在升级以后的安全LDAP问题对CUCM 10.5(2)SU2

目录

简介

本文在升级以后描述可以采取解决问题与安全轻量级目录访问协议(LDAP)的问题给Cisco Unified Communications Manager (CUCM) 10.5(2)SU2或者9.1(2)SU3和步骤。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据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可以配置使用IP地址或完全合格的域名(FQDN)安全LDAP认证。FQDN preffered。CUCM默认行为是使用FQDN。如果使用IP地址希望**ipaddr命令使用情况ldap的设置**可以从CUCM发行商的命令行界面(CLI)运行。

在10.5(2)SU2和9.1(2)SU3介绍的CSCun63825的修正之前， CUCM没有严格强制执行传输层安全(TLS)连接的FQDN验证对LDAP。 FQDN验证在CUCM (**CUCM Admin >System > LDAP > LDAP认证)**介入配置的主机名的比较和LDAP服务器提交的LDAP证书的共同名称(CN)或者附属的替代方案名称(SAN)字段在从CUCM的TLS连接时到LDAP服务器。因此，如果LDAP认证启用(检查**使用SSL)，**并且LDAP服务器/服务器由IP地址定义，验证将成功，即使**ipaddr命令使用情况ldap的设置没有**发出。

在对10.5(2)SU2的CUCM升级， 9.1(2)SU3，或以上版本， FQDN验证被强制执行后和所有更改使用**使用情况ldap设置**被恢复对默认行为，是使用FQDN。此更改结果是CSCux83666开端。并且，如果使用， CLI命令**使用情况ldap设置状态**被添加显示IP地址或FQDN。

场景 1

在升级LDAP认证启用前，服务器/服务器由IP地址定义，**使用情况的设置**在CUCM发行商的CLI配置**ipaddr命令的ldap**。

在升级LDAP认证发生故障后和**使用情况ldap设置status命令**在CUCM发行商的CLI显示FQDN使用验证。

场景 2

在升级LDAP认证启用前，服务器/服务器由IP地址定义，**使用情况的设置**在CUCM发行商的CLI没有配置**ipaddr命令的ldap**。

在升级LDAP认证发生故障后和**使用情况ldap设置status命令**在CUCM发行商的CLI显示FQDN使用验证。

问题

安全LDAP认证发生故障，如果LDAP认证配置使用在CUCM的安全套接字协议层(SSL)，并且LDAP服务器/服务器配置使用IP地址在升级之前。

为了确认LDAP认证设置请导航对**CUCM管理员页面>System > LDAP > LDAP认证**并且验证LDAP服务器由IP地址定义，不是FQDN。如果您的LDAP服务器由FQDN定义，并且CUCM配置使用FQDN (请参阅下面命令关于验证)不太可能这是您的问题。

为了验证，如果CUCM (在升级以后)配置使用IP地址或FQDN使用**使用情况ldap设置status命令**从CUCM发行商的CLI。

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

为了验证您遇到此问题您能检查CUCM DirSync日志此错误。此错误表明LDAP服务器配置使用在LDAP认证配置页的一个IP地址在CUCM，并且不匹配LDAP证书的CN字段。

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

解决方案

导航对**CUCM Admin >System > LDAP > LDAP认证**页并且更改从LDAP服务器的IP地址的LDAP服务器配置对LDAP服务器的FQDN。如果必须使用LDAP服务器使用的IP地址从CUCM发行商的CLI的此命令

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

能的其他原因能导致FQDN与此特定的isuse没涉及的验证失败：

1. 在CUCM配置的LDAP主机名不匹配LDAP证书的(LDAP服务器的主机名CN字段)。

为了解决此问题请导航对**CUCM Admin >System > LDAP > LDAP认证**页并且修改**LDAP服务器信息**使用从CN字段的主机名/FQDN在LDAP证书。并且，请验证使用的名称可路由的，并且可以从CUCM被到达使用**使用情况**从CUCM发行商的CLI的**网络ping**。

2. DNS负载平衡器在网络部署，并且在CUCM配置的LDAP服务器使用DNS负载平衡器。例如，配置指向adaccess.example.com，然后装载在根据地理的几个LDAP服务器之间的平衡，或者其他要素。答复请求除adaccess.example.com之外的LDAP服务器能有FQDN。因为有主机名不匹配，这导致验证失败。

```
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.
```

为了解决此问题请更改LDAP loadbalancer方案这样TLS连接终止在loadbalancer，而不是LDAP服务器。如果这不是可能的唯一选择是禁用FQDN验证和验证使用IP地址。