Contenu

Introduction

Ce document fournit des informations sur valider la configuration de Protocole LDAP (Lightweight Directory Access Protocol) sur la suite d'Unified Communications Management (UCSM) et des étapes pour étudier des questions de panne d'authentification LDAP.

Guides de configuration :

[UCSM configurant l'authentification](#)

[Configuration de Répertoire actif témoin (AD)](#)

Vérifiez la configuration de LDAP UCSM

Assurez-vous qu'UCSM a déployé la configuration avec succès en vérifiant l'état de la machine à état défini (FSM) et il affiche terminé à 100%.

Du contexte de l'interface de ligne de commande UCSM (CLI)

Du contexte du système d'exploitation CLI de Nexus (NX-OS)

Pratiques recommandées de configuration de LDAP

1. Créez les domaines supplémentaires d'authentification au lieu de changer le royaume « d'Authenitcation indigène »

2. Utilisez toujours le royaume local pour la « authentification de console », au cas où l'utilisateur serait verrouillé d'utiliser « l'authentification indigène », admin pourrait toujours l'accéder à de la console.

3. UCSM échoue toujours de nouveau à l'authentification locale si tous les serveurs dans l'authentique-domaine donné ne répondaient pas pendant la tentative de procédure de connexion (pas applicable pour la commande d'AAA de test).

Validation de la configuration de LDAP

Testez l'authentification LDAP utilisant la commande NX-OS. la commande « d'AAA de test » est fournie seulement par l'interface CLI NX-OS.

1. Validez la configuration de particularité de groupe de LDAP.

La commande suivante passe par la liste de tous les serveurs LDAP configurés basés sur leur commande configurée.

2. Validez la configuration de serveur LDAP spécifique

REMARQUE: la chaîne de <password> sera affichée sur le terminal.

Dans ce cas, UCSM teste l'authentification contre le serveur spécifique et peut échouer s'il n'y a aucun filtre configuré pour le serveur LDAP spécifié.

Dépannage des pannes de procédure de connexion de LDAP

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

Scénario #1 de problème - Ne peut pas ouvrir une session

Ne peut pas ouvrir une session comme utilisateur de LDAP par l'intermédiaire de l'interface utilisateur graphique UCSM (GUI) et du CLI

L'utilisateur reçoit la **« erreur authentifiant au serveur »** tout en testant l'authentification LDAP.

Recommandation

Vérifiez la connexion réseau entre l'interface de gestion de serveur LDAP et de Fabric Interconnect (fi) par ping et l'établissement de Protocole ICMP (Internet Control Message Protocol) de la connexion de telnet du contexte de gens du pays-gestion

Étudiez la connexion réseau de Procotole IP (Internet Protocol) si UCSM ne peut pas cingler le serveur LDAP ou ouvrir la session de telnet au serveur LDAP.

Vérifiez si le domain name service (DN) renvoie l'adresse IP correcte à l'UCS pour l'adresse Internet de serveur LDAP et assurez-vous que le trafic de LDAP n'est pas bloqué entre ces deux périphériques.

Scénario #2 de problème - Peut se connecter dans le GUI, ne peut pas se connecter dans le SSH

L'utilisateur de LDAP peut ouvrir une session par l'intermédiaire du GUI UCSM mais ne peut pas ouvrir la session de SSH au fi.

Recommandation

En établissant la session de SSH au fi comme utilisateur de LDAP, UCSM exige du « UCS » d'être ajouté au début avant domain-name de LDAP

* De l'ordinateur de Linux/MAC

* Du client de mastic

REMARQUE: Le nom de domaine distingue les majuscules et minuscules et devrait apparier le domain-name configuré dans UCSM. La longueur maximum de nom d'utilisateur peut être 32 cars qui inclut le nom de domaine.

« ucs-<domain-name> \ <user-name> » = 32 cars.

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

L'utilisateur de LDAP peut ouvrir une session mais avoir des privilèges en lecture seule quoique des cartes de LDAP-groupe soient correctement configurées dans UCSM.

Recommandation

Si aucun rôle n'était récupéré pendant le processus de procédure de connexion de LDAP, on permet à l'utilisateur distant avec le par défaut-rôle (seulement accès lu) ou l'accès refusé (NO--procédure de connexion) pour ouvrir une session à UCSM, basé sur la stratégie de remote login.

Quand l'utilisateur distant ouvre une session et l'utilisateur a été donné l'accès en lecture seule, du fait le cas vérifient les détails d'adhésion de groupe d'utilisateurs dans LDAP/AD.
Par exemple, nous pouvons utiliser l'utilitaire ADSIEDIT pour le Répertoire actif de MS. ou ldapserach en cas de Linux/de MAC.

Il peut également être vérifié avec la commande « d'AAA de test » du shell NX-OS.

Scénario #4 de problème - Ne peut pas ouvrir une session avec la « authentification à distance »

L'utilisateur ne peut pas ouvrir une session ou a l'accès en lecture seule à UCSM comme utilisateur distant quand « l'authentification indigène » a été changée au mécanisme

d'authentification à distance (LDAP etc.)

Recommandation

Pendant que le fallsback UCSM à l'authentification locale pour l'accès de console quand il ne peut pas atteindre le serveur d'authentification à distance, nous peut suivre au-dessous des étapes pour le récupérer.

1. Déconnectez le câble d'interface de mgmt du fi primaire (l'état de show cluster indiquerait ce qui agit en tant que primaire)
2. Connectez à la console du fi primaire
3. Commandes suivantes Execute de changer l'authentification indigène

4. Connectez le câble d'interface de mgmt
5. Ouvrez une session par l'intermédiaire d'UCSM utilisant le compte local et créez l'authentique-domaine pour le groupe d'authentification à distance (LDAP ex).
REMARQUE: Déconnecter l'interface de mgmt n'affecterait aucun trafic de plan de données.

Scénario #4 de problème - Travaux d'authentification LDAP mais pas avec le SSL activé

L'authentification LDAP fonctionne bien sans Protocole SSL (Secure Socket Layer) mais échoue quand l'option SSL est activée.

Recommandation

Le client de LDAP UCSM utilise les confiance-points configurés (Certificats d'Autorité de certification (CA)) tout en établissant la connexion SSL.

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

2. Le champ d'identifier dans le CERT devrait être la « adresse Internet « du serveur LDAP. Assurez-vous que l'adresse Internet configurée dans UCSM apparie l'adresse Internet actuelle dans le certificat et est valide.

3. Assurez-vous qu'UCSM n'est configuré avec « l'IP address » de « adresse Internet » pas du serveur LDAP et il est recheable de l'interface de gens du pays-gestion.

Scénario #5 de problème - L'authentification échoue après que le fournisseur de LDAP change

L'authentification échoue après avoir supprimé le vieux serveur LDAP et avoir ajouté le nouveau serveur LDAP

Recommandation

Quand le LDAP est utilisé dans le royaume, supprimer et ajouter d'authentification de nouveaux serveurs n'est pas laissé. De la version UCSM 2.1, il aurait comme conséquence la panne FSM.

Les étapes à suivre quand retirer/ajoutant de nouveaux serveurs dans la même transaction est

1. Assurez-vous que tous les royaumes d'authentification utilisant le LDAP sont changés aux gens

du pays et ont enregistré la configuration.
2. Mettez à jour les serveurs LDAP et les vérifiez que l'état FSM s'est terminé avec succès.
3. Changez les royaumes authentiques des domaines modifiés dans l'étape 1, au LDAP.

Pour tous autres scénarios de problème - LDAP de débogage

Activez met au point, tentative d'ouvrir une session comme utilisateur de LDAP et de recueillir les logs suivants avec le techsupport UCSM que les captures ont manqué événement de procédure de connexion.

1) Ouvrez une session de SSH au fi et la procédure de connexion comme utilisateur local et changez en le contexte NX-OS CLI.

2) Suivre d'enable mettent au point des indicateurs et sauvegardent la session de SSH sortie au fichier journal.

3) Maintenant ouvrez un nouveau GUI ou session ILC et les tentez d'ouvrir une session en tant qu'utilisateur distant (de LDAP)
4) Une fois que vous receviez le message d'échec de procédure de connexion, **arrêtez met au point.**

Caputure de paquet du trafic de LDAP

Dans les scénarios où la capture de paquet est priée, l'Ethanalyzer pouvez utilisé pour capturer le trafic de LDAP entre le fi et le serveur LDAP.

Dans la commande ci-dessus, le fichier de pcap est enregistré sous le répertoire de /workspace/diagnostics et peut être récupéré du fi par l'intermédiaire du contexte CLI de gens du pays-gestion

Au-dessus de la commande peut être utilisé pour capturer des paquets pour n'importe quel (LDAP, TACACS, RAYON) trafic distant d'authenitcation.
5. Paquet approprié de techsupport des logins UCSM

Dans le techsupport UCSM, les logs appropriés se trouvent sous le **répertoire <FI>/var/sysmgr/sam_logs**

Mises en garde connues

CSCth96721
le rootdn du serveur de LDAP sur Sam devrait permettre plus de 128 caractères

La version UCSM plus tôt que 2.1 a la limite de 127 caractères pour la chaîne de base de DN/DN de grippage.

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

--------- bout ----------

Le nom unique spécifique dans la hiérarchie de LDAP où le serveur devrait commencer une recherche quand un utilisateur distant ouvre une session et les tentatives de système d'obtenir le DN de l'utilisateur basé sur leur nom d'utilisateur. La longueur de chaîne prise en charge par maximum est 127 caractères.

La question est réparée dans 2.1.1 et au-dessus de la release

CSCuf19514
Démon de LDAP tombé en panne

Le client de LDAP peut tomber en panne tout en initialisant la bibliothèque SSL si l'appel de ldap_start_tls_s prend plus de 60 sec pour remplir l'initialisation. Ceci a pu se produire seulement en cas d'entrée DNS non valide/de retards dans la résolution de DN.

Prenez les mesures pour adresser les retards et les erreurs de résolution de DN.