Informatica® Cloud Data Integration

LDAP Connector

Informatica Cloud Data Integration LDAP Connector
November 2023

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

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: 2023-11-19

Table of Contents

Preface

Use *LDAP Connector* to learn how to read from or write to the LDAP directory server by using Cloud Data Integration. Learn to create a connection, develop and run synchronization tasks, mappings, and mapping tasks in Cloud Data Integration.

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 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 Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

Use the Informatica Intelligent Cloud Services Community to discuss and resolve technical issues. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Intelligent Cloud Services Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Intelligent Cloud Services Marketplace

Visit the Informatica Marketplace to try and buy Data Integration Connectors, templates, and mapplets:

https://marketplace.informatica.com/

Data Integration connector documentation

You can access documentation for Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit https://docs.informatica.com.

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 Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at https://www.informatica.com/trust-center.html.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The Informatica Intelligent Cloud Services Status page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, on the Informatica Intelligent Cloud Services Status page, click **SUBSCRIBE TO UPDATES**. You can choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

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

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

Introduction to LDAP Connector

You can use LDAP Connector to connect to a Microsoft Active Directory server from Data Integration. You can read and integrate data from LDAP directory servers or other applications, transform the data, and write data to LDAP directory servers or other applications.

Use LDAP Connector to connect to an LDAP directory server, browse metadata, and import source and target objects into Data Integration. You can use LDAP data objects in synchronization tasks, mapping tasks, or mappings.

The LDAP data objects represent metadata for LDAP entries. The Secure Agent uses the JNDI APIs to connect to the LDAP directory server and read and write data based on the operation you specify.

You can switch mappings to advanced mode to include transformations and functions that enable advanced functionality.

Example

You work in the Human Resources department and you manage employee information. Your organization 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. Use LDAP Connector to synchronize the list of employees, aliases, roles provisioned to users, profile information, contacts, and calendar resources to Active Directory.

LDAP Connector assets

Create assets in Data Integration to integrate data using LDAP Connector.

When you use LDAP Connector, you can include the following Data Integration assets:

- Mapping
- Mapping task
- Synchronization task

For more information about configuring assets and transformations, see *Mappings*, *Transformations*, and *Tasks* in the Data Integration documentation.

Introduction to 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.

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 entires in the LDAP directory. LDAP carries the messages over TCP/IP.

An LDAP directory server is a specialized database that stores typed and ordered information about objects. A directory contains 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.

Each entry in an LDAP directory tree consists of a set of attributes that define that entry. Each attribute has a name and contains one or more values. The attributes are defined in a schema. Every directory entry has an objectClass attribute that lists the schema describing 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
```

You can use the directories to find resources with the characteristics required for a particular task. LDAP searches the directory for data to satisfy the specified criteria. You need to 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 specified condition.

For example, a directory can list information about printers that consists of typed information, such as location, speed in pages for each minute, and supported print streams. You can access the data based on the privileges set for the LDAP directory server or the user. You can also add new entries, update existing entries, and remove entries.

Administration of LDAP Connector

As a user, you can use LDAP Connector after the organization administrator performs the following tasks:

- Install LDAP Connector.
- Optional. Configure TLS authentication to establish a one-way or two-way secure connection with the LDAP directory server.

Configuring TLS authentication

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

The Secure Agent establishes a secure connection with the LDAP directory server over TLS. You can use one-way SSL or two-way SSL.

Use One-Way SSL

To use one-way SSL, you must perform any one of the following steps:

- Copy the server certificate to the following directory: `<Secure Agent installation directory>\jdk\jre\lib\security\cacerts`. Then, restart the Secure Agent.

- Navigate to the `<Secure Agent installation directory>\apps\Data_Integration_Server\ext` directory and perform the following steps:

1. Create the following directory structures:
   - `deploy_to_main\bin\rdtm`
   - `deploy_to_main\tomcat`
2. Copy the truststore file that contains the server certificate to the following directories:
   - `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat`
   - `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm`
3. Specify the name of the truststore file and password in the connection properties.
4. Restart the Secure Agent.

Use Two-Way SSL

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

1. Copy the keystore file to the following directories:
   - `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat`
   - `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm`

2. Specify the name of the keystore file and password in the connection properties.
3. Restart the Secure Agent.

The Secure Agent checks for the certificate in the keystore of the tomcat directory and then in the Java cacerts file. If you do not specify a value of the truststore file in the connection properties, the Secure Agent searches the certificate in the Java cacerts file.

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

CHAPTER 2

LDAP connections

Create an LDAP connection to connect to LDAP directory server. The Secure Agent reads data from and writes data to LDAP directory server. You can specify the LDAP source and target in synchronization tasks, mapping tasks, or mappings.

You create an LDAP connection on the **Connections** page. Use the connection when you create a synchronization task, mapping task, or a mapping.

You can also configure LDAP over SSL.

LDAP connection properties

When you set up an LDAP connection, you must configure the connection properties.

The following table describes the LDAP connection properties:

Property	Description
Runtime Environment	The name of the run-time environment where you want to run the tasks. **Note:** You can specify only the Secure Agent as the run-time environment for an LDAP connection.
Host Name	Required. LDAP directory server host name. You can use the LDAP or LDAPS protocol to connect to LDAP Server. - To use the LDAP protocol, use one of the following formats: - `ldap://<hostname>` - `<hostname>` - To use the LDAPS protocol, use the `ldaps://<hostname>` format. **Note:** If you use SSL, use the host name that you specify in the SSL certificate.
Port	Required. 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. Required if you want to connect to Active Directory.

Property	Description
Password	The password to connect to the LDAP directory server. If you do not enter the password, the Client establishes an anonymous connection. Required if you want to connect to Active Directory.
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 one-way secure connection with the LDAP directory server. 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 two-way secure communication with the LDAP directory server. Contact the LDAP Administrator for the keystore file name and password.
KeyStore Password	The password for the keystore file required for secure communication.
Base DN	Required. The distinguished name (DN) of the root directory in the LDAP directory server. For example, use the following base DN to connect to the Informatica domain: `dc=informatica-connector,dc=com` If you do not specify the base DN, the Secure Agent fails to fetch the metadata.

CHAPTER 3

LDAP objects

You can use an LDAP object as a source or target in a synchronization task, mapping task, or a mapping.

When you configure the advanced source properties or advanced target properties , configure properties specific to LDAP.

LDAP sources

You can use an LDAP single object as a source in a synchronization task, mapping task, or a mapping.

When you configure the advanced source properties, you configure properties specific to LDAP. You can filter data, capture change data on LDAP directory server, and query LDAP entries.

Use the object class or the distinguished name to fetch metadata

When you create an LDAP data object, you can specify the object class or the distinguished name (DN) to import metadata from an LDAP directory server. The Secure Agent searches object classes from the specified location in the LDAP directory and imports the metadata.

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 filter field and fetch the attributes for that object class. The object class inherits all the attributes of the superclasses.

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.

You can also use the DN 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 available 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.

Using the filter expression to query LDAP entries

You can configure a filter condition in a synchronization task, mapping task, or a mapping to query the LDAP entries from an LDAP directory server. You can create basic or advanced data filters for the LDAP source types.

When you create a basic filter, specify the object on which to create the data filter, and then enter the filter condition based on the field, operator, and field value.

When you create an advanced filter, use the LDAP query format to enter the filter expression. For example, specify the expression *(&(!(maxStorage=0))(maxStorage=*))* to fetch all user entires with maximum storage value and with the condition that the value must not be equal to 0.

LDAP Connector supports the following operators:

- Equals
- Not Equals
- Less Than or Equals
- Greater Than or Equals
- AND
- OR

Note: You cannot configure the OR operator using basic filter.

Specify the search scope

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

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 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 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 captures the changes that are present under the specified base DN and extracts the changed data. The 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 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 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 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 fetches the changes that occur after the uSNChanged value read from the file. The 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 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 also updates the CDC file with the latest uSNChanged value.
- When you provide only the start time, the fetches the changes from the specified start time to the latest changes.
- If you provide only the end time, the 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 ignores the uSNChanged value in the CDC file. The 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 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 reads the uSNchanged value stored in the CDC file. The 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 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 ignores the uSNchanged value in the CDC file. The 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 captures all the changes that occurred during the specified CDC start time and end time. The then updates the CDC file with the latest uSNchanged value.

In a subsequent run, the 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 then updates the CDC file with the latest uSNchanged value.

Do not set time stamp and enable reset CDC.

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

In a subsequent run, the 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 then updates the CDC file with the latest uSNchanged value.

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 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 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.

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 &amp;
- < as &lt;
- > as &gt;

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

LDAP targets

You can use an LDAP object as a target in a synchronization task, mapping task, or mapping.

You can insert, update, and delete data from LDAP targets. When you configure the advanced target properties, you configure properties specific to LDAP.

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 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 .

You can set one of the following update strategy options:

Update as Update

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

Update else Insert

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

Rules and guidelines for LDAP objects

Consider the following rules and guidelines for LDAP sources and targets:

- You cannot use multiple lookup condition when you configure a synchronization task.
- The session log shows incorrect row statistics when you perform a delete operation and the Base DN in the connection properties contains special characters, even though it successfully performs delete operation.
- You cannot use filters for data that contains the Binary data type.
- You can use only the advanced filter for Generalized Time and UTCTime data types.
- You cannot use Less Than, Greater Than, Starts With, Ends With, Contains, Is Null, and Is Not Null operators in a basic filter.
- Ensure that the advanced filter expression has a valid LDAP syntax.
- The **Base DN** does not appear as a mandatory field in the LDAP connection. If you do not specify the base DN, the Secure Agent fails to fetch the metadata.
- You cannot preview data for both an LDAP source and target. The **Show Data Preview** icon that appears on the **Target** tab of a data synchronization task is not applicable.
- For large binary data that is equal to or more than 10 MB, the Secure Agent fails to apply the update strategies on the LDAP target.
- You cannot use LDAP Connector to 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 using the JNDI APIs.
- When you use a basic filter for an LDAP source, you must map the fields on which you applied the filter before you run the task.
- The Secure Agent fetches the attributes of security principal object classes only for the User, Group, and Computer object class from Active Directory.
- When you write data that contains reserved characters to a distinguished name, you must add a backslash before each occurrence of a reserved character. The reserved characters include space or # character at the beginning of a string and space character at the end of a string. Other characters include , `+ " \ < > ; LF CR = /`

- When you read data from Active Directory, you can view extension attributes for all object classes if the Active Directory schema supports it. Extension attributes are custom attributes that you can use to store custom values for object classes that do not have an existing attribute. The extension attributes are certified for the user, contact, group, and computer object classes.
- You cannot use SQL ELT optimization for an LDAP source.
- You cannot configure the proxy servers and communicates with the LDAP server directly.

CHAPTER 4

Synchronization tasks with LDAP Connector

Use a Synchronization task to synchronize data between a source and target.

You can configure a synchronization task using the Synchronization Task wizard. You can use LDAP objects as source, target, or lookup objects.

When you create a task, you can associate it with a schedule to run it at specified times or on regular intervals. Or, you can run it manually. You can monitor tasks that are currently running in the activity monitor and view logs about completed tasks in the activity log.

LDAP sources in synchronization tasks

When you configure a synchronization task to use an LDAP source, you can configure the source properties.

The source properties appear on the **Source** page of the Synchronization Task wizard when you specify an LDAP connection.

The following table describes the LDAP source properties:

Source Property	Description
Connection	Name of the source connection.
Source Type	Type of the source object. Select Single as the source type.
Source Object	Name of the source object. Select the source object for the task.

LDAP source properties in synchronization tasks

You can configure the advanced source properties on the **Schedule** page of the Synchronization Task wizard.

The following table describes the LDAP advanced source properties:

Property	Description
Page Size	Size of the page set to retrieve the maximum number of entries for each request. 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 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.
CDC Start Time	The start time from when you want the to capture the changed data. If you select CDC and specify a start time, but do not specify an end time, the captures the changed data until the last change. Use the following sample format to specify the start time: *20150312081001.0Z*

Property	Description
CDC End Time	The end time until when you want the to capture the changed data. When you specify only the end time, the 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 captures the changes made to the LDAP directory server from the beginning.

LDAP source synchronization task example

You work for the IT department and you have an LDAP directory server to store data of assets allotted to employees. You want to track the availability and utilization of virtual machines across employees in the organization.

You want to generate an analytic report in Tableau Server. Based on the report, you want to take decisions to allocate unused hardware effectively.

You perform the following synchronization tasks:

Define the synchronization task.

Configure a synchronization task to use the insert operation.

Use an LDAP source object.

The source object for a synchronization task is an LDAP *computer* class object that contains the asset details. Use the LDAP connection to connect to the LDAP directory server and read data. The LDAP object is a single source in the synchronization task.

The following table describes the fields for the computer source object that you can include:

Field	Description
name	The name of the asset.
description	Description of the asset.
managedBy	Name of the employee who owns the asset.
memberOf	Team or group that the employee belongs to.

Create a Tableau target.

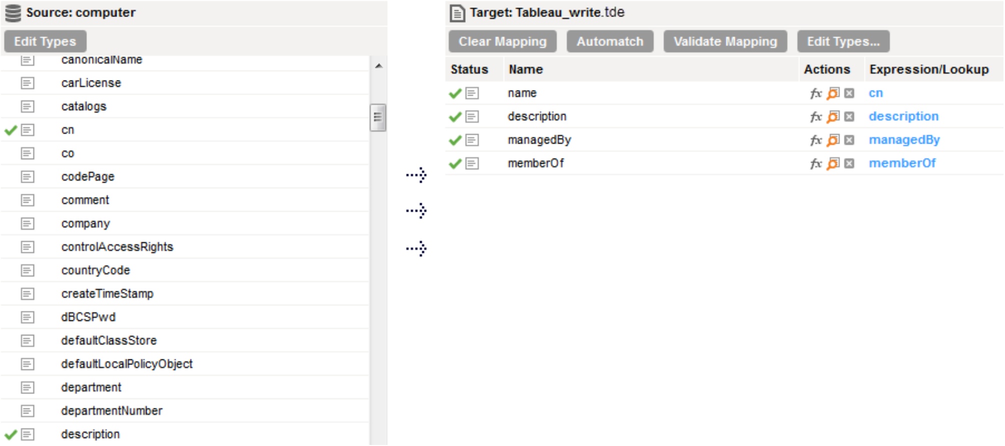
The target in a synchronization task is Tableau Server. Use the Tableau connection to connect to Tableau Server. Use the *target_write.tde* as the target object in the synchronization task.

Include the *name*, *description*, *mangedBy*, and *memberOf* target fields from the source object that you want to insert into the target object.

Configure a field mapping.

Map the fields of the LDAP computer source object to the Tableau target object.

The following image shows the mapping of the computer source with the Tableau target:



Source: computer

Edit Types

- canonicalName
- carLicense
- catalogs
- ✓ cn
- co
- codePage
- comment
- company
- controlAccessRights
- countryCode
- createTimeStamp
- dBCSPwd
- defaultClassStore
- defaultLocalPolicyObject
- department
- departmentNumber
- ✓ description

Target: Tableau_write.tde

Clear Mapping | Automatch | Validate Mapping | Edit Types...

Status	Name	Actions	Expression/Lookup
✓	name		cn
✓	description		description
✓	managedBy		managedBy
✓	memberOf		memberOf

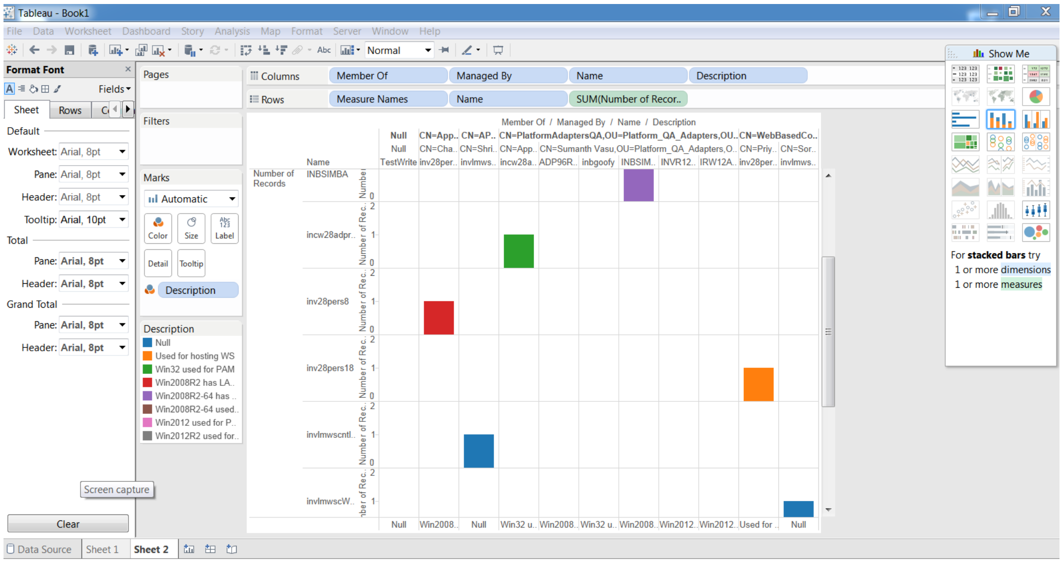
Configure the advanced source and target properties.

In the advanced source properties, you choose properties that are specific to LDAP. Specify *OU=Platform_QA_Adapters,OU=R&D,OU=INFA,DC=ADPQATEST,DC=COM* as the parent DN in the LDAP directory server namespace from where you want to fetch the data.

In the advanced target properties, you choose properties that are specific to Tableau Server. Save and run the task. The Secure Agent retrieves the computer data from LDAP directory server and writes to Tableau Server based on the fields you mapped in the synchronization task.

Open the project in Tableau Server to visualize the exported data.

The following image shows the data categorized by asset availability in Tableau Server:



IT managers can use the information to visualize and query the computer assets to make decisions.

LDAP targets in synchronization tasks

When you configure a synchronization task to write to an LDAP target, you can configure the target properties.

The target properties appear on the Target page of the Synchronization Task wizard when you specify an LDAP connection. You can only insert, update, or delete data in an LDAP target.

The following table describes the LDAP target properties:

Target Property	Description
Connection	Name of the target connection.
Target Object	The target object for the task. Select the target object.

LDAP target properties in synchronization tasks

Configure the advanced target properties on the **Schedule** page of the Synchronization Task wizard. The following table describes the LDAP advanced target properties:

Advanced Target Property	Description
ReplaceAll	Replaces the existing values in LDAP server when you use the update operation to write data. To delete multivalued attributes, you must enable this option and pass a null value.
Update Strategy	Updates the rows in the LDAP 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 then inserts any remaining rows marked for insert. Default is Update as Update.
KeyColumn	Required with the parent DN to write data to LDAP server. Select the key column for the entry you want to create. For example, the key column for a user is cn. **Note:** You cannot update a key column because LDAP Connector does not allow updating the relative distinguished name (RDN) of the entry.
Success File Directory	Not applicable.
Error File Directory	Not applicable.

LDAP target synchronization task example

You work in the Human Resources department and you manage employee information. Your organization had a recent acquisition and you want to synchronize the employee information from the third-party LDAP directory service to the Microsoft Active Directory of your organization.

Configure a synchronization task to synchronize employee information to Active Directory.

You perform the following synchronization tasks:

Define the synchronization task.

Configure a synchronization task to use the insert operation.

Create an LDAP source object.

The source for the mapping is an LDAP user object that contains the user details. The user object is a single source in the synchronization task. You can include the *ParentDN*, *cn*, *co*, *manager*, *postalAddress*, and *telephoneNumber* source columns. Specify *user* as the resource for the source object. Specify the connection as LDAP.

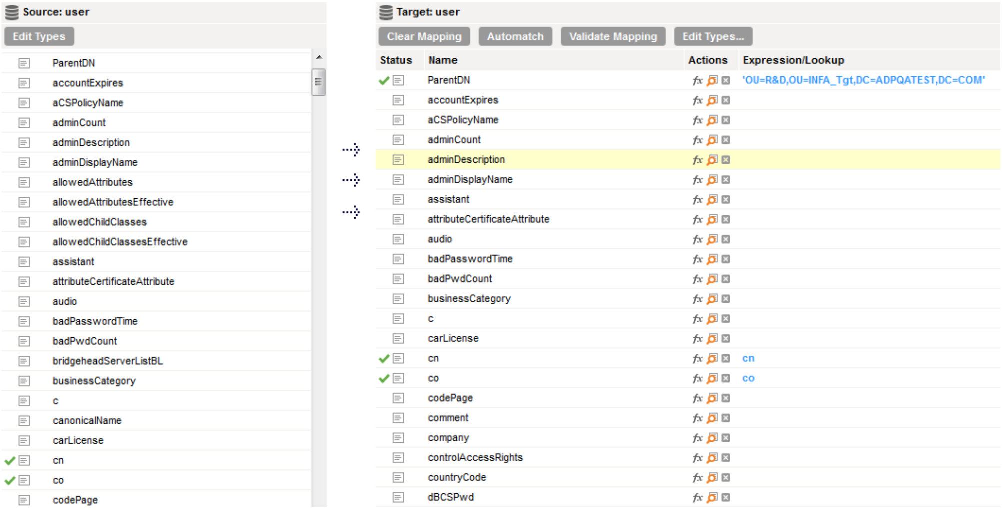
Create an LDAP target object.

The target for the mapping is the Active Directory target. Include the *ParentDN*, *cn*, *co*, *manager*, *postalAddress*, and *telephoneNumber* in the LDAP target object. Specify user as the target object and specify the connection type as LDAP.

Configure a field mapping.

Map all the fields under the *user* source fields to the target *user* fields. When you run the task, the Secure Agent writes the mapped source data to the target LDAP server.

The following image shows the mapping of the source with the target that you specified in the connection properties:



	Source: user
	ParentDN
	accountExpires
	aCSPolicyName
	adminCount
	adminDescription
	adminDisplayName
	allowedAttributes
	allowedAttributesEffective
	allowedChildClasses
	allowedChildClassesEffective
	assistant
	attributeCertificateAttribute
	audio
	badPasswordTime
	badPwdCount
	bridgeheadServerListBL
	businessCategory
	c
	canonicalName
	carLicense
✓	cn
✓	co
	codePage

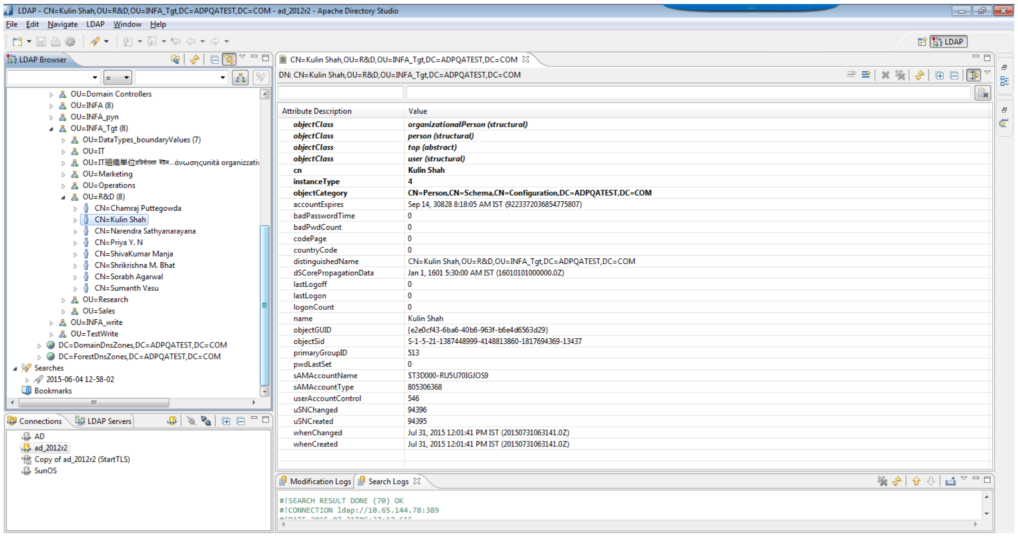
Status	Name	Actions	Expression/Lookup
✓	ParentDN	fx	'OU=R&D,OU=INFA_Tgt,DC=ADPQATEST,DC=COM'
	accountExpires	fx	
	aCSPolicyName	fx	
	adminCount	fx	
	adminDescription	fx	
	adminDisplayName	fx	
	assistant	fx	
	attributeCertificateAttribute	fx	
	audio	fx	
	badPasswordTime	fx	
	badPwdCount	fx	
	businessCategory	fx	
	c	fx	
	carLicense	fx	
✓	cn	fx	cn
✓	co	fx	co
	codePage	fx	
	comment	fx	
	company	fx	
	controlAccessRights	fx	
	countryCode	fx	
	dBCSPwd	fx	

Configure the advanced source and target properties.

In the advanced source properties, specify the parent DN as *OU=Platform_QA_Adapters,OU=R&D,OU=INFA,DC=ADPQATEST,DC=COM* where you want to read the user entries form the third-party LDAP application. In the advanced target properties, specify the key column as *cn* for the user entry you want to create in Active Directory. Save and run the task.

Open Active Directory server to visualize the exported data.

The following image shows the data in Active Directory:



LDAP - CN=Kulin Shah,OU=R&D,OU=INFA_Tgt,DC=ADPQATEST,DC=COM - ad_2012r2 - Apache Directory Studio

```
OU=Domain Controllers
OU=INFA (8)
OU=INFA_pyn
OU=INFA_Tgt (8)
  OU=DataTypes_boundaryValues (7)
  OU=IT
  OU=IT組織単位 ...άνωσηςunità organizzativ
  OU=Marketing
  OU=Operations
  OU=R&D (8)
    CN=Chamraj Puttegowda
    CN=Kulin Shah
    CN=Narendra Sathyanarayana
    CN=Priya Y. N
    CN=ShivaKumar Manja
    CN=Shrikrishna M. Bhat
    CN=Sorabh Agarwal
    CN=Sumanth Vasu
  OU=Research
  OU=Sales
OU=INFA_write
OU=TestWrite
DC=DomainDnsZones,DC=ADPQATEST,DC=COM
DC=ForestDnsZones,DC=ADPQATEST,DC=COM
Searches
  2015-06-04 12-58-02
Bookmarks
```

```
AD
ad_2012r2
Copy of ad_2012r2 (StartTLS)
SunOS
```

CN=Kulin Shah,OU=R&D,OU=INFA_Tgt,DC=ADPQATEST,DC=COM

DN: CN=Kulin Shah,OU=R&D,OU=INFA_Tgt,DC=ADPQATEST,DC=COM

Attribute Description	Value
objectClass	***organizationalPerson (structural)***
objectClass	***person (structural)***
objectClass	***top (abstract)***
objectClass	***user (structural)***
cn	**Kulin Shah**
instanceType	**4**
objectCategory	**CN=Person,CN=Schema,CN=Configuration,DC=ADPQATEST,DC=COM**
accountExpires	Sep 14, 30828 8:18:05 AM IST (9223372036854775807)
badPasswordTime	0
badPwdCount	0
codePage	0
countryCode	0
distinguishedName	CN=Kulin Shah,OU=R&D,OU=INFA_Tgt,DC=ADPQATEST,DC=COM
dSCorePropagationData	Jan 1, 1601 5:30:00 AM IST (16010101000000.0Z)
lastLogoff	0
lastLogon	0
logonCount	0
name	Kulin Shah
objectGUID	{e2e0cf43-6ba6-40b6-963f-b6e4d6563d29}
objectSid	S-1-5-21-1387448999-4148813860-1817694369-13437
primaryGroupID	513
pwdLastSet	0
sAMAccountName	$T3D000-RU5U70IGJOS9
sAMAccountType	805306368
userAccountControl	546
uSNChanged	94396
uSNCreated	94395
whenChanged	Jul 31, 2015 12:01:41 PM IST (20150731063141.0Z)
whenCreated	Jul 31, 2015 12:01:41 PM IST (20150731063141.0Z)

```
#!SEARCH RESULT DONE (70) OK
#!CONNECTION ldap://10.65.144.78:389
```

LDAP lookups in synchronization tasks

When you configure field mappings in a synchronization task, you can create a lookup to an LDAP object.

When you use an LDAP object as a lookup, you must specify the parent DN.

CHAPTER 5

Mappings with LDAP Connector

Use the Data Integration Mapping Designer to create a mapping. When you create a mapping, you configure a source or target to represent an LDAP object.

In advanced mode, the Mapping Designer updates the mapping canvas to include transformations and functions that enable advanced functionality.

Describe the flow of data from source and target along with the required transformations before the agent writes data to the target. When you create a mapping task, select the mapping that you want to use. Use the Mapping Task wizard to create a mapping task. Validate and run the mapping to read data from sources and write to a target. The mapping task processes data based on the data flow logic you define in the mapping.

LDAP objects in mappings

When you create a mapping, you can configure a Source or Target transformation to represent an LDAP object.

After you configure a mapping, deploy the mapping in a mapping task. If you parameterize the connection, object, or query in a mapping, you must specify the parameterized values when you create the mapping task.

LDAP sources in mappings

To read data from LDAP directory server, configure an LDAP object as the Source transformation in a mapping. You can configure a Source transformation to represent a single LDAP source.

Specify the name and description of the LDAP source. Configure the source and advanced properties for the source object.

The following table describes the LDAP source properties that you can configure in a Source transformation:

Source Property	Description
Connection	Name of the source connection or create a connection parameter.
Source Type	Type of source object. Select Single or Parameter as the source type.

Source Property	Description
Object	Name of the source object. Select the source object for the task.
Parameter	The parameter for the source object. Create or select the parameter for the source object. **Note:** The parameter property appears only if you select parameter as the source type.

The following table describes the LDAP query properties that you can configure in a Source transformation:

Source Property	Description
Query Options	Filter value in a read operation. Click **Configure** to add conditions to filter records and reduce the number of rows that the Secure Agent reads from the source. You can specify the following filter conditions: - Not parameterized. Use a basic filter to specify the object, field, operator, and value to select specific records. - Completely parameterized. Use a parameter to specify the filter query. - Advanced. Use an advanced filter to define a more complex filter condition that uses the LDAP query format.

The following table describes the LDAP source advanced properties that you can configure in a Source transformation:

Property	Description
Page Size	Size of the page set to retrieve the maximum number of entries for each request. 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.

Property	Description
Use Object Category Filter	Fetches entries based on the object category value. When disabled, the 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.
CDC Start Time	The start time from when you want the to capture the changed data. If you select CDC and specify a start time, but do not specify an end time, the 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 to capture the changed data. When you specify only the end time, the 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 captures the changes made to the LDAP directory server from the beginning.

LDAP targets in mappings

In a mapping, you can configure a Target transformation to represent a single LDAP target. You can also create an LDAP target at run-time based on the input fields.

When you use an LDAP target object, select an LDAP object as the target.

The following table describes the LDAP target properties that you can configure in a Target transformation:

Target Property	Description
Connection	Name of the target connection or create a connection parameter.
Target Type	Type of target object. Select Single Object or Parameter.
Object	The target object for the task. Select the target object.

Target Property	Description
Parameter	The parameter for the target object. Create or select the parameter for the target object. **Note:** The parameter property appears only if you select parameter as the target type.
Operation	The target operation. Select the target operation. You can only insert, update, or delete data in an LDAP target.

The following table describes the LDAP target advanced properties that you can configure in a Target transformation:

Advanced Target Property	Description
ReplaceAll	Replaces the existing values in LDAP server when you use the update operation to write data. To delete multivalued attributes, you must enable this option and pass a null value.
Update Strategy	Updates the rows in the LDAP 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 then inserts any remaining rows marked for insert. Default is Update as Update.
KeyColumn	Required with the parent DN to write data to LDAP server. Select the key column for the entry you want to create. For example, the key column for a user is cn. **Note:** You cannot update a key column because LDAP Connector does not allow updating the relative distinguished name (RDN) of the entry.
Success File Directory	Not applicable.
Error File Directory	Not applicable.

LDAP lookups in mappings

When you configure field mappings in a mapping, you can create a lookup to an LDAP object.

When you use an LDAP object as a lookup, you must specify the parent DN.

CHAPTER 6

Rules and guidelines for LDAP

When you run a task to read data from LDAP and exceptions occur from Active Directory, the Secure Agent does not display an error. To view the **SizeLimitException** and the **TimeLimitException**errors in Cloud Data Integration, set the DLDAP_CATCH_LIMIT_EXCEPTION=true custom flag.

To set the flag, perform the following tasks:

- Log in to Informatica Intelligent Cloud Services.
- Open Administrator and select **Runtime Environments**.
- Select the Secure Agent for which you want to configure the flag and on the upper-right corner of the page, click **Edit**.
- In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Service.
- Select the **Name** as JVMOption<N>, where N is an unused number and select the **Value** as DLDAP_CATCH_LIMIT_EXCEPTION=true.

APPENDIX A

Data type reference

Data Integration uses the following data types in synchronization tasks, mapping tasks, or mappings with LDAP:

LDAP Native Data Types

LDAP data types appear in the Source and Target transformations when you choose to edit metadata for the fields.

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 run-time environment uses to move data across platforms. Transformation data types appear in all transformations in synchronization tasks, mapping tasks, or mappings.

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

LDAP Data Type	Description	Transformation Data Type	Range
Generalized Time	A time value in string format.	Date/Time	Jan 1, 1753 AD to Dec 31, 9999 AD (precision to nanosecond)
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
OctetString	Binary data.	Binary	1 to 104,857,600 bytes
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:

Rules and guidelines for LDAP data types

You cannot pass IA5String, DirectoryString, and PrintableString data types that exceed 9MB because of a restriction from the JNDI API.

INDEX