Leitfaden zur Fehlerbehebung für UCSM LDAP

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Validierung der LDAP-Konfiguration (Lightweight Directory Access Protocol) im Unified Computing System Manager (UCSM) sowie Schritte zur Untersuchung von Fehlern bei der LDAP-Authentifizierung.

Konfigurationsanleitungen:

Authentifizierung mit UCSM-Konfiguration

Beispiel für Active Directory (AD)-Konfiguration

Überprüfen der UCSM-LDAP-Konfiguration

Vergewissern Sie sich, dass UCSM die Konfiguration erfolgreich bereitgestellt hat, indem Sie den FSM-Status (Finite State Machine) überprüfen. Der Status wird mit 100 % abgeschlossen angezeigt.

Aus dem CLI-Kontext (UCSM Command Line Interface)

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

Über Nexus Operating System (NX-OS) CLI-Kontext

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

Best Practices für die LDAP-Konfiguration

1. Erstellen Sie zusätzliche Authentifizierungsdomänen, anstatt den Bereich "Native Authenitation" zu ändern.

2. Verwenden Sie für die Konsolenauthentifizierung immer den lokalen Bereich. Falls der Benutzer nicht die 'native Authentifizierung' verwendet, kann der Administrator trotzdem von der Konsole aus darauf zugreifen.

3. UCSM schlägt immer bei der lokalen Authentifizierung fehl, wenn alle Server in der angegebenen Authentifizierungsdomäne während des Anmeldeversuchs nicht reagieren konnten (nicht anwendbar für den Test aaa-Befehl).

Überprüfen der LDAP-Konfiguration

Testen Sie die LDAP-Authentifizierung mit dem NX-OS-Befehl. Der Befehl 'test aaa' ist nur über die CLI-Schnittstelle von NX-OS verfügbar.

1. Validieren Sie die LDAP-Gruppenkonfiguration.

Der folgende Befehl führt die Liste aller konfigurierten LDAP-Server anhand der konfigurierten Reihenfolge durch.

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

2. Bestimmte LDAP-Serverkonfiguration validieren

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

HINWEIS 1: Die Zeichenfolge <password> wird im Terminal angezeigt.

HINWEIS 2: Die IP- oder FQDN des LDAP-Servers muss mit einem konfigurierten LDAP-Anbieter übereinstimmen.

In diesem Fall testet UCSM die Authentifizierung anhand eines bestimmten Servers und kann fehlschlagen, wenn kein Filter für den angegebenen LDAP-Server konfiguriert ist.

Fehlerbehebung bei LDAP-Anmeldefehlern

Dieser Abschnitt enthält Informationen zur Diagnose von LDAP-Authentifizierungsproblemen.

Problemszenario 1: Anmeldung nicht möglich

Anmeldung als LDAP-Benutzer über die grafische Benutzeroberfläche (GUI) und Kommandozeile von UCSM nicht möglich

Beim Testen der LDAP-Authentifizierung erhält der Benutzer **"Fehler bei Serverauthentifizierung"**.

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

Empfehlung

Überprüfen der Netzwerkverbindung zwischen dem LDAP-Server und der Verwaltungsschnittstelle des Fabric Interconnects (FI) mithilfe des ICMP-Pings (Internet Control Message Protocol) und Einrichten einer Telnet-Verbindung vom lokalen Mgmt-Kontext aus

```
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>
```

Prüfen Sie die IP-Netzwerkverbindung (Internet Protocol), wenn UCSM den LDAP-Server nicht pingen oder Telnet-Sitzungen mit dem LDAP-Server öffnen kann.

Überprüfen Sie, ob der DNS (Domain Name Service) die richtige IP-Adresse für den Hostnamen des LDAP-Servers an das UCS zurückgibt, und stellen Sie sicher, dass der LDAP-Datenverkehr zwischen diesen beiden Geräten nicht blockiert wird.

Problemszenario 2 - Anmeldung bei GUI nicht möglich bei SSH

LDAP-Benutzer können sich über die UCSM-GUI anmelden, können jedoch keine SSH-Sitzung mit FI öffnen.

Empfehlung

Beim Einrichten einer SSH-Sitzung mit FI als LDAP-Benutzer muss UCSM " ucs- " vor dem LDAP-Domänennamen vorgezogen werden.

* Vom Linux-/MAC-System

```
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>
```

* Von putty client

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

HINWEIS: Beim Domänennamen wird die Groß- und Kleinschreibung beachtet, und er muss mit

dem in UCSM konfigurierten Domänennamen übereinstimmen. Die maximale Länge für Benutzernamen kann 32 Zeichen betragen, die den Domänennamen enthalten.

"ucs-<Domänenname>\<Benutzername>" = 32 Zeichen.

Problemszenario 3 - Benutzer hat schreibgeschützte Berechtigungen

Der LDAP-Benutzer kann sich anmelden, verfügt aber über schreibgeschützte Berechtigungen, auch wenn LDAP-Gruppenzuordnungen in UCSM korrekt konfiguriert sind.

Empfehlung

Wenn während des LDAP-Anmeldeprozesses keine Rollen abgerufen wurden, ist der Remote-Benutzer entweder mit der Standardrolle (schreibgeschützter Zugriff) oder mit dem verweigerten Zugriff (keine Anmeldung) zur Anmeldung bei UCSM zugelassen, basierend auf der Richtlinie für die Remote-Anmeldung.

Wenn sich der Remote-Benutzer anmeldet und dem Benutzer Lesezugriff gewährt wurde, überprüfen Sie in diesem Fall die Details zur Benutzergruppenmitgliedschaft im LDAP/AD. Beispielsweise können wir das ADSIEDIT-Dienstprogramm für MS Active Directory verwenden. oder ldapserach im Fall von Linux/Mac.

Sie kann auch mit dem Befehl " test aaa " in der NX-OS-Shell verifiziert werden.

Problemszenario 4 - Anmeldung mit "Remote Authentication" nicht möglich

Benutzer kann sich nicht anmelden oder hat nur Lesezugriff auf UCSM als Remote-Benutzer, wenn "Native Authentication" auf einen Remote-Authentifizierungsmechanismus (LDAP usw.) geändert wurde.

Empfehlung

Da UCSM auf die lokale Authentifizierung für den Konsolenzugriff zurückgreift, wenn der Remote-Authentifizierungsserver nicht erreicht werden kann, können wir die folgenden Schritte ausführen, um ihn wiederherzustellen.

1. Trennen Sie das Management-Schnittstellenkabel des primären FI (der Cluster-Status zeigt an, welcher als primär agiert).
2. Herstellen einer Verbindung zur Konsole des primären FI
3. Führen Sie folgende Befehle aus, um die systemeigene Authentifizierung zu ändern

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

4. Verbinden Sie das Management-Schnittstellenkabel.
5. Melden Sie sich über das UCSM mit dem lokalen Konto an, und erstellen Sie eine Authentifizierungsdomäne für die Remote-Authentifizierungsgruppe (ex LDAP).
HINWEIS: Das Trennen der Mgmt-Schnittstelle würde KEINEN Datenverkehr auf Datenebene beeinträchtigen.

Problemszenario 4: LDAP-Authentifizierung funktioniert, aber nicht mit SSL aktiviert

Die LDAP-Authentifizierung funktioniert ohne SSL (Secure Socket Layer), schlägt aber fehl, wenn die SSL-Option aktiviert ist.

Empfehlung

Der UCSM LDAP-Client verwendet die konfigurierten Vertrauenspunkte (CA-Zertifikate) beim Herstellen einer SSL-Verbindung.

1. Stellen Sie sicher, dass der Vertrauensbereich korrekt konfiguriert wurde.

2. Das Identifikationsfeld in cert sollte der " Hostname "des LDAP-Servers sein. Stellen Sie sicher, dass der in UCSM konfigurierte Hostname mit dem im Zertifikat vorhandenen Hostnamen übereinstimmt und gültig ist.

3. Stellen Sie sicher, dass UCSM mit 'hostname' und nicht 'ipaddress' des LDAP-Servers konfiguriert ist und von der lokalen Verwaltungsschnittstelle wiederhergestellt werden kann.

Problemszenario 5: Authentifizierung schlägt fehl, nachdem der LDAP-Anbieter geändert wurde

Die Authentifizierung schlägt fehl, nachdem der alte LDAP-Server gelöscht und der neue LDAP-Server hinzugefügt wurde.

Empfehlung

Wenn LDAP im Authentifizierungsbereich verwendet wird, ist das Löschen und Hinzufügen neuer Server nicht zulässig. Ab UCSM 2.1-Version würde FSM-Fehler auftreten.

Beim Entfernen/Hinzufügen neuer Server in derselben Transaktion müssen folgende Schritte ausgeführt werden:

1. Stellen Sie sicher, dass alle Authentifizierungsbereiche, die ldap verwenden, auf lokal geändert und die Konfiguration gespeichert werden.
2. Aktualisieren Sie die LDAP-Server, und überprüfen Sie, ob der FSM-Status erfolgreich abgeschlossen wurde.
3. Ändern Sie die Authentifizierungsbereiche der in Schritt 1 geänderten Domänen in LDAP.

Für alle anderen Problemszenarien - Debuggen von LDAP

Aktivieren Sie die Debugging-Funktion, versuchen Sie, sich als LDAP-Benutzer anzumelden, und sammeln Sie die folgenden Protokolle zusammen mit der UCSM-Technologie, die das fehlgeschlagene Anmeldeereignis erfasst.

1) Öffnen Sie eine SSH-Sitzung mit FI, melden Sie sich als lokaler Benutzer an, und wechseln Sie in den NX-OS CLI-Kontext.

```
ucs # connect nxos
```

2) Aktivieren Sie die folgenden Debug-Flags, und speichern Sie die Ausgabe der SSH-Sitzung in der Protokolldatei.

```
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) Öffnen Sie jetzt eine neue GUI- oder CLI-Sitzung, und versuchen Sie, sich als Remote-Benutzer (LDAP) anzumelden.
4) Wenn Sie die Meldung eines Anmeldefehlers erhalten haben, **deaktivieren Sie die Debugging-Funktion.**

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

Paketerfassung von LDAP-Datenverkehr

In Szenarien, in denen die Paketerfassung erforderlich ist, kann der Ethanalyzer zum Erfassen des LDAP-Datenverkehrs zwischen FI und LDAP-Server verwendet werden.

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

Mit dem obigen Befehl wird die pcap-Datei im Verzeichnis /workspace/diagnostics gespeichert und kann über den CLI-Kontext für lokales Management aus dem FI abgerufen werden.

Der obige Befehl kann verwendet werden, um Pakete für jeden Remote-Authentifizierungsverkehr (LDAP, TACACS, RADIUS) zu erfassen.
5. Relevante Protokolle im UCSM-Technologie-Supportpaket

Im UCSM-Technologiesupport befinden sich die relevanten Protokolle im **<FI>/var/sysmgr/sam_logs-Verzeichnis.**

```
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
```

Bekannte Vorbehalte

CSCth96721
Der LDAP-Server-Root sollte mehr als 128 Zeichen enthalten.

Die UCSM-Version vor 2.1 hat eine Beschränkung von 127 Zeichen für die Basis-DN/Binding-DN-Zeichenfolge.

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 —
Der spezielle DN in der LDAP-Hierarchie, unter dem der Server eine Suche starten soll, wenn sich ein Remote-Benutzer anmeldet und das System versucht, die DN des Benutzers auf Basis seines Benutzernamens abzurufen. Die maximal unterstützte Zeichenfolgenlänge ist 127 Zeichen.
—

Problem in Version 2.1.1 und höher behoben

CSCuf19514
LDAP-Daemon abgestürzt

Der LDAP-Client kann bei der Initialisierung der SSL-Bibliothek abstürzen, wenn der Aufruf von ldap_start_tls_s mehr als 60 Sekunden in Anspruch nimmt, um die Initialisierung abzuschließen. Dies kann nur bei ungültigen DNS-Eingaben/Verzögerungen bei der DNS-Auflösung der Fall sein.

Gehen Sie wie folgt vor, um Verzögerungen und Fehler bei der DNS-Auflösung zu beheben.