SAP NetWeaver® Identity Management
Virtual Directory Server

Tutorial
- Accessing LDAP servers
Preface

The product

The SAP NetWeaver Identity Management Virtual Directory Server can logically represent information from a number of disparate directories, databases, and other data repositories in a virtual directory tree. Different users and applications can, based on their access rights, get different views of the information.

Features like namespace conversion and schema adaptations provide a flexible solution that can continually grow and change to support demands from current and future applications, as well as requirements for security and privacy, without changing the underlying architecture and design of data stores like databases and directories.

The reader

This manual is written for people who are to access LDAP servers with the Virtual Directory Server.

Prerequisites

To get the most benefit from this tutorial, you should have the following knowledge:

- Basic knowledge of LDAP.
- Basic knowledge of Java.

The following software is required:

- SAP NetWeaver Identity Management Virtual Directory Server version 7.0 or newer, correctly installed and licensed.
- A Java development environment. This can be downloaded from http://java.sun.com (version 1.5).
- The source file for this tutorial:
  - The mvd-ldap.xml configuration file with a minimum configuration for the Virtual Directory Server, including the Java classes necessary to access the LDAP directory.
  - The directory server for the tutorials that is installed with the product.

The manual

This document contains a tutorial for accessing LDAP directory servers with the Virtual Directory Server. You will also see how you can modify an attribute using a Java class and how you can implement access control in the virtual tree.
Related documents

You can find useful information in the following documents:

- The X.500 standard, which can be ordered from [http://www.itu.int](http://www.itu.int).
- LDAP v. 3, RFC 2251, "Lightweight Directory Access Protocol (V3)".

RFCs and Internet drafts can be downloaded from [http://www.ietf.org](http://www.ietf.org).
Table of contents

Introduction........................................................................................................................................ 1
   Verifying the configuration of the Virtual Directory Server..........................................................1
   Section overview ............................................................................................................................2
Section 1: Opening the server configuration ...................................................................................3
   Starting the directory server ............................................................................................................3
   Opening the server configuration ....................................................................................................3
   Configuring the data source .............................................................................................................5
   Configuring the virtual tree ............................................................................................................6
   Specifying the port number ...........................................................................................................8
   Enabling the operation log ............................................................................................................9
   Running the server .......................................................................................................................10
   Testing the configuration ..............................................................................................................11
Section 2: Adding a directory server .............................................................................................12
Section 3: Modifying the virtual tree ............................................................................................ 17
   Creating the static nodes ...............................................................................................................17
   Creating the data source node .......................................................................................................19
   Moving the existing node .............................................................................................................20
   Moving the access rights .............................................................................................................21
   Running the server .......................................................................................................................22
Section 4: Differentiating access rights ..........................................................................................23
   Adding the user group ....................................................................................................................23
   Adding the user profile ..................................................................................................................24
   Creating the rule ............................................................................................................................25
   Implementing the access rights in the virtual tree ........................................................................26
   Adding LDAP attributes to the static node ..................................................................................27
   Running the server .......................................................................................................................28
Section 5: Altering an attribute using a Java method .....................................................................29
   Creating the class ..........................................................................................................................29
   Adding the method .......................................................................................................................30
   Calling the method .......................................................................................................................32
   Running the server .......................................................................................................................32
Introduction

The purpose of this tutorial is to describe the common tasks involved in configuring the Virtual Directory Server to access directory servers. You will also see how you can implement access control and modify attributes using a Java class.

The tutorial and the necessary files are installed in a sub-directory below the product installation directory. For a default installation, the tutorial will be located in C:\Program Files\SAP\IdM\Virtual Directory Server\Tutorials.

The tutorial includes the following files:

- The configuration file mvd-ldap.xml. Copy this file to a directory where you can access it from the Virtual Directory Server before you start working with the configuration so that you can repeat this tutorial if you wish to do so.
- Additionally you need to start the directory server that you will access in this tutorial. This is described in the first section of this tutorial.

Verifying the configuration of the Virtual Directory Server

When you installed the Virtual Directory Server, you specified the location of the Java runtime environment. This tutorial includes modifying and compiling a Java class. To be able to do this, a Java compiler is required. If necessary, you can download a compiler from http://java.sun.com (version 1.5).

The configuration may look like this when choosing Tools/Options…:

![Options dialog box](image)

Verify that "Enable compilation" is selected and that you have selected a Java compiler.
# Section overview

The tutorial consists of the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1: Opening the server configuration</strong></td>
<td>In this section you open the server configuration and perform some initial configuration.</td>
</tr>
<tr>
<td><strong>Section 2: Adding a directory server</strong></td>
<td>This section describes how you add a second directory server to the configuration.</td>
</tr>
<tr>
<td><strong>Section 3: Modifying the virtual tree</strong></td>
<td>The section explains how you include the new LDAP server in the virtual tree.</td>
</tr>
<tr>
<td><strong>Section 4: Differentiating access rights</strong></td>
<td>In this section you apply a more detailed access control to the virtual tree to make it possible to distinguish between anonymous clients and clients logging on with user name and password.</td>
</tr>
<tr>
<td><strong>Section 5: Altering an attribute using a Java method</strong></td>
<td>The last section describes how you can use a simple Java method to modify an attribute value before it is returned to the client.</td>
</tr>
</tbody>
</table>
Section 1: Opening the server configuration

In this section, you will start the directory server that we are going to access in this tutorial. We will also open the configuration file accompanying this tutorial for some initial configuration that is necessary to make this configuration work.

Starting the directory server

You will access a directory server that is part of the installation.

To start the database server:

- Choose Programs/SAP NetWeaver Identity Management/Virtual Directory Server/Start tutorial prerequisites from the Start menu.

A status window is displayed where you verify that the server started successfully. The port number to use is 7389 to avoid conflicts with any other LDAP servers on the system.

Opening the server configuration

To open the configuration file:

2. Choose File/Open file…. The "Open server configuration" dialog box is displayed:

Select the configuration file mvd-ldap.xml that accompanies this tutorial.
3. Expand the tree by choosing "Collapse/Expand" in the toolbar. The expanded configuration tree looks like this:

![Expanded Configuration Tree]

**Note:**

The appearance of the user interface depends on what you have chosen in View/Look & Feel. This screen shot shows the "MaXware" Look & Feel.
Configuring the data source

To configure the data source:

1. Select the data source "My LDAP server" and choose "Properties..." from the context menu. Select the "LDAP" tab:

2. Modify the value of the "Server" field to match the directory server you are using. Enter the starting point in the directory server. You may also need to modify the login credentials or remove them to use anonymous login. Just keep the default values for the method parameters. If you are accessing the tutorial directory, the values will be: Server: localhost, Port: 7389, Starting point: o=maxware,c=no, LDAP authentication: Anonymous

3. Choose "Test connection" to verify that you can access the directory server.

4. Choose "OK" to close the "LDAP server properties" dialog box.
Configuring the virtual tree

Nodes in the virtual tree are referenced by their qualified name. A node's qualified name includes the relative distinguished name (RDN) of all nodes above it in the virtual tree, starting with the top node. The RDNs are separated by `/`. For instance:

```
o=MyOrg/ou=MyDep/*/```

Renaming the virtual tree

First, we are renaming the default virtual tree created by the Virtual Directory Server.

1. View the properties of the entry "Tree 1" to open the "Virtual tree properties" dialog box:

   ![Virtual tree properties dialog box]

2. Enter `LDAP tree` as the name of the tree.

3. Choose "OK" to close the dialog box.
Modifying the node

To modify the nodes in the virtual tree:

1. Select the node *o=maxware* in the virtual tree and choose "Properties..." from the context menu. Select the "Data source" tab:

   Change the "Relative DN" (relative distinguished name) to a value matching the directory server you are using. This value is returned to the client as part of the objects' distinguished name. In this example, we kept the default value. Also ensure that the object class matches the DN you specify. This is returned to the client as the entry's object class.

2. Choose "OK" to close the dialog box.
Specifying the port number

We will deploy this configuration as an LDAP server. An LDAP server normally runs on port 389, but when testing it can be necessary to use another port number to avoid conflicts. If the port number is already in use, the server will not be able to start. We will deploy this configuration as an LDAP deployment. The port number is specified as part of the deployment parameters.

1. Select the LDAP deployment "main_listener" and choose "Properties…" from the context menu. Select the "Deployment" tab:

   ![Deployment Configuration Screen]

   If the port number conflicts with another LDAP server (or other process), enter another valid port number.

2. Choose "OK" to close the dialog box.
Enabling the operation log

Before we start the server we can enable the operation log to be able to see any error messages.

1. Choose **Configure/Logging/Operation log…** to open the "Operation log" dialog box:

![Operation Log Dialog Box](image)

2. Fill in the fields:
   - Select "Debug" as the log level to get a detailed log.
   - Select "Debug" in "Log level for extensions" to include any log messages written from the Java classes.

3. Choose "OK" to close the dialog box.
4. Choose the "Operation" button from the toolbar.
Running the server

Start the server by clicking the button. When the server is starting, the indicator in the status bar turns green. You can follow the process in the "Console" pane of the utility panel.
Testing the configuration

To test the configuration, you can use the integrated LDAP client. The default location of the "LDAP browser" tab is in the left pane of the work area. Select the "LDAP browser" tab:

Choose "Refresh" to display the tree and then select an object to view the properties below. Double-click to expand the next level in the tree.

If you want to use an external LDAP client, specify the following information:

- Server address (host name) according to your system's configuration, for instance localhost if you are running locally.
- The same port number as you used when configuring the VDS server (in this case 7015).
- LDAP version 3.
- No starting point (to include the whole virtual tree in the search).
- Anonymous login.

Browse or search the directory and view properties about the items you find.
Section 2: Adding a directory server

This section describes how you add a second directory server. You may add the directory server used as an example, or you can add a server of your choice.

**Note:**
Some parameters in the configuration are server specific, so the values that are explained here may not match the server you are using.

1. Select the entry "Singles" below "Data sources" and choose "New…" from the context menu. The "Select template" dialog box is displayed:

2. Choose "LDAP" in the "Group" list and "Generic LDAP server" in the "Template" list. You see a description of the template in the field below.
3. Choose "OK". The "LDAP Directory" wizard is displayed:

```
Server: localhost
Port: 7389
Starting point: o=tutorial
User name: tutorial
Password: ********
```

Using the template:

Fill in the fields with the required information and complete the wizard.

Server
Enter localhost as the host name of the directory server.

Port
Enter 7389 as the directory server's port number.

Starting point
Enter o=tutorial the starting point in the directory server.

User name/Password
Enter tutorial both as user name and password to access the directory server.
4. Choose "OK". The "LDAP server properties" dialog box is displayed:

![LDAP server properties dialog box]

Enter the following information about the data source:

**Enable**
Select "Enable" to enable the data source.

**Display name**
Enter a name for the data source. This name is used to identify the data source internally in the Virtual Directory Server.

**Unique name**
Enter a unique name for the data source. This will be used when referencing the data source from a Java class.
Section 2: Adding a directory server
SAP NetWeaver Identity Management Virtual Directory Server Tutorial - Accessing LDAP servers

5. Choose the "Connectors" tab:

Verify that "Use default connector" is selected to specify that you want to use the internal class for handling incoming LDAP requests. The methods in the class are generic, and should work with most LDAP servers.
6. Select the "LDAP" tab:

![LDAP server properties](image-url)

Some of the fields are filled in with the values you entered in the wizard.

**Cache connection to data source**
Leaving the check box empty should work under all circumstances. This means that the server initiates a new BIND for each SEARCH operation against the LDAP server. If possible, you can select the check box to enhance performance.

You can keep the default values for the other fields.

7. Choose "Test connection" to verify that you can access the data source.

8. Choose "OK" to close the dialog box.

You have now added the directory server. The next step is to modify the virtual tree to include this directory server.
Section 3: Modifying the virtual tree

The next step is to modify the virtual tree to create a node for the new data source. The existing tree has the following structure:

```
Virtual trees
+---------------------------------
| LDAP tree                        |
| +--------------------------------|
| | o=maxware                      |
```

We are going to add a new top node and a second branch for the new data source. The node `o=maxware` will be moved and renamed. The modified tree will have the following structure:

```
Virtual trees
+---------------------------------
| LDAP tree                        |
| +--------------------------------|
| | o=operNode                      |
| |   +--------------------------------|
| |   | ou=maxware                     |
| |   +--------------------------------|
| |   | ou=FIX                         |
```

This process involves the following tasks:

- Creating three nodes: two static nodes and one data source node.
- Moving the existing node.
- Moving the access rights from the original top node to the new top node.

Creating the static nodes

In this structure we need two static nodes. They do not reference any data source.

Creating the new top node

First we are going to add a static top node.

1. Select the entry "LDAP tree" and choose "New..." from the context menu. The "Node properties" dialog box is displayed:
Fill in the following fields:

**Relative DN**
Enter the node's relative distinguished name (RDN). The name must comply with the rules for LDAP distinguished names.

**Source**
As this is a static node, it does not reference a data source.

**Object class**
The object class you specify here is returned in response to base SEARCH operations and must match the attribute type of the node's relative distinguished name, in this case the RDN is "o=TopNode". Select "organization" from the list "Append Object Class".

2. Choose "OK" to close the dialog box.

The node o=TopNode is now added to the virtual tree:

```
Virtual trees:
  LDAP tree:
    o=maxware
    o=TopNode
```

**Creating the sub-node**
The next step is to create the sub-node that represents the starting point of the LDAP server and some attributes for the node.

1. Select the node o=TopNode and choose "New…" from the context menu. The "Node properties" dialog box is displayed:

```
Node properties - LDAP tree, o=TopNode, New entry 6:4

Data source | Access control list | Additional method parameters | Advanced

Enable

Relative DN: o=TopNode
Data source category: Data source
Source: None
Object class: organizationalUnit

LDAP attributes:

Attribute name | Attribute value
---|---

Priority: High

OK | Cancel | Apply | Help
```

Enter the following information about the node:

**Relative DN**
Enter the node's relative distinguished name.

**Source**
This is also a static node, and does not reference a data source, so we select "None".

**Object class**
Select "organizationalUnit" as the node's object class.

2. Choose "OK" to close the dialog box.
The virtual tree now has the following nodes:

Creating the data source node

The next step is to add the data source node. This node represents all entries below the DN we created in the previous step. To match all possible DNs on this level, this node is named *.

1. Select the node you created in the previous step and choose "New..." from the context menu. The "Node properties" dialog box is displayed:

Enter the following information about the node:

Relative DN
Enter * as the node's relative distinguished name.

Source
Select the data source you created in Section 2.

Object class
The node's object class is set to "*" to match all object classes that may be found in a client's request. This means that the object classes of the entries in the LDAP server are used when performing the client's LDAP request.

2. Choose "OK" to close the dialog box.

The virtual tree now includes these nodes:
Moving the existing node

The existing node \texttt{o=maxware} must be moved below the static node \texttt{o=TopNode}. As the node gets a new position in the virtual tree, the relative distinguished name (RDN) becomes invalid. According to the LDAP standard, two subsequent \texttt{o} are not allowed in a DN.

We also need to change the data source node's virtual starting point to match the new structure.

1. Select the node that now has the qualified name \texttt{o=maxware} and choose "Cut" from the context menu. Select the node \texttt{o=TopNode} and choose "Paste" from the context menu.
2. View the properties of the node \texttt{o=TopNode/o=maxware}:

   \begin{itemize}
   \item \textbf{Relative DN} \newline
   Modify the attribute type of the RDN from \texttt{o=} to \texttt{ou=}.
   \item \textbf{Object class} \newline
   Select \texttt{organizationalUnit} as the node’s object class.
   \end{itemize}

3. Choose "OK".

The virtual tree now has the final structure:
Moving the access rights

In the original configuration, the access rights were defined for the top node `o=maxware`. All sub-nodes in the tree inherit the access rights of a parent node. As the tree's structure is modified, the access rights must be moved to the new top node to cover the whole tree.

First we will remove the access rights from the original top node. Then we will apply the access rights to the new top node:

1. View the properties of the node `o=TopNode/ou=maxware` and select the "Access control list" tab:

   Select the user group/rule pair in the list, right-click and choose "Delete line" from the context menu.

2. Choose "OK".

3. View the properties of the node `o=TopNode` and select the "Access control list" tab:

   Select the user group/rule pair in the list, right-click and choose "Delete line" from the context menu.
At this point, we apply the original access rights:

**User group**
Select the "Anonymous" user group. It provides access for anonymous users. You can view the properties of the user group by selecting it in the "User groups" section in the configuration tree.

**Rule**
Select "LimitedReadAccess" from the list. This rule only allows SEARCH operations. You can view the properties of the rule by selecting it in the "Rules" section in the configuration tree.

4. Choose "OK" to close the dialog box.

**Running the server**

Reload the server configuration by choosing the "Update" button. Perform a SEARCH operation using an LDAP client.
Section 4: Differentiating access rights

In this section we want to modify the access control to be able to differentiate between "external" and "internal" users.

Until now, we have used anonymous login, and the same user group and rule have been used for the whole tree. The rule has been configured to return all attributes in response to a SEARCH request. We are now going to modify this rule to limit the number of attributes returned to clients using anonymous login.

We will create a user group that requires clients to log in with a specific user name and password. We will also create a rule that does not restrict the number of attributes returned to the client. This user group and rule will be applied to one of the branches in the virtual tree.

Clients belonging to this user groups will have maximum access to "their" data source, but limited access to the other, and vice versa.

The process involves the following tasks:

- Creating the user group and user profile.
- Creating a rule that returns all attributes.
- Implementing the access rights in the virtual tree.

Adding the user group

The first step is to add the user group and corresponding user profile.

To add the user group:

1. Select the entry "User groups" and choose "New…" from the context menu. The "User group properties" dialog box is displayed:

   ![User group properties dialog box](image)

   Fill in the following fields:

   **Allow general access to the service**
   Select this check box to specify that this user group is allowed to access the server.

   **Display name**
   Fill in a name that is used to identify the group. Here we have used a part of the static node's name, but this is not a requirement.
Associate with virtual tree
Select "LDAP tree" in the list to specify that this user group should be available when defining access control for the nodes in this tree.

2. Choose "OK" to close the dialog box.

Adding the user profile

To add the user profile:

1. Select the user group you just created and select "Add user…” from the context menu. The "User properties" dialog box is displayed:

   Fill in the following fields:

   **Name**
   Enter a user name that clients must use when logging on to the server. The login name does not have to be a full legal DN, since it is only used by the Virtual Directory Server.

   **Password**
   Choose "Reset…” to the right of the field and enter the password to be used with the user name you specified. The scrambled password is displayed in the field.

2. Choose "OK" to close the dialog box.

The "User groups" section may now look like this:
Creating the rule

The "LimitedReadAccess" returns only a limited set of attributes in response to a SEARCH request. We will now create a rule that returns all available attributes. This rule will be used in combination with the user group we have added to give clients extended access to their data source.

To add the rule:

1. Select the entry "Rules" and select "New…" from the context menu. The "Rule properties" dialog box is displayed:

   Fill in the following fields:

   **Enable rule**
   Make sure that this check box is selected.

   **Display name**
   Enter a name to identify the rule.

2. Select the "Search operation" tab:

   Select "Allow SEARCH operation" and "Search for all attributes".

3. Choose "OK" to close the dialog box.

© Copyright 2008 SAP AG. All rights reserved.
The "Rules" section now may look like this:

```
Rules
  FullAccess
  FullReadAccess
  LimitedReadAccess
```

**Implementing the access rights in the virtual tree**

The next step is to modify the access rights in the virtual tree. The "LimitedReadAccess" will be used for anonymous logins in the whole tree. We will apply the user group and rule we just created to the node `o=TopNode/ou=mx`.

This means that clients logging on with the correct user name and password will be using this user group. For their "native" node, they are using a rule that does not restrict the selection of returned attributes. For the other data source, they are using a rule that limits the number of returned attributes.

Clients using anonymous login will be using the "Anonymous" user group with a rule that limits the number of returned attributes in the whole tree.

**Modifying access rights for the sub-node**

To modify the access rights for the sub-nodes:

1. View the properties of the node `o=TopNode/ou=mx` and select the "Access control list" tab:

   ![Node properties - LDAP tree, o=TopNode,ou=mx](image)

   Select the user group "MaXdata" and the rule "FullReadAccess".

2. Choose "OK" to close the dialog box.
Modifying access rights for the top node

To give the user group access rights to the other data source, we must add the user group to the top level. But this time, we will use the same rule as for anonymous clients.

1. View the properties of the node o=TopNode and select the "Access control list" tab:

Select the user group "MaXdata" and the rule "LimitedReadAccess".

2. Choose "OK" to close the dialog box.

Adding LDAP attributes to the static node

You can add LDAP attributes to a static node that will be returned to the client:

1. View the properties of the node o=TopNode,ou=mx.

LDAP attributes

Add other LDAP attributes you want to associate with this node. These values are returned in response to LDAP base SEARCH operations.

2. Choose "OK".
Running the server

Update the server configuration and use an LDAP client to verify that the configuration has the expected effect on the attributes that are displayed for the objects. Try both anonymous login and login using the user name and password you specified.

Also verify that you can see the LDAP attributes you added to the static node.
This section shows how we can use a simple method to modify one of the values before it is returned to the client. We have already implemented a virtual directory that distinguishes between clients that log on with a user name and password, and clients that use anonymous login. We can assume that these are "internal" and "external" clients respectively. The method will change an internal telephone number to the switchboard's telephone number, which is then returned to external clients.

Creating the class

So far we have been using the classes in the \Externals folder. To be able to modify the class, we need to create the class in the configuration:

1. Open the "Server properties" dialog box and select the "Classes" tab:

2. Choose "New..." to the right of the "Attribute class" field and choose "SampleAttributeFixClass":

3. Choose "OK".

The class is added to the "Attributes" classes in the configuration tree.
Adding the method

To add the method:

1. The Java class is displayed in the "Java class" window:

   ```java
   public String Location(String param) {
       String Location = "Norway";
       //MVDLogger.Debug("Running method: Location");
       return (Location);
   }
   ```

   Enter the code that is highlighted here, or write a more advanced method. The above method will always return one specific location, regardless of the existing value.

2. Choose **File/Save** to save the Java class in the configuration file.

3. Compile the class by choosing **Tools/Compile**. The resulting .class file is stored in the configuration's work area.
4. Close the window to return to the "Server configuration" dialog box.

5. Choose "OK" to close the dialog box.
Section 5: Altering an attribute using a Java method

SAP NetWeaver Identity Management Virtual Directory Server Tutorial - Accessing LDAP servers

Calling the method

The method is used when returning the search result to anonymous clients.

To add the method:

1. View the properties of the "Anonymous" user group and select the "Conversion to client attributes" tab:

```
Select "l" in the "From" column, as this is the internal attribute we are going to manipulate.

Enter "l" in the "To" column. This is the attribute that will be returned to the client.
Although we are not performing any attribute conversion here, this is the way we the method is called.

Select the method "Location" in the "Method" column. This will call the location method whenever the location is to be returned to clients accessing the server with the "Anonymous" user group, substituting the value originally contained in the locality attribute l by the value "Norway".

2. Choose "OK" to close the dialog box.

Running the server

Reload the server configuration. Use an LDAP client to verify that the location is added. Remember that you have to use anonymous login to see the effect of the modification.