Guida alla risoluzione dei problemi di UCSM LDAP

Sommario

Introduzione

In questo documento vengono fornite informazioni sulla convalida della configurazione del protocollo LDAP (Lightweight Directory Access Protocol) in Unified Computing System Manager (UCSM) e vengono illustrati i problemi relativi agli errori di autenticazione LDAP.

Guide alla configurazione:

[UCSM: configurazione dell'autenticazione](#)

[Esempio di configurazione di Active Directory (AD)](#)

Verifica della configurazione LDAP UCSM

Verificare che UCSM abbia distribuito la configurazione correttamente controllando lo stato della macchina a stati finiti (FSM) e che risulti completato al 100%.

Dal contesto UCSM Command Line Interface (CLI)

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

Dal contesto CLI di Nexus Operating System (NX-OS)

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

Procedure ottimali per la configurazione LDAP

1. Creare domini di autenticazione aggiuntivi anziché modificare l'area di autenticazione "Autenticazione nativa"

2. Utilizza sempre l'area di autenticazione locale per l'autenticazione della console. Se l'utente non può utilizzare l'autenticazione nativa, l'amministratore potrà comunque accedervi dalla console.

3. UCSM esegue sempre il failback all'autenticazione locale se tutti i server in un determinato dominio di autenticazione non rispondono durante il tentativo di accesso (non applicabile per il comando test aaa).

Convalida della configurazione LDAP

Verificare l'autenticazione LDAP utilizzando il comando NX-OS. il comando 'test aaa' è disponibile solo dall'interfaccia CLI di NX-OS.

1. Convalidare la configurazione specifica del gruppo LDAP.

Il comando seguente esamina l'elenco di tutti i server LDAP configurati in base all'ordine di configurazione.

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

2. Convalida configurazione server LDAP specifica

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

NOTA 1: Sul terminale verrà visualizzata la stringa <password>.

NOTA 2: L'IP o l'FQDN del server LDAP deve corrispondere a un provider LDAP configurato.

In questo caso, UCSM verifica l'autenticazione rispetto a un server specifico e può non riuscire se non è configurato alcun filtro per il server LDAP specificato.

Risoluzione dei problemi relativi agli errori di login LDAP

In questa sezione vengono fornite informazioni sulla diagnosi dei problemi di autenticazione

LDAP.

Scenario con problemi 1: impossibile accedere

Impossibile accedere come utente LDAP tramite l'interfaccia grafica (GUI) e la CLI di UCSM

L'utente riceve **"Error authentication to server"** durante la verifica dell'autenticazione LDAP.

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

Suggerimento

Verificare la connettività di rete tra il server LDAP e l'interfaccia di gestione Fabric Interconnect (FI) eseguendo il ping Internet Control Message Protocol (ICMP) e stabilire una connessione telnet dal contesto di gestione locale

```
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>
```

Verificare la connettività di rete IP (Internet Protocol) se UCSM non è in grado di eseguire il ping tra il server LDAP o aprire una sessione telnet e il server LDAP.

Verificare che DNS (Domain Name Service) restituisca a UCS l'indirizzo IP corretto per il nome host del server LDAP e accertarsi che il traffico LDAP tra questi due dispositivi non sia bloccato.

Scenario del problema n. 2 - Possibilità di accedere alla GUI, impossibile accedere al protocollo SSH

L'utente LDAP può eseguire l'accesso tramite l'interfaccia GUI di UCSM ma non può aprire la sessione SSH su FI.

Suggerimento

Quando si stabilisce una sessione SSH per FI come utente LDAP, UCSM richiede che " ucs- " sia anteposto al nome di dominio LDAP

* Da macchina Linux / MAC

```
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>
```

* Da client putty

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

NOTA: Il nome di dominio fa distinzione tra maiuscole e minuscole e deve corrispondere al nome di dominio configurato in UCSM. La lunghezza massima del nome utente può essere di 32 caratteri, incluso il nome del dominio.

"ucs-<nome-dominio>\<nome-utente>" = 32 caratteri.

Scenario problema n. 3 - L'utente dispone di privilegi di sola lettura

L'utente LDAP può eseguire l'accesso ma dispone di privilegi di sola lettura anche se le mappe del gruppo LDAP sono configurate correttamente in UCSM.

Suggerimento

Se durante il processo di accesso LDAP non è stato recuperato alcun ruolo, all'utente remoto è consentito l'accesso a UCSM con ruolo predefinito (accesso in sola lettura) o accesso negato (nessun accesso) in base al criterio di accesso remoto.

Quando l'utente remoto esegue l'accesso e l'utente dispone di accesso in sola lettura, verificare i dettagli di appartenenza al gruppo di utenti in LDAP/AD.
Ad esempio, è possibile utilizzare l'utilità ADSIEDIT per MS Active Directory. o ldapsearch in caso di Linux/Mac.

Èinoltre possibile verificarlo con il comando " test aaa " dalla shell di NX-OS.

Scenario del problema n. 4 - Impossibile accedere con 'Autenticazione remota'

L'utente non può accedere o ha accesso in sola lettura a UCSM come utente remoto quando " Autenticazione nativa " è stato modificato in meccanismo di autenticazione remota (LDAP e così via)

Suggerimento

Poiché UCSM torna all'autenticazione locale per l'accesso alla console quando non è in grado di raggiungere il server di autenticazione remota, è possibile eseguire la procedura seguente per ripristinarlo.

1. Scollegare il cavo dell'interfaccia di gestione dell'infrastruttura primaria (il comando show cluster state indica quale cavo funziona come primario)
2. Connettersi alla console dell'FI principale
3. Eseguire i seguenti comandi per modificare l'autenticazione nativa

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

4. Collegare il cavo dell'interfaccia di gestione
5. Accedere tramite UCSM utilizzando un account locale e creare un dominio di autenticazione per il gruppo di autenticazione remota (ad esempio LDAP).
NOTA: La disconnessione dell'interfaccia di gestione NON influisce sul traffico del piano dati.

Scenario di problema 4: l'autenticazione LDAP funziona ma non con SSL abilitato

L'autenticazione LDAP funziona correttamente senza SSL (Secure Sockets Layer), ma ha esito negativo quando l'opzione SSL è abilitata.

Suggerimento

Il client LDAP UCSM utilizza i trust point configurati (certificati CA) durante la creazione della connessione SSL.

1. Verificare che il trust-point sia stato configurato correttamente.

2. Il campo di identificazione nel certificato deve essere il " nomehost "del server LDAP. Verificare che il nome host configurato in UCSM corrisponda al nome host presente nel certificato e che sia valido.

3. Verificare che UCSM sia configurato con 'hostname' diverso da 'ipaddress' del server LDAP e che sia recuperabile dall'interfaccia di gestione locale.

Scenario di problema n. 5 - Autenticazione non riuscita dopo la modifica del provider LDAP

Autenticazione non riuscita dopo l'eliminazione del server LDAP precedente e l'aggiunta di un nuovo server LDAP

Suggerimento

Quando si utilizza LDAP nel realm di autenticazione, non è consentito eliminare e aggiungere nuovi server. A partire dalla versione UCSM 2.1, si verificherebbe un fallimento degli FSM.

La procedura da seguire quando si rimuovono/aggiungono nuovi server nella stessa transazione è

1. Verificare che tutti i realm di autenticazione che utilizzano LDAP siano stati modificati in locale e salvati nella configurazione.
2. Aggiornare i server LDAP e verificare che lo stato FSM sia stato completato correttamente.
3. Modificare i realm di autenticazione dei domini modificati nel passo 1 in LDAP.

Per tutti gli altri scenari di problemi - Debug di LDAP

Attivare i debug, tentare di accedere come utente LDAP e raccogliere i seguenti log insieme al supporto tecnico UCSM che acquisisce l'evento di accesso non riuscito.

1) Aprire una sessione SSH su FI e accedere come utente locale e passare al contesto CLI di NX-OS.

```
ucs # connect nxos
```

2) Abilitare i seguenti flag di debug e salvare l'output della sessione SSH nel file di log.

```
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) Aprire una nuova sessione GUI o CLI e tentare di accedere come utente remoto (LDAP)
4) Una volta ricevuto il messaggio di errore di login, **disattivare i debug.**

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

Acquisizione pacchetti del traffico LDAP

Negli scenari in cui è richiesta l'acquisizione di pacchetti, Ethanalyzer può essere utilizzato per acquisire il traffico LDAP tra FI e il server LDAP.

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

Nel comando precedente, il file pcap viene salvato nella directory /workspace/diagnostics e può essere recuperato da FI tramite il contesto CLI local-mgmt

Il comando precedente può essere usato per acquisire pacchetti per qualsiasi traffico di autenticazione remoto (LDAP, TACACS, RADIUS).
5. Log pertinenti nel pacchetto di supporto tecnico UCSM

Nel supporto tecnico per UCSM, i log rilevanti si trovano nella **directory <FI>/var/sysmgr/sam_logs**

```
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
```

Avvertenze note

CSCth96721
la radice del server ldap su sam deve consentire più di 128 caratteri

La versione UCSM precedente alla 2.1 prevede un limite di 127 caratteri per il DN di base/stringa DN di binding.

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

— cattura —

Il nome distinto specifico nella gerarchia LDAP in cui il server deve iniziare una ricerca quando un utente remoto esegue l'accesso e il sistema tenta di ottenere il DN dell'utente in base al nome utente. La lunghezza massima supportata per la stringa è di 127 caratteri.
—

Il problema è risolto nella release 2.1.1 e successive

CSCuf19514
Arresto anomalo del daemon LDAP

Il client LDAP può bloccarsi durante l'inizializzazione della libreria ssl se la chiamata ldap_start_tls_s richiede più di 60 secondi per completare l'inizializzazione. Ciò può verificarsi solo in caso di voce DNS non valida o ritardi nella risoluzione DNS.

Adottare misure per risolvere i ritardi e gli errori di risoluzione DNS.