升级到CUCM 10.5(2)SU2后的安全LDAP问题

目录

简介

本文档介绍升级到Cisco Unified Communications Manager(CUCM)10.5(2)SU2或9.1(2)SU3后安全轻量级目录访问协议(LDAP)的问题，以及可以采取的步骤。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于CUCM版本10.5(2)SU2。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

CUCM可配置为使用IP地址或完全限定域名(FQDN)进行安全LDAP身份验证。FQDN已覆盖。CUCM的默认行为是使用FQDN。如果需要使用IP地址，则可以从CUCM发布方的命令行界面(CLI)运行**utils ldap config ipaddr**命令。

在10.5(2)SU2和9.1(2)SU3中引入的CSCun63825修复之前，CUCM未严格对LDAP的传输层安全(TLS)连接执行FQDN验证。FQDN验证涉及对LDAP中配置的主机名进行比较CUCM(**CUCM Admin**

> System > LDAP > LDAP Authentication)，以及LDAP服务器在从CUCM到LDAP服务器的TLS连接期间提供的LDAP证书的公用名称(CN)或使用者备用名称(SAN)字段。因此，如果启用LDAP身份验**证(**检查使用SSL)，且LDAP服务器/服务器由IP地址定义，则即使未发出**utils ldap config ipaddr**命令，身份验证也会成功。

在CUCM升级到10.5(2)SU2、9.1(2)SU3或更高版本后，将执行FQDN验证，并且使用**utils ldap config的任何更改将恢复为默认行为**，即使用FQDN。此更改的结果是打开CSCux83666。此外，还添加了CLI命令**utils ldap config status**，以显示是否使用IP地址或FQDN。

场景 1

在启用升级LDAP身份验证之前，服务器/服务器由IP地址定义，在CUCM发布方的CLI上配置**utils ldap config ipaddr**命令。

升级LDAP身份验证失败后，CUCM发布者的CLI上的**utils ldap config status**命令显示FQDN用于身份验证。

场景 2

在启用升级LDAP身份验证之前，服务器/服务器由IP地址定义，CUCM发布服务器的CLI上未配置**utils ldap config ipaddr**命令。

升级LDAP身份验证失败后，CUCM发布者的CLI上的**utils ldap config status**命令显示FQDN用于身份验证。

问题

如果LDAP身份验证配置为在CUCM上使用安全套接字层(SSL)，并且在升级之前使用IP地址配置了LDAP服务器/服务器，则安全LDAP身份验证失败。

要确认LDAP身份验证设置，请导航至**CUCM Admin**页面> System > LDAP > LDAP > LDAP Authentication，并验证LDAP服务器是由IP地址而非FQDN定义的。如果LDAP服务器由FQDN定义，而CUCM配置为使用FQDN（请参阅下面的命令进行验证），则不太可能是您的问题。

要验证CUCM（升级后）是否配置为使用IP地址或FQDN，请在CUCM发布方的CLI中使用**utils ldap config status命令**。

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

为了验证您遇到此问题，您可以检查CUCM DirSync日志中是否存在此错误。此错误表示LDAP服务器在CUCM的LDAP身份验证配置页面上使用IP地址进行配置，并且与LDAP证书中的CN字段不匹配。

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

URL contains IP Address

解决方案

导航至**CUCM Admin > System > LDAP > LDAP Authentication页**，并将LDAP服务器配置从LDAP服务器的IP地址更改为LDAP服务器的FQDN。如果必须使用LDAP服务器的IP地址，请从CUCM发布服务器的CLI使用此命令

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

可能导致FQDN验证失败的其他原因与此特定问题无关：

1.在CUCM中配置的LDAP主机名与LDAP证书（LDAP服务器的主机名）中的CN字段不匹配。

要解决此问题，请导航至**CUCM Admin > System > LDAP > LDAP Authentication页**面，并修改**LDAP Server Information**以使用LDAP证书中CN字段中的主机名/FQDN。此外，验证使用的名称是可路由的，并且可以通过CUCM使用**utils network ping** 从CUCM发布方的CLI访问。

2. DNS负载均衡器部署在网络中，CUCM中配置的LDAP服务器使用DNS负载均衡器。例如，配置指向adaccess.example.com，然后根据地理位置或其他因素在多个LDAP服务器之间进行负载均衡。响应请求的LDAP服务器可以具有除adaccess.example.com之外的FQDN。这会导致验证失败，因为主机名不匹配。

```
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.
```

为解决此问题，请更改LDAP负载均衡器方案，使TLS连接终止于负载均衡器，而不是LDAP服务器本身。如果这不可能，则唯一的选项是禁用FQDN验证，而是使用IP地址进行验证。