Problèmes sécurisés de LDAP après une mise à jour à CUCM 10.5(2)SU2

Contenu

Introduction

Ce document décrit des problèmes avec le Protocole LDAP (Lightweight Directory Access Protocol) sécurisé après évolution à Cisco Unified Communications Manager (CUCM) 10.5(2)SU2, ou 9.1(2)SU3 et les mesures qui peuvent être pris pour résoudre le problème.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 10.5(2)SU2 CUCM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

CUCM peut être configuré pour utiliser l'adresse IP ou le nom de domaine complet (FQDN) pour

l'authentification LDAP sécurisée. Le FQDN est préféré. Le comportement par défaut de CUCM est d'utiliser le FQDN. Si l'utilisation de l'adresse IP est désirée la commande d'**ipaddr de config de LDAP d'utils** peut être exécutée de l'interface de ligne de commande (CLI) du CUCM Publisher.

Avant la difficulté pour CSCun63825 qui est introduit dans 10.5(2)SU2 et 9.1(2)SU3, CUCM n'a pas strictement imposé la validation FQDN pour des connexions de Transport Layer Security (TLS) au LDAP. La validation FQDN comporte une comparaison de l'adresse Internet configurée dans CUCM (**admin > système > LDAP > authentification LDAP CUCM)**, et le nom commun (NC) ou champ alternatif soumis du nom (SAN) du certificat de LDAP présenté par le serveur LDAP pendant la connexion de TLS de CUCM au serveur LDAP. Ainsi, si l'authentification LDAP est activée (**SSL d'utilisation de** contrôle**)** et le serveur LDAP/serveurs sont définis par l'adresse IP, l'authentification réussira même si la commande d'**ipaddr de config de LDAP d'utils** n'est pas émise.

Après qu'une mise à jour CUCM à 10.5(2)SU2, 9.1(2)SU3, ou des versions ultérieures, validation FQDN soit imposée et toutes les modifications utilisant le **config de LDAP d'utils** sont retournées au comportement par défaut, qui est d'utiliser le FQDN. Le résultat de cette modification était l'ouverture de CSCux83666. En outre, l'**état de config de LDAP d'utils de** commande CLI est ajouté pour afficher si l'adresse IP ou le FQDN est utilisée.

Scénario 1

Avant que l'authentification LDAP de mise à jour soit activée, le serveur/serveurs sont définis par l'adresse IP, les **utils que la** commande d'**ipaddr de config de LDAP** est configurée sur le CLI du CUCM Publisher.

Après que l'authentification LDAP de mise à jour échoue, et la commande d'**état de config de LDAP d'utils** sur le CLI du CUCM Publisher prouve que le FQDN est utilisé pour l'authentification.

Scénario 2

Avant que l'authentification LDAP de mise à jour soit activée, le serveur/serveurs sont définis par l'adresse IP, les **utils que la** commande d'**ipaddr de config de LDAP** n'est pas configurée sur le CLI du CUCM Publisher.

Après que l'authentification LDAP de mise à jour échoue, et la commande d'**état de config de LDAP d'utils** sur le CLI du CUCM Publisher prouve que le FQDN est utilisé pour l'authentification.

Problème

L'authentification LDAP sécurisée échoue si l'authentification LDAP est configurée pour utiliser Secure Sockets Layer (SSL) sur CUCM et le serveur LDAP/serveurs étaient configurés utilisant l'adresse IP avant la mise à jour.

Afin de confirmer les configurations d'authentification LDAP naviguez vers la **page > le système > le LDAP > l'authentification LDAP d'admin CUCM** et vérifiez que les serveurs LDAP sont définis par l'adresse IP, pas FQDN. Si votre serveur LDAP est défini par FQDN et le CUCM est configuré pour utiliser le FQDN (voir la commande ci-dessous pour la vérification) qu'il est peu probable que ce soit votre question.

Afin de vérifier si CUCM (après une mise à jour) est configuré pour utiliser l'adresse IP ou l'utilisation FQDN la commande d'**état de config de LDAP d'utils du** CLI de l'éditeur CUCM.

```
admin:utils ldap config status utils ldap config fqdn configured
```

Afin de vous vérifier que vous rencontrez ce problème peut vérifier les logs CUCM DirSync pour cette erreur. Cette erreur indique que le serveur LDAP est configuré utilisant une adresse IP à la page de configuration d'authentification LDAP dans CUCM et il n'apparie pas le champ NC dans le certificat de LDAP.

```
2016-02-09 14:08:32,718 DEBUG [http-bio-443-exec-1] impl.AuthenticationLDAP -
URL contains IP Address
```

Solution

Naviguez vers la page d'**admin > de système > de LDAP > d'authentification LDAP CUCM** et changez la configuration de serveur LDAP de l'adresse IP du serveur LDAP au FQDN du serveur LDAP. Si vous devez utiliser l'adresse IP de l'utilisation de serveur LDAP cette commande du CLI du CUCM Publisher

```
admin:utils ldap config ipaddr Now configured to use IP address admin:
```

D'autres raisons qui peut mettre en boîte le résultat dans la panne de validation FQDN non liée à cet isuse particulier :

1. L'adresse Internet de LDAP configurée dans CUCM n'apparie pas le champ NC dans le certificat de LDAP (adresse Internet du serveur LDAP).

Afin d'aborder cette question naviguez vers la page d'**admin > de système > de LDAP > d'authentification LDAP CUCM** et modifiez les **informations de serveur LDAP** pour utiliser le hostname/FQDN du champ NC dans le certificat de LDAP. En outre, vérifiez que le nom utilisé est routable et peut être atteint de CUCM utilisant le **ping de réseau d'utils du** CLI de l'éditeur CUCM.

2. Un équilibreur de charge de DN est déployé dans le réseau et le serveur LDAP configuré dans CUCM utilise l'équilibreur de charge de DN. Par exemple, la configuration indique adaccess.example.com, qui équilibrent la charge alors entre plusieurs serveurs LDAP basés sur la zone géographique, ou d'autres facteurs. Le serveur LDAP qui répond à la demande peut avoir un FQDN autre qu'adaccess.example.com. Ceci a comme conséquence une panne de validation puisqu'il y a une non-concordance d'adresse Internet.

```
2016-02-06 09:19:51,702 ERROR [http-bio-443-exec-23] impl.AuthenticationLDAP -
verifyHostName:Exception.javax.net .ssl.SSLPeerUnverifiedException: hostname of the server
'adlab.testing.cisco.local' does not match the hostname in the server's certificate.
```

Afin d'aborder cette question changez le schéma de loadbalancer de LDAP tels que la connexion de TLS se termine au loadbalancer, plutôt que le serveur LDAP lui-même. Si ce n'est pas possible la seule option est de désactiver la validation FQDN et de la valider à la place utilisant l'adresse IP.