

UCS Director 5.4 – Microsoft Active Directory Integration

The purpose of this document is to illustrate the steps to integrate UCS Director 5.4 with Microsoft Active Directory. Previous versions of UCS Director have had issues with UCS Director pulling down all users in Active Directory even though you specifically drilled down to a specific group level during setup. This could potentially be devastating to the performance UCS Director if your Active Directory has a large number of users. With UCS Director 5.4, this issue has been resolved.

Assumptions/Requirements

- You have a Single or Multi-Node Deployment of UCS Director 5.4.
- You have an Administrator account on Microsoft Active Directory.
- You have access to vCenter where your UCS Director has been deployed.

Useful Documents

[Cisco UCS Director Administration Guide, Release 5.4](#)

Software/OS levels

Listed below are the software and OS versions that were used for the testing and building this document.

- UCS Director 5.4
- VMware 5.1
- Windows Server 2008 R2 Enterprise
- Schema Version 47

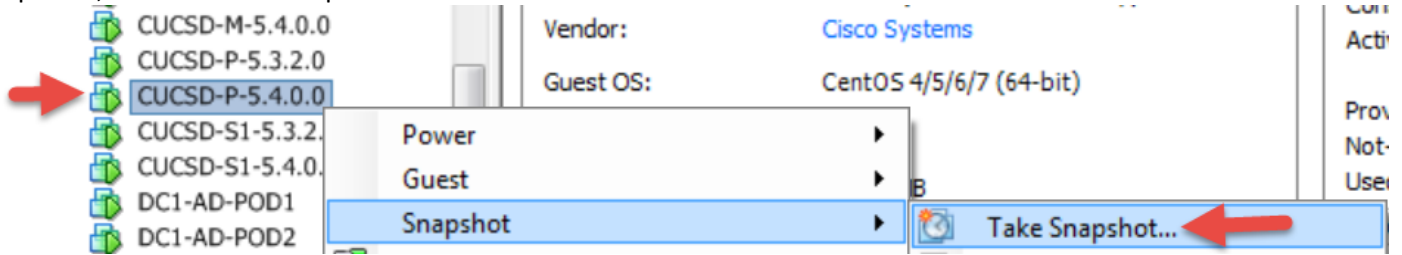
Table of Contents

- Table of Contents 2
- 1. Clone or Snapshot all of you Nodes 3
- 2. Add LDAP Account to UCS Director..... 6
- 3. Test and Verification 11
- 4. Clean Up/Remove all Clones or Snapshots 14

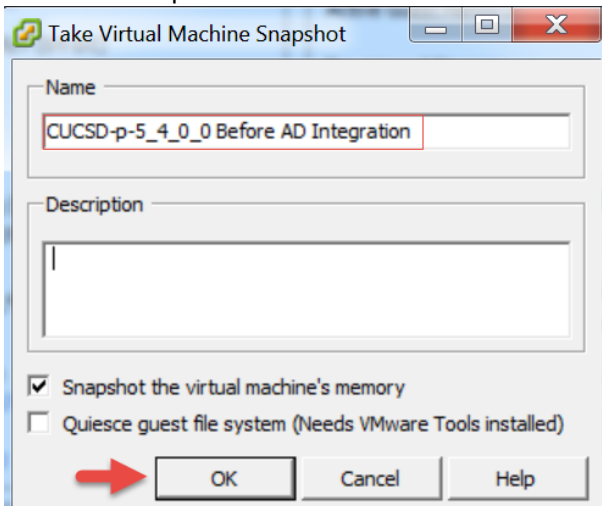
1. Clone or Snapshot all of you Nodes

Before integrating UCS Director with Active Directory, it is wise to clone or snapshot all of your UCS Director Nodes in the event that you make a mistake and accidentally pull down all of your 100,000 users from your Active Directory to your UCS Director. If this were to happen, your UCS Director would probably become unresponsive so you would need to roll back to a previous state of UCS Director.

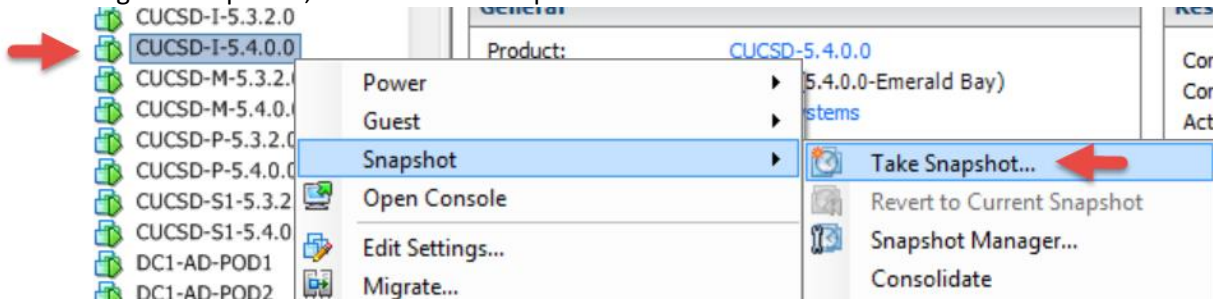
Take a snapshot of the Primary Node. Log into your vCenter -> navigate to the Primary Node VM ->right click on the VM -> Snapshot -> select '**Take Snapshot**'. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



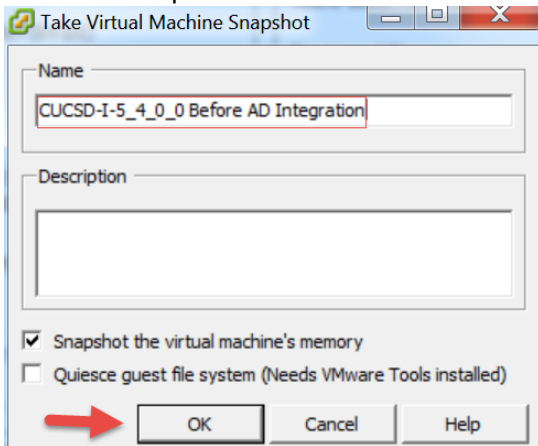
Name the Snapshot and click '**OK**'.



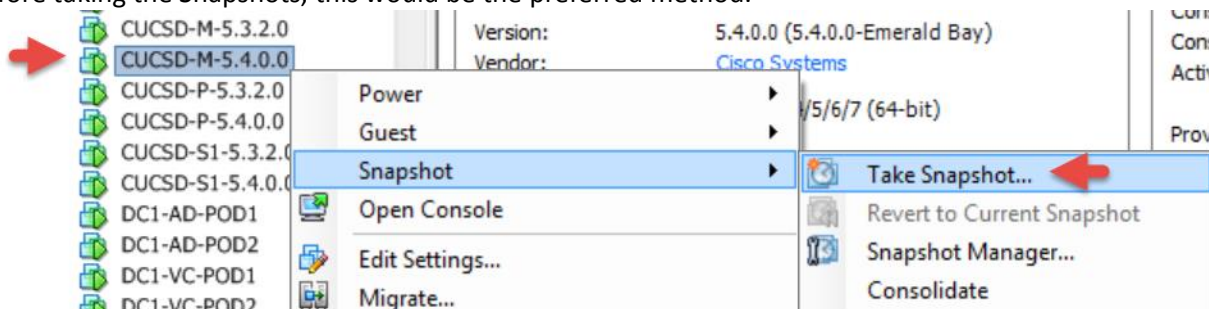
Take a snapshot of the Inventory Database Node. Log into your vCenter -> navigate to the Inventory Database Node VM ->right click on the VM -> Snapshot -> select **'Take Snapshot'**. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



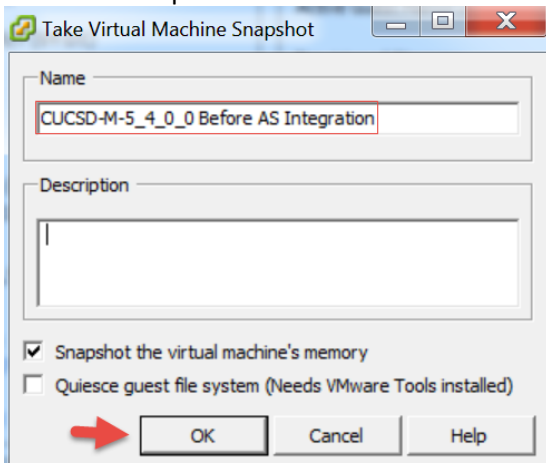
Name the Snapshot and click **'OK'**.



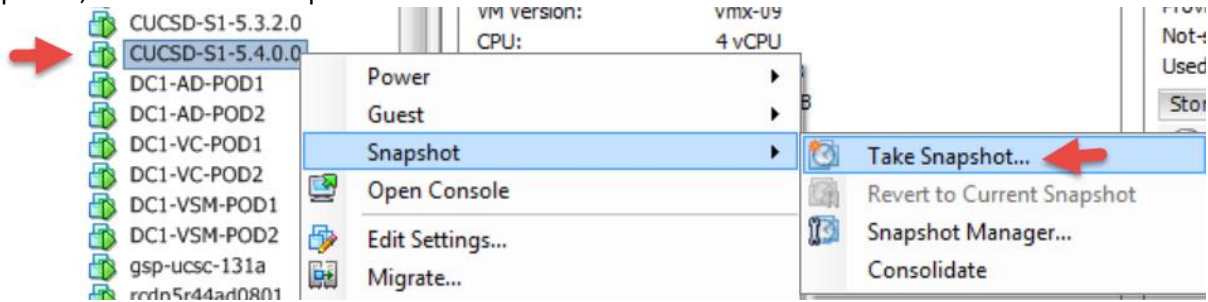
Take a snapshot of the Monitoring Database Node. Log into your vCenter -> navigate to the Monitoring Database Node VM ->right click on the VM -> Snapshot -> select **'Take Snapshot'**. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



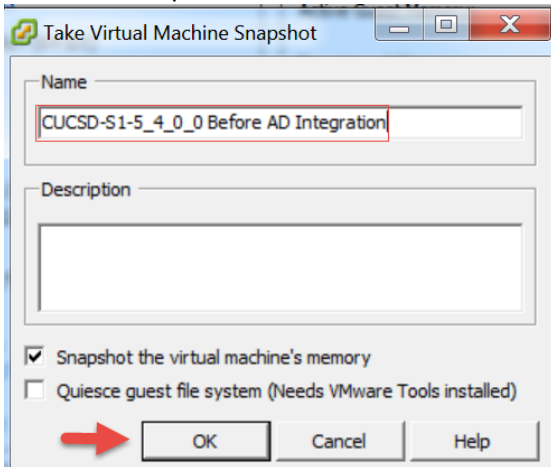
Name the Snapshot and click **'OK'**.



Take a snapshot of the Service Node. Log into your vCenter -> navigate to the Service Node VM ->right click on the VM -> Snapshot -> select 'Take Snapshot'. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



Name the Snapshot and click 'OK'.



2. Add LDAP Account to UCS Director

Navigate to Administration -> Users and Groups -> LDAP Integration -> select 'Add'.

The screenshot shows the Cisco UCS Director Administration interface. The top navigation bar includes 'Administration' with a dropdown arrow. Below it, the 'Users and Groups' section is active, with a sub-menu containing 'LDAP Integration'. The 'Add' button is highlighted with a red arrow. The table below shows the LDAP Integration configuration fields: LDAP Account, Server, Type, Port, SSL Enabled, User, and Domain.

Enter an Account Name, drop down and select 'Microsoft Active Directory', enter 'yourASIP' for Server, enter 'yourDomainName' for the Domain Name field, enter a Username, enter a Password, select 'Next'.

The screenshot shows the 'LDAP Server Configuration' form. The 'LDAP Configuration' tab is selected. The form fields are: Account Name (RCDN5-AD), Server Type (Microsoft Active Directory), Server (172.17.80.104), Port (389), Domain Name (gsp-r5.cloudlab.cisco.com), Username (ucsadmin), Password (*****), and Synchronization Frequency (1 Hours). A red arrow points to the 'Server Type' dropdown menu.

Press 'Select'.

The screenshot shows the 'LDAP Search Base' configuration step. The 'LDAP Search Base' tab is selected. The form field is 'Search Base' with a 'Select...' button. A red arrow points to the 'Select...' button. A message above the field states: 'The page may take a while to load depending on the number of OUs in the Domain.'

Select the 'Search Base DN' you want to search for user in and click 'Select'.

Select

Search Base DN	Search Base Name
<input type="checkbox"/> OU=Domain Controllers@DC=gsp-r5@DC=cloudlab@DC=cisco@DC=com	OU=Domain Controllers,DC=gsp-r5,DC=cloudlab,DC=cisco,DC=com
<input type="checkbox"/> OU=Application Groups@DC=gsp-r5@DC=cloudlab@DC=cisco@DC=com	OU=Application Groups,DC=gsp-r5,DC=cloudlab,DC=cisco,DC=com
<input type="checkbox"/> OU=Access Control Groups@OU=Application Groups@DC=gsp-r5@DC=com	OU=Access Control Groups,OU=Application Groups,DC=gsp-r5,DC=cloudlab,DC=com
<input checked="" type="checkbox"/> OU=Shares@OU=Access Control Groups@OU=Application Groups@DC=gsp-r5@DC=com	OU=Shares,OU=Access Control Groups,OU=Application Groups,DC=gsp-r5,DC=cloudlab,DC=com
<input type="checkbox"/> CN=Users@DC=gsp-r5@DC=cloudlab@DC=cisco@DC=com	CN=Users,DC=gsp-r5,DC=cloudlab,DC=cisco,DC=com
<input type="checkbox"/> CN=Builtin@DC=gsp-r5@DC=cloudlab@DC=cisco@DC=com	CN=Builtin,DC=gsp-r5,DC=cloudlab,DC=cisco,DC=com

Select Cancel

Verify and click 'Next'.

LDAP Server Configuration

- LDAP Configuration
- LDAP Search Base
- Configure User and Group
- LDAP User Role Filter

The page may take a while to load depending on the number of OUs in the Domain.

Search Base OU=Shares,OU=Access Control Groups,OU=Application Groups,DC=gsp-r5...

Select '+' to add either 'User Filters' or 'Group Filters'. I am going to filter at the Group level.

LDAP Server Configuration

- LDAP Configuration
- LDAP Search Base
- Configure User and Group
- LDAP User Role Filter

Configure User and Group Filters
At-least one of the Group/User Filters must be configured.

Attribute Name	Operator	Attribute Value
----------------	----------	-----------------

Group Filters

Enter a filter value for the 'Attribute Value' Field and click '**Submit**'.


Add Entry to Group Filters

Attribute Name *

Operator *

Attribute Value *


Recommended to use alphanumeric characters (a-z, A-Z, 0-9) and Wild-card (*) inputs like *, John* etc.



Click '**OK**'.

Submit Result

Added entry successfully



Verify settings and click '**Next**'.


LDAP Server Configuration

- ✓ LDAP Configuration
- ✓ LDAP Search Base
- Configure User and Group**
- LDAP User Role Filter

Configure User and Group Filters
At-least one of the Group/User Filters must be configured.

Attribute Name	Operator	Attribute Value
sAMAccountName	equals	NSS-Admins

Total 1 items



Click '+' to add the users to a User Role.

LDAP Server Configuration

- ✓ LDAP Configuration
- ✓ LDAP Search Base
- ✓ Configure User and Group
- LDAP User Role Filter**

LDAP User Role Filter

User Role Filters

Attribute Name	Operator	Attribute Value	Map User Rol

Drop down and select 'Service End-User' for Map User Role and click 'Submit'.

Add Entry

Attribute Name *

Operator *

Attribute Value

Map User Role *

Click 'OK'.

Submit Result

Added entry successfully

Verify and click **'Submit'**.

LDAP Server Configuration

- ✓ LDAP Configuration
- ✓ LDAP Search Base
- ✓ Configure User and Group
- LDAP User Role Filter**

LDAP User Role Filter

User Role Filters

Attribute Name	Operator	Attribute Value	Map User Role
sAMAccountName	equals	NSS-Admins	Regular

Total 1 items

Note:
* Users belonging to matched groups will be mapped to user role specified in the user role filter

Back Submit Close

Click **'OK'**.

Submit Result

Added successfully

OK

Test Connectivity to Active Directory by clicking **'Test Connection'**.

Cisco UCS Director

Converged HyperConverged Virtual Physical Organizations Policies Administration Close

Users and Groups

User Groups Users Current Online Users Login Page Branding Authentication Preferences **LDAP Integration**

Refresh Favorite Add Delete Modify View Test Connection Search BaseDN

LDAP Integration

LDAP Account	Server	Type	Port	SSL Enabled	User	Domain	
RCDN5-AD	172.17.80.104	Microsoft Active	389	No	ucsdadmin	gsp-r5.cloudlab.	1

After verifying a successful response, click **'Close'**.

Test LDAP Connectivity

LDAP Connection test successful.

Close

3. Test and Verification

Verify users are synced from the group you filtered on. Navigate to Administration -> Users and Groups -> Users -> select 'Refresh'. I have a user 'ucsd user' in the group I filtered on and you can see that it imported this user from RCDN5-AD LDAP Account.

The screenshot shows the Cisco UCS Director Administration interface. The 'Administration' menu is expanded, and 'Users and Groups' is selected. The 'Users' tab is active, and the 'Refresh' button is highlighted with a red arrow. Below the navigation, there is a table of users. The user 'ucsduser@gsp-r' is highlighted in red, indicating it is the user of interest.

Status	Login Name	First Name	Last Name	Access Level	User Group	Contact Email	User Principa	Source	LDAP Account	Host
Enabled	admin	Sam	Fontenot	System Admin		safonten@cisco.	safonten@cisco.	Local		
Enabled	infraUser			System Admin				Local		
Enabled	ucsduser@gsp-r	ucsd	user	Service End-User	NSS-Admins@gsp-r		ucsduser@gsp-r	External	RCDN5-AD	172.17.80.104

Verify this newly synchronized user 'ucsduser' can login UCS Director.

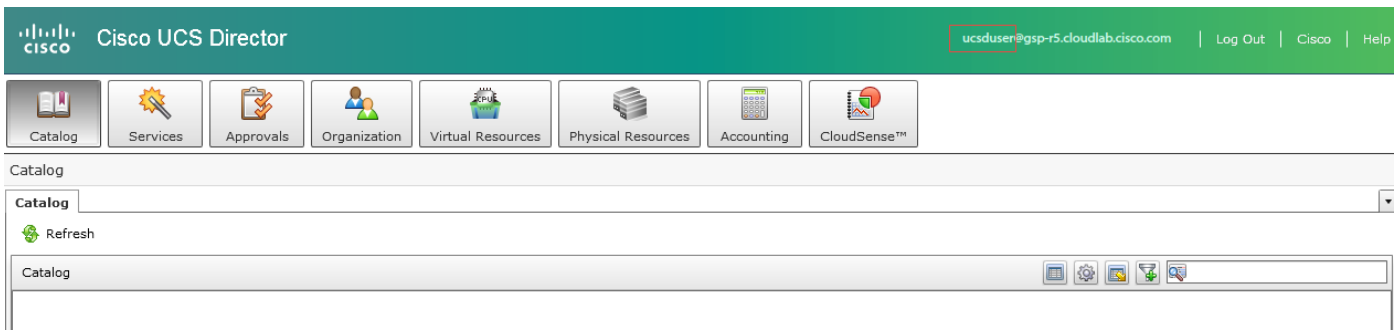
Cisco UCS Director

Username:

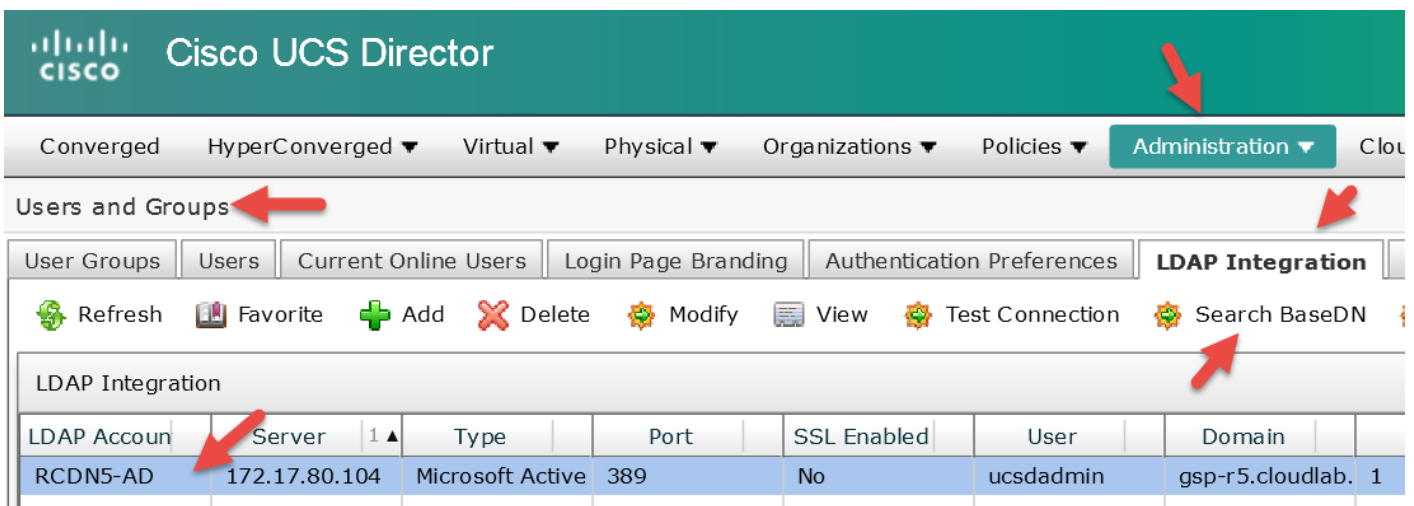
Password:



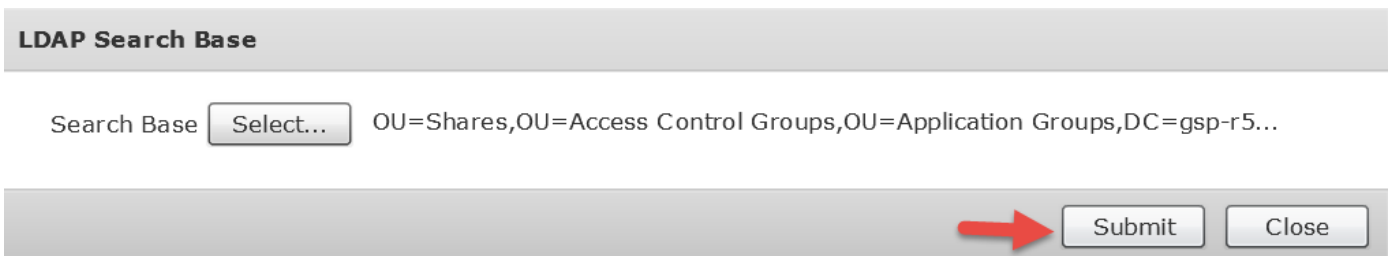
Verify user 'ucsduser' was able to login to the UCSD portal using his AD credentials.



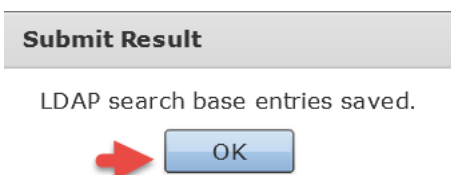
In the previous step, I only had 1 user defined in that group. For this step, I added a second user, 'ucsd user2' and now we want to sync immediately instead of waiting for the duration time to end before synchronizing automatically with AD. Navigate to Administration -> Users and Groups -> LDAP Integration -> select 'RCDN5-AD' account -> select 'Search BaseDN'.



Click 'Submit'.



Click 'OK'.



Refresh the Users to verify the new user has synced with UCS Director. Navigate to Administration -> Users and Groups -> Users -> select 'Refresh'. You can see the new user 'ucsd user2' has been pulled down to UCS Director.

The screenshot shows the Cisco UCS Director Administration interface. The 'Administration' menu is selected, and the 'Users and Groups' section is active. The 'Users' tab is selected, and the 'Refresh' button is highlighted with a red arrow. The 'Users' table below shows the following data:

Status	Login Name	First Name	Last Name	Access Level	User Group	Contact Email	User Principa	Source	LDAP Accoun	Host
Enabled	admin	Sam	Fontenot	System Admin		safonten@cisco.	safonten@cisco.	Local		
Enabled	infraUser			System Admin				Local		
Enabled	ucsduser2@gsp-	ucsd	user2	Service End-User	NSS-Admins@g		ucsduser2@gsp-	External	RCDN5-AD	172.17.80.104
Enabled	ucsduser@gsp-r	ucsd	user	Service End-User	NSS-Admins@g		ucsduser@gsp-r	External	RCDN5-AD	172.17.80.104

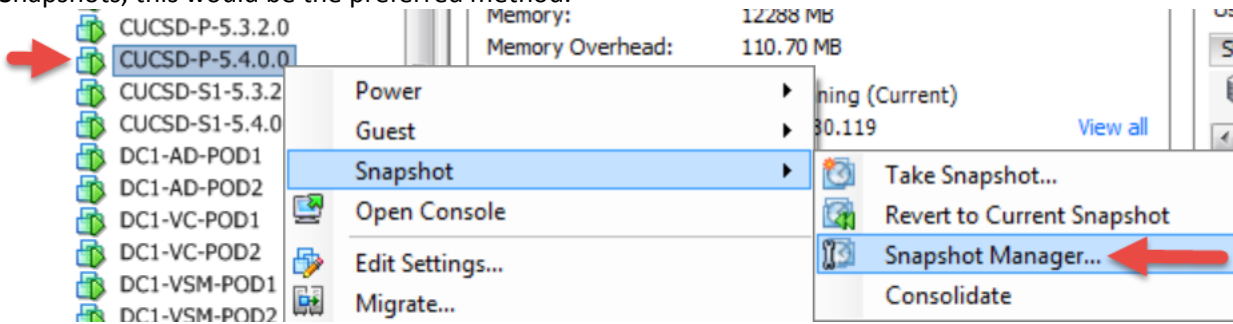
Add a third user 'ucsduser3' to AD but this time wait for the sync duration timer to expire before checking. When setting up the 'RCDN5-AD' account, I left the default of 1 hour for the synchronization frequency.

The screenshot shows the Cisco UCS Director Administration interface. The 'Administration' menu is selected, and the 'Users and Groups' section is active. The 'Users' tab is selected, and the 'Refresh' button is highlighted with a red arrow. The 'Users' table below shows the following data:

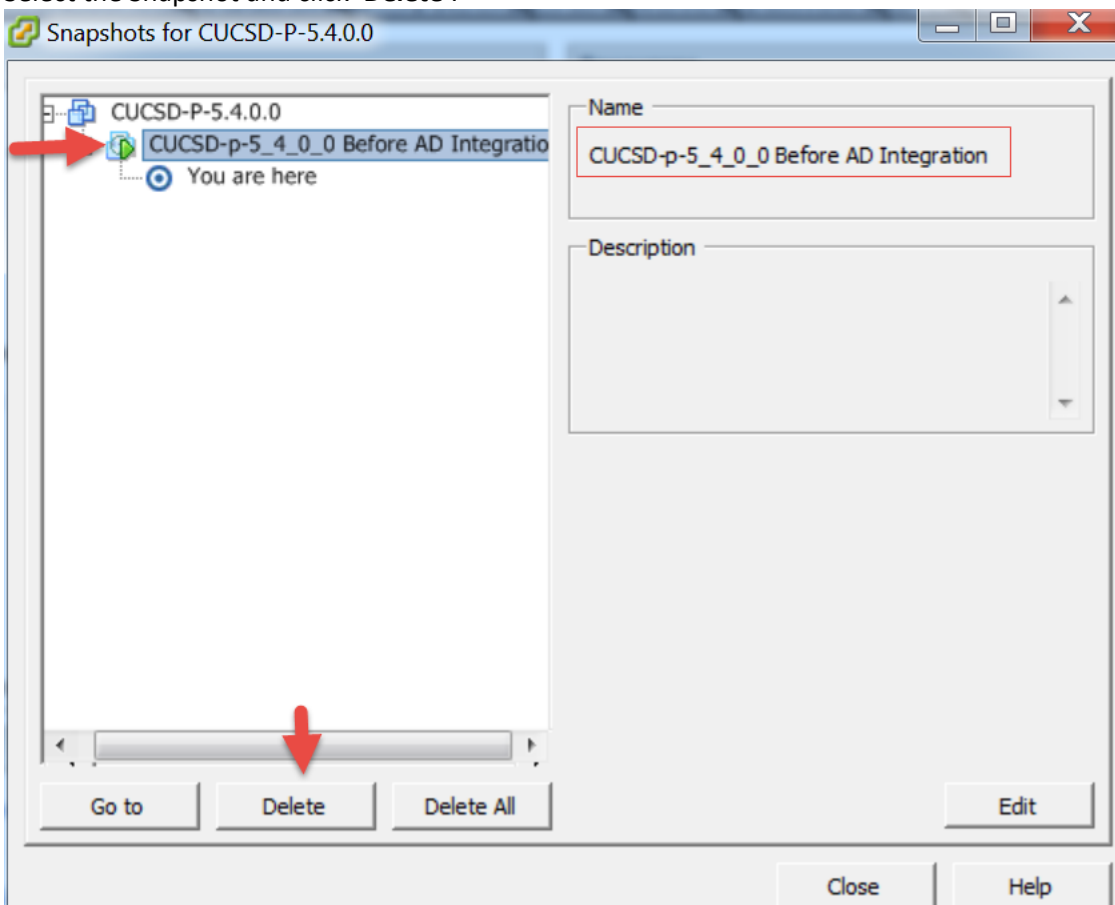
Status	Login Name	First Name	Last Name	Access Level	User Group	Contact Email	User Principa	Source	LDAP Accoun	Host
Enabled	admin	Sam	Fontenot	System Admin		safonten@cisco.	safonten@cisco.	Local		
Enabled	infraUser			System Admin				Local		
Enabled	ucsduser2@gsp-	ucsd	user2	Service End-User	NSS-Admins@g		ucsduser2@gsp-	External	RCDN5-AD	172.17.80.104
Enabled	ucsduser3@gsp-	ucsd	user3	Service End-User	NSS-Admins@g		ucsduser3@gsp-	External	RCDN5-AD	172.17.80.104
Enabled	ucsduser@gsp-r	ucsd	user	Service End-User	NSS-Admins@g		ucsduser@gsp-r	External	RCDN5-AD	172.17.80.104

4. Clean Up/Remove all Clones or Snapshots

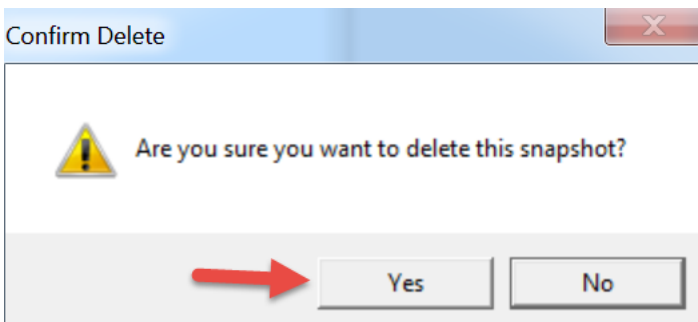
Remove the Primary Node Snapshot. Log into your vCenter -> navigate to the Primary Node VM ->right click on the VM -> Snapshot -> select **'Snapshot Manager'**. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



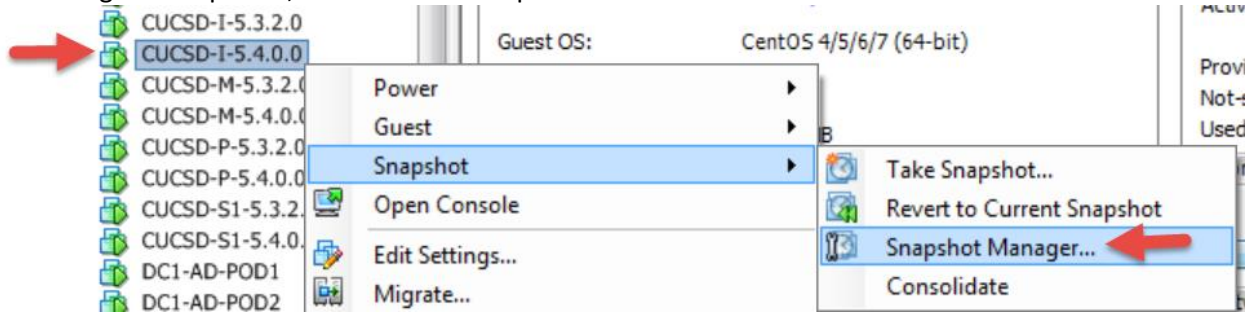
Select the Snapshot and click **'Delete'**.



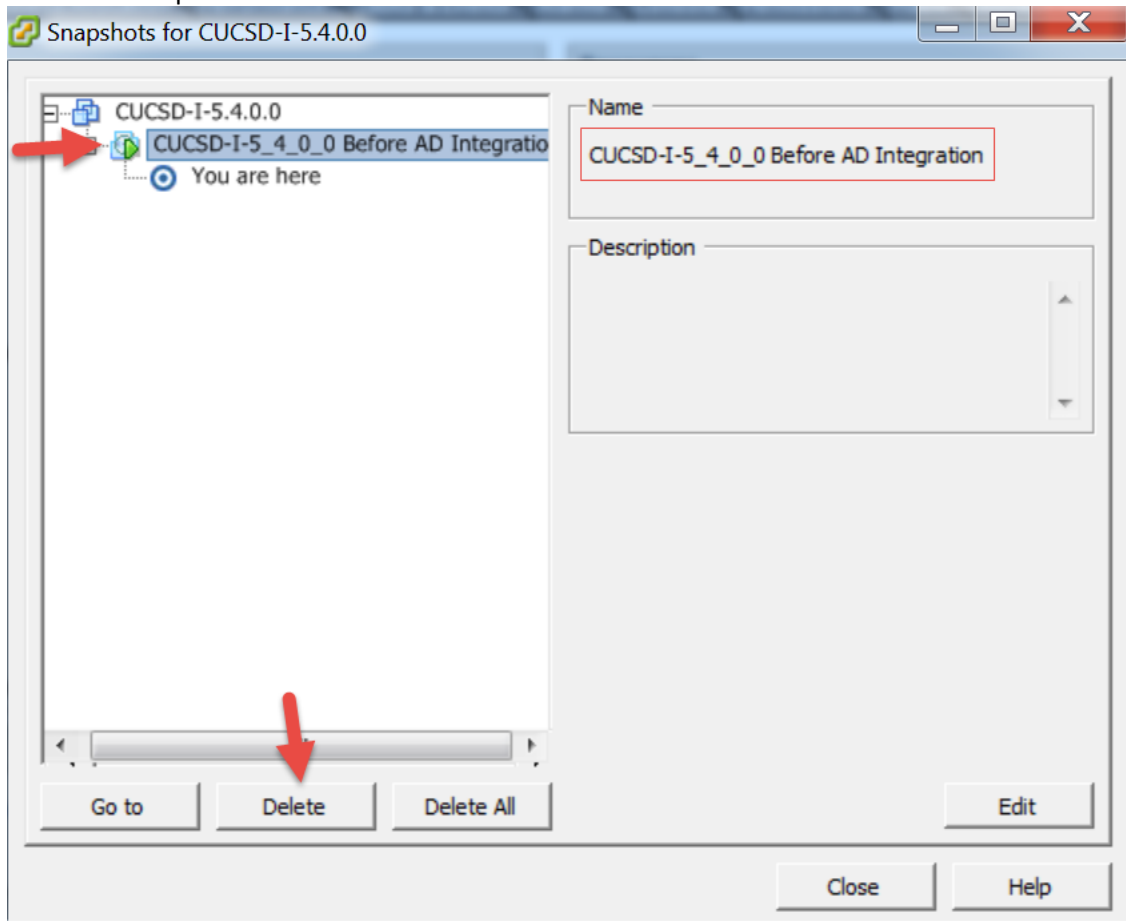
Click **'Yes'** to confirm the deletion then click **'Close'** to Close the Snapshot Manager.



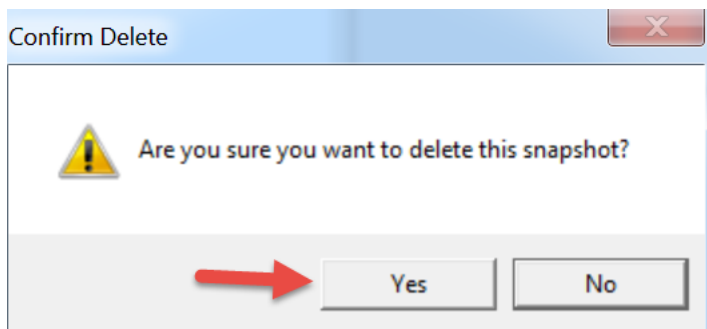
Remove the Inventory Database Node Snapshot. Log into your vCenter -> navigate to the Inventory Database Node VM ->right click on the VM -> Snapshot -> select '**Snapshot Manager**'. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



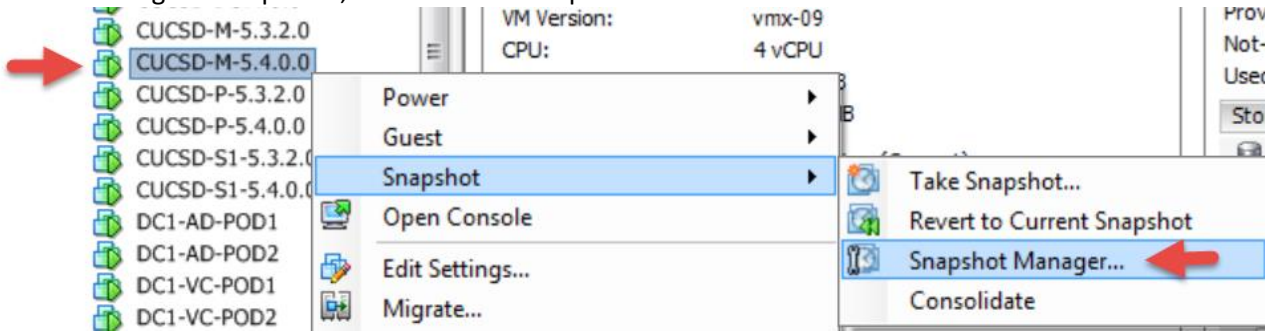
Select the Snapshot and click '**Delete**'.



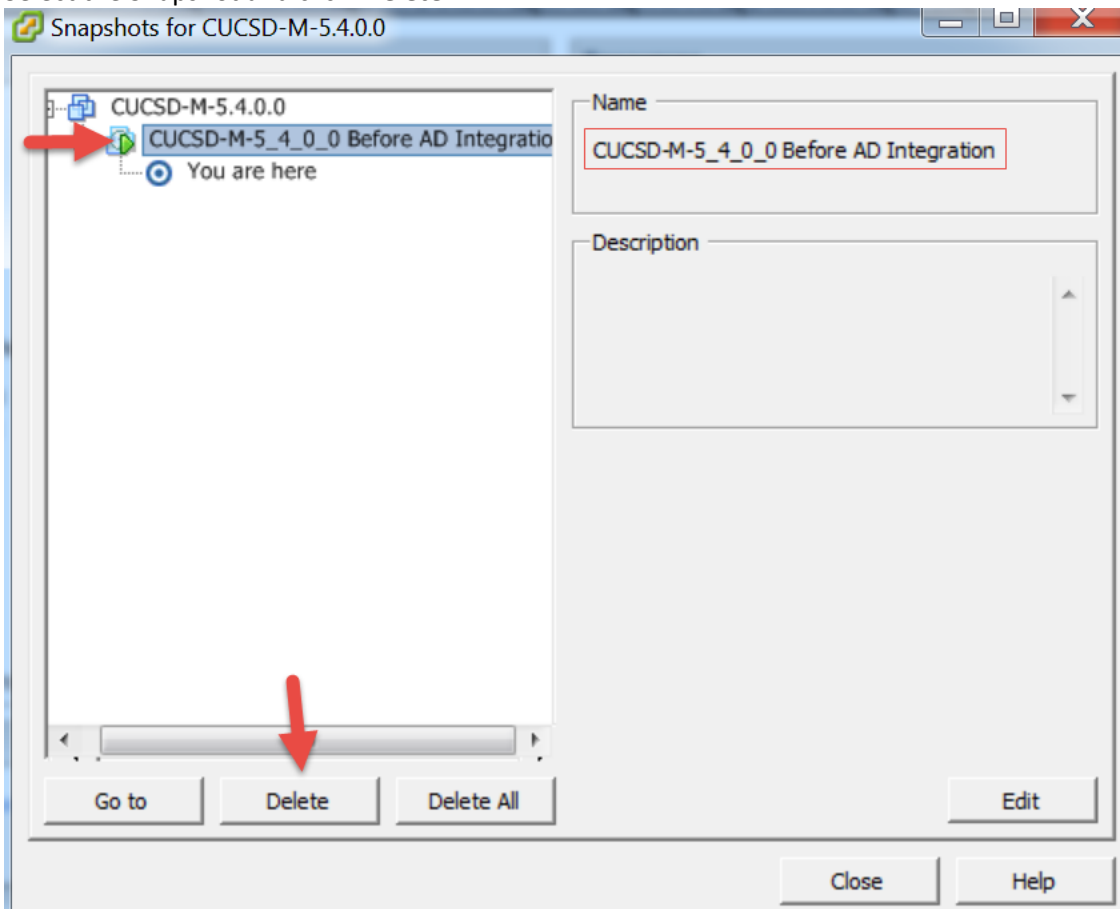
Click '**Yes**' to confirm the deletion then click '**Close**' to Close the Snapshot Manager.



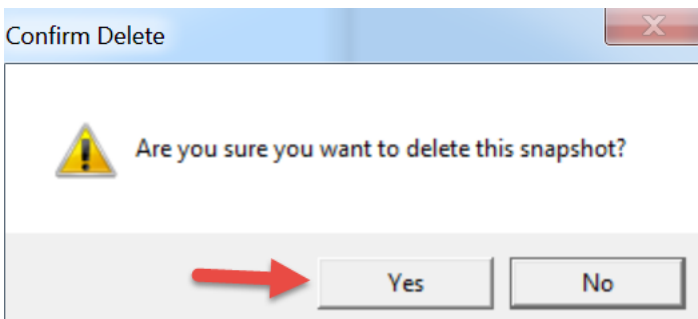
Remove the Monitoring Database Node Snapshot. Log into your vCenter -> navigate to the Monitoring Database Node VM ->right click on the VM -> Snapshot -> select '**Snapshot Manager**'. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



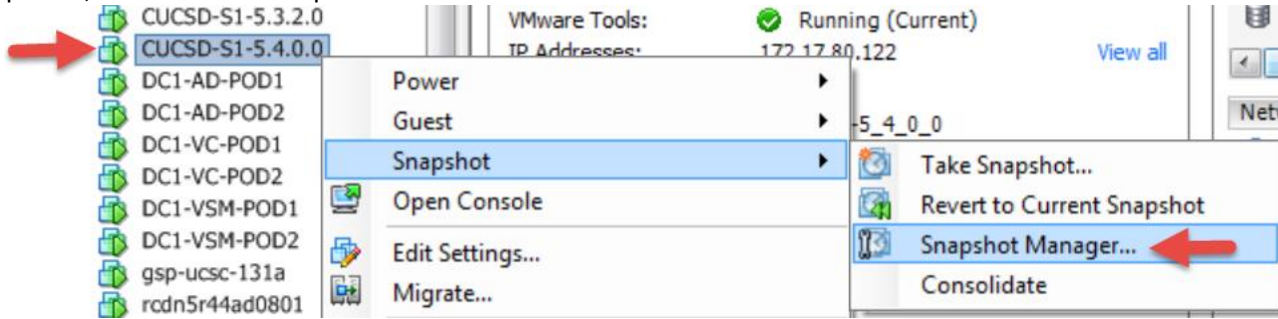
Select the Snapshot and click '**Delete**'.



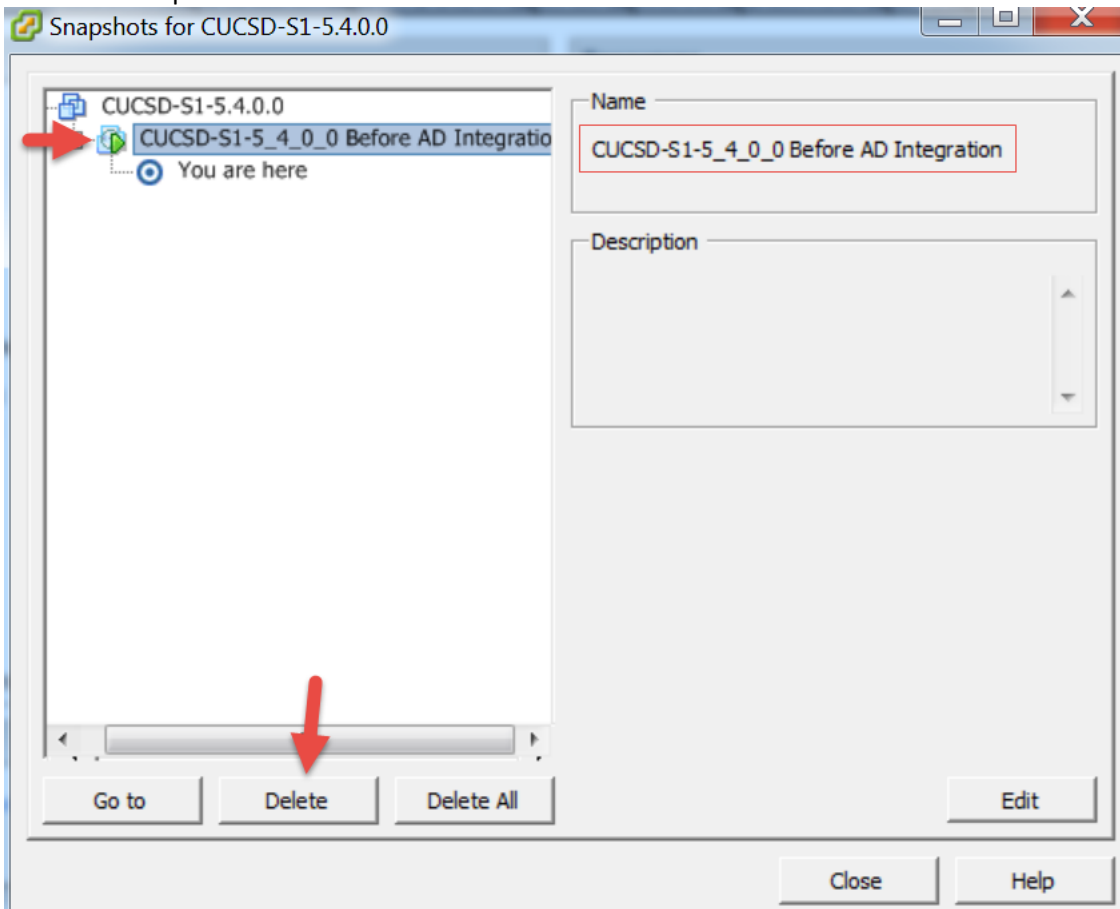
Click '**Yes**' to confirm the deletion then click '**Close**' to Close the Snapshot Manager.



Remove the Service Node Snapshot. Log into your vCenter -> navigate to the Service Node VM ->right click on the VM -> Snapshot -> select **'Snapshot Manager'**. **Note:** If you have the luxury of shutting down the VM before taking the Snapshots, this would be the preferred method.



Select the Snapshot and click **'Delete'**.



Click **'Yes'** to confirm the deletion then click **'Close'** to Close the Snapshot Manager.

