为ILS配置加入集群并排除故障

目录

简介
先决条件
要求
使用的组件
配置
网络图
配置
方法1.在集群之间使用密码身份验证
方法2.在群集之间使用TLS身份验证
方法3.在群集之间使用TLS和密码身份验证。
方法4.在集群与密码身份验证加入后切换到TLS身份验证。
验证
故障排除
方法1的ILS注册日志分析
分支注册在集群之间使用密码身份验证成功注册到集线器
分支到尝试注册到中心，但由于密码不匹配而失败
方法2的ILS注册日志分析
分支使用TLS身份验证成功注册到中心
连接失败，因为中心的Tomcat证书未在分支中导入
连接失败，因为分支的Tomcat证书未导入中心
方法3的ILS注册日志分析
使用带密码身份验证的TLS成功注册到集线器
连接失败，因为辐条的Tomcat证书是自签名的
连接失败，因为集线器的Tomcat证书是自签名的
方法4的ILS注册日志分析
当从已建立的连接使用密码身份验证切换到TLS身份验证时，分支成功注册到中心。
连接失败，因为当从已建立的连接使用密码身份验证切换到TLS身份验证时，集线器具有自签名证书。
连接失败，因为分支具有自签名证书，当从使用密码身份验证的已建立连接切换到TLS身份验证时。

简介

本文档介绍加入集群以进行集群间查找服务(ILS)的可能配置方法，并记录分析以排除每种方法的故障。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

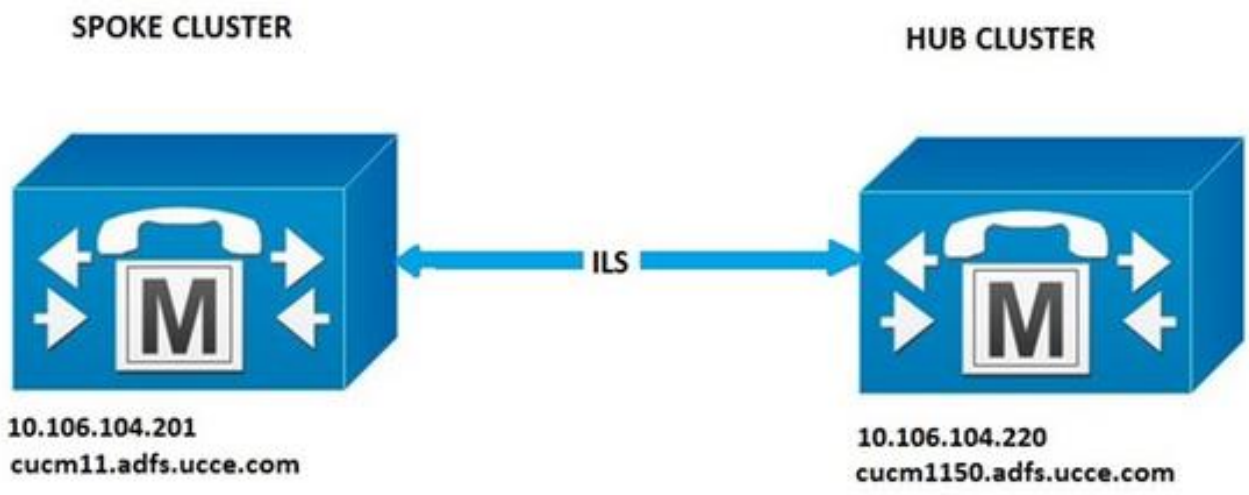
本文档中的信息基于以下软件和硬件版本：

- Cisco Unified Communications Manager (CUCM) 11.5 版

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。

配置

网络图



配置

方法1.在集群之间使用密码身份验证

登录CUCM Administration页面，导航至Advanced Features **> ILS Configuration**。
在ILS Configuration（ILS配置）窗口中，选中**Use Password(使用密**码)复选框。

管理密码，然后点击**Save**。ILS网络中所有集群的口令必须相同。

方法2.在群集之间使用TLS身份验证

要使用此方法，请确保作为ILS网络一部分的所有集群已在其tomcat-trust中导入远程集群Tomcat证

书。

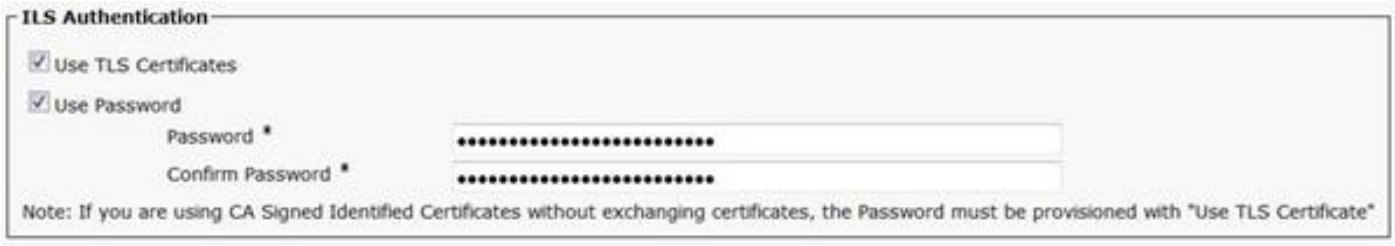
在CUCM管理中，导航至**高级功能> ILS配置**。在ILS配置窗口中，选中ILS身份验**证下的**使用TLS证书复选框。

方法3.在群集之间使用TLS和密码身份验证。

此方法的优点是，如果由外部证书颁发机构(CA)签名，则无需交叉导入集群之间的Tomcat证书以建立TLS连接。 此方法可从CUCM 11.5及更高版本获得。

要使用此方法，请确保要成为ILS网络一部分的所有集群都具有由外部CA签名的tomcat证书，并且此CA的根证书存在于tomcat-trust中。此外，ILS网络中所有集群的口令必须相同。

在CUCM管理中，导航至ILS**身份验证下的高级功**能> ILS配置，选中**使用TLS证书**和**使用密码**复选框。



方法4.在集群与密码身份验证加入后切换到TLS身份验证。

这是使用TLS的另一种方法，如果群集之间由外部CA签名，则无需交叉导入Tomcat证书。这对于不支持方法3的11.5之前的CUCM版本非常有用。

要使用此方法，请确保要成为ILS网络一部分的所有集群都具有由外部CA签名的tomcat证书，并且此CA的根证书存在于tomcat-trust中。

首先使用密码身份验证加入集群。在Cisco Unified CM管理中，导航至高级功**能> ILS配置。**在ILS身份验证下，选中**使用密**码复选框。管理密码。Click Save.

加入集群时，客户端和服务器端的密码必须相同。

建立连接后，将身份验证方法更改为TLS。 在CUCM管理中，导航至**高级功能> ILS配置**。在ILS Configuration（ILS配置）窗口中，选中ILS Authentication（ILS身份验证）下**的Use TLS Certificates（使用TLS证书）复选框。**

验证

在的ILS集群和全局拨号方案导入目录下可以看到成功注册

高级功能> ILS配置

使用命令run sql select * from remotecluster列出***远程群集详细信息***

```
admin:run sql select * from remotecluster
pkid                                 fullyqualifiedname   clusterid description version
==================================== ==================== ========= =========== ================
5edbbde9-d72b-4cd1-8f8e-93ab32cb58da cucm11.adfs.ucce.com 1                       11.5.1.10000(4)
admin:
```

故障排除

将思科集群间查找服务的调试跟踪级别设置为debug trace level（详细）。

跟踪的位置： activelog /cm/trace/ils/sdl/

举例说明了每种ILS注册方法的成功和失败场景的日志分析。

方法1的ILS注册日志分析

分支注册在集群之间使用密码身份验证成功注册到集线器

集线器中的日志片段：

```
00154617.001 |16:58:42.888 |AppInfo  |IlsD IlsHandler: Ils::wait_SdlConnectionInd(): New
connection accepted. DeviceName=, TCPPid = [1.600.13.5], IPAddr=10.106.104.201, Port=37816,
Controller=[1,20,1]

00154617.002 |16:58:42.888 |AppInfo  |IlsD Ils::ConnectInd TCPPid([1, 600, 13, 5]),
PeerIP/Port(10.106.104.201:37816), LocalIP/Port(10.106.104.220:7502) (10.106.104.201:37816)

00154618.012 |16:58:42.889 |AppInfo  |IlsD ::ConnectIndInner Server Connection to
PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPid([1, 600, 13, 5]),
PeerIP/Port(10.106.104.201:37816), LocalIP/Port(10.106.104.220:7502) TLSReq(f) established
```

Spoke中的日志片段：

```
00145095.017 |16:58:42.878 |AppInfo  |IlsD Ils::ConnectReq(): Requesting Connection to
IpAddr(10.106.104.220), IpPort(7502), TLSReq(f)

00145095.018 |16:58:42.878 |AppInfo  |IlsD Ils::ConnectReq() Pub IP/Port(10.106.104.220:7502)
Pri IP/Port(:7502) TLSReq(false)

00145095.024 |16:58:42.879 |AppInfo  |IlsD Ils::processConnectReq Initiating non-TLS Connection

00145096.001 |16:58:42.881 |AppInfo  |IlsD Ils::ConnectRes() appCorr(1029) TCPPid([1, 600, 13,
5]), PeerIP/Port(10.106.104.220:7502), LocalIP/Port(10.106.104.201:37816) TLSReq(f) found

00145096.002 |16:58:42.881 |AppInfo  |IlsD DEBUG(0000FA0E): Client Connection to
peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7502) TLSReq(f) succeeded

00145097.010 |16:58:42.896 |AppInfo  |IlsD ::ConnectIndInner starting  to
PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPPid([1, 600, 13, 5]),
PeerIP/Port(10.106.104.220:7502), LocalIP/Port(10.106.104.201:37816) TLSReq(f) established
```

分支到尝试注册到中心，但由于密码不匹配而失败

DecryptData失败，集线器日志中的ILSPwdAuthenticationFailed警报表示密码不匹配。

集线器中的日志片段：

```
00155891.005 |17:25:26.197 |AppInfo  |IlsD IlsHandler: wait_SdlDataInd EncrUtil::decryptData
failed. DeviceName=, TCPPid = [1.600.13.7], IPAddr=10.106.104.201, Port=40592,
Controller=[1,20,1]

 00155891.006 |17:25:26.197 |AppInfo  |IlsD wait_SdlDataInd sending ILSPwdAuthenticationFailed
alarm with IPAddress= 10.106.104.201; mAlarmedConnections count= 1
```

注意：当由于密码不匹配而连接失败时，其余方法中的错误也相同。

方法2的ILS注册日志分析

分支使用TLS身份验证成功注册到中心

集线器中的日志片段：

```
00000901.001 |15:46:27.238 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): peer certificates are
in certificate store
```

```
00000902.008 |15:46:27.240 |AppInfo  |IlsD ::ConnectIndInner Server Connection to
PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPid([1, 600, 17, 4]),
PeerIP/Port(10.106.104.201:60938), LocalIP/Port(10.106.104.220:7501) TLSReq(t) established
```

从Spoke记录代码段：

```
00000646.001 |15:46:27.189 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): peer certificates are
in certificate store

00000647.006 |15:46:27.199 |AppInfo  |IlsD ::ConnectIndInner starting  to
PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPPid([1, 600, 17, 3]),
PeerIP/Port(10.106.104.220:7501), LocalIP/Port(10.106.104.201:36115) TLSReq(t) established
```

连接失败，因为中心的Tomcat证书未在分支中导入

来自分支的日志表示中心的证书验证失败。

Spoke中的日志片段：

```
00001821.000 |16:34:01.765 |AppInfo  |[1, 600, 17, 5]: HandleSSLError - Certificate verification
failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501

00001822.000 |16:34:01.765 |AppInfo  |[1, 600, 17, 5]: HandleSSLError - Certificate verification
failed for 10.106.104.220:7501

00001827.002 |16:34:01.766 |AppInfo  |IlsD Ils::wait_SdlConnectErrRsp sending
ILSTLSAuthenticationFailed alarm with Cluster1 = 10.106.104.220; mAlarmedConnections count= 1

00001827.004 |16:34:01.770 |AppInfo  |IlsD ERROR(000005C9): Connection to
peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7501) TLSReq(t) failed,
ConnReason(1)
```

连接失败，因为分支的Tomcat证书未导入中心

中心的日志表示连接已关闭，既不是本地存储中分支的证书，也不是对等体信息矢量中的FQDN。

集线器中的日志片段：

```
00003366.001 |17:06:30.877 |AppInfo  |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject
failed.

00003366.002 |17:06:30.877 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): certificate is not in
the local store and the FQDN (cucm11.adfs.ucce.com) is not in the peer info vector, closing the
connection

00003366.003 |17:06:30.877 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): sending
ILSTLSAuthenticationFailed alarm for Cluster1= cucm11.adfs.ucce.com; mAlarmedConnections count=
1

00003366.004 |17:06:30.882 |AppInfo  |IlsD IlsHandler: Close Req. DeviceName=, TCPPid =
[1.600.17.16], IPAddr=10.106.104.201, Port=39267, Controller=[1,20,1
```

方法3的ILS注册日志分析

使用带密码身份验证的TLS成功注册到集线器

集线器中的日志片段：

```
00000211.001 |08:06:58.798 |AppInfo  |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject
failed.

00000211.002 |08:06:58.798 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): peer certificates are
not in certificate store but Root CA signed certs are uploaded locally

00000212.001 |08:06:58.803 |AppInfo  |EncrUtil Function: decryptData at line 163 succedded

00000212.002 |08:06:58.803 |AppInfo  |EncrUtil Function: decryptData at line 165 succedded

00000212.003 |08:06:58.803 |AppInfo  |EncrUtil Function: decryptData at line 168 succedded

00000212.004 |08:06:58.803 |AppInfo  |EncrUtil decryptData: inlen 1956, outlen 1949 succeed

00000212.012 |08:06:58.804 |AppInfo  |IlsD ::ConnectIndInner Server Connection to
PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPid([1, 600, 17, 1]),
PeerIP/Port(10.106.104.201:56181), LocalIP/Port(10.106.104.220:7501) TLSReq(t) established
```

Spoke中的日志片段：

```
00000064.000 |08:06:58.802 |SdlSig   |SdlConnectRsp
|wait                          |Ils(1,600,20,1)
|SdlSSLTCPConnection(1,600,17,1)  |1,600,16,1.1^*^*                          |*TraceFlagOverrode

00000064.001 |08:06:58.802 |AppInfo  |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject
failed.

00000064.002 |08:06:58.802 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): peer certificates are
not in certificate store but Root CA signed certs are uploaded locally.

00000064.004 |08:06:58.802 |AppInfo  |IlsD DEBUG(00000407): Client Connection to
peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7501) TLSReq(t) succeeded

00000065.010 |08:06:58.812 |AppInfo  |IlsD ::ConnectIndInner starting  to
PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPPid([1, 600, 17, 1]),
PeerIP/Port(10.106.104.220:7501), LocalIP/Port(10.106.104.201:56181) TLSReq(t) established
```

连接失败，因为辐条的Tomcat证书是自签名的

中心的日志表示分支的自签名证书的证书验证失败。

集线器中的日志片段：

```
00000103.000 |09:44:16.896 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification
failed:(Verification error:18)-
self signed certificate for 10.106.104.201:52124

00000104.000 |09:44:16.896 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification
failed for 10.106.104.201:52124

00000106.000 |09:44:16.896 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - TLS protocol error(ssl
reason code=internal error [68]),lib=SSL routines [20],fun=SSL_clear [164], errno=0 for
10.106.104.201:52124
```

连接失败，因为集线器的Tomcat证书是自签名的

来自分支的日志表示中心的自签名证书的证书验证故障。

从Spoke记录代码段：

```
00000064.000 |12:44:19.641 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification
failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501

00000065.000 |12:44:19.641 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification
failed for 10.106.104.220:7501

00000067.000 |12:44:19.641 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - TLS protocol error(ssl
reason code=bad message type [114]),lib=SSL routines [20],fun=ssl3_get_server_hello [146],
errno=0 for 10.106.104.220:7501
```

注意：当中心辐射点和辐射点都具有自签名时，本例中出现的错误也相同。

方法4的ILS注册日志分析

当从已建立的连接使用密码身份验证切换到TLS身份验证时，分支成功注册到中心。

PeerInfoVector中显示的远程群集的FQDN，因为连接已使用密码身份验证方法建立。 从密码身份验证方法切换到TLS时，**日志中**会显示“X509_STORE_get_by_subject failed”错误，因为tomcat证书未交叉导入。但是，由于“FQDN在PeerInfoVector中”，因此仍使用TLS接受连接。

集线器中的日志片段：

```
00000169.001 |19:41:50.255 |AppInfo  |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject
failed.

00000169.002 |19:41:50.255 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): FQDN is in
PeerInfoVector

00000169.003 |19:41:50.255 |AppInfo  |IlsD IlsHandler: Ils::wait_SdlConnectionInd(): New
connection accepted. DeviceName=, TCPPid = [1.600.17.1], IPAddr=10.106.104.201, Port=51887,
Controller=[1,20,1]
```

Spoke中的日志片段：

```
00000072.001 |19:41:50.257 |AppInfo  |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject
failed.

00000072.002 |19:41:50.257 |AppInfo  |IlsD Ils::VerifyCertificateInfo(): FQDN is in
PeerInfoVector
```

连接失败，因为集线器在切换到TLS身份验证时具有自签名证书 从已建立的连接使用密码身份验证。

来自辐条的日志表示中心的自签名证书的证书验证失败。

Spoke中的日志片段：

```
00000151.000 |12:29:18.600 |AppInfo  |[1, 600, 17, 2]: HandleSSLError - Certificate verification
failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501

00000152.000 |12:29:18.600 |AppInfo  |[1, 600, 17, 2]: HandleSSLError - Certificate verification
failed for 10.106.104.220:7501
```

当切换到TLS身份验证时，连接失败，因为分支具有自签名证书 从已建立的连接使用密码身份验证

- 中心日志指示分支的自签名证书的证书验证失败

集线器中的日志片段：

```
00000089.000 |09:32:27.365 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.201:41295

00000090.000 |09:32:27.365 |AppInfo  |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed for 10.106.104.201:41295
```