Problèmes LDAP sécurisés après une mise à niveau vers CUCM 10.5(2)SU2

Contenu

Introduction

Ce document décrit les problèmes liés au protocole LDAP (Lightweight Directory Access Protocol) sécurisé après la mise à niveau vers Cisco Unified Communications Manager (CUCM) 10.5(2)SU2 ou 9.1(2)SU3 et les étapes à suivre pour résoudre le problème.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

CUCM peut être configuré pour utiliser l'adresse IP ou le nom de domaine complet (FQDN) pour l'authentification LDAP sécurisée. Le nom de domaine complet (FQDN) est préféré. Le

comportement par défaut de CUCM consiste à utiliser le nom de domaine complet (FQDN). Si vous souhaitez utiliser l'adresse IP, la commande **utils ldap config ipaddr** peut être exécutée à partir de l'interface de ligne de commande (CLI) du serveur de publication CUCM.

Avant la correction pour CSCun63825 introduite dans 10.5(2)SU2 et 9.1(2)SU3, CUCM n'appliquait pas strictement la validation FQDN pour les connexions TLS (Transport Layer Security) à LDAP. La validation FQDN implique une comparaison du nom d'hôte configuré dans CUCM (**CUCM Admin > System > LDAP > LDAP Authentication)**, et du champ Nom commun (CN) ou Nom alternatif de sujet (SAN) du certificat LDAP présenté par le serveur LDAP lors de la connexion TLS de CUCM au serveur LDAP. Ainsi, si l'authentification LDAP est activée (cochez **la** case **SSL)** et que le/les serveur(s) LDAP sont définis par adresse IP, l'authentification réussira même si la commande **utils ldap config ipaddr n'est pas exécutée**.

Après une mise à niveau de CUCM vers les versions 10.5(2)SU2, 9.1(2)SU3 ou ultérieures, la validation FQDN est appliquée et toute modification utilisant **utils ldap config** est rétablie au comportement par défaut, qui est d'utiliser FQDN. Le résultat de ce changement a été l'ouverture de CSCux83666. En outre, la commande CLI **utils ldap config status** est ajoutée pour indiquer si l'adresse IP ou le nom de domaine complet est utilisé.

Scénario 1

Avant l'activation de l'authentification LDAP de mise à niveau, le serveur/les serveurs sont définis par adresse IP, la commande **utils ldap config ipaddr** est configurée sur l'interface de ligne de commande du serveur de publication CUCM.

Après l'échec de la mise à niveau de l'authentification LDAP, et la commande **utils ldap config status** sur l'interface de ligne de commande du serveur de publication CUCM indique que le nom de domaine complet (FQDN) est utilisé pour l'authentification.

Scénario 2

Avant l'activation de l'authentification LDAP de mise à niveau, le serveur/les serveurs sont définis par adresse IP, la commande **utils ldap config ipaddr** n'est pas configurée sur l'interface de ligne de commande du serveur de publication CUCM.

Après l'échec de la mise à niveau de l'authentification LDAP, et la commande **utils ldap config status** sur l'interface de ligne de commande du serveur de publication CUCM indique que le nom de domaine complet (FQDN) est utilisé pour l'authentification.

Problème

L'authentification LDAP sécurisée échoue si l'authentification LDAP est configurée pour utiliser SSL (Secure Sockets Layer) sur CUCM et que le/les serveur(s) LDAP ont été configurés à l'aide de l'adresse IP avant la mise à niveau.

Afin de confirmer les paramètres d'authentification LDAP, accédez à la **page Administrateur CUCM > Système > LDAP > Authentification LDAP** et vérifiez que les serveurs LDAP sont définis par adresse IP et non par nom de domaine complet. Si votre serveur LDAP est défini par FQDN et que CUCM est configuré pour utiliser FQDN (voir la commande ci-dessous pour la vérification), il est peu probable que ce problème soit lié à votre problème.

Afin de vérifier si CUCM (après une mise à niveau) est configuré pour utiliser une adresse IP ou un nom de domaine complet, utilisez la commande **utils ldap config status** de l'interface de ligne de commande de l'éditeur CUCM.

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

Afin de vérifier que vous rencontrez ce problème, vous pouvez vérifier les journaux DirSync de CUCM pour cette erreur. Cette erreur indique que le serveur LDAP est configuré à l'aide d'une adresse IP sur la page de configuration de l'authentification LDAP dans CUCM et qu'il ne correspond pas au champ CN du certificat LDAP.

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

Solution

Accédez à la page **Administration CUCM > Système > LDAP > Authentification LDAP** et modifiez la configuration du serveur LDAP de l'adresse IP du serveur LDAP en nom de domaine complet du serveur LDAP. Si vous devez utiliser l'adresse IP du serveur LDAP, utilisez cette commande à partir de l'interface de ligne de commande du serveur de publication CUCM

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

D'autres raisons qui peuvent entraîner un échec de validation du nom de domaine complet non lié à ce problème particulier :

1. Le nom d'hôte LDAP configuré dans CUCM ne correspond pas au champ CN du certificat LDAP (nom d'hôte du serveur LDAP).

Pour résoudre ce problème, accédez à la **page** The **CUCM Admin > System > LDAP > LDAP Authentication** et modifiez les **informations du serveur LDAP** pour utiliser le nom d'hôte/FQDN du champ CN dans le certificat LDAP. Vérifiez également que le nom utilisé est routable et peut être atteint à partir de CUCM à l'aide de la **requête ping réseau utils** à partir de l'interface de ligne de commande de l'éditeur CUCM.

2. Un équilibrage de charge DNS est déployé sur le réseau et le serveur LDAP configuré dans CUCM utilise l'équilibrage de charge DNS. Par exemple, la configuration pointe vers adaccess.example.com, qui équilibre ensuite la charge entre plusieurs serveurs LDAP en fonction de la géographie ou d'autres facteurs. Le serveur LDAP qui répond à la demande peut avoir un nom de domaine complet autre que adaccess.example.com. Cela entraîne un échec de validation

car il y a une non-correspondance de nom d'hôte.

```
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.
```

Pour résoudre ce problème, modifiez le schéma d'équilibrage de charge LDAP de sorte que la connexion TLS se termine au niveau de l'équilibreur de charge, plutôt que sur le serveur LDAP lui-même. Si ce n'est pas possible, la seule option est de désactiver la validation FQDN et de valider à la place à l'aide de l'adresse IP.