Using LDAP Authentication in a PowerCenter Domain
Overview
LDAP user accounts can access PowerCenter applications. To provide LDAP user accounts access to the PowerCenter applications, configure the PowerCenter domain to use LDAP authentication.

To use LDAP authentication, configure a connection to the LDAP server, create LDAP security domains, and synchronize the list of users and groups in the LDAP security domains with the LDAP directory service. Then assign roles, privileges, and permissions to users and groups in LDAP security domains.

Security Domains and User Synchronization
When you configure LDAP authentication, it is important to understand what a security domain is and how the Service Manager uses security domains to synchronize users in the domain.

Security Domains
The LDAP security domain contains users and groups imported from the LDAP directory Service. You can define multiple security domains for LDAP authentication. When you create a 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.

The Service Manager uses the following criteria when it imports or synchronizes users and groups for a 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 groups and the list of users that belong to the 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 Synchronization
The Service Manager synchronizes users to update the list of LDAP users and groups in the security domain. When you configure LDAP authentication you can schedule user synchronization.

The Service Manager performs the following steps during synchronization:
- The Service Manager connects to the LDAP directory service using the distinguished name and password of the principle user, if you configure the distinguished name and password in the connectivity setup. Otherwise, the Service Manager uses anonymous login.
- The Service Manager retrieves an updated list of users and groups, based on the search base and filters you configured for the security domain.
- The Service Manager 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 Administrator.

Note: During synchronization, the Service Manager locks the user account it synchronizes. Users might not be able to log in to the Administration Console and PowerCenter applications. If users are logged in to the Administration Console when synchronization starts, they might not be able to perform tasks. The duration of the synchronization process depends on the number of users and groups to be synchronized. To avoid usage disruption, synchronize the security domains during times when most users are not logged in.

Before you Begin
Before you configure LDAP authentication, verify that the LDAP Directory Service, LDAP users, and LDAP groups meet the PowerCenter requirements.
**LDAP Directory Services Requirements**
You can use the following LDAP directory services for LDAP authentication:
- Microsoft Active Directory Service
- Sun Java System Directory Service
- Novell e-Directory Service
- IBM Tivoli Directory Service
- Open LDAP Directory Service

**Unique ID Requirements**
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 provides 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</td>
<td>uid</td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Novell E</td>
<td>uid</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>uid</td>
</tr>
<tr>
<td>Sun Java System Directory</td>
<td>uid</td>
</tr>
</tbody>
</table>

**LDAP Users and Groups Requirements**
Before you import LDAP users and groups, verify that users and groups meet the following requirements.
- The names of users and groups that you import 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 the names do not conform to the rules of native user and group names.
- LDAP nested groups that you import from the LDAP directory service must be created in the following manner:
  - The groups are created under the same organizational units (OU).
  - The relationship is set between the groups.
You cannot import nested LDAP groups into an LDAP security domain that are created in a different way. You also cannot import nested groups for Novell e-Directory Service or IBM Tivoli Directory Service.

**Configuring LDAP Authentication for the PowerCenter Domain**
To configure LDAP authentication for the domain, complete the following steps:
1. Set up the connection to the LDAP server.
2. Configure a security domain.
3. Schedule the synchronization times.

**Step 1: Set up the LDAP Connection**
The Service Manager uses the LDAP connection to import the user accounts of all LDAP security domains from the LDAP server.

Note: 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 existing security domains or create new security domains so that the Service Manager can import the users and groups that you want to use in the PowerCenter domain.
To set up a connection to the LDAP server:
1. Click the LDAP Configuration icon on the Security page of the PowerCenter Administration Console.
2. In the LDAP Configuration dialog box, click the LDAP Connectivity tab.
3. Configure the following LDAP server properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Name 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.</td>
</tr>
</tbody>
</table>
| LDAP Directory Service | Type of LDAP directory service. Select from the following directory services:  
• Microsoft Active Directory Service  
• Sun Java System Directory Service  
• Novell e-Directory Service  
• IBM Tivoli Directory Service  
• Open LDAP Directory Service |
| Name              | 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, refer to the documentation for the LDAP directory service. |
| Password          | Password for the principal user. Leave blank for anonymous login. |
| Use SSL Certificate | Indicates that the LDAP directory service uses Secure Socket Layer (SSL) protocol. |
| Trust LDAP Certificate | Determines whether PowerCenter can trust the SSL certificate of the LDAP server. If selected, PowerCenter connects to the LDAP server without verifying the SSL certificate. If not selected, PowerCenter verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.  
To enable PowerCenter to recognize a self-signed certificate as valid, specify the truststore file and password to use. |
| 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 groups and user accounts to import into a security domain. For example, if the value is set to 100, you can import a maximum of 100 groups and 100 user accounts into the security domain.  
If the number of user and groups 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 a large number of users and groups to import.  
Default is 1000. |

4. Click Test Connection to verify that the connection configuration is correct.

**Using a Self-Signed SSL Certificate**

You can connect to an LDAP server that uses an SSL certificate signed by a certificate authority (CA). PowerCenter uses the truststore file to verify the SSL certificate. By default, PowerCenter does not connect to an LDAP server that uses a self-signed certificate.

`keytool` is a key and certificate management utility that allows you to generate and administer keys and certificates for use with the SSL security protocol. You can use `keytool` to create a truststore file or to import a certificate to an existing truststore file. You can find the `keytool` utility in the following directory:

```bash
<PowerCenterClientDir>CMD_Utilities\PC\java\bin
```
For more information about using keytool, see the documentation on the Sun web site:
http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html

To use a self-signed certificate, complete the following steps:

1. Import the self-signed certificate into a truststore file.
2. Configure INFA_JAVA_OPTS environment variable on each PowerCenter node in the domain. Use the
   INFA_JAVA_OPTS to specify the truststore file and password to use.
   
   On UNIX, enter the following command:
   ```bash
   setenv INFA_JAVA_OPTS -Djavax.net.ssl.trustStore=<TrustStoreFile>
   -Djavax.net.ssl.trustStorePassword=<TrustStorePassword>
   ```
   
   On Windows, configure INFA_JAVA_OPTS as a system variable.
3. Restart each node in the domain for the change to take effect.

**Step 2: Configure a Security Domain**

Create a security domain for each set of user accounts and groups you want to import from the LDAP server.

**To add an LDAP security domain:**

1. In the LDAP Configuration dialog box, click the Security Domains tab.
2. Click Add.
3. Use LDAP query syntax to create filters to specify the users and groups to be included in this 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 security domain name is not case sensitive and can be between 1 and 80 characters long. It cannot include a tab, newline character, or the following special characters: .,+</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. (&amp;(objectClass=user)(!(cn=susan))) searches all user objects except “susan.” 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>

4. 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.
5. 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 immediately synchronizes all LDAP security domains with 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.
6. Click OK to save the security domains.

**Step 3: Schedule the Synchronization Times**

By default, the Service Manager does not have a 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, create a schedule for the Service Manager to synchronize the users and groups.

You can schedule the time of day when the Service Manager synchronizes the list of users and groups in the LDAP security domains with the LDAP directory service. The Service Manager synchronizes the LDAP security domains with the LDAP directory service every day during the times you set.

**To schedule the synchronization times:**

1. On the LDAP Configuration dialog box, click the Schedule tab.
2. Click the Add button (+) to add a new 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 several times a day.
3. To immediately synchronize the users and groups in the security domains with the users and groups in the LDAP directory service, click Synchronize Now.
4. Click OK to save the synchronization schedule.

**Managing LDAP Users in the PowerCenter Domain**

You can assign roles, privileges, and permissions to LDAP users and groups in an LDAP security domain. You can assign LDAP user accounts to native groups to organize them based on their roles in the PowerCenter domain. You cannot use the Administration Console to create, edit, or delete users and groups in an LDAP security domain.

The Service Manager does not import the LDAP attribute that indicates that a user account is enabled or disabled. You must enable or disable an LDAP user account in the Administration Console. The status of the user account in the LDAP directory service affects user authentication in the PowerCenter applications. For example, a user account is enabled in the PowerCenter domain but disabled in the LDAP directory service. If the LDAP directory service allows disabled user accounts to log in, then the user can log in to PowerCenter applications. If the LDAP directory service does not allow disabled user accounts to log in, then the user cannot log in to PowerCenter applications.

To permanently prohibit users in an LDAP security domain from accessing PowerCenter 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 domain configuration database.

For more information about managing users, see the *PowerCenter Administrator Guide*.

**Author**

Padma Heid
Technical Writer