Using LDAP Authentication in an Informatica Domain
Abstract

Lightweight Directory Access Protocol (LDAP) is a software protocol for accessing users and resources on a network. You can configure an Informatica domain to use LDAP to authenticate Informatica application client users.

Supported Versions

- Informatica Big Data Management™ 9.6.1, 10.0, 10.1.x
- Informatica Data Quality 9.6.1, 10.0, 10.1.x
- Informatica Data Services 9.6.1, 10.0, 10.1.x
- Informatica Data Transformation 10.0, 10.1.x
- Informatica PowerCenter® 9.6.1, 10.0, 10.1.x

Table of Contents

Overview .......................................................... 2
LDAP Security Domains ........................................ 3
User Account Synchronization ................................ 3
Before You Begin .................................................. 3
LDAP Directory Service Requirements ..................... 3
Configuring LDAP Authentication for an Informatica Domain ........................................ 4
  Step 1. Set Up the Connection to the LDAP Server  ................................................. 4
  Step 2. Configure the Security Domain ............................................................... 6
  Step 3. Set Up the Synchronization Schedule ....................................................... 8
Connecting to a Secure LDAP Server .......................... 10
Managing Users in an LDAP Security Domain ............... 11

Overview

You can configure an Informatica domain to enable user accounts imported from an LDAP directory service to log in to Informatica application clients such as Informatica Developer and Informatica Analyst.

An LDAP directory service stores account user names and passwords. Using LDAP authentication enables you to consolidate the credentials for all of your Informatica users in a single identity store, simplifying the task of creating and updating account credentials.

You can use native authentication and LDAP authentication together in an Informatica domain. The Service Manager running on the master gateway node within the domain authenticates users based on the security domain the users belong to. If a user belongs to the default native security domain, the Service Manager authenticates the user against account information in the domain configuration repository. If the user belongs to an LDAP security domain, the Service Manager passes the user's credentials to the LDAP server for authentication.
**LDAP Security Domains**

An LDAP security domain contains users and groups imported from an LDAP directory service. You can define multiple LDAP security domains within an Informatica domain. You can then import accounts from a single LDAP directory service into the security domains.

You must create an LDAP security domain if you configure an Informatica domain to use Kerberos authentication. When you install Informatica services and enable Kerberos authentication, the Informatica installer creates an LDAP security domain with the name of the Kerberos realm that you specify during installation.

When you create an LDAP security domain, you configure search bases and filters that define the set of LDAP user accounts and groups to include in the security domain. The Service Manager uses the security domain configuration to import or synchronize users and groups in the security domain with users and groups in the LDAP directory service.

The Service Manager uses the following criteria when it imports or synchronizes users and groups within an LDAP security domain:

- The Service Manager uses the user search bases and filters to import user accounts.
- The Service Manager uses the group search bases and filters to import groups.
- The Service Manager imports the groups that are included in the group filter and the user accounts that are included in the user filter.

**User Account Synchronization**

The Service Manager updates the security domain with the users and groups in an LDAP directory service on a scheduled basis. You can set up the synchronization schedule when you configure LDAP authentication.

The Service Manager performs the following steps during synchronization:

- Retrieves an updated list of users and groups from the LDAP directory service, based on the search base and filters you configured for the security domain.
- Updates the list of LDAP users and groups in the security domain. If an LDAP user in the security domain has been deleted in the LDAP directory service, the Service Manager transfers ownership of the user’s objects to the domain administrator account.

**Before You Begin**

Before you configure LDAP authentication, verify that the LDAP directory service, LDAP users, and LDAP groups meet the Informatica requirements.

**LDAP Directory Service Requirements**

You can import users from the following LDAP directory services:

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- Sun Java System Directory Server

**Note:** If you use Kerberos authentication, you can import users only from Microsoft Active Directory.
When you set up the LDAP directory service, you can use different attributes for the unique ID (UID). The Service Manager requires a particular UID to identify users in each LDAP directory service. Before you configure the security domain, verify that the LDAP directory service uses the required UID.

The following table lists the required UID for each LDAP directory service:

<table>
<thead>
<tr>
<th>LDAP Directory Service</th>
<th>UID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Tivoli Directory Server</td>
<td>uid</td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>uid</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>uid</td>
</tr>
<tr>
<td>Sun Java System Directory Server</td>
<td>uid</td>
</tr>
</tbody>
</table>

**Configuring LDAP Authentication for an Informatica Domain**

To use LDAP authentication, you must set up a connection to an LDAP server, and then import the user accounts into your LDAP security domains. Use search filters to specify the users and groups to import.

To create an LDAP security domain, perform the following steps:

1. Set up the connection to the LDAP directory service.
2. Configure the security domain.
3. Set up the synchronization schedule.

**Step 1. Set Up the Connection to the LDAP Server**

Configure the connection to the LDAP server that contains the directory service from which you want to import the user accounts.

When you configure the connection to the LDAP server, indicate that the Service Manager must ignore the case sensitivity of the distinguished name attributes of the LDAP user accounts when it assigns users to groups in the Informatica domain. If the Service Manager does not ignore case sensitivity, the Service Manager might not assign all the users that belong to a group.

If the LDAP server uses SSL, you must import the certificate into the cacerts truststore file on every gateway node within the Informatica domain. For more information, see “Connecting to a Secure LDAP Server” on page 10.

To set up a connection to the LDAP directory service, perform the following tasks:

1. In the Administrator tool, click the **Security** tab.
2. Click the **Actions** menu and select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **LDAP Connectivity** tab.
4. Configure the connection properties for the LDAP server.

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Host name or IP address of the machine hosting the LDAP directory service.</td>
</tr>
<tr>
<td>Port</td>
<td>Listening port for the LDAP server. This is the port number to communicate with the LDAP directory service. Typically, the LDAP server port number is 389. If the LDAP server uses SSL, the LDAP server port number is 636. The maximum port number is 65535.</td>
</tr>
<tr>
<td>LDAP Directory Service</td>
<td>Type of LDAP directory service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you use Kerberos authentication, you must select Microsoft Active Directory Service.</td>
</tr>
<tr>
<td>Name</td>
<td>Distinguished name (DN) for the principal user. The user name often consists of a common name (CN), an organization (O), and a country (C). The principal user name is an administrative user with access to the directory. Specify a user that has permission to read other user entries in the LDAP directory service. Leave blank for anonymous login. For more information, see the documentation for the LDAP directory service.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the principal user. Leave blank for anonymous login.</td>
</tr>
<tr>
<td>Use SSL Certificate</td>
<td>Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol.</td>
</tr>
<tr>
<td>Trust LDAP Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>Not Case Sensitive</td>
<td>Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups.</td>
</tr>
<tr>
<td>Group Membership Attribute</td>
<td>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, <em>member</em> or <em>memberof</em>.</td>
</tr>
<tr>
<td>Maximum Size</td>
<td>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.</td>
</tr>
</tbody>
</table>

The following image shows the connection details for an LDAP server set in the LDAP Connectivity panel of the **LDAP Configuration** dialog box:
5. Click **Test Connection** to verify that the connection to the LDAP server is valid.

**Step 2. Configure the Security Domain**

Create an LDAP security domain for each set of user accounts and groups you want to import from the LDAP directory service. Set up search bases and filters to define the set of user accounts and groups to include in a security domain.

The names of users and groups to be imported from the LDAP directory service must conform to the same rules as the names of native users and groups. The Service Manager does not import LDAP users or groups if names do not conform to the rules of native user and group names. Note that unlike native user names, LDAP user names can be case sensitive.

The Service Manager uses the user search bases and filters to import user accounts and the group search bases and filters to import groups. The Service Manager uses the filters to imports groups and the list of users that belong to each group.

If you modify the LDAP connection properties to connect to a different LDAP server, the Service Manager does not delete the existing security domains. You must ensure that the LDAP security domains are correct for the new LDAP server. Modify the user and group filters in the security domains or create additional security domains so that the Service Manager correctly imports the users and groups that you want to use in the Informatica domain.

To configure an LDAP security domain, perform the following steps:

1. In the Administrator tool, click the **Security** tab.
2. Click the **Actions** menu and select **LDAP Configuration**.
3. In the **LDAP Configuration** dialog box, click the **Security Domains** tab.

4. Click **Add**.

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Domain</td>
<td>Name of the LDAP security domain. The name is not case sensitive and must be unique within the domain. The string cannot exceed 128 characters or contain the following special characters: , + / &lt; &gt; @ \ % ? The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.</td>
</tr>
<tr>
<td>User search base</td>
<td>Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The search finds an object in the directory according to the path in the distinguished name of the object. For example, in Microsoft Active Directory, the distinguished name of a user object might be cn=UserName,ou=OrganizationalUnit,dc=DomainName, where the series of relative distinguished names denoted by dc=DomainName identifies the DNS domain of the object.</td>
</tr>
<tr>
<td>User filter</td>
<td>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 &quot;susan&quot;. For more information about search filters, see the documentation for the LDAP directory service.</td>
</tr>
<tr>
<td>Group search base</td>
<td>Distinguished name (DN) of the entry that serves as the starting point to search for group names in the LDAP directory service.</td>
</tr>
<tr>
<td>Group filter</td>
<td>An LDAP query string that specifies the criteria for searching for groups in the directory service.</td>
</tr>
</tbody>
</table>

The following image shows the properties for an LDAP security domain named **APP_USERS** set in the Security Domains panel of the **LDAP Configuration** dialog box. The user filter is set to import all users beginning with the letter "s."
5. Click Preview to view a subset of the list of users and groups that fall within the filter parameters. If the preview does not display the correct set of users and groups, modify the user and group filters and search bases to get the correct users and groups.

6. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, 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.

7. Click OK to save the security domain.

**Step 3. Set Up the Synchronization Schedule**

You can set up a daily schedule for the Service Manager to update all LDAP security domains with new or changed users and groups in the LDAP directory service.

When the Service Manager synchronizes the LDAP security domains with the LDAP directory service, it imports all users that match the user filter settings from the LDAP directory service into the security domain. The Service Manager then imports all groups that match the group filter settings, and associates users with their corresponding groups. The Service Manager also deletes any user or group not found in the LDAP directory service from the security domain.

By default, the Service Manager is not scheduled time to synchronize with the LDAP directory service. To ensure that the list of users and groups in the LDAP security domains is accurate, schedule when the Service Manager...
synchronizes the LDAP security domains with the LDAP directory service. The Service Manager synchronizes the LDAP security domains with the LDAP directory service every day at the times you set.

To ensure that synchronization succeeds, consider the following recommendations before set up the synchronization schedule:

Verify that the /etc/hosts file contains an entry for the LDAP server.

Verify that the /etc/hosts file on each node gateway in the domain contains an entry with the host name and IP address of the LDAP server. If the Service Manager cannot resolve the host name for the LDAP server, synchronization can fail.

Enable paging in LDAP if you are synchronizing more than 100 users or groups.

Enable paging on the LDAP directory service before you synchronize more than 100 users or groups. If you do not enable paging on the LDAP directory service, synchronization can fail.

Synchronize security domains during times when most users are not logged in to Informatica applications.

During synchronization, the Service Manager locks each user account it synchronizes. Users might not be able to log in to the Informatica application clients during synchronization. Users logged in to an application client when synchronization starts might not be able to perform certain tasks.

To set up a schedule that synchronizes LDAP security domains with the LDAP directory service, perform the following steps:

1. In the Administrator tool, click the Security tab.
2. Click the Actions menu and select LDAP Configuration.
3. In the LDAP Configuration dialog box, click the Schedule tab.
4. Click the Add button (+) to add a time.

The synchronization schedule uses a 24-hour time format.

You can add as many synchronization times in the day as you require. If the list of users and groups in the LDAP directory service changes often, you can schedule the Service Manager to synchronize multiple times a day.

The following image shows the properties set in the Schedule panel of the LDAP Configuration dialog box to synchronize the LDAP security domains with the LDAP directory service daily at 8:00 a.m. and 8:00 p.m.
5. To immediately synchronize the users and groups in the LDAP security domains with the users and groups in the LDAP directory service, click **Synchronize Now**.

6. Click **OK** to save the synchronization schedule.

**Note:** Wait until the Service Manager synchronizes with the LDAP directory service before restarting the Informatica domain to avoid losing the synchronization times that you set in the schedule.

**Connecting to a Secure LDAP Server**

You can connect to an LDAP server that uses an SSL certificate signed by a certificate authority (CA).

Import the LDAP server's SSL certificate into the **cacerts** truststore file on every gateway node within the Informatica domain. Use the Java **keytool** key and certificate management utility to import the certificate into the truststore file.

To import the certificate into the **cacerts** truststore file, perform the following steps:

1. Copy the certificate to a local folder on a gateway node within the Informatica domain.

2. From the command line, go to the following directory on the gateway node:

   `<Informatica installation directory>\java\jre\lib\security`

3. From the command line, run the following command:

   ```bash
   keytool -importcert -alias <certificate alias name> -file <certificate path>\<certificate filename> -keystore cacerts -storepass <truststore password>
   ```

   **Note** that you must include the password for the truststore.
4. Restart the node.

Managing Users in an LDAP Security Domain

After you import user accounts into an LDAP security domain, you can manage the accounts using Informatica clients and the LDAP directory service.

You can assign roles, privileges, and permissions to user accounts in the LDAP security domain using the Administrator tool or the infacmd isp migrateusers command. An LDAP directory service stores the credentials for Informatica user accounts. A directory service does not store user roles, privileges, and permissions.

See “Assigning Privileges and Roles to Users and Groups” in the Informatica Security Guide for instructions on assigning roles, privileges, and permissions to user accounts using the Administrator tool. See the Informatica Command Reference for instructions on migrating native user roles, privileges, and permissions to the corresponding accounts in the LDAP security domain using the infacmd isp migrateusers command.

You must use the Administrator tool to enable or disable a user account in an LDAP security domain. The Service Manager does not import the LDAP attribute that indicates that a user account is enabled or disabled.

However, the status of a user account in the LDAP directory service affects user authentication for the Informatica applications. A user account that is disabled in the LDAP directory service can log in to Informatica applications based on whether the LDAP directory service allows disabled user accounts to log in. For example, Informatica user accounts can log in to Informatica applications if the user is disabled in the LDAP directory service, and the directory service allows disabled user accounts to log in.

You must make changes to LDAP users and groups in the LDAP directory service, then synchronize the LDAP security domain with the LDAP directory service. You cannot use the Administrator tool to create, edit, or delete users and groups in an LDAP security domain.

To permanently deny users in an LDAP security domain access to Informatica applications, you can delete the LDAP security domain. When you delete an LDAP security domain, the Service Manager deletes all user accounts and groups in the LDAP security domain from the Informatica domain configuration database.

Author

Dan Hynes
Principal Technical Writer