# UCSM LDAP-handleiding voor probleemoplossing

## Inhoud



## Inleiding

Dit document bevat informatie over het valideren van de lichtgewicht Directory Access Protocol (LDAP)-configuratie op de Unified Computing System Manager (UCSM) en stappen om kwesties met betrekking tot de authenticatie van de LMP te onderzoeken.

Configuratiehandleidingen:

UCSM-configuratie-verificatie

Configuratie van actieve map (AD) in voorbeelden

## Controleer de configuratie van UCSM LDAP

Zorg ervoor dat UCSM de configuratie met succes heeft uitgevoerd door de Finite State Machine (FSM) status te controleren en deze is voltooid op 100%.

Van CLI-context (UCSM Opdracht Line)

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

Van Nexus Operating System (NX-OS) CLI-context

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

### Best practices voor configuratie van LDAP

1. Maak aanvullende authenticatiedomeinen in plaats van het wijzigen van "Native Authentiation " - gebied

2. Gebruik altijd een lokaal domein voor 'console-authenticatie', indien de gebruiker niet op 'Eigen authenticatie' kan rekenen, kan admin het nog vanaf console gebruiken.

3. UCSM faalt altijd terug naar lokale authenticatie als alle servers in een bepaald auth-domein niet reageren tijdens inlogpoging (niet van toepassing voor testaaanopdracht).

## Validering van de LMP-configuratie

Test de LDAP-verificatie met NX-OS-opdracht. 'test aaa' opdracht is alleen beschikbaar via NX-OS CLI interface.

1. Valideren van de LDAP-groepsspecifieke configuratie.

De volgende opdracht wordt gegeven door een lijst van alle geconfigureerde LDAP-servers op basis van hun geconfigureerde volgorde.

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

2. Speciaal valideren van de LAN-serverconfiguratie

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

*LET OP 1: <password> string wordt weergegeven op de terminal.*

*OPMERKING 2: De IP- of FQDN-server-server moet overeenkomen met een geconfigureerde LDAP-provider.*

In dit geval test UCSM de authenticatie tegen een bepaalde server en kan deze falen als er geen filter is ingesteld voor de gespecificeerde LDAP server.

## Problemen oplossen bij inloggen van LDAP

Dit deel bevat informatie over het diagnosticeren van problemen met de authenticatie van de LGO.

## Probleemscenario #1 - Kan niet inloggen

Kan niet inloggen als LDAP-gebruiker via zowel UCSM Graphical User Interface (GUI) als CLI

Gebruiker ontvangt **"Fout bij authenticatie aan server"** tijdens testen van LDAP-verificatie.

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

### Aanbeveling

Controleer de netwerkconnectiviteit tussen de LDP-server en de Fabric Interconnect (FI)-beheerinterface door ICMP-ping (Internet Control Message Protocol) en het opzetten van een telnet-verbinding vanuit de lokale 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>
```

Onderzoek IP-netwerkconnectiviteit (Internet Protocol) als UCSM de LDAP-server niet kan typen of geen telnet-sessie kan openen naar de LDAP-server.

Controleer of Domain Name Service (DNS) het juiste IP-adres naar UCS teruggeeft voor de bestandsnaam van de server en zorg ervoor dat het LDAP-verkeer niet tussen deze twee apparaten wordt geblokkeerd.

## Probleemscenario #2 - Kan in GUI inloggen, kan niet in SSH inloggen

LDAP-gebruiker kan inloggen via UCSM GUI, maar kan geen SSH-sessie voor FI openen.

### Aanbeveling

Bij het opzetten van een SSH-sessie aan FI als LDAP-gebruiker, vereist UCSM dat " ucs-" wordt toegevoegd vóór de LDAP-domeinnaam

* Van 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>
```

* Van een putclient

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

*OPMERKING: De domeinnaam is hoofdlettergevoelig en zou aan de domeinnaam in UCSM moeten passen. De maximale gebruikersnaamlengte kan 32 tekens zijn die de domeinnaam bevatten.*

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

## Probleemscenario #3 - Gebruiker heeft alleen-lezen rechten

LDAP-gebruiker kan inloggen, maar heeft alleen-lezen rechten, ook al zijn de lijngroepkaarten correct ingesteld in UCSM.

### Aanbeveling

Als er tijdens het inlogproces van LDAP geen rollen zijn opgehaald, is de gebruiker op afstand ofwel standaard toegestaan (alleen lezen) of heeft hij geen toegang (geen-inlognaam) om in te loggen op UCSM, op basis van het beleid voor inloggen op afstand.

Wanneer de gebruiker op afstand inlogt en de gebruiker alleen-lezen toegang heeft gekregen, dient hij in dat geval de gegevens van de gebruikersgroep in de LDAP/AD te verifiëren.
We kunnen bijvoorbeeld ADSIEDIT-hulpprogramma gebruiken voor MS Active Directory. of ldapserach in het geval van Linux/Mac.

Kan ook worden geverifieerd met " test aaa " opdracht van NX-OS shell.

## Probleemscenario nr. 4 - Kan niet inloggen met 'Remote-verificatie'

Gebruiker kan niet inloggen of heeft alleen-lezen toegang tot UCSM als gebruiker op afstand wanneer "Native Authentication" is veranderd in een extern verificatiemechanisme (LDAP etc.)

### Aanbeveling

Aangezien UCSM terugval naar lokale authenticatie voor toegang tot console wanneer het niet kan bereiken van externe authenticatieserver, kunnen we onderstaande stappen volgen om het te herstellen.

1. Koppel de GMT-interfacekabel van primaire FI los (indien de clusterstaat van de show aangeeft welke lidstaat als Primair fungeert)
2. Sluit aan op de console van de primaire FI
3. Voer de volgende opdrachten uit om de oorspronkelijke verificatie te wijzigen

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

4. Sluit de verbindingskabel aan
5. Meld u aan via UCSM met behulp van een lokale account en creëer een AUTOMATISCH domein voor externe verificatie (ex LDAP).
*OPMERKING: Het loskoppelen van de GMT-interface heeft GEEN invloed op het vliegtuigverkeer.*

## Probleemscenario #4 - LDAP-verificatie werkt niet met SSL ingeschakeld

LDAP-verificatie werkt prima zonder Secure Socket Layer (SSL) maar faalt als SSL-optie is ingeschakeld.

### Aanbeveling

UCSM LDAP-client gebruikt de geconfigureerde trust-points (CA-certificaten) bij het opzetten van een SSL-verbinding.

1. Controleer of het trust-punt goed is geconfigureerd.

2. Het identificatieveld in cert moet de "hostname" van de LDAP-server zijn. Zorg ervoor dat de hostname die in UCSM is ingesteld, overeenkomt met de hostname die in het certificaat aanwezig is en geldig is.

3. Zorg ervoor dat UCSM wordt ingesteld met 'hostname' en niet 'ipaddress' van de LDAP server en dat deze herbruikbaar is vanuit de lokale GMT-interface.

## Probleemscenario nr. 5 - Verificatie mislukt na wijzigingen in de LMP-provider

Verificatie mislukt na het verwijderen van oude LDAP-server en het toevoegen van nieuwe LDAP-server

### Aanbeveling

Bij gebruik van LDAP in de echtheidscontrole is het verwijderen en toevoegen van nieuwe servers niet toegestaan. Van de UCSM 2.1 versie zal dit leiden tot een defect aan de FSM.

De te volgen stappen bij het verwijderen/toevoegen van nieuwe servers in dezelfde transactie zijn:

1. Controleer of alle verificatiegebieden die gebruik maken van ldap, lokaal zijn gewijzigd en de configuratie hebben opgeslagen.
2. update de LDAP-servers en controleer of de FSM-status met succes is voltooid.
3. Verander de automatische gebieden van in stap 1 gewijzigde domeinen naar LDAP.

## Voor alle andere probleemscenario's - Afluisteren van LDAP

Zet de debugs aan, probeer aan te loggen als LDAP-gebruiker en verzamel de volgende logbestanden samen met de UCSM-technische ondersteuning die de mislukte inloggebeurtenis opneemt.

1) Open een SSH-sessie voor FI en inloggen als lokale gebruiker en wijzig de context van NX-OS CLI.

```
ucs # connect nxos
```

2) Schakel de volgende debug-vlaggen in en bewaar de SSH-sessieuitvoer naar het logbestand.

```
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) Open nu een nieuwe GUI- of CLI-sessie en probeer u in te loggen als gebruiker op afstand (LDAP)
4) Nadat u een melding van een storing hebt ontvangen, **schakelt** u **de apparaten uit.**

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

### Packet-opname van LDAP-verkeer

In scenario's waarin pakketvastlegging is vereist, kan Ethanalyzer worden gebruikt om Ldap-verkeer tussen FI- en Ldap-server op te nemen.

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host
```

In de bovenstaande opdracht wordt het PPPpcap-bestand opgeslagen onder een directory/werkruimte/diagnostiek en kan het vanuit FI opgeroepen worden via een lokale CLI-context

Deze opdracht kan worden gebruikt om pakketten op te nemen voor elk afstandsbediening (LDAP, TACACS, RADIUS).
5. Relevante stammen in de technische ondersteuningsbundel van UCSM

In de technische ondersteuning van UCSM zijn relevante logbestanden te vinden onder **<FI>/var/sysmgr/sam_logs folder**

```
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
```

## Bekende uitzonderingen

CSCth96721
LAN-server op sam moet meer dan 128 tekens bevatten

UCSM versie eerder dan 2.1 heeft een beperking van 127 tekens voor basis 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

— knip —
De specifieke merknaam in de LDAP-hiërarchie waar de server zou moeten beginnen met een zoekopdracht wanneer een externe gebruiker inlogt en het systeem probeert om de DNA-naam van de gebruiker op basis van hun gebruikersnaam te krijgen. De maximum ondersteunde string

lengte is 127 tekens.
—

Uitgifte wordt vastgesteld in punt 2.1.1 en boven release

CSCuf19514
LDAP daemon crasht

LDAP client kan crashen tijdens het initialiseren van de ssl bibliotheek als de ldap_start_tls_s aanroep meer dan 60 seconden nodig heeft om de initialisatie te voltooien. Dit kan alleen gebeuren bij ongeldige DNS-ingang/vertragingen in de DNS-resolutie.

ondernemen stappen om de DNS-resolutie vertragingen en fouten aan te pakken.