Sichere LDAP-Probleme nach einem Upgrade auf CUCM 10.5(2)SU2

Inhalt

Einführung

Dieses Dokument beschreibt Probleme mit dem sicheren LDAP (Lightweight Directory Access Protocol) nach dem Upgrade auf Cisco Unified Communications Manager (CUCM) 10.5(2)SU2 oder 9.1(2)SU3 und beschreibt die Schritte, die zur Behebung des Problems ergriffen werden können.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der CUCM-Version 10.5(2)SU2.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der CUCM kann so konfiguriert werden, dass er für die sichere LDAP-Authentifizierung entweder IP-Adresse oder FQDN (Fully Qualified Domain Name) verwendet. FQDN wird bevorzugt. Das Standardverhalten von CUCM ist die Verwendung von FQDN. Wenn die Verwendung der IP-Adresse gewünscht wird, kann der Befehl **utils ldap config ipaddr** über die Befehlszeilenschnittstelle (CLI) des CUCM Publisher ausgeführt werden.

Vor dem Fix für CSCun63825, der in 10.5(2)SU2 und 9.1(2)SU3 eingeführt wurde, hat CUCM keine strikte FQDN-Validierung für TLS-Verbindungen (Transport Layer Security) mit LDAP durchgesetzt. Die FQDN-Validierung beinhaltet einen Vergleich des im CUCM konfigurierten Hostnamens (**CUCM Admin > System > LDAP > LDAP Authentication)** und des Felds Common Name (CN) oder Subject Alternative Name (SAN) des LDAP-Zertifikats, das der LDAP-Server während der TLS-Verbindung vom CUCM zum LDAP-Server vorlegt. Wenn also die LDAP-Authentifizierung aktiviert ist (**SSL verwenden)** und der LDAP-Server/die LDAP-Server/Server durch die IP-Adresse definiert sind, ist die Authentifizierung auch dann erfolgreich, wenn der Befehl **utils ldap config ipaddr** nicht ausgegeben wird.

Nach einem CUCM-Upgrade auf Version 10.5(2)SU2, 9.1(2)SU3 oder neuere Versionen wird die FQDN-Validierung erzwungen, und alle Änderungen mit der **utils ldap-Konfiguration** werden auf das Standardverhalten zurückgesetzt, d. h. die Verwendung von FQDN. Das Ergebnis dieser Änderung war die Eröffnung von CSCux83666. Außerdem wird der CLI-Befehl **utils ldap config status** hinzugefügt, um anzuzeigen, ob IP-Adresse oder FQDN verwendet wird.

Szenario 1

Bevor die LDAP-Aktualisierungsauthentifizierung aktiviert ist, werden Server/Server durch die IP-Adresse definiert. Der Befehl **utils ldap config ipadr** wird auf der CLI des CUCM Publisher konfiguriert.

Wenn die LDAP-Aktualisierungsauthentifizierung fehlschlägt und der Befehl **utils ldap config status** auf der CLI des CUCM Publisher anzeigt, dass FQDN für die Authentifizierung verwendet wird.

Szenario 2

Bevor die LDAP-Aktualisierungsauthentifizierung aktiviert ist, werden Server/Server durch die IP-Adresse definiert. Der Befehl **utils ldap config ipadr** wird nicht in der CLI des CUCM Publisher konfiguriert.

Wenn die LDAP-Aktualisierungsauthentifizierung fehlschlägt und der Befehl **utils ldap config status** auf der CLI des CUCM Publisher anzeigt, dass FQDN für die Authentifizierung verwendet wird.

Problem

Die sichere LDAP-Authentifizierung schlägt fehl, wenn die LDAP-Authentifizierung so konfiguriert ist, dass sie Secure Sockets Layer (SSL) auf dem CUCM verwendet und die LDAP-Server/Server vor dem Upgrade mithilfe der IP-Adresse konfiguriert wurden.

Um die LDAP-Authentifizierungseinstellungen zu bestätigen, navigieren Sie zur **Seite CUCM Admin > System > LDAP > LDAP Authentication** und überprüfen Sie, ob die LDAP-Server durch die IP-Adresse und nicht durch den FQDN definiert sind. Wenn Ihr LDAP-Server durch FQDN definiert ist und der CUCM für die Verwendung von FQDN konfiguriert ist (zur Überprüfung siehe Befehl unten), ist es unwahrscheinlich, dass dies Ihr Problem ist.

Um zu überprüfen, ob CUCM (nach einem Upgrade) für die Verwendung von IP-Adresse oder FQDN konfiguriert ist, verwenden Sie den Befehl **utils ldap config status** aus der CLI des CUCM-Publishers.

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

Um zu überprüfen, ob dieses Problem vorliegt, können Sie die CUCM DirSync-Protokolle auf diesen Fehler überprüfen. Dieser Fehler weist darauf hin, dass der LDAP-Server auf der Konfigurationsseite für die LDAP-Authentifizierung im CUCM mit einer IP-Adresse konfiguriert wird und nicht mit dem CN-Feld im LDAP-Zertifikat übereinstimmt.

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

Lösung

Navigieren Sie zur Seite **CUCM Admin > System > LDAP > LDAP Authentication**, und ändern Sie die LDAP-Serverkonfiguration von der IP-Adresse des LDAP-Servers in den FQDN des LDAP-Servers. Wenn Sie die IP-Adresse des LDAP-Servers verwenden müssen, verwenden Sie diesen Befehl aus der CLI des CUCM Publisher.

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

Weitere Gründe, die zu Fehlern bei der FQDN-Validierung führen können, sind nicht in Zusammenhang mit diesem speziellen Problem:

1. Der im CUCM konfigurierte LDAP-Hostname stimmt nicht mit dem CN-Feld im LDAP-Zertifikat (Hostname des LDAP-Servers) überein.

Um dieses Problem zu beheben, navigieren Sie zur Seite **CUCM Admin > System > LDAP > LDAP Authentication (CUCM-Administrator > System > LDAP > LDAP-Authentifizierung),** und ändern Sie die **LDAP-Serverinformationen**, um den Hostnamen/FQDN aus dem CN-Feld im LDAP-Zertifikat zu verwenden. Stellen Sie außerdem sicher, dass der verwendete Name routingfähig ist und vom CUCM mithilfe des **utils-Netzwerk-Pings** von der CLI des CUCM-Publishers erreicht werden kann.

2. Im Netzwerk wird ein DNS Load Balancer bereitgestellt, und der im CUCM konfigurierte LDAP-Server verwendet den DNS Load Balancer. Beispielsweise verweist die Konfiguration auf adaccess.example.com, das dann die Last auf mehrere LDAP-Server verteilt, je nach Region oder anderen Faktoren. Der LDAP-Server, der die Anforderung beantwortet, kann einen anderen

FQDN als adaccess.example.com haben. Dies führt zu einem Validierungsfehler, da ein Hostname-Ungleichgewicht vorliegt.

```
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.
```

Um dieses Problem zu beheben, ändern Sie das LDAP Load Balancer-Schema, sodass die TLS-Verbindung am Load Balancer statt am LDAP-Server selbst endet. Ist dies nicht möglich, besteht die einzige Option darin, die FQDN-Validierung zu deaktivieren und stattdessen die IP-Adresse zu verwenden.