Guide de dépannage UCSM LDAP

Table des matières

Introduction

Ce document fournit des informations sur la validation de la configuration LDAP (Lightweight Directory Access Protocol) sur le Unified Computing System Manager (UCSM) et des étapes pour examiner les problèmes d'échec d'authentification LDAP.

Guides de configuration :

Configuration de l'authentification UCSM

Exemple de configuration d'Active Directory (AD)

Vérification de la configuration UCSM LDAP

Assurez-vous que UCSM a déployé la configuration avec succès en vérifiant l'état FSM (Finite State Machine) et qu'elle est terminée à 100 %.

À partir du contexte de l'interface de ligne de commande UCSM

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

À partir du contexte CLI Nexus Operating System (NX-OS)

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

Meilleures pratiques de configuration LDAP

1. Créez des domaines d'authentification supplémentaires au lieu de modifier le domaine « Authentification native »

2. Utilisez toujours le domaine local pour l'« authentification de console ». Si l'utilisateur n'est pas autorisé à utiliser l'« authentification native », l'administrateur peut toujours y accéder à partir de la console.

3. UCSM revient toujours à l'authentification locale si tous les serveurs dans un domaine d'authentification donné n'ont pas répondu pendant la tentative de connexion (non applicable pour la commande test aaa).

Validation de la configuration LDAP

Testez l'authentification LDAP à l'aide de la commande NX-OS. La commande « test aaa » est disponible uniquement à partir de l'interface CLI de NX-OS.

1. Validez la configuration spécifique au groupe LDAP.

La commande suivante parcourt la liste de tous les serveurs LDAP configurés en fonction de leur ordre de configuration.

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

2. Validez la configuration spécifique du serveur LDAP

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

REMARQUE 1 : la chaîne **<password>** s'affiche sur le terminal.

REMARQUE 2 : l'adresse IP ou le nom de domaine complet du serveur LDAP doit correspondre à un fournisseur LDAP configuré.

Dans ce cas, UCSM teste l'authentification par rapport à un serveur spécifique et peut échouer si aucun filtre n'est configuré pour le serveur LDAP spécifié.

Dépannage des échecs de connexion LDAP

Cette section fournit des informations sur le diagnostic des problèmes d'authentification LDAP.

Scénario de problème #1 - Connexion impossible

Impossible de se connecter en tant qu'utilisateur LDAP via l'interface utilisateur graphique UCSM et l'interface de ligne de commande

L'utilisateur reçoit "Erreur d'authentification auprès du serveur" lors du test de l'authentification 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
```

Recommandation
Vérifier la connectivité réseau entre le serveur LDAP et l'interface de gestion Fabric Interconnect (FI) par ping ICMP (Internet Control Message Protocol) et établir une connexion Telnet à partir du contexte de gestion 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>
```

Étudiez la connectivité réseau IP (Internet Protocol) si UCSM ne peut pas envoyer de requête ping au serveur LDAP ou ouvrir une session Telnet vers le serveur LDAP.

Vérifiez si le service de noms de domaine (DNS) renvoie l'adresse IP correcte à UCS pour le nom d'hôte du serveur LDAP et assurez-vous que le trafic LDAP n'est pas bloqué entre ces deux

périphériques.

Scénario de problème #2 - Peut se connecter à l'interface utilisateur graphique, ne peut pas se connecter à SSH

L'utilisateur LDAP peut se connecter via l'interface utilisateur graphique UCSM, mais ne peut pas ouvrir de session SSH vers FI.

Recommandation

Lors de l'établissement d'une session SSH vers FI en tant qu'utilisateur LDAP, UCSM nécessite que « ucs- » soit ajouté avant le nom de domaine LDAP

* À partir d'une machine 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>
```

* Du client mastic

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

REMARQUE : le nom de domaine est sensible à la casse et doit correspondre au nom de domaine configuré dans UCSM. La longueur maximale du nom d'utilisateur peut être de 32 caractères, ce qui inclut le nom de domaine.

"ucs-<nom-domaine>\<nom-utilisateur>" = 32 caractères.

Scénario de problème #3 - L'utilisateur dispose de privilèges en lecture seule

L'utilisateur LDAP peut se connecter mais dispose de privilèges en lecture seule, même si les mappages de groupe ldap sont correctement configurés dans UCSM.

Recommandation

Si aucun rôle n'a été récupéré pendant le processus de connexion LDAP, remote-user est autorisé avec default-role (accès en lecture seule) ou refusé (no-login) à se connecter à UCSM, en

fonction de la stratégie de connexion à distance.

Lorsque l'utilisateur distant se connecte et que l'utilisateur a reçu un accès en lecture seule, dans ce cas, vérifiez les détails d'appartenance au groupe d'utilisateurs dans LDAP/AD.
Par exemple, nous pouvons utiliser l'utilitaire ADSIEDIT pour MS Active Directory. ou ldapserach dans le cas de Linux/Mac.

Elle peut également être vérifiée à l'aide de la commande « test aaa » du shell NX-OS.

Scénario de problème #4 - Impossible de se connecter avec 'Authentification à distance'

L'utilisateur ne peut pas se connecter ou dispose d'un accès en lecture seule à UCSM en tant qu'utilisateur distant lorsque l'« authentification native » a été remplacée par un mécanisme d'authentification à distance (LDAP, etc.)

Recommandation
Comme UCSM revient à l'authentification locale pour l'accès à la console lorsqu'il ne peut pas atteindre le serveur d'authentification distant, nous pouvons suivre les étapes ci-dessous pour le récupérer.

1. Débranchez le câble d'interface de gestion de l'interface principale (la commande show cluster state indique laquelle agit en tant qu'interface principale)
2. Connectez-vous à la console de l'interface FI principale
3. Exécutez les commandes suivantes pour modifier l'authentification native

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

4. Branchez le câble d'interface de gestion
5. Connectez-vous via UCSM à l'aide d'un compte local et créez un domaine d'authentification pour le groupe d'authentification à distance (ex LDAP).
REMARQUE : la déconnexion de l'interface de gestion n'affecterait PAS le trafic du plan de données.

Scénario de problème #4 - L'authentification LDAP fonctionne mais pas avec SSL activé

L'authentification LDAP fonctionne correctement sans SSL (Secure Socket Layer), mais échoue

lorsque l'option SSL est activée.

Recommandation
Le client LDAP UCSM utilise les points de confiance configurés (certificats d'autorité de certification) lors de l'établissement de la connexion SSL.

1. Assurez-vous que le point de confiance a été configuré correctement.

2. Le champ d'identification dans cert doit être le nom d'hôte du serveur LDAP. Assurez-vous que le nom d'hôte configuré dans UCSM correspond au nom d'hôte présent dans le certificat et qu'il est valide.

3. Assurez-vous que UCSM est configuré avec 'hostname' et non 'ipaddress' du serveur LDAP et qu'il est accessible depuis l'interface de gestion locale.

Scénario de problème #5 - L'authentification échoue après la modification du fournisseur LDAP

L'authentification échoue après la suppression de l'ancien serveur LDAP et l'ajout d'un nouveau serveur LDAP

Recommandation
Lorsque LDAP est utilisé dans le domaine d'authentification, la suppression et l'ajout de nouveaux serveurs ne sont pas autorisés. À partir de la version UCSM 2.1, il en résulterait une défaillance FSM.

Les étapes à suivre lors de la suppression/l'ajout de nouveaux serveurs dans la même transaction sont

1. Assurez-vous que tous les domaines d'authentification utilisant ldap sont modifiés en local et que la configuration est enregistrée.
2. Mettez à jour les serveurs LDAP et vérifiez que l'état FSM s'est terminé correctement.
3. Remplacez les domaines d'authentification des domaines modifiés à l'étape 1 par LDAP.

Pour tous les autres scénarios de problème - Débogage LDAP

Activez les débogages, tentez de vous connecter en tant qu'utilisateur LDAP et collectez les journaux suivants avec l'assistance technique UCSM qui capture l'événement d'échec de connexion.

1) Ouvrez une session SSH sur FI et connectez-vous en tant qu'utilisateur local et passez au contexte de l'interface de ligne de commande de NX-OS.

```
ucs # connect nxos
```

2) Activez les indicateurs de débogage suivants et enregistrez le résultat de la session SSH dans un fichier journal.

```
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) Ouvrez une nouvelle session GUI ou CLI et essayez de vous connecter en tant qu'utilisateur (LDAP) distant
4) Une fois que vous avez reçu le message d'échec de connexion, désactivez les débogages.

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

Capture de paquets du trafic LDAP

Dans les scénarios où la capture de paquets est requise, Ethanalyzer peut être utilisé pour capturer le trafic LDAP entre le serveur FI et le serveur LDAP.

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host <LDAP-server-IP-address>" detail limit
```

Dans la commande ci-dessus, le fichier pcap est enregistré dans le répertoire /workspace/diagnostics et peut être récupéré à partir de FI via le contexte CLI local-mgmt

La commande ci-dessus peut être utilisée pour capturer des paquets pour tout trafic d'authentification distant (LDAP, TACACS, RADIUS).
5. Journaux pertinents dans l'offre UCSM techsupport

Dans l'assistance technique UCSM, les journaux pertinents se trouvent dans le répertoire <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
```

Avertissements connus

CSCth96721
la racine du serveur ldap sur sam doit comporter plus de 128 caractères

La version d'UCSM antérieure à 2.1 est limitée à 127 caractères pour le DN de base / la chaîne DN de liaison.

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configurati

--------- snip ----------
Nom unique spécifique de la hiérarchie LDAP dans laquelle le serveur doit lancer une recherche lorsqu'un utilisateur distant se connecte et que le système tente d'obtenir le nom unique de l'utilisateur en fonction de son nom d'utilisateur. La longueur de chaîne maximale prise en charge est de 127 caractères.

Le problème est résolu dans la version 2.1.1 et les versions ultérieures

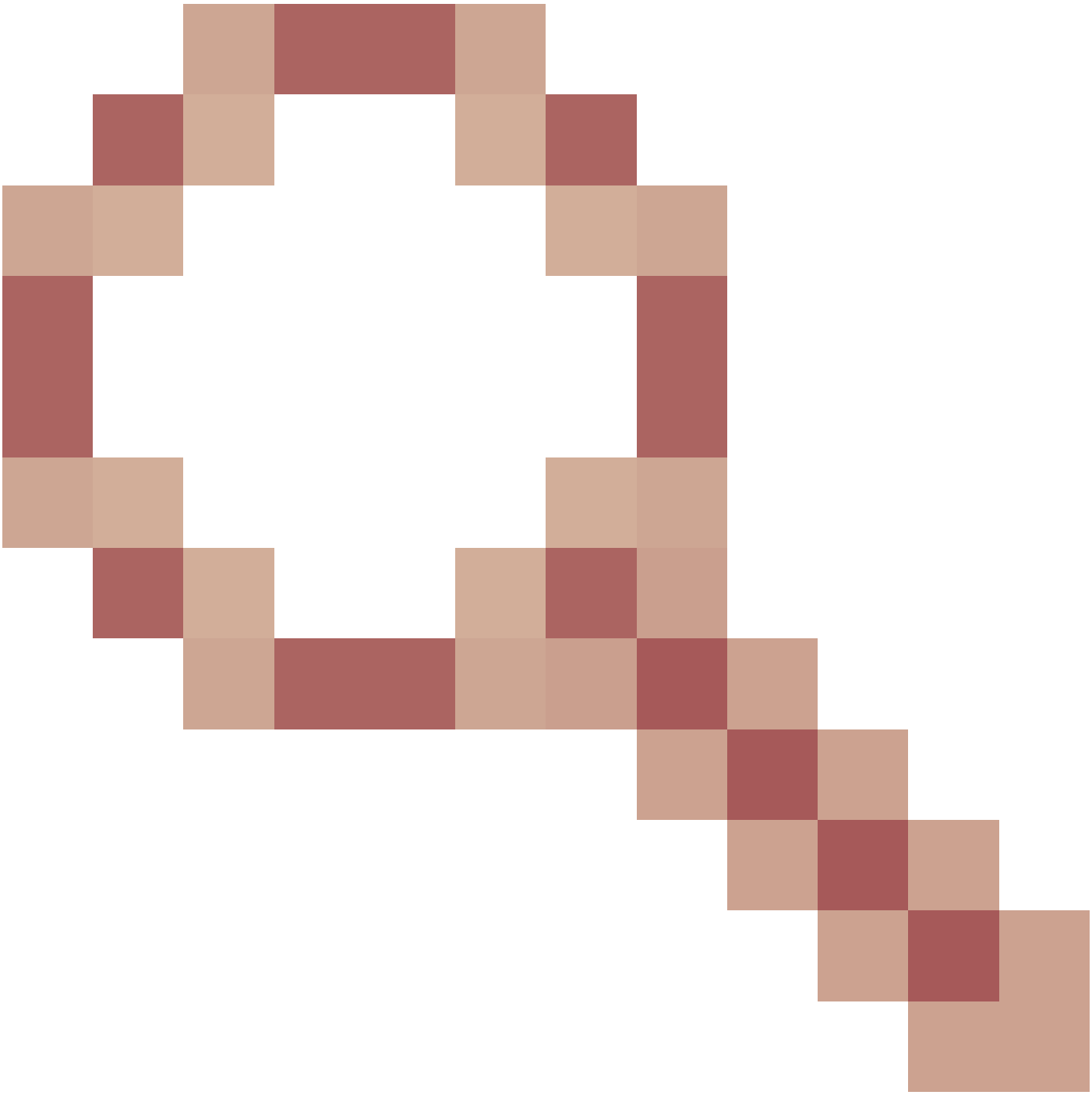
CSCuf19514
Démon LDAP bloqué

Le client LDAP peut se bloquer lors de l'initialisation de la bibliothèque ssl si l'appel ldap_start_tls_s prend plus de 60 secondes pour terminer l'initialisation. Cela ne peut se produire qu'en cas d'entrée DNS non valide / de retards dans la résolution DNS.

Prenez les mesures nécessaires pour résoudre les retards et les erreurs de résolution DNS.

CSCvt31344 - LDAP sécurisé échoue après la mise à niveau infra UCS de 4.0.4 à 4.1

Les mises à jour LDAP dans le microprogramme d'infrastructure 4.1 et versions ultérieures ont entraîné des exigences de configuration LDAP plus strictes dans UCSM. Après la mise à niveau d'UCSM, l'authentification LDAP peut échouer jusqu'à ce que la configuration soit ajustée. Consultez les notes de version de CSCvt31344



pour plus de détails.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.