HP CloudSystem Enterprise and Foundation Software

Configuring Directory Services in HP CloudSystem

CloudSystem identity management includes support for Microsoft Active Directory and OpenLDAP. This white paper details step-by-step how to set up directory services in CloudSystem Foundation and Enterprise.

Directory Tree Samples

Two directory tree samples are employed in this white paper. The Directory Tree 1 represents a Microsoft Active Directory tree while the Directory Tree 2 exemplifies an OpenLDAP tree. Both are detailed in the right side column.

CloudSystem Foundation

Use the CloudSystem Console to manage directory services in CloudSystem Foundation. Infrastructure administrators can configure directories and associate directory groups to administrative roles. Create a directory entry using the CloudSystem Console > Settings > Security > Edit > Directories > Add directory screen.

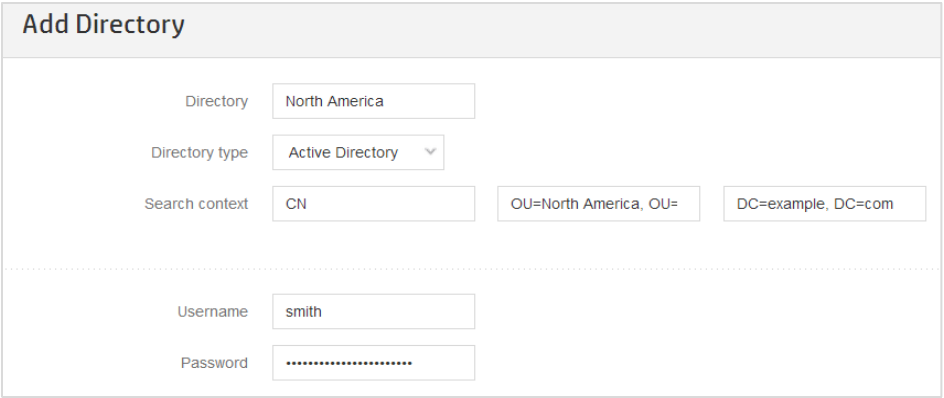
The CloudSystem Portal and its underlying OpenStack Keystone service are automatically configured based on the default directory set in the CloudSystem Console. Cloud administrators can then manage directory users within the directory service itself, without any other configuration in CloudSystem.

The following sections depict how to set up Microsoft Active Directory and OpenLDAP. in CloudSystem.

Microsoft Active Directory

Step 1. Add the directory. Name the directory entry and select the “Active Directory” type. Enter the search context which consists of user identifier, user search base and base DN (suffix) as shown below.

Important: Be sure to enter the search context correctly and identically in Foundation (CloudSystem Console) and Enterprise (Cloud Service Management Console).



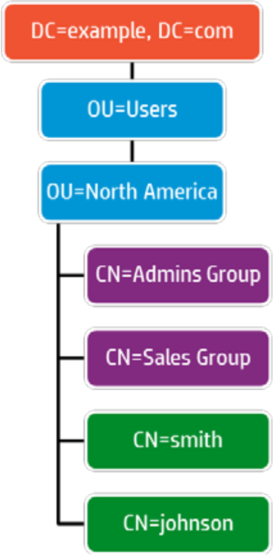
Add Directory

Directory	North America		
Directory type	Active Directory		
Search context	CN	OU=North America, OU=	DC=example, DC=com
Username	smith		
Password	••••••••••••••••••••••••		

Figure 1 – Creating the “North America” directory

Directory Tree 1 – Active Directory sample

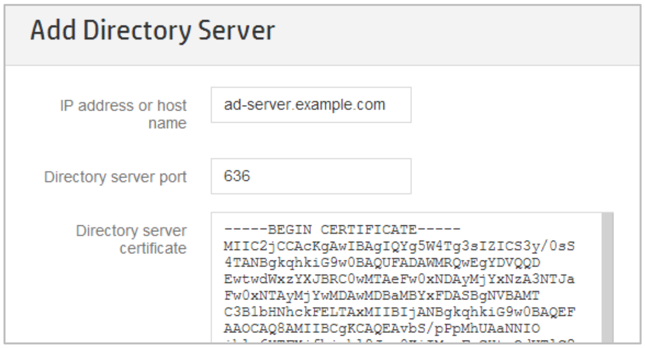
Below is an Active Directory tree sample that contains hierarchical organizational units. The “North America” organizational unit contains the “Admins Group” and “Sales Group” groups as well as the “smith” and “johnson” user accounts. Let’s consider that the “smith” user account belongs to the “Admins Group” while “johnson” is a member of “Sales Group”.



The search context is interpreted as follows:

- **User Name/ID:** CN
- **User search base:** OU=North America, OU=Users
- **Base DN:** DC=example, DC=com

Step 2. Configure the server. Enter an IP address or host name, directory server port and directory server certificate:



Add Directory Server

IP address or host name: ad-server.example.com

Directory server port: 636

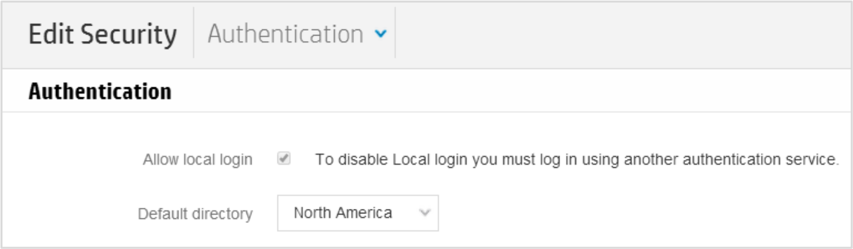
Directory server certificate:

```
-----BEGIN CERTIFICATE-----
MIIC2jCCAcKgAwIBAgIQYg5W4Tg3sIZICS3y/0sS
4TANBgkqhkiG9w0BAQUFADAWMRQwEgYDVQQD
EwtwdWxzYXJBRC0wMTAeFw0xNDAyMjYxNzA3NTJa
Fw0xNTAyMjYwMDAwMDBaMBYxFDASBgNVBAMT
C3B1bHNhckFELTAxMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAvbS/pPpMhUAaNNIO
```

Figure 2 - Configuring a server for the “North America” directory

Step 3. Check and save the settings. On the “Add directory” dialog, enter valid user credentials in the username and password textboxes. Make sure the user account is located under the **user search base**. Then check the connectivity and save the configuration.

Step 4. Set the default directory. On the “Edit Security” dialog, choose a directory as the default directory. For example:



Edit Security | Authentication

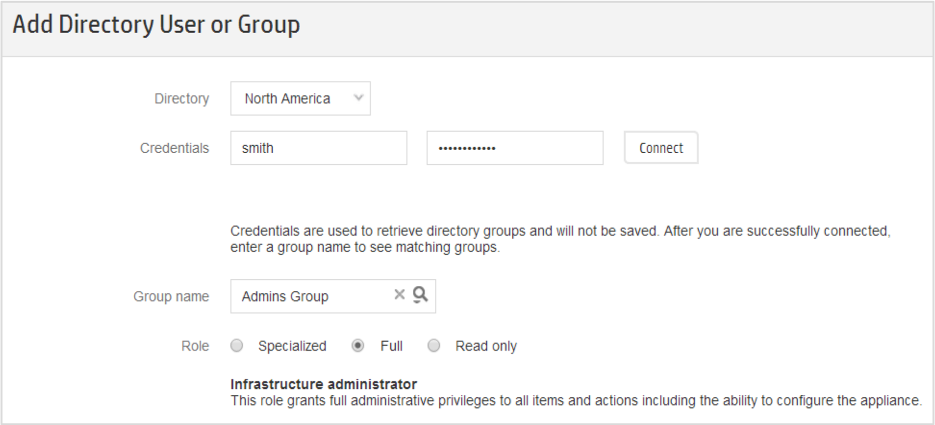
Authentication

Allow local login: ☑ To disable Local login you must log in using another authentication service.

Default directory: North America

Figure 3 – Setting the “North America” as the default directory

Step 5. Add a directory group. Go to CloudSystem Console > User and Groups > Add Directory User or Group. Connect to a pre-defined directory using a user account. Then select a group from the list and assign a role to it. For example:



Add Directory User or Group

Directory: North America

Credentials: smith ••••••••••••• Connect

Credentials are used to retrieve directory groups and will not be saved. After you are successfully connected, enter a group name to see matching groups.

Group name: Admins Group

Role: ○ Specialized ● Full ○ Read only

Infrastructure administrator
This role grants full administrative privileges to all items and actions including the ability to configure the appliance.

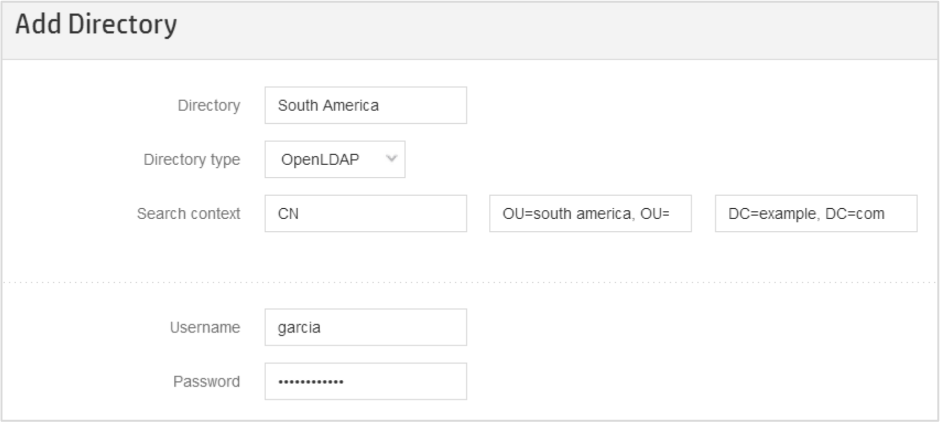
Figure 4 - Assigning the "Admins Group" to the Full Infrastructure administrator role

Active Directory constraints. Below are listed the main constraints in CloudSystem Foundation for Microsoft Active Directory:

- Directory tree: groups must be located under the user search base
- Directory schema
  - Users: supports the “user” objectClass only
  - Groups: supports the “group” and “groupOfNames” objectClasses only

OpenLDAP

Step 1. Add the directory. Give a name to the directory entry and select the “OpenLDAP” type. Then enter the search context which consists of user identifier, user search base and base DN (suffix) as shown below:



Add Directory

Directory: South America

Directory type: OpenLDAP

Search context: CN | OU=south america, OU= | DC=example, DC=com

Username: garcia

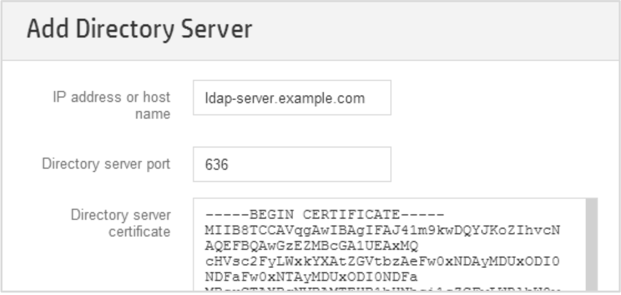
Password: ••••••••••••

Figure 5 - Creating the “South America” directory

The search context is interpreted as following:

- User Name/ID: CN
- User search base: OU=south america, OU=people
- Base DN: DC=example, DC=com

Step 2. Configure the server. Enter an IP address or host name, directory server port and directory server certificate as follows:



Add Directory Server

IP address or host name: ldap-server.example.com

Directory server port: 636

Directory server certificate:

```
-----BEGIN CERTIFICATE-----
MIIB8TCCAVqgAwIBAgIFAJ41m9kwDQYJKoZIhvcN
AQEFBQAwGzEZMBcGA1UEAxMQ
cHVsc2FyLWxkYXAtZGVtbzAeFw0xNDAyMDUxODI0
NDFaFw0xNTAyMDUxODI0NDFa
```

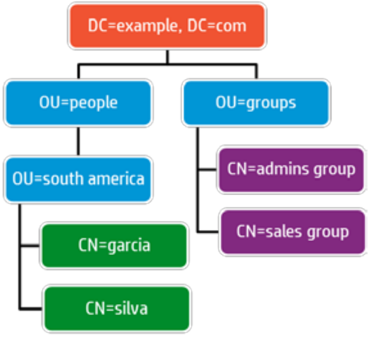
Figure 6 - Configuring a server for the “South America” directory

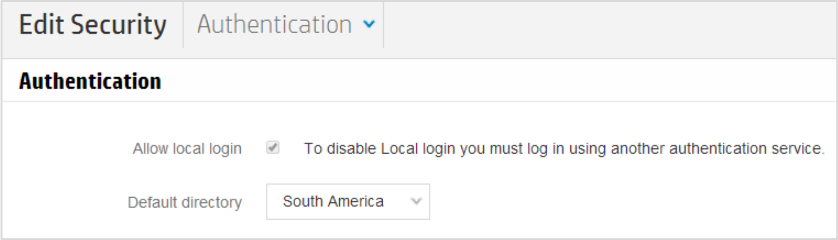
Step 3. Check and save the settings. On the “Add directory” dialog, enter valid user credentials in the username and password textboxes. Make sure the user account is located under the user search base. Then check the connectivity and save the configuration.

Step 4. Set the default directory. On the “Edit Security” dialog, choose a directory as the default:

Directory Tree 2 – OpenLDAP sample

Below is an OpenLDAP tree sample that contains tree organizational units. The “south america” organizational unit contains “garcia” and “silva” user accounts. On the other side, the “groups” organizational unit holds “admins group” and “sales group”. Let’s consider the “garcia” user account belongs to the “admins group” while “silva” is a member of “sales group”.





Edit Security

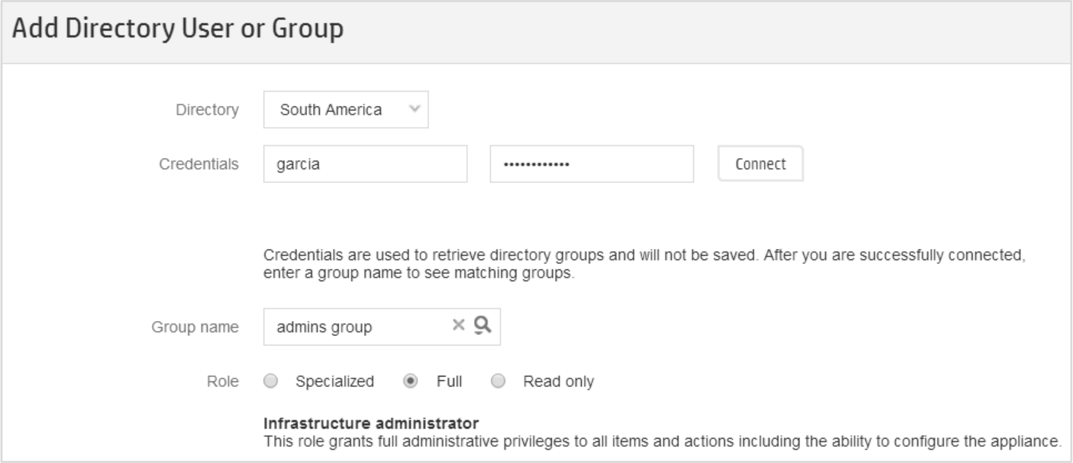
Authentication

Allow local login ☑ To disable Local login you must log in using another authentication service.

Default directory: South America

Figure 7 - Setting the "South America" as the default directory

Step 5. Create a directory group. Go to CloudSystem Console > User and Groups > Add Directory User or Group. Connect to a pre-defined directory using a user account. Then select a group from the list and assign a role to it. For instance:



Add Directory User or Group

Directory: South America

Credentials: garcia ••••••••••••

Credentials are used to retrieve directory groups and will not be saved. After you are successfully connected, enter a group name to see matching groups.

Group name: admins group

Role ○ Specialized ● Full ○ Read only

Infrastructure administrator
This role grants full administrative privileges to all items and actions including the ability to configure the appliance.

Figure 8 - Assigning the "admins group" to the Full Infrastructure administrator role

OpenLDAP constraints. Below are listed the main constraints in CloudSystem Foundation for OpenLDAP:

- **Directory tree:** groups must be located under the OU=groups from the Base DN
- **Directory schema**
  - **Users:** supports the "inetOrgPerson" objectClass only
  - **Groups:** supports the "groupOfNames" objectClass only

Summary about User Authorization

In a nutshell, the Foundation user permissions are:

- User accounts from a directory group can log into the CloudSystem Console. Currently only Full Infrastructure administrator and Read only roles are supported.
- User accounts from the default directory that are assigned to an OpenStack project can log into the CloudSystem Portal. By default, Full Infrastructure administrators are assigned to the "administrator" project.

General Constrains

CloudSystem Portal. It is automatically configured based on the default directory and the first server from the server list. In other words, the CloudSystem Portal does not support multiple directories nor load balancing servers.

FQDN. Although CloudSystem Console accepts an IP address for the directory server, HP strongly recommends the usage of FQDN.

Strong certificate validation. By default CloudSystem Foundation does not validate the directory server certificate in a strict manner. To enable the strong SSL/TLS validation for the CloudSystem Portal, you must export the CA certificate from the directory server and import it to the Foundation appliance through the appliance console. For more information, see the "Enabling strong certificate validation in the CloudSystem Portal" appendix in the *HP CloudSystem Administrator Guide* at www.hp.com/go/cloudsystem/docs.

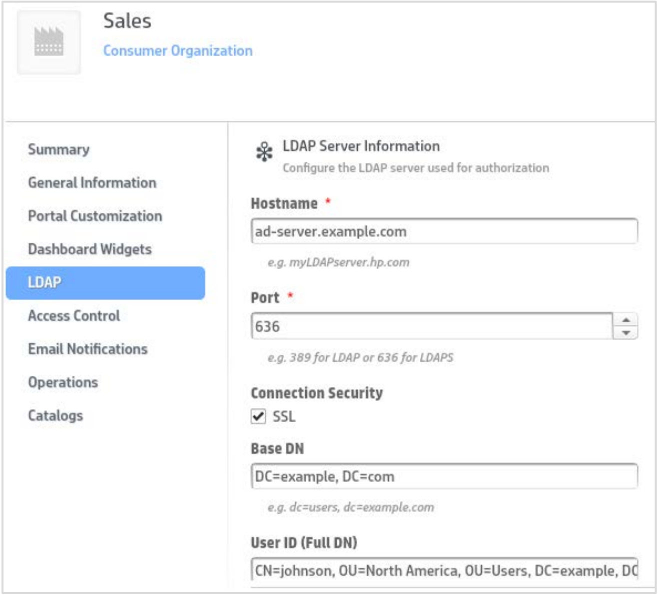
CloudSystem Enterprise

CloudSystem Enterprise supports the multi-tenancy features in Cloud Service Automation (CSA). With CSA you can bind Organizations to directory services and then assign user groups from that directory to be a part of the Organization.

The next sections describe how to configure Microsoft Active Directory and OpenLDAP in HP CSA. Both assume the “Sales” consumer organization was created previously.

Microsoft Active Directory

Step 1. Configure base AD settings. In the Cloud Service Automation Console, open a consumer organization and click on the “LDAP” panel. Enter the hostname, port and optionally check the SSL option for a secure connection. Then set the Base DN, User ID and password. For instance:



Sales
Consumer Organization

LDAP Server Information
Configure the LDAP server used for authorization

Hostname *
ad-server.example.com
e.g. myLDAPserver.hp.com

Port *
636
e.g. 389 for LDAP or 636 for LDAPS

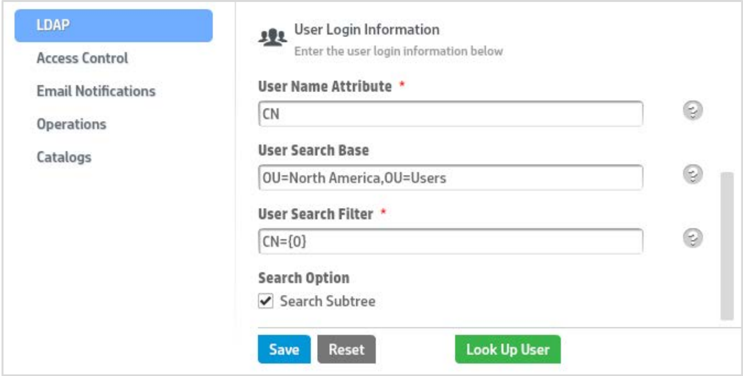
Connection Security
☑ SSL

Base DN
DC=example, DC=com
e.g. dc=users, dc=example.com

User ID (Full DN)
CN=johnson, OU=North America, OU=Users, DC=example, DC

Figure 9 - Configuring LDAP server information for the “Sales” Organization on AD

Step 2. Configure the user login. Enter the user name attribute, user search base and optionally check the “Search Subtree” for a recursive lookup. For example:



User Login Information
Enter the user login information below

User Name Attribute *
CN

User Search Base
OU=North America,OU=Users

User Search Filter *
CN={0}

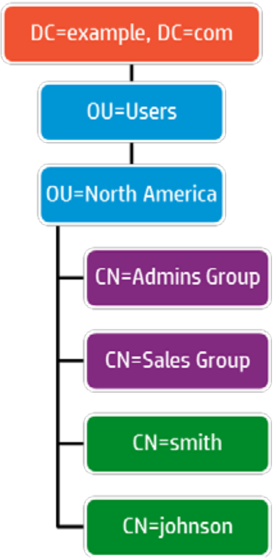
Search Option
☑ Search Subtree

Figure 10 - Configuring user login for the "Sales" Organization on AD

Notice the search context is identical to CloudSystem Foundation:

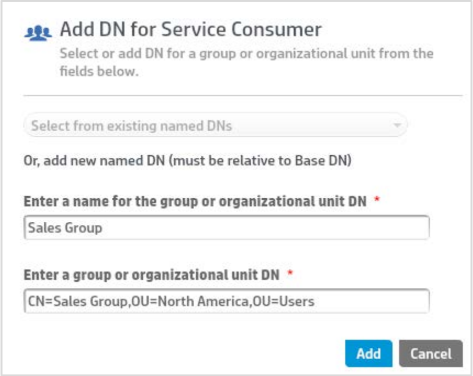
- **User Name:** CN
- **User search base:** OU=North America, OU=Users
- **Base DN:** DC=example, DC=com

Directory Tree 1 – Active Directory sample



Step 3. Save and check the settings. Save the settings and then click on the "Look Up User" button to search for a regular user.

Step 4. Configure the access control. Click on the "Access Control" panel. Enter name and DN for a group or organizational unit. For example:



Add DN for Service Consumer

Select or add DN for a group or organizational unit from the fields below.

Select from existing named DNs

Or, add new named DN (must be relative to Base DN)

Enter a name for the group or organizational unit DN *

Sales Group

Enter a group or organizational unit DN *

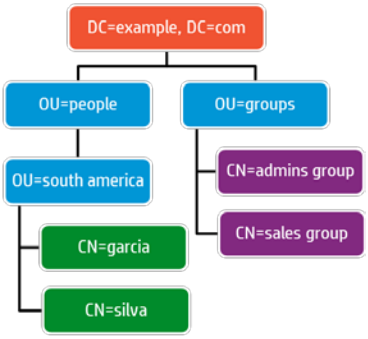
CN=Sales Group,OU=North America,OU=Users

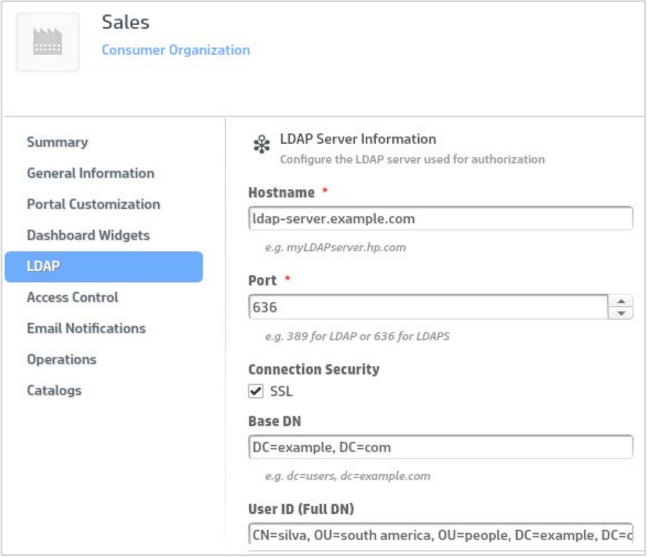
Figure 11 - Assigning the "Sales Group" to the Service Consumer role

OpenLDAP

Step 1. Configure base LDAP settings. In the Cloud Service Automation Console, open a consumer organization and click on the "LDAP" panel. Enter the hostname, port and optionally check the SSL option for a secure connection. Then set the Base DN, User ID and password. For instance:

Directory Tree 2 – OpenLDAP sample





Sales

Consumer Organization

LDAP Server Information

Configure the LDAP server used for authorization

Hostname *

ldap-server.example.com

e.g. myLDAPserver.hp.com

Port *

636

e.g. 389 for LDAP or 636 for LDAPS

Connection Security

☑ SSL

Base DN

DC=example, DC=com

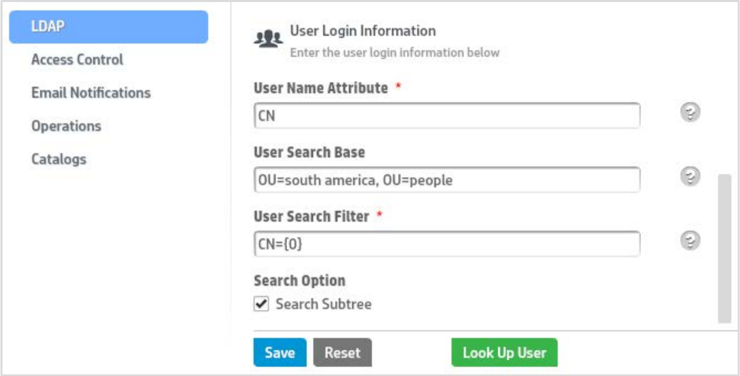
e.g. dc=users, dc=example.com

User ID (Full DN)

CN=silva, OU=south america, OU=people, DC=example, DC=c

Figure 12 - Configuring LDAP server information for the "Sales" Organization on OpenLDAP

Step 2. Configure the user login. Enter the user name attribute, user search base and optionally check the "Search Subtree" for a recursive lookup. For example:



User Login Information
Enter the user login information below

User Name Attribute *: CN

User Search Base: OU=south america, OU=people

User Search Filter *: CN={0}

Search Option: ☑ Search Subtree

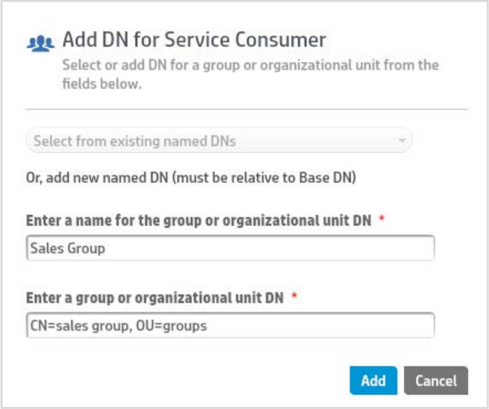
Figure 13 - Configuring user login for the "Sales" Organization on OpenLDAP

Make sure that the search context is identical to CloudSystem Foundation:

- User Name: CN
- User search base: OU=south america, OU=people
- Base DN: DC=example, DC=com

Step 3. Save and check the settings. Save the settings and then click on the "Look Up User" button to search for a regular user.

Step 4. Configure the access control. Click on the "Access Control" panel. Enter name and DN for the group or organizational unit. For instance:



Add DN for Service Consumer
Select or add DN for a group or organizational unit from the fields below.

Or, add new named DN (must be relative to Base DN)

Enter a name for the group or organizational unit DN *: Sales Group

Enter a group or organizational unit DN *: CN=sales group, OU=groups

Figure 14 - Assigning the "Sales Group" to the Service Consumer role

Summary about User Authorization

Essentially, user accounts from groups or organizational units which are set in the Organization's access control can access the respective Marketplace Portal.

General Constraints

Secure connection. The LDAP certificate must be imported to the HP CSA keystore. For more information, see the "Supported operations on the CloudSystem appliances" appendix in the *HP CloudSystem Administrator Guide* at www.hp.com/go/cloudsystem/docs.

Access control. Group or organizational unit must be relative to Base DN.

Learn more about HP CloudSystem

http://www.hp.com/go/CloudSystem and
http://www.hp.com/go/CloudSystem/docs

5900-3794, September 2014