升級到CUCM 10.5(2)SU2後的安全LDAP問題

目錄

簡介

本文說明升級到Cisco Unified Communications Manager(CUCM)10.5(2)SU2或9.1(2)SU3後安全輕量級目錄訪問協定(LDAP)的問題，以及可採取的解決此問題的步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於CUCM版本10.5(2)SU2。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

可以將CUCM配置為使用IP地址或完全限定域名(FQDN)進行安全LDAP身份驗證。已預置FQDN。CUCM的預設行為是使用FQDN。如果需要使用IP地址，則可以從CUCM發佈器的命令列介面(CLI)運行**utils ldap config ipaddr**命令。

在10.5(2)SU2和9.1(2)SU3中引入的CSCun63825修復之前，CUCM沒有嚴格強制對傳輸層安全(TLS)連線進行FQDN驗證。FQDN驗證包括對CUCM(**CUCM Admin > System > LDAP > LDAP驗證**

)中配置的主機名和LDAP證書提供的公用名(CN)或主題備用名稱(SAN)欄位的比較從CUCM到LDAP伺服器的TLS連線期間的LDAP伺服器。因此，如果啟用LDAP身份驗證(選中**使用SSL)**，並且由IP地址定義LDAP伺服器/伺服器，則即使未發出**utils ldap config ipaddr**命令，身份驗證也會成功。

在CUCM升級到10.5(2)SU2、9.1(2)SU3或更高版本後，將強制執行FQDN驗證，並且使用**utils ldap config的任何更改將還原為預設行為，即使用FQDN。**此更改的結果是開啟了CSCux83666。此外，CLI命令**utils ldap config status**被新增以顯示是否正在使用IP地址或FQDN。

案例 1

啟用升級LDAP身份驗證之前，伺服器/伺服器由IP地址定義，在CUCM發佈伺服器的CLI上配置**utils ldap config ipaddr**命令。

升級後LDAP身份驗證失敗，CUCM發佈器的CLI上的**utils ldap config status**命令顯示FQDN用於身份驗證。

案例 2

啟用升級LDAP身份驗證之前，伺服器/伺服器由IP地址定義，未在CUCM發佈伺服器的CLI上配置**utils ldap config ipaddr**命令。

升級後LDAP身份驗證失敗，CUCM發佈器的CLI上的**utils ldap config status**命令顯示FQDN用於身份驗證。

問題

如果LDAP身份驗證配置為在CUCM上使用安全套接字層(SSL)，並且LDAP伺服器/伺服器在升級之前使用IP地址配置，則安全LDAP身份驗證失敗。

若要確認LDAP身份驗證設定，請導航到**CUCM Admin**頁>系統> LDAP > LDAP身份驗證，並驗證LDAP伺服器是由IP地址而不是FQDN定義的。如果LDAP伺服器由FQDN定義，並且CUCM配置為使用FQDN（請參閱下面的命令進行驗證），則此問題不太可能是您的問題。

要驗證CUCM（升級後）是否配置為使用IP地址或FQDN，請從CUCM發佈器的CLI使用**utils ldap config status**命令。

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

若要確認您遇到此問題，您可以檢查CUCM DirSync日誌中是否存在此錯誤。此錯誤表示LDAP伺服器是使用CUCM中LDAP身份驗證配置頁面上的IP地址配置的，並且與LDAP證書中的CN欄位不匹配。

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

URL contains IP Address

解決方案

導航到**CUCM Admin > System > LDAP > LDAP Authentication**頁，並將LDAP伺服器配置從LDAP伺服器的IP地址更改為LDAP伺服器的FQDN。如果必須使用LDAP伺服器的IP地址，請從CUCM Publisher的CLI使用此命令

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

可能導致與此特定問題無關的FQDN驗證失敗的其他原因：

1. CUCM中配置的LDAP主機名與LDAP證書中的CN欄位（LDAP伺服器的主機名）不匹配。

為了解決此問題，請導航到**CUCM Admin > System > LDAP > LDAP Authentication**頁，然後修改**LDAP Server Information**以使用LDAP證書中CN欄位中的主機名/FQDN。此外，驗證使用的名稱是可路由的，並且可以使用CUCM發佈器的CLI通過**utils network ping**從CUCM訪問。

2.網路中部署了DNS負載平衡器，在CUCM中配置的LDAP伺服器使用DNS負載平衡器。例如，配置指向adaccess.example.com，然後它會根據地理位置或其他因素在多個LDAP伺服器之間實現負載均衡。響應請求的LDAP伺服器可以具有adaccess.example.com以外的FQDN。這會導致驗證失敗，因為存在主機名不匹配。

```
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.
```

為了解決此問題，請更改LDAP負載平衡器方案，以使TLS連線終止於負載平衡器，而不是LDAP伺服器本身。如果不能，則唯一的選項是禁用FQDN驗證，而是使用IP地址進行驗證。