UCSM LDAP Troubleshooting guide

Contents

Introduction

This document provides information on validating the Lightweight Directory Access Protocol (LDAP) configuration on the Unified Computing System Manager (UCSM) and steps to investigate LDAP authentication failure issues.

Configuration Guides:

UCSM Configuring Authentication

Sample Active Directory (AD) Configuration

Verify UCSM LDAP configuration

Make sure UCSM has deployed the configuration successfully by checking the Finite State Machine (FSM) status and it shows completed at 100%.

From UCSM Command Line Interface (CLI) context

```
ucs # scope security
ucs /security # scope ldap
ucs /security/ldap # show configuration
ucs /security/ldap # show fsm status
```

From Nexus Operating System (NX-OS) CLI context

```
ucs # scope security
ucs(nxos)# show ldap-server
ucs(nxos)# show ldap-server groups
```

LDAP configuration best practices

1. Create additional authentication domains instead of changing "Native Authenitcation " realm

2. Always use local realm for 'console authentication', In case the user is locked out from using 'native authentication', admin would still be able to access it from console.

3. UCSM always fails back to local authentication if all the servers in given auth-domain failed to respond during login attempt (not applicable for test aaa command) .

Validating LDAP configuration

Test the LDAP authentication using NX-OS command. 'test aaa' command is available only from NX-OS CLI interface.

1. Validate LDAP group specific configuration.

The following command goes through list of all configured LDAP servers based on their configured order.

```
ucs(nxos)# test aaa group ldap <username> <password>
```

2. Validate specific LDAP server configuration

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
```

NOTE 1: <password> string will be displayed on the terminal.

NOTE 2: The LDAP server IP or FQDN must match a configured LDAP provider.

In this case, UCSM tests the authentication against specific server and can fail if there is no filter configured for the specified LDAP server.

Troubleshooting LDAP login failures

This section provides information on diagnosing LDAP authentication problems.

Problem scenario #1 - Cannot log in

Cannot login as LDAP user via both UCSM Graphical User Interface (GUI) and CLI

User receives **"Error authenticating to server"** while testing LDAP authentication.

```
(nxos)# test aaa server ldap <LDAP-server> <user-name> <password>
error authenticating to server
bind failed for <base DN>: Can't contact LDAP server
```

Recommendation

Verify network connectivity between LDAP server and Fabric Interconnect (FI) management interface by Internet Control Message Protocol (ICMP) ping and establishing telnet connection from local-mgmt context

```
ucs# connect local
ucs-local-mgmt # ping <LDAP server-IP-address OR FQDN>
ucs-local-mgmt # telnet <LDAP-Server-IP-Address OR FQDN> <port-number>
```

Investigate Internet Protocol (IP) network connectivity if UCSM cannot ping LDAP server or open telnet session to LDAP server.

Verify if Domain Name Service (DNS) returns correct IP address to UCS for LDAP server hostname and make sure that LDAP traffic is not blocked between these two devices.

Problem scenario #2 - Can log into GUI, cannot log into SSH

LDAP user can login via UCSM GUI but cannot open SSH session to FI.

Recommendation

When establishing SSH session to FI as LDAP user, UCSM requires " ucs- " to be prepended before LDAP domain-name

* From Linux / MAC machine

```
ssh ucs-<domain-name>\\<username>@<UCSM-IP-Address>
ssh -l ucs-<domain-name>\\<username> <UCSM-IP-address>
ssh <UCSM-IP-address> -l ucs-<domain-name>\\<username>
```

* From putty client

```
Login as: ucs-<domain-name>\<username>
```

NOTE: Domain name is case sensitive and should match the domain-name configured in UCSM. The maximum username length can be 32 chars which includes the domain name.

"ucs-<domain-name>\<user-name>" = 32 chars.

Problem scenario #3 - User has read-only privileges

LDAP user can login but has read-only privileges even though ldap-group maps are correctly configured in UCSM.

Recommendation
If no roles were retrieved during the LDAP login process,remote-user is either allowed with default-role (read only access) or denied access (no-login) to login to UCSM, based on the remote-login policy.

When remote-user logs-in and user was given read-only access, In that case verify the user group membership details in LDAP/AD.
For example, we can use ADSIEDIT utility for MS Active Directory. or ldapserach in case of Linux/Mac.

It can also be verified with " test aaa " command from NX-OS shell.

Problem scenario #4 - Cannot log in with 'Remote Authentication'

User cannot login or has read-only access to UCSM as remote user when " Native Authentication " was changed to remote authentication mechanism (LDAP etc)

Recommendation
As UCSM fallsback to local authentication for console access when it cannot reach remote authentication server, we can follow below steps to recover it.

1. Disconnect the mgmt interface cable of primary FI (show cluster state would indicate which is acting as Primary)
2. Connect to the console of the primary FI
3. Execute following commands to change the native authentication

```
scope security
show authentication
set authentication console local
set authentication default local
commit-buffer
```

4. Connect the mgmt interface cable
5. Login via UCSM using local account and create auth-domain for remote authentication (ex LDAP) group.

NOTE: Disconnecting the mgmt interface would NOT affect any data plane traffic.

Problem scenario #4 - LDAP Authentication works but not with SSL enabled

LDAP authentication is working fine without Secure Socket Layer (SSL) but fails when SSL option is enabled.

Recommendation
UCSM LDAP client uses the configured trust-points (Certificate Authority (CA) certificates) while establishing SSL connection.

1. Make sure the trust-point was configured correctly.

2. The identify field in cert should be the " hostname "of the LDAP server. Make sure the hostname configured in UCSM matches the hostname present in certificate and are valid.

3. Make sure UCSM is configured with 'hostname' not 'ipaddress' of the LDAP server and it is recheable from local-mgmt interface.

Problem scenario #5 - Authentication fails after LDAP provider changes

Authentication fails after deleting old LDAP server and adding new LDAP server

Recommendation
When LDAP is being used in authentication realm, deleting and adding of new servers is not permitted. From UCSM 2.1 version, it would result in FSM failure.

The steps to follow when removing/adding new servers in same transaction is

1. Make sure all the authentication realms using ldap are changed to local and saved the configuration.
2. Update the LDAP servers and verify that the FSM status has completed successfully.
3. Change the auth realms of domains modified in step 1, to LDAP.

For all other problem scenarios - Debugging LDAP

Turn on the debugs, attempt to login as LDAP user and gather following logs along with UCSM techsupport that captures failed login event.

1) Open a SSH session to FI and login as local user and change to NX-OS CLI context.

```
ucs # connect nxos
```

2) Enable following debug flags and save the SSH session output to log file.

```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug aaa aaa-requests

ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug ldap aaa-request-lowlevel
ucs(nxos)# debug ldap aaa-request
```

3) Now open a new GUI or CLI session and attempt to login as remote (LDAP) user
4) Once you received login failure message, **turn off the debugs.**

```
ucs(nxos)# undebug all
```

Packet capture of LDAP traffic

In scenarios where packet capture is required, Ethanalyzer can used to capture LDAP traffic between FI and LDAP server.

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host <LDAP-server-IP-address>"
detail limit-captured-frames 0 write /bootflash/sysdebug/diagnostics/test-ldap.pcap
```

In the above command, pcap file is saved under /workspace/diagnostics directory and can be retrieved from FI via local-mgmt CLI context

Above command can be used to capture packets for any remote (LDAP, TACACS, RADIUS) authenitcation traffic.
5. Relevant logs in UCSM techsupport bundle

In UCSM techsupport, relevant logs are located under **<FI>/var/sysmgr/sam_logs directory**

```
httpd.log
svc_sam_dcosAG
svc_sam_pamProxy.log

NX-OS commands or from <FI>/sw_techsupport log file

ucs-(nxos)# show system internal ldap event-history errors
ucs-(nxos)# show system internal ldap event-history msgs
ucs-(nxos)# show log
```

Known caveats

CSCth96721
rootdn of ldap server on sam should allow more than 128 characters

UCSM version earlier than 2.1 has limitation of 127 characters for base DN / bind DN string.

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

--------- snip ----------
The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters.

Issue is fixed in 2.1.1 and above release

CSCuf19514
LDAP daemon crashed

LDAP client may crash while initialising the ssl library if the ldap_start_tls_s call takes more than 60 secs to complete the initialisation. This could happen only incase of invalid DNS entry / delays in DNS resolution.

Take steps to address the DNS resolution delays and errors.