How-To Library

Informatica

Configuring Kerberos Authentication in an Informatica Domain

Abstract

Kerberos is a network authentication protocol that provides strong authentication between users and services in a network. This article explains how you can configure clients and services within an Informatica domain to use Kerberos authentication.

Supported Versions

- Informatica Big Data Management™ 10.x
- Informatica Data Quality 10.x
- Informatica Data Services 10.x
- Informatica Data Transformation 10.x
- Informatica PowerCenter® 10.x

Table of Contents

Kerberos Overview

Kerberos is a computer network authentication protocol that enables Informatica nodes communicating over a network to connect to one another in a secure manner. Kerberos authentication eliminates Informatica native accounts and removes the need for the domain to pass user credentials to LDAP servers. After you enable Kerberos authentication in a domain, Informatica clients use the Kerberos tickets created during the Windows authentication process to log in to the Informatica services running in the domain.

The Kerberos protocol 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, processes, 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. Informatica can run on a network that uses Kerberos authentication with Microsoft Active Directory Domain Services (AD DS) as the principal database.

The Kerberos authentication protocol uses keytab files to authenticate Informatica clients with services that run within the domain, including node processes, web application processes, and Informatica application services. A *keytab* contains the *service principal name (SPN)* that identifies the service within the Kerberos realm. The keytab also contains the encrypted key assigned to the SPN in Active Directory.

When the KDC gives a service ticket to a client, it encrypts the ticket with the key assigned to the SPN. The same key is stored in a keytab file on the node on which the service runs. The requested service uses the key to decrypt the service ticket.

Configuring Kerberos Authentication in Informatica

You can enable Kerberos authentication in an Informatica domain when you install the Informatica services, or you can enable Kerberos authentication in an existing domain. This article provides a scenario for configuring and enabling Kerberos authentication in an existing domain.

In this scenario, an Informatica domain named InfaDomain runs on a Windows network that uses Kerberos authentication.

The Informatica domain consists of the following nodes:

- node01 is a gateway node that runs on the host US001DEV
- node02 is a gateway node that runs on the host US005DEV
- node03 is a worker node that runs on the host US007DEV

The Informatica domain nodes run within a Windows domain named example.com, and belong to a Kerberos realm named EXAMPLE.COM. The Windows domain uses Microsoft Active Directory Domain Services (AD DS) as the principal database.

You can enable Kerberos at the node level, or at the process level. 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 enable Kerberos at the node level.

Preparing to Enable Kerberos Authentication

Complete the steps outlined in this section to prepare to enable Kerberos authentication in a domain.

Note: You must complete the steps in this section even if you use the Informatica installer to enable Kerberos when you install the Informatica services.

Step 1. Configure and Deploy 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.

The configuration file is named *krb5.conf*. You can find a copy of the file in the following directory on a node:

```
<Informatica installation directory>\server\bin\javalib\msdcrm\conf
```

1. Enter the following 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. 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.
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.

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

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

3. Enter the following 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.

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

4. Map the Active Directory domain to the Kerberos domain in the *default_realm* section of the file. The Active Directory domain name must be all lowercase. The Kerberos domain name must be all uppercase.

```
[default_realm]
.company.com = COMPANY.COM
company.com = 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:

```
[libdefaults]
default_realm = COMPANY.COM
```

```
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1

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

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

Step 2. Create Kerberos User Accounts in Active Directory

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

You create an account for each node process running in the domain. You also create an account for the HTTP process running on each gateway node in the domain.

You must also create a user account that is used to synchronize the LDAP security domain that contains Kerberos user accounts with Active Directory.

1. Create an account for each Informatica node process in the domain. For example, you might create the following accounts for the nodes in the example domain used in this scenario:
   - `nodeuser01` for the node process running on node01
   - `nodeuser02` for the node process running on node02
   - `nodeuser03` for the node process running on node03
2. Create an account for the HTTP process running on each gateway node in the domain. For example, you might create the following accounts for the gateway nodes in the example domain used in this scenario:
   - `httpuser01` for the HTTP process running on node01
   - `httpuser02` for the HTTP process running on node02

   You do not need to create an account for the HTTP process running on the worker node named node03.
3. Create an account that is used to access and search Active Directory during LDAP synchronization. For example, you might create an account named `ldapuser`.

Step 3. Generate the Service Principal Name and Keytab Formats

Use the Informatica Kerberos SPN Format Generator utility to generate the Service Principal Names (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 shows the correct format for the SPN and keytab file names.

1. On a machine that hosts an Informatica node, go to the following directory:

   `<Informatica installation directory>\tools\Kerberos`
2. Run the SPNFormatGenerator.exe utility.
3. Click **Next**.
4. Select **Node Level**.
5. Click **Next**.

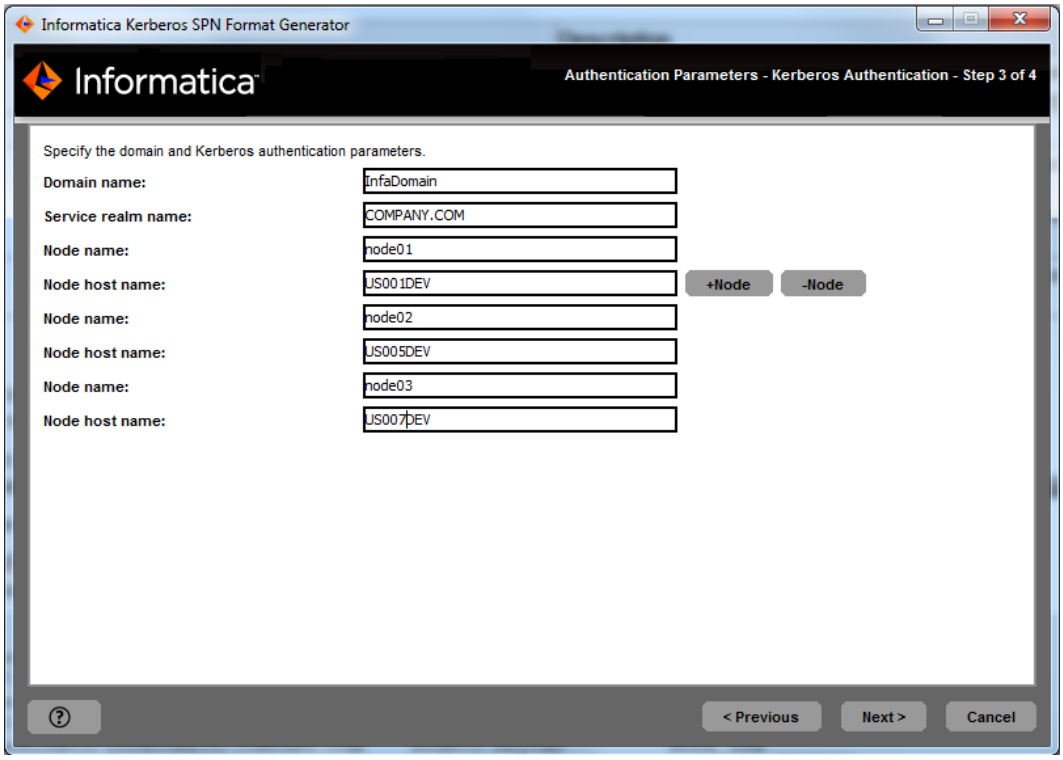
6. Enter the properties required to generate the SPN and keytab file formats.

   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: ` % * + ; " ? , < > \ /
Node Name	Name of the Informatica node.
Node Host Name	Fully qualified name or the IP address of the node host machine. 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 as defined in the Kerberos configuration file. The realm name must be in uppercase.

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 and keytab file names.

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

10. Open the SPNKeytabFormat.txt file.

The following example shows the contents of the SPNKeytabFormat.txt file generated based on the entries in the preceding image:

```
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
node03      isp/node03/InfaDomain/COMPANY.COM      node03.keytab        NODE_SPN
node03      HTTP/US007DEV.company.com@COMPANY.COM  webapp_http.keytab   NODE_SPN
```

Step 4. Generate the Keytab Files

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  <KeytabFilename> -princ <ServicePrincipalName> -mapuser <UserAccount> [-pass
<UserAccountPassword>]-crypto <Keys> -ptype <PrincipalType>
```

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.
-mapuser	The Active Directory user account to associate with the SPN.
-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.

When you run ktpass, you associate each node account and HTTP process account with the corresponding SPN in Active Directory. The following table shows the association between the accounts and the SPNs described in this article:

User Account	Keytab Type	SPN
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

User Account	Keytab Type	SPN
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
nodeuser03	NODE_SPN	isp/node03/InfaDomain/COMPANY.COM

1. Create a keytab file for each node process user account you created.

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

   The following example creates a keytab file for the nodeuser01 user:

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

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

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

   The following example creates a keytab file for the httpuser01 service principal user:

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

3. Create a keytab for the 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 the ldapuser account:

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

4. Copy each keytab file to the following directory on each node:

   ```
   <Informatica installation directory>\isp\config\keys
   ```

   The following table shows the node to which to copy each keytab file:

Keytab File	Location on Node
<node name>.keytab	Copy each file to the corresponding node.
webapp_http.keytab	Copy each file to the corresponding node.
ldapuser.keytab	Copy the file to each gateway node.

Step 5. Enable Delegation for the User Accounts in Active Directory

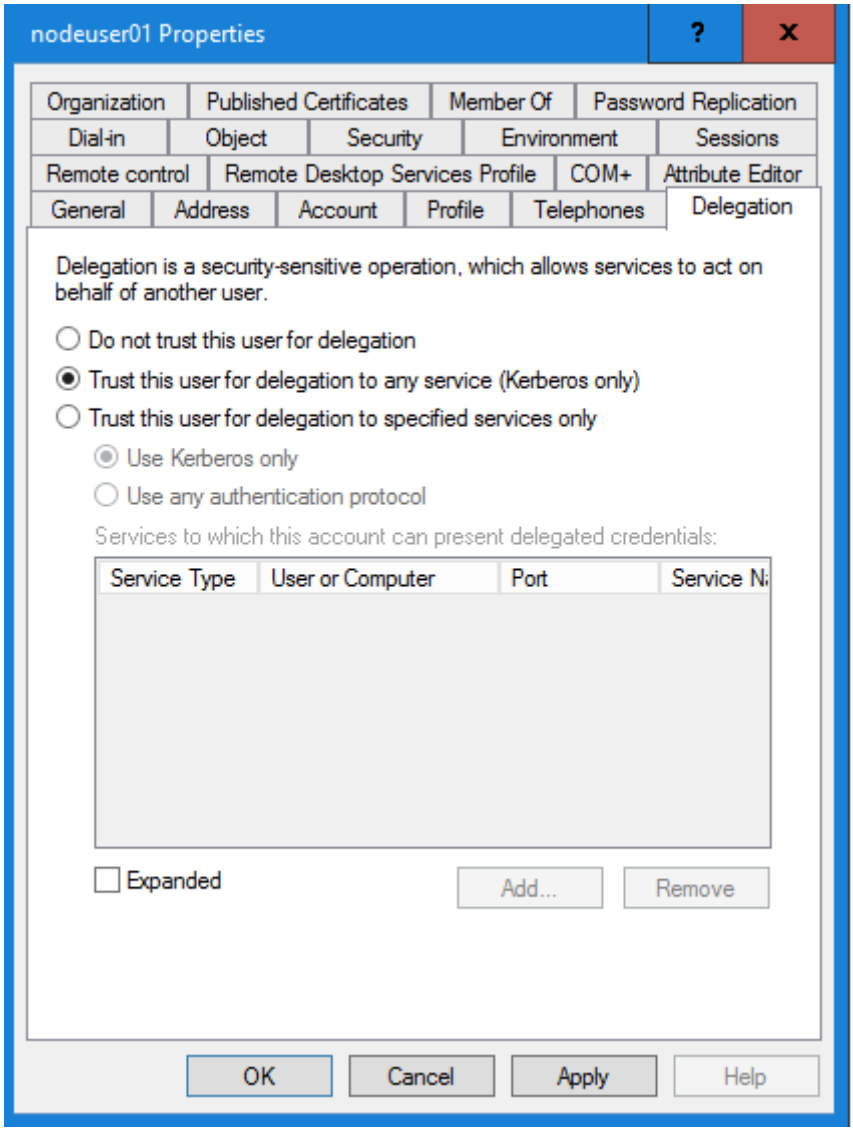
Enable delegation for the node process and HTTP process user accounts you created in Active Directory.

Delegated authentication happens when a user is authenticated with one service and that service uses the credentials of the authenticated user to connect to another service. Because services in the Informatica domain need to connect to other services to complete an operation, the Informatica domain requires the delegation option to be enabled in Active Directory.

You must enable delegation for all accounts for all of the accounts you created, except for the account that is used to access and search Active Directory during LDAP synchronization. Set delegation to **Trust this user for delegation to any service (Kerberos only)** in the Delegation tab in the properties dialog box for each user account.

Note: The Delegation tab is not available in the properties dialog box until you run ktpass to create the keytab files.

The following image shows the Delegation tab in the nodeuser01 properties dialog box:



Step 6. Verify the Keytab Files

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 Informatica nodes:

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

You must create the Kerberos configuration file (krb5.conf) before you can run kinit. You can either copy the configuration file to the `\etc` directory on the kinit host, or use the following property to specify the path and file name for the Kerberos configuration file on the command line: `-Djava.security.krb5.conf=<PathAndFileName>`

To use kinit to request a ticket-granting ticket for a keytab file, run the following command:

```
kinit -c <CacheName> -k -t <KeytabFileName> <ServicePrincipalName>
```

The following table describes the command options:

Option	Description
-c	The cache containing the requested ticket.
-k	Specify to request a ticket for the specified keytab file.
-t	The keytab file name, followed by the associated service principal name.

The following example requests a ticket for the nodeuser01 account:

```
kinit -c \temp\krb -k -t node01.keytab isp/node01/InfaDomain/EXAMPLE.COM
```

The following example shows the ticket-granting ticket written to the specified cache for the specified keytab file and SPN:

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

Enabling Kerberos Authentication in a Domain

Complete the steps in this section to enable Kerberos authentication in an existing Informatica domain.

Step 1. Enable Kerberos Authentication on a Gateway Node

Run the infasetup switchToKerberosMode command on a gateway node within the domain to change the authentication to Kerberos network authentication.

The infasetup command creates an administrator user account in an LDAP security domain with the name *_infaInternalNamespace*. Specify one of the user accounts you created in Active Directory as the administrator account. You use the account to log in to your Windows machine after you enable Kerberos authentication in the domain.

1. Shut down the domain and all Informatica services. Shut down the services in the following order:
   - Metadata Manager Service
   - PowerCenter® Integration Service
   - PowerCenter® Repository Service
   - Content Management Service
   - Analyst Service
   - Data Integration Service
   - Model Repository Service
2. At the command prompt on a gateway node, switch to the directory where the infasetup executable is located:

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

3. Run the following command:

```
infasetup switchToKerberosMode -ad <AdministratorName> -srn <ServiceRealmName> -urn
<UserRealmName> -spnSL <ServicePrincipalLevel>
```

The following table describes the options for the infasetup switchToKerberosMode command:

Option	Description
-administratorName -ad	User name for the domain administrator account that is created when you configure Kerberos authentication. Specify the name of an account that exists in Active Directory. After you configure Kerberos authentication, this user is included in the *_infaInternalNamespace* security domain that the command creates.
-ServiceRealmName -srn	Name of the Kerberos realm as specified in the Kerberos configuration file. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.
-UserRealmName -urn	Name of the Kerberos realm as specified in the Kerberos configuration file. The service realm name and the user realm name must be the same.
-SPNShareLevel -spnSL	Service principal level for the domain. Set to NODE to enable Kerberos at the node level.

The following example changes the domain authentication to Kerberos and sets the nodeuser01 user account as the administrator account:

```
infasetup switchToKerberosMode -ad nodeuser01 -srn EXAMPLE.COM -urn EXAMPLE.COM -spnSL
NODE
```

Step 2. Update All Other Nodes in the Domain

Update all gateway and worker nodes with the Kerberos authentication server information except the gateway nodes on which you ran the infasetup switchToKerberosMode command.

To update the gateway and worker nodes, use the following commands:

infasetup UpdateGatewayNode

Use the UpdateGatewayNode command to set the Kerberos authentication parameters on a gateway node in the domain. If the domain has multiple gateway nodes, run the UpdateGatewayNode command on each gateway node.

infasetup UpdateWorkerNode

Use the UpdateWorkerNode command to set the Kerberos authentication parameters on a worker node in the domain. If the domain has multiple worker nodes, run the UpdateWorkerNode command on each worker node.

1. Shut down the domain and all Informatica services. Shut down the services in the following order:
   - Metadata Manager Service
   - PowerCenter® Integration Service
   - PowerCenter® Repository Service
   - Content Management Service

- Analyst Service
- Data Integration Service
- Model Repository Service

2. At the command prompt on a node, switch to the directory where the infasetup executable is located:

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

3. To set the Kerberos authentication parameters on a gateway node, run the following command:

   ```
   infasetup UpdateGatewayNode -krb -srn <ServiceRealmName> -urn <UserRealmName>
   ```

   To set the Kerberos authentication parameters on a worker node, run the following command:

   ```
   infasetup UpdateWorkerNode -krb -srn <ServiceRealmName> -urn <UserRealmName>
   ```

   The following table describes the options required to update the Kerberos authentication information for a node:

Option	Description
-EnableKerberos -krb	Configures the Informatica domain to use Kerberos authentication.
-ServiceRealmName -srn	Name of the Kerberos realm specified in the Kerberos configuration file. The realm name must be in uppercase and is case-sensitive. The service realm name and the user realm name must be the same.
-UserRealmName -urn	Name of the Kerberos realm specified in the Kerberos configuration file. The service realm name and the user realm name must be the same.

   The following example updates a worker node to use Kerberos authentication:

   ```
   infasetup updateWorkerNode -krb -srn EXAMPLE.COM -urn EXAMPLE.COM
   ```

Step 3. Enable Kerberos Authentication for Informatica Clients

Copy the Kerberos configuration file to each machine that hosts an Informatica client, and the set an environment variable to point to the configuration file. You must also configure the browser to access the Informatica web applications.

After you configure the Informatica domain to run with Kerberos authentication, perform the following tasks on the Informatica client tools:

Copy the Kerberos configuration file to the client machines.

Copy the Kerberos configuration file to each machine that hosts an Informatica client. You must copy the `krb5.conf` file to the following directory: `<Informatica Client Directory>\shared\security`

Set the KRB5_CONFIG environment variables with the Kerberos configuration file.

Set the KRB5_CONFIG environment variable to the path and file name of the Kerberos configuration file on each machine that hosts an Informatica client.

Configure web browsers to use Kerberos authentication.

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.

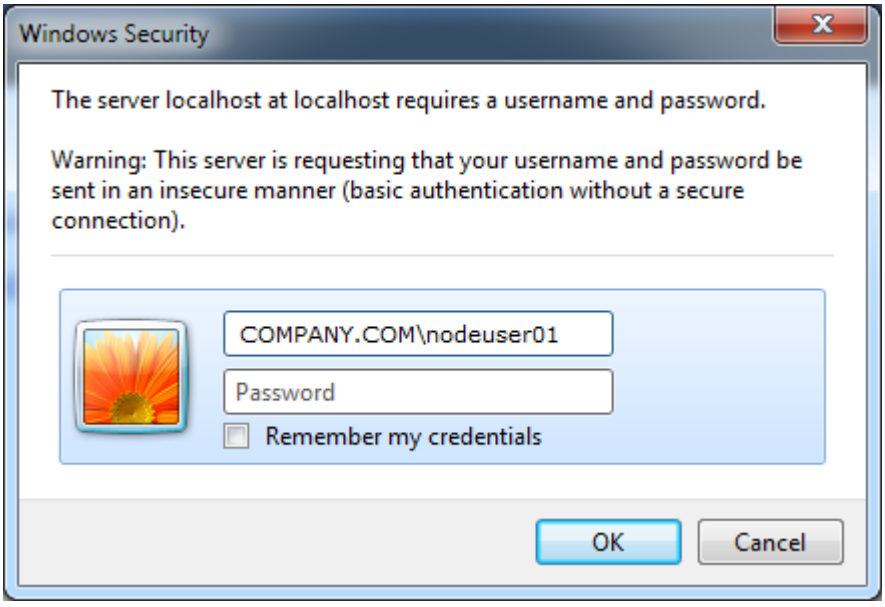
Step 4. Synchronize the Kerberos Security Domain with Active Directory

Use Informatica Administrator (the Administrator tool) to import the user accounts that use Kerberos authentication from Active Directory users into an LDAP security domain.

When you run the infasetup switchToKerberosMode command to change the domain authentication, the command creates an empty LDAP security domain with the same name as the Kerberos realm defined in the Kerberos configuration file. You can import user accounts from Active Directory into this LDAP security domain, or you can import the user accounts into a different LDAP security domain.

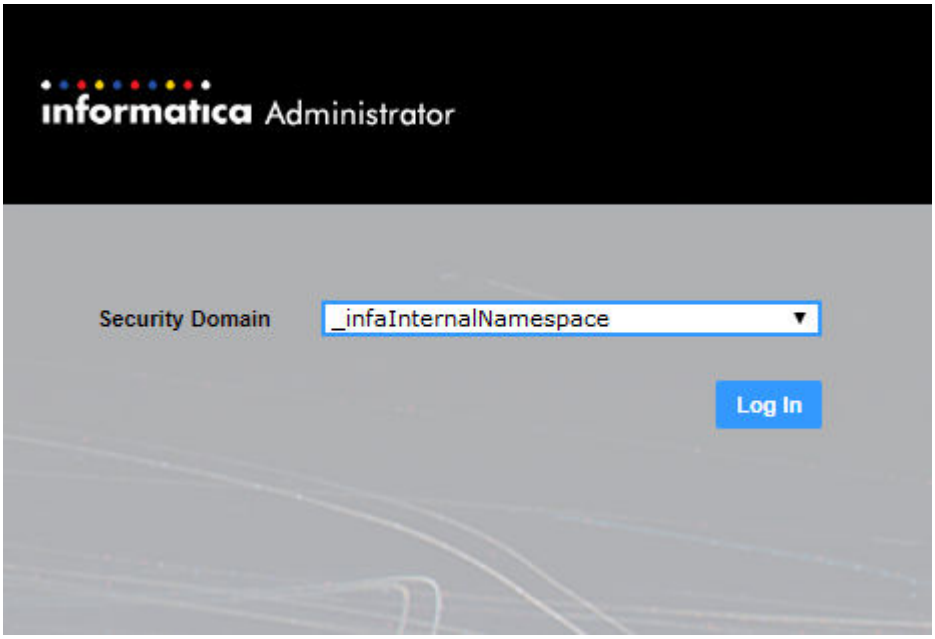
1. Start the domain and all Informatica services. Start the services in the following order:
   - Model Repository Service
   - Data Integration Service
   - Analyst Service
   - Content Management Service
   - PowerCenter® Repository Service
   - PowerCenter® Integration Service
   - Metadata Manager Service
2. Log in to the Windows machine with the administrator account you specified in the infasetup switchToKerberosMode command.

   The following image shows the user name and password for nodeuser01 entered in the login dialog box:



3. Log in to the Administrator tool. Select _infaInternalNamespace as the security domain.

   The following image shows _infaInternalNamespace selected as the security domain:



4. In the Administrator tool, click the **Security** tab.
5. Click the **Actions** menu and select **LDAP Configuration**.
6. In the **LDAP Configuration** dialog box, click the **LDAP Connectivity** tab.
7. Configure the connection properties for the Active Directory.

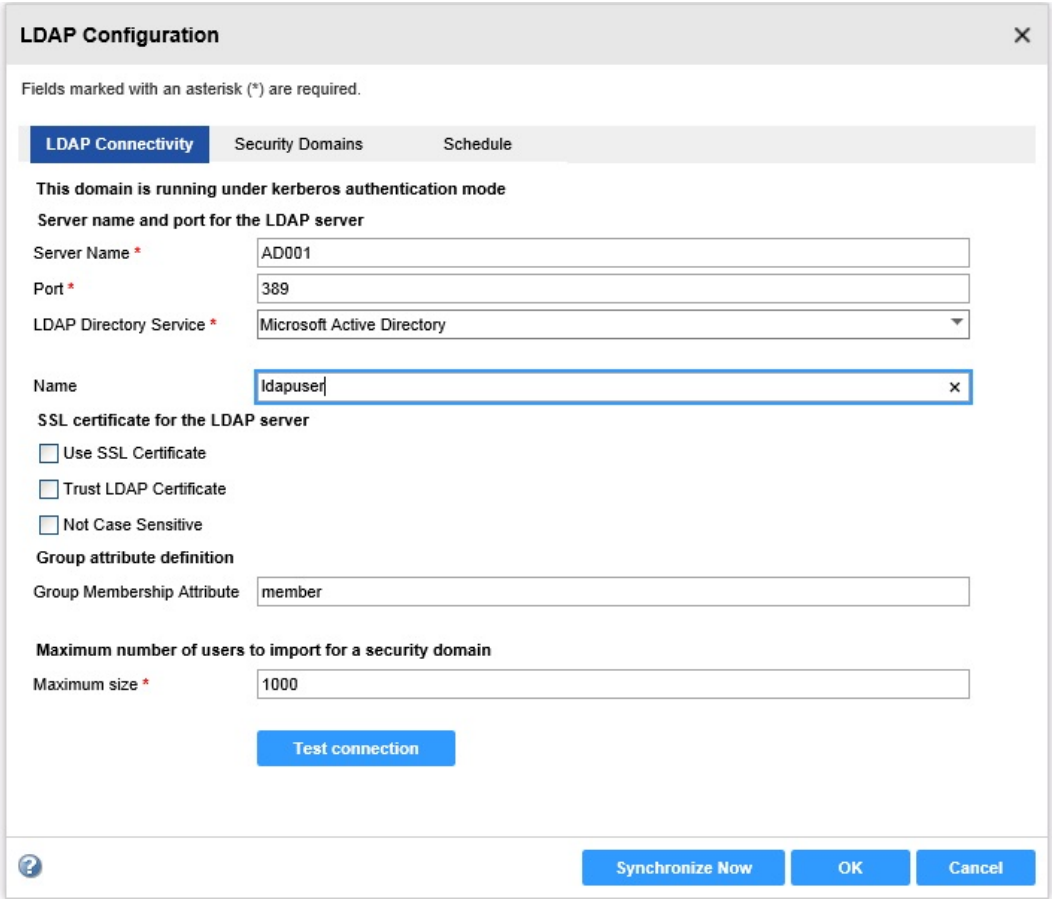
   You might need to consult the LDAP administrator to get the information needed to connect to the LDAP server.

   The following table describes the LDAP server configuration properties:

Property	Description
Server name	Host name or IP address of the machine hosting the Active Directory server.
Port	Listening port for the Active Directory server.
LDAP Directory Service	Select Microsoft Active Directory Service.
Name	Specify the user account you created in Active Directory to synchronize accounts in Active Directory with the LDAP security domain. Because the domain is enabled for Kerberos authentication, you do not have the option to provide a password for the account.
Use SSL Certificate	Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol.
Trust LDAP Certificate	Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.
Not Case Sensitive	Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups.

Property	Description
Group Membership Attribute	Name of the attribute that contains group membership information for a user. This is the attribute in the LDAP group object that contains the DNs of the users or groups who are members of a group. For example, *member* or *memberof*.
Maximum Size	Maximum number of user accounts to import into a security domain. For example, if the value is set to 100, you can import a maximum of 100 user accounts into the security domain. If the number of user to be imported exceeds the value for this property, the Service Manager generates an error message and does not import any user. Set this property to a higher value if you have many users to import. Default is 1000.

The following image shows the ldapuser user account specified with the connection details for an Active Directory server set in the LDAP Connectivity panel of the **LDAP Configuration** dialog box:

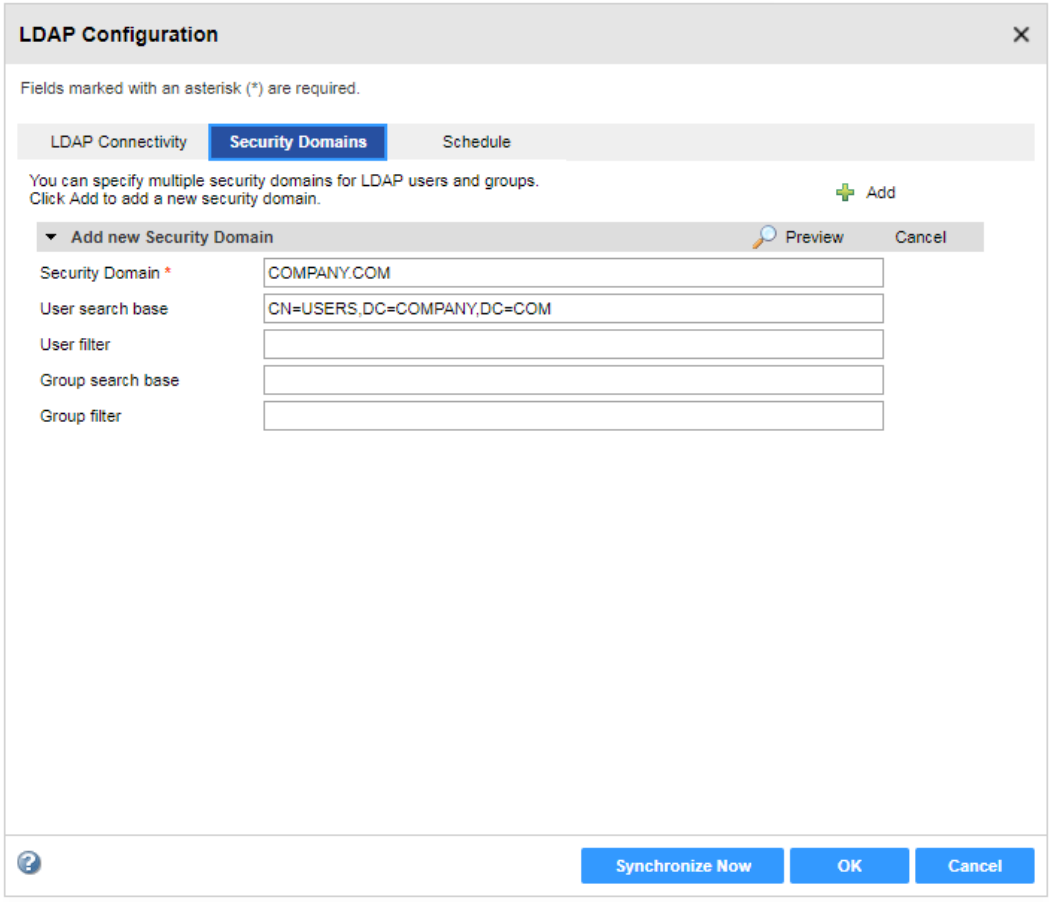


8. In the **LDAP Configuration** dialog box, click the **Security Domains** tab.
9. Click **Add**.

The following table describes the filter properties that you can set for a security domain:

Property	Description
Security Domain	Name of the LDAP security domain into which you want to import user accounts from Active Directory.
User search base	Distinguished name (DN) of the entry that serves as the starting point to search for user names in Active Directory. The search finds an object in the directory according to the path in the distinguished name of the object. For example, to search the USERS container that contains Informatica user accounts in the example.com Windows domain, specify CN=USERS,DC=EXAMPLE,DC=COM.
User filter	An LDAP query string that specifies the criteria for searching for users in the directory service. The filter can specify attribute types, assertion values, and matching criteria. For example: `(objectclass=*)` searches all objects. `(&(objectClass=user)(!(cn=susan)))` searches all user objects except "susan". For more information about search filters, see the documentation for the LDAP directory service.
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

The following image shows the information required to import LDAP users from Active Directory into the LDAP security domain created by the infasetup switchToKerberosMode command:



10. Click **Synchronize Now**.

    The Service Manager synchronizes the users in all the LDAP security domains with the users in the LDAP directory service. The time it takes for the synchronization process to complete depends on the number of users and groups to be imported.

11. Click **OK** to save the LDAP security domain.

Step 5. Migrate Native User Privileges and Permissions to the Kerberos Security Domain

If the Informatica domain has user accounts in the native security domain, the corresponding Active Directory user accounts in the Kerberos security domain must have the same groups, roles, privileges, and permissions. Migrate the groups, roles, privileges, and permissions of the native users to the user accounts in the Kerberos security domain.

1. Review the list of native user accounts and determine the accounts that you want to migrate to the LDAP security domain for Kerberos authentication.

   To list the user accounts in the Informatica domain, run the following command:

   ```
   infacmd isp ListAllUsers
   ```

   Each native user account that you want to migrate to the Kerberos security domain must have a corresponding account in the Microsoft Active Directory service that you use for Kerberos authentication.

2. Create the user migration file.

The user migration file is a plain text file that contains the list of native users and the corresponding Kerberos users that require the same groups, roles, privileges, and permissions.

Use the following format to list entries in the user migration file:

```
Native/<SourceUserName>,<LDAPSecurityDomain>/<TargetUserName>
```

The following example shows a user migration file containing the following list of users to migrate to the COMPANY.COM security domain:

```
Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3
```

3. Run the infacmd isp migrateUsers command to migrate account privileges and permissions in the native security domain to the accounts in the Kerberos security domain.

   Before you run the infacmd isp migrateUsers command, ensure that all instances of the following services on the domain are running:

   - Analyst Service
   - Content Management Service
   - Data Integration Service
   - Model Repository Service
   - Metadata Manager Service
   - PowerCenter® Integration Service
   - PowerCenter® Repository Service

   Ensure that the PowerCenter Repository Service is running in normal mode.

   To migrate the groups, roles, privileges, and permissions for users, run the following command:

   ```
   infacmd isp migrateUsers -dn <DomainName> -un <AdministratorUserName> -pd
   <AdministratorPassword> -sdn <SecurityDomain> -umf <UserMigrationFile>
   ```

   The following table describes the options for the command:

Option	Description
-DomainName -dn	Name of the Informatica domain.
-UserName -un	User name to connect to the domain. Specify the user name of the administrator account you specified in the infasetup switchToKerberosMode command.
-Password -pd	Password for the administrator account.
-SecurityDomain -sdn	LDAP security domain of the administrator account used to connect to the domain. Specify _infaInternalNamespace.
-UserMigrationFile -umf	Path and file name of the user migration file. The command skips entries with a duplicate source user name or target user name.

   The following example migrates the groups, roles, privileges, and permissions for users based on the `um_s.txt` user migration file:

   ```
   infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
   _infaInternalNamespace -umf C:\Infa\um_s.txt
   ```

The command overwrites the connection object permissions assigned to the LDAP user with the connection object permissions for the native user. The command merges the groups, roles, privileges, and domain object permissions for native users and corresponding LDAP users.

The migrateUsers command creates a detailed log file named `infacmd_umt_<date>_<time>.txt` in the directory where you run the command.

Author

Dan Hynes