UCSM LDAP故障排除指南

目錄

[簡介](#)
[驗證UCSM LDAP配置](#)
[LDAP配置最佳實踐](#)
[正在驗證LDAP配置](#)
[排除LDAP登入故障](#)
[問題方#1 — 無法登入](#)
[問題方#2 — 可以登入GUI，無法登入SSH](#)
[問題場景#3 — 使用者具有只讀許可權](#)
[問題方#4 — 無法使用「遠端身份驗證」登入](#)
[問題場景#4 - LDAP身份驗證工作正常，但是未啟用SSL](#)
[問題場景#5 - LDAP提供程式更改後身份驗證失敗](#)
[對於所有其他問題方案 — 調試LDAP](#)
[LDAP流量的資料包捕獲](#)
[已知警告](#)

簡介

本文檔提供有關在統一計算系統管理器(UCSM)上驗證輕量級目錄訪問協定(LDAP)配置的資訊，以及調查LDAP身份驗證失敗問題的步驟。

疑難排解技術筆記：

[UCSM配置身份驗證](#)

[Active Directory(AD)配置示例](#)

驗證UCSM LDAP配置

通過檢查有限狀態機(FSM)狀態，確保UCSM已成功部署配置，並且顯示配置已完成100%。

從UCSM命令列介面(CLI)上下文

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

從Nexus作業系統(NX-OS)CLI環境

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

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

LDAP配置最佳實踐

1.建立其他身份驗證域，而不是更改「本機身份驗證」領域

2.始終將本地領域用於「控制檯身份驗證」，如果使用者被鎖定為無法使用「本機身份驗證」，管理員仍可以從控制檯訪問它。

3.如果在登入嘗試期間，給定身份驗證域中的所有伺服器均無法響應（不適用於test aaa命令），則UCSM始終無法返回本地身份驗證。

正在驗證LDAP配置

使用NX-OS命令測試LDAP身份驗證。「test aaa」命令僅在NX-OS CLI介面中可用。

1.驗證LDAP組特定配置。

以下命令根據配置的LDAP伺服器的順序瀏覽所有已配置的LDAP伺服器的清單。

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

2.驗證特定的LDAP伺服器配置

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

附註1:<password>字串將顯示在終端上。

附註2:LDAP伺服器IP或FQDN必須與配置的LDAP提供程式匹配。

在這種情況下，UCSM會針對特定伺服器測試身份驗證，如果沒有為指定的LDAP伺服器配置過濾器，則可能會失敗。

排除LDAP登入故障

本節提供有關診斷LDAP身份驗證問題的資訊。

問題方#1 — 無法登入

無法通過UCSM圖形使用者介面(GUI)和CLI作為LDAP使用者登入

使用者在測**試LDAP身份驗證時收到**「Error authenticating to server」（向伺服器驗證時出錯）。

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

建議
通過網際網路控制消息協定(ICMP)ping和從本地管理上下文建立telnet連線，驗證LDAP伺服器和交換矩陣互聯(FI)管理介面之間的網路連線

```
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>
```
如果UCSM無法ping通LDAP伺服器或開啟與LDAP伺服器的telnet會話，請檢查Internet協定(IP)網路連線。

驗證域名服務(DNS)是否為LDAP伺服器主機名向UCS返回正確的IP地址，並確保這兩台裝置之間的LDAP流量未被阻止。

問題方#2 — 可以登入GUI，無法登入SSH

LDAP使用者可以通過UCSM GUI登入，但無法開啟到FI的SSH會話。

建議

當作為LDAP使用者建立與FI的SSH會話時，UCSM要求在LDAP域名之前預置「 ucs- 」

*從Linux/MAC電腦

```
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>
```

*來自putty客戶端

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

附註：域名區分大小寫，應該與UCSM中配置的域名匹配。最大使用者名稱長度可以是32個字元，其中包括域名。

"ucs-<domain-name>\<user-name>" = 32個字元。

問題場景#3 — 使用者具有只讀許可權

即使UCSM中正確配置了LDAP組對映，LDAP使用者可以登入，但擁有只讀許可權。

建議
如果在LDAP登入過程中未檢索到任何角色，則根據遠端登入策略，遠端使用者可以使用預設角色（只讀訪問）或拒絕訪問（無登入）登入到UCSM。

當遠端使用者登入且使用者被授予只讀訪問許可權時，在這種情況下，請驗證LDAP/AD中的使用者組成員身份詳細資訊。
例如，我們可以將ADSIEDIT實用程式用於MS Active Directory。或ldapserach。

也可使用NX-OS shell中的「test aaa」命令進行驗證。

問題方#4 — 無法使用「遠端身份驗證」登入

當「本機身份驗證」更改為遠端身份驗證機制（LDAP等）時，使用者無法作為遠端使用者登入或對UCSM具有只讀訪問許可權

建議
由於UCSM在無法到達遠端身份驗證伺服器時回退到本地身份驗證以進行控制檯訪問，我們可以按照以下步驟進行恢復。

1.斷開主FI的mgmt介面電纜（show cluster state將指示哪個充當主）
2.連線到主FI的控制檯
3.執行以下命令更改本機身份驗證

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

4.連線管理介面電纜
5.使用本地帳戶通過UCSM登入，並為遠端身份驗證（如LDAP）組建立身份驗證域。
附註：斷開管理介面不會影響任何資料平面流量。

問題場景#4 - LDAP身份驗證工作正常，但是未啟用SSL

LDAP身份驗證在沒有安全套接字層(SSL)的情況下工作正常，但在啟用SSL選項時失敗。

建議
UCSM LDAP客戶端在建立SSL連線時使用已配置的信任點(證書頒發機構(CA)證書)。

1.確保信任點配置正確。

2. cert中的identify欄位應該是LDAP伺服器的「 hostname 」。確保UCSM中配置的主機名與證書中的主機名匹配且有效。

3.確保UCSM配置為LDAP伺服器的「hostname」而不是「ipaddress」，並且可以從本地管理介面重新檢查。

問題場景#5 - LDAP提供程式更改後身份驗證失敗

刪除舊LDAP伺服器並新增新LDAP伺服器後，身份驗證失敗

建議
在身份驗證領域使用LDAP時，不允許刪除和新增新伺服器。從UCSM 2.1版本開始，它將導致FSM故障。

刪除/新增同一事務中的新伺服器時需遵循的步驟

1.確保使用ldap的所有身份驗證領域都更改為本地並儲存了配置。
2.更新LDAP伺服器並驗證FSM狀態是否已成功完成。
3.將步驟1中修改的域的身份驗證領域更改為LDAP。

對於所有其他問題方案 — 調試LDAP

開啟調試，嘗試以LDAP使用者身份登入，並收集以下日誌以及捕獲失敗登入事件的UCSM技術支援。

1)開啟與FI的SSH會話並以本地使用者身份登入，然後轉到NX-OS CLI上下文。

```
ucs # connect nxos
```

2)啟用以下調試標誌，並將SSH會話輸出儲存到日誌檔案。

```
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)現在開啟新的GUI或CLI會話，並嘗試以遠端(LDAP)使用者身份登入
4)收到登入失敗消息後，**關閉調試。**

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

LDAP流量的資料包捕獲

在需要捕獲資料包的情況下，Ethanalyzer可用於捕獲FI和LDAP伺服器之間的LDAP流量。

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

在上述命令中，pcap檔案儲存在/workspace/diagnostics目錄下，並可通過本地管理CLI上下文從FI中檢索

上述命令可用於捕獲任何遠端(LDAP、TACACS、RADIUS)身份驗證流量的資料包。
5. UCSM技術支援捆綁包中的相關日誌

在UCSM技術支援中，相關日誌位於**<FI>/var/sysmgr/sam_logs目錄下**

```
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
```

已知警告

CSCth96721
sam上的ldap伺服器的rootdn應允許超過128個字元

低於2.1的UCSM版本對基本DN/繫結DN字串具有127個字元的限制。

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 ----------
LDAP層次結構中的特定可分辨名稱，當遠端使用者登入且系統嘗試根據使用者的使用者名稱獲取使用者的DN時，伺服器應在此開始搜尋。支援的最大字串長度為127個字元。

2.1.1及更新版本中已修復此問題

CSCuf19514
LDAP守護程式崩潰

如果ldap_start_tls_s呼叫需要超過60秒才能完成初始化，則LDAP客戶端可能會在初始化ssl庫時崩潰。只有當DNS條目無效/DNS解析延遲時，才會發生這種情況。

採取措施解決DNS解析延遲和錯誤。