LDAP Authentication on Windows Server

LDAP Authentication on Windows Server

ProVision supports LDAP authentication (including Windows Server). To setup an LDAP server for authentication, you must perform the following procedures:

Configuring the LDAP functions on your Windows Server

You should confirm these steps with your LDAP admin - the purpose of this walkthrough is to provide some level of detail on how to extend LDAP functionality to support integration with an application like ProVision.

Step 1: Prepare to extend the Schema (http://technet.microsoft.com/en-us/library/cc961754.aspx)

This is not a minor operation and requires interaction with various control modification areas of Windows Server:

- If you have not modified the schema before, you will need to use the Active Directory Schema console on a DC (Domain Controller) to permit write access to the DC schema.
- Since the schema object has dedicated permissions, admins must be a member of the Schema Administrator group (Schema Admins).
- Note that the DC that is holding the Schema Master Role is the only one allowed to write to it.

Step 2: Decide on method for Installing/executing Schema Extensions (http://technet.microsoft.com/en-us/library/cc961742.aspx)

If you have already used other AD integrations, this should be straightforward. We recommend using the LDIF script method

Step 3: Add and Modify a Schema Object (http://technet.microsoft.com/en-us/library/cc961575.aspx)

To add a new attribute to the schema, you first have to create a attribute object. The you will need to complete the following steps:

- Select a name for the attribute (ProVision assumes that the name will be '**sixConnGroup**')
- Get a valid Object Identifier (OID) from an issuing authority (http://msdn.microsoft.com/en-us/library/ms677620.aspx)

> **Generate an Object Identifier**
>
> Microsoft has released a script that can generate an Object Identifier (OID): https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06

- Document the attribute syntax
- Confirm that the attribute should be single-value
- Confirm the attribute indexing behavior
- Decide if the attribute needs to be distributed to the Global Catalog

LDAP Schema - Example

```
attributetype (1.3.6.1.4.1.5023215.2.3.21 NAME 'sixConnGroup' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
objectclass ( 1.3.6.1.4.1.5023215.2.4.2 NAME 'sixConnectPermissionsV2' DESC '6Connect Permissions Object v2'
SUP top AUXILIARY MUST ( sixConnGroup ) )
```

LDAP User Example

SSH into your openLDAP server and create a new 'ldif' file. Example:

```
dn: cn=JoeSmith,ou=people,dc=6connect,dc=com
cn: JoeSmith
sn: JoeSmith
objectclass: top
objectclass: person
objectclass: sixConnectPermissionsV2
sixConnGroup: "Global Admins"
sixConnGroup: "IT Engineering"
sixConnGroup: "Sales"
sixConnGroup: "Customer Admin"
userPassword: testpass
```

To create a new user, make a new ldif file and change all instances of "JoeSmith" to whatever username you wish to create and update the password. Keep all of the object class definitions as listed above. Add a sixConnGroup declaration for each ProVision user group a user is in.

After the file is created, run the following command to add the new user to LDAP server:

```
ldapadd -h [SERVER] -x -f [LDIF FILE] -D [ROOTDN] -w [ROOT PW] -v
```

Example:

```
ldapadd -h localhost -x -f 6connect.ldif -D "cn=Manager,dc=6connect,dc=com" -w secret -v
```

The user will now be active in openLDAP and can be used to login to ProVision.

Test the LDAP Server

To query the LDAP server, run the following command on any server which has openLDAP enabled:

```
ldapsearch -b [BASE] -h [IPADDRESS] -D [DOMAIN] -w [PASSWORD] [USER]
```

Note: We have not been able to use a v6 address at with this tool, even though multiple sources say it should work.

At the end of the command where [USER] is specified, user or groups can be used (in LDAP format) to query.

Example:

```
ldapsearch -b "dc=6connect,dc=com" -h 50.240.195.129 -D "cn=Mayor,ou=people,dc=6connect,dc=com" -w testpass
"cn=MajorMiner"
```

Configure ProVision for LDAP Authentication

To configure the use of LDAP authentication, follow the steps below.

1. Log into 6connect ProVision
2. Go to Settings Tab Admin Settings -> Authentication
3. Select "LDAP" under "Authentication Options"
4. Move the LDAP Enable selector to the "ON" position.
5. Fill in the hostname or ip address, authentication port, LDAP Security, Auth DN, Fetch DN, and Filter DN.
    a. Optionally, enter the LDAP Username and Password in order to allow ProVision to import LDAP Contacts and sync LDAP contact information (see: Contact Manager)
6. Click "Save Changes".

Example values in this case would be:

- LDAP Enable: (Checked)

- LDAP Server Address: 52.240.195.12
- LDAP Port: 389 (or SSL/TLS port is 636)
- LDAP Security: None
- LDAP Auth DN: cn=%LOGIN%,ou=people,dc=6connect,dc=com
- LDAP Fetch DN: cn=%LOGIN%
- LDAP Filter DN: cn=%LOGIN%

Setting default login authentication options

In the login screen, you would select the authentication method from the dropdown. If you like, you can set the default login option in the following way:

Go to the /data/globals.php and open in vi (or other editor). Add in the following text as the last line of the file (before the closing ?>)

define('DEFAULT_LOGIN_TYPE', 'radius');

Acceptable values are "local", "radius" and "ldap". If this line is not present in globals.php, the default option is "local".

Using SSL encryption

To use SSL encryption with LDAP, the ldap.conf file must be correctly configured on the ProVision server.

Typically, the LDAP configuration file is kept at "/etc/ldap/ldap.conf". Make sure the following line is present:

```
TLS_REQCERT allow
```

and restart the webserver.

Add or Update LDAP Settings

To add or update LDAP settings, go to the Settings Tab Admin to enter the Admin area.

Then, click the "Authentication" sub-tab at the top of the Admin Settings page, and select "LDAP" from the "Authentication Options" module.

Enter or update the following settings:

- **LDAP Enable:** check the box to enable LDAP functionality.

- **LDAP Server Address:** Set the IP address of your LDAP server.
- **LDAP Port:** Set the port for your LDAP server
- **LDAP Security:** Select the security method of your LDAP server - SSL, TLS or None
- **LDAP Auth DN/Fetch DN/Filter DN:** These strings are used to first authentication the 6connect user and then to retrieve their permissions. The string '%LOGIN%' should be inserted in place of the user's common name both strings. (ex: cn=%LOGIN%,ou=people, dc=6connect,dc=com)
- **LDAP Group Attribute:** If using an internal list of user groups instead of 6connect groups, enter the attribute name for the LDAP groups here. If a Group Attribute is set, it will be used first, otherwise the 6connect schema will be used.
- **LDAP Username / LDAP Password:** Optionally, you may enter LDAP admin credentials to allow ProVision to import and sync LDAP contacts. See Contact Manager for details on LDAP contacts.
- **Mapping Permissions to 6connect schema:** To integrate 6connect permissions with your existing directory structure then you will need the 6connect schema. It should snap in with any existing LDAP structure and allow you to assign 6connect permissions to your existing users. You can download a copy of the schema from this section.

Once at least one LDAP server has been added, a list will appear at the top of the Radius module. Add an additional Radius server by clicking "Add new server".

ProVision will try to connect to each server listed in the order listed, until a success is returned. Disabled servers will display in grey, and the currently selected server will display in bold.

When done, click "Save Changes".