CONTENTS

CHAPTER 1
Overview 1
LDAP and Multiple Authentication Server Configuration Using Active Directory 1
Prerequisites 2

CHAPTER 2
Configuring the Active Directory Server 3
Creating an Organizational Unit and Adding Groups 3
Creating a Non-Admin Bind User Account 4
Creating Users and Adding Them to the Cisco UCS OU 5
Collecting Information for the UCS LDAP Configuration 5

CHAPTER 3
Configuring Cisco UCS 7
Creating a Local Authentication Domain 7
Creating an LDAP Provider 8
Configuring the LDAP Group Rule 9
Creating an LDAP Provider Group 9
Creating an LDAP Group Map 10
Creating an LDAP Authentication Domain 10

CHAPTER 4
Testing Your Configuration 13
Testing Your Configuration Using the UCS Manager CLI 13
Testing Your Configuration Using the UCS Manager GUI 14

APPENDIX A
FAQs 15
Overview

This chapter includes the following sections:

- LDAP and Multiple Authentication Server Configuration Using Active Directory, page 1
- Prerequisites, page 2

LDAP and Multiple Authentication Server Configuration Using Active Directory

Cisco UCS can be configured to authenticate user logins remotely using LDAP and various remote authentication providers, such as Active Directory (AD).

This sample configuration is intended to show you the complete process—from start to finish—of implementing Cisco UCS LDAP and multiple server authentication using an AD server. It also includes steps for testing your implementation in the Cisco UCS Manager GUI and Cisco UCS Manager CLI.

Specifically, this configuration includes the following tasks in the AD server:

- Creating an Organizational Unit and Adding Groups, on page 3
- Creating a Non-Admin Bind User Account, on page 4
- Creating Users and Adding Them to the CiscoUCS OU, on page 5
- Collecting Information for the UCS LDAP Configuration, on page 5

The following tasks are completed in Cisco UCS Manager:

- Creating a Local Authentication Domain, on page 7
- Creating an LDAP Provider, on page 8
- Configuring the LDAP Group Rule, on page 9
- Creating an LDAP Provider Group, on page 9
- Creating an LDAP Group Map, on page 10
- Creating an LDAP Authentication Domain, on page 10
Prerequisites

To complete this sample configuration, you must have the following:

- Cisco UCS system
- Cisco UCS Manager Release 2.x
- Microsoft Active Directory server 2003 or later
- Administrative privileges for the Active Directory server
- ADSI Edit
CHAPTER 2

Configuring the Active Directory Server

This chapter includes the following sections:

• Creating an Organizational Unit and Adding Groups, page 3
• Creating a Non-Admin Bind User Account, page 4
• Creating Users and Adding Them to the CiscoUCS OU, page 5
• Collecting Information for the UCS LDAP Configuration, page 5

Creating an Organizational Unit and Adding Groups

Organizational units (OUs) in the AD server contain AD groups that map to user roles in Cisco UCS. For every role maintained in AD, you must have the same role configured in Cisco UCS.

Maintaining matching role names in both AD and Cisco UCS is a requirement for integration.

Procedure

Step 1 Open Active Directory Users and Computers.
Step 2 Right-click the AD instance, sampledesign.com, and select New > Organizational Unit.
Step 3 For Name, type CiscoUCS.
Step 4 Create a new group called ucsaaa and assign it to the newly created CiscoUCS OU:
   a) Right-click the new CiscoUCS OU and select New > Group.
   b) In the New Object - Group dialog box, type ucsaaa in the Group name field.
   c) In the Group scope area, click the Global radio button.
   d) In the Group type area, click the Security radio button and click OK.
Step 5 Repeat Step 4 for each of the following roles:
   • ucsaaa
   • ucsadmin

Sample Configuration: Cisco UCS, LDAP and Active Directory
Creating a Non-Admin Bind User Account

Cisco UCS uses the non-admin bind user account to regularly check which groups the user is included in within the AD server.

Note
To prevent unnecessary authentication errors, we recommend that this account be set up with a non-expiring password.

If you already have a non-admin user account in the AD server that can be used by Cisco UCS to authenticate users, then it is not necessary to create a new non-admin bind user account. You can skip this task and move on to creating sample users and adding them to the Cisco UCS OU.

Procedure

Step 1 Right-click the CiscoUCS OU and select New > User.
Step 2 For First name, type ucs.
Step 3 Leave the Initials field blank.
Step 4 For Last name, type binduser.
Step 5 For User logon name, type ucsbind, select the UPN suffix in the drop-down list, and click Next.

A user account called ucsbind appears in the CiscoUCS OU.

What to Do Next
Create sample users and add them to the CiscoUCS OU.
Creating Users and Adding Them to the CiscoUCS OU

Procedure

Step 1  Right-click CiscoUCS and select New > User.
Step 2  For First name, type sample.
Step 3  For Last name, type admin.
Step 4  For Full name, type sampleadmin.
Step 5  For User logon name, type sampleadmin, select the UPN suffix from the drop-down list, and click Next.
Step 6  In the work pane, right-click the sampleadmin user and click Properties.
Step 7  Click the MemberOf tab, and click Add.
Step 8  In the Enter the object names to select field of the Select Groups dialog box, type ucsadmin and click OK.
Step 9  Click OK again to close the Sample Admin Properties dialog box.
Step 10 (Optional) Repeat Steps 1 through 9 to create the following users:

- sampleaaa
- samplenetwork
- sampleoperation
- samplesecurity
- samplestorage

What to Do Next

Collect information needed for the Cisco UCS LDAP configuration.

Collecting Information for the UCS LDAP Configuration

To configure LDAP and multiple simultaneous authorizations in Cisco UCS Manager, you need to access several values from the AD server. This example uses ADSI Edit, a free third-party utility, to find the required values.

Before You Begin

Install and configure ADSI Edit.

Procedure

Step 1  Open ADSI Edit and navigate to DC=sampledesign,DC=com. This is the BaseDN folder.
Step 2  To find the BaseDN values required by Cisco UCS Manager to configure LDAP authentication, complete the following steps:
   a) Right-click the DC=sampledesign,DC=com instance and choose Properties.
   b) On the Attribute Editor tab, select distinguishedName.
   c) In the String Attribute Editor dialog box, select and copy the string in the Value field.
      The BaseDN value follows the DC=sampledesign,DC=com format.
   d) Paste the BaseDN value string into a text file for later use.

Step 3  To find the DN for each role that you have added to the CiscoUCS OU in AD, complete the following steps:
   a) Expand the CiscoUCS OU, right-click the CN=ucsadmin role, and choose Properties.
   b) On the Attribute Editor tab, select distinguishedName.
   c) In the String Attribute Editor dialog box, select and copy the string in the Value field.
      It should follow the CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com format.
   d) Paste the DN value string into a text file for later use.
   e) Repeat these steps for each AD group in the CiscoUCS OU.

Step 4  To find the BindDN for the non-admin bind user account, complete the following steps:
   a) Navigate to the user account named ucsbind.
   b) Right-click the ucsbind user account in the CiscoUCS OU and choose Properties.
   c) On the Attribute Editor tab, select distinguishedName.
   d) In the String Attribute Editor dialog box, select and copy the string in the Value field.
      The BindDN should follow the CN=ucsbind,OU=CiscoUCS,DC=sampledesign,DC=com format.
   e) Paste the BindDN value string into a text file for later use.

Step 5  On the Attribute Editor tab, verify that the sAMAccountName attribute exists.

What to Do Next
Configure Cisco UCS using these values.
Configuring Cisco UCS

This chapter includes the following sections:

- Creating a Local Authentication Domain, page 7
- Creating an LDAP Provider, page 8
- Configuring the LDAP Group Rule, page 9
- Creating an LDAP Provider Group, page 9
- Creating an LDAP Group Map, page 10
- Creating an LDAP Authentication Domain, page 10

Creating a Local Authentication Domain

This sample configuration recommends that you create a local authentication domain before you configure LDAP settings in Cisco UCS Manager. Logging in as a local admin user guarantees that you will have the access rights required to complete the steps in this procedure, and could prevent you from having to spend time correcting an invalid configuration.

Before You Begin
Log into Cisco UCS Manager GUI as an admin user.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, expand All &gt; User Management &gt; Authentication.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click Authentication Domains and select Create a Domain.</td>
</tr>
<tr>
<td>Step 4</td>
<td>For the Name field, type local.</td>
</tr>
<tr>
<td>Step 5</td>
<td>For the Realm, click the local radio button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>
What to Do Next
Configure LDAP properties in Cisco UCS Manager.

Creating an LDAP Provider

This sample configuration does not include steps to configure LDAP with SSL.

Procedure

Step 1
In the Navigation pane, click the Admin tab.

Step 2
On the Admin tab, expand All > User Management > LDAP.

Step 3
In the Work pane, click the General tab.

Step 4
In the Actions area, click Create LDAP Provider.

Step 5
In the Create LDAP Provider page of the wizard, do the following:

a) In the Hostname field, type the IP address or the hostname of the AD server.

b) In the Order field, accept the lowest-available default.

c) In the BindDN field, copy and paste the BindDN from your AD configuration.
   For this sample configuration, the BindDN value is CN=ucsbind,OU=CiscoUsers,DC=sampledesign,DC=com.

d) In the BaseDN field, copy and paste the BaseDN from your AD configuration.
   For this sample configuration, the BaseDN value is DC=sampledesign,DC=com.

e) Leave the Enable SSL check box unchecked.

f) In the Port field, accept the 389 default.

   g) In the Filter field, copy and paste the filter attribute from your AD configuration.
   Cisco UCS uses the filter value to determine if the user name provided on the logon screen by Cisco UCS Manager is in AD.
   For this sample configuration, the filter value is sAMAccountName=$userid, where $userid is the user name you enter in the Cisco UCS Manager logon screen.

   h) Leave the Attribute field blank.

   i) In the Password field, type the password for the ucsbind account configured in AD.
   If you ever need to go back into the Create LDAP Provider wizard to reset the password, do not be alarmed if the password field is blank. The "Set: yes" message that appears next to the password field indicates that a password has been set.

   j) In the Confirm Password field, retype the password for the ucsbind account configured in AD.

   k) In the Timeout field, accept the 30 default.

   l) In the Vendor field, select the radio button for MS-AD for Microsoft Active Directory.

Step 6
Click Next.

What to Do Next
Configure the LDAP Group Rule.
Configuring the LDAP Group Rule

Procedure

**Step 1**
On the **LDAP Group Rule** page of the wizard, complete the following fields:

a) For the **Group Authentication** field, click the **enable** radio button. Enabling group authentication indicates to UCSM that it should use the target attribute (in this example, memberOf) to see if the user you are trying to authenticate is in a group like ucsaaa.

b) For the **Group Recursion** field, click the **recursive** radio button. Setting group recursion to recursive allows the system to continue digging down, level by level, until it finds a qualifying user. Setting the group recursion to non-recursive limits UCS to a search of the first-level, even if the search does not locate a qualified user.

c) In the **Target Attribute** field, accept the memberOf default.

**Step 2**
Click **Finish**.

*Note* In a real-world scenario you would most likely have multiple LDAP providers. For multiple LDAP providers, you would repeat the steps to configure the LDAP Group Rule for each LDAP provider, changing the order as warranted for your configuration. However, in this sample configuration there is only one LDAP provider, so this is not necessary.

The IP address for the AD server displays in the Navigation pane under **LDAP > LDAP Providers**.

**What to Do Next**
Create an LDAP Provider Group.

Creating an LDAP Provider Group

Procedure

**Step 1**
In the **Navigation** pane, right-click **LDAP Provider Groups** and select **Create LDAP Provider Group**.

**Step 2**
In the **Create LDAP Provider Group** dialog box, do the following:

a) In the **Name** field, enter a unique name for the group such as LDAP Providers.

b) In the **LDAP Providers** table, choose the IP address for your AD server.

c) Click the >> button to add the AD server to your **Included Providers** table.

**Step 3**
Click **OK**.

Your provider group appears in the LDAP Provider Groups folder.

**What to Do Next**
Configure LDAP Group Maps.
Creating an LDAP Group Map

Procedure

Step 1  In the Navigation pane, click the Admin tab.

Step 2  On the Admin tab, expand All > User Management > LDAP.

Step 3  In the Work pane, click Create LDAP Group Map.

Step 4  In the Create LDAP Group Map dialog box, complete the following:
   a) In the LDAP Group DN field, copy and paste the value you saved from the AD server configuration section for your LDAP group.
      The LDAP Group DN value requested in this step maps to the distinguished name for each of the groups you created in AD under UCS Groups. For this reason, the Group DN value entered in Cisco UCS Manager must match exactly with the Group DN value in the AD server. In this sample configuration, this value is CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com.
   b) In the Roles table, click the admin check box and click OK.
      Clicking the check box for a role indicates that you want to assign admin privileges to all users who are included in the group map.

Step 5  Create new LDAP group maps (using the information you recorded earlier from AD) for each of the remaining roles in the AD server that you want to test.

What to Do Next
Create your LDAP authentication domain.

Creating an LDAP Authentication Domain

Procedure

Step 1  On the Admin tab, expand All > User Management > Authentication.

Step 2  Right-click Authentication Domains and select Create a Domain.

Step 3  In the Create a Domain dialog box, complete the following:
   a) In the Name field, type a name for your domain such as LDAP.
   b) In the Realm area, click the ldap radio button.
   c) From the Provider Group drop-down list, select the LDAP provider group previously created and click OK.

The authentication domain appears under Authentication Domains.
What to Do Next

Test your LDAP configuration using the Cisco UCS Manager GUI.
Testing Your Configuration

This chapter includes the following sections:

- Testing Your Configuration Using the UCS Manager CLI, page 13
- Testing Your Configuration Using the UCS Manager GUI, page 14

Testing Your Configuration Using the UCS Manager CLI

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log into the Cisco UCS Manager CLI.</td>
<td>Purpose</td>
</tr>
<tr>
<td>Step 2</td>
<td>UCS-A# connect nxos</td>
<td>Enters NXOS mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>UCS-A (nxos)# test aaa server ldap ip-address username password</td>
<td>Tests the LDAP configuration for any user that you have configured.</td>
</tr>
</tbody>
</table>

The following example tests the LDAP configuration:

```plaintext
UCS-A# connect nxos
UCS-A (nxos) # test aaa server ldap 10.29.96.77 sampleaaa password
user has been authenticated
Attributes downloaded from remote server:
User Groups:
  CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com
Roles:
  admin
```
Testing Your Configuration Using the UCS Manager GUI

Procedure

Step 1  Launch the Cisco UCS Manager GUI.
Step 2  In the User Name field, type sampleaaa.
Step 3  In the Password field, type your sampleaaa AD password.
Step 4  From the Domain drop-down list, select your LDAP provider and click OK.
Step 5  Navigate to All > User Management > User Services > Remotely Authenticated Users and confirm that your authentication domain and AD username are listed. This value takes the format AuthenticationDomain\ADUserName.
FAQs

Q  When recursive search is enabled, how many levels deep will recursion go?
A  First, all groups which the user is directly a member of will be retrieved. Then, for each of these groups, their ancestor groups are traversed. The recursion continues until the top-level group is reached.

Q  Will the AD integration and Cisco UCS Manager support two-factor authentication using AD certificates?
A  No. Cisco UCS Manager only supports password-based authentication.

Q  What are the known limitations of Cisco UCS Manager and AD integration? (For example, limits on AD traversal results, max groups searched, max AD objects, etc.)
A  • Currently there are no known limitations to the size of an AD instance for plain user authentication, although the filter value limits the search results to one or two. Cisco UCS Manager Release 1.3(x) and earlier allowed random filters, resulting in a large number of search results. In release 2.x, a validation is in place that prevents this.
  • If a user belongs to large number of first-level groups, the retrieval of those groups is limited by the memory available for the UCS Manager LDAP client. UCS Manager processes only those groups that have been configured with roles and/or locales and discards all other groups.

The maximum number of groups that the user can be member of is 32. This is consistent with the number of group-to-role mappings allowed in UCS Manager.

Q  What is the maximum AD structure that has been tested and qualified?
A  We have determined that user authentication is not dependent on AD size. We have tested the AD integration with users belonging to more than 120 groups, with each group name having 100 characters.

Q  Does Cisco UCS Manager support AD nested groups?
A  Yes. In Cisco UCS Manager Release 2.x, Active Directory nested groups are supported for LDAP group to UCSM role mappings.