H2L How-To Library

Informatica

# How to Install Informatica Using a Docker Utility

## Abstract

Informatica provides the Docker utility to install the Infomatica domain quickly. This article describes how to install Informatica using Docker image.

## Supported Versions

- PowerCenter 10.2 HotFix 1

## Table of Contents

Overview. . . . 2
Docker Utility Process. . . . 3
Prerequisites. . . . 3
Install Docker. . . . 3
Verify System Requirements. . . . 4
Create a System User Account. . . . 4
Set Up a Keystore and Truststore Files. . . . 4
Extract the Installer Files. . . . 6
Create a Volume Directory. . . . 6
Verify the License Key. . . . 6
Set Up the Domain Configuration Repository Database. . . . 6
Build the Informatica Docker Image. . . . 7
Run the Informatica Docker Image. . . . 8
Run the Image to Create a Domain . . . . 8
Run the Image to Join a Domain . . . . 14
Build the Informatica Docker Image in Silent Mode. . . . 18
Configuring the Properties File. . . . 18
Running the Silent Installer. . . . 19
Run the Docker Image in Silent Mode. . . . 19
Configuring the Properties File. . . . 19
Running the Docker Image in Silent Mode. . . . 26
Post-Installation Tasks. . . . 26
Complete the Domain Configuration. . . . 26
Create the Application Services. . . . 26
Install the PowerCenter Client. . . . 27
Starting and Stopping the Informatica Services on Linux . . . . 28

## Overview

Docker is an open source platform that provides an isolated environment called containers to run the applications. Docker allows independent containers to run within a single Linux instance.

The Informatica Docker utility provides an easy and quick process to install the Informatica domain.

When you run the Informatica Docker utility, you can build the Informatica docker image with base operating system and Informatica binaries and run the existing docker image to configure the Informatica domain. When you run the Informatica docker image you are prompted to create a domain or join a domain. You can create the application services in Informatica Administrator after the installation is complete.

# Docker Utility Process

The installation of the Informatica domain services using Docker utility consists of multiple phases.

Consider the following high-level tasks of the installation process:

1. Before you install the Informatica domain services, perform the following tasks to plan and prepare for the domain services installation:
    a. Plan the Informatica domain. Consider the number of nodes in the domain, the system requirements, domain configuration repository information, and permissions to read and write to the temp directory.
    b. Prepare the databases for the domain. Verify the database requirements and set up the databases.
    c. Set up the machines to meet the Linux requirements to ensure that you can successfully install and run the Informatica domain services.
2. Build the Informatica Docker image. Use the Informatica Docker utility to build the Informatica docker image with base operating system and Informatica binaries.
3. Run the Informatica Docker image. Use the Informatica Docker utility to run the existing docker image to configure the Informatica domain. The first time you run the image, you must create the domain. During the installation on the additional containers, you create worker nodes that you join to the domain.
4. After you install the Informatica domain 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.
    b. Create the application services in the Administrator tool.
5. Install the Informatica clients.

# Prerequisites

Before you install the Docker utility, verify that the machine meets the pre-installation requirements.

## *Install Docker*

Before you run the Informatica Docker utility, you must install Docker. You can use Docker to create, manage, and monitor the containers.
**Note:** It is recommended that you install Docker version 1.13.x.

## Verify System Requirements

Verify that your environment meets the minimum system requirements for the installation process.

The following table describes the system requirements for the installation:

| Requirements | Description |
|---|---|
| Red Hat Enterprise Linux version | 7.x |
| Kernel version | Linux 3.10.0-229.el7.x86_64<br>Linux 3.10.0-327.el7.x86_64<br>Linux 3.10.0-514.el7.x86_64<br>Linux 3.10.0-693.el7.x86_64<br>Linux 3.10.0-862.el7.x86_64 |
| Disk space | 50 GB |
| Memory | 16 GB |
| CPU cores | 16 |

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

## 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 a 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). To configure the security options, you can use the keystore and truststore packaged with the installer.

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`.

The keystore files must contain the root and intermediate SSL certificates.

**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_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

**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: Create Keystore and Truststore Files for Secure Communication in the Informatica Domain .

## 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.

Download the installer files. Use a zip utility to extract the .zip files to a directory on your machine. You can download the .zip file at https://marketplace.informatica.com/solutions/informatica_powercenter_docker_utility.

Use a native tar 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`.

## Create a Volume Directory

Create a temporary file system to store the Informatica license key and certificates. The directory must have read, write, and execute permissions.

## Verify the License Key

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

PowerCenter is provided as a Bring Your Own License (BYOL). Copy the license key file to a directory accessible to the user account that installs the product. You can use an existing Informatica license agreement or contact Informatica Global Customer Support if you do not have a license key or if you have an incremental license key.

## Set Up the Domain Configuration Repository Database

Set up a database and user account for the domain configuration repository. The domain configuration repository stores metadata for the 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.

You can create a database in your domain environment or in the container.

Use the following rules and guidelines when you set up the domain configuration database and user account:

- The database must be accessible to all gateway nodes in the Informatica domain.
- To prevent database errors in the domain configuration repository from affecting other repositories in the domain, create the domain configuration repository in a separate database schema with a different database user account.
- If you create more than one domain, each domain configuration repository must have a separate user account.
- Allow 200 MB of disk space for the database.

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

### 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.

### 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.
- 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.

## Build the Informatica Docker Image

1. Log in to the machine with a system user account. The user must have read, write, and execute permissions. You must have access to Docker server and client.
2. Close all other applications.
3. On a shell command line, run the install.sh file from the sudo directory.
4. On the Welcome screen, press **Enter** to continue the installation.

   The **Image Selection** section appears.
5. Press **1** to build the Informatica Docker image.

   The **Build Informatica Docker Image** section appears.
6. Enter the information to build Informatica Docker image.

   The following table describes the information to enter to build the Informatica Docker image:

| Prompt | Description |
|---|---|
| Enter the base OS image | Base operating system to create the docker image. Default is `registry.access.redhat.com/rhel7` |
| Informatica installer tar file location | Location of the Informatica binaries. |
| Informatica Docker base image name | Name of the docker image. Default is `informatica1020hf1:1.0` |

   The post installation summary appears.

You can view the installation log files to get more information about the tasks performed by the utility.

# Run the Informatica Docker Image

Run the docker image to create nodes in the Informatica domain. You can run the docker image to create a domain or join a domain.

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.

Create a domain if you are installing for the first time. Join a domain if you are installing on multiple containers and you have created a node on another container.

If you are installing on multiple containers, you can create multiple domains. If you create a domain, the node on the container where you install becomes a gateway node in the domain.

## *Run the Image to Create a Domain*

Create a domain the first time you run the image.

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 sudo directory.
4. On the Welcome screen, press Enter to **Continue** the installation.

   The **Image selection** section appears.
5. Press **2** to run the Informatica Docker image.

   The **Docker Container** section appears.
6. Enter the information to run the Informatica Docker image.

   The following table describes the information to enter to run the Informatica Docker image:

| Option | Description |
|---|---|
| Informatica docker image name | Name of the Informatica docker image. |
| Informatica container name | Name of the Informatica docker container. |
| Informatica host name | Host name of the Informatica domain. |
| Volume directory | Directory where the Informatica license key and certificates are stored. You must have read, write, and execute permissions on the directory. |
| Enter the qualified path to license file | Path and file name of the Informatica license key. |

   The **Domain selection** section appears.
7. 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.
8. 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.

9. 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 connection 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.<br>1 - Use the default keystore generated by the installer<br>2 - Specify the location and password of a custom keystore file<br>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.

   d. Select if you want to use the container database to configure Informatica domain.

      The following table describes the option to use the container database to configure Informatica domain:

| Option | Description |
|---|---|
| Use the container database to configure Informatica domain | Select whether to use the container database to configure Informatica domain:<br>1 - Yes<br>2 - No<br>If you select Yes, enter the database container name. If you select No, you can enter domain configuration repository database. |

   If you enabled secure connection for the domain, the **Domain Security - Secure Communication** section appears. If you did not enable secure connection for the domain, the **Domain Configuration Repository** section appears. Skip to step 11.

10. 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 certificates | Use the default SSL certificates provided by Informatica.<br>**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 custom SSL certificates | Use SSL certificates that you provide. You must specify the location of the keystore and truststore files.<br>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:

| Option | 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.

11. Select the database to use for the domain configuration repository.

The following table lists the databases you can use for the domain configuration repository:

| Option | Description |
|---|---|
| Database type | Type of database for the domain configuration repository. Choose from the following options:<br>1 - Oracle<br>2 - Microsoft SQL Server |

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.

12. Enter the properties for the database user account.

    The following table lists the properties for the database user account:

| Option | Description |
|---|---|
| Database user ID | Name for the domain configuration database user account. |
| User password | Password for the domain configuration database user account. |

13. 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 15.

    To create a domain configuration repository in an unsecure database, press 2.

14. If you do not create a secure domain configuration repository, enter the parameters for the database.

    a. 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:

| Option | 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. |

    b. 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**.

    c. 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:

| Option | Description |
|---|---|
| Database address | Host name and port number for the database. Default is `host_name:port_no` |
| Database service name | Service or database name :<br>- Oracle: Enter the service name.<br>- Microsoft SQL Server: Enter the database name. |
| Configure JDBC Parameters | Select whether to add additional JDBC parameters to the connection string:<br>1 - Yes<br>2 - No<br>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.
  You can use the following syntax in the JDBC connection string to connect to a secure database:
  **Oracle**

  ```
  jdbc:Informatica:oracle://
  host_name:port_no;ServiceName=service_name;EncryptionMethod=SSL;HostNameInCertific
  ate=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
  ```

15. 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:

| Option | 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. |

    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`
- 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`

16. 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:

| Option | 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:<br>- From 8 to 20 characters long<br>- Includes at least one uppercase letter<br>- Includes at least one lowercase letter<br>- Includes at least one number<br>- Does not contain spaces<br>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 **Domain and Node Configuration** section appears.

17. 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:

| Option | Description |
|---|---|
| Domain name | Name of the Informatica domain to create. The default domain name is Domain.<br>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. The node host name must be same as host name of the Informatica domain. |
| Node port number | Port number for the node. The default port number for the node is 6005. |
| 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:<br>- The name is not case sensitive and cannot exceed 128 characters.<br>- The name cannot include a tab, newline character, or the following special characters: % * + / ? ; < >.<br>- 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.<br>Not available if you configure the Informatica domain to run on a network with Kerberos authentication. |
| Confirm password | Enter the password again to confirm.<br>Not available if you configure the Informatica domain to run on a network with Kerberos authentication. |

The post-Installation summary section appears.

You can view the installation log files to get more information about the tasks performed by the utility.

## *Run the Image to Join a Domain*

If you want to create other nodes and join the domain, you must run the image to create a container for each node.

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 sudo directory.
4. On the Welcome screen, press **Enter** to continue the installation.

   The **Image Selection** section appears.
5. Press **2** to run Informatica image.

   The **Docker Container** section appears.
6. Enter the information to run the Informatica Docker image.

The following table describes the information to enter:

| Prompt | Description |
|---|---|
| Informatica docker image name | Name of the Informatica docker image. |
| Informatica container name | Name of the Informatica docker container. |
| Informatica host name | Host name of the Informatica domain to join. |
| Volume directory | Directory where the Informatica license key and certificates are stored. The directory must have read, write, and execute permissions. |
| Enter the qualified path to license file | Path and file name of the Informatica license key. |

The **Domain selection** section appears.

7. Press **2** to join a domain.

   The installer creates a node on the container where you install. You can specify the type of node to create and the domain to join.

8. Specify whether the domain you want to join has the secure communication option enabled.

   Press 1 to join an unsecured domain or press 2 to join a secure domain.

9. 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 | Choose whether to configure the node as a gateway or worker node.<br>1 - Yes<br>2 - No<br>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.

10. 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.<br>1 - Use the default keystore generated by the installer.<br>2 - Specify the location and password of a custom keystore file.<br>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.

11. 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 container 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. |
| Gateway container name | Container name of the master gateway node. |

The Domain Security - Encryption Key section appears.

12. 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 a volume directory.

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.<br>If you copied the encryption key file to the volume directory to make it accessible to the nodes in the domain, specify the path and file name of the encryption key file in the volume 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: `</home/Informatica/10.2.0/isp/config/keys`. |

13. 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 or IP address of the machine on which to create the node. The node host name must be same as host name of the Informatica domain. |
| 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. |
| Secure master domain database | Select if you want to secure the domain configuration repository database:<br>1- Yes<br>2- No<br>If you select Yes, enter the path and password for the database truststore. If you select No, post-installation summary section appears. |
| 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.<br>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.<br>Required if you join a gateway node to a domain that uses a secure domain configuration repository database. |

    The post-Installation summary section appears.

You can view the installation log files to get more information about the tasks performed by the utility.

# Build the Informatica Docker Image in Silent Mode

You can build the Docker image in silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options.

To build the Docker image 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, called SilentInput_BuildImage.properties, 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.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput_BuildImage.properties` file.
3. Use a text editor to open the file and modify the values of the installation parameters.

   The following example shows the contents of the file:

```
# Use the following guidelines when editing this file:
# * Use this file to install without user interaction. Save the file
#   with the following name:  SilentInput.properties
# * Any error condition that leads to failure, such as an invalid
#   installation directory, generates a log file in the user home
#   directory. For example: /home/<user name>/silentErrorLog.log

############################################################
# Informatica Installer Build Details
# Copyright (c) 1993-2018 Informatica LLC
# This software contains confidential and proprietary
# information of Informatica LLC.
# All Rights Reserved.
############################################################

#######
# Use this file (SilentInput.properties) to install Informatica services without user
interaction.
# Use this sample properties file to define the parameters for the silent installation.
# Use the following guidelines when you edit this file:
#     Back up the file before you modify it.
#     Any error condition that causes the installation to fail, such as an installation
directory that is not valid,
#     generates a log file in /home/<user name>. For example: /home/informatica/
silentErrorLog.log
#######

IMAGE_NAME=informatica:1020hf1

TAR_FILE_LOC=

OS_NAME=

##############################################################################################
###################### DO NOT MODIFY THE FOLLOWING PROPERTIES ######################
##############################################################################################

INSTALL_TYPE=0
BUILD_IMAGE=1
CONFIGURE_PCRS=0

#######
```

```
# After you create the properties file, save the file with the name
SilentInput.properties and
#     run the silent installer to build Docker image.
#######
```

4. 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.
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 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>_Docker_Utility<timestamp>.log` file is created in the directory where you extracted the Docker utility.

## Run the Docker Image in Silent Mode

To run the Informatica Docker utility in silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options.

To run the Informatica Docker utility 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, called SilentInput_RunImage.properties, 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.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput_RunImage.properties` file.
3. Use a text editor to open the file and modify the values of the installation parameters.

   The following example shows the contents of the file:

```
# Use the following guidelines when editing this file:
# * Use this file to install without user interaction. Save the file
#   with the following name:  SilentInput.properties
# * Any error condition that leads to failure, such as an invalid
#   installation directory, generates a log file in the user home
#   directory. For example: /home/<user name>/silentErrorLog.log

############################################################
# Informatica Installer Build Details
# Copyright (c) 1993-2018 Informatica LLC
# This software contains confidential and proprietary
# information of Informatica LLC.
# All Rights Reserved.
############################################################
```

```
#######
# Use this file (SilentInput.properties) to install Informatica services without user
interaction.
# Use this sample properties file to define the parameters for the silent installation.
# Use the following guidelines when you edit this file:
#     Back up the file before you modify it.
#     Any error condition that causes the installation to fail, such as an installation
directory that is not valid,
#     generates a log file in /home/<user name>. For example: /home/informatica/
silentErrorLog.log
#######


# Docker Container Details
IMAGE_NAME=

INFA_CONTAINER_NAME=

CONTAINER_HOST_NAME=

VOLUME_DIRECTORY=

#Set this variable if you want to join a domain
GATEWAY_CONTAINER_NAME=

USE_DB_CONTAINER=false

#Set the DB container name if USE_DB_CONTAINER=true
DB_CONTAINER_NAME=

# Set ENABLE_USAGE_COLLECTION  to 1 to accept the product usage toolkit end user license
agreement.
# You must set the value as 1 to install the Informatica platform.
# The product usage toolkit end user license agreement is available at: http://
www.informatica.com/us/eula/en-support-eula.aspx.
# As further described in the EULA, your use of the Informatica platform will enable the
product usage toolkit
# to collect certain product usage and failure information. You may disable this feature
at any time.
# For more information on how to disable this feature refer the Informatica
Administrator Guide.

ENABLE_USAGE_COLLECTION=0

# The LICENSE_KEY_LOC property represents the absolute path and file name of the license
key file.
#     Set the property if you are installing or upgrading Informatica.

LICENSE_KEY_LOC=/home/license.key


# The HTTPS_ENABLED property determines whether to secure the connection to Informatica
Administrator.
#     Value     0     Use HTTP connection. Set up an unsecure HTTP connection to
Informatica Administrator.
#     Value     1     Use HTTPS connection. Set up a secure HTTPS connection to the
Informatica Administrator.

HTTPS_ENABLED=0


# The DEFAULT_HTTPS_ENABLED property determines whether the installer creates a keystore
file.
#     Set the property if HTTPS_ENABLED=1 (uses HTTPS connection).
#     Value     0     Use a keystore file that you specify.
#     Value     1     Create a keystore and use it for the HTTPS connection.
```

```
DEFAULT_HTTPS_ENABLED=1


# The CUSTOM_HTTPS_ENABLED property determines whether the installer uses an existing
keystore file.
#     Value    0     Set the property to 0 if DEFAULT_HTTPS_ENABLED=1.
#     Value    1     Install Informatica using a keystore file that you specify. Set the
property to 1 if DEFAULT_HTTPS_ENABLED=0.

CUSTOM_HTTPS_ENABLED=0


# The KSTORE_PSSWD property represents the password for the keystore file.
#     Set the property to the plain text password for the keystore file if
CUSTOM_HTTPS_ENABLED=1.

KSTORE_PSSWD=MyKeystorePassword


#     Set the property to the absolute path and file name of the keystore file if
CUSTOM_HTTPS_ENABLED=1.

KSTORE_FILE_LOCATION=/home/MyKeystoreFile


# The HTTPS_PORT property represents the port number to use for the secure connection to
Informatica Administrator.

HTTPS_PORT=8443


# The CREATE_DOMAIN property determines whether to create an Informatica domain.
#     Value    0     Create a node and join the node to another domain created in a
previous installation. Set the property to 0 if JOIN_DOMAIN=1.
#     Value    1     Create a node and an Informatica domain.

CREATE_DOMAIN=1



#Keyword to use to create an encryption key to secure sensitive data in the domain. Set
the property only when you create a 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

PASS_PHRASE_PASSWD=



# The JOIN_DOMAIN property determines whether to join the node to another domain created
in a previous installation.
#     Value    0     Create a node and an Informatica domain. Set the property to 0 if
CREATE_DOMAIN=1.
#     Value    1     Create a node and join the node to another domain created in a
previous installation. Set the property to 1 if CREATE_DOMAIN=0.




JOIN_DOMAIN=0



# Directory that contains the encryption key on the master gateway node of the
Informatica domain that you want to join.
```

```
KEY_SRC_LOCATION=/home/temp/siteKey


# The SSL_ENABLED property enables or disables Transport Layer Security (TLS).
# Set the property to true to enable secure communication between services within the
domain.
# Set the property to true or false if CREATE_DOMAIN=1.
# If SSL_ENABLED=true, then set HTTPS_ENABLED=1 and set HTTPS_PORT.

SSL_ENABLED=false


################################################
#Provide TLS information for domain. Set TLS_CUSTOM_SELECTION equals to true if you want
domain level TLS option.

TLS_CUSTOM_SELECTION=false
################################
#Below fields are only required when you set  TLS_CUSTOM_SELECTION=true
NODE_KEYSTORE_DIR=/home/<username>/temp
NODE_KEYSTORE_PASSWD=
NODE_TRUSTSTORE_DIR=/home/<username>/temp
NODE_TRUSTSTORE_PASSWD=


# The SERVES_AS_GATEWAY property determines whether to create a gateway or worker node.
#     Set the property if JOIN_DOMAIN=1.
#     Value    0    The installer configures the node as a worker node.
#     Value    1    The installer configures the node as a gateway node.

SERVES_AS_GATEWAY=0



# The DB_TYPE property represents the database type for the domain configuration
database.
#     Set the property to one of the following database types (case-sensitive): Oracle
or MSSQLServer

DB_TYPE=Oracle/MSSQLServer


# The DB_UNAME property represents the database user account name for the domain
configuration repository.

DB_UNAME=UserName


# The DB_PASSWD property represents the database password for the database user account.

DB_PASSWD=UserPassword

# The DB_SSL_ENABLED property 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 property is set to True then the DB_CUSTOM_STRING_SELECTION property must be
# set to 1 to use the custom string option. The DB_CUSTOM_STRING property must include
# the following secure database parameters:
# EncryptionMethod=SSL;HostNameInCertificate=;ValidateServerCertificate=
# Set this property to 1 to join a domain where the Master Doamin Database is secured.

DB_SSL_ENABLED=false


# The TRUSTSTORE_DB_FILE indicates the 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_FILE=


# TRUSTSTORE_DB_PASSWD to the password for the truststore file for the secure domain
# configuration repository database.


TRUSTSTORE_DB_PASSWD=


# The SQLSERVER_SCHEMA_NAME property represents the name of the schema that will contain
domain configuration tables.
#     Set the property if DB_TYPE=MSSQLServer.
#     If SQLSERVER_SCHEMA_NAME is empty, the installer creates the tables in the default
schema.

SQLSERVER_SCHEMA_NAME=


# The TRUSTED_CONNECTION property determines whether to connect to the Microsoft SQL
Server database through a
# trusted connection using the Windows credentials of the current user account.
# In Create domain scenario ,when CREATE_DOMAIN=1
#     Set the property if DB_TYPE=MSSQLServer and you are installing on Windows.
#     Set TRUSTED_CONNECTION=0 if DB_TYPE is set to another database type or if you are
installing Informatica on Linux or UNIX.
#     If the property is empty, the installer uses Microsoft SQL Server authentication.
#     Value    0     Connect to the Microsoft SQL Server database using a Microsoft SQL
Server user account.
#     Value    1     Connect to the Microsoft SQL Server database through a trusted
connection using the Windows credentials of the current user account.
#                    If TRUSTED_CONNECTION flag is set to 1, Make sure that
DB_CUSTOM_STRING_SELECTION is also set to 1 and provide connection details in
DB_CUSTOM_STRING_SELECTION.
# In join node scenario, when JOIN_DOMAIN=1
# Set this value to empty,for all cases.



TRUSTED_CONNECTION=



# The DB_CUSTOM_STRING_SELECTION property determines whether to use a JDBC URL or a
custom connection string to connect to the domain configuration database.
#     Set DB_CUSTOM_STRING_SELECTION=1 if TRUSTED_CONNECTION=1. Also provide the default
valid connection string in DB_CUSTOM_STRING.
#     Value    0     The installer creates a JDBC URL from the database properties you
provide
#     Value    1     The installer uses the custom connection string you provide.

DB_CUSTOM_STRING_SELECTION=0


# The DB_SERVICENAME property represents the service name or database name of the
database.
#     Set the property if DB_CUSTOM_STRING_SELECTION=0.
#     Set the property to the service name for Oracle database.
#     Set the property to the database name for Microsoft SQL Server database.
#     Leave the property blank if DB_CUSTOM_STRING_SELECTION=1.

DB_SERVICENAME=DBServiceName


# The DB_ADDRESS property represents the host name and port number for the database
instance.
#     Set the property if DB_CUSTOM_STRING_SELECTION=0.
```

```
#     Set the property in the format HostName:PortNumber.
#     Leave the property blank if DB_CUSTOM_STRING_SELECTION=1.

DB_ADDRESS=HostName:PortNumber


# The ADVANCE_JDBC_PARAM property represents additional parameters in the JDBC URL
connection string.
#     If DB_CUSTOM_STRING_SELECTION=0, you can set the property to include optional
parameters in the JDBC URL connection string.
#     The parameter string must be valid.
#     If the parameter is empty, the installer creates the JDBC URL without additional
parameters.

ADVANCE_JDBC_PARAM=


# The DB_CUSTOM_STRING property represents a valid custom JDBC connection string.
#     Set the property if DB_CUSTOM_STRING_SELECTION=1.

DB_CUSTOM_STRING=


# The DOMAIN_NAME property represents the name of the domain to create. The default
domain name is Domain_<MachineName>.
#     Set the property if CREATE_DOMAIN=1.
#     The domain 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_NAME=DomainName


# The DOMAIN_HOST_NAME property represents the host name of the machine.
#     * If you create a domain, this is the host name of the machine on which to create
the node.
#         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.
#     Do not use localhost. The host name must explicitly identify the machine.

DOMAIN_HOST_NAME=HostName


# The NODE_NAME property represents the node to create on the machine. The node name is
not the host name for the machine.

NODE_NAME=NodeName


# The DOMAIN_PORT property represents the port number.
#     * If you create a domain, set the property to 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, set the property to the port number of the gateway node of
the domain you want to join.

DOMAIN_PORT=


# The DOMAIN_USER property represents the user name for the domain administrator.
#     If you create a domain, you can use this user name to initially log in to the
Informatica Administrator.
#     If you join a domain, this is the user name to use to log in to the domain that
you want to join.
```

```
DOMAIN_USER=AdminUser


# The DOMAIN_PSSWD property represents the password for the domain administrator.
#     The password must be more than 2 characters but cannot exceed 128 characters.

DOMAIN_PSSWD=


# The DOMAIN_CNFRM_PSSWD property confirms the password you set for the domain
administrator.
#     Set the property to the password you set in the DOMAIN_PSSWD property to confirm
the password.


DOMAIN_CNFRM_PSSWD=




# The JOIN_NODE_NAME property represents the name of the node to create on this machine.
The node name is not the host name for the machine.
#     Set the property if JOIN_DOMAIN=1.

JOIN_NODE_NAME=NodeName


# The JOIN_HOST_NAME property represents the host name of the machine that hosts the
gateway node of the domain you want to join.
#     Set the property if JOIN_DOMAIN=1.

JOIN_HOST_NAME=DomainHostName


# The JOIN_DOMAIN_PORT property represents the port number of the gateway node of the
domain you want to join.
#     Set the property if JOIN_DOMAIN=1.

JOIN_DOMAIN_PORT=



################################################################################
###################### DO NOT MODIFY THE FOLLOWING PROPERTIES ##################
################################################################################
USER_INSTALL_DIR=/home/Informatica/10.2.0
KEY_DEST_LOCATION=/home/Informatica/10.2.0/isp/config/keys
INSTALL_TYPE=0
RUN_IMAGE=1
ENABLE_KERBEROS=0
ADVANCE_PORT_CONFIG=0
SAML_AUTHENTICATION=false
CREATE_SERVICES=0
CREATE_MONITORING_STATS=0
CLOUD_SUPPORT_ENABLE=0


#######
# After you create the properties file, save the file with the name
SilentInput.properties and
#     run the silent installer to perform the Informatica services installation.
#######
```

4. Save the properties file with the name `SilentInput.properties`.

## *Running the Docker Image in Silent Mode*

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. Run the silent installation. 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>_Docker_Utility<timestamp>.log` file is created in the directory where you extracted the Docker utility.

# Post-Installation Tasks

After you run the Informatica Docker utility, perform the post-installation tasks.

## *Complete the Domain Configuration*

To complete the domain configuration after you install the Informatica services, perform the following tasks:

**Verify local 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.
- 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 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.
- To configure environment variables, log in with the system user account you used to install Informatica.

For more information about configuring the domain, see the chapter "Complete the Domain Configuration" in the *Informatica 10.2.0 HotFix 1 Installation and Configuration Guide.*

## *Create the Application Services*

Before you create the application services, perform the following tasks:

**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. When you run Informatica on 64-bit platforms, configure the environment to use the correct libraries, database clients, and session cache sizes.

**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.

**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.

**Create 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.

Use the service creation wizard in the Administrator tool to create the service.

**Create 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.

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.

For more information about creating the application services, see the chapter "Create the Application Services" in the *Informatica 10.2.0 HotFix 1 Installation and Configuration Guide*.

## *Install the PowerCenter Client*

You can install the PowerCenter Client to create data objects, create and run mappings, and create virtual databases. To install the PowerCenter Client, perform the following tasks:

**Before you install the clients.**

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.

- 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.

**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. 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.

**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.

For more information about installing the PowerCenter Client, see the section on "Install the PowerCenter Client" in the *Informatica 10.2.0 HotFix 1 Installation and Configuration Guide*.

## Starting and Stopping the Informatica Services on Linux

On Linux, 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.

## Authors

**Nishitha RP**
**Technical Writer**