Informatica

Informatica® PowerExchange for LDAP
10.2.2

User Guide

Informatica PowerExchange for LDAP User Guide
10.2.2
February 2019

© Copyright Informatica LLC 2015, 2019

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, the Informatica logo, and PowerExchange are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2019-02-21

Table of Contents

Preface 5

Informatica Resources. 5

Informatica Network. 5

Informatica Knowledge Base. 5

Informatica Documentation. 5

Informatica Product Availability Matrices. 6

Informatica Velocity. 6

Informatica Marketplace. 6

Informatica Global Customer Support. 6

Chapter 1: Understanding PowerExchange for LDAP. 7

Understanding PowerExchange for LDAP Overview. 7

Understanding LDAP 7

LDAP Security. 8

LDAP Architecture. 8

LDAP Directory Server. 8

Informatica Integration with LDAP. 9

Chapter 2: PowerExchange for LDAP Configuration. 10

Prerequisites. 10

Configuring TLS Authentication. 10

Adding the Certificate to the Keystore File. 11

Chapter 3: LDAP Connections. 13

LDAP Connection Overview. 13

LDAP Connection Properties. 13

Creating an LDAP Connection in the Developer Tool. 14

Creating an LDAP Connection in the Administrator Tool. 15

Chapter 4: LDAP Data Objects. 16

LDAP Data Objects Overview 16

LDAP Data Object Views. 16

LDAP Data Object Overview Properties. 17

LDAP Data Object Read Operation Properties. 17

Source Properties of the Data Object Read Operation. 17

Output Properties of the Data Object Read Operation. 19

LDAP Data Object Write Operation Properties. 22

Input Properties of the Data Object Write Operation. 22

Target Properties of the Data Object Write Operation. 24

Importing an LDAP Data Object. 25

Importing LDAP Metadata Using Name Filter or Distinguished Name Filter. 26
Creating an LDAP Data Object Read or Write Operation. 27
Rules and Guidelines for LDAP Objects. 27

Chapter 5: LDAP Mappings. 28

LDAP Mappings Overview. 28
LDAP Mapping Example. 28

Chapter 6: LDAP Lookup. 30

LDAP Lookup Overview. 30
LDAP Lookup Properties. 30
General Properties. 31
Ports Properties. 31
Lookup Properties. 32
Adding an LDAP Data Object Operation as an LDAP Lookup in a Mapping. 32

Chapter 7: LDAP Run-Time Processing. 33

LDAP Run-time Processing Overview. 33
Using the Filter Expression to Query LDAP Entries. 33
Native Expression. 33
Platform Expression. 35
Reading and Writing Multivalued Attributes. 35
Specify the Search Scope. 36
Capturing Changed Data in Active Directory. 36
CDC Configuration Scenarios in Active Directory. 37
Configure Update Strategy 38
Parameterization. 38

Appendix A: Data Type Reference. 40

Data Type Reference Overview. 40
LDAP and Transformation Data Types. 41

Index. 43

Preface

The *Informatica PowerExchange® for LDAP User Guide* provides information about Informatica integration with LDAP directory server to read data from and write data to the LDAP directory server. The *User Guide* is written for database administrators and developers responsible for developing mappings that read or write data from LDAP directory server. This book assumes that you have knowledge of LDAP and Informatica.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and 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 find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.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.

Informatica maintains documentation for many products on the Informatica Knowledge Base in addition to the Documentation Portal. If you cannot find documentation for your product or product version on the Documentation Portal, search the Knowledge Base at https://search.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 Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica 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 and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find 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 extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Understanding PowerExchange for LDAP

This chapter includes the following topics:

- Understanding PowerExchange for LDAP Overview, 7
- Understanding LDAP , 7
- Informatica Integration with LDAP, 9

Understanding PowerExchange for LDAP Overview

Use PowerExchange for LDAP to connect to V3 compliant LDAP directory servers from Informatica. You can read data from and write data to LDAP directory servers such as Active Directory.

You can use PowerExchange for LDAP to access user profile data from Microsoft Active Directory. You can also integrate the directory information to Active Directory 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.

Example

You work in the Human Resources department and you manage employee information. Your company had a recent acquisition and you want to synchronize the data from the third-party LDAP directory service to the Microsoft Active Directory of your organization. You use PowerExchange for LDAP to synchronize the list of employees, roles provisioned to users, profile information, contacts, and calendar resources to Active Directory.

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 PowerCenterModel 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.

   Note: The client cannot establish an anonymous session with Active Directory.
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
```

Informatica 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 Informatica Developer to import data objects. When you import LDAP metadata, you connect to the directory server through JNDI and Service Provider APIs. The Informatica Developer uses the JNDI or Service Provider APIs, also called as the Service Provider Interface (SPI), to start a binding with the LDAP directory server to import LDAP data objects. The LDAP data objects represent metadata for LDAP entries.

The Data Integration Service connects to the LDAP directory server to extract data from LDAP sources and load data into LDAP targets. You then create mappings with the LDAP data objects. The Data Integration Service reads and writes data based on the read or write operation you specify.

CHAPTER 2

PowerExchange for LDAP Configuration

This chapter includes the following topics:

- Prerequisites, 10
- Configuring TLS Authentication, 10
- Adding the Certificate to the Keystore File, 11

Prerequisites

PowerExchange for LDAP is installed with the Informatica services.

Before you use PowerExchange for LDAP, install and configure Informatica Services and Informatica Clients.

Create the following services in the Informatica domain:

- Data Integration Service
- Model Repository Service

Configuring TLS Authentication

Before you can work with PowerExchange for LDAP over a secure connection, you need to configure TLS authentication.

The Data Integration Service establishes a secure connection with the LDAP directory server over TLS. You can use one-way SSL or two-way SSL communication.

Use One-Way SSL Communication

You must configure both the Informatica Client and Server for one-way SSL communication.

1. Perform one the following steps for the Informatica Server:
    - Copy the truststore file that has the server certificate in the path specified in INFA _TRUSTSTORE.

- Add the server certificate to the Java cacerts file in following directory: `<Informatica Installation Directory>\java\jre\lib\security`
- Copy the truststore file that has the server certificate file to the following directory: `<Informatica Installation Directory>\tomcat\bin`

2. Perform one of the following steps for the Informatica Client:
   - Copy the trustore file that has the server certificate in the path specified in INFA _TRUSTSTORE.
   - Add the server certificate to the Java cacerts file in the following directory: `<Informatica Client Installation Directory>\java\jre\lib\security`
   - Copy the truststore file that has the server certificate file to the following directory: `<Informatica Client Installation Directory>Clients\DeveloperClient`
3. Specify the name of the truststore file and password in the LDAP connection properties.
4. Restart the Data Integration Service.

Use Two-Way SSL Communication

To use two-way SSL communication, you must first perform the steps for one-way SSL, and then perform the following steps:

1. Copy the keystore file to either the current working directory or the INFA_TRUSTORE path:
   - Current working directory is `<Informatica Installation Directory>\tomcat\bin` for the server and `<Informatica Installation Directory>\client\DeveloperClient` for the client.
   - Path specified in INFA _TRUSTSTORE.
2. Specify the name of the keystore file and password in the connection properties.
3. Restart the Data Integration Service.

Based on the truststore or keystore file name that you specify in the connection properties, the Data Integration Service checks for the trust certificate in the INFA _TRUSTSTORE path, followed by the current working directory, and finally the Java cacerts file. If you do not specify a value for the truststore file in the connection properties, the Data Integration Service searches the certificate only in the Java cacerts file.

For two-way SSL communication, ensure that the trustore and keystore files are available in the same location. For more information about the trust certificates, contact your LDAP system administrator.

Adding the Certificate to the Keystore File

Add the keystore or truststore certificate to the keystore file of the Developer client and server machines.

For example, if you want to add the certificate to the INFA _TRUSTSTORE location, perform the following steps:

1. Copy the certificate files to a local folder.
2. From the command line, browse to `<Informatica Installation Directory>\clients\shared\security` on the client machine and `<Informatica Installation Directory>\services\shared\security` on the server machine.
3. From the command line, run the following command: `keytool -importcert -alias <certificate alias name> -file " <certificate path>\<certificate filename>" -keystore ..\lib\security\infa_truststore.jks` in Windows and `keytool -import -alias rootcer1 -file "<certificate path>/<certificate filename>" -keystore ..\lib\security\infatruststore.jks` in Unix.

4. Enter the password for the keystore.

   The certificate is added to the keystore file.

CHAPTER 3

LDAP Connections

This chapter includes the following topics:

- LDAP Connection Overview, 13
- LDAP Connection Properties, 13
- Creating an LDAP Connection in the Developer Tool, 14
- Creating an LDAP Connection in the Administrator Tool, 15

LDAP Connection Overview

Create a connection to import LDAP metadata to create data objects, preview data, and run mappings.

Configure an LDAP connection before the Data Integration Service can read data from the LDAP sources or write data to the LDAP targets.

You can create an LDAP connection in the Developer tool, the Administrator tool, or through the infacmd isp command.

LDAP Connection Properties

Use an LDAP connection to connect to an LDAP object.

The following table describes the LDAP connection properties:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: `~ ` ! $ % ^ & * ( ) - + = { [}] | \ : ; " ' < , > . ? /`
ID	The string that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.

Property	Description
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	The connection type. Select LDAP.
Host Name	LDAP directory server host name. Default is localhost.
Port	LDAP directory server port number. Default is 389.
Anonymous Connection	Establishes an anonymous connection with the LDAP directory server. Select anonymous connection to access a directory server as an anonymous user without authentication. **Note:** You cannot establish an anonymous connection with Active Directory.
User Name	The LDAP user name to connect to the LDAP directory server.
Password	The password to connect to the LDAP directory server.
Secure Connection	Establishes a secure connection with the LDAP directory server through the TLS protocol.
TrustStore File Name	The file name of the truststore that contains the TLS certificate to establish a secure connection with the LDAP directory server. Default is `infa_truststore.jks`. Required if you select Secure Connection. Contact the LDAP Administrator for the truststore file name and password.
TrustStore Password	The password for the truststore file that contains the SSL certificate.
KeyStore File Name	The file name of the keystore that contains the keys and certificates required to establish a secure communication with the LDAP directory server. Required if you select Secure Connection. Contact the LDAP Administrator for the keystore file name and password.
KeyStore Password	The password for the keystore file required for secure communication.

Creating an LDAP Connection in the Developer Tool

Create a connection before you import LDAP data objects, preview data, or run mappings.

1. Click **Window** > **Preferences**.
2. Select **Informatica** > **Connections**.
3. Expand the domain.
4. Select **Enterprise Applications** > **LDAP** and click **Add**.
5. Enter a connection name.
6. Enter an ID for the connection.

7. Optionally, enter a connection description.
8. Select the domain where you want to create the connection.
9. Select **LDAP** as the connection type.
10. Click **Next**.
11. Configure the connection properties.
12. Click **Test Connection** to verify that you can connect to the LDAP directory server.
13. Click **Finish**.

Creating an LDAP Connection in the Administrator Tool

Create a connection before you import LDAP data objects, preview data, or run mappings.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.
3. In the Navigator, select the domain.
4. In the Navigator, click **Actions** > **New** > **Connection**.

   The New Connection dialog box appears.
5. In the **New Connection** dialog box, select LDAP, and then click **OK**.

   The **New Connection** wizard appears.
6. Enter a connection name.
7. Enter an ID for the connection.
8. Optionally, enter a connection description.
9. Enter the connection properties
10. Click **Test Connection** to verify that you can connect to the LDAP server.
11. Click **Finish**.

CHAPTER 4

LDAP Data Objects

This chapter includes the following topics:

- LDAP Data Objects Overview , 16
- LDAP Data Object Views, 16
- LDAP Data Object Overview Properties, 17
- LDAP Data Object Read Operation Properties, 17
- LDAP Data Object Write Operation Properties, 22
- Importing an LDAP Data Object, 25
- Importing LDAP Metadata Using Name Filter or Distinguished Name Filter, 26
- Creating an LDAP Data Object Read or Write Operation, 27
- Rules and Guidelines for LDAP Objects, 27

LDAP Data Objects Overview

After you configure an LDAP connection, create an LDAP data object to read data from or write data to LDAP directory server.

The LDAP data objects represent metadata for LDAP entries. An LDAP source or target can contain attributes that have single or multiple values. The attributes can be optional or mandatory. A single-valued attribute can store one value at a time, and a multivalued attribute can store more than one value at a time.

LDAP Data Object Views

The LDAP data object contains views to edit the object name and the properties.

After you create an LDAP data object, you can change the data object properties in the following data object views:

- **Overview** view. Edit the LDAP data object name, description, and object.
- **Data Object Operation** view. View and edit the properties that the Data Integration Service uses when it reads data from or writes data to an LDAP data object.

When you create a mapping that uses an LDAP source or a target, you can view the data object read or write properties in the **Properties** view.

LDAP Data Object Overview Properties

The **Overview** view displays general information about the LDAP data object and detailed information about the LDAP object that you imported.

The following table describes the general properties that you configure for an LDAP data object:

Property	Description
Name	Name of the LDAP data object.
Description	Description of the LDAP data object.
Connection	Name of the LDAP connection.

The following table describes the LDAP object properties that you can view:

Property	Description
Name	Name of the LDAP object.
Type	Native data type of the LDAP object.
Description	Description of the LDAP object.

LDAP Data Object Read Operation Properties

The Data Integration Service reads data from an LDAP object based on the data object read operation. The Developer tool displays the data object read operation properties of the LDAP data object in the **Data Object Operation** view.

You can view or configure the data object read operation from the source and output properties.

Source properties

Represents data that the Data Integration Service reads from the LDAP object. Select the source properties to view data, such as the name and description of the LDAP object, the column, and advanced properties.

Output properties

Represents data that the Data Integration Service passes into the mapping pipeline. Select the output properties to edit the port properties of the data object read operation. You can also set advanced properties, such as the parent DN, page size, and CDC.

Source Properties of the Data Object Read Operation

When you create a data object, the source properties populate based on the LDAP object that you add. The source properties of the data object read operation include general, column, and advanced properties that apply to the LDAP object.

You can view the source properties of the data object read operation from the **General**, **Column**, and **Advanced** tabs.

General Properties

The following table describes the source general properties of the data object read operation:

Property	Description
Name	Name of the LDAP source object.
Description	Description of the data object read operation.
Physical Name	The physical name of the source object. For example, `user`.
Path Information	The path to which the source object belongs. For example, the path for the user is `/DC=ADPQA,DC=COM/user`.

Column Properties

The column properties display the data types, precision, and scale of the source property in the data object read operation.

The following table describes the source column properties of the data object read operation:

Property	Description
Name	Name of the column.
Native Name	The name of the attribute in the LDAP server. For any changes in the LDAP attribute name in the LDAP server, you can manually change the native name for the LDAP object to synchronize the imported LDAP data object with the LDAP server object class.
Type	Native data type of the column.
Precision	Maximum number of significant digits for numeric data types, or maximum number of characters for string data types. For numeric data types, precision includes scale.
Scale	Maximum number of digits after the decimal point for numeric values.
Description	Description of the column.
Mandatory	The mandatory attributes of each object class.
MultiValued	An attribute of an ObjectClass that contains multiple values.
Access Type	Indicates whether the field has read and write permissions.

Advanced Properties

The advanced properties display the physical name of the LDAP object.

The following table describes the source column properties of the data object read operation:

Property	Description
Superclasses	A class from which one or more other classes inherit information.
Objectclasses	The type of object that represents a directory entry or record. For example, the objectClass property of a user object identifies the top, person, organizationalPerson, and user classes.
Class Type	The category to which the object classes are assigned: - Structural: Object classes that can have instances in the directory. Structural classes are used to create directory objects or entries. - Abstract: Template object classes that are used only to derive new structural classes. You cannot instantiate abstract classes in the directory. - Auxiliary: A list of attributes that you can append to the definition of a Structural or Abstract class. You cannot instantiate an Auxiliary class in the directory. - Deduced: The Informatica object class type resulting from the union of attributes of all the object classes of the selected DN.
objectCategory	A single-valued property of an instance of an object class that contains the distinguished name of either the class of which the object is an instance or one of its superclasses. When an object is created, the system sets its objectCategory property to the value specified by the defaultObjectCategory property of its object class.

Output Properties of the Data Object Read Operation

The output properties represent data that the Data Integration Service passes into the mapping pipeline. Select the output properties to edit the port properties of the data object read operation.

The output properties of the data object read operation include general properties that apply to the data object operation. The output properties also include port, source, query, and advanced properties that apply to the LDAP object.

You can view and change the output properties of the data object read operation from the **General**, **Ports**, **Sources**, **Query**, and **Advanced** tabs.

General Properties

The general properties display the name and description of the data object read operation.

Ports Properties

The output ports properties display the data types, precision, and scale of the data object read operation.

The following table describes the output ports properties that you configure in the data object read operation:

Property	Description
Name	Name of the port.
Type	Data type of the port.

Property	Description
Precision	Maximum number of significant digits for numeric data types, or maximum number of characters for string data types. For numeric data types, precision includes scale.
Scale	Maximum number of digits after the decimal point for numeric values.
Description	Description of the port.

Sources Properties

The sources properties list the LDAP objects used in the data object read operation. You cannot join data from multiple sources of the LDAP data object in a read operation.

Query Properties

Use the query property to select specific records from LDAP.
The following table describes the query properties that you configure for a data object read operation:

Property	Description
Query	Filter value in a read operation. The filter specifies the where clause of select statement. Use a filter to reduce the number of rows that the Data Integration Service reads from the source. When you enter a source filter, the Developer tool adds a WHERE clause to the default query. You can use the Native or Platform expression to select specific records.

Run-time Properties

The run-time properties displays the name of the connection used for the data object read operation.

The following table describes the run-time properties that you configure for the LDAP source:

Property	Description
Connection	Name of the LDAP connection.

Advanced Properties

Use the advanced properties to specify the data object read operation properties to read data from LDAP objects.

The following table describes the advanced properties that you configure in the data object read operation:

Property	Description
Operation Type	The read operation for the LDAP data object.
Page Size	Size of the page set to retrieve the maximum number of entries for each request. Default is 0. If you set the value of the **Page Size** to 0, the Secure Agent retrieves the number of entries that is set in the **MaxPageSize** LDAP property in one request. For example, if you set the value of the **Page Size** to 0 and the **MaxPageSize** LDAP property is set to 1000, the Secure Agent retrieves 1000 entries in one request. If you set the value of the **Page Size** to a non-zero value, the Secure Agent retrieves all the entries from LDAP in multiple requests. The number of requests made to retrieve the entries are calculated based on the total number of entries in LDAP divided by the **Page Size** value. For example, if you set the value of the **Page Size** to 100, the **MaxPageSize** LDAP property is set to 1000, and there are 1100 entries in LDAP, the Secure Agent retrieves all the entries in 11 requests.
Parent DN	Required. The DN in an LDAP directory server namespace from where you want to fetch data. For example, you can specify the following DN to read data about people from Informatica: ou=people, o= infa.com
Search Level	Searches for entries while reading from the LDAP directory server. You can select one of the following search options: - One-level. Retrieves immediate children of a base object, but excludes the base object. - Subtree. Retrieves all objects subordinate to the base object including the base object. Default is one-level.
Use Object Category Filter	Fetches entries based on the object category value. When disabled, the Data Integration ServiceSecure Agent fetches the entries based on the object class value. For example, when you disable the filter, the user object class fetches the entries from both the user and computer because computer is derived from the user object class. To fetch only the user entry, enable the object category filter as both user and computer have different object category values.
CDC	Captures the changed data in Active Directory based on the time stamp or the last extracted point. Select CDC and configure the following options to capture changed data: - Specify the start time and end time to capture changed data for that period. - Specify only the start time to capture changed data until the last change. - Do not specify a start time and end time to capture data from the last recorded update sequence number (USN). - Specify only the end time to capture changes from the beginning till the specified end time. - Reset the value of the CDC to capture changes by ignoring the values stored in the CDC file.

Property	Description
CDC Start Time	The start time from when you want the Data Integration ServiceSecure Agent to capture the changed data. If you select CDC and specify a start time, but do not specify an end time, the Data Integration ServiceSecure Agent captures the changed data until the last change. Use the following sample format to specify the start time: *20150312081001.0Z*
CDC End Time	The end time until when you want the Data Integration ServiceSecure Agent to capture the changed data. When you specify only the end time, the Data Integration ServiceSecure Agent captures the changed data from the beginning until the specified end time. Use the following sample format to specify the end time: *2050412081001.0Z*
CDC File Path	Absolute path of the file that stores the change number for the last read changed entry.
Reset CDC	Ignores the CDC change number stored in the CDC file. After the reset, the Data Integration ServiceSecure Agent captures the changes made to the LDAP directory server from the beginning.

LDAP Data Object Write Operation Properties

The Data Integration Service writes data to an LDAP object based on the data object write operation. The Developer tool displays the data object write operation properties for the LDAP data object in the **Data Object Operation** section.

You can view the data object write operation from the Input and Target properties.

Input properties

Represent data that the Data Integration Service reads from an LDAP directory server. Select the input properties to edit the port properties and specify the advanced properties of the data object write operation.

Target properties

Represent data that the Data Integration Service writes to LDAP. Select the target properties to view data, such as the name, description, and the relationship of the LDAP object.

Input Properties of the Data Object Write Operation

Input properties represent data that the Data Integration Service writes to an LDAP directory server. Select the input properties to edit the port properties of the data object write operation. You can also specify advanced data object write operation properties to write data to LDAP objects.

The input properties of the data object write operation include general properties that apply to the data object write operation. Input properties also include port, source, and advanced properties that apply to the data object write operation.

You can view and change the input properties of the data object write operation from the **General**, **Ports**, **Sources**, and **Advanced** tabs.

General Properties

The general properties list the name and description of the data object write operation.

Ports Properties

The input ports properties list the data types, precision, and scale of the data object write operation.

The following table describes the input ports properties that you must configure in the data object write operation:

Property	Description
Name	Name of the port.
Type	Data type of the port.
Precision	Maximum number of significant digits for numeric data types, or maximum number of characters for string data types. For numeric data types, precision includes scale.
Scale	Maximum number of digits after the decimal point for numeric values.
Description	Description of the port.

Sources Properties

The sources properties list the LDAP object in the data object write operation.

Run-time Properties

The run-time properties displays the name of the connection used for write transformation.

The following table describes the run-time properties that you configure for an LDAP write operation:

Property	Description
Connection	Name of the LDAP connection.

Advanced Properties

The advanced properties allow you to specify data object write operation properties to write data to an LDAP server.

You can configure the following advanced properties in the data object write operation:

Property	Description
Operation Type	The write operation for an LDAP data object.
ReplaceAll	Replaces the existing values of a multivalued attribute in the LDAP directory server when you use the update operation to write data. To delete multivalued attributes, you must enable this option and pass a null value.

Property	Description
Update Strategy	Updates the rows in the LDAP directory server based on the following update strategy options you set: - Update as Update. Updates all rows flagged for update. - Update else Insert. Updates all rows flagged for update if they exist in the target and inserts those rows that do not exist in the target. Default is Update as Update.
KeyColumn	Required with the parent DN to write data to the LDAP directory server. Select the key column for the entry you want to create. For example, the key column for a user is cn. However, you cannot update a key column because PowerExchange for LDAP does not support updating the relative distinguished name (RDN) of the entry.

Target Properties of the Data Object Write Operation

The target properties represent the data that is used to populate the LDAP data object that you added when you created the data object. The target properties of the data object write operation include general and column properties that apply to the LDAP objects. You can view the target properties of the data object write operation from the **General**, **Column**, and **Advanced** tabs.

General Properties

The general properties display the name, description, physical name, and path of the LDAP object.

Column Properties

The column properties display the data types, precision, and scale of the target property in the data object write operation.

You can view the following target column properties of the data object write operation:

Property	Description
Name	Name of the column.
Type	Native data type of the column property.
Precision	Maximum number of significant digits for numeric data types, or maximum number of characters for string data types. For numeric data types, precision includes scale.
Scale	Maximum number of digits after the decimal point for numeric values.
Primary Key	Determines whether the column property is a part of the primary key.
Description	Description of the column property.

Advanced Properties

The advanced properties displays the superclasses, object classes, class type, and object category of the LDAP object.

The following table describes the advanced properties that you configure for an LDAP write operation:

Property	Description
Superclasses	A class from which one or more other classes inherit information.
Objectclasses	The type of object that represents a directory entry or record. For example, the objectClass property of a user object identifies the top, person, organizationalPerson, and user classes.
Class Type	The category to which the object classes belong: - Structural: Object classes that can have instances in the directory. Structural classes are used to create directory objects or entries. - Abstract: Template object classes that are used only to derive new structural classes. You cannot instantiate abstract classes in the directory. - Auxiliary: A list of attributes that you can append to the definition of a Structural or Abstract class. You cannot instantiate an Auxiliary class in the directory. - Deduced: The Informatica object class type resulting from the union of attributes of all the object classes of the selected DN.
objectCategory	A single-valued property of an instance of an object class that contains the distinguished name of either the class of which the object is an instance or one of its superclasses. When an object is created, the system sets its objectCategory property to the value specified by the defaultObjectCategory property of its object class.

Importing an LDAP Data Object

Import an LDAP data object to add to a mapping.

1. Select a project or folder in the **Object Explorer** view.
2. Click **File** > **New** > **Data Object**.
3. Select **LDAP Data Object** and click **Next**.

   The **LDAP Data Object** dialog box appears.
4. Enter a name for the data object.
5. Click **Browse** next to the **Location** option and select the target project or folder.
6. Click **Browse** next to the **Connection** option and select the LDAP connection from which you want to import the LDAP resource metadata.
7. To add a resource, click **Add** next to the **Selected Resources** option.

   The **Add Resource** dialog box appears.
8. From the Package Explorer, select a naming context from which you want to import the schema.
9. Perform one of the following tasks to import an object class, and then click **OK**:
   - Navigate to the LDAP object classes that you want to import.
   - To filter a specific object class by name, use the Name Filter. You can also use wildcards `'*'`.

- To filter an object class by DN, use the Distinguished Name filter available in the advanced filter. Objects imported using the Distinguished Name filter is of deduced type.

10. If required, add more object classes to the LDAP data object.

    You can also add object classes to an LDAP data object after you create it.

11. Click **Finish**.
    The data object appears under Data Objects in the project or folder in the **Object Explorer** view.

Importing LDAP Metadata Using Name Filter or Distinguished Name Filter

When you create an LDAP data object, you can use the Name filter or Distinguished Name filter to import metadata from an LDAP directory server. The Data Integration Service imports the specified object classes based on the filter type.

Use the following filters to view the Directory Information Tree (DIT) of the LDAP directory server and import the metadata:

Name Filter

Select the LDAP schema to list all the object classes in that schema. When you use the name filter, you can navigate through the displayed object classes and select a specific object class. You can also type the name of the object class in the **Name** filter field and fetch the attributes for that object class. The object class inherits all the attributes of the superclasses. When you select the object class, the **Entity Information** pane displays the attributes for that object class.

You can specify the full name of the object class or you can use wildcards in a name filter.

For example, you can specify `organization unit` to filter entries with the specified object class. To retrieve all object classes, use a wildcard `o*` that filters all object classes.

Distinguished Name Filter

You can also use the Distinguished Name (DN) filter to import the object class. The imported object class is of deduced type, which contains a union of all the structural, auxiliary, and abstract object classes present in that directory hierarchy.

When you type the DN, the search fetches the deduced object class. For example, specify the following DN for the entry:

```
CN=Alpha,OU=DevTestWrite,DC=ADPQATEST,DC=COM
```

The top person organizationalPerson and user object classes form the deduced object class. The **Entity Information** pane displays a union of attributes for this object class.

Note: The Data Integration Service does not fetch the attributes of the securityPrincipalObject class.

Creating an LDAP Data Object Read or Write Operation

You can add a LDAP data object read or write operation to a mapping or mapplet as a source. You can create the data object read or write operation for one or more LDAP data objects.

Before you create a LDAP data object read or write operation, you must create at least one LDAP data object.

1. Select the data object in the Object Explorer view.
2. Right-click and select **New** > **Data Object Operation**.

   The **Data Object Operation** dialog box appears.
3. Enter a name for the data object read or write operation.
4. Select **Read** or **Write** as the type of data object operation.
5. Click **Add**.

   The **Select Resources** dialog box appears.
6. Select the LDAP object for which you want to create the data object read or write operation and click **OK**.
7. Click **Finish**.

The Developer tool creates the data object read or write operation for the selected data object.

Rules and Guidelines for LDAP Objects

Consider the following rules and guidelines for LDAP objects:

- When you write data to LDAP directory server, you cannot update the description attribute as there is a restriction from the JNDI API.
- When you create entries for a user in Active Directory, you cannot set the password for that user. You do not have the required permissions to update passwords because of a restriction from the JNDI APIs.
- You cannot use the Lookup transformation to read data with CDC enabled.
- When you write data to LDAP directory server, ensure that the size of each of the attributes in the entry does not exceed 9 MB.
- PowerExchange for LDAP does not support pushdown optimization when you use != operator in a filter transformation.

CHAPTER 5

LDAP Mappings

This chapter includes the following topic:

- LDAP Mappings Overview, 28

LDAP Mappings Overview

After you create a LDAP data object read and write operation, you can develop a mapping.

You can define the following objects in the mapping:

- LDAP data object read operation as the input to read data from LDAP metadata.
- LDAP data object write operation as the output to write data to LDAP data objects.

Validate and run the mapping to read data from and write data to LDAP server.

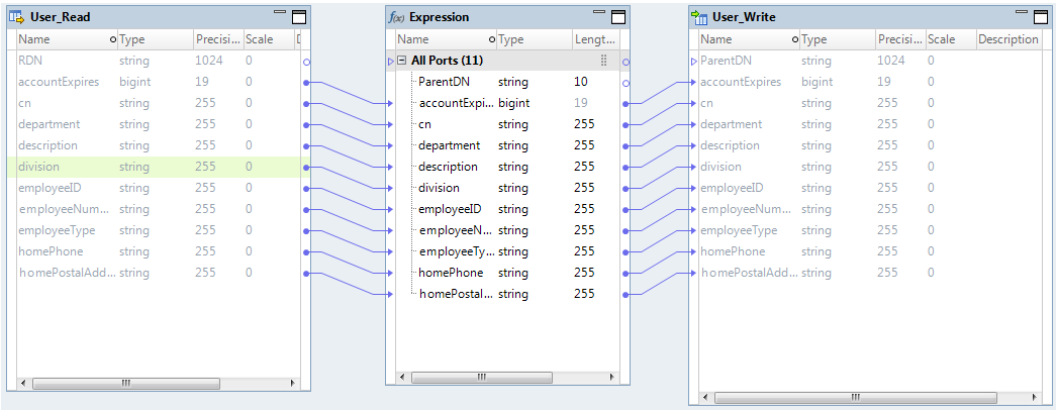
LDAP Mapping Example

You work in the Human Resources department and you manage employee information. Your company wants to merge the sales and marketing teams. You want to synchronize the list of employee information from the Sales team to the Sales and Marketing team so that you can manage users at the enterprise level.

You want to retrieve all user objects from the *Sales* organizational unit (OU) and write the user information to the *Sales&Marketing* OU within the *DC=ADPQAINFA,DC=COM* domain.

Create a mapping that reads the user objects and writes these records to Active Directory.

The following image shows the LDAP mapping example:

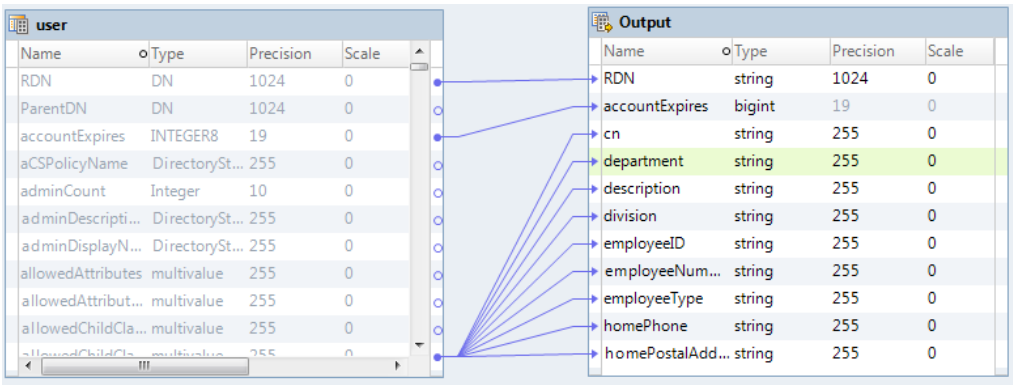


The mapping contains an LDAP source that contains Sales employee information. The Expression transformation transforms the parent DN of Sales to Sales&Marketing. The mapping output contains an LDAP data object write operation to write data to the Sales and Marketing team.

Mapping Input

The source for the mapping is an LDAP user object. To read data from the LDAP server, create a data object read operation called User_Read.

The following image shows the user information from the Sales team:



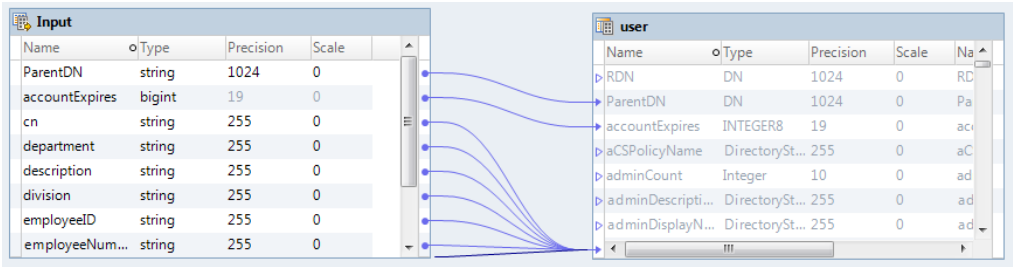
Transformations

Expression transformation. Transforms the parent DN from OU=Sales to OU=Sales&Marketing.

Mapping Output

The mapping output is an LDAP data object. To write data to the LDAP server, create a data object write operation called User_Write for the OU=Sales&Marketing.

The following image shows the target columns:



When you run the mapping, the Data Integration Service writes the sales information from the Sales OU to the Sales&Marketing OU.

CHAPTER 6

LDAP Lookup

This chapter includes the following topics:

- LDAP Lookup Overview, 30
- LDAP Lookup Properties, 30
- Adding an LDAP Data Object Operation as an LDAP Lookup in a Mapping, 32

LDAP Lookup Overview

You can use an LDAP data object read operation to look up data in an LDAP object. You add an LDAP data object read operation to a mapping as an LDAP lookup. You can look up data from LDAP in a mapping based on a lookup condition.

For example, you can look up the profile details of the user object when you add the LDAP data object read operation as a lookup in a mapping. The Data Integration Service queries the lookup source based on the properties and conditions that you specify in the LDAP lookup.

LDAP Lookup Properties

The LDAP lookup properties represent data that the Data Integration Service uses to look up records in the LDAP directory server. Select the LDAP lookup properties to edit the port properties of the LDAP lookup.

The LDAP lookup properties include general properties that apply to the data object operation. They also include port, column, run-time, lookup, query, and advanced properties that apply to the LDAP lookup. You can view and change the lookup properties of the data object read operation from the **General**, **Ports**, **Columns**, **Run-time**, **Lookup**, **Query**, and **Advanced** tab.
The runtime, query, and advanced properties display the properties that you have set for the LDAP data object read operation.

General Properties

The general properties display the name and description of the LDAP lookup.

The following table describes the general properties that you can view and edit for an LDAP lookup:

Property	Description
Name	Name of the LDAP lookup.
Description	Description of the LDAP lookup.
Physical Data Object	Name of the LDAP data object read operation.
On multiple matches	Determines which row the LDAP Lookup returns when it finds multiple rows that match the lookup condition. You can choose one of the following options: - Return first row - Return last row - Return any row - Return all rows - Report error

Ports Properties

The ports properties display the input ports from the source in the mapping to the LDAP lookup. You can specify the ports to be available as output ports from the LDAP lookup. The ports properties display the datatypes, precision, and scale of the source port.

The following table describes the ports properties:

Property	Description
Name	Name of the source port.
Type	Datatype of the source port.
Precision	Maximum number of significant digits for numeric datatypes, or maximum number of characters for string datatypes. For numeric datatypes, precision includes scale.
Scale	Maximum number of digits after the decimal point of numeric values.
Output	Specify the ports that must be available as output ports from the LDAP lookup.
Description	Description of the port.
Input Rules	A set of rules that filter the ports to include or exclude in the transformation based on port names or data type. Configure input rules when you define dynamic ports.

Lookup Properties

You can specify the properties to look up an LDAP object.

The following table describes the lookup properties that you can specify for an LDAP lookup:

Property	Description
Lookup Column	The name of the columns that you want to look up.
Operator	Operators that you can use to filter records. You can select one of the following operators: =, !=, <=, >=, and
Imput Port	The input source port.

You cannot apply the Lookup transformation for Date/Time and Binary data types.

Adding an LDAP Data Object Operation as an LDAP Lookup in a Mapping

Use an LDAP lookup to look up data in a flat file, reference table, or relational data object.

1. Open a mapping from the **Object Explorer** view.
2. From the **Object Explorer** view, drag an LDAP data object read operation to the editor.

   The **Add to Mapping** dialog box appears.
3. Select **Lookup** to add the data object read operation as a lookup in the mapping.
4. Click inside the LDAP data object operation and connect the lookup input ports and the lookup output ports.
5. In the **Properties** view, configure the following parameters:
   a. On the **General** tab, select the option that you want the Data Integration Service to return when it finds multiple rows that match the lookup condition.
   b. On the **Lookup** tab, enter the lookup condition properties.
6. When the mapping is valid, click **File** > **Save** to save the mapping to the Model repository.

CHAPTER 7

LDAP Run-Time Processing

This chapter includes the following topics:

- LDAP Run-time Processing Overview, 33
- Using the Filter Expression to Query LDAP Entries, 33
- Reading and Writing Multivalued Attributes, 35
- Specify the Search Scope, 36
- Capturing Changed Data in Active Directory, 36
- Configure Update Strategy , 38
- Parameterization, 38

LDAP Run-time Processing Overview

When you develop an LDAP mapping, you define the data object operation read or write properties. The data object read operation determines how the Data Integration Service reads data from the LDAP directory server. The data object write operation determines how the Data Integration Service writes data to the LDAP directory server.

Using the Filter Expression to Query LDAP Entries

To read data from an LDAP directory server, you can configure a filter condition to query the LDAP entries. You can use the Native or Platform expression to query specific LDAP entries.

You can apply filters to capture changed data for inserted or updated records fetched from the LDAP directory server. You cannot also apply filters to capture changed data for deleted records from the LDAP directory server. When you use the filter to capture changes for deleted records, the Data Integration Service fetches only the RDN and the parent DN records for the entry.

Native Expression

When you use the native expression, you use the standard LDAP syntax for filter expressions.

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. Default is blank.

To filter records from an LDAP source, set the native expression in the data object read operation. You can use wildcards as values.

For example, enter the following filter condition to search for all entries that have the `user` object class and `Marketing` common name attribute:

```
(&(objectClass=user)(cn=*Marketing*))
```

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 where value of a field is equal to all the specified values. For example, (&(roomNumber=2000)(roomNumber=3000))

You can also use a wildcard to extract data that contains a specified value.

You can use a wildcard entry in the following filter conditions:

- 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.

Platform Expression

You can use the platform expression to select specific records from LDAP based on the filter condition you specify.

The following table describes the properties you specify when you filter records from LDAP when you use the platform expression filter:

Property	Description
Expression Type	The type of filter expression that you want to use to filter records. Default is Platform Expression.
Left Field	The LDAP object on which you want to apply the filter condition.
Operator	Simple operators you can use to filter records. You can select one of the following operators: `=, !=, <=, >=, and`
Right Field	The value you specify to filter LDAP objects.

Note: You cannot use the platform expression for data that contains the Date/Time and Binary data types. PowerExchange for LDAP does not support pushdown optimization for data that contains the Date/Time and Binary data types.

Reading and Writing Multivalued Attributes

Multivalued attributes can have multiple values assigned to the attribute. If the data that you want to read from the LDAP directory server contains multivalued attributes, the Data Integration ServiceSecure Agent reads the multivalued attributes and converts them into XML format.

For example, a group membership list with names of everyone in the group is a multivalued attribute. If the list contains four values, test1, test2, test3, and test4, the Data Integration ServiceSecure Agent converts the attributes into the following XML format:

```
 <?xml version="1.0"
encoding="UTF-8"?><Objects><Object>test1</Object><Object>test2</Object><Object>test3</
Object><Object>test4</Object></Objects>
```

To write data with multivalued attributes to an LDAP directory server, you must provide the data in XML format. You can use B2B or Java transformation to convert multivalued attributes into XML format, or read multivalued attributes from XML format.

When you pass special characters, such as & , >, and < in a multivalued attribute, you must convert the special characters into the following equivalent HTML entities:

- & as &
- < as <
- > as >

When reading data, the Data Integration ServiceSecure Agent converts the special characters to its equivalent HTML entity when it serializes the XML.

Specify the Search Scope

You can specify the scope of a search as one-level or subtree.

Use the Search Level flag in the advanced properties of the data object read operation properties.Use the Search Level flag in the advanced properties of a Data Synchronization task, Mapping Configuration task, or mapping.

You can specify the following search scope to search for entries from the LDAP directory server:

One-level

When you specify one-level, the search is restricted to the immediate children of a base object, but excludes the base object. You can use one-level to perform a search for immediate child objects of a parent object.

For example, consider a parent object P1 and its immediate children C1, C2, and C3. When you specify one-level, the search evaluates C1, C2, and C3 against the search criteria, but does not evaluate P1. Use a one-level search to include all children of an object.

Subtree

A subtree search returns all child objects that are subordinate to the base object including the base object.

Capturing Changed Data in Active Directory

The Data Integration ServiceSecure Agent can capture changed records from an LDAP source object. Change data capture (CDC) helps you identify and process the changed data. You can configure CDC in the source advance properties to capture changes while reading data from Active Directory for a specified time interval or from the last extraction point.

Active Directory uses the uSNChanged attribute to store the entry and the details of the changes made to the entry. You can track the changes made to the contents of a directory based on the update sequence number (USN) assigned by the local server after the last change to the object.

The Data Integration ServiceSecure Agent determines the change type based on the values for uSNCreated, uSNChanged, isDeleted, whenCreated, and whenChanged attributes of an entry. Every entry in Active Directory contains the uSNCreated, uSNChanged, whenCreated, and whenChanged values. For an updated entry, the uSNChanged value increments to indicate the updated entry in the directory server. For a deleted entry, the isDeleted value sets to True to indicate the deleted entry from the directory server.

When you configure CDC, the Data Integration ServiceSecure Agent captures the changes that are present under the specified base DN and extracts the changed data. The Data Integration ServiceSecure Agent stores the change number for the last read entry in the CDC file.

Note: You can apply a filter query to capture changed data for inserted or updated records fetched from LDAP directory server. You cannot use the query to capture changes for deleted records because the Data Integration ServiceSecure Agent fetches only the RDN and the parent DN records for the deleted records.

Configuring Changed Data Capture from the Last Extraction Point

To fetch changes from the last extraction point, enable CDC and set the absolute path of the file that stores the change number for the last read changed entry.

By default, the Data Integration ServiceSecure Agent fetches the changed data based on the last read uSNChanged value:

- If the CDC file does not exist, or if the CDC file has an uSNChanged value as 0, the Data Integration ServiceSecure Agent fetches all the changes in the base DN until the latest uSNChanged value and then updates the CDC file with the latest uSNChanged value.
- If the CDC file has a uSNChanged value greater than 0, the Data Integration ServiceSecure Agent fetches the changes that occur after the uSNChanged value read from the file. The Data Integration ServiceSecure Agent then updates the CDC file with the latest uSNChanged value.

Configuring Changed Data Capture for a Specified Time Interval

To fetch changes for a specified time interval, you can set the following values in the advanced source properties:

- Specify the CDC along with the start time and end time in the advanced source properties. The Data Integration ServiceSecure Agent reads the CDC file from the uSNChanged value and fetches the changes that occur after the uSNChanged value read from the file, but according to the time interval you specify. The Data Integration ServiceSecure Agent also updates the CDC file with the latest uSNChanged value.
- When you provide only the start time, the Data Integration ServiceSecure Agent fetches the changes from the specified start time to the latest changes.
- If you provide only the end time, the Data Integration ServiceSecure Agent fetches the changes from the beginning to the specified end time.

Reset Change Data Capture

You can reset CDC to fetch the changes from the beginning. The Data Integration ServiceSecure Agent ignores the uSNChanged value in the CDC file. The Data Integration ServiceSecure Agent then updates the CDC file with the last uSNChanged value.

CDC Configuration Scenarios in Active Directory

The following scenarios describe the configurations for capturing changed data when you enable CDC:

Do not set time stamp and disable reset CDC.

The Data Integration ServiceSecure Agent captures all the changes that occurred in the parent DN until the current time and updates the CDC file with the latest uSNchanged value.

When you next capture data changes from the LDAP directory server, the Data Integration ServiceSecure Agent reads the uSNchanged value stored in the CDC file. The Data Integration ServiceSecure Agent captures all the changes from the specified uSNchanged value in the file until the current time and updates the CDC file with the latest uSNchanged value.

Do not set time stamp and enable reset CDC.

The Data Integration ServiceSecure Agent captures all the changes that occurred in the parent DN until the current time and updates the CDC file with the latest uSNchanged value.

In a subsequent capture, the Data Integration ServiceSecure Agent ignores the uSNchanged value in the CDC file. The Data Integration ServiceSecure Agent captures all the changes that occurred in the parent DN until the current time and updates the CDC file with the latest uSNchanged value.

Set time stamp and disable reset CDC.

The Data Integration ServiceSecure Agent captures all the changes that occurred during the specified CDC start time and end time. The Data Integration ServiceSecure Agent then updates the CDC file with the latest uSNchanged value.

In a subsequent run, the Data Integration ServiceSecure Agent reads the uSNchanged value in the CDC file and captures all the changes from the specified uSNchanged value in the file until the specified CDC end time. The Data Integration ServiceSecure Agent then updates the CDC file with the latest uSNchanged value.

Do not set time stamp and enable reset CDC.

The Data Integration ServiceSecure Agent captures all the changes that occurred during the time period that you specified in the CDC start and end time. The Data Integration ServiceSecure Agent then updates the CDC file with the latest uSNchanged value.

In a subsequent run, the Data Integration ServiceSecure Agent ignores the uSNchanged value in the CDC file and captures all the changes that occurred during the time period that you specified in CDC start and end time. The Data Integration ServiceSecure Agent then updates the CDC file with the latest uSNchanged value.

Configure Update Strategy

You can configure the update strategy for a target object when you want to write data to an LDAP directory server.

When you set the update strategy, the Data Integration ServiceSecure Agent updates the rows in the LDAP directory server based on the option you choose. You can define the update strategy options in the **Advanced** properties of a target data objecttarget object.

You can set one of the following update strategy options:

Update as Update

When you configure Update as Update, the Data Integration ServiceSecure Agent updates all rows flagged for update if the entries exist.

Update else Insert

When you configure Update else Insert, the Data Integration ServiceSecure Agent first updates all rows flagged for update if the entries exist in the target. If the entries do not exist, the Data Integration ServiceSecure Agent inserts the entries.

Parameterization

You can parameterize the LDAP data object operation properties to override the read and write data object operation properties during run time.

You can parameterize the following advanced properties of the data object read operation:

- Page Size
- Parent DN
- Search Level
- CDC Start Time
- CDC End Time
- CDC File Path

You can parameterize the following advanced properties of the data object write operation:

- KeyColumn
- Update Strategy

You can also parameterize the connection used in the run-time property of the read and write operation.

APPENDIX A

Data Type Reference

This appendix includes the following topics:

- Data Type Reference Overview, 40
- LDAP and Transformation Data Types, 41

Data Type Reference Overview

The Developer tool uses the following data types in PowerExchange for LDAP mappings.

LDAP native data types

LDAP native data types appear in the physical data object column properties.

Transformation data types

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

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

LDAP and Transformation Data Types

The following table lists the LDAP data types that the Data Integration ServiceSecure Agent supports and the corresponding transformation data types for Active Directory:

LDAP Data Type	Description	Transformation Data Type	Range
IA5String	A case-sensitive string. Each character belongs to the International Alphabet 5 (IA5) character set.	String	1 to 104,857,600 characters
DirectoryString	A value that consists of a string of unicode characters.	String	1 to 104,857,600 characters
PrintableString	A value that consists of a string of characters. Each character is valid and printable.	String	1 to 104,857,600 characters
Integer	A 32-bit integer value.	Integer	-2,147,483,648 to 2,147,483,647 Precision 10, scale 0
Generalized Time	A time value in string format.	Date/Time	Jan 1, 1753 AD to Dec 31, 9999 AD (precision to nanosecond) You can also set GeneralizedTime to string transformation data type. For example, you can specify the string format as 20150323060844.0Z. You can also set GeneralizedTime to string transformation data type. For example, you can specify the string format as 20150323060844.0Z.
UTCTime	A time value in string format defined by ASN.1 standards. For more information, see standards ISO 8601 and X.680. UTC, or Coordinated Universal Time, is roughly the same as GMT, or Greenwich Mean Time. The UTCTime syntax uses only two characters to represent the year.	Date/Time	Jan 1, 1753 AD to Dec 31, 9999 AD (precision to nanosecond)
Boolean	A true or false value.	String	1 to 104,857,600 characters

LDAP Data Type	Description	Transformation Data Type	Range
OctetString	Binary data.	Binary	1 to 104,857,600 bytes If the binary data type is a multivalued attribute, the Secure Agent reads or writes only the first value. If the binary data type is a multivalued attribute, the Data Integration Service reads or writes only the first value.
Integer8	A 64-bit integer value.	BigInt	-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 Precision 19, scale 0

Note: The data type of an LDAP attribute is set to text if its data type is not included in the LDAP data types. You can edit the LDAP source or target definitions to set the corresponding data types. The data type of an LDAP attribute is set to text if its data type is not included in the LDAP Connector data types. You can edit the precision of the LDAP source or target attributes but not the data types.

INDEX

A

advanced properties
  input 23

C

column properties 18
configuring
  TLS authentication 10
creating
  LDAP connection 14
  LDAP data object read operation 27

D

data object read operation
  creating 27
datatype reference overview 40
directory server
  LDAP directory server 8

G

general properties
  input 23

I

importing
  LDAP data object 25
input properties 22
Installation
  adding certificates to the keystore 11

L

LDAP
  importing a data object 25
  mapping example 28
  mapping input 28
  mapping overview 28
LDAP connection
  creating 14
LDAP connection *(continued)*
  overview 13
  properties 13
LDAP data object read operation
  creating 27
  properties 17
LDAP data types
  data types 41
LDAP lookup
  creating 32
  general properties 31
  lookup properties 32
  overview 30
  ports properties 31
  properties 30

M

mapping output 28
multivalued attribute
  XML format 35

P

properties
  LDAP data object 17
  LDAP data object read operation 17

Q

query
  native expression 33
  platform expression 33, 35

R

run-time processing
  overview 33

S

source properties 17