create.
TLS_CUSTOM_SELECTION	Indicates whether to use SSL certificates that you provide to enable secure communication in the Informatica domain. To use SSL certificates that you provide, set this property to True.
NODE_KEYSTORE_DIR	Required if TLS_CUSTOM_SELECTION is set to True. Directory that contains the keystore files. The directory must contain files named infa_keystore.jks and infa_keystore.pem.
NODE_KEYSTORE_PASSWD	Required if TLS_CUSTOM_SELECTION is set to True. Password for the keystore infa_keystore.jks.
NODE_TRUSTSTORE_DIR	Required if TLS_CUSTOM_SELECTION is set to True. Directory that contains the truststore files. The directory must contain files named infa_truststore.jks and infa_truststore.pem.
NODE_TRUSTSTORE_PASSWD	Required if TLS_CUSTOM_SELECTION is set to True. Password for the infa_truststore.jks file.

Property Name	Description
SERVES_AS_GATEWAY	Indicates whether to create a gateway or worker node. If the value is 1, the installer configures the node as a gateway node. If the value is 0, the installer configures the node as a worker node.
DB_TYPE	Database for the domain configuration repository. Enter one of the following values: - Oracle - MSSQLServer - DB2 - Sybase
DB_UNAME	Database user account name for the domain configuration repository.
DB_PASSWD	Password for the database user account.
DB_SSL_ENABLED	Indicates whether the database for the domain configuration repository is secure. To create the domain configuration repository in a secure database, set this parameter to True. If this parameter is set to True, you must provide the JDBC connection string with the secure database parameters.
TRUSTSTORE_DB_FILE	Path and file name of the truststore file for the secure domain configuration repository database. If the domain that you create or join uses a secure domain configuration repository, set this property to the truststore file of the repository database.
TRUSTSTORE_DB_PASSWD	Password for the truststore file for the secure domain configuration repository database.
SQLSERVER_SCHEMA_NAME	For Microsoft SQL Server. Name of the schema that will contain domain configuration tables. If this parameter is empty, the installer creates the tables in the default schema.
TRUSTED_CONNECTION	For Microsoft SQL Server. Indicates whether to connect to Microsoft SQL Server through a trusted connection. If this parameter is empty, the installer uses Microsoft SQL Server authentication. Set this parameter only if you are installing on Windows.
DB2_TABLESPACE	For IBM DB2. Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, if DB2_TABLESPACE is empty, the installer creates the tables in the default tablespace. In a multi-partition database, define the tablespace in the catalog partition of the database.

Property Name	Description
DB_CUSTOM_STRING_SELECTION	Determines whether to use a JDBC URL or a custom connection string to connect to the domain configuration database. If the value is 0, the installer creates a JDBC URL from the database properties you provide. If the value is 1, the installer uses the custom connection string you provide. If you create the domain configuration repository on a secure database, set this parameter to 1.
DB_SERVICENAME	Required if DB_CUSTOM_STRING_SELECTION=0. Service name for Oracle and IBM DB2 databases. Database name for Microsoft SQL Server and Sybase ASE.
DB_ADDRESS	Required if DB_CUSTOM_STRING_SELECTION=0. Host name and port number for the database instance in the format *HostName*:*Port*.
ADVANCE_JDBC_PARAM	You can set this parameter if DB_CUSTOM_STRING_SELECTION=0. Optional parameters to include in the JDBC URL connection string. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If this parameter is empty, the installer creates the JDBC URL without additional parameters.
DB_CUSTOM_STRING	Required if DB_CUSTOM_STRING_SELECTION=1. Valid custom JDBC connection string.
DOMAIN_NAME	If you create a domain, name of the domain to create. If you join a domain, name of the domain to join that was created in a previous installation. The default domain name is Domain_<*MachineName*>. The name must not exceed 128 characters and must be 7-bit ASCII only. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
DOMAIN_HOST_NAME	If you create a domain, this is the host name of the machine on which to create the node. The node host name cannot contain the underscore (_) character. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. Optionally, you can use the IP address. If you join a domain, this is the host name of the machine that hosts the gateway node of the domain you want to join. Note: Do not use localhost. The host name must explicitly identify the machine.

Property Name	Description
NODE_NAME	Required if CREATE_DOMAIN=1. Name of the node to create on this machine. The node name is not the host name for the machine.
DOMAIN_PORT	If you create a domain, this is the port number for the node to create. The default port number for the node is 6005. If the default port number is not available on the machine, the installer displays the next available port number. If you join a domain, this is the port number of the gateway node of the domain you want to join.
DOMAIN_USER	User name for the domain administrator. If you create a domain, you can use this user name to initially log in to Informatica Administrator. Use the following guidelines: - The name is not case sensitive and cannot exceed 128 characters. - The name cannot include a tab, newline character, or the following special characters: % * + \ / ' . ? ; < > - The name can include an ASCII space character except for the first and last character. Other space characters are not allowed. If you join a domain, this is the user name to use to log in to the domain that you want to join.
DOMAIN_PSSWD	Password for the domain administrator. The password must be more than 2 characters but cannot exceed 16 characters.
DOMAIN_CNFRM_PSSWD	Enter the password again to confirm.
SAML_AUTHENTICATION	Required if ENABLE_KERBEROS=0. Set this parameter to True to configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain. If this parameter is set to True, you must provide the IDP URL. Default is true (0).
IDP_URL	Required if ENABLE_KERBEROS=0 and SAML_AUTHENTICATION=True. Enter the Identity Provider URL for the domain.
JOIN_NODE_NAME	Required if JOIN_DOMAIN=1. Name of the node that you are joining to the domain. The node name is not the host name for the machine.

Property Name	Description
JOIN_HOST_NAME	Required if JOIN_DOMAIN=1. Host name of the machine on which to create the node that you are joining to the domain. The node host name cannot contain the underscore (_) character. Note: Do not use localhost. The host name must explicitly identify the machine.
JOIN_DOMAIN_PORT	Required if JOIN_DOMAIN=1. Port number of the gateway node of the domain that you want to join.
ADVANCE_PORT_CONFIG	Indicates whether to display the list of port numbers for the domain and node components. If the value is 0, the installer assigns default port numbers to the domain and node components. If the value is 1, you can set the port numbers for the domain and node components.
MIN_PORT	You can set this parameter if ADVANCE_PORT_CONFIG=1. Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node.
MAX_PORT	You can set this parameter if ADVANCE_PORT_CONFIG=1. Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node.
TOMCAT_PORT	You can set this parameter if ADVANCE_PORT_CONFIG=1. Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. This is the port that the Informatica command line programs use to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
AC_PORT	You can set this parameter if CREATE_DOMAIN=1 and ADVANCE_PORT_CONFIG=1. Port number used by Informatica Administrator. Default is 6007.
SERVER_PORT	You can set this parameter if ADVANCE_PORT_CONFIG=1. Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6008.

Property Name	Description
AC_SHUTDWN_PORT	You can set this parameter if CREATE_DOMAIN=1 and ADVANCE_PORT_CONFIG=1. Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
ENABLE_USAGE_COLLECTION	Enables Informatica DiscoveryIQ, a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to not send any usage statistics to Informatica. For more information on how to disable sending usage statistics, see the *Informatica Administrator Guide*. You must set the value to 1 to apply the hotfix.

5. Optionally, create a Model Repository Service and a Data Integration Service during installation.

   The following table describes the properties that you set if you want to create a Model Repository Service and a Data Integration Service during installation:

Property	Description
CREATE_SERVICES	Enables creation of Model Repository Service and Data Integration Service during installation. Set the value to 1 to enable service creation during installation. Default is 0.
KERBEROS_SECURITY_DOMAIN_NAME	Kerberos security domain name. You must enter the Kerberos security domain name if the domain is enabled for Kerberos authentication.
KERBEROS_DOMAIN_PSSWD	Kerberos security domain password. You must enter the Kerberos security domain password if the domain is enabled for Kerberos authentication.
MRS_DB_TYPE	The Model repository database type. Enter one of the following values: - Oracle - DB2 - MSSQLServer
MRS_DB_UNAME	Database user account name for the Model repository database.
MRS_DB_PASSWD	Password for the database user account.

Property	Description
MRS_DB_SSL_ENABLED	Indicates whether the database for the Model repository database is secure. To create the Model repository database in a secure database, set this parameter to True. If this parameter is set to True, you must provide the JDBC connection string with the secure database parameters.
MRS_SSL_DEFAULT_STRING	Security parameters for the JDBC connection string used to connect to the Model repository database. For example: `EncryptionMethod=SSL;HostNameInCertificate=;ValidateServerCertificate=`
TRUSTSTORE_MRS_DB_FILE	Path and file name of the truststore file for the secure Model repository database.
TRUSTSTORE_MRS_DB_PASSWD	Password for the truststore file for the secure Model repository database.
MRS_SQLSERVER_SCHEMA_NAME	For Microsoft SQL Server. Name of the schema that will contain the Model repository tables. If this parameter is empty, the installer creates the tables in the default schema.
MRS_DB2_TABLESPACE	For IBM DB2. Name of the tablespace in which to create the tables for the Model repository. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, if DB2_TABLESPACE is empty, the installer creates the tables in the default tablespace. In a multi-partition database, define the tablespace in the catalog partition of the database.
MRS_DB_CUSTOM_STRING_SELECTION	Determines whether to use a JDBC URL or a custom connection string to connect to the Model repository database. If the value is 0, the installer creates a JDBC URL from the database properties you provide. If the value is 1, the installer uses the custom connection string you provide. If you create the Model repository database on a secure database, set this parameter to 1.
MRS_DB_SERVICENAME	Service or database name for the Model repository database. Required if MRS_DB_CUSTOM_STRING_SELECTION=0. If the Model repository is on an Oracle or IBM DB2 database, set the property to the service name. If the Model repository is on a Microsoft SQL Server or Sybase ASE database, set the property to the database name.
MRS_DB_ADDRESS	Required if MRS_DB_CUSTOM_STRING_SELECTION=0. Host name and port number for the database instance in the format *HostName*:*Port*.

Property	Description
MRS_ADVANCE_JDBC_PARAM	You can set this parameter if MRS_DB_CUSTOM_STRING_SELECTION=0. Optional parameters to include in the JDBC URL connection string. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If this parameter is empty, the installer creates the JDBC URL without additional parameters.
MRS_DB_CUSTOM_STRING	Required if MRS_DB_CUSTOM_STRING_SELECTION=1. Valid custom JDBC connection string.
MRS_SERVICE_NAME	Name of the Model Repository Service.
MRS_KEYTAB_FILELOC	Required if ENABLE_KERBEROS=1 and SPN_SHARE_LEVEL=PROCESS Directory where the keytab file for the Model Repository Service is stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
DIS_SERVICE_NAME	Name of the Data Integration Service.
DIS_KEYTAB_FILELOC	Required if ENABLE_KERBEROS=1 and SPN_SHARE_LEVEL=PROCESS Directory where the keytab file for the Data Integration Service is stored. The name of a keytab file in the Informatica domain must follow a format set by Informatica.
DIS_PROTOCOL_TYPE	HTTP protocol type of the Data Integration Service. Use one of the following values: - http - https - both
DIS_HTTP_PORT	Required if DIS_PROTOCOL_TYPE is http or both. HTTP port of the Data Integration Service.
DIS_HTTPS_PORT	Required if DIS_PROTOCOL_TYPE is https or both. HTTPS port of the Data Integration Service.
DIS_CUSTOM_SELECTION	Optional parameter if you set the value of DIS_PROTOCOL_TYPE to https or both. If you set the value to true, you provide the SSL certificates to secure the Data Integration Service. You must provide the keystore and truststore files to use to secure the Data Integration Service.
DIS_KEYSTORE_DIR	Required if DIS_CUSTOM_SELECTION is set to true. Location of the keystore file for the Data Integration Service.

Property	Description
DIS_KEYSTORE_PASSWD	Required if DIS_CUSTOM_SELECTION is set to true. Password of the keystore file for the Data Integration Service.
DIS_TRUSTSTORE_DIR	Required if DIS_CUSTOM_SELECTION is set to true. Location of the truststore file for the Data Integration Service.
DIS_TRUSTSTORE_PASSWD	Required if DIS_CUSTOM_SELECTION is set to true. Password for the truststore file for the Data Integration Service.

6. On Windows, specify whether to run the Informatica service under the same user account as the account used for installation.

   The following table describes the properties that you set if you want to run the Informatica service under a different user account:

Property	Description
USE_LOGIN_DETAILS	Indicates whether to run the Windows service under a different user account. If the value is 0, the installer configures the service to run under the current user account. If the value is 1, the installer configures the service to run under a different user account.
WIN_USER_ID	User account with which to run the Informatica Windows service. Use the following format: `<domain name>\<user account>` This user account must have the Act as operating system permission.
WIN_USER_PSSWD	Password for the user account with which to run the Informatica Windows service.

7. Save the properties file with the name SilentInput.properties.

Running the Silent Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.

   On Windows, open the command prompt as administrator. If you do not open the command prompt as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file SilentInput.properties that you edited and resaved.
4. Run the silent installation. On Windows, run silentInstall.bat. On UNIX, run silentInstall.sh.

The silent installer runs in the background. The process can take a while. The silent installation is complete when the Informatica_<Version>_Services_InstallLog<timestamp>.log file is created in the installation directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

Secure the Passwords in the Properties File

After you run the silent installer, ensure that passwords in the properties file are kept secure.

When you configure the properties file for a silent installation, you enter passwords in plain text. After you run the silent installer, use one of the following methods to secure the passwords:

- Remove the passwords from the properties file.
- Delete the properties file.
- Store the properties file in a secure location.

CHAPTER 8

Troubleshooting

This chapter includes the following topics:

Installation Troubleshooting Overview

The topics in this section provides you information on troubleshooting probable issues that you might encounter during Informatica installation process. The examples included in the topics describe general troubleshooting strategies and are not a comprehensive list of possible causes of installation issues.

Troubleshooting with Installation Log Files

You can use the following log files to troubleshoot an Informatica installation:

Installation log files

The installer produces log files during and after the installation. You can use these logs to get more information about the tasks completed by the installer and errors that occurred during installation. The installation log files include the following logs:

- Debug logs
- File installation logs

Service Manager log files

Log files generated when the Service Manager starts on a node.

Debug Log Files

The installer writes actions and errors to the debug log file. The name of the log file depends on the Informatica component you install.

The following table describes the properties of the debug log files:

Property	Description
Log File Name	- Informatica_<Version>_Services.log - Informatica_<Version>_Client.log - Informatica_<Version>_Services_Upgrade.log - Informatica_<Version>_Client_Upgrade.log
Location	Installation directory.
Usage	Get more information about the actions performed by the installer and get more information about installation errors. The installer writes information to this file during the installation. If the installer generates an error, you can use this log to troubleshoot the error.
Contents	Detailed summary of each action performed by the installer, the information you entered in the installer, each command line command used by the installer, and the error code returned by the command.

The debug log contains output from the infacmd and infasetup commands used to create the domain, node, and application services. It also contains information about starting the application services.

File Installation Log File

The file installation log file contains information about the installed files.

The following table describes the properties of the installation log file:

Property	Description
Log File Name	- Informatica_<Version>_Services_InstallLog.log - Informatica_<Version>_Client_InstallLog.log
Location	Installation directory.
Usage	Get information about the files installed and registry entries created.
Contents	Directories created, names of the files installed and commands run, and status for each installed file.

Service Manager Log Files

The installer starts the Informatica service. The Informatica service starts the Service Manager for the node. The Service Manager generates log files that indicate the startup status of a node. Use these files to troubleshoot issues when the Informatica service fails to start and you cannot log in to Informatica Administrator. The Service Manager log files are created on each node.

The following table describes the files generated by the Service Manager:

Property	Description
catalina.out	Log events from the Java Virtual Machine (JVM) that runs the Service Manager. For example, a port is available during installation, but is in use when the Service Manager starts. Use this log to get more information about which port was unavailable during startup of the Service Manager. The catalina.out file is in the following directory: `<Informatica installation directory>/logs/<node name>/catalina.out`
node.log	Log events generated during the startup of the Service Manager on a node. You can use this log to get more information about why the Service Manager for a node failed to start. For example, if the Service Manager cannot connect to the domain configuration database after 30 seconds, the Service Manager fails to start. The node.log file is in the /tomcat/logs directory.

Note: The Service Manager also uses node.log to record events when the Log Manager is unavailable. For example, if the machine where the Service Manager runs does not have enough available disk space to write log event files, the Log Manager is unavailable.

Troubleshooting Domains and Nodes

The installer can generate errors when creating and configuring domains and nodes during the Informatica installation.

You can encounter errors with the following installer tasks:

- Adding the domain configuration database
- Creating or joining a domain
- Starting Informatica
- Pinging the domain
- Adding a license

Creating the Domain Configuration Repository

If you create a domain, the installer creates a domain configuration repository to store domain metadata. The installer uses the options you enter during installation to add configuration metadata to the domain configuration repository. The installer uses JDBC to communicate with the database. You do not need to configure ODBC or native connectivity on the machine where you install the Informatica services.

The installer creates and drops a table in the domain configuration repository database to verify the connection information. The user account for the database must have create privileges on the database. Each domain must have a separate domain configuration repository.

Creating or Joining a Domain

The installer completes different tasks depending on whether you create a domain or join a domain:

- **Creating a domain.** The installer runs the infasetup DefineDomain command to create the domain and the gateway node for the domain on the current machine based on the information you enter in the Configure Domain window.
- **Joining a domain.** The installer runs the infasetup DefineWorkerNode command to create a node on the current machine, and runs the infacmd AddDomainNode command to add the node to the domain. The installer uses the information you enter in the Configure Domain window to run the commands.

The infasetup and infacmd commands fail if the gateway node is unavailable. If the gateway node is unavailable, you cannot log in to Informatica Administrator.

For example, the DefineDomain command fails if you click Test Connection and the connection test passes but the database becomes unavailable before you click Next. The DefineDomain command can also fail if the host name or IP address does not belong to the current machine. Verify that the database for the domain configuration is available and that the host name is correct and try again.

If the AddDomainNode command fails, verify that the Informatica service is running on the gateway node and try again.

Starting Informatica

The installer runs infaservice to start the Informatica service. To troubleshoot issues when Informatica fails to start, use the information in the installation debug log and the node.log and catalina.out Service Manager log files to identify the cause of the error.

If you create a domain, log in to Informatica Administrator after the Informatica service starts to verify that the domain is available. If you join a domain, log in to Informatica Administrator after the Informatica service starts to verify that the node was successfully created and started.

Informatica can fail to start for the following reasons:

- **The Service Manager is out of system memory.** The Java Runtime Environment (JRE) that starts Informatica and runs the Service Manager may not have enough system memory to start. Set the INFA_JAVA_OPTS environment variable to configure the amount of system memory used by Informatica. On UNIX, you can set the memory configuration when you start Informatica.
- **The domain configuration database is not available.** Informatica fails to start on a node if the Service Manager on a gateway node cannot connect to the domain configuration database within 30 seconds. Verify that the domain configuration repository is available.
- **You incorrectly configure the Informatica service user account.** Informatica fails to start if you incorrectly configure the Windows domain, user name, or password when you configure the user account to start the Informatica service on Windows. In addition, the user account must have the Act as operating system permission.
- **The content of the PATH environment variable exceeds the maximum length allowed.** On Windows, Informatica fails to start if files or libraries required by Informatica are not in the system path and cannot be accessed. This problem can occur if the total number of characters in the PATH environment variable exceeds the limit.
- **Some of the folders in the Informatica installation directory do not have the appropriate execute permissions.** Grant execute permission on the Informatica installation directory.

Pinging the Domain

The installer runs the *infacmd* Ping command to verify that the domain is available before it continues the installation. The domain must be available so that license objects can be added to the domain. If the Ping command fails, start Informatica on the gateway node.

Adding a License

The installer runs the *infacmd* AddLicense command to read the Informatica license key file and create a license object in the domain. To run the application services in Informatica Administrator, a valid license object must exist in the domain.

If you use an incremental license and join a domain, the serial number of the incremental license must match the serial number for an existing license object in the domain. If the serial numbers do not match, the AddLicense command fails.

You can get more information about the contents of the license key file used for installation, including serial number, version, expiration date, operating systems, and connectivity options in the installation debug log. You can get more information about existing licenses for the domain in Informatica Administrator.

Part IV: After You Install the Services

This part contains the following chapters:

CHAPTER 9

Complete the Domain Configuration

This chapter includes the following topics:

Complete the Domain Configuration Overview

After you install Informatica services and before you create the application services, complete the configuration for the domain services.

Domain configuration includes tasks such as verifying code pages, configuring the environment variables for the domain, and configuring the firewall.

Verify Locale Settings and Code Page Compatibility

The code pages for application services must be compatible with code pages in the domain.

Verify and configure the locale settings and code pages:

Verify that the domain configuration database is compatible with the code pages of the application services that you create in the domain.

The Service Manager synchronizes the list of users in the domain with the list of users and group 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.

Verify that the locale settings on machines that access the Administrator tool and the Informatica client tools are compatible with code pages of repositories in the domain.

If the locale setting is not compatible with the repository code page, you cannot create an application service.

On Windows, verify the locale settings in the regional options of Control Panel. For information, see the Windows documentation.

Configure Locale Environment Variables on UNIX

Verify that the locale setting is compatible with the code page for the repository. If the locale setting is not compatible with the repository code page, you cannot create an application service.

Use LANG, LC_CTYPE, or LC_ALL to set the UNIX code page.

Different UNIX operating systems require different values for the same locale. The value for the locale variable is case sensitive.

Use the following command to verify that the value for the locale environment variable is compatible with the language settings for the machine and the type of code page you want to use for the repository:

```
locale -a
```

The command returns the languages installed on the UNIX operating system and the existing locale settings.

Set the following locale environment variables:

Locale on Linux

All UNIX operating systems except Linux have a unique value for each locale. Linux allows different values to represent the same locale. For example, “utf8,” “UTF-8,” “UTF8,” and “utf-8” represent the same locale on a Linux machine. Informatica requires that you use a specific value for each locale on a Linux machine. Make sure that you set the LANG environment variable appropriately for all Linux machines.

Locale for Oracle database clients

For Oracle database clients, set NLS_LANG to the locale that you want the database client and server to use with the login. A locale setting consists of the language, territory, and character set. The value of NLS_LANG depends on the configuration.

For example, if the value is american_america.UTF8, set the variable in a C shell with the following command:

```
setenv NLS_LANG american_america.UTF8
```

To read multibyte characters from the database, set the variable with the following command:

```
setenv NLS_LANG=american_america.AL32UTF8
```

You must set the correct variable on the Data Integration Service machine so that the Data Integration Service can read the Oracle data correctly.

Configure Environment Variables

Informatica uses environment variables to store configuration information when it runs the application services and connects to the clients. Configure the environment variables to meet the Informatica requirements.

Incorrectly configured environment variables can cause the Informatica domain or nodes to fail to start or can cause connection problems between the Informatica clients and the domain.

To configure environment variables on UNIX, log in with the system user account you used to install Informatica.

Configure Informatica Environment Variables

You can configure Informatica environment variables to store memory, domain, and location settings.

Set the following environment variables:

INFA_JAVA_OPTS

By default, Informatica uses a maximum of 512 MB of system memory.

The following table lists the minimum requirement for the maximum heap size settings, based on the number of users and services in the domain:

Number of Domain Users	Maximum Heap Size (1-5 Services)	Maximum Heap Size (6-10 Services)
1,000 or less	512 MB (default)	1024 MB
5,000	2048 MB	3072 MB
10,000	3072 MB	5120 MB
20,000	5120 MB	6144 MB
30,000	5120 MB	6144 MB

Note: The maximum heap size settings in the table are based on the number of application services in the domain.

If the domain has more than 1,000 users, update the maximum heap size based on the number of users in the domain.

You can use the INFA_JAVA_OPTS environment variable to configure the amount of system memory used by Informatica. For example, to configure 1 GB of system memory for the Informatica daemon in a C shell, use the following command:

```
setenv INFA_JAVA_OPTS "-Xmx1024m"
```

On Windows, configure INFA_JAVA_OPTS as a system variable.

Restart the node for the changes to take effect.

INFA_DOMAINS_FILE

The installer creates a domains.infa file in the Informatica installation directory. The domains.infa file contains the connectivity information for the gateway nodes in a domain, including the domain names, domain host names, and domain host port numbers.

Set the value of the INFA_DOMAINS_FILE variable to the path and file name of the domains.infa file.

Configure the INFA_DOMAINS_FILE variable on the machine where you install the Informatica services. On Windows, configure INFA_DOMAINS_FILE as a system variable.

INFA_HOME

Use INFA_HOME to designate the Informatica installation directory. If you modify the Informatica directory structure, you need to set the environment variable to the location of the Informatica installation directory or the directory where the installed Informatica files are located.

For example, you use a softlink for any of the Informatica directories. To configure INFA_HOME so that any Informatica application or service can locate the other Informatica components it needs to run, set INFA_HOME to the location of the Informatica installation directory.

INFA_TRUSTSTORE

If you enable secure communication for the domain, set the INFA_TRUSTSTORE variable with the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named infa_truststore.jks and infa_truststore.pem.

You must set the INFA_TRUSTSTORE variable if you use the default SSL certificate provided by Informatica or a certificate that you provide.

INFA_TRUSTSTORE_PASSWORD

If you enable secure communication for the domain and you specify the SSL certificate to use, set the INFA_TRUSTSTORE_PASSWORD variable with the password for the infa_truststore.jks that contains the SSL certificate. The password must be encrypted. Use the command line program pmpasswd to encrypt the password.

Configure Library Path Environment Variables on UNIX

Configure library path environment variables on the machines that run the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes. The variable name and requirements depend on the platform and database.

Linux

Configure the LD_LIBRARY_PATH environment variable.

The following table describes the values that you set for the LD_LIBRARY_PATH for the different databases:

Database	Value
Oracle	<*DatabasePath*>/lib
IBM DB2	<*DatabasePath*>/lib
Sybase ASE	"${SYBASE_OCS}/lib:${SYBASE_ASE}/lib:${LD_LIBRARY_PATH}"
Informix	<*DatabasePath*>/lib
Teradata	<*DatabasePath*>/lib
ODBC	<CLOSEDODBCHOME>/lib

AIX

Configure the LIBPATH environment variable for the following Java-based components and databases:

Java component variables

The PowerCenter Integration Service requires the Java Runtime Environment libraries to process the following Java-based components:

- Custom transformations that use Java
- Java transformations

- PowerExchange® adapters that use Java: PowerExchange for JMS, PowerExchange for Web Services, and PowerExchange for webMethods.

Configure the library path environment variable to point to the installed Java directory on machines where the PowerCenter Integration Service process runs. Configure the LIBPATH environment variable with the following values:

- *INFA_JRE_HOME*/bin
- *JAVA_HOME*/java/jre/bin/classic

Databases

The following table describes the values that you set for the LIBPATH environment variable for the different databases:

Database	Value
Oracle	<*DatabasePath*>/lib
IBM DB2	<*DatabasePath*>/lib
Sybase ASE	"${SYBASE_OCS}/lib:${SYBASE_ASE}/lib:${LIBPATH}"
Informix	<*DatabasePath*>/lib
Teradata	<*DatabasePath*>/lib
ODBC	<CLOSEDODBCHOME>/lib

Configure Kerberos Environment Variables

If you configure the Informatica domain to run on a network with Kerberos authentication, you must set the Kerberos configuration and credential cache environment variables.

Set the following environment variables:

KRB5_CONFIG

Use the KRB5_CONFIG environment variable to store the path and file name of the Kerberos configuration file. The name of the Kerberos configuration file is *krb5.conf*. You must set the KRB5_CONFIG environment variable on each node in the Informatica domain.

KRB5CCNAME

Set the KRB5CCNAME environment variable with the path and file name of the Kerberos user credential cache. Kerberos single sign-on requires Kerberos credential cache for user accounts.

When you cache the user credential, you must use the *forwardable* option. For example, if you use *kinit* to get and cache the user credential, you must use the *-f* option to request forwardable tickets.

Configure the Windows Firewall

When you start the Informatica Windows service, the machines where you install the Informatica clients cannot access the Service Manager in the Informatica domain. To allow the clients access to the Service Manager, you must configure the firewall to grant client machines access to the domain.

On the machine where you created the Informatica domain, add the client machines to the list of firewall exceptions.

1. On the Windows Control Panel, open **Windows Firewall**.
2. On the Windows Firewall window, click the **Exceptions** tab.
3. Click **Add Program**.
4. On the Add a Program window, click **Browse**.

   The infasvcs.exe file runs the Service Manager in the domain.
5. Go to the following directory:

   ```
   <Informatica installation directory>\tomcat\bin
   ```
6. Select **infasvcs.exe** and click **Open**.

   The infasvcs.exe file appears in the list of programs.

   You can click **Change Scope** to specify the machines that you want to access Informatica.
7. Verify that the infasvcs.exe file appears in the list of programs and services and that it is enabled.
8. Click **OK**.

CHAPTER 10

Prepare to Create the Application Services

This chapter includes the following topics:

Prepare to Create the Application Services Overview

Before you create an application service, verify the setup and configuration on the node.

Log in to the Administrator tool and create connections to the databases that the application services access through native connectivity.

Verify the Setup for 64-bit Windows

On Windows, you must run the Informatica services and the Developer tool on the 64-bit platform. You can run the PowerCenter Client on a 32-bit or 64-bit platform.

A 64-bit architecture provides larger memory space that can improve caching and data throughput performance of the Integration Services. The Informatica 64-bit platform addresses up to 18 million terabytes (2^64 bytes) of system memory and has up to 256 terabytes (2^48 bytes) available for a single application.

When you run Informatica on 64-bit platforms, configure the environment to use the correct libraries, database clients, and session cache sizes.

Use the following guidelines when you install Informatica services on 64-bit Windows:

- Link 64-bit applications with 64-bit libraries.

- Link 64-bit machines where the Data Integration Service, PowerCenter Repository Service, or PowerCenter Integration Service runs with a 64-bit database client.

Create Directories for the Analyst Service

Before you create the Analyst Service, you must create directories for the Analyst tool to store temporary files.

Create the following directories on the node that runs the Analyst Service:

Flat file cache directory

Create a directory for the flat file cache where the Analyst tool stores uploaded flat files. The Data Integration Service must also be able to access this directory. If the Analyst Service and the Data Integration Service run on different nodes, configure the flat file directory to use a shared directory. If the Data Integration Service runs on primary and back-up nodes or on a grid, each Data Integration Service process must be able to access the files in the shared directory.

For example, you can create a directory named "flatfilecache" in the following mapped drive that all Analyst Service and Data Integration Service processes can access:

```
F:\shared\<InformaticaInstallationDir>\server
```

When you import a reference table or flat file source, the Analyst tool uses the files from this directory to create a reference table or flat file data object.

Temporary export file directory

Create a directory to store the temporary business glossary files that the business glossary export process creates. Create the directory on the node that runs the Analyst Service.

For example, you can create a directory named "exportfiledirectory" in the following location:
`<Informatica installation directory>/server`

Asset attachments directory

Create a directory to store the files that content managers add as attachments to Glossary assets. Create the directory on the node that runs the Analyst Service.

For example, you can create a directory named "attachmentdirectory" in the following location:
`<Informatica installation directory>/server`

Create the Service Principal Names and Keytab Files for the Application Services

If the Informatica domain uses Kerberos authentication and you set the service principal level for the domain to process level, the domain requires an SPN and keytab file for each application service that you create in the domain. Before you enable a service, verify that an SPN and a keytab file are available for the service. Kerberos cannot authenticate the application service if the service does not have a keytab file in the Informatica directory.

The Informatica domain requires the SPNs and keytab file names in a specific format. You can use the Informatica Kerberos SPN Format Generator to generate the format of the SPN and keytab file name for the

service. To save time, decide on the names of the services you want to create and the nodes on which they will run. Then run the utility to generate the SPN and keytab file name format for all the services at one time. The SPN and keytab file names are case sensitive.

You can run the Informatica Kerberos SPN Format Generator from the following directory: `<Informatica installation directory>/Tools/Kerberos`

For more information about running the Informatica Kerberos SPN Format Generator, see GUID-1E2C3772-CCDA-40AC-A882-C880B3587387.

Send a request to the Kerberos administrator to add the SPNs to the principal database and to create the corresponding keytab file.

When you receive the keytab files from the Kerberos administrator, copy the files to the directory for the keytab file. By default, keytab files are stored in the following directory: `<Informatica installation directory>/isp/config/keys`. If you specified a different keytab file directory during installation, copy the files to that directory.

Note: If the service principal for the domain is at node level, you can create and enable application services without creating additional SPNs and keytab files.

Create a Keystore for a Secure Connection to a Web Application Service

You can secure the connection between the Informatica domain and a web application service, such as the Analyst service. Informatica uses the SSL/TLS protocol to encrypt network traffic. To secure the connection, you must create the required files.

Before you can secure the connection to a web application service, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

The keystore is in an accessible directory.

The keystore must be in a directory that is accessible to the Administrator tool.

Log In to Informatica Administrator

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

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 and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:
   - If the Administrator tool is not configured to use a secure connection, enter the following URL:

     ```
     http://<fully qualified hostname>:<http port>/administrator/
     ```
   - If the Administrator tool is configured to use a secure connection, enter the following URL:

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

   Host name and port in the URL represent the host name and port number of the master gateway node. If you configured secure communication for the domain, you must use HTTPS in the URL to ensure that you can access the Administrator tool.

   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.
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 Informatica domain contains an LDAP security domain. If you do not know the security domain that your user account belongs to, contact the Informatica domain administrator.

   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 and most application services take a long time to run on Microsoft Windows Server 2016.

Troubleshooting the Login to Informatica Administrator

If the Informatica 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 Informatica 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.

Create Connections

In the Administrator tool, create connections to the databases that the application services use. You need to specify the connection details while you configure the application service.

When you create the database connection, specify the database connection properties and test the connection.

The following table describes the database connections that you must create before you create the associated application services:

Database Connection	Description
Data object cache database	To access the data object cache, create the data object cache connection for the Data Integration Service.
Workflow database	To store run-time metadata for workflows, create the workflow database connection for the Data Integration Service.
Profiling warehouse database	To create and run profiles and scorecards, create the profiling warehouse database connection for the Data Integration Service. Use this instance of the Data Integration Service when you configure the run-time properties of the Analyst Service. You can create the following types of profiles when you use a JDBC connection for the profiling warehouse: - Column profile - Rule profile - Data domain discovery profile - Enterprise discovery profile without enabling the foreign key discovery You can also create scorecards when you use a JDBC connection for the profiling warehouse. **Note:** To use the Microsoft SQL Server database as the profiling warehouse, choose ODBC as the provider type, and clear the **use DSN** option in the **Microsoft SQL Server connection properties** dialog box when you configure the Microsoft SQL Server connection.
Reference data warehouse	To store reference table data, create the reference data warehouse connection for the Content Management Service.

IBM DB2 Connection Properties

Use a DB2 for LUW connection to access tables in a DB2 for LUW database.

The following table describes the DB2 for LUW connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
Connection String for metadata access	Connection string to import physical data objects. Use the following connection string: `jdbc:informatica:db2://<host>:50000;databaseName=<dbname>`
Connection String for data access	Connection string to preview data and run mappings. Enter `dbname` from the alias configured in the DB2 client.

Property	Description
Code Page	Database code page.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Tablespace	Tablespace name of the DB2 for LUW database.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

Microsoft SQL Server Connection Properties

Use a Microsoft SQL Server connection to access tables in a Microsoft SQL Server database.

The following table describes the Microsoft SQL Server connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
Use Trusted Connection	Optional. When enabled, the Data Integration Service uses Windows authentication to access the Microsoft SQL Server database. The user name that starts the Data Integration Service must be a valid Windows user with access to the Microsoft SQL Server database.
Connection String for metadata access	Connection string to import physical data objects. Use the following connection string: `jdbc:informatica:sqlserver://<host>:<port>;databaseName=<dbname>`
Connection String for data access	Connection string to preview data and run mappings. Enter `<ServerName>@<DBName>`
Domain Name	Optional. Name of the domain where Microsoft SQL Server is running.
Packet Size	Required. Optimize the ODBC connection to Microsoft SQL Server. Increase the packet size to increase performance. Default is 0.

Property	Description
Code Page	Database code page.
Owner Name	Name of the schema owner. Specify for connections to the profiling warehouse database or data object cache database.
Schema Name	Name of the schema in the database. Specify for connections to the profiling warehouse or data object cache 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 you manage the cache with an external tool.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

Note: When you use a Microsoft SQL Server connection to access tables in a Microsoft SQL Server database, the Developer tool does not display the synonyms for the tables.

Oracle Connection Properties

Use an Oracle connection to access tables in an Oracle database.

The following table describes the Oracle connection properties:

Property	Description
User name	Database user name.
Password	Password for the user name.
Connection String for metadata access	Connection string to import physical data objects. Use the following connection string: `jdbc:informatica:oracle://<host>:1521;SID=<sid>`

Property	Description
Connection String for data access	Connection string to preview data and run mappings. Enter `dbname.world` from the TNSNAMES entry.
Code Page	Database code page.
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Parallel Mode	Optional. Enables parallel processing when loading data into a table in bulk mode. Default is disabled.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

Creating a Connection

In the Administrator tool, you can create relational database, social media, and file systems connections.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Connections** view.
3. In the Navigator, select the domain.
4. In the Navigator, click **Actions** > **New** > **Connection**.

   The **New Connection** dialog box appears.
5. In the **New Connection** dialog box, select the connection type, and then click **OK**.

   The **New Connection** wizard appears.
6. Enter the connection properties.

   The connection properties that you enter depend on the connection type. Click **Next** to go to the next page of the **New Connection** wizard.
7. When you finish entering connection properties, you can click **Test Connection** to test the connection.
8. Click **Finish**.

CHAPTER 11

Create the Application Services

This chapter includes the following topics:

Create the Application Services Overview

Use the Administrator tool to create the application services in the required order.

Some application services depend on other application services. When you create these dependent application services, you must provide the name of other running application services. Review the application service dependencies to determine the order that you must create the services. For example, you must create a Model Repository Service and a Data Integration Service before you create an Analyst Service.

Before you create the application services, verify that you have completed the prerequisite tasks required by the installation and configuration process.

After you create each application service, review the next tasks that you need to complete.

Verify Application Service Prerequisites

Before you create an application service, verify that you have performed the following prerequisite tasks that are described earlier in this guide:

Set up the database.

Set up the following databases:

- Model repository for the Model Repository Service.
- Data object cache database to cache logical data objects and virtual tables.
- Profiling warehouse to perform data profiling and discovery.
- Workflow database to store run-time metadata for workflows.
- Reference data warehouse to store reference table data for the Content Management Service.
- PowerCenter repository for the PowerCenter Repository Service.
- Metadata Manager repository for the Metadata Manager Service.

Install database client software on the service machines.

Configure native connectivity for the following:

- Install and configure the native database client software associated with the relational data sources and the repository databases on the machine that runs the Data Integration Service.
- Install database client software and configure connectivity on the machines where the PowerCenter Repository Service and the PowerCenter Repository Service processes run.
- Install database client software associated with the relational data sources and the repository databases on the machines where the PowerCenter Integration Service runs.

Configure database client environment variables on UNIX.

You must configure the database client environment variables on the machines that run the following services:

- Data Integration Service
- PowerCenter Repository Service
- PowerCenter Integration Service

Create a keytab file for the service.

If the domain uses Kerberos authentication and you set the service principal level at the process level, create a unique keytab file for the following services:

- Model Repository Service
- Data Integration Service
- Analyst Service
- Content Management Service
- Search Service
- PowerCenter Repository Service
- PowerCenter Integration Service
- Metadata Manager Service

Note: The name of the service that you create must match the service name in the keytab file name.

Set up keystore files.

To set up a secure connection to the application client, create a keystore file for the following services:

- Analyst Service
- Metadata Manager Service

- Web Services Hub Service

Configure POSIX Asynchronous I/O.

If you installed Informatica on IBM AIX, configure POSIX Asynchronous I/O on any node where you want to run a PowerCenter Integration Service.

Determine the code page to use for the repository.

Verify code page compatibility for the following:

- Domain configuration database is compatible with the code pages of the application services that you create in the domain.
- PowerCenter repository code page is compatible with the code pages for the PowerCenter Client and all application services in the Informatica domain.
- Code page for the PowerCenter Integration Service is compatible with the code page of the associated PowerCenter repository.
- Metadata Manager repository code page, the code page on the machine where the associated PowerCenter Integration Service runs, and the code page for any database management and PowerCenter resources that you want to load into the Metadata Manager warehouse are the same.

Configure locale environment variables on UNIX.

Verify that the locale settings on machines that access the Administrator tool and the Informatica client tools is compatible with the code page of the PowerCenter repository.

Configure library path environment variables on UNIX.

Configure the library path environment variables on the machines that run the following services:

- Data Integration Service
- PowerCenter Repository Service
- PowerCenter Integration Service

Verify the setup for 64-bit Windows.

Verify the setup for 64-bit Windows for the following services:

- Data Integration Service
- PowerCenter Repository Service
- PowerCenter Integration Service

Create directories for the Analyst Service.

On the node that runs the Analyst Service, create the following directories:

- Flat file cache directory where the Analyst tool stores uploaded flat files. Ensure that the Data Integration Service can also access this directory.
- Temporary export file directory to store the temporary business glossary files that the business glossary export process creates.

Create connections to the databases that the application services access though native connectivity.

In the Administrator tool, create connections to the following databases:

- Data object cache database
- Profiling warehouse database
- Reference data warehouse
- Workflow database

Application Service Dependencies

A dependent application service is an application service that requires one or more other application services. Before you create a dependent service, you must create all of the application services that the dependent service requires.

For example, the Data Integration Service depends on the Model Repository Service. When you create a Data Integration Service, the Administrator tool prompts you for the name of a Model Repository Service. Therefore, you must create a Model Repository Service before you create a Data Integration Service.

Services that access Model repository objects can depend on each other. In addition, services that access PowerCenter repository objects can depend on each other. The application service dependencies determine the order that you must create the services.

Services that Access Model Repository Objects

Create the application services that access Model repository objects in the following order:

1. Model Repository Service.
   The Model Repository Service has no application service dependencies.
2. Data Integration Service.
   The Data Integration Service depends on the Model Repository Service.
3. Analyst Service.
   The Analyst Service depends on the Model Repository Service and the Data Integration Service.

   If you want to run data lineage for scorecards in the Analyst tool, the Analyst Service depends on the Metadata Manager Service. You can create the Analyst Service and the Metadata Manager Service in any order. You can select the Metadata Manager Service that runs data lineage for the Analyst Service when you create the Analyst Service or after you create the Analyst Service.
4. Content Management Service.
   The Content Management Service depends on the Model Repository Service and the Data Integration Service.
5. Search Service.
   The Search Service depends on the Model Repository Service, the Data Integration Service, and the Analyst Service.

Services that Access PowerCenter Repository Objects

Create the application services that access PowerCenter repository objects in the following order:

1. PowerCenter Repository Service.
   The PowerCenter Repository Service has no application service dependencies.
2. PowerCenter Integration Service.
   The PowerCenter Integration Service depends on the PowerCenter Repository Service.
3. Metadata Manager Service.
   The Metadata Manager Service depends on the PowerCenter Repository Service and the PowerCenter Integration Service.
4. Web Services Hub.
   The Web Services Hub Service depends on the PowerCenter Repository Service.

Create and Configure the Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services.

When you access a Model repository object from the Developer tool, the Analyst tool, the Administrator tool, or the Data Integration Service, the client or service sends a request to the Model Repository Service. The Model Repository Service process fetches, inserts, and updates the metadata in the Model repository database tables.

Create the Model Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Model Repository Service**.

   The **New Model Repository Service** dialog box appears.
3. On the **New Model Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.

   The **New Model Repository Service - Step 2 of 2** page appears.
5. Enter the following properties for the Model repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.

Property	Description
Password	Repository database password for the database user.
Database Schema	Available for Microsoft SQL Server. Name of the schema that will contain Model repository tables.
Database Tablespace	Available for IBM DB2. Name of the tablespace in which to create the tables. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.

6. Enter the JDBC connection string that the service uses to connect to the Model repository database.

   Use the following syntax for the connection string for the selected database type:

Database Type	Connection String Syntax
IBM DB2	`jdbc:informatica:db2://<host_name>:<port_number>;DatabaseName=<database_name>;BatchPerformanceWorkaround=true;DynamicSections=3000`

Microsoft SQL Server	- Microsoft SQL Server that uses the default instance
	`jdbc:informatica:sqlserver://<host_name>:<port_number>;DatabaseName=<database_name>;SnapshotSerializable=true`
	- Microsoft SQL Server that uses a named instance
	`jdbc:informatica:sqlserver://<host_name>\<named_instance_name>;DatabaseName=<database_name>;SnapshotSerializable=true`

Oracle	`jdbc:informatica:oracle://<host_name>:<port_number>;SID=<database_name>;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true`

7. If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters in the **Secure JDBC Parameters** field.

   Enter the parameters as `name=value` pairs separated by semicolon characters (;). For example:

   ```
   param1=value1;param2=value2
   ```

Enter the following secure database parameters:

Secure Database Parameter	Description
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 the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. 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 the database server sends. 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	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to `cryptoProtocolVersion=TLSv1.1` or `cryptoProtocolVersion=TLSv1.2` based on the cryptographic protocol used by the database server.
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate for the database. If you do not include the path for the truststore file, Informatica looks for the file in the following default directory: `<Informatica installation directory>/tomcat/bin`
TrustStorePassword	Required. Password for the truststore file for the secure database.

Note: Informatica appends the secure JDBC parameters to the JDBC connection string. If you include the secure JDBC parameters directly in the connection string, do not enter any parameter in the **Secure JDBC Parameters** field.

8. Click **Test Connection** to verify that you can connect to the database.
9. Select **No content exists under specified connection string. Create new content.**
10. Click **Finish**.

    The domain creates the Model Repository Service, creates content for the Model repository in the specified database, and enables the service.

    Note: When you update the Model Repository Service properties, you must restart the Model Repository Service and the Catalog Service for the modifications to take effect.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the Model Repository Service

After you create the Model Repository Service, perform the following tasks:

- Create the Model repository user if the domain does not use Kerberos authentication.
- Create other application services.

Create the Model Repository User

If the domain does not use Kerberos authentication, the domain uses a user account to authenticate other application services that make requests to the Model Repository Service. You must create a user account and assign the user the Administrator role for the Model Repository Service.

When you create an application service that depends on the Model Repository Service, you provide the name of the Model Repository Service and of this Model repository user.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create User** to create a native user account.

   Note: If you set up LDAP authentication in the domain, you can use an LDAP user account for the Model repository user.
3. Enter the following properties for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > “
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > “

4. Click **OK**.

   The user properties appear.
5. Click the **Privileges** tab.
6. Click **Edit**.

   The **Edit Roles and Privileges** dialog box appears.
7. On the **Roles** tab, expand the Model Repository Service.
8. Under **System Defined Roles**, select Administrator and click **OK**.

Create Other Services

After you create the Model Repository Service, create the application services that depend on the Model Repository Service.

Create the dependent services in the following order:

1. Data Integration Service
2. Analyst Service
3. Content Management Service
4. Search Service

Create and Configure the Data Integration Service

The Data Integration Service is an application service that performs data integration jobs for the Analyst tool, the Developer tool, and external clients.

When you preview or run data profiles, SQL data services, and mappings in the Analyst tool or the Developer tool, the client tool sends requests to the Data Integration Service to perform the data integration jobs. When you run SQL data services, mappings, and workflows from the command line program or an external client, the command sends the request to the Data Integration Service.

Create the Data Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Data Integration Service, verify that you have created and enabled the Model Repository Service. If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Data Integration Service can use to access the Model Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Domain Navigator, select the domain.
4. Click **Actions** > **New** > **Data Integration Service**.

   The **New Data Integration Service** wizard appears.
5. On the **New Data Integration Service - Step 1 of 14** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.

Property	Description
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Assign	Select **Node** to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Next**.

   The **New Data Integration Service - Step 2 of 14** page appears.
7. Enter the HTTP port number to use for the Data Integration Service.
8. Accept the default values for the remaining security properties. You can configure the security properties after you create the Data Integration Service.
9. Select **Enable Service**.

   The Model Repository Service must be running to enable the Data Integration Service.
10. Verify that the **Move to plugin configuration page** is not selected.
11. Click **Next**.

    The **New Data Integration Service - Step 3 of 14** page appears.
12. Set the **Launch Job Options** property to one of the following values:

    - In the service process. Configure when you run SQL data service and web service jobs. SQL data service and web service jobs typically achieve better performance when the Data Integration Service runs jobs in the service process.
    - In separate local processes. Configure when you run mapping, profile, and workflow jobs. When the Data Integration Service runs jobs in separate local processes, stability increases because an unexpected interruption to one job does not affect all other jobs.

    If you configure the Data Integration Service to run on a grid after you create the service, you can configure the service to run jobs in separate remote processes.
13. Accept the default values for the remaining execution options and click **Next**.

    The **New Data Integration Service - Step 4 of 14** page appears.

14. If you created the data object cache database for the Data Integration Service, click **Select** to select the cache connection. Select the data object cache connection that you created for the service to access the database.
15. Accept the default values for the remaining properties on this page and click **Next**.

    The **New Data Integration Service - Step 5 of 14** page appears.
16. For optimal performance, enable the Data Integration Service modules that you plan to use.

    The following table lists the Data Integration Service modules that you can enable:

Module	Description
Web Service Module	Runs web service operation mappings.
Mapping Service Module	Runs mappings and previews.
Profiling Service Module	Runs profiles and scorecards.
SQL Service Module	Runs SQL queries from a third-party client tool to an SQL data service.
Workflow Orchestration Service Module	Runs workflows.

17. Click **Next**.

    The **New Data Integration Service - Step 6 of 14** page appears.

    You can configure the HTTP proxy server properties to redirect HTTP requests to the Data Integration Service. You can configure the HTTP configuration properties to filter the web services client machines that can send requests to the Data Integration Service. You can configure these properties after you create the service.
18. Accept the default values for the HTTP proxy server and HTTP configuration properties and click **Next**.

    The **New Data Integration Service - Step 7 of 14** page appears.

    The Data Integration Service uses the result set cache properties to use cached results for SQL data service queries and web service requests. You can configure the properties after you create the service.
19. Accept the default values for the result set cache properties and click **Next**.

    The **New Data Integration Service - Step 8 of 14** page appears.
20. If you created the profiling warehouse database for the Data Integration Service, select the Profiling Service module.
21. If you created the workflow database for the Data Integration Service, select the Workflow Orchestration Service module.
22. Verify that the remaining modules are not selected.

    You can configure properties for the remaining modules after you create the service.
23. Click **Next**.

    The **New Data Integration Service - Step 11 of 14** page appears.
24. If you created the profiling warehouse database for the Data Integration Service, click **Select** to select the database connection. Select the profiling warehouse connection that you created for the service to access the database.
25. Select whether or not content exists in the profiling warehouse database.

    If you created a new profiling warehouse database, select **No content exists under specified connection string**.

26. Click **Next**.

    The **New Data Integration Service - Step 12 of 14** page appears.

27. Accept the default values for the advanced profiling properties and click **Next**.

    The **New Data Integration Service - Step 14 of 14** page appears.

28. If you created the workflow database for the Data Integration Service, click **Select** to select the database connection. Select the workflow database connection that you created for the service to access the database.

29. Click **Finish**.

    The domain creates and enables the Data Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the Data Integration Service

After you create the Data Integration Service, perform the following tasks:

- Verify the host file configuration on UNIX.
- Create other application services.

Verify the Host File Configuration on UNIX

If you configured the Data Integration Service on UNIX to launch jobs as separate processes, verify that the host file on the node that runs the service contains a localhost entry. Otherwise, jobs fail when the **Launch Jobs as Separate Processes** property for the Data Integration Service is enabled.

Note: Windows does not require a localhost entry in the host file.

Verify the Maximum Heap Size for Data Integration Service

If you work with rule specifications in the Analyst tool or in the Developer tool, verify the Maximum Heap Size property on the Data Integration Service. The property determines the amount of memory that the Data Integration Service can use to test rule specifications and to run mappings that contain rule specifications.

Find the Maximum Heap Size property in the Advanced Properties on the Data Integration Service. Verify that the Maximum Heap Size value is at least 2048 MB.

Create Other Services

After you create the Data Integration Service, create the application services that depend on the Data Integration Service.

Create the dependent services in the following order:

1. Analyst Service
2. Content Management Service
3. Search Service

Create and Configure the Analyst Service

The Analyst Service is an application service that runs the Analyst tool in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to the Analyst tool.

When you run profiles, scorecards, or mapping specifications in the Analyst tool, the Analyst Service connects to the Data Integration Service to perform the data integration jobs. When you work on Human tasks in the Analyst tool, the Analyst Service connects to the Data Integration Service to retrieve the task metadata from the workflow database.

When you view, create, or delete a Model repository object in the Analyst tool, the Analyst Service connects to the Model Repository Service to access the metadata. When you view data lineage analysis on scorecards in the Analyst tool, the Analyst Service sends the request to the Metadata Manager Service to run data lineage.

Create the Analyst Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Analyst Service, verify that you have created and enabled the following services:

- Model Repository Service

  If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Analyst Service can use to access the Model Repository Service.
- Data Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Analyst Service**.

   The **New Analyst Service** dialog box appears.
3. On the **New Analyst Service - Step 1 of 6** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Click **Next**.

   The **New Analyst Service - Step 2 of 6** page appears.
5. Enter the HTTP port number to use for communication from the Analyst tool to the Analyst Service.

6. To enable secure communication from the Analyst tool to the Analyst Service, select **Enable Secure Communication**.

   Enter the following properties to configure secure communication for the Analyst Service:

Property	Description
HTTPS Port	Port number that the Analyst tool runs on when you enable secure communication. Use a different port number than the HTTP port number.
Keystore File	Directory where the keystore file that contains the digital certificates is stored.
Keystore Password	Plain-text password for the keystore file. If this property is not set, the Analyst Service uses the default password `changeit`.
SSL Protocol	Optional. Indicates the protocol to be used. Set this property to `SSL`.

7. Select **Enable Service**.

   The Model Repository Service and the Data Integration Service must be running to enable the Analyst Service.

8. Click **Next**.

   The **New Analyst Service - Step 3 of 6** page appears.

9. Enter the following properties to associate the Model Repository Service with the Analyst Service:

Description	Property
Model Repository Service	Model Repository Service to associate with the service.
User name	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

10. To enable Analyst tool users to work on Human task data, set the **Data Integration Service** property to the Data Integration Service that you configure to run workflows.

    If Analyst tool users do not need to work on Human task records, do not configure this property.

11. Click **Next**.

    The **New Analyst Service - Step 4 of 6** page appears.

12. Enter the following run-time properties for the Analyst Service:

Property	Description
Data Integration Service	Data Integration Service to associate with the service. The Analyst Service manages the connection to the Data Integration Service that enables users to perform data preview, mapping specification, scorecard, and profile jobs in the Analyst tool. You can associate the Analyst Service with the Data Integration Service that you configured to run workflows. Or, you can associate the Analyst Service with different Data Integration Services for the different operations.
Flat File Cache Directory	Directory of the flat file cache where the Analyst tool stores uploaded flat files. The Data Integration Service must also be able to access this directory. If the Analyst Service and the Data Integration Service run on different nodes, configure the flat file directory to use a shared directory.
Metadata Manager Service	If you created a Metadata Manager Service that runs data lineage for scorecards in the Analyst tool, select the Metadata Manager Service. Or you can select the Metadata Manager Service that runs data lineage for the Analyst tool after you create the Analyst Service. If you do not want to run data lineage for scorecards, do not configure this property.

13. Click **Next**.

    The **New Analyst Service - Step 5 of 6** page appears.

14. Enter the directory to store the temporary business glossary files that the business glossary export process creates and the directory to store files that content managers attach to the Glossary assets. These directories must be on the node that runs the Analyst Service.

15. Click **Finish**.

    The domain creates and enables the Analyst Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the Analyst Service

After you create the Analyst Service, create the Search Service that depends on the Analyst Service.

Create and Configure the Content Management Service

The Content Management Service is an application service that manages reference data. A reference data object contains a set of data values that you can search while performing data quality operations on source data. The Content Management Service also compiles rule specifications into mapplets. A rule specification object describes the data requirements of a business rule in logical terms.

The Content Management Service uses the Data Integration Service to run mappings to transfer data between reference tables and external data sources. The Content Management Service also provides transformations, mapping specifications, and rule specifications with the following types of reference data:

- Address reference data
- Identity populations

- Probabilistic models and classifier models
- Reference tables

Create the Content Management Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Content Management Service, verify that you have created and enabled the following services:

- Model Repository Service

  If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Content Management Service can use to access the Model Repository Service.
- Data Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Content Management Service**.

   The **New Content Management Service** dialog box appears.
3. On the **New Content Management Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
HTTP Port	HTTP port number to use for the Content Management Service.
Data Integration Service	Data Integration Service to associate with the service. The Data Integration Service and the Content Management Service must run on the same node.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.

Property	Description
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.
Reference Data Location	Reference data warehouse connection that you created for the Content Management Service to access the reference data warehouse. Click **Select** to select the connection.

4. Click **Next**.

   The **New Content Management Service - Step 2 of 2** page appears.
5. Accept the default values for the security properties.
6. Select **Enable Service**.

   The Model Repository Service and Data Integration Service must be running to enable the Content Management Service.
7. Click **Finish**.

   The domain creates and enables the Content Management Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

Create and Configure the Search Service

The Search Service is an application service that manages search in the Analyst tool and Business Glossary Desktop.

By default, the Search Service returns search results from a Model repository, such as data objects, mapping specifications, profiles, reference tables, rules, scorecards, and business glossary terms. The search results can also include column profile results and domain discovery results from a profiling warehouse.

Create the Search Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Search Service, verify that you have created and enabled the following services:

1. Model Repository Service
   If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Search Service can use to access the Model Repository Service.
2. Data Integration Service
   Verify that the Model repository user has permissions to the Data Integration Service.
3. Analyst Service
   Verify that the Model repository user has permissions to the Analyst Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Search Service**.

   The **New Search Service** dialog box appears.

3. On the **New Search Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Click **Next**.

   The **New Search Service - Step 2 of 2** page appears.

5. Enter the following search properties for the Search Service:

Description	Property
Port Number	Port number to use for the Search Service.
Index Location	Directory that contains the search index files. Enter a directory on the machine that runs the Search Service. If the directory does not exist, Informatica creates the directory when it creates the Search Service.
Extraction Interval	Interval in seconds at which the Search Service extracts and indexes updated content. Default is 60 seconds.
Model Repository Service	Model Repository Service to associate with the service.
User Name	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Finish**.

   The domain creates the Search Service. The domain does not enable the Search Service during the creation process. You must enable the Search Service before users can perform searches in the Analyst tool and Business Glossary Desktop.

7. To enable the Search Service, select the service in the Navigator, and then click **Actions** > **Enable Service**.

   The Model Repository Service, Data Integration Service, and Analyst Service must be running to enable the Search Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

Create and Configure the PowerCenter Repository Service

The PowerCenter Repository Service is an application service that manages the PowerCenter repository. The PowerCenter repository stores metadata created by the PowerCenter Client and application services in a relational database.

When you access a PowerCenter repository object from the PowerCenter Client or the PowerCenter Integration Service, the client or service sends a request to the PowerCenter Repository Service. The PowerCenter Repository Service process fetches, inserts, and updates metadata in the PowerCenter repository database tables.

Create the PowerCenter Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **PowerCenter Repository Service**.

   The **New PowerCenter Repository Service** dialog box appears.
3. On the **New PowerCenter Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.

   The **New PowerCenter Repository Service - Step 2 of 2** page appears.

5. Enter the following properties for the PowerCenter repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	Password for the PowerCenter repository database user. Must be in 7-bit ASCII.
Connection String	Native connection string the PowerCenter Repository Service uses to access the repository database. Use the following native connect string syntax for each supported database: - `servername@databasename` for Microsoft SQL Server and Sybase. - `databasename.world` for Oracle. - `databasename` for IBM DB2.
Code Page	Repository database code page. The PowerCenter Repository Service uses the character set encoded in the database code page to write data. You cannot change the code page in the PowerCenter Repository Service properties after you create the PowerCenter Repository Service.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 and Sybase databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.

6. Select **No content exists under specified connection string. Create new content.**
7. Optionally, choose to create a global repository.

   After you create the service, you can promote a local repository to a global repository, but you cannot change a global repository to a local repository.
8. If your license has the team-based development option, you can optionally enable version control of the repository.

   After you create the service, you can convert a non-versioned repository to a versioned repository, but you cannot convert a versioned repository to a non-versioned repository.
9. Click **Finish**.

   The domain creates the PowerCenter Repository Service, starts the service, and creates content for the PowerCenter repository.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the PowerCenter Repository Service

After you create the PowerCenter Repository Service, perform the following tasks:

- Configure the PowerCenter Repository Service to run in the Normal mode.
- Create the PowerCenter repository user if the domain does not use Kerberos authentication.
- Create other application services.

Run the PowerCenter Repository Service in Normal Mode

After you create the PowerCenter Repository Service, it starts in exclusive mode and access is restricted to the administrator. Edit the service properties to run the service in normal operating mode to provide access to other users.

1. In the Administrator tool, click the **Manage** tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. Click **Properties**.
4. Click **Edit Repository Properties**.
5. In the **Operating Mode** field, select Normal.
6. Click **OK.**

   You must recycle the PowerCenter Repository Service for the changes to take effect.
7. Select **Actions** > **Recycle Service**.

Create the PowerCenter Repository User

If the domain does not use Kerberos authentication, the domain uses a user account to authenticate other application services that make requests to the PowerCenter Repository Service. You must create a user account and assign the user the Administrator role for the PowerCenter Repository Service.

When you create an application service that depends on the PowerCenter Repository Service, you provide the name of the PowerCenter Repository Service and of this PowerCenter repository user.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create User** to create a native user account.

   Note: If you set up LDAP authentication in the domain, you can use an LDAP user account for the PowerCenter repository user.
3. Enter the following properties for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs. The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? & The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.

Property	Description
Full Name	Full name for the user account. The full name cannot include the following special characters: < > “
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > “

4. Click **OK**.

   The user properties appear.
5. Click the **Privileges** tab.
6. Click **Edit**.

   The **Edit Roles and Privileges** dialog box appears.
7. On the **Roles** tab, expand the PowerCenter Repository Service.
8. Under **System Defined Roles**, select Administrator and click **OK**.

Create Other Services

After you create the PowerCenter Repository Service, create the application services that depend on the PowerCenter Repository Service.

You can create the following application services:

1. PowerCenter Integration Service
2. Metadata Manager Service
3. Web Services Hub Service

Create and Configure the PowerCenter Integration Service

The PowerCenter Integration Service is an application service that runs workflows and sessions for the PowerCenter Client.

When you run a workflow in the PowerCenter Client, the client sends the requests to the PowerCenter Integration Service. The PowerCenter Integration Service connects to the PowerCenter Repository Service to fetch metadata from the PowerCenter repository, and then runs and monitors the sessions and workflows.

Create the PowerCenter Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the PowerCenter Integration Service, verify that you created and enabled the PowerCenter Repository Service. If the domain does not use Kerberos authentication, verify that you created a

PowerCenter repository user that the PowerCenter Integration Service can use to access the PowerCenter Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **PowerCenter Integration Service**.

   The **New PowerCenter Integration Service** dialog box appears.
3. On the **New PowerCenter Integration Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Assign	Select **Node** to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.
5. On the **New PowerCenter Integration Service - Step 2 of 2** page, enter the following properties:

Property	Description
PowerCenter Repository Service	PowerCenter Repository Service you want to associate with the service.
Username	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

Property	Description
Password	Password associated with the PowerCenter repository user. Not available for a domain with Kerberos authentication.
Security Domain	LDAP security domain for the PowerCenter repository user. The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

6. Select the data movement mode that determines how the PowerCenter Integration Service handles character data. Choose ASCII or Unicode. Default is ASCII.

   In ASCII mode, the PowerCenter Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. In Unicode mode, the PowerCenter Integration Service recognizes multibyte character sets as defined by the supported code pages. Use Unicode mode when the sources or targets use 8-bit or multibyte character sets and contain character data.
7. Click **Finish**.
8. On the **Specify Code Pages** dialog box, assign a code page for the PowerCenter Integration Service.

   The code page for the PowerCenter Integration Service must be compatible with the code page of the associated repository.
9. Click **OK**.

   The domain creates the PowerCenter Integration Service. The domain does not enable the PowerCenter Integration Service during the service creation process.
10. To enable the PowerCenter Integration Service, select the service in the Navigator, and click **Actions** > **Enable Service**. The PowerCenter Repository Service must be running to enable the PowerCenter Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the PowerCenter Integration Service

After you create the PowerCenter Integration Service, create the Metadata Manager Service that depends on the PowerCenter Integration Service.

Create and Configure the Metadata Manager Service

The Metadata Manager Service is an application service that runs the Metadata Manager web client in the Informatica domain. The Metadata Manager Service manages the connections between service components and the users that have access to Metadata Manager.

When you load metadata into the Metadata Manager warehouse, the Metadata Manager Service connects to the PowerCenter Integration Service. The PowerCenter Integration Service runs workflows in the PowerCenter repository to read from metadata sources and load metadata into the Metadata Manager warehouse. When you use Metadata Manager to browse and analyze metadata, the Metadata Manager Service accesses the metadata from the Metadata Manager repository.

Create the Metadata Manager Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Metadata Manager Service, verify that you created and enabled the following services:

- PowerCenter Repository Service
  If the domain does not use Kerberos authentication, verify that you created a PowerCenter repository user that the Metadata Manager Service can use to access the PowerCenter Repository Service.
- PowerCenter Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Metadata Manager Service**.

   The **New Metadata Manager Service** dialog box appears.
3. On the **New Metadata Manager Service - Step 1 of 3** page, enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Specify the following properties of the associated repository service:

Property	Description
Associated Integration Service	Select the PowerCenter Integration Service used by Metadata Manager to load metadata into the Metadata Manager warehouse.
Repository User Name	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.
Repository Password	Password associated with the PowerCenter repository user. Not available for a domain with Kerberos authentication.
Security Domain	LDAP security domain for the PowerCenter repository user. The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

5. Click **Next**.

   The **New Metadata Manager Service - Step 2 of 3** page appears.

6. Enter the following database properties for the Metadata Manager repository:

Property	Description
Database Type	The type of the repository database.
Code Page	Metadata Manager repository code page. The Metadata Manager Service and the Metadata Manager application use the character set encoded in the repository code page when writing data to the Metadata Manager repository. You can enable the Metadata Manager Service only after you specify the code page.
Connect String	Native connect string to the Metadata Manager repository database. The Metadata Manager Service uses the connect string to create a connection object to the Metadata Manager repository in the PowerCenter repository. Use the following native connect string syntax for each supported database: - `servername@databasename` for Microsoft SQL Server. - `databasename.world` for Oracle. - `databasename` for IBM DB2.
Database User	The database user name for the repository.
Database Password	Password for the Metadata Manager repository database user. Must be in 7-bit ASCII.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.
Database Hostname	The name of the machine that hosts the database server.
Database Port	The port number on which you configure the database server listener service.
SID/Service Name	For Oracle databases. Indicates whether to use the SID or service name in the JDBC connection string. For Oracle RAC databases, select from Oracle SID or Oracle service name. For other Oracle databases, select Oracle SID.
Database Name	The name of the database server. Specify the full service name or SID for Oracle databases, service name for IBM DB2 databases, and database name for Microsoft SQL Server databases.

7. If you want to append parameters to the database connection URL, configure additional parameters in the **Additional JDBC Parameters** field. Enter the parameters as name=value pairs separated by semicolon characters (;). For example: `param1=value1;param2=value2`

You can use this property to specify the following parameters:

Parameter	Description
Backup server location	If you use a database server that is highly available such as Oracle RAC, enter the location of a backup server.
Oracle Advanced Security Option (ASO) parameters	If the Metadata Manager repository database is an Oracle database that uses ASO, enter the following additional parameters: `EncryptionLevel=[encryption level];EncryptionTypes=[encryption types];DataIntegrityLevel=[data integrity level];DataIntegrityTypes=[data integrity types]` **Note:** The parameter values must match the values in the `sqlnet.ora` file on the machine where the Metadata Manager Service runs.

Authentication information for Microsoft SQL Server	To authenticate the user credentials with Windows authentication and establish a trusted connection to a Microsoft SQL Server repository, enter the following text:
	`AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll].`
	`jdbc:informatica:sqlserver://[host]:[port];DatabaseName=[DB name];AuthenticationMethod=ntlm;LoadLibraryPath=[directory containing DDJDBCx64Auth04.dll]`
	When you use a trusted connection to connect to a Microsoft SQL Server database, the Metadata Manager Service connects to the repository with the credentials of the user logged in to the machine on which the service is running.
	To start the Metadata Manager Service as a Windows service with a trusted connection, configure the Windows service properties to log on with a trusted user account.

8. If the Metadata Manager repository database is configured for secure communication, you can configure additional JDBC parameters in the **Secure JDBC Parameters** field.

   Use this property to specify secure connection parameters such as passwords. The Administrator tool does not display secure parameters or parameter values in the Metadata Manager Service properties. Enter the parameters as name=value pairs separated by semicolon characters (;). For example: `param1=value1;param2=value2`.
   Enter the following secure database parameters:

Secure Database Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to `SSL`.
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate of the database server.
TrustStorePassword	Required. Password used to access the truststore file.
HostNameInCertificate	Host name of the machine that hosts the secure database. If you specify a host name, the Metadata Manager Service validates the host name included in the connection string against the host name in the SSL certificate.

Secure Database Parameter	Description
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. 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 the database server sends. Informatica ignores any truststore information that you specify.
KeyStore	Path and file name of the keystore file that contains the SSL certificates that the Metadata Manager Service sends to the database server.
KeyStorePassword	Password used to access the keystore file.

9. Click **Next.**

   The **New Metadata Manager Service - Step 3 of 3** page appears.

10. Enter the HTTP port number to use for the service.
11. To enable secure communications with the Metadata Manager Service, select **Enable Secured Socket Layer**.

    Enter the following properties to configure secure communication for the service:

Property	Description
HTTPS Port	Port number to use for a secure connection to the service. Use a different port number than the HTTP port number.
Keystore File	Path and file name of the keystore file that contains the private or public key pairs and associated certificates. Required if you use HTTPS connections for the service.
Keystore Password	Plain-text password for the keystore file.

12. Click **Finish**.

    The domain creates the Metadata Manager Service. The domain does not enable the Metadata Manager Service during the service creation process.

13. To enable the Metadata Manager Service, select the service in the Navigator and click **Actions** > **Enable Service**. The PowerCenter Repository Service and PowerCenter Integration Service must be running to enable the Metadata Manager Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

After You Create the Metadata Manager Service

After you create the Metadata Manager Service, perform the following tasks:

- Create the contents for the Metadata Manager repository.
- Create other application services.

When you create the Metadata Manager Service, you create the repository tables and import models for metadata sources.

1. In the Navigator, select the Metadata Manager Service.
2. Click **Actions** > **Repository Contents** > **Create**.
3. Click **OK**.

After you create the Metadata Manager Service, create the application services that depend on the Metadata Manager Service.

Create and Configure the Web Services Hub Service

The Web Services Hub Service is an application service in the Informatica domain that exposes PowerCenter functionality to external clients through web services.

The Web Services Hub Service receives requests from web service clients and passes them to the PowerCenter Integration Service or PowerCenter Repository Service based on the type of request. The PowerCenter Integration Service or PowerCenter Repository Service processes the requests and sends a response to the Web Services Hub. The Web Services Hub sends the response back to the web service client.

Create the Web Services Hub Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Web Services Hub Service, verify that you created and enabled the PowerCenter Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions** > **New** > **Web Services Hub**.

   The **New Web Services Hub Service** dialog box appears.
3. Enter the following properties:

Property	Description
Name	Name of the service. 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 service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Enter the following properties of the associated PowerCenter Repository Service:

Property	Description
Associated Repository Service	PowerCenter Repository Service you want to associate with the service.
Repository User Name	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. The Web Services Hub Service requires the repository user name even if Kerberos authentication is enabled.
Repository Password	Password associated with the PowerCenter repository user. The Web Services Hub Service requires the repository password even if Kerberos authentication is enabled.
Security Domain	LDAP security domain for the PowerCenter repository user. The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service.

5. Click **Next**.
6. Enter the following service properties:

Property	Description
URL Scheme	Indicates the security protocol that you configure for the Web Services Hub. You can choose one of the following options: - HTTP. Run the Web Services Hub on HTTP only. - HTTPS. Run the Web Services Hub on HTTPS only. - HTTP and HTTPS. Run the Web Services Hub in HTTP and HTTPS modes.
Hub Host Name	Name of the machine hosting the Web Services Hub.
Hub Port Number (HTTP)	Port number for the Web Services Hub running on HTTP. Default is 7333.
Hub Port Number (HTTPS)	Port number for the Web Services Hub running on HTTPS. Default is 7343.
Keystore File	Path and file name of the keystore file that contains the private or public key pairs and associated certificates. Required if you use HTTPS connections for the service.
Keystore Password	Plain-text password for the keystore file.
Internal Host Name	Optional. Host name on which the Web Services Hub listens for connections from the PowerCenter Integration Service.
Internal Port Number	Port number on which the Web Services Hub listens for connections from the PowerCenter Integration Service. Default is 15555.

7. Click **Finish**.

The domain creates the Web Services Hub Service. The domain does not enable the Web Services Hub Service during the service creation process.

8. To enable the Web Services Hub Service, select the service in the Navigator, and then click **Actions** > **Enable Service**.

After you create the service through the wizard, you can edit the properties or configure other properties.

Part V: Client Installation

This part contains the following chapters:

CHAPTER 12

Before You Install the Clients

This chapter includes the following topics:

Before You Install the Clients Overview

Before you install the Informatica clients on Windows, verify that the minimum system and third-party software requirements are met. If the machine where you install the Informatica clients is not configured correctly, the installation can fail.

Review the Patch Requirements

Before you install the Informatica clients, verify that the machine has the required operating system patches and libraries.

The following table lists the patches and libraries that the Informatica clients require on a Windows platform:

Platform	Operating System	Operating System Patch
Windows x64	10 64-bit	None required
Windows x64	2016 64-bit	None required

Verify Installation Requirements

Before you install the Informatica clients, verify the installation requirements to run the Informatica client tools are met.

You can install all the Informatica client tools on the same machine or on separate machines. You can also install the clients on multiple machines. The requirements for the Informatica clients depend on the client tools that you install.

Before you install the Informatica clients, verify the following installation requirements:

Disk space for the temporary files

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

Permissions to install the clients

Verify that the user account that you use to install the Informatica clients has write permission on the installation directory and Windows registry.

Minimum system requirements to run the Informatica client tools

The following table lists the minimum system requirements to run the Informatica client tools:

Client	Processor	RAM	Disk Space
PowerCenter Client	1 CPU	1GB	3 GB
Informatica Developer	1 CPU	1GB	6 GB

Verify Third-Party Software Requirements

Before you install the Informatica clients, verify that you installed the third-party software required by the clients.

PowerCenter Client Requirements

The PowerCenter Client installation includes Mapping Architect for Visio and Mapping Analyst for Excel.

If you plan to use Mapping Architect for Visio, install the following third-party software before you install the PowerCenter Client:

- Microsoft Visio version 2007 or 2010
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4

Important: If you do not install the correct version and service pack level of Microsoft .NET Framework, Mapping Architect for Visio will not install properly.

Mapping Analyst for Excel includes an Excel add-in that adds a Metadata menu or ribbon to Microsoft Excel. You can install the add-in only for Excel 2007 or 2010. If you plan to use Mapping Analyst for Excel, install the following third-party software before you install the PowerCenter Client:

- Microsoft Office Excel version 2007 or 2010
- Java version 1.8 or later

Data Transformation Requirements

If you plan to use Data Processor or Hierarchical-To-Relational transformations, install .NET Framework 4.0 or later before you install the Developer tool.

CHAPTER 13

Install the Clients

This chapter includes the following topics:

Install the Clients Overview

You can install the Informatica clients on Windows in graphical or silent mode.

Complete the pre-installation tasks to prepare for the installation. You can install the Informatica clients on multiple machines.

When you run the client installer, you can select the following Informatica client tools:

Informatica Developer

Informatica Developer is a client application that you use to create data objects, create and run mappings, and create virtual databases. You can also use Informatica Developer to run profiles and perform data discovery. Objects created in Informatica Developer are stored in a Model repository and are run by a Data Integration Service.

PowerCenter Client

The PowerCenter Client is a set of tools you can use to manage the PowerCenter repository, mappings, and sessions. The PowerCenter Client includes the following tools:

- PowerCenter Designer
- PowerCenter Mapping Architect for Visio
- PowerCenter Repository Manager
- PowerCenter Workflow Manager
- PowerCenter Workflow Monitor

Note: Informatica recommends that you install the Informatica services and the PowerCenter Client in different install directories because If you install the Informatica services and the PowerCenter Client in the same install directory, the service binaries will be uninstalled when you uninstall the PowerCenter Client.

Installing in Graphical Mode

You can install the Informatica clients in graphical mode on Windows.

1. Close all other applications.
2. Go to the root of the directory for the installation files and run install.bat as administrator.

   To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.

   If you encounter problems when you run the install.bat file from the root directory, run the following file:
   `<installer files directory>\client\install.exe`
3. Select **Install Informatica <Version> Clients** and click **Next**.

   The **Installation Pre-requisites** page displays the system requirements. Verify that all installation requirements are met before you continue the installation.
4. Click **Next**.

   On the **Application Client Selection** page, select the Informatica clients you want to install.

   You can install the following Informatica client applications on the same machine:

   - Informatica Developer
   - PowerCenter Client

   You can install multiple clients at the same time.
5. On the **Installation Directory** page, enter the absolute path for the installation directory.

   The installation directory must be on the current computer. The maximum length of the path must be less than 260 characters. The directory names in the path must not contain spaces or the following special characters: @|* $ # ! % ( ) { } [ ] , ; '

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
6. Click **Next**.
7. On the **Pre-Installation Summary** page, review the installation information, and click **Install**.

   The installer copies the Informatica client files to the installation directory.

   The **Post-installation Summary** page indicates whether the installation completed successfully.
8. Click **Done** to close the installer.

You can view the installation log files to get more information about the tasks performed by the installer.

Installing in Silent Mode

To install the Informatica clients without user interaction, install in silent mode.

Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the Informatica clients on multiple machines on the network or to standardize the installation across machines.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.

Configuring the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample SilentInput.properties file is stored in the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the SilentInput.properties file.
4. Use a text editor to open and modify the values of the properties in the file.

   The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
UPG_BACKUP_DIR	Directory of the previous version of the Informatica client that you want to upgrade.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.
CLIENT_COMP	Indicates whether to install PowerCenter Client. If the value is 1, PowerCenter Client will be installed. If the value is 0, PowerCenter Client will not be installed. Default is 1.

5. Save the properties file.

Running the Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file SilentInput.properties that you edited and resaved.

4. To run the silent installation, run silentInstall.bat.

   The silent installer runs in the background. The process can take a while. The silent installation is complete when the Informatica_<Version>_Client_InstallLog<timestamp>.log file is created in the installation directory.

   The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

CHAPTER 14

After You Install the Clients

This chapter includes the following topics:

Install Languages

To view languages other than the system locale and to work with repositories that use a UTF-8 code page, install additional languages on Windows for use with the Informatica clients.

You also must install languages to use the Windows Input Method Editor (IME).

1. Click **Start** > **Settings** > **Control Panel**.
2. Click **Regional Options**.
3. Under Language settings for the system, select the languages you want to install.
4. Click **Apply**.

If you change the system locale when you install the language, restart the Windows machine.

Configure the Client for a Secure Domain

When you enable secure communication within the domain, you also secure connections between the domain and Informatica client applications, such as the Developer tool. Based on the truststore files used, you might need to specify the location and password for the truststore files in environment variables on each client host.

You might need to set the following environment variables on each client host:

INFA_TRUSTSTORE

Set this variable to the directory that contains the truststore files for the SSL certificates. The directory must contain truststore files named `infa_truststore.jks` and `infa_truststore.pem`.

INFA_TRUSTSTORE_PASSWORD

Set this variable to the password for the `infa_truststore.jks` file. The password must be encrypted. Use the command line program pmpasswd to encrypt the password.

Informatica provides an SSL certificate that you can use to secure the domain. When you install the Informatica clients, the installer sets the environment variables and installs the truststore files in the following directory by default: `<Informatica installation directory>\clients\shared\security`

If you use the default Informatica SSL certificate, and the `infa_truststore.jks` and `infa_truststore.pem` are in the default directory, you do not need to set the INFA_TRUSTSTORE or INFA_TRUSTSTORE_PASSWORD environment variables.

You must set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables on each client host in the following scenarios:

You use a custom SSL certificate to secure the domain.

If you provide an SSL certificate to use to secure the domain, copy the `infa_truststore.jks` and `infa_truststore.pem` truststore files to each client host. You must specify the location of the files and the truststore password.

You use the default Informatica SSL certificate, but the truststore files are not in the default Informatica directory.

If you use the default Informatica SSL certificate, but the `infa_truststore.jks` and `infa_truststore.pem` truststore files are not in the default Informatica directory, you must specify the location of the files and the truststore password.

Important: If you push processing to a compute cluster and the Data Integration Service runs on a grid, import the certificates one time and then copy them to each Data Integration Service on the grid. Each time you import a certificate, the contents of the certificate are identical, but the hex values are different. As a result, concurrent mappings that run on the grid fail with initialization errors.

Configure the Developer Tool Workspace Directory

Configure Informatica Developer to write the workspace metadata to the machine where the user is logged in.

1. Go to the following directory: `<Informatica installation directory>\clients\DeveloperClient\configuration\`
2. Locate the config.ini file.
3. Create a backup copy of the config.ini file.
4. Use a text editor to open the config.ini file.
5. Add the `osgi.instance.area.default` variable to the end of the config.ini file and set the variable to the directory location where you want to save the workspace metadata. The file path cannot contain non-ANSI characters. Folder names in the workspace directory cannot contain the number sign (#) character. If folder names in the workspace directory contain spaces, enclose the full directory in double quotes.
   - If you run Informatica Developer from the local machine, set the variable to the absolute path of the workspace directory:

     ```
     osgi.instance.area.default=<Drive>/<WorkspaceDirectory>
     ```

     or

     ```
     osgi.instance.area.default=<Drive>\\<WorkspaceDirectory>
     ```
   - If you run Informatica Developer from a remote machine, set the variable to the directory location on the local machine:

     ```
     osgi.instance.area.default=\\\\<LocalMachine>/<WorkspaceDirectory>
     ```

or

```
osgi.instance.area.default=\\\\<LocalMachine>\\<WorkspaceDirectory>
```

The user must have write permission to the local workspace directory.

Informatica Developer writes the workspace metadata to the workspace directory. If you log into Informatica Developer from a local machine, Informatica Developer writes the workspace metadata to the local machine. If the workspace directory does not exist on the machine from which you logged in, Informatica Developer creates the directory when it writes the files.

You can override the workspace directory when you start Informatica Developer.

CHAPTER 15

Starting Informatica Clients

This chapter includes the following topics:

Starting the Developer Tool

When you start the Developer tool, you connect to a Model repository. The Model repository stores metadata created in the Developer tool. The Model Repository Service manages the Model repository. Connect to the repository before you create a project.

1. From the Windows Start menu, click **Programs** > **Informatica[Version]** > **Client** > **Developer Client** > **Launch Informatica Developer**.

   The first time you run the Developer tool, the Welcome page displays several icons. The Welcome page does not appear when you run the Developer tool subsequently.
2. Click **Workbench.**

   The first time you start the Developer tool, you must select the repository in which to save the objects you create.
3. Click **File** > **Connect to Repository**.

   The **Connect to Repository** dialog box appears.
4. If you have not configured a domain in the Developer tool, click **Configure Domains** to configure a domain.

   You must configure a domain to access a Model Repository Service.
5. Click **Add** to add a domain.

   The **New Domain** dialog box appears.
6. Enter the domain name, host name, and port number.
7. Click **Finish**.
8. Click **OK**.
9. In the **Connect to Repository** dialog box, click **Browse** and select the Model Repository Service.
10. Click **OK**.
11. Click **Next**.
12. Enter a user name and password.

13. Click **Finish**.

    The Developer tool adds the Model repository to the Object Explorer view. When you run the Developer tool the next time, you can connect to the same repository.

Starting the PowerCenter Client

When you start PowerCenter Client, you connect to a PowerCenter repository.

1. From the Windows Start menu, click **Programs** > **Informatica[Version]** > **Client** > **[Client Tool Name]**.

   The first time you run a PowerCenter Client tool, you must add a repository and connect to it.
2. Click **Repository** > **Add Repository**.

   The **Add Repository** dialog box appears.
3. Enter the repository and user name.
4. Click **OK**.

   The repository appears in the Navigator.
5. Click **Repository** > **Connect**.

   The Connect to Repository dialog box appears.
6. In the connection settings section, click **Add** to add the domain connection information.

   The **Add Domain** dialog box appears.
7. Enter the domain name, gateway host, and gateway port number.
8. Click **OK**.
9. In the **Connect to Repository** dialog box, enter the password for the Administrator user.
10. Select the security domain.
11. Click **Connect**.

    After you connect to the repository, you can create objects.

Troubleshooting the Client Installation

I installed the PowerCenter Client, but Mapping Architect for Visio does not appear in the Windows Start menu, and the MappingTemplate folder in the client directory is empty.

You must have the correct version and service pack level of the Microsoft .NET Framework for Mapping Architect for Visio to install properly.

Uninstall PowerCenter Client, install the correct version of the Microsoft .NET Framework, and reinstall PowerCenter Client.

Part VI: Uninstallation

This part contains the following chapter:

CHAPTER 16

Uninstallation

This chapter includes the following topics:

Uninstallation Overview

Uninstall Informatica to remove the Informatica server or clients from a machine.

The Informatica uninstallation process deletes all Informatica files and clears all Informatica configurations from a machine. The uninstallation process does not delete files that are not installed with Informatica. For example, the installation process creates temporary directories. The uninstaller does not keep a record of these directories and therefore cannot delete them. You must manually delete these directories for a clean uninstallation.

When you install the Informatica server or Informatica clients, the installer creates an uninstaller. The uninstaller is stored in the uninstallation directory.

The following table lists the uninstallation directory for each type of installation:

Installation	Uninstallation Directory Name
Informatica Server	`<Informatica installation directory>/Uninstaller_Server`
Informatica Clients	`<Informatica installation directory>/Uninstaller_Client`

To uninstall Informatica, use the uninstaller created during the installation. On UNIX, uninstall Informatica from the command line. On Windows, uninstall Informatica from the Windows Start menu or Control Panel.

Warning: If you installed the PowerCenter Client and the Informatica services in the same install directory, the service binaries will be uninstalled when you uninstall the PowerCenter Client.

Rules and Guidelines for Uninstallation

Use the following rules and guidelines when you uninstall Informatica components:

- The Informatica server uninstallation mode depends on the mode you use to install Informatica server. For example, you install Informatica server in console mode. When you run the uninstaller, it runs in console mode. The Informatica clients uninstallation mode does not depend on the mode you use to install Informatica clients. For example, you install Informatica clients in silent mode. When you run the uninstaller, it can run in graphical or silent mode.
- Uninstalling Informatica does not affect the Informatica repositories. The uninstaller removes the Informatica files. It does not remove repositories from the database. If you need to move the repositories, you can back them up and restore them to another database.
- Uninstalling Informatica does not remove the metadata tables from the domain configuration database. If you install Informatica again using the same domain configuration database and user account, you must manually remove the tables or choose to overwrite the tables. You can use the infasetup BackupDomain command to back up the domain configuration database before you overwrite the metadata tables. To remove the metadata tables manually, use the infasetup DeleteDomain command before you run the uninstaller.
- Uninstalling Informatica removes all installation files and subdirectories from the Informatica installation directory. Before you uninstall Informatica, stop all Informatica services and processes and verify that all of the files in the installation directory are closed. At the end of the uninstallation process, the uninstaller displays the names of the files and directories that could not be removed.
- The Informatica server installation creates the following folder for the files and libraries required by third party adapters built using the Informatica Development Platform APIs:
  `<Informatica installation directory>/services/shared/extensions`

  Uninstalling the Informatica server deletes this folder and any subfolders created under it. If you have adapter files stored in the /extensions folder, back up the folder before you start uninstallation.
- If you perform the uninstallation on a Windows machine that has the services and clients installed, you must back up the ODBC folder before you uninstall. Restore the folder after the uninstallation completes.

Informatica Server Uninstallation

You can uninstall the Informatica server in graphical mode or silent mode on Windows and in console mode or silent mode on UNIX.

Uninstalling on Windows

If the Informatica services and clients are installed on the same Windows machine, the clients and the server use the same ODBC folder. If you uninstall the client or the server, the uninstall process also removes the ODBC folder.

1. Before you uninstall the Informatica services or clients, copy the ODBC directory to a temporary directory on your local drive.

   For example, if you are uninstalling the Informatica services, copy the `<Informatica installation directory>\ODBC<version>` directory and its contents to `C:\temp`.
2. Perform the uninstallation.
3. After you uninstall the Informatica services or clients, re-create the ODBC directory path.

4. Copy the ODBC directory from the temporary directory to the re-created directory.

   For example, if you uninstalled the Informatica services, copy the ODBC folder and its contents to the Informatica installation directory.

Uninstalling the Informatica Server in Graphical Mode

If you installed the Informatica server in graphical mode, uninstall the Informatica server in graphical mode.

Uninstalling the Informatica Server in Graphical Mode on Windows

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Click **Start** > **Program Files** > **Informatica [Version]** > **Server** > **Uninstaller**.

   The **Uninstallation** page appears.
2. Click **Uninstall** to begin the uninstallation.

   After the installer deletes all of the Informatica files from the directory, the **Post-Uninstallation Summary** page appears.
3. Click **Done** to close the uninstaller.

After you uninstall the the Informatica server, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica _<Version>_Client_InstallLog.log file
- Informatica_<Version>_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

Uninstalling the Informatica Server in Console Mode

If you installed the Informatica server in console mode, uninstall the Informatica server in console mode.

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Go to the following directory:

   ```
   <Informatica installation directory>/Uninstaller_Server
   ```
2. Type the following command to run the uninstaller:

   ```
   ./uninstaller
   ```

   If you installed the Informatica server in console mode, the uninstaller launches in console mode.

Uninstalling the Informatica Server in Console Mode on UNIX

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Go to the following directory:

   ```
   <Informatica installation directory>/Uninstaller_Server
   ```

2. Type the following command to run the uninstaller:

   ```
   ./uninstaller
   ```

   If you installed the Informatica server in console mode, the uninstaller launches in console mode.

Uninstalling the Informatica Server in Silent Mode

If you installed the Informatica server in silent mode, uninstall the Informatica server in silent mode.

Uninstalling the Informatica Server in Silent Mode on UNIX

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Go to the following directory:

   ```
   <Informatica installation directory>/Uninstaller_Server
   ```

2. Type the following command to run the silent uninstaller:

   ```
   ./uninstaller.sh
   ```

   If you installed the Informatica server in silent mode, the uninstaller launches in silent mode. The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if the installation directory is not accessible.

After you uninstall the the Informatica server, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica _<Version>_Services_InstallLog.log file
- Informatica_<Version>_Services_<timestamp>.log file

Uninstalling the Informatica Server in Silent Mode on Windows

Before you run the uninstaller, stop all Informatica services and processes and verify that all files in the installation directory are closed. The uninstallation process cannot remove files that are open or are being used by a service or process that is running.

1. Open a command prompt.
2. Go to the following directory:

   ```
   <Informatica installation directory>\Uninstaller_Server
   ```

3. Run the following file to run the silent uninstallation:

   ```
   Uninstall.bat
   ```

   The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if the installation directory is not accessible.

After you uninstall the Informatica server, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica _<Version>_Services_InstallLog.log file
- Informatica_<Version>_Services_<timestamp>.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

Informatica Clients Uninstallation

You can uninstall the Informatica clients in graphical mode and silent mode on Windows.

When you uninstall Informatica clients, the installer does not remove the environment variables, INFA_TRUSTSTORE, that it creates during installation. When you install a later version of Informatica clients, you must edit the environment variable to point to the new value of the SSL certificate.

For more information about setting the truststore environment variables, see Chapter 14, “After You Install the Clients” on page 226.

Uninstalling on Windows

If the Informatica services and clients are installed on the same Windows machine, the clients and the server use the same ODBC folder. If you uninstall the client or the server, the uninstall process also removes the ODBC folder.

1. Before you uninstall the Informatica services or clients, copy the ODBC directory to a temporary directory on your local drive.

   For example, if you are uninstalling the Informatica services, copy the `<Informatica installation directory>\ODBC<version>` directory and its contents to `C:\temp`.
2. Perform the uninstallation.
3. After you uninstall the Informatica services or clients, re-create the ODBC directory path.
4. Copy the ODBC directory from the temporary directory to the re-created directory.

   For example, if you uninstalled the Informatica services, copy the ODBC folder and its contents to the Informatica installation directory.

Uninstalling Informatica Clients in Graphical Mode

If you installed the Informatica clients in graphical mode, uninstall the Informatica clients in graphical mode.

Uninstalling Informatica Clients in Graphical Mode

1. Click **Start** > **Program Files** > **Informatica [Version]** > **Client** > **Uninstaller**.

   The **Uninstallation** page appears.
2. Click **Next**.

   The **Application Client Uninstall Selection** page appears.
3. Select the client applications you want to uninstall and click **Uninstall**.
4. Click **Done** to close the uninstaller.

   After the uninstallation is complete, the **Post-Uninstallation Summary** page appears, displaying the results of the uninstallation.

After you uninstall the Informatica clients, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica _<Version>_Client_InstallLog.log file
- Informatica_<Version>_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

Uninstalling Informatica Clients in Silent Mode

If you installed the Informatica clients in silent mode, uninstall the Informatica clients in silent mode.

Configuring the Properties File

Informatica provides a sample properties file that includes the properties required by the installer.

Customize the sample properties file to create a properties file and specify the options for your uninstallation. Then run the silent uninstallation.

1. Go to `<Informatica installation directory>/Uninstaller_Client`.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the SilentInput.properties file.
4. Use a text editor to open and modify the values of the properties file.

   The following table describes the properties that you can modify:

Property Name	Description
DXT_COMP	Indicates whether to uninstall Informatica Developer. If the value is 1, the Developer tool will be uninstalled. If the value is 0, the Developer tool will not be uninstalled. Default is 1.
CLIENT_COMP	Indicates whether to uninstall PowerCenter Client. If the value is 1, PowerCenter Client will be uninstalled. If the value is 0, PowerCenter Client will not be uninstalled. Default is 1.

5. Save the `SilentInput.properties` file.

Running the Silent Uninstaller

After you configure the properties file, run the silent uninstallation.

1. Go to `<Informatica installation directory>/Uninstaller_Client`.
2. To run the silent installation, double-click the `uninstaller.bat` or `uninstaller.exe` file.

   The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if you incorrectly configure the properties file or if the installation directory is not accessible.

After you uninstall the Informatica clients, delete any remaining folders and files from the Informatica installation directory. For example:

- Informatica _<Version>_Client_InstallLog.log file
- Informatica_<Version>_Client.log file

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

APPENDIX A

Starting and Stopping Informatica Services

This appendix includes the following topics:

Starting and Stopping Informatica Services Overview

On each node where you install Informatica, the installer creates a Windows service or UNIX daemon to run Informatica. When the installation completes successfully, the installer starts the Informatica service on Windows or the Informatica daemon on UNIX.

The Informatica service runs the Service Manager on the node. The Service Manager manages all domain functions and starts application services configured to run on the node. The method you use to start or stop Informatica depends on the operating system. You can use Informatica Administrator to shut down a node. When you shut down a node, you stop Informatica on the node.

You can configure the behavior of the Informatica Windows service.

The Informatica service also runs Informatica Administrator. You use Informatica Administrator to administer the Informatica domain objects and user accounts. Log in to Informatica Administrator to create the user accounts for users of Informatica and to create and configure the application services in the domain.

Starting and Stopping Informatica on UNIX

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

```
<Informatica installation directory>/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: 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.

Starting and Stopping Informatica on Windows

You can use the Services window in the Control Panel, the Start menu shortcut, or a command prompt to start or stop the Informatica services.

Starting or Stopping Informatica from the Start Menu

To start Informatica from the Windows Start menu, click **Programs** > **Informatica[Version]** > **Server**. Right-click **Start Informatica Services** and select **Run as Administrator**.

To stop Informatica from the Windows Start menu, click **Programs** > **Informatica[Version]** > **Server**. Right-click **Stop Informatica Services** and select **Run as Administrator**.

Starting or Stopping Informatica from the Control Panel

The procedure to start or stop the Informatica Windows service is the same as for all other Windows services.

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Right-click **Services** and select **Run as Administrator**.
4. Right-click the Informatica service.
5. If the service is running, click **Stop**.

   If the service is stopped, click **Start**.

Starting or Stopping Informatica from a Command Prompt

You can run infaservice.bat from the command line to start and stop the Informatica services on Windows.

By default, infaservice.bat is installed in the following directory:

```
<Informatica installation directory>\tomcat\bin
```

1. Open a command prompt as administrator.

2. Go to the directory where infaservice.bat is located.
3. Enter the following command to start the Informatica services:

   ```
   infaservice.bat startup
   ```

   Enter the following command to stop the Informatica services:

   ```
   infaservice.bat shutdown
   ```

Configure the Informatica Windows Service

You can configure the behavior of the Informatica Windows service when the operating system starts or when the service fails. You can also configure the user account that logs in to the service.

Rules and Guidelines for the User Account

Consider the following rules and guidelines when you configure the user account that logs in to the service:

- If you store files on a network drive, use a system account instead of the Local System account to run the Informatica service.
- If you configure shared storage on a network drive to store files used by the domain or the application services that run on the domain, the user account that runs the Informatica service must have access to the shared location.
- If you want to use the Local System account, verify that the user starting the Informatica service has access to the network location.
- If the user that starts the Informatica service cannot access the shared storage location, service processes on the node fail or the node or domain will not start.
- If you configure a system user account, the user account must have the *Act as operating system* permission. For more information, see the Windows documentation.

Configuring the Informatica Windows Service

Use the Windows Control Panel to configure the user account that logs in to the Informatica Windows service and to configure the service restart option.

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Select **Services**.
4. Double-click Informatica <Version>.

   The **Informatica <Version> Properties** dialog box appears.
5. Click the **Log On** tab.
6. Select **This account**.
7. Enter the domain and user name or click **Browse** to locate a system user.
8. Enter and confirm the password for the selected user account.
9. Click the **Recovery** tab. Select the options to restart the Informatica service if the service fails.

For more information about configuring system accounts for services and service restart options on Windows, see the Windows documentation.

Stopping Informatica in Informatica Administrator

When you shut down a node using Informatica Administrator, you stop the Informatica service on that node.

You can abort the processes that are running or allow them to complete before the service shuts down. If you shut down a node and abort the repository service processes running on the node, you can lose changes that have not yet been written to the repository. If you abort a node running integration service processes, the workflows will abort.

1. Log in to Informatica Administrator.
2. In the Navigator, select the node to shut down.
3. On the Domain tab **Actions** menu, select **Shutdown Node**.

Rules and Guidelines for Starting or Stopping Informatica

Consider the following rules and guidelines when starting and stopping Informatica on a node:

- When you shut down a node, the node is unavailable to the domain. If you shut down a gateway node and do not have another gateway node in the domain, the domain is unavailable.
- When you start Informatica, verify that the port used by the service on the node is available. For example, if you stop Informatica on a node, verify that the port is not used by any other process on the machine before you restart Informatica. If the port is not available, Informatica will fail to start.
- If you do not use Informatica Administrator to shut down a node, any process running on the node will be aborted. If you want to wait for all processes to complete before shutting down a node, use Informatica Administrator.
- If you have two nodes in a domain with one node configured as a primary node for an application service and the other node configured as a backup node, start Informatica on the primary node before you start the backup node. Otherwise, the application service will run on the backup node and not the primary node.

APPENDIX B

Connecting to Databases from Windows

This appendix includes the following topics:

Connecting to Databases from Windows Overview

Configure connectivity to enable communication between clients, services, and other components in the domain.

To use native connectivity, you must install and configure the database client software for the database that you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To increase performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third party ODBC drivers that are Level 2 compliant or higher.

The Informatica installation includes DataDirect JDBC drivers. You can use these drivers without performing additional steps. You can also download JDBC Type 4 drivers from third-party vendors to connect to sources and targets. You can use any third-party JDBC driver that is JDBC 3.0 or later.

You must configure a database connection for the following services in the Informatica domain:

- PowerCenter Repository Service
- Model Repository Service

- Data Integration Service
- Analyst Service

Connecting to an IBM DB2 Universal Database from Windows

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Configuring Native Connectivity

You can configure native connectivity to an IBM DB2 database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. Verify that the following environment variable settings have been established by IBM DB2 Client Application Enabler (CAE):

   ```
   DB2HOME=C:\IBM\SQLLIB
   DB2INSTANCE=DB2
   DB2CODEPAGE=1208 (Sometimes required. Use only if you encounter problems. Depends on
   the locale, you may use other values.)
   ```

2. Verify that the PATH environment variable includes the IBM DB2 bin directory. For example:

   ```
   PATH=C:\WINNT\SYSTEM32;C:\SQLLIB\BIN;...
   ```

3. Configure the IBM DB2 client to connect to the database that you want to access. To configure the IBM DB2 client:
   a. Launch the IBM DB2 Configuration Assistant.
   b. Add the database connection.
   c. Bind the connection.
4. Run the following command in the IBM DB2 Command Line Processor to verify that you can connect to the IBM DB2 database:

   ```
   CONNECT TO <dbalias> USER <username> USING <password>
   ```

5. If the connection is successful, run the TERMINATE command to disconnect from the database. If the connection fails, see the database documentation.

Connecting to an Informix Database from Windows

Use ODBC to connect to an Informix database on Windows. Create an ODBC data source by using the DataDirect ODBC drivers installed with Informatica. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Note: If you use the DataDirect ODBC driver provided by Informatica, you do not need the database client. The ODBC wire protocols do not require the database client software to connect to the database.

Configuring ODBC Connectivity

You can configure ODBC connectivity to an Informix database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source using the DataDirect ODBC Wire Protocol driver for Informix provided by Informatica.
2. Verify that you can connect to the Informix database using the ODBC data source.

Connecting to Microsoft Access and Microsoft Excel from Windows

Configure connectivity to the Informatica components on Windows.

Install Microsoft Access or Excel on the machine where the Data Integration Service and PowerCenter Integration Service processes run. Create an ODBC data source for the Microsoft Access or Excel data you want to access.

Configuring ODBC Connectivity

You can configure ODBC connectivity to a Microsoft Access or Excel database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source using the driver provided by Microsoft.
2. To avoid using empty string or nulls, use the reserved words PmNullUser for the user name and PmNullPasswd for the password when you create a database connection.

Connecting to a Microsoft SQL Server Database from Windows

You can connect to a Microsoft SQL Server database through the ODBC or the OLEDB provider type.

Configuring Native Connectivity

You can configure native connectivity to the Microsoft SQL Server database by using the ODBC (default) or OLEDB provider types.

If you choose the ODBC provider type, you can enable the Use DSN option to use the DSN configured in the Microsoft ODBC Administrator as the connect string. If you do not enable the Use DSN option, you must specify the server name and database name in the connection properties.

If you choose the OLEDB provider type, you must install the Microsoft SQL Server Native Client to configure native connectivity to the Microsoft SQL Server database. If you cannot connect to the database, verify that you correctly entered all of the connectivity information.

You can download the Microsoft SQL Server Native Client from the Microsoft website.

When you upgrade from Informatica 9.x, the Microsoft SQL Server connection is set to the OLEDB provider type by default. You can upgrade all the Microsoft SQL Server connections to the ODBC provider type by using the following commands:

- If you are using PowerCenter, run the following command: pmrep upgradeSqlServerConnection
- If you are using the Informatica platform, run the following command: infacmd.sh isp upgradeSQLSConnection

For specific connectivity instructions, see the database documentation.

Rules and Guidelines for Microsoft SQL Server

Consider the following rules and guidelines when you configure ODBC connectivity to a Microsoft SQL Server database on Windows:

- If you want to use a Microsoft SQL Server connection without using a Data Source Name (DSN less connection), you must configure the odbcinst.ini environment variable.
- If you are using a DSN connection, you must add the entry "EnableQuotedIdentifiers=1" to the ODBC DSN. If you do not add the entry, data preview and mapping run fail.
- You can use the Microsoft SQL Server NTLM authentication on a DSN less Microsoft SQL Server connection on the Microsoft Windows platform.
- When you use a DSN connection, you can configure the DataDirect specific properties. For more information about how to configure and use the Data Direct specific properties, see the DataDirect documentation.
- If the Microsoft SQL Server table contains a UUID data type and if you are reading data from an SQL table and writing data to a flat file, the data format might not be consistent between the OLE DB and ODBC connection types.
- You cannot use SSL connection on a DSN less connection. If you want to use SSL, you must use the DSN connection. Enable the Use DSN option and configure the SSL options in the odbc.ini file.
- If the Microsoft SQL Server uses Kerberos authentication, you must set the GSSClient property to point to the Informatica Kerberos libraries. Use the following path and filename: `<Informatica installation directory>/server/bin/libgssapi_krb5.so.2`. Create an entry for the GSSClient property in the DSN entries section in `odbc.ini` for a DSN connection or in the SQL Server wire protocol section in `odbcinst.ini` for a connection that does not use DSN.
- If you use the DataDirect ODBC driver to connect to Microsoft SQL Server, the Decimal data rounds off within the target database based on the scale values in the database tables. For example, if the scale is 5, the target Decimal data rounds off after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 rounds off to a target Decimal value of 12.34568.
- If you use Microsoft SQL Sever Native Client to connect to Microsoft SQL Server, the Decimal data truncates based on the specified scale in the target database tables. For example, if the scale is 5, the Decimal data truncation occurs after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 truncates to a target Decimal value of 12.34567.

Configuring Custom Properties for Microsoft SQL Server

You can configure custom properties for Microsoft SQL Server to improve bulk load performance.

1. Launch the PowerCenter client and connect to Workflow Manager.
2. Open a workflow and select a session that you want to configure.
3. Click the **Config Object** tab.
4. Change the value of the **Default Buffer Block** size to 5 MB. You can also use the following command:
   ```
   $INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>
   ```
   To get optimum throughput for a row size of 1 KB, you must set the Buffer Block size to 5 MB.
5. Click the **Properties** tab.
6. Change the **Commit Interval** to 100000 if the session contains a relational target.
7. Set the **DTM Buffer Size**. The optimum DTM Buffer Size is ((10 x Block Buffer size) x number of partitions).

Connecting to a Netezza Database from Windows

Install and configure ODBC on the machines where the PowerCenter Integration Service process runs and where you install the PowerCenter Client. You must configure connectivity to the following Informatica components on Windows:

- **PowerCenter Integration Service.** Install the Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity.
- **PowerCenter Client.** Install the Netezza ODBC driver on each PowerCenter Client machine that accesses the Netezza database. Use the Microsoft ODBC Data Source Administrator to configure ODBC connectivity. Use the Workflow Manager to create a database connection object for the Netezza database.

Configuring ODBC Connectivity

You can configure ODBC connectivity to a Netezza database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source for each Netezza database that you want to access.

   To create the ODBC data source, use the driver provided by Netezza.

   Create a System DSN if you start the Informatica service with a Local System account logon. Create a User DSN if you select the This account log in option to start the Informatica service.

   After you create the data source, configure the properties of the data source.
2. Enter a name for the new ODBC data source.
3. Enter the IP address/host name and port number for the Netezza server.
4. Enter the name of the Netezza schema where you plan to create database objects.
5. Configure the path and file name for the ODBC log file.

6. Verify that you can connect to the Netezza database.

   You can use the Microsoft ODBC Data Source Administrator to test the connection to the database. To test the connection, select the Netezza data source and click Configure. On the Testing tab, click Test Connection and enter the connection information for the Netezza schema.

Connecting to an Oracle Database from Windows

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Configuring Native Connectivity

You can configure native connectivity to an Oracle database to increase performance.

The following steps provide a guideline for configuring native connectivity using Oracle Net Services or Net8. For specific connectivity instructions, see the database documentation.

1. Verify that the Oracle home directory is set.

   For example:

   ```
   ORACLE_HOME=C:\Oracle
   ```

2. Verify that the PATH environment variable includes the Oracle bin directory.

   For example, if you install Net8, the path might include the following entry:

   ```
   PATH=C:\ORANT\BIN;
   ```

3. Configure the Oracle client to connect to the database that you want to access.

   Launch SQL*Net Easy Configuration Utility or edit an existing `tnsnames.ora` file to the home directory and modify it.

   Note: By default, the `tnsnames.ora` file is stored in the following directory: `<OracleInstallationDir>\network\admin`.

   Enter the correct syntax for the Oracle connect string, typically `databasename.world`. Make sure the SID entered here matches the database server instance ID defined on the Oracle server.

   Here is a sample `tnsnames.ora` file. Enter the information for the database.

   ```
   mydatabase.world =
      (DESCRIPTION
      (ADDRESS_LIST =
           (ADDRESS =
              (COMMUNITY = mycompany.world
              (PROTOCOL = TCP)
              (Host = mymachine)
              (Port = 1521)
           )
      )
      (CONNECT_DATA =
         (SID = MYORA7)
         (GLOBAL_NAMES = mydatabase.world)
   ```

4. Set the NLS_LANG environment variable to the locale, including language, territory, and character set, you want the database client and server to use with the login.

The value of this variable depends on the configuration. For example, if the value is american_america.UTF8, you must set the variable as follows:

```
NLS_LANG=american_america.UTF8;
```

To determine the value of this variable, contact the database administrator.

5. To set the default session time zone when the Data Integration Service reads or writes the Timestamp with Local Time Zone data, specify the ORA_SDTZ environment variable.

   You can set the ORA_SDTZ environment variable to any of the following values:

   - Operating system local time zone ('OS_TZ')
   - Database time zone ('DB_TZ')
   - Absolute offset from UTC (for example, '-05:00')
   - Time zone region name (for example, 'America/Los_Angeles')

   You can set the environment variable at the machine where Informatica server runs.

6. If the tnsnames.ora file is not in the same location as the Oracle client installation location, set the TNS_ADMIN environment variable to the directory where the tnsnames.ora file resides.

   For example, if the tnsnames.ora file is in the C:\oracle\files directory, set the variable as follows:

   ```
   TNS_ADMIN= C:\oracle\files
   ```

7. Verify that you can connect to the Oracle database.

   To connect to the database, launch SQL*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   Use the connect string as defined in the `tnsnames.ora` file.

Connecting to a Sybase ASE Database from Windows

For native connectivity, install the version of Open Client appropriate for your database version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

Configuring Native Connectivity

You can configure native connectivity to a Sybase ASE database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. Verify that the SYBASE environment variable refers to the Sybase ASE directory.

   For example:

   ```
   SYBASE=C:\SYBASE
   ```

2. Verify that the PATH environment variable includes the Sybase OCS directory.

For example:

```
PATH=C:\SYBASE\OCS-15_0\BIN;C:\SYBASE\OCS-15_0\DLL
```

3. Configure Sybase Open Client to connect to the database that you want to access.

   Use SQLEDIT to configure the Sybase client, or copy an existing SQL.INI file (located in the %SYBASE% \INI directory) and make any necessary changes.

   Select NLWNSCK as the Net-Library driver and include the Sybase ASE server name.

   Enter the host name and port number for the Sybase ASE server. If you do not know the host name and port number, check with the system administrator.

4. Verify that you can connect to the Sybase ASE database.

   To connect to the database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   User names and database names are case sensitive.

Connecting to a Teradata Database from Windows

Install and configure native client software on the machines where the Data Integration Service and PowerCenter Integration Service process runs and where you install Informatica Developer and the PowerCenter Client. To ensure compatibility between Informatica and databases, use the appropriate database client libraries. You must configure connectivity to the following Informatica components on Windows:

- **Integration Service.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the Data Integration Service and PowerCenter Integration Service run. You must also configure ODBC connectivity.
- **Informatica Developer.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each machine that hosts a Developer tool that accesses Teradata. You must also configure ODBC connectivity.
- **PowerCenter Client.** Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on each PowerCenter Client machine that accesses Teradata. Use the Workflow Manager to create a database connection object for the Teradata database.

Note: Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata.

Configuring ODBC Connectivity

You can configure ODBC connectivity to a Teradata database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Create an ODBC data source for each Teradata database that you want to access.

   To create the ODBC data source, use the driver provided by Teradata.

   Create a System DSN if you start the Informatica service with a *Local System account* logon. Create a User DSN if you select the *This account* log in option to start the Informatica service.

2. Enter the name for the new ODBC data source and the name of the Teradata server or its IP address.

To configure a connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC data source, leave the DefaultDatabase field and the user name and password fields empty.

3. Configure Date Options in the Options dialog box.

   In the Teradata Options dialog box, specify AAA for DateTime Format.

4. Configure Session Mode in the Options dialog box.

   When you create a target data source, choose ANSI session mode. If you choose ANSI session mode, Teradata does not roll back the transaction when it encounters a row error. If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the Integration Service cannot detect the rollback and does not report this in the session log.

5. Verify that you can connect to the Teradata database.

   To test the connection, use a Teradata client program, such as WinDDI, BTEQ, Teradata Administrator, or Teradata SQL Assistant.

APPENDIX C

Connecting to Databases from UNIX

This appendix includes the following topics:

Connecting to Databases from UNIX Overview

To use native connectivity, you must install and configure the database client software for the database that you want to access. To ensure compatibility between the application service and the database, install a client software that is compatible with the database version and use the appropriate database client libraries. To increase performance, use native connectivity.

The Informatica installation includes DataDirect ODBC drivers. If you have existing ODBC data sources created with an earlier version of the drivers, you must create new ODBC data sources using the new drivers. Configure ODBC connections using the DataDirect ODBC drivers provided by Informatica or third party ODBC drivers that are Level 2 compliant or higher.

You must configure a database connection for the following services in the Informatica domain:

- PowerCenter Repository Service
- Model Repository Service
- Data Integration Service
- Analyst Service

When you connect to databases from Linux or UNIX, use native drivers to connect to IBM DB2, Oracle, or Sybase ASE databases. You can use ODBC to connect to other sources and targets.

Connecting to an IBM DB2 Universal Database from UNIX

For native connectivity, install the version of IBM DB2 Client Application Enabler (CAE) appropriate for the IBM DB2 database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Configuring Native Connectivity

You can configure native connectivity to an IBM DB2 database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. To configure connectivity on the machine where the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process runs, log in to the machine as a user who can start a service process.
2. Set the DB2INSTANCE, INSTHOME, DB2DIR, and PATH environment variables.

   The UNIX IBM DB2 software always has an associated user login, often db2admin, which serves as a holder for database configurations. This user holds the instance for DB2.

   DB2INSTANCE. The name of the instance holder.

   Using a Bourne shell:

   ```
   $ DB2INSTANCE=db2admin; export DB2INSTANCE
   ```

   Using a C shell:

   ```
   $ setenv DB2INSTANCE db2admin
   ```

   INSTHOME. This is db2admin home directory path.

   Using a Bourne shell:

   ```
   $ INSTHOME=~db2admin
   ```

   Using a C shell:

   ```
   $ setenv INSTHOME ~db2admin>
   ```

   DB2DIR. Set the variable to point to the IBM DB2 CAE installation directory. For example, if the client is installed in the /opt/IBM/db2/V9.7 directory:

   Using a Bourne shell:

   ```
   $ DB2DIR=/opt/IBM/db2/V9.7; export DB2DIR
   ```

   Using a C shell:

   ```
   $ setenv DB2DIR /opt/IBM/db2/V9.7
   ```

   PATH. To run the IBM DB2 command line programs, set the variable to include the DB2 bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:$DB2DIR/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$DB2DIR/bin
   ```
3. Set the shared library variable to include the DB2 lib directory.

   The IBM DB2 client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load

dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

The shared library path must also include the Informatica installation directory *(server_dir)*.

Set the shared library environment variable based on the operating system.

The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

For example, use the following syntax for Solaris and Linux:

- Using a Bourne shell:

```
$ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib; export
LD_LIBRARY_PATH
```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$DB2DIR/lib
```

For AIX:

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$DB2DIR/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$DB2DIR/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

5. If the DB2 database resides on the same machine on which the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process runs, configure the DB2 instance as a remote instance.

   Run the following command to verify if there is a remote entry for the database:

   ```
   DB2 LIST DATABASE DIRECTORY
   ```

   The command lists all the databases that the DB2 client can access and their configuration properties. If this command lists an entry for “Directory entry type” of “Remote,” skip to 7.

6. If the database is not configured as remote, run the following command to verify whether a TCP/IP node is cataloged for the host:

   ```
   DB2 LIST NODE DIRECTORY
   ```

   If the node name is empty, you can create one when you set up a remote database. Use the following command to set up a remote database and, if needed, create a node:

   ```
   db2 CATALOG TCPIP NODE <nodename> REMOTE <hostname_or_address> SERVER <port number>
   ```

Run the following command to catalog the database:

```
db2 CATALOG DATABASE <dbname> as <dbalias> at NODE <nodename>
```

For more information about these commands, see the database documentation.

7. Verify that you can connect to the DB2 database. Run the DB2 Command Line Processor and run the command:

   ```
   CONNECT TO <dbalias> USER <username> USING <password>
   ```

   If the connection is successful, clean up with the `CONNECT RESET` or `TERMINATE` command.

Connecting to an Informix Database from UNIX

Use ODBC to connect to an Informix database on UNIX.

Configuring ODBC Connectivity

You can configure ODBC connectivity to an Informix database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. Set the ODBCHOME environment variable to the ODBC installation directory. For example:
   Using a Bourne shell:

   ```
   $ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME <Informatica server home>/ODBC7.1
   ```

2. Set the ODBCINI environment variable to the location of the odbc.ini file. For example, if the odbc.ini file is in the $ODBCHOME directory:

   Using a Bourne shell:

   ```
   ODBCINI=$ODBCHOME/odbc.ini; export ODBCINI
   ```

   Using a C shell:

   ```
    $ setenv ODBCINI $ODBCHOME/odbc.ini
   ```

3. Edit the existing odbc.ini file in the $ODBCHOME directory or copy this odbc.ini file to the UNIX home directory and edit it.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

4. Add an entry for the Informix data source under the section [ODBC Data Sources] and configure the data source. For example:

   ```
   [Informix Wire Protocol]
   Driver=/export/home/Informatica/10.0.0/ODBC7.1/lib/DWifcl27.so
   Description=DataDirect 7.1 Informix Wire Protocol
   AlternateServers=
   ApplicationUsingThreads=1
   CancelDetectInterval=0
   ConnectionRetryCount=0
   ConnectionRetryDelay=3
   Database=<database_name>
   HostName=<Informix_host>
   LoadBalancing=0
   LogonID=
   Password=
   PortNumber=<Informix_server_port>
   ```

```
ReportCodePageConversionErrors=0
ServerName=<Informix_server>
TrimBlankFromIndexName=1
```

5. Set the PATH and shared library environment variables by executing the script odbc.sh or odbc.csh in the $ODBCHOME directory.

   Using a Bourne shell:

   ```
   sh odbc.sh
   ```

   Using a C shell:

   ```
   source odbc.csh
   ```

6. Verify that you can connect to the Informix database using the ODBC data source. If the connection fails, see the database documentation.

Connecting to a Microsoft SQL Server Database from UNIX

Use the Microsoft SQL Server connection to connect to a Microsoft SQL Server database from a UNIX machine.

Configuring Native Connectivity

You can use the ODBC provider type while configuring a Microsoft SQL Server connection in UNIX.

The server name and database name are retrieved from the connect string if you enable the Use DSN option. The connect string is the DSN configured in the odbc.ini file. If you do not enable the Use DSN option, you must specify the server name and database name in the connection properties. If you cannot to connect to the database, verify that you correctly entered all of the connectivity information.

When you upgrade from Informatica 9.x, the Microsoft SQL Server connection is set to the OLEDB provider type by default. You can upgrade all your Microsoft SQL Server connections to use the ODBC provider type. You can upgrade all your Microsoft SQL Server connections to the ODBC provider type by using the following commands:

- If you are using PowerCenter, run the following command: pmrep upgradeSqlServerConnection
- If you are using the Informatica platform, run the following command: infacmd.sh isp upgradeSQLSConnection

After you run the upgrade command, you must set the environment variable on each machine that hosts the Developer tool and on the machine that hosts Informatica services in the following format:

```
ODBCINST=<INFA_HOME>/ODBC7.1/odbcinst.ini
```

After you set the environment variable, you must restart the node that hosts the Informatica services.

For specific connectivity instructions, see the database documentation.

Rules and Guidelines for Microsoft SQL Server (UNIX)

Consider the following rules and guidelines when you configure ODBC connectivity to a Microsoft SQL Server database on UNIX:

- If you want to use a Microsoft SQL Server connection without using a Data Source Name (DSN less connection), you must configure the odbcinst.ini environment variable.

- If you are using a DSN connection, you must add the entry "EnableQuotedIdentifiers=1" to the ODBC DSN. If you do not add the entry, data preview and mapping run fail.
- You can use the Microsoft SQL Server NTLM authentication on a DSN less Microsoft SQL Server connection on the Microsoft Windows platform.
- When you use a DSN connection, you can configure the DataDirect specific properties. For more information about how to configure and use the Data Direct specific properties, see the DataDirect documentation.
- If the Microsoft SQL Server table contains a UUID data type and if you are reading data from an SQL table and writing data to a flat file, the data format might not be consistent between the OLE DB and ODBC connection types.
- You cannot use SSL connection on a DSN less connection. If you want to use SSL, you must use the DSN connection. Enable the Use DSN option and configure the SSL options in the odbc.ini file.
- If the Microsoft SQL Server uses Kerberos authentication, you must set the GSSClient property to point to the Informatica Kerberos libraries. Use the following path and filename: `<Informatica installation directory>/server/bin/libgssapi_krb5.so.2`. Create an entry for the GSSClient property in the DSN entries section in `odbc.ini` for a DSN connection or in the SQL Server wire protocol section in `odbcinst.ini` for a connection that does not use DSN.
- If you use the DataDirect ODBC driver to connect to Microsoft SQL Server, the Decimal data rounds off within the target database based on the scale values in the database tables. For example, if the scale is 5, the target Decimal data rounds off after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 rounds off to a target Decimal value of 12.34568.
- If you use Microsoft SQL Sever Native Client to connect to Microsoft SQL Server, the Decimal data truncates based on the specified scale in the target database tables. For example, if the scale is 5, the Decimal data truncation occurs after the fifth digit that follows the decimal point. When the scale is 5, the input value 12.3456789 truncates to a target Decimal value of 12.34567.

Configuring SSL Authentication through ODBC

You can configure SSL authentication for Microsoft SQL Server through ODBC using the DataDirect New SQL Server Wire Protocol driver.

1. Open the odbc.ini file and add an entry for the ODBC data source and DataDirect New SQL Server Wire Protocol driver under the section [ODBC Data Sources].
2. Add the attributes in the odbc.ini file for configuring SSL.

   The following table lists the attributes that you must add to the odbc.ini file when you configure SSL authentication:

Attribute	Description
EncryptionMethod	The method that the driver uses to encrypt the data sent between the driver and the database server. Set the value to 1 to encrypt data using SSL.
ValidateServerCertificate	Determines whether the driver validates the certificate sent by the database server when SSL encryption is enabled. Set the value to 1 for the driver to validate the server certificate.
TrustStore	The location and name of the trust store file. The trust store file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication.

Attribute	Description
TrustStorePassword	The password to access the contents of the trust store file.
HostNameInCertificate	Optional. The host name that is established by the SSL administrator for the driver to validate the host name contained in the certificate.

Configuring Custom Properties for Microsoft SQL Server

You can configure custom properties for Microsoft SQL Server to improve bulk load performance.

1. Launch the PowerCenter client and connect to Workflow Manager.
2. Open a workflow and select a session that you want to configure.
3. Click the **Config Object** tab.
4. Change the value of the **Default Buffer Block** size to 5 MB. You can also use the following command:
   `$INFA_HOME/server/bin/./pmrep massupdate -t session_config_property -n "Default buffer block size" -v "5MB" -f $<folderName>`

   To get optimum throughput for a row size of 1 KB, you must set the Buffer Block size to 5 MB.
5. Click the **Properties** tab.
6. Change the **Commit Interval** to 100000 if the session contains a relational target.
7. Set the **DTM Buffer Size**. The optimum DTM Buffer Size is ((10 x Block Buffer size) x number of partitions).

Connecting to a Netezza Database from UNIX

Install and configure Netezza ODBC driver on the machine where the PowerCenter Integration Service process runs. Use the DataDirect Driver Manager in the DataDirect driver package shipped with the Informatica product to configure the Netezza data source details in the odbc.ini file.

Configuring ODBC Connectivity

You can configure ODBC connectivity to a Netezza database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the ODBCHOME, NZ_ODBC_INI_PATH, and PATH environment variables.

   ODBCHOME. Set the variable to the ODBC installation directory. For example:

   Using a Bourne shell:

   ```
   $ ODBCHOME=<Informatica server home>/ODBC7.1; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME =<Informatica server home>/ODBC7.1
   ```

PATH. Set the variable to the ODBCHOME/bin directory. For example:

Using a Bourne shell:

```
PATH="${PATH}:$ODBCHOME/bin"
```

Using a C shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin
```

NZ_ODBC_INI_PATH. Set the variable to point to the directory that contains the odbc.ini file. For example, if the odbc.ini file is in the $ODBCHOME directory:

Using a Bourne shell:

```
NZ_ODBC_INI_PATH=$ODBCHOME; export NZ_ODBC_INI_PATH
```

Using a C shell:

```
$ setenv NZ_ODBC_INI_PATH $ODBCHOME
```

3. Set the shared library environment variable.

   The shared library path must contain the ODBC libraries. It must also include the Informatica services installation directory `(server_dir)`.

   Set the shared library environment variable based on the operating system. Set the Netezza library folder to <NetezzaInstallationDir>/lib64.

   The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   For example, use the following syntax for Solaris and Linux:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/
     lib:<NetezzaInstallationDir>/lib64”
     export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/
     lib:<NetezzaInstallationDir>/lib64"
     ```

   For AIX

   - Using a Bourne shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:<NetezzaInstallationDir>/
     lib64; export LIBPATH
     ```

   - Using a C shell:

     ```
     $ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/
     lib:<NetezzaInstallationDir>/lib64
     ```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Add an entry for the Netezza data source under the section [ODBC Data Sources] and configure the data source.

For example:

```
[NZSQL]
Driver = /export/home/appsqa/thirdparty/netezza/lib64/libnzodbc.so
Description = NetezzaSQL ODBC
Servername = netezza1.informatica.com
Port = 5480
Database = infa
Username = admin
Password = password
Debuglogging = true
StripCRLF = false
PreFetch = 256
Protocol = 7.0
ReadOnly = false
ShowSystemTables = false
Socket = 16384
DateFormat = 1
TranslationDLL =
TranslationName =
TranslationOption =
NumericAsChar = false
```

For more information about Netezza connectivity, see the Netezza ODBC driver documentation.

5. Verify that the last entry in the odbc.ini file is InstallDir and set it to the ODBC installation directory.

   For example:

   ```
   InstallDir=<Informatica install directory>/<ODBCHOME directory>
   ```

6. Edit the .cshrc or .profile file to include the complete set of shell commands.
7. Restart the Informatica services.

Connecting to an Oracle Database from UNIX

For native connectivity, install the version of Oracle client appropriate for the Oracle database server version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

You must install compatible versions of the Oracle client and Oracle database server. You must also install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

Configuring Native Connectivity

You can configure native connectivity to an Oracle database to increase performance.

The following steps provide a guideline for configuring native connectivity through Oracle Net Services or Net8. For specific instructions, see the database documentation.

1. To configure connectivity for the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. Set the ORACLE_HOME, NLS_LANG, TNS_ADMIN, and PATH environment variables.

   ORACLE_HOME. Set the variable to the Oracle client installation directory. For example, if the client is installed in the /HOME2/oracle directory. set the variable as follows:

   Using a Bourne shell:

   ```
   $ ORACLE_HOME=/HOME2/oracle; export ORACLE_HOME
   ```

Using a C shell:

```
$ setenv ORACLE_HOME /HOME2/oracle
```

NLS_LANG. Set the variable to the locale (language, territory, and character set) you want the database client and server to use with the login. The value of this variable depends on the configuration. For example, if the value is american_america.UTF8, set the variable as follows:

Using a Bourne shell:

```
$ NLS_LANG=american_america.UTF8; export NLS_LANG
```

Using a C shell:

```
$ NLS_LANG american_america.UTF8
```

To determine the value of this variable, contact the administrator.

ORA_SDTZ. To set the default session time zone when the Data Integration Service reads or writes the Timestamp with Local Time Zone data, specify the ORA_SDTZ environment variable.

You can set the ORA_SDTZ environment variable to any of the following values:

- Operating system local time zone ('OS_TZ')
- Database time zone ('DB_TZ')
- Absolute offset from UTC (for example, '-05:00')
- Time zone region name (for example, 'America/Los_Angeles')

You can set the environment variable at the machine where Informatica server runs.

TNS_ADMIN. If the tnsnames.ora file is not in the same location as the Oracle client installation location, set the TNS_ADMIN environment variable to the directory where the tnsnames.ora file resides. For example, if the file is in the /HOME2/oracle/files directory, set the variable as follows:

Using a Bourne shell:

```
$ TNS_ADMIN=$HOME2/oracle/files; export TNS_ADMIN
```

Using a C shell:

```
$ setenv TNS_ADMIN=$HOME2/oracle/files
```

Note: By default, the `tnsnames.ora` file is stored in the following directory: `$ORACLE_HOME/network/admin`.

PATH. To run the Oracle command line programs, set the variable to include the Oracle bin directory.

Using a Bourne shell:

```
$ PATH=${PATH}:$ORACLE_HOME/bin; export PATH
```

Using a C shell:

```
$ setenv PATH ${PATH}:ORACLE_HOME/bin
```

3. Set the shared library environment variable.

   The Oracle client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load dynamically. To locate the shared libraries during run time, set the shared library environment variable.

   The shared library path must also include the Informatica installation directory `(server_dir)`.

   Set the shared library environment variable to LD_LIBRARY_PATH.

   For example, use the following syntax:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib; export
     LD_LIBRARY_PATH
     ```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$ORACLE_HOME/lib
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

   ```
   $ source .profile
   ```

   Using a C shell:

   ```
   $ source .cshrc
   ```

5. Verify that the Oracle client is configured to access the database.

   Use the SQL*Net Easy Configuration Utility or copy an existing `tnsnames.ora` file to the home directory and modify it.

   The `tnsnames.ora` file is stored in the following directory: `$ORACLE_HOME/network/admin`.

   Enter the correct syntax for the Oracle connect string, typically `databasename.world`.

   Here is a sample `tnsnames.ora` file. Enter the information for the database.

   ```
   mydatabase.world =
      (DESCRIPTION
      (ADDRESS_LIST =
           (ADDRESS =
              (COMMUNITY = mycompany.world
              (PROTOCOL = TCP)
              (Host = mymachine)
              (Port = 1521)
           )
      )
      (CONNECT_DATA =
         (SID = MYORA7)
         (GLOBAL_NAMES = mydatabase.world)
   ```

6. Verify that you can connect to the Oracle database.

   To connect to the Oracle database, launch SQL*Plus and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   Enter the user name and connect string as defined in the `tnsnames.ora` file.

Connecting to a Sybase ASE Database from UNIX

For native connectivity, install the version of Open Client appropriate for your database version. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

If you want to create, restore, or upgrade a Sybase ASE repository, set *allow nulls by default* to TRUE at the database level. Setting this option changes the default null type of the column to null in compliance with the SQL standard.

Configuring Native Connectivity

You can configure native connectivity to a Sybase ASE database to increase performance.

The following steps provide a guideline for configuring native connectivity. For specific instructions, see the database documentation.

1. To configure connectivity to the Data Integration Service, PowerCenter Integration Service, or PowerCenter Repository Service process, log in to the machine as a user who can start the server process.
2. Set the SYBASE and PATH environment variables.

   SYBASE. Set the variable to the Sybase Open Client installation directory. For example if the client is installed in the /usr/sybase directory:

   Using a Bourne shell:

   ```
   $ SYBASE=/usr/sybase; export SYBASE
   ```

   Using a C shell:

   ```
   $ setenv SYBASE /usr/sybase
   ```

   PATH. To run the Sybase command line programs, set the variable to include the Sybase OCS bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:/usr/sybase/OCS-15_0/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:/usr/sybase/OCS-15_0/bin
   ```
3. Set the shared library environment variable.

   The Sybase Open Client software contains a number of shared library components that the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes load dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

   The shared library path must also include the installation directory of the Informatica services *(server_dir)*.

   Set the shared library environment variable based on the operating system.

   The following table describes the shared library variables for each operating system.

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   For example, use the following syntax for Solaris and Linux:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;
     $SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64; export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;
     $SYBASE/OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
     ```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/OCS-15_0/lib3p;
$SYBASE/OCS-15_0/lib3p64; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$SYBASE/OCS-15_0/lib;$SYBASE/
OCS-15_0/lib3p;$SYBASE/OCS-15_0/lib3p64;
```

4. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

```
$ source .profile
```

   Using a C shell:

```
$ source .cshrc
```

5. Verify the Sybase ASE server name in the Sybase interfaces file stored in the $SYBASE directory.
6. Verify that you can connect to the Sybase ASE database.

   To connect to the Sybase ASE database, launch ISQL and enter the connectivity information. If you fail to connect to the database, verify that you correctly entered all of the connectivity information.

   User names and database names are case sensitive.

Connecting to a Teradata Database from UNIX

Install and configure native client software on the machines where the Data Integration Service or PowerCenter Integration Service process runs. To ensure compatibility between Informatica and databases, use the appropriate database client libraries.

Install the Teradata client, the Teradata ODBC driver, and any other Teradata client software that you might need on the machine where the Data Integration Service or PowerCenter Integration Service runs. You must also configure ODBC connectivity.

Note: Based on a recommendation from Teradata, Informatica uses ODBC to connect to Teradata. ODBC is a native interface for Teradata.

Configuring ODBC Connectivity

You can configure ODBC connectivity to a Teradata database.

The following steps provide a guideline for configuring ODBC connectivity. For specific instructions, see the database documentation.

1. To configure connectivity for the integration service process, log in to the machine as a user who can start a service process.
2. Set the TERADATA_HOME, ODBCHOME, and PATH environment variables.

   TERADATA_HOME. Set the variable to the Teradata driver installation directory. The defaults are as follows:

   Using a Bourne shell:

```
$ TERADATA_HOME=/opt/teradata/client/<version>; export TERADATA_HOME
```

Using a C shell:

```
$ setenv TERADATA_HOME /opt/teradata/client/<version>
```

ODBCHOME. Set the variable to the ODBC installation directory. For example:

Using a Bourne shell:

```
$ ODBCHOME=$INFA_HOME/ODBC<version>; export ODBCHOME
```

Using a C shell:

```
$ setenv ODBCHOME $INFA_HOME/ODBC<version>
```

PATH. To run the *ddtestlib* utility, to verify that the DataDirect ODBC driver manager can load the driver files, set the variable as follows:

Using a Bourne shell:

```
PATH="${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin"
```

Using a C shell:

```
$ setenv PATH ${PATH}:$ODBCHOME/bin:$TERADATA_HOME/bin
```

3. Set the shared library environment variable.

   The Teradata software contains multiple shared library components that the integration service process loads dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

   The shared library path must also include installation directory of the Informatica service *(server_dir)*.

   Set the shared library environment variable based on the operating system.

   The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   For example, use the following syntax for Solaris and Linux:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH="${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:

     $TERADATA_HOME/lib64:$TERADATA_HOME/odbc_64/lib";

     export LD_LIBRARY_PATH
     ```

   - Using a C shell:

     ```
     $ setenv LD_LIBRARY_PATH "${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib:
     $TERADATA_HOME/lib64:

     $TERADATA_HOME/odbc_64/lib"
     ```

   For AIX

   - Using a Bourne shell:

     ```
     $ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/
     lib64:$TERADATA_HOME/odbc_64/lib; export LIBPATH
     ```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib:$TERADATA_HOME/lib64:
$TERADATA_HOME/odbc_64/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

   ```
   $ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
   ```

   Add an entry for the Teradata data source under the section [ODBC Data Sources] and configure the data source.

   For example:

   ```
   MY_TERADATA_SOURCE=Teradata Driver
   [MY_TERADATA_SOURCE]
   Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
   Description=NCR 3600 running Teradata V1R5.2
   DBCName=208.199.59.208
   DateTimeFormat=AAA
   SessionMode=ANSI
   DefaultDatabase=
   Username=
   Password=
   ```

5. Set the DateTimeFormat to AAA in the Teradata data ODBC configuration.
6. Optionally, set the SessionMode to ANSI. When you use ANSI session mode, Teradata does not roll back the transaction when it encounters a row error.

   If you choose Teradata session mode, Teradata rolls back the transaction when it encounters a row error. In Teradata mode, the integration service process cannot detect the rollback, and does not report this in the session log.
7. To configure connection to a single Teradata database, enter the DefaultDatabase name. To create a single connection to the default database, enter the user name and password. To connect to multiple databases, using the same ODBC DSN, leave the DefaultDatabase field empty.

   For more information about Teradata connectivity, see the Teradata ODBC driver documentation.
8. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

   For example:

   ```
   InstallDir=<Informatica installation directory>/ODBC<version>
   ```

9. Edit the .cshrc or .profile to include the complete set of shell commands.
10. Save the file and either log out and log in again, or run the source command.

    Using a Bourne shell:

    ```
    $ source .profile
    ```

    Using a C shell:

    ```
    $ source .cshrc
    ```

11. For each data source you use, make a note of the file name under the Driver=<parameter> in the data source entry in odbc.ini. Use the *ddtestlib* utility to verify that the DataDirect ODBC driver manager can load the driver file.

    For example, if you have the driver entry:

    ```
    Driver=/u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

    run the following command:

    ```
    ddtestlib /u01/app/teradata/td-tuf611/odbc/drivers/tdata.so
    ```

12. Test the connection using BTEQ or another Teradata client tool.

Connecting to an ODBC Data Source

Install and configure native client software on the machine where the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service run. Also install and configure any underlying client access software required by the ODBC driver. To ensure compatibility between Informatica and the databases, use the appropriate database client libraries.

The Informatica installation includes DataDirect ODBC drivers. If the odbc.ini file contains connections that use earlier versions of the ODBC driver, update the connection information to use the new drivers. Use the System DSN to specify an ODBC data source on Windows.

1. On the machine where the application service runs, log in as a user who can start a service process.
2. Set the ODBCHOME and PATH environment variables.

   ODBCHOME. Set to the DataDirect ODBC installation directory. For example, if the install directory is `/export/home/Informatica/10.0.0/ODBC7.1`.

   Using a Bourne shell:

   ```
   $ ODBCHOME=/export/home/Informatica/10.0.0/ODBC7.1; export ODBCHOME
   ```

   Using a C shell:

   ```
   $ setenv ODBCHOME /export/home/Informatica/10.0.0/ODBC7.1
   ```

   PATH. To run the ODBC command line programs, like *ddtestlib*, set the variable to include the odbc bin directory.

   Using a Bourne shell:

   ```
   $ PATH=${PATH}:$ODBCHOME/bin; export PATH
   ```

   Using a C shell:

   ```
   $ setenv PATH ${PATH}:$ODBCHOME/bin
   ```

   Run the *ddtestlib* utility to verify that the DataDirect ODBC driver manager can load the driver files.
3. Set the shared library environment variable.

   The ODBC software contains a number of shared library components that the service processes load dynamically. Set the shared library environment variable so that the services can find the shared libraries at run time.

   The shared library path must also include the Informatica installation directory *(server_dir)*.

   Set the shared library environment variable based on the operating system.

   The following table describes the shared library variables for each operating system:

Operating System	Variable
Solaris	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
AIX	LIBPATH

   For example, use the following syntax for Solaris and Linux:

   - Using a Bourne shell:

     ```
     $ LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:$HOME/server_dir:$ODBCHOME/lib; export
     LD_LIBRARY_PATH
     ```

- Using a C shell:

```
$ setenv LD_LIBRARY_PATH $HOME/server_dir:$ODBCHOME:${LD_LIBRARY_PATH}
```

For AIX

- Using a Bourne shell:

```
$ LIBPATH=${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib; export LIBPATH
```

- Using a C shell:

```
$ setenv LIBPATH ${LIBPATH}:$HOME/server_dir:$ODBCHOME/lib
```

4. Edit the existing odbc.ini file or copy the odbc.ini file to the home directory and edit it.

   This file exists in $ODBCHOME directory.

```
$ cp $ODBCHOME/odbc.ini $HOME/.odbc.ini
```

   Add an entry for the ODBC data source under the section [ODBC Data Sources] and configure the data source.

   For example:

```
MY_MSSQLSERVER_ODBC_SOURCE=<Driver name or data source description>
[MY_SQLSERVER_ODBC_SOURCE]
Driver=<path to ODBC drivers>
Description=DataDirect 7.1 SQL Server Wire Protocol
Database=<SQLServer_database_name>
LogonID=<username>
Password=<password>
Address=<TCP/IP address>,<port number>
QuoteId=No
AnsiNPW=No
ApplicationsUsingThreads=1
```

   This file might already exist if you have configured one or more ODBC data sources.

5. Verify that the last entry in the odbc.ini is InstallDir and set it to the odbc installation directory.

   For example:

```
InstallDir=/export/home/Informatica/10.0.0/ODBC7.1
```

6. If you use the odbc.ini file in the home directory, set the ODBCINI environment variable.

   Using a Bourne shell:

```
$ ODBCINI=/$HOME/.odbc.ini; export ODBCINI
```

   Using a C shell:

```
$ setenv ODBCINI $HOME/.odbc.ini
```

7. Edit the .cshrc or .profile to include the complete set of shell commands. Save the file and either log out and log in again, or run the source command.

   Using a Bourne shell:

```
$ source .profile
```

   Using a C shell:

```
$ source .cshrc
```

8. Use the *ddtestlib* utility to verify that the DataDirect ODBC driver manager can load the driver file you specified for the data source in the odbc.ini file.

   For example, if you have the driver entry:

```
Driver = /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

   run the following command:

```
ddtestlib /export/home/Informatica/10.0.0/ODBC7.1/lib/DWxxxxnn.so
```

9. Install and configure any underlying client access software needed by the ODBC driver.

   Note: While some ODBC drivers are self-contained and have all information inside the .odbc.ini file, most are not. For example, if you want to use an ODBC driver to access Sybase IQ, you must install the Sybase IQ network client software and set the appropriate environment variables.

   To use the Informatica ODBC drivers (DWxxxxnn.so), manually set the PATH and shared library path environment variables. Alternatively, run the odbc.sh or odbc.csh script in the $ODBCHOME folder. This script will set the required PATH and shared library path environment variables for the ODBC drivers provided by Informatica.

Sample odbc.ini File

The following sample shows the entries for the ODBC drivers in the ODBC.ini file:

```
[ODBC Data Sources]
DB2 Wire Protocol=DataDirect 7.1 DB2 Wire Protocol
Informix Wire Protocol=DataDirect 7.1 Informix Wire Protocol
Oracle Wire Protocol=DataDirect 8.0 Oracle Wire Protocol
Sybase Wire Protocol=DataDirect 7.1 Sybase Wire Protocol
SQL Server Wire Protocol=DataDirect 8.0 SQL Server Wire Protocol
MySQL Wire Protocol=DataDirect 7.1 MySQL Wire Protocol
PostgreSQL Wire Protocol=DataDirect 7.1 PostgreSQL Wire Protocol
Greenplum Wire Protocol=DataDirect 7.1 Greenplum Wire Protocol

[ODBC]
IANAAppCodePage=4
InstallDir=/<Informatica installation directory>/ODBC7.1
Trace=0
TraceFile=odbctrace.out
TraceDll=/<Informatica installation directory>/ODBC7.1/lib/DWtrc27.so

[DB2 Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWdb227.so
Description=DataDirect 7.1 DB2 Wire Protocol
AccountingInfo=
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CatalogSchema=
CharsetFor65535=0
ClientHostName=
ClientUser=
#Collection applies to z/OS and iSeries only
Collection=
ConcurrentAccessResolution=0
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CurrentFuncPath=
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=1000
EnableBulkLoad=0
EncryptionMethod=0
```

```
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
PackageCollection=NULLID
PackageNamePrefix=DD
PackageOwner=
Pooling=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
TcpPort=50000
TrustStore=
TrustStorePassword=
UseCurrentSchema=0
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10

[Informix Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWifcl27.so
Description=DataDirect 7.1 Informix Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
CancelDetectInterval=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
HostName=<Informix_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<Informix_server_port>
ServerName=<Informix_server>
TrimBlankFromIndexName=1
UseDelimitedIdentifiers=0

[Oracle Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWora28.so
Description=DataDirect 8.0 Oracle Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
AccountingInfo=
Action=
ApplicationName=
ArraySize=60000
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
CachedCursorLimit=32
CachedDescLimit=0
CatalogIncludesSynonyms=1
CatalogOptions=0
```

```
ClientHostName=
ClientID=
ClientUser=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
DataIntegrityLevel=0
DataIntegrityTypes=MD5,SHA1
DefaultLongDataBuffLen=1024
DescribeAtPrepare=0
EditionName=
EnableBulkLoad=0
EnableDescribeParam=0
EnableNcharSupport=0
EnableScrollableCursors=1
EnableStaticCursorsForLongData=0
EnableTimestampWithTimeZone=0
EncryptionLevel=0
EncryptionMethod=0
EncryptionTypes=AES128,AES192,AES256,DES,3DES112,3DES168,RC4_40,RC4_56,RC4_128,
RC4_256
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
GSSClient=native
HostName=<Oracle_server>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LocalTimeZoneOffset=
LockTimeOut=-1
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Module=
Password=
Pooling=0
PortNumber=<Oracle_server_port>
ProcedureRetResults=0
ProgramID=
QueryTimeout=0
ReportCodePageConversionErrors=0
ReportRecycleBin=0
ServerName=<server_name in tnsnames.ora>
ServerType=0
ServiceName=
SID=<Oracle_System_Identifier>
TimestampeEscapeMapping=0
TNSNamesFile=<tnsnames.ora_filename>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WireProtocolMode=2

[Sybase Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWase27.so
Description=DataDirect 7.1 Sybase Wire Protocol
AlternateServers=
ApplicationName=
ApplicationUsingThreads=1
ArraySize=50
AuthenticationMethod=0
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
```

```
BulkLoadBatchSize=1024
BulkLoadFieldDelimiter=
BulkLoadRecordDelimiter=
Charset=
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
CursorCacheSize=1
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableBulkLoad=0
EnableDescribeParam=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
GSSClient=native
HostNameInCertificate=
InitializationString=
Language=
LoadBalancing=0
LoadBalanceTimeout=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
NetworkAddress=<Sybase_host,Sybase_server_port>
OptimizePrepare=1
PacketSize=0
Password=
Pooling=0
QueryTimeout=0
RaiseErrorPositionBehavior=0
ReportCodePageConversionErrors=0
SelectMethod=0
ServicePrincipalName=
TruncateTimeTypeFractions=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=

[SQL Server Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWsqls28.so
Description=DataDirect 8.0 SQL Server Wire Protocol
AlternateServers=
AlwaysReportTriggerResults=0
AnsiNPW=1
ApplicationName=
ApplicationUsingThreads=1
AuthenticationMethod=1
BulkBinaryThreshold=32
BulkCharacterThreshold=-1
BulkLoadBatchSize=1024
BulkLoadOptions=2
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableBulkLoad=0
EnableQuotedIdentifiers=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=1
GSSClient=native
HostName=<SQL_Server_host>
HostNameInCertificate=
```

```
InitializationString=
Language=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
PacketSize=-1
Password=
Pooling=0
PortNumber=<SQL_Server_server_port>
QueryTimeout=0
ReportCodePageConversionErrors=0
SnapshotSerializable=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
WorkStationID=
XML Describe Type=-10

[MySQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWmysql27.so
Description=DataDirect 7.1 MySQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=1024
EnableDescribeParam=0
EncryptionMethod=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
HostName=<MySQL_host>
HostNameInCertificate=
InteractiveClient=0
LicenseNotice=You must purchase commercially licensed MySQL database software or
a MySQL Enterprise subscription in order to use the DataDirect Connect for ODBC
for MySQL Enterprise driver with MySQL software.
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LogonID=
LoginTimeout=15
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<MySQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TreatBinaryAsChar=0
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1

[PostgreSQL Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWpsql27.so
Description=DataDirect 7.1 PostgreSQL Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=1
```

```
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<PostgreSQL_host>
HostNameInCertificate=
InitializationString=
KeyPassword=
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<PostgreSQL_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
TrustStore=
TrustStorePassword=
ValidateServerCertificate=1
XMLDescribeType=-10

[Greenplum Wire Protocol]
Driver=/<Informatica installation directory>/ODBC7.1/lib/DWgplm27.so
Description=DataDirect 7.1 Greenplum Wire Protocol
AlternateServers=
ApplicationUsingThreads=1
ConnectionReset=0
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
DefaultLongDataBuffLen=2048
EnableDescribeParam=0
EnableKeysetCursors=0
EncryptionMethod=0
ExtendedColumnMetadata=0
FailoverGranularity=0
FailoverMode=0
FailoverPreconnect=0
FetchTSWTZasTimestamp=0
FetchTWFSasTime=0
HostName=<Greenplum_host>
InitializationString=
KeyPassword=
KeysetCursorOptions=0
KeyStore=
KeyStorePassword=
LoadBalanceTimeout=0
LoadBalancing=0
LoginTimeout=15
LogonID=
MaxPoolSize=100
MinPoolSize=0
Password=
Pooling=0
PortNumber=<Greenplum_server_port>
QueryTimeout=0
ReportCodepageConversionErrors=0
TransactionErrorBehavior=1
XMLDescribeType=-10
```

Note: You might have to customize the DSN entries in the `ODBC.ini` file based on the third-party driver that you use. For more information about the DSN entries, see the corresponding third-party driver documentation.

APPENDIX D

Updating the DynamicSections Parameter of a DB2 Database

This appendix includes the following topics:

DynamicSections Parameter Overview

IBM DB2 packages contain the SQL statements to be executed on the database server. The DynamicSections parameter of a DB2 database determines the maximum number of executable statements that the database driver can have in a package. You can raise the value of the DynamicSections parameter to allow a larger number of executable statements in a DB2 package. To modify the DynamicSections parameter, connect to the database using a system administrator user account with BINDADD authority.

Updating the DynamicSections Parameter

Use the DataDirect Connect for JDBC utility to raise the value of the DynamicSections parameter in the DB2 database.

To use the DataDirect Connect for JDBC utility to update the DynamicSections parameter, complete the following tasks:

- Download and install the DataDirect Connect for JDBC utility.
- Run the Test for JDBC tool.

Downloading and Installing the DataDirect Connect for JDBC Utility

Download the DataDirect Connect for JDBC utility from the DataDirect download web site to a machine that has access to the DB2 database server. Extract the contents of the utility file and run the installer.

1. Go to the DataDirect download site: http://www.datadirect.com/support/product-documentation/downloads
2. Choose the Connect for JDBC driver for an IBM DB2 data source.

3. Register to download the DataDirect Connect for JDBC Utility.
4. Download the utility to a machine that has access to the DB2 database server.
5. Extract the contents of the utility file to a temporary directory.
6. In the directory where you extracted the file, run the installer.

The installation program creates a folder named testforjdbc in the installation directory.

Running the Test for JDBC Tool

After you install the DataDirect Connect for JDBC Utility, run the Test for JDBC tool to connect to the DB2 database. You must use a system administrator user account with the BINDADD authority to connect to the database.

1. In the DB2 database, set up a system adminstrator user account with the BINDADD authority.
2. In the directory where you installed the DataDirect Connect for JDBC Utility, run the Test for JDBC tool.

   On Windows, run testforjdbc.bat. On UNIX, run testforjdbc.sh.
3. On the Test for JDBC Tool window, click Press Here to Continue.
4. Click Connection > Connect to DB.
5. In the Database field, enter the following text:

   ```
   jdbc:datadirect:db2://
   HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackag
   e=TRUE;DynamicSections=3000
   ```

   HostName is the name of the machine hosting the DB2 database server.

   PortNumber is the port number of the database.

   DatabaseName is the name of the DB2 database.
6. In the User Name and Password fields, enter the system administrator user name and password you use to connect to the DB2 database.
7. Click Connect, and then close the window.

APPENDIX E

Installation and Configuration Checklist

This appendix includes the following topics:

Installation Checklist Overview

The installation and configuration checklist summarizes the tasks that you must perform to complete an installation.

Plan the Domain

To plan the domain, perform the following tasks:

- ❑ Plan the application services that will run in the domain. You must also plan for the associated services that connect to the application service and the relational databases that are required to create the application service.
- ❑ Decide whether to create one domain or a split domain. You might want to configure a split domain so that you can upgrade Metadata Manager without having to upgrade the primary components of your installation bundle at the same time.
- ❑ Plan for the following application services based on the license key generated for your organization:
  - Analyst Service
  - Content Management Service
  - Data Integration Service
  - Metadata Manager Service
  - Model Repository Service
  - PowerCenter Integration Service
  - PowerCenter Repository Service
  - Search Service
  - Web Services Hub
- ❑ Verify that your machine meets the minimum system requirements to install the Informatica services.
- ❑ Verify that you have enough available disk space on the machine to support the installation.
- ❑ Verify that the port numbers to use for application service processes are available on the machines where you install the Informatica services.
- ❑ Verify that the database server has adequate disk space for the domain configuration repository and for the other databases required by the application services.
- ❑ Verify that the nodes in the domain have adequate hardware for the Service Manager and the application services that run on the nodes.
- ❑ Record information about the domain, nodes, and application services that you plan to create.

Related Topics:

- "Plan the Domain" on page 18

Prepare Databases for the Informatica Domain

To prepare the databases for the Informatica domain, perform the following tasks:

- ❑ Set up a database and user account for the domain configuration repository and for the repository databases associated with the application services.

- ❑ Verify the database requirements for the databases that you need:
  - Domain configuration repository. Stores configuration and user information in a domain configuration repository.
  - Data object cache database. Stores cached logical data objects and virtual tables for the Data Integration Service.
  - Exception management audit database. Stores data that describes the work that Analyst tool users perform on Human task instances.
  - Metadata Manager repository. Stores the Metadata Manager warehouse and models.
  - Model repository. Stores data and metadata corresponding to Informatica services and clients.
  - PowerCenter repository. Stores a collection of database tables that contain metadata.
  - Profiling warehouse. Stores profiling and scorecard results.
  - Reference data warehouse. Stores the data values for reference table objects that you define in a Model repository.
  - Workflow database. Stores run-time metadata for workflows.
- ❑ Install the database clients on the machine where each service runs based on the databases that the service accesses.
- ❑ Configure database client environment variables on the machines that run the following services:
  - Data Integration Service
  - PowerCenter Integration Service
  - PowerCenter Repository Service

Related Topics:

- " Prepare Databases for the Informatica Domain " on page 42

Single Sign-on for Informatica Web Applications

To enable the single sign-on for Informatica web applications, perform the following tasks:

- Create a security domain for web application user account.
- Export the Assertion Signing certificate from AD FS.
- Import the Assertion Signing certificate into the default Informatica truststore file on every gateway node within the Informatica domain.
- Configure AD FS to issue SAML tokens to Informatica web applications.
- Add the URL for each Informatica web application using single sign-on to AD FS.
- Get the Identity Provider URL

Prepare for Kerberos Authentication

To prepare for Kerberos authentication, perform the following tasks:

- ❑ Setup the Kerberos configuration file.
- ❑ Perform the following tasks to generate the service principal and keytab file name format:
  - Set the service principal to the node level or the process level based on your requirements.
  - Run the Informatica Kerberos SPN Format Generator.
- ❑ Review the SPN and keytab format text file to ensure that there are no errors.
- ❑ Create the service principal names and keytab files.

Related Topics:

- "Prepare for Kerberos Authentication Setup" on page 61

Before You Install the Services on Windows

Before you install the services on Windows, perform the following tasks:

- ❑ Read the Informatica Release Notes for updates to the installation and upgrade process.
- ❑ Review the patch requirements to verify that the machine has the required operating system patches and libraries.
- ❑ Back up the Data Transformation files that were created in a previous version.
- ❑ Review the environment variables you must configure to work with the Informatica installation.
- ❑ Create a system user account to perform the installation and to run the Informatica service.
- ❑ Set up keystore and truststore files if you want to configure secure communication for the domain and set up a secure connection to web client applications.
- ❑ Extract the installer files.
- ❑ Verify the license key.
- ❑ Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation.

Related Topics:

- "Before You Install the Services on Windows" on page 77

Before You Install the Services on UNIX

Before you install the services on UNIX, perform the following tasks:

- ❑ Read the Informatica Release Notes for updates to the installation and upgrade process.

- ❑ Review the patch requirements to verify that the machine has the required operating system patches and libraries.
- ❑ Install the Java Runtime Environment when you install Informatica on AIX.
- ❑ Back up the Data Transformation files that were created in a previous version.
- ❑ Review the environment variables you must configure to work with the Informatica installation.
- ❑ Create a system user account to perform the installation and to run the Informatica service.
- ❑ Set up keystore and truststore files if you want to configure secure communication for the domain and set up a secure connection to web client applications.
- ❑ Verify that the operating system meets the file descriptor requirement.
- ❑ Configure POSIX asynchronous I/O on any node where you want to run a PowerCenter Integration Service, when you install Informatica on IBM AIX.
- ❑ Extract the installer files.
- ❑ Verify the license key.
- ❑ Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation.

Related Topics:

- "Before You Install the Services on UNIX" on page 87

Informatica Services Installation

Use the Informatica server installer to install the Informatica services on a Windows or UNIX machine. You can install the Informatica services on multiple machines to create multiple nodes.

Related Topics:

- "Informatica Services Installation" on page 98

Complete the Domain Configuration

To complete the domain configuration after you install the Informatica services, perform the following tasks:

- ❑ Perform the following tasks to ensure the locale settings and code page compatibility:
  - Verify that the domain configuration database is compatible with the code pages of the application services that you create in the domain.
  - Verify that the locale settings on machines that access the Administrator tool and the Informatica client tools is compatible with the code pages of repositories in the domain.
  - Configure the locale environment variables on UNIX.

- ❑ Configure the following environment variables:
  - Informatica environment variables to store memory, domain, and location settings.
  - Library path environment variables on UNIX on the machines that run the Data Integration Service, PowerCenter Integration Service, and PowerCenter Repository Service processes.
  - Kerberos environment variables if you configure the Informatica domain to run on a network with Kerberos authentication.
- ❑ Configure the Windows firewall on the machine where you created the Informatica domain.

Related Topics:

- "Complete the Domain Configuration" on page 173

Prepare to Create the Application Services

Before you create the application services, perform the following tasks:

- ❑ Verify the setup for 64-bit Windows.
- ❑ Create directories for the Analyst Service to store temporary files.
- ❑ Create the service principal names and keytab files for the application services.
- ❑ Log in to Informatica Administrator.
- ❑ Create connections to the following databases that the application services access though native connectivity:
  - Data object cache database
  - Profiling warehouse database
  - Reference data warehouse
  - Workflow database

Related Topics:

- "Prepare to Create the Application Services" on page 179

Create the Application Services

To create the application services, perform the following tasks:

- ❑ Create the Model Repository Service.
  - Create the Model repository user if the domain does not use Kerberos authentication.

    Note: If you plan to monitor objects that run in the domain, create an additional Model Repository Service that is dedicated to storing monitoring data.

- ❑ Create the Data Integration Service.
  - Verify the host file configuration on UNIX.
  - If you work with rule specifications in the Analyst tool or the Developer tool, verify the Maximum Heap Size value.
- ❑ Create the Analyst Service.
- ❑ Create the Content Management Service.
- ❑ Create the Search Service.
- ❑ Create the PowerCenter Repository Service.
  - Configure the PowerCenter Repository Service to run in Normal mode.
  - Create the PowerCenter repository user if the domain does not use Kerberos authentication.
- ❑ Create the PowerCenter Integration Service.
- ❑ Create the Metadata Manager Service.
  - Create the contents for the Metadata Manager repository.
- ❑ Create the Web Services Hub Service.

Related Topics:

- "Create the Application Services" on page 187

Before You Install the Clients

Before you install the clients, perform the following tasks:

- ❑ Verify the disk space for temporary files.
- ❑ Verify that the user account that you use to install the Informatica clients has write permission on the installation directory and Windows registry.
- ❑ Verify the minimum system requirements to run the Informatica client tools.
- ❑ Verify that you installed the third-party software required by the PowerCenter client.

Related Topics:

- "Before You Install the Clients" on page 219

Install the Clients

Use the Informatica client installer to install the Informatica clients on Windows.

You can install the following Informatica client applications:

- ❑ Informatica Developer

- ❑ PowerCenter Client

Related Topics:

- "Install the Clients" on page 222

After You Install the Clients

After you install the clients, perform the following tasks:

- ❑ Install additional languages on Windows to view languages other than the system locale and to work with repositories that use a UTF-8 code page.
- ❑ If you configured secure communication for the domain, configure the Informatica truststore environment variables on the machines that host the Informatica clients.
- ❑ Configure the Developer tool to write the workspace metadata to the machine where the user is logged in.

Related Topics:

- "After You Install the Clients" on page 226

APPENDIX F

Split Domain Configuration for Metadata Manager

This appendix includes the following topics:

Split Domain Configuration for Metadata Manager Overview

In a split domain, the application services associated with the primary components of your product bundle run in one domain, and the application services associated with Metadata Manager run in a separate, secondary domain. You can create each domain on the same machine or on separate machines.

For example, your product bundle includes PowerCenter and Metadata Manager. In a split domain, the application services that you use to perform data integration operations with PowerCenter run in the primary domain. Therefore, the primary domain contains a PowerCenter Repository Service and a PowerCenter Integration Service.

The application services that you use to perform metadata extraction with Metadata Manager run in the secondary domain. Therefore, the secondary domain contains a Metadata Manager Service. It also contains a separate PowerCenter Repository Service and PowerCenter Integration Service that support metadata extraction operations but are not used for data integration operations.

When you create a split domain, you must duplicate some repositories. For example, you must create a separate domain configuration repository in each domain. If your product bundle includes PowerCenter and Metadata Manager, you must also create a separate PowerCenter repository in each domain. You must create each repository in a separate database schema.

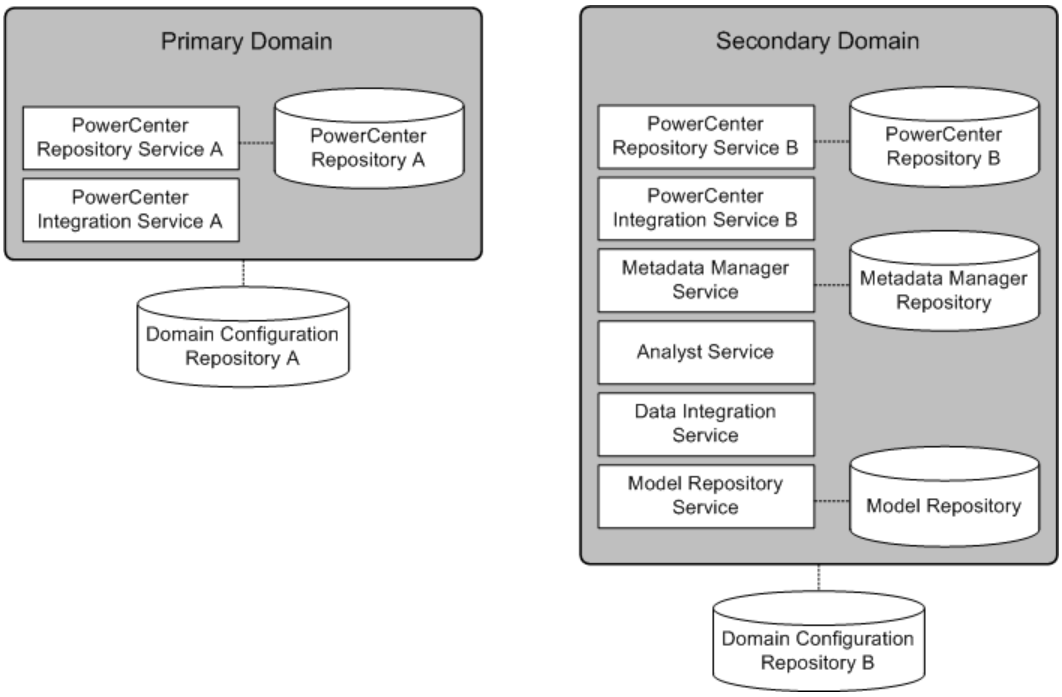
Note: Your license might limit the application services that you can duplicate and the product components that you run in each domain. For example, if your product bundle includes PowerCenter and Metadata Manager, you cannot run data integration operations in both domains. For questions about configuring a split domain without violating your license agreement, contact your Informatica products representative.

Split Domain Example

Configure a split domain when you use Metadata Manager and want to be able to upgrade Metadata Manager without upgrading other components in your product bundle.

For example, your product bundle includes PowerCenter, Metadata Manager, and Informatica Analyst (Analyst tool). You use PowerCenter for data integration. You use Metadata Manager for metadata extraction and data lineage. You use the Analyst tool to create and maintain business glossaries.

The following image shows the configuration for each domain:



In this configuration, all data integration operations are performed in the primary domain. The PowerCenter services in the secondary domain support the Metadata Manager workflows that extract metadata and load it into the Metadata Manager repository. You cannot use the PowerCenter services in the secondary domain for data integration. The Analyst Service, Data Integration Service, and Model Repository Service in the secondary domain support business glossary creation and maintenance. You cannot use these services for data integration.

Application Services Configuration

When you configure a split domain for Metadata Manager, the application services that you create might go in one domain or in both domains.

The following table lists the application services that you can configure and the domains in which you configure them:

Services	Domains
Analyst Service, Data Integration Service, Model Repository Service	Configure these services in the following domains: - Primary domain when you use these services for data integration. - Secondary domain when you do not perform data integration operations, but you use business glossaries or run data lineage on scorecards. - Both domains when you perform data integration in the primary domain and use business glossaries in the secondary domain. **Note:** You cannot perform data integration in the secondary domain, and you cannot create business glossaries in the primary domain.
Content Management Service, Search Service	Configure these services in the same domain as the Data Integration Service and Model Repository Service.
Metadata Manager Service	Configure this service in the secondary domain.
PowerCenter Integration Service, PowerCenter Repository Service	Configure these services in both domains. **Note:** In the secondary domain, you cannot use these services for data integration.
Web Services Hub	Configure this service in the primary domain.

Product Installation for a Split Domain

When you configure a split domain, you run the Informatica services installer each time you create a domain. When you create a domain, you configure the user authentication method and security protocol and create the domain configuration repository. You then create the required users and groups in the domain.

You can create the domains on one machine or on two different machines. If you create the domains on one machine, you must avoid possible port, node name, and directory conflicts.

When you install Informatica services, you specify the user authentication method and security protocol for the domain. Each domain can have a different user authentication method and different security protocol. However, it is easier to maintain the domains when the user authentication methods and security protocols are identical.

During installation, you create the domain configuration repository. You must create each domain configuration repository in a separate database schema with different user accounts. The repositories can be in the same database instance.

You might have to duplicate some users or groups across domain configuration repositories. For example, if a user creates PowerCenter mappings in the primary domain and uses Metadata Manager for data lineage in the secondary domain, the user must exist in the domain configuration repository in both domains.

Split Domain Pre-Installation Tasks

Before you install Informatica services in a split domain, verify your product license and create the required database user accounts and schemas.

Perform the following tasks:

- Verify that your license agreement allows you to duplicate the required application services.
- Verify that your license agreement supports the machine configuration that you want to implement, either on one machine or on two machines.
- If you need a different license file for each domain, verify that you have both license files.
- Create an additional database user account for the domain configuration repository of each domain.
- Create separate database schemas for the two domain configuration repositories and for other duplicated repositories.

Single Machine Rules and Guidelines

If you create both domains on one machine, there are rules and guidelines that you must consider.

Consider the following rules and guidelines:

- The machine must have enough RAM and disk space to meet the requirements of two installations.
- The installation directory for each domain must be unique.

  For example: `C:\Informatica\10.1.0_PC` and `C:\Informatica\10.1.0_MM`.
- The name of each domain must be unique.
- You must verify that there are no port conflicts.

  For example, if you accept the default node port as 6005 in the primary domain, you must specify a different node port in the secondary domain.
- On Windows, you might have to start one of the Windows services manually.

  When the domains are of the same major and minor version but different hotfixes, the names of the Informatica services are identical. Therefore, Windows starts only one instance of the Informatica services when the operating system starts. To start the other instance, run the following command at the command prompt:

  ```
  <Informatica services installation directory>\tomcat\bin\infaservice.bat startup
  ```

INDEX

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

W