Informatica

Informatica® PowerExchange for LDAP
10.5

User Guide for PowerCenter

Informatica PowerExchange for LDAP User Guide for PowerCenter
10.5
March 2021

Publication Date: 2021-03-17

Table of Contents

Preface

Use the *Informatica® PowerExchange® for LDAP User Guide* to learn how to read from or write to LDAP by using the PowerCenter Client. Learn to create an LDAP connection, develop mappings, and run sessions in an Informatica domain.

Informatica Resources

Informatica Network

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

As a member, you can:

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

Informatica Knowledge Base

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

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

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

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

Informatica Product Availability Matrixes

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

Informatica Velocity

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

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

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

Informatica Marketplace

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

Informatica Global Customer Support

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

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

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

CHAPTER 1

Understanding PowerExchange for LDAP

This chapter includes the following topics:

Understanding PowerExchange for LDAP Overview

Use PowerExchange for LDAP to access and integrate the user profile data with the third-party systems or other LDAP directory servers for decision making. The user profile data is stored on directory servers such as SunOne Directory Server, iPlanet Directory Server, Netscape DS, Active Directory, and Novell eDirectory.

You can use PowerExchange for LDAP to integrate the directory information and perform common updates. For example, you can assign an employee ID, email address, and designation to each employee. PowerExchange for LDAP also synchronizes data among the LDAP directory servers and any other target database, ERP application, or database application.

Understanding LDAP

You can use Lightweight Directory Access Protocol (LDAP) to access X.500-based directory services. LDAP defines a method to access and update information in a directory. A directory server is a specialized database that stores typed and ordered information about objects. You can use directories to find resources with the characteristics required for a particular task. For example, a directory can list information about printers, such as the location, speed in pages for each minute, and supported print streams.

LDAP Security

Verify that you have the required privileges to read the schema and to read and write the contents to the LDAP directory server. You can access the data based on the privileges set for the directory or the user. The Active Directory writes an error into the session log if you do not have the required privileges to access the data. Certain LDAP directory servers do not extract any data if you do not have the required privileges.

LDAP Architecture

LDAP defines the communication protocol and content of the messages exchanged between an LDAP client and an LDAP directory server. The messages specify the operations requested by the client, the responses from the server, and the format of the data carried in the messages. An LDAP client can request operations such as search, add, modify, and delete. LDAP carries the messages over TCP/IP.

Use PowerExchange for LDAP to connect to the LDAP directory server, browse metadata, and import source and target definitions into the repository. Create a mapping to read from and write to the LDAP directory server.

LDAP uses the following process to interact between an LDAP client and an LDAP directory server:

1. The client establishes a session or binding with the LDAP directory server.

   The client specifies the host name or IP address and the port number to which the LDAP directory server is listening.
2. The client can either enter a user name and password for authentication with the server or establish an anonymous session with default access rights. The client can also use one-way or two-way secure communication.
3. The client performs operations on the directory data. LDAP has both read and write capabilities. You can manage and query the directory information.
4. LDAP also searches the directory for data to satisfy the specified criteria. Specify the part of the directory to search and the information to return. A search filter that uses Boolean conditions displays data, based on the condition.
5. After completing the client requests, the client closes the session or unbinds with the server.

LDAP Directory Server

A directory is a set of objects with similar attributes organized in a logical and hierarchical manner. For example, a telephone directory consists of a series of names organized alphabetically. Each name in the telephone directory has an associated address and a phone number.

An LDAP directory is a tree of entries, each of which consists of a set of attributes. An attribute has a name and has one or more values. The schema defines the attributes. Every directory entry has an objectClass attribute that lists the schema which describes the entry. Each entry has a unique identifier called the distinguished name (DN). A DN consists of its Relative Distinguished Name (RDN) constructed from the attributes in the entry, followed by the parent entry DN.

The following table describes the entry details for a person in the LDAP directory:

Attribute/ Entries	Attribute Name	Description	Example
dn	Distinguished Name	Name of the entry.	-
cn	Common Name	RDN of the entry.	John Doe
dc	Domain Component	DN of the parent entry.	example, com
sn	Surname	Surname of the common name.	Doe
mail	Email Address	Email address of the common name.	john@example.com

The following example shows the entries in the LDAP directory:

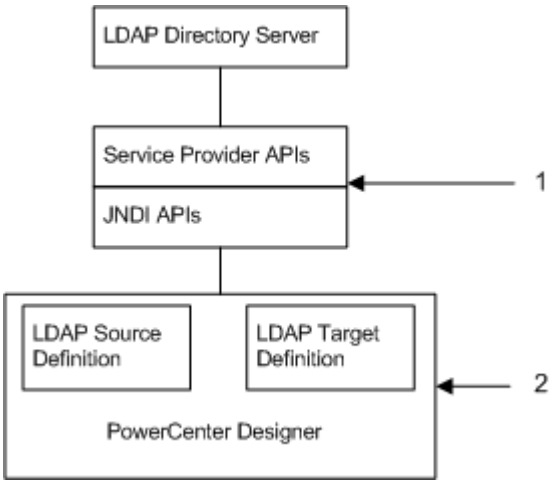
```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

PowerCenter Integration with LDAP

PowerExchange for LDAP reads data from the LDAP directory server and writes data to the LDAP directory server. PowerExchange for LDAP tracks changes made to the directory contents through Change Data Capture (CDC).

Use the Designer to import source and target metadata. When you import LDAP metadata, you connect to the directory server through JNDI and Service Provider APIs. Create mappings with LDAP source and target definitions.

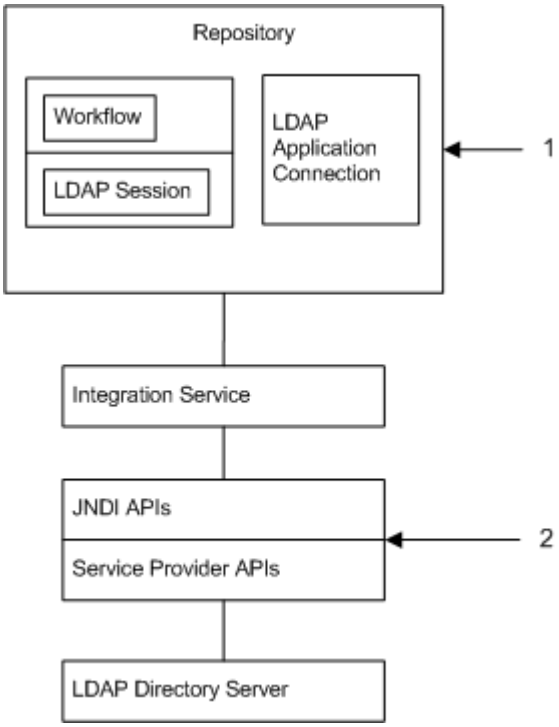
The following figure shows Designer integration with the LDAP directory server:



1. The Designer starts a session (binding) with the LDAP directory server to import source and target definitions using the JNDI or Service Provider APIs (also called as the Service Provider Interface (SPI)).
2. The LDAP source and target definitions represent metadata for LDAP entries.

The PowerCenter Integration Service connects to the LDAP directory server to extract data from LDAP sources and load data into LDAP targets. The PowerCenter Integration Service connects to the LDAP directory server through JNDI APIs.

The following figure shows how the PowerCenter Integration Service integrates with LDAP to extract and load data:



1. The PowerCenter Integration Service reads and writes data based on the session and application connection.
2. The PowerCenter Integration Service connects to the LDAP directory server using the JNDI APIs to read and write data.

When you run a session, the PowerCenter Integration Service uses JNDI APIs to read and write LDAP data. In case of CDC, the first session performs the initial migration of all LDAP data into the target. Subsequent sessions retrieve the changed data.

LDAP Models

The LDAP models describe the LDAP operation, data that can be stored in the LDAP directories, and the data security.

LDAP has the following models:

- LDAP information model. Describes the structure of the information stored in an LDAP directory.
- LDAP naming model. Describes how information is organized and identified.
- LDAP functional model. Describes the operations that can be performed on the information stored in an LDAP directory.
- LDAP security model. Describes how the information in an LDAP directory can be protected from an unauthorized access.

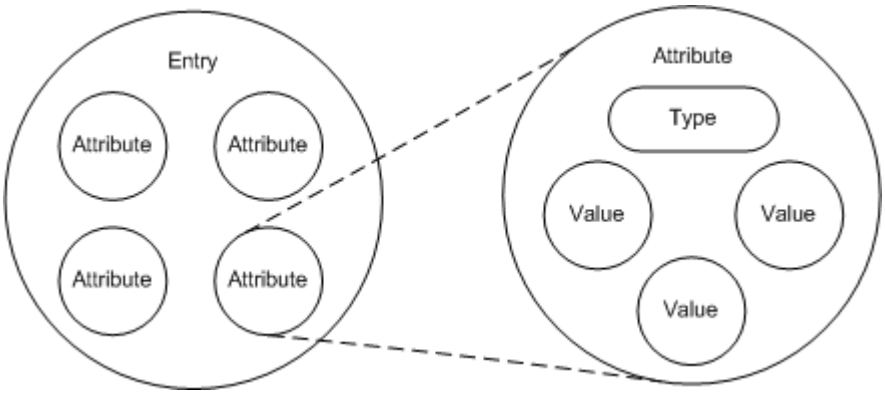
LDAP Information Model

The LDAP information model is based on the entry that contains information about an object.

The following entities represent the LDAP information model:

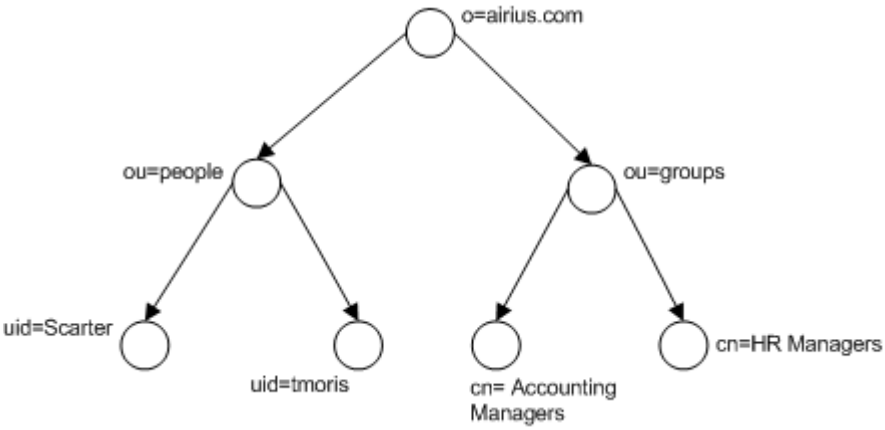
- Entries. An entry is a basic unit of information stored in a directory and consists of a collection of attributes.
- Attribute. Each attribute has a type and is associated with one or more values.

The following figure shows the LDAP information model:



In LDAP, directory entries are arranged in a tree-like structure called Directory Information Tree (DIT).

The following figure shows an example of LDAP DIT:



The following example shows an LDAP record for Sam Carter, an employee with Airius, Inc.:

```
dn: uid=Scarter,ou=People,o=airius.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
uid: scarter
givenname: Sam
sn: Scarter
telephonenumber: +1 408 555 4798
roomnumber: 4612
mail: scarter@airius.com
userpassword: SSHA encrypted password
```

This example shows the full DN of the LDAP entry for Sam Carter, including the absolute path to the entry in the DIT.

The entry belongs to the following object classes:

```
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: airiusPerson
```

The person object class requires that the common name and surname have values. You can add optional fields, such as givenname and telephonenumber, to the object class. The object class organizationalPerson adds more options to the values from person, and inetOrgPerson adds more options to the object class. The Airius customized object class airiusPerson adds all the custom attributes confirming to the schema that the organization wants to track.

LDAP Naming Model

The LDAP naming model defines how entries are identified and organized. Entries are arranged within the DIT based on the company DN.

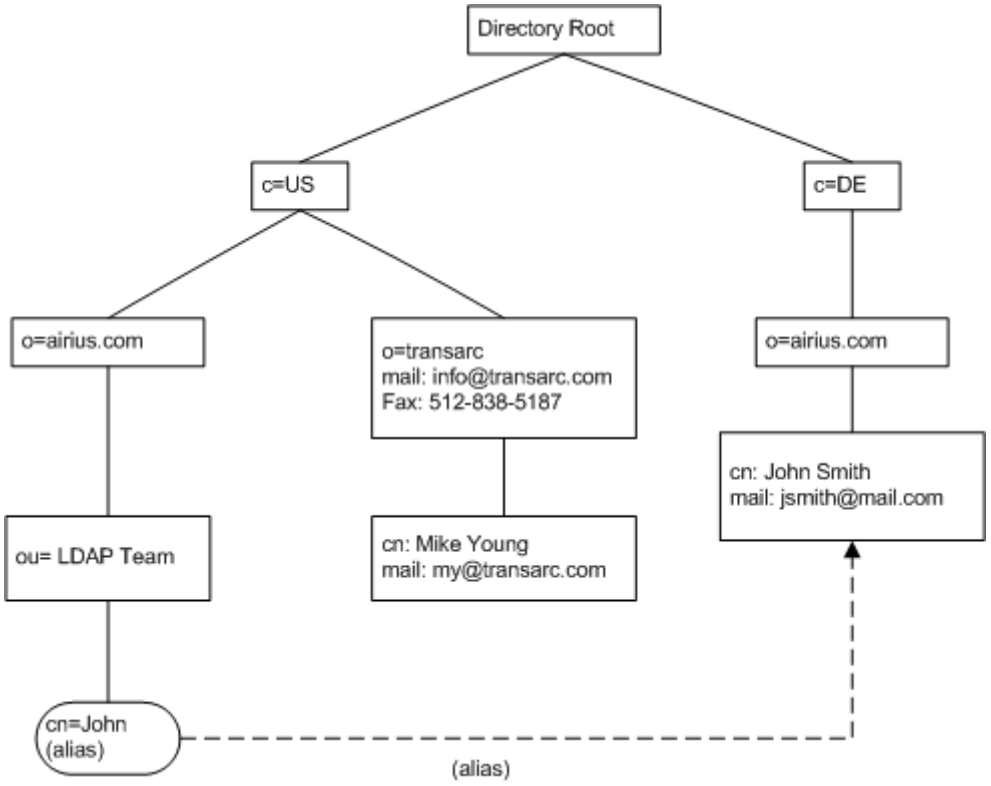
The LDAP directory entries contains the following naming conventions:

- A DN is a unique name that identifies a single entry.
- An RDN consists of a sequence of relative distinguished names.
- Each RDN is derived from the attributes of the directory entry.
- An RDN has the form <attribute name> = <value>.

The DN is formed, based on the RDN in the following example:

```
DN cn=John Smith, o=airius.com, c=DE
RDN cn=John Smith + DN of ancestor o=airius.com, c=DE
```

The following figure shows the LDAP naming model:



LDAP directory entries are arranged in a hierarchy that reflects political, geographical, or organizational boundaries. Entries that represent countries or regions appear at the top of the hierarchy. Entries that represent states or national organizations occupy the second level in the hierarchy. The entries that follow the second level in the hierarchy can represent people, organizational units, printers, documents, or other items.

The following DN represents the complete DN for the example in "LDAP Naming Model" on page 13:

```
dn: cn=John, ou=LDAP Team, o=airius.com, c=US
```

cn=John is the RDN of the entry and ou=LDAP Team, o=airius.com, c=US is the DN of the parent entry.

LDAP Functional Model

The LDAP functional model includes the following categories of operations that are performed against the LDAP directory server:

- Authentication. Bind, unbind, and abandon operations used to connect to and disconnect from an LDAP directory server, establish access rights, and protect information.
- Query or Interrogation. Search and compare entries satisfying the user-specified criteria.
- Update. Add, delete, or modify an entry, and modify the DN or RDN of an entry.

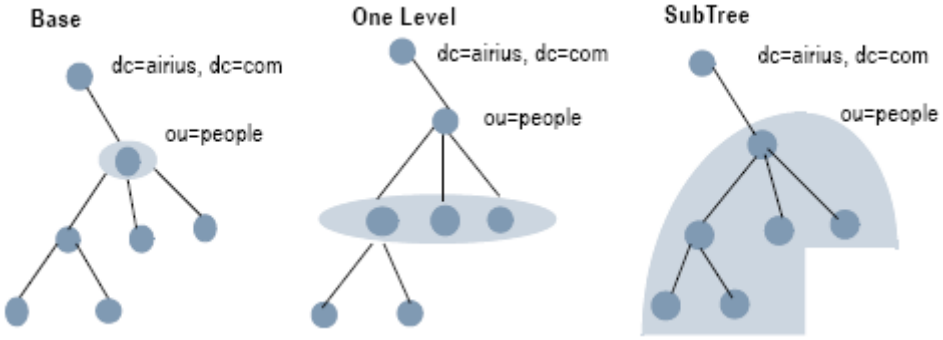
Use the following options to perform the search operation:

- Base DN. The starting point within the DIT.
- Scope. Specifies the search level in the query that limits the scope of the search performed on the directory data.

  LDAP uses the following search levels to limit the scope of the search performed on the directory data:

  - Base or Object. Specifies that the search is carried out on the base DN.
  - One Level. Specifies that the search is carried out on the entries that are directly below the base DN.
  - SubTree. Specifies that the search is carried out on the entire SubTree rooted at the base DN.
- Search Filter. Specifies the filter for querying the LDAP entries.
- Returning Attributes. Attributes to retrieve from entries that match the search criteria.

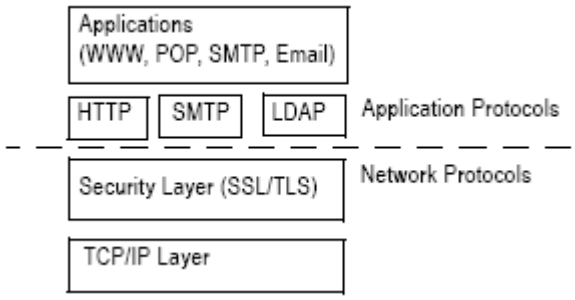
The following figure shows the LDAP functional model:



LDAP Security Model

The LDAP security model protects the directory from any unauthorized access. The LDAP security model uses Secure Socket Layer (SSL) and Transport Layer Security (TLS) that encrypt the data exchanged between a client and a server. LDAP offers a standard method for clients to encrypt data with SSL and TLS.

The following figure shows the LDAP security model:



CHAPTER 2

PowerExchange for LDAP Configuration

This chapter includes the following topics:

PowerExchange for LDAP Configuration Overview

PowerExchange for LDAP installs with the Informatica services. Before you use PowerExchange for LDAP, you must complete the configuration tasks.

Configuring PowerExchange for LDAP

To configure PowerExchange for LDAP, complete the following steps:

1. Create a registry entry for PowerExchange for LDAP on the client machine:
   a. Access the following directory:

      ```
      <Informatica installation directory>\clients\PowerCenterClient\client\bin
      ```

   b. Run the `PWX_LDAP_64.reg` file to create the registry entry.
2. Register the PowerExchange for LDAP plug-in.
3. Configure SSL or TLS authentication (Optional).

After you configure PowerExchange for LDAP, you can create connections to access the LDAP directory server. Create connection objects in Workflow Manager so that the PowerCenter Integration Service can connect to the LDAP directory server.

Registering the Plug-in

After you create a registry entry for PowerExchange for LDAP on the client machine, register the plug-in with the repository. If you are upgrading from a previous version, update the plug-in registration when you register the plug-in.

To register the plug-in, the repository must be running in exclusive mode. Use the Administrator tool or the pmrep RegisterPlugin command line program to register the plug-in. If you do not have the correct privileges to register the plug-in, contact the user who manages the PowerCenter Repository Service.

The plug-in file is an .xml file that defines the functionality of the adapter. When you install the server component, the installer copies the plug-in file to the following directory:

```
<Informatica installation directory>/server/bin/plugin
```

The name of the plug-in file for PowerExchange for LDAP is `pmldap.xml`.

Registering the Plug-in from the Administrator Tool

Register a repository plug-in to add its functionality to the repository.

1. Run the PowerCenter Repository Service in exclusive mode.
2. In the **Navigator**, select the PowerCenter Repository Service to which you want to add the plug-in.
3. In the **Contents** panel, click the **Plug-ins** view.
4. In the **Actions** menu of the **Domain** tab, select **Register Plug-in**.
5. On the **Register Plugin** page, click the **Browse** button to locate the plug-in file.
6. Enter your user name, password, and security domain.

   The **Security Domain** field appears when the Informatica domain contains an LDAP security domain.
7. Click **OK**.

   The PowerCenter Repository Service registers the plug-in with the repository. The results of the registration operation appear in the activity log.
8. Run the PowerCenter Repository Service in normal mode.

Registering the Plug-in from the Command Line Program

You can use the pmrep RegisterPlugin command to register the plug-in from the command line program.

1. Run the PowerCenter Repository Service in exclusive mode.
2. Run the `pmrep Connect` command to connect to the Repository Service using a user account with Administrator Repository privilege.

   The RegisterPlugin command uses the following syntax:

   ```
   pmrep connect -r <repository name> -d <domain_name> -n <domain user name> -x
   <domain_password>
   ```
3. Find `<adaptername>.xml` in the following directory:

   ```
   <Informatica installation directory>\server\bin\Plugin
   ```
4. Run the `pmrep RegisterPlugin` command to update the repository.

   The `RegisterPlugi`n command uses the following syntax:

   ```
   pmrep registerplugin -i <Informatica installation directory>\server\bin\Plugin
   \<adaptername>.xml -e
   ```

Configuring SSL or TLS Authentication (Optional)

The PowerCenter Integration Service uses a trust certificate file to establish a secure connection with the LDAP directory server over SSL or TLS. To establish a secure connection with the LDAP directory server over SSL or TLS, add the trust certificates to the cacerts keystore in the JRE. The cacerts keystore is located in the following directory:

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

For example, use the following syntax to add the certificate certificate.cer to the cacerts keystore:

```
<Informatica installation directory>\java\bin\keytool -import -alias <certificate alias>
-file certificate.cer -keystore <PowerCenter Installation Directory>\java\jre\lib
\security\cacerts –v
```

Note: For more information about the trust certificates, contact your LDAP system administrator.

CHAPTER 3

LDAP Sources and Targets

This chapter includes the following topics:

LDAP Sources and Targets Overview

The LDAP source and target definitions represent metadata for LDAP entries. An LDAP source or target definition can contain single-valued and multi-valued attributes. A single-valued attribute can store one value at a time, and a multi-valued attribute can store more than one value at a time.

A multi-group source or target contains groups for single-valued and multi-valued attributes. All the single-valued attributes are part of a single group that is the parent group. The multi-group source or target contains a group for each multi-valued attribute.

The first group in a multi-group source or target is a parent group for all the groups in that source or target. The other groups are child groups of the parent group.

When the PowerCenter Integration Service extracts data from the source or loads data into the target, it converts the data based on the datatypes associated with the source or the target.

Importing LDAP Source and Target Definitions

Use the Import from LDAP Directory Wizard to import LDAP source and target definitions into the PowerCenter repository. When you import the LDAP source and target definitions, the Designer displays a table with columns and LDAP datatypes.

The following table lists the default precisions for creating a source or a target in the Designer:

Attribute / Datatype	Precision
dn	1024
String	255

Attribute / Datatype	Precision
Binary	65535
Date/Time	255
Integer	10

If you create a source or a target with the precision greater than the default precision, you can update the precision value as required. For the string datatype, if the extracted data is longer than the set precision, the PowerCenter Integration Service truncates the data. For all other datatypes, the PowerCenter Integration Service fails to read or write the data if the precision is greater than the default or the set precision.

1. In the Source Analyzer, click Sources > Import from LDAP Directory. Or, in the Target Designer, click Targets > Import from LDAP Directory.

   The Import from LDAP Directory Server wizard appears.

2. Enter the following information:

Connection Parameter	Description
LDAP Host	LDAP directory server host name.
LDAP Port	LDAP directory server port number. Default is 389.
Anonymous Access	You can access a directory server as an anonymous user without authentication.
LDAP User	LDAP user name to connect to the LDAP directory server.
Password	Password to connect to the LDAP directory server. If you do not enter the password, the Client establishes an anonymous connection.
Secure Connection	Establishes a secure connection to the LDAP directory server. Select this option to specify the SSL or TLS type of connection.
Security Type	The security type used to establish secure connection with SSL or TLS. If you use TLS to establish a secure connection, select one or both of the following options: - Connection. Secures the connection. - Data Transfer. Secures the data transfer.

   Note: For more information about the connection parameters, contact your LDAP system administrator.

3. Click Connect.

   If you click Connect after entering any details in the subsequent pages of the wizard, a new connection is established.

4. Click Next.

   Step 2 of the wizard appears.

5. Enter the following information to view the LDAP directory server DIT:

Parameter	Description
Naming Context	Naming context for the LDAP directory server.
Filter Value	Filters the entries based on the standard LDAP filters.
Maximum Entries	Maximum number of entries to display in the DIT.
Maximum Search Time	Maximum amount of time in milliseconds to wait for the search results.

Click Show Entries to browse the LDAP directory server DIT to select the base DN node. The Attribute pane displays the attribute details for the selected base DN. The selected base DN appears at the bottom of the page. If you select the naming context and click Next without viewing the entire DIT, the selected naming context appears as the base DN at the bottom of the page.

6. Click Next.

Step 3 of the wizard appears.

7. Enter the following information to select the object classes and attributes:

Parameter	Description
Object Classes	Displays the list of object classes present in the schema.
Object Class Attributes	Displays the attributes for the selected object class along with the attribute identifiers such as Name, Description, and Must or May attributes. Use the following options to select the object class attributes: - Select None. Select this option to clear the selection. You can manually select the object class attributes. - Select All. Select all the object class attributes. - Select All Must. Select all the MUST object class attributes. - Select All May. Select all the MAY object class attributes.
Include parent class attributes	Includes the parent class attributes of the selected object class in the Object Class Attributes list.
Selected Attributes	Displays the selected single-valued or multi-valued attributes as the column of the source or target table.

Note: For a target, in the Select Attributes section, select at least one field as the primary key.

For a source, the dn attribute is used to retrieve the distinguished name for the entries from the LDAP directory server. For a target, the dn attribute is used to insert, update, or delete the entries on the basis of their distinguished name from the LDAP directory server.

8. Optionally, click the Data Preview tab to preview the data for the selected attributes.

You can preview data for an LDAP source. You cannot preview data for an LDAP target.

9. Click Next.

The summary page appears.

10. Enter the source or target definition name.
11. Click Add to Import List to add the source or target definition to the import list.

If you select all single-valued attributes, the Designer creates a single group definition. If you select a multi-valued attribute, the Designer creates a multi-group definition.

12. Optionally, click Import Another Source to import another source. Or, click Import Another Target to import another target.
13. Repeat steps 2 to 11 to import another source or target definition.
14. Click Finish.

Configuring Application Source Qualifier Properties

Configure the Application Source Qualifier properties for an LDAP source on the LDAP Properties tab.

The following table describes the LDAP properties for LDAP sources:

Property	Description
Source Filter	Configure a filter condition to query for the LDAP entries. Use the standard LDAP syntax for filter expressions. For example, "(&(sn=Geisel)(mail=*))" Default is blank. You can include parameters and variables in a filter condition. The PowerCenter Integration Service handles parameters and variables in the following order: - Predefined server variables - Mapping parameters and variables - Workflow variables - Session parameters
Search Level	Limits the scope of search performed on the directory data. You can use the following search levels: - Base. The PowerCenter Integration Service performs the search operation on the base DN. - One Level. The PowerCenter Integration Service performs the search operation on the entries that are one level below the base DN. - SubTree Level. The PowerCenter Integration Service performs the search operation on the entire SubTree of the base DN. Default is SubTree Level.
Include Object classes in filter	Includes the selected object classes in the LDAP filter when the queries are executed. Select this option to retrieve the entries that belong to all the selected object classes. Disable this option to retrieve entries regardless of their object class.
Server Side Sorting	Determines whether the server-side sorting is enabled and critical. You can use the following server-side sorting options: - No. The unsorted data is displayed. - Yes. If the server supports sorting, the sorted data is displayed. If the server does not support sorting, the unsorted data is displayed. - Critical. If the server supports sorting, the sorted data is displayed. If the server does not support sorting, the PowerCenter Integration Service does not perform the search operation and returns an error. Default is No.
Sorted Ports	List of ports selected for server-side sorting. The selected ports appear as a comma-separated list of attributes that are used for server-side sorting. Default is blank.

Property	Description
Dereference Aliases	Indicates how the PowerCenter Integration Service dereference aliases during the search operations. You can select the following options to dereference aliases: - Always. Always dereference aliases. - Never. Never dereference aliases. - Finding. Dereference aliases when you locate the target entry. - Searching. Dereference aliases after you locate the target entry. Default is Always.
Follow Referrals	Specify whether you want to automatically follows referrals. The following options determine how to follow referrals: - Ignore. Ignores referrals. - Follow. Follows referrals automatically. - Throw. Follows referrals if the PowerCenter Integration Service successfully binds the entries to the referred directory server with supplied credentials. If the PowerCenter Integration Service does not successfully bind the entries to the referred directory server, it writes a non-fatal error into the session log. When the PowerCenter Integration Service extracts data from an LDAP source, it counts the errors encountered during resolving the referral entry. The PowerCenter Integration Service fails the session when the error count reaches the error threshold. Default is Ignore. For the Follow and Throw options, the dn attribute value is modified from the URL format to the simple format by removing the protocol and the referred directory server details. For example, “ldap://ldapserver:389/cn=refEntry,o=airius.com,cn=testref2,o=airius.com” is modified to the simple format “cn=refEntry,o=airius.com,cn=testref2,o=airius.com”.
Maximum Entries	Maximum number of entries to be returned as a result of the search. If the value is 0, the PowerCenter Integration Service returns all the entries. The Count Limit session attribute overrides the Maximum Entries value. Default is 0.
Maximum Search Time	Maximum time in milliseconds to wait for the search results. A value of 0 indicates that there is no maximum time limit. The Time Limit session attribute overrides the Maximum Search Time value. Default is 0.
Page Size	Size of the page set to retrieve the maximum number of entries for each page. A value of 0 indicates that all the entries are retrieved in one page. Default is 0.

Syntax for the Filter Condition

An LDAP filter consists of one or more Boolean expressions.

The Boolean expressions use the following format:

```
<Attribute><Operator><Value>
```

Attribute is the LDAP attribute name and Value is the field value. If you use logical operators, add the operators as a prefix to the expression list.

Operators

The following table describes the operators that you can use in a filter condition:

Operator	Description
=	Extracts data where value of a field is equal to the specified value. For example, (cn=Directory Administrators)
<=	Extracts data where value of a field is lesser than or equal to the specified value. For example, (roomNumber<=2200)
>=	Extracts data where value of a field is greater than or equal to the specified value. For example, (roomNumber>=2000)
!	Extracts data where value of a field is not equal to the specified value. For example, (!(roomNumber=2290))
|	Extracts data where value of a field is equal to any one of the specified values. For example, (|(cn=Anne-Louise)(cn=Andy Bergin))
*	Extracts data that contains the specified value. - Filter condition as a prefix. For example, enter (ou=Special*) to display the data that begins with Special. - Filter condition as a suffix. For example, enter (ou=*ISV) to display the data that ends with ISV. - Filter condition as a substring. For example, enter(objectClass=*Org*) to display the data that contains Org.
&	Extracts data where value of a field is equal to all the specified values. For example, (&(roomNumber=2000)(roomNumber=3000))

Configuring a Page Control

You can configure one of the following page controls to retrieve directory entries in pages:

- Virtual List View Control. Configure the Virtual List View Control if the page control for the directory server is set to Virtual List View Control.
- Paged Results Control. Configure the Paged Results Control if the page control for the directory server is set to Paged Results Control.

You can also select the Auto Select Page Control option in the session-level properties to allow the PowerCenter Integration Service to automatically choose the page control to retrieve the directory entries. By default, the PowerCenter Integration Service selects the page control that is set for the directory server. If the page control for the directory server allows both Virtual List View Control and Paged Results Control, the PowerCenter Integration Service selects Virtual List View Control to retrieve the directory entries in pages.

CHAPTER 4

LDAP Mappings

This chapter includes the following topics:

Mappings for Single-Group and Multi-Group Sources

Consider a multi-valued source that has single-valued and multi-valued attributes.

The multi-valued source contains the following single-valued attributes:

- dn
- employeeNumber
- displayName

The multi-valued source contains the following multi-valued attributes:

- mail
- objectClass

The multi-valued source definition contains a group for the dn, displayName, and employeeNumber attributes. It also contains groups for the objectClass and mail attributes.

Generating Key Values

When you import a multi-group LDAP source definition, the Designer creates a key relationship between each child group in the source definition and the parent group. Each key uses the following naming convention:

GPK__<group_name>

GFK__<parentgroup_name>__<group_name>

The following table describes the key naming conventions:

Key Name Component	Description
GPK|GFK	Type of key. A group primary key name begins with GPK. A group foreign key name begins with GFK.
group_name	Name of the group to which the key belongs.
parentgroup_name	Name of the parent group with which you have established a primary key relationship.

In the multi-valued group, the Designer generates a primary key GPK__Parent_Group for the parent group. The Designer generates GFK__Parent_Group__objectClass and GFK__Parent_Group__mail foreign keys for the child groups. The PowerCenter Integration Service generates the values for the update strategy.

The following table shows the sample rows in the Parent_Group parent group from the source:

GPK__Parent_Group	displayName	employeeNumber
1	Sam Carter	4576
2	Ted Morris	6712

The following table shows the sample rows in the objectClass child group:

GFK__ Parent_Group__objectClass	objectClass
1	top
1	person
1	organizationalPerson
1	inetOrgPerson
2	top
2	person
2	organizationalPerson
2	inetOrgPerson

The following table shows the sample rows in the mail child group from the source:

GFK__Parent_Group__mail	mail
1	scarter@airius.com
1	samcarter@gmail.com
2	tmorris@airius.com

GFK__Parent_Group__mail	mail
2	ted@gmail.com
2	tedmorris@rediffmail.com

To maintain key relationships when you connect mapping objects, connect source columns to the corresponding groups into the target definitions.

Note: When you create mappings with the primary key-foreign key relationship, the Designer might not create the relationship for the tables. You need to manually set the primary key relationship in the foreign key table.

The following table lists the column relationships between the groups in the multi-valued source definition and the target definitions:

Source Group Name	Source Column Name	Target Name	Target Column Name
Parent_Group	GPK__Parent_Group	single3	GPK_Parent_Group
Parent_Group	dn	single3	dn
Parent_Group	employeeNumber	single3	employeeNumber
Parent_Group	displayName	single3	displayName
objectClass	GFK__Parent_Group__objectClass	single11	GFK_Parent_objectClass
objectClass	objectClass	single11	objectClass
mail	GFK__Parent_Group__mail	single21	GFK_Parent_mail
mail	mail	single21	mail

The PowerCenter Integration Service extracts the following rows from the source definition:

```
[Parent (“Sam Carter”, “4576”), objectClass (top, person, organizationalPerson,
inetOrgPerson), mail (scarter@airius.com, samcarter@gmail.com)]
[Parent (“Ted Morris”, “6712”), objectClass (top, person, organizationalPerson,
inetOrgPerson), mail (tmorris@airius.com, ted@gmail.com, tedmorris@rediffmail.com)]
```

Note: The PowerCenter Integration Service fails the session if you change the order of the groups or columns in the source definition.

Mappings for Single-Group and Multi-Group Targets

Consider a multi-valued target that has single-valued and multi-valued attributes.

The multi-valued target contains the following single-valued attributes:

- dn
- employeeNumber
- displayName

The multi-valued target contains the following multi-valued attributes:

- ou
- mail

The multi-valued target definition contains a group for the dn, displayName, and employeeNumber attributes. It also contains a group for the ou attribute and a group for the mail attribute.

Generating Key Values

When you import an LDAP target definition, the Designer creates a key relationship between a group in the target definition and its parent group.

Note: When you create mappings with the primary key-foreign key relationship, the Designer might not create the relationship for the tables. You need to manually set the primary key relationship in the foreign key table.

For more information about the naming conventions, see "Generating Key Values" on page 25.

For the multi-valued target, the Designer generates the primary key GPK__Parent_Group for the parent group. The Designer generates the primary keys, GPK__mail and GPK__ou for the child groups. The Designer generates GFK__Parent_Group__mail and GFK__Parent_Group__ou foreign keys for the child groups.

The GPK is a unique field of the data rows for the child group. The GFK field relates each child group row with a parent group entry. Verify that the values of GFK field are selected from the values provided for the GPK field in the parent group.

Note: The GPK and GFK fields must not be NULL. If GPK and GFK fields are NULL, the PowerCenter Integration Service writes an error in the session log.

Configuring the Update Strategy

Each group in the target definition contains an attribute that determines the update strategy for the rows in that group. Configure the update strategy attribute in the mapping to specify the operation that you need to perform on the rows. You can perform INSERT, UPDATE, and DELETE operations on the rows. The default is INSERT.

The following table lists the valid values for the update strategy field for the parent group:

Operation	Value
INSERT	0
UPDATE AS UPDATE	1
DELETE	2
UPDATE ELSE INSERT	3

If you specify an invalid value for this field, the PowerCenter Integration Service treats the invalid value as INSERT. If you mark an entry for INSERT, the PowerCenter Integration Service treats the entry as INSERT. If the entry exists, the PowerCenter Integration Service writes an error into the session log. The session fails if the error count reaches the error threshold.

Note: At the session level, the PowerCenter Integration Service ignores the value of the Treat Source Rows As property.

For child rows, an update operation is treated as replace. If a child row is marked for update, all values for the multi-valued attribute are replaced with the updated values. UPDATE AS UPDATE and UPDATE ELSE INSERT are skipped for child rows.

For example, consider an entry with a@infa.com mail attribute. You can add b@infa.com and c@infa.com as another mail attributes. As the child rows are marked for update, the entries b@infa.com and c@infa.com child rows will be marked for update. The rows in the target are replaced with b@infa.com and c@infa.com.

To reflect the changes made in the target, the PowerCenter Integration Service replaces the child rows marked for update with the changed values.

The following table lists the valid values for the update strategy for child group:

Operation	Value
INSERT	0
REPLACE	1
DELETE	2
REPLACE	3

The naming convention for the update strategy field is Update_Strategy_<group_name>. The Parent_Group group contains the Update_Strategy_Parent_Group field, the ou group contains the Update_Strategy_ou field, and the mail group contains the Update_Strategy_mail field.

The following table shows the sample rows in the source ParentGroup_src:

GPK__Parent_Group	Update Strategy	displayName	employeeNumber
1	0	Emanuell Lott	2678
1	0	John Walker	1253

The following table shows the sample rows in the source ou_src:

GPK__ou	GFK__Parent_Group__ou	Update_Strategy_ou	ou
1	1	0	Human Resources
2	1	0	People
3	2	0	Accounting
4	2	0	Product Development

The following table shows the sample rows in the source mail_src:

GPK_mail	GFK_Parent_mail	UpdateStrategy	mail
1	1	0	elott@airius.com
2	1	0	emanuel@gmail.com

GPK_mail	GFK_Parent_mail	UpdateStrategy	mail
3	1	0	elott@rediffmail.com
4	2	0	jwalker@airius.com
5	2	0	johnwalke@gmail.com

In this example, each source represents a group in the target definition. To maintain key relationships when you connect mapping objects, connect the source columns to the corresponding group in the target definition.

Note: The PowerCenter Integration Service fails the session if you change the order of the groups or columns in the target definition.

The following table lists the column relationships between the source definitions and the groups in the multi-valued target definition:

Source Name	Source Column Name	Multi-Valued Group Name	Target Column Name
ParentGroup_src	GPK_Parent	Parent_Group	GPK__Parent_Group
ParentGroup_src	displayName	Parent_Group	displayName
ParentGroup_src	employeeNumber	Parent_Group	employeeNumber
mail_src	GPK_mail	mail	GPK__mail
mail_src	GFK_Parent_mail	mail	GFK__Parent_Group__mail
mail_src	mail	mail	mail
ou_src	GPK_ou	ou	GPK__ou
ou_src	GFK_Parent_ou	ou	GFK__Parent_Group__ou
ou_src	ou	ou	ou

The PowerCenter Integration Service inserts the following rows into the target definition:

```
[Parent (Emanuel Lott, 2678, ou (Human resources, People), mail (elott@airius.com,
emanuel@gmail.com, elott@rediffmail.com)]
[Parent (John Walker, 1253, ou (Accounting, Product Development), mail
(jwalker@airius.com, johnwalker@gmail.com)]
```

Note: If the DN field is linked and is configured as the primary key for the target, the entry is inserted according to the DN value for the field.

```
DN = Primary key value + Base DN
```

For example, the base DN value for the LDAP target is ou=People, o=airius.com, and cn is selected as the primary key. If the value for the cn attribute is John, the DN value of the inserted entry is cn=John, ou=People, o=airius.com. Otherwise, the entry is inserted under the base DN selected for the target definition.

CHAPTER 5

LDAP Sessions

This chapter includes the following topics:

LDAP Connections

Use a LDAP connection to connect to the LDAP database. The PowerCenter Integration Service uses the connection when you run an LDAP session.

PowerExchange for LDAP Connection Properties

When you configure a LDAP connection, you define the connection attributes that the PowerCenter Integration Service uses to connect to the LDAP.

The following table describes the connection properties:

Property	Description
User Name	User name to connect to the LDAP directory server.
Password	Password to connect to the LDAP directory server. If the user name does not require the password, enter `infa_blank`.
Host Name	LDAP directory server host name. Default is localhost.
Port Number	LDAP directory server port number. Default is 389.
Anonymous Access	Select this option to establish an anonymous connection with the LDAP directory server. If you select this option, enter the user name and password as `anonymous`.

Property	Description
Security	Type of security used to establish secure connection with SSL or TLS. Default is None. If you do not select the security type or select the SSL option to establish a secure connection, the PowerCenter Integration Service ignores the TLS options.
TLS Options	TLS options used to establish secure connection or transfer data, or both, with the LDAP directory server. Default is None.

Configuring Application Connections

Configure an LDAP application connection before the PowerCenter Integration Service can read data from the LDAP sources or write data to the LDAP targets. When you configure an LDAP connection, you can specify the connection attributes that the PowerCenter Integration Service uses to connect to the LDAP directory server.

1. In the **Workflow Manager**, click **Connections** > **Application**.

   The Application Connection Browser dialog box appears.
2. Click **New**.
3. Select **LDAP Connection** from the **Select Subtype** list.
4. Click **OK**.

   The **Connection Object Definition** dialog box appears.
5. Enter the LDAP connection properties.

Configuring Sessions for LDAP Sources

You can configure the following session properties for LDAP sources:

Source Filter

Configure a filter condition to query for the LDAP entries. Use the standard LDAP syntax for filter expressions. For example, “(&(sn=Geisel)(mail=*))” Default is blank.

You can include parameters and variables in a filter condition.

The PowerCenter Integration Service handles parameters and variables in the following order:

- Predefined server variables
- Mapping parameters and variables
- Workflow variables
- Session parameters

Source Filter File Name

Directory location of the file and the file name that contains multiple filter conditions to query the LDAP entries.

For example, `C:\export\LDAPSourceFilter.txt`

Use the LDAP syntax for filter expressions. For example, `(&(sn=Geisel)(mail=*))`. Specify each filter condition on a new line.

Note: The source filter takes precedence over the source filter file you specify in the session properties.

Change Data Capture

The PowerCenter Integration Service captures the changed data and writes the changed data into the target. The PowerCenter Integration Service runs a session to migrate the data and the subsequent sessions report the changed data.

Change Data Capture file directory

Directory location where the change data file is created. The file stores the change number and time for the last read changed entry. Default is $PMRootDir/CdcFiles.

Change Data Capture filename

File name for Change data capture where the changeNumber and changeTime attributes are stored for the session.

Reset Changelog Cache

Migrates the LDAP data into a target and indicates that the changes are not to be fetched. Default is No.

Treat Data Conversion Error As

Set the following values to indicate how the PowerCenter Integration Service treats the data conversion errors:

- Fatal. The PowerCenter Integration Service fails the session if the data conversion error occurs.
- Replace with Null. If a data conversion error occurs, the PowerCenter Integration Service sets the LDAP attribute value to null and increments the error count. The PowerCenter Integration Service fails the session when the error count reaches the error threshold.

  Default is Fatal.

Auto Select Page Control

Specifies the page control which is configured for the LDAP directory server to retrieve entries in pages.

Page Controls

Specifies the page control to retrieve directory entries in pages. Use the following page controls:

- Virtual List View Control
- Paged Results Control

Note: If you change the default value for the session properties, the PowerCenter Integration Service overrides the value of the corresponding property in the Application Source Qualifier.

You can include parameters and variables in a sorted port condition for the session level. The PowerCenter Integration Service processes parameters and variables in the following order:

- Predefined server variables
- Mapping parameters and variables
- Workflow variables
- Session parameters

Note: You can view load statistics in the session log. The load summary in the Workflow Monitor does not display load statistics.

Error Handling for LDAP Sources

You can set the error threshold for a session. In the Stop on Errors session property, enter the number of non-fatal errors the PowerCenter Integration Service can encounter before it fails the session.

The PowerCenter Integration Service counts the errors that occur when it converts data and resolves the referral entry when the Follow Referral property is set to Throw.

The session fails when the PowerCenter Integration Service extracts data from the source and the error count for the sum of the data conversion errors and other non-fatal errors reaches the error threshold.

Configuring Sessions for LDAP Targets

The following table describes the session properties for LDAP targets:

Session Property	Description
Duplicate Parent Row Handling	Indicates how the PowerCenter Integration Service handles duplicate parent rows: - First Row. The PowerCenter Integration Service passes the first duplicate row to the target. The PowerCenter Integration Service rejects rows with the same primary key that it processes after this row. - Last Row. The PowerCenter Integration Service passes the last duplicate row to the target. The PowerCenter Integration Service rejects rows with the same primary key that it processes before this row. - Error. The PowerCenter Integration Service passes the first row to the target. Rows that follow with duplicate primary keys increment the error count. The session fails when the error count reaches the error threshold.
Orphan Row Handling	Indicates how the PowerCenter Integration Service handles orphan rows: - Ignore. The PowerCenter Integration Service ignores orphan rows. - Error. The PowerCenter Integration Service treats orphan rows as error. Error count is incremented for each such row. The session fails when the error count reaches the error threshold.
Include Superclass in Insert	Includes the superclass of the selected object class, in the objectClass attribute of the entry inserted in the LDAP directory server. Default is Yes.
One level update	Performs the update and delete operation on a single level. One level deep entries are affected in the update and delete operation. Default is No.
Delete old RDN on update	Deletes the old RDN when the RDN value of an entry is updated. Default is No.
Cache Directory	Directory for the LDAP cache files. Default is $PMCacheDir service process variable.
Cache Size	Maximum buffer size in bytes to cache the LDAP data. Default is 10485760 bytes (10 MB).
Duplicate Row Error Count	Error threshold for the duplicate rows. Default is 0.
Orphan Row Error Count	Error threshold for the orphan rows. Default is 0.

Orphan and Duplicate Rows

Multi-valued attributes have primary key-foreign key relationships with single-valued attributes.

Each group in an LDAP target contains a dummy primary key, and each group other than the parent group contains a dummy foreign key. Use the source fields or the PowerCenter transformations to enter the dummy

keys. If the value for a foreign key in a child group is not from the list of the values for the primary key of the first parent group, the child row is treated as an orphan row. If the value of a primary key is duplicated in more than one row in a particular group, these rows are treated as duplicate rows.

The PowerCenter Integration Service loads the data rows into the LDAP directory server that retains the primary key-foreign key relationship. The orphan and duplicate rows are discarded. For more information about orphan and duplicate rows, see "Configuring Sessions for LDAP Targets" on page 34.

Error Handling for LDAP Targets

You can set the error threshold for a session. In the Stop on Errors session property, enter the number of non-fatal errors the PowerCenter Integration Service can encounter before it fails the session.

When the PowerCenter Integration Service writes data to an LDAP target, the PowerCenter Integration Service counts the duplicate and orphan rows as non-fatal errors.

The following table describes the behavior of the PowerCenter Integration Service based on the session properties:

Stop on Errors	Orphan Row Handling	Duplicate Parent Row Handling	Description
0	n/a	n/a	The PowerCenter Integration Service writes all rows except the duplicate, orphan, and invalid rows to the target.
>0	Ignore	Error	If the number of duplicate rows in the source data reaches the error threshold, the PowerCenter Integration Service does not write data to the target and the session fails.
>0	Error	First Row or Last Row	If the number of orphan rows in the source data reaches the error threshold, the PowerCenter Integration Service does not write data to the target and the session fails.
>0	Error	Error	If the sum of orphan row count and duplicate row count in the source data reaches the error threshold, the PowerCenter Integration Service does not write data to the target and the session fails.
>0	Ignore	First Row or Last Row	The PowerCenter Integration Service starts writing data into the target. If the non-fatal error count reaches the error threshold, the PowerCenter Integration Service does not write data to the target for that entry and the session fails. However, the PowerCenter Integration Service writes the data to the target for the previous entries.

Set the following values for the PowerCenter Integration Service to write data into the target:

- Error threshold to a value greater than 0
- Orphan row handling and duplicate parent row handling to error

The session fails when the PowerCenter Integration Service starts writing the data to the target, and the sum of duplicate row count, orphan row count, and other non-fatal error count reaches the error threshold.

When the Duplicate Parent Row Handling is set to error and the number of duplicate rows reaches the duplicate row error count, the session fails.

When the Orphan Row Handling is set to error and the number of orphan rows reaches the orphan row error count, the session fails.

The PowerCenter Integration Service does not display the number of duplicate and orphan rows for each group as part of the LDAP session load summary. When the orphan row handling is set to error, the PowerCenter Integration Service writes the total number of orphan rows in the session log. When the duplicate row handling is set to error, the PowerCenter Integration Service writes the total number of duplicate rows in the session log.

Configuring Change Data Capture

LDAP uses the session level attributes to capture the changes from the source.

Change Data Capture

Captures the changes in the source definition and extracts the changed data. If this option is not selected, the session returns all the data that is present under the specified base DN. If you select this option, the PowerCenter Integration Service runs a session to migrate the data and the subsequent sessions report the changed data.

Change Data Capture File Directory

Points to the directory location where the file is created. The change data capture file is created to store the last read changed number for the LDAP source. By default, the file is created under the directory $PMRootDir/CdcFiles. You can change this value to specify another location.

Change Data Capture File Name

Name of the file that stores the change data capture details. The PowerCenter Integration Service captures the change data and updates the file to store the change number and time for the last read changed entry. If you do not provide the file name, the default file name is created based on the source instance name and the partition name for which the PowerCenter Integration Service captures the change data from the LDAP directory server.

Note: The change data capture file is maintained for each source instance, for each partition level. Provide a unique change data capture file name to capture the changes correctly when multiple sessions that are marked for change data capture extracts data from the same source.

Reset Changelog Cache

Indicates to perform the initial migration. It resets the change number stored in a file to the highest change number read during the initial migration. After initial migration, you can manually reset the value of the Reset Changelog Cache to capture the changes made to the LDAP source during the session.

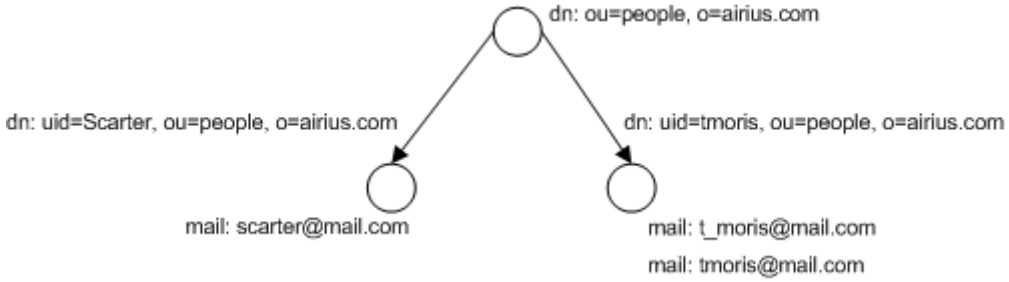
Methods for Tracking Changes in Different Directories

LDAP tracks the changes made to the contents of a directory. LDAP uses the following methods to track changes in different directories:

- Active directory. Active Directory stores the entry and the details for the changes made to the entry along with the entry. The PowerCenter Integration Service determines the change type based on the values for uSNCreated, uSNChanged, and isDeleted attributes of an entry. If an entry is created, the uSNCreated and uSNChanged contains same value. If you update an entry, the uSNChanged value is modified indicating that the entry is updated in the directory server. If you delete an entry, isDeleted is set to True indicating that the entry is deleted from the directory server. Data is retrieved for the uSNChanged attribute, regardless of whether uSNChanged is included as one of the columns in the LDAP source.
- Other directory servers. The different directory servers are Netscape, IPlanet, SunOne, and IBM. The changes are logged under the default cn=changelog node. The directory server adds an entry for each add, modify, and delete operation to the directory under the cn=changelog node. Verify that the changelog option is enabled on the LDAP directory server.

  Note: OpenLDAP does not support Change Data Capture because it does not provide change entries or changelogs.

The following figure shows an entry logged in the session log if you select Change Data Capture when you run the session:



The first time you run the session, the PowerCenter Integration Service migrates the following data to the LDAP directory server:

dn: ou=people, o=airius.com

mail: people@mail.com

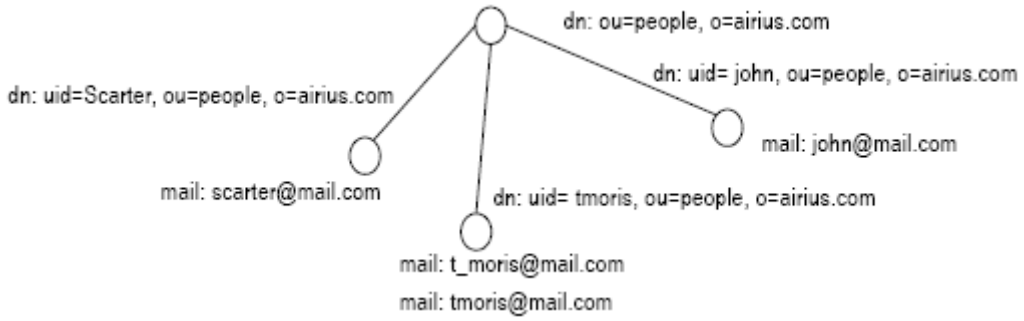
The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 0, ou=people, o=airius.com 2, 0, uid=scarter, ou=people, o=airius.com 3, 0, uid=tmoris, ou=people, o=airius.com
uid	1, 0, <NULL> 2, 0, scarter 3, 0, tmoris
mail	1, 0, people@mail.com 2, 0, scarter@mail.com 3, 0, t_moris@mail.com 3, 0, tmoris@mail.com

When you subsequently run the session, the PowerCenter Integration Service migrates the changes made to the existing data.

Inserting Entries to the dn

The following figure shows the data migrated to the LDAP directory server when you insert an entry to the dn:

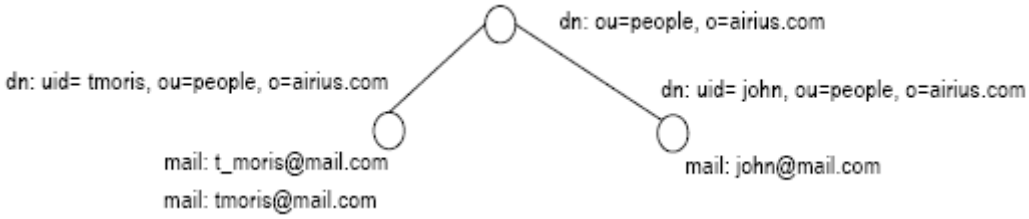


The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 0, uid=John, ou=people, o=airius.com
uid	1, 0, john
mail	1, 0, john@mail.com

Deleting Entries from the dn

The following figure shows the data migrated to the LDAP directory server when you delete an entry from the dn:



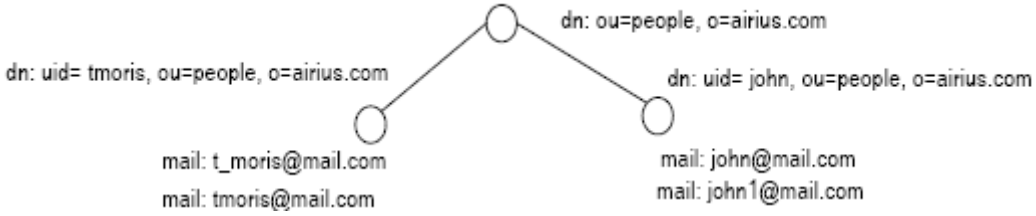
The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 2, uid=scarter, ou=people, o=airius.com
uid	1, 2, <NULL>
mail	1, 2, <NULL>

Note: If you delete an entry, the dn contains the value. The other LDAP attributes will be set to NULL value. To flow the delete operation to the target, ensure that the dn column is linked in the mapping.

Inserting Attributes for the Entry

The following figure shows the data migrated to the LDAP directory server when you insert an attribute for the entry:



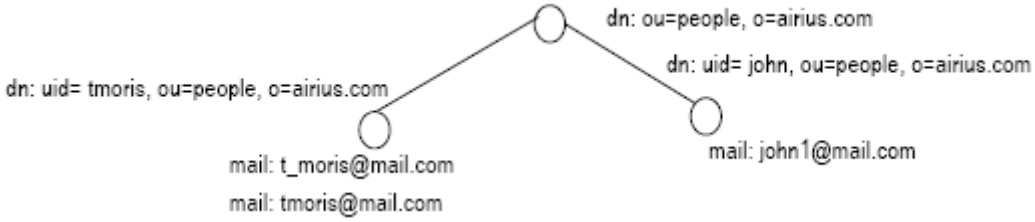
Note: When you insert, delete, or update an attribute for the entry, the entire entry is marked for update.

The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 1, uid=john, ou=people, o=airius.com
uid	1, 1, john
mail	1, 1, john@mail.com 1, 1, john1@mail.com

Deleting Attributes for the Entry

The following figure shows the data migrated to the LDAP directory server on deleting an attribute for the entry:

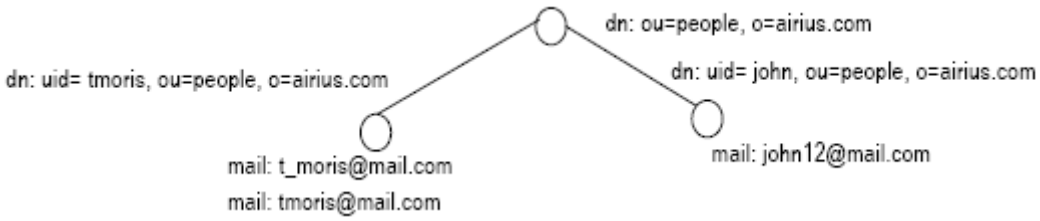


The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 1, uid=john, ou=people, o=airius.com
uid	1, 1, john
mail	1, 1, john1@mail.com

Updating Attributes for the Entry

The following figure shows the data migrated to the LDAP directory server on updating an attribute for the entry:

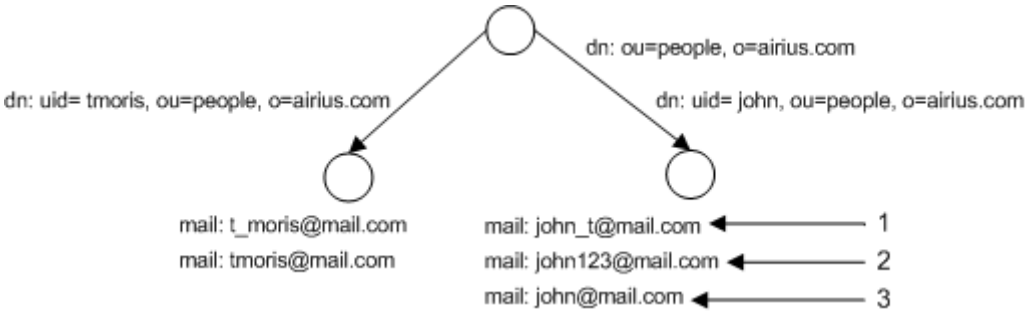


The following table displays the data that the PowerCenter Integration Service migrates to the LDAP directory server:

Group	Data
parent	1, 1, uid=john, ou=people, o=airius.com
uid	1, 1, john
mail	1, 1, john12@mail.com

Multiple Changes to an Entry

The following figure shows the multiple changes made to an entry:



1. Insert an attribute.
2. Update an attribute.
3. Delete an attribute.

The following table displays the data such that if you make multiple changes to an entry between the two sessions run for the change data capture, the PowerCenter Integration Service transfers only one row for the Active Directory Server, which migrates the final entry.

Group	Data
parent	1, 1, uid=john, ou=people, o=airius.com
uid	1, 1, john
mail	1, 1, john_t@mail.com 1, 1, john123@mail.com

The following table displays the data such that if you make multiple changes to an entry between the two sessions run for the change data capture, the PowerCenter Integration Service migrates a separate row for each change that also contains the existing data, for the SunOne directory server:

Group	Data
parent	1, 1, uid=john, ou=people, o=airius.com 2, 1, uid=john, ou=people, o=airius.com 3, 1, uid=john, ou=people, o=airius.com
uid	1, 1, john 2, 1, john 3, 1, john
mail	1, 1, john_t@mail.com 1, 1, john123@mail.com 2, 1, john_t@mail.com 2, 1, john123@mail.com 3, 1, john_t@mail.com 3, 1, john123@mail.com

Troubleshooting LDAP Sessions

The session fails when you extract a large number of entries with the default page size.

If you extract a large number of entries with the default page size, the session may fail due to insufficient memory. Use the following options to extract the required number of entries:

- Increase the Java SDK Maximum Memory in the PowerCenter Integration Service process properties.
- Set the appropriate page size at the Application Source Qualifier level.

The session may not retrieve all source data when you extract entries from the Active Directory Server.

If you extract the number of entries greater than the value set for the MaxPageSize property of the Active Directory Server with the default page size, the session may not retrieve all source data. Use the following options to extract the required number of entries:

- Set the MaxPageSize greater than the number of entries you need to extract.
- Set the page size at the Application Source Qualifier level less than or equal to MaxPageSize.

APPENDIX A

LDAP Datatype Reference

This appendix includes the following topic:

LDAP and Transformation Datatypes

PowerCenter uses the following datatypes in LDAP mappings:

- LDAP native datatypes. LDAP datatypes appear in LDAP definitions in a mapping.
- Transformation datatypes. Set of datatypes that appear in the transformations. They are internal datatypes based on ANSI SQL-92 generic datatypes, which the PowerCenter Integration Service uses to move data across platforms. They appear in all transformations in a mapping.

When the PowerCenter Integration Service reads source data, it converts the native datatypes to the comparable transformation datatypes before transforming the data. When the PowerCenter Integration Service writes to a target, it converts the transformation datatypes to the comparable native datatypes.

The following table lists the LDAP datatypes that PowerCenter supports and the corresponding transformation datatypes:

LDAP Datatype	Transformation Datatype	Range
IA5String	String	1 to 104,857,600 characters
DirectoryString	String	1 to 104,857,600 characters
PrintableString	String	1 to 104,857,600 characters
OctetString	String	1 to 104,857,600 characters
PostalAddress[1]	String	1 to 104,857,600 characters
CountryString	String	1 to 104,857,600 characters
NumericString	String	1 to 104,857,600 characters
Integer	Integer	Precision 10, scale 0
GeneralizedTime	Date/Time	Jan 1, 1753 AD to Dec 31, 9999 AD (precision to nanosecond)

LDAP Datatype	Transformation Datatype	Range
TelephoneNumber	String	1 to 104,857,600 characters
Boolean	String	1 to 104,857,600 characters
Binary	Binary	1 to 104,857,600 bytes
DN	String	1 to 104,857,600 characters
BitString	String	1 to 104,857,600 characters

1. When the PowerCenter Integration Service reads the data from the LDAP source, a new line character in the PostalAddress datatype is replaced by the $ symbol. When the PowerCenter Integration Service writes the data to the LDAP target, the $ symbol in the PostalAddress datatype is replaced by a new line character.

Note: The datatype of an LDAP attribute is set to Printable String if its datatype is not included in the LDAP datatypes. You can edit the LDAP source or target definitions to set the corresponding datatypes.

APPENDIX B

Error Messages

This appendix includes the following topic:

Designer Error Messages

Failed to load the LDAP .jar files.

Explanation: The Designer could not find pmldapc.jar, swt.jar, and log4j-1.2.13.jar files at the following location:

```
<PowerCenter Installation Directory>\9.1.0\clients\PowerCenterClient\client\bin
\javalib
```

User Response: Verify that the .jar files are present in the specified location. If any .jar file is missing, reinstall PowerExchange for LDAP.

Insufficient privileges to access the LDAP data.

Explanation: The user associated with the connection does not have the read permission on the namingContext system attribute and the schema associated with the LDAP data.

User Response: Verify that the user associated with the connection has the read permission on the namingContext system attribute and the schema associated with the LDAP data.

Invalid connection parameters or unable to connect to the LDAP directory server.

Explanation: Either the host name or port number or both are incorrect.

User Response: Verify that the host name and port number are correct.

-or-

Explanation: The LDAP directory server is down or the LDAP services have stopped.

User Response: Start the LDAP services and verify that the network is running.

-or-

Explanation: The Certificate Authority (CA) certificate is not correct or it does not exist.

User Response: Verify that the CA certificate is correct.

-or-

Contact your LDAP directory server administrator for the CA certificate.

No records found matching the search criteria.

Explanation: The parameters specified to search the base DN are not valid.

-or-

There are no records that match the search criteria.

User Response: Verify that the search parameters are valid.

APPENDIX C

Glossary

Directory Information Tree (DIT)

The hierarchy of objects that creates the local directory structure. The LDAP directory server can contain one or more DITs.

directory server

A specialized database or data repository that stores typed and ordered information about the objects.

Distinguished Name (DN)

A series of RDNs that describe the naming attributes of the DIT from the required entry to the directory root.

LDAP model

A model that describes the LDAP operation, the data stored in directories, and the data usage. The LDAP models include the Information model, Naming model, Functional model, and the Security model. These models promote interoperability between directory installations. You can however customize the directory to your specific needs.

multi-valued attribute

An LDAP attribute that can store more than one value at a time.

Relative Distinguished Name (RDN)

A unique name given to an attribute for its level in the hierarchy. RDNs can be single-valued or multi-valued. Two or more attributes are combined to create an RDN. RDN is meaningful when used as part of a DN to describe the attributes.

single-valued attribute

An LDAP attribute that can store one value at a time.

INDEX