配置ILS加入集群並對其進行故障排除

目錄

簡介

本文檔介紹用於加入群集以進行群集間查詢服務(ILS)的可能配置方法，並記錄分析以排除每種方法的故障。

必要條件

需求

本文件沒有特定需求。

採用元件

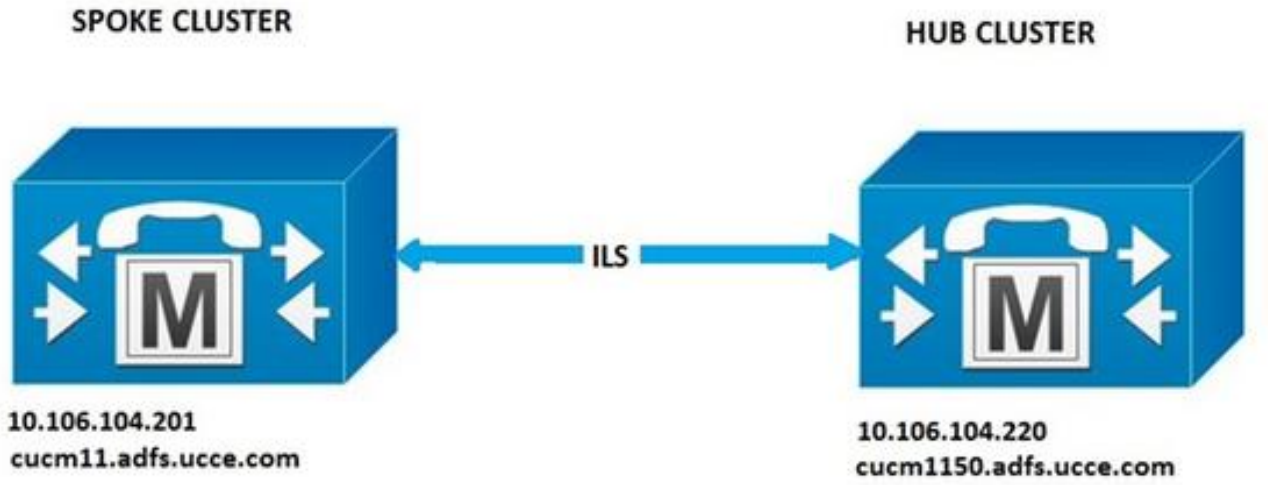
本文中的資訊係根據以下軟體和硬體版本：

- 思科整合通訊管理員(CUCM)版本11.5

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。

設定

網路圖表



組態

方法1.在群集之間使用密碼身份驗證

登入到CUCM管理頁面，導航到**高級功能> ILS配置**。
在ILS配置視窗中，選中**Use Password**覈取方塊。

管理密碼，然後按一下「**Save**」。在ILS網路中的所有集群中密碼必須相同。

方法2.在集群之間使用TLS身份驗證

要使用此方法，請確保所有要成為ILS網路一部分的群集都已匯入其tomcat-trust中的遠端群集Tomcat Certificates。

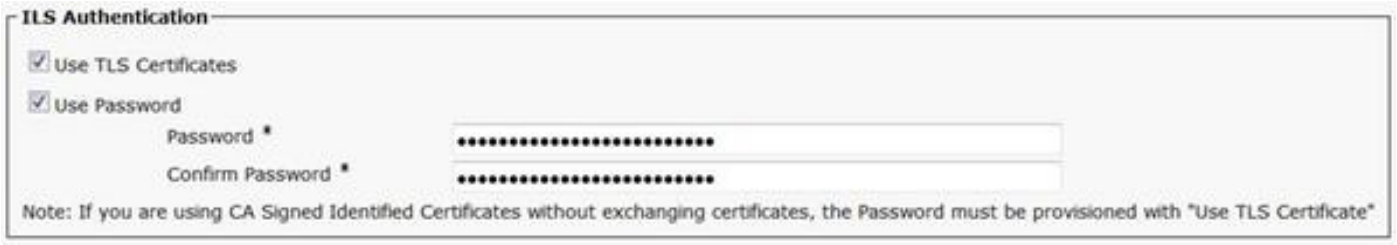
在CUCM管理中，導航到**高級功能> ILS配置**。在ILS配置視窗中，選中ILS身份驗證下的**使用TLS證書**覈取方塊。

方法3.在群集之間使用帶有密碼身份驗證的TLS。

此方法的優點在於，如果外部證書頒發機構(CA)已簽署，則無需在群集之間交叉匯入Tomcat證書來建立TLS連線。 CUCM 11.5及更高版本提供此方法。

要使用此方法，請確保要成為ILS網路一部分的所有群集都擁有由外部CA簽名的tomcat證書，並且此CA的根證書存在於tomcat-trust中。此外，在ILS網路中的所有群集中，密碼必須相同。

在CUCM管理中，導航到ILS身份驗證下的**高級功能>ILS配置**，選中**使用TLS證書**和**使用密碼**覈取方塊。



方法4.使用密碼身份驗證加入群集後切換到TLS身份驗證。

這是使用TLS的另一種方式，它不會在群集之間交叉匯入Tomcat證書（如果它由外部CA簽名）。這對於11.5之前的CUCM版本非常有用，其中不支援方法3。

要使用此方法，請確保要成為ILS網路一部分的所有群集都擁有由外部CA簽名的tomcat證書，並且此CA的根證書存在於tomcat-trust中。

首先使用密碼身份驗證加入群集。在Cisco Unified CM管理中，導航到**高級功能> ILS配置**。在ILS身份驗證下，選中**使用密碼**覈取方塊。管理密碼。按一下「Save」。

加入群集時，客戶端和伺服器端的密碼必須相同。

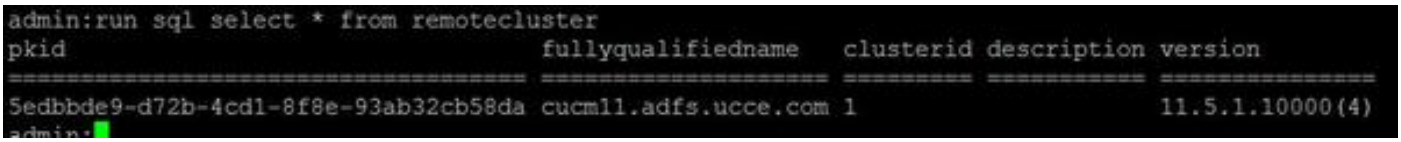
建立連線後，將驗證方法更改為TLS。 在CUCM管理中，導航到**高級功能> ILS Configuration**。在ILS Configuration視窗中，選中ILS Authentication下的**Use TLS Certificates**覈取方塊。

驗證

可在中的ILS群集和全域性撥號計畫匯入目錄下看到成功的註冊

高級功能> ILS配置

使用命令*run sql select * from remotecluster列出遠端群集詳細資訊*



疑難排解

將Cisco Intercluster Lookup Service的調試跟蹤級別設定為detailed。

跟蹤的位置： activelog /cm/trace/ils/sdl/

通過示例說明了每個ILS註冊方法的成功和失敗方案的日誌分析。

方法1的ILS註冊日誌分析

分支在群集之間使用密碼身份驗證成功註冊到中心

來自集線器的日誌片段：

```
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
```

來自分支的日誌片段：

```
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
```

分支到嘗試註冊到中心，但由於密碼不匹配而失敗

DecryptData失敗，中心日誌中的ILSPwdAuthenticationFailed警報表示密碼不匹配。

來自集線器的日誌片段：

```
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
```

附註：當連線由於密碼不匹配而失敗時，其餘方法的錯誤也相同。

方法2的ILS註冊日誌分析

分支使用TLS身份驗證成功註冊到中心

來自集線器的日誌片段：

```
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
```

來自分支的日誌片段：

```
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
```

連線失敗，因為中心的Tomcat證書未匯入到分支

「分支中的日誌」表示中心伺服器的證書驗證失敗。

來自分支的日誌片段：

```
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)
```

連線失敗，因為未在中心匯入分支的Tomcat證書

來自集線器的日誌指示連線已關閉，既不是本地儲存中的分支證書，也不是對等體資訊向量中的FQDN。

來自集線器的日誌片段：

```
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註冊日誌分析

分支使用帶有密碼身份驗證的TLS成功註冊到中心

來自集線器的日誌片段：

```
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
```

來自分支的日誌片段：

```
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
```

連線失敗，因為分支的Tomcat證書是自簽名的

來自中心的日誌指示分支的自簽名證書的證書驗證失敗。

來自集線器的日誌片段：

```
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
```

連線失敗，因為集線器的Tomcat證書是自簽名的

來自分支的日誌指示中心自簽名證書的證書驗證失敗。

來自分支的日誌片段：

```
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
```

附註：在此案例中出現的錯誤在中心和分支都已自簽名時也相同。

方法4的ILS註冊日誌分析

在使用密碼身份驗證從已建立的連線切換到TLS身份驗證時，分支已成功註冊到中心。

已使用密碼身份驗證方法建立連線時在PeerInfoVector中顯示的遠端群集的FQDN。 從密碼驗證方法切換到TLS時，日誌中會顯示"X509_STORE_get_by_subject failed"錯誤，因為tomcat證書沒有交叉匯入。但是，由於「FQDN位於PeerInfoVector」，因此連線仍使用TLS接受。

來自集線器的日誌片段：

```
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]
```

來自分支的日誌片段：

```
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
```

當集線器切換到TLS身份驗證時具有自簽名證書時，連線失敗 使用密碼身份驗證從已建立的連線。

來自分支的日誌指示中心自簽名證書的證書驗證失敗。

來自分支的日誌片段：

```
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
```

切換到TLS身份驗證時，連線失敗，因為分支具有自簽名證書 使用密碼身份驗證從已建立的連線。

來自中心的日誌指示分支的自簽名證書的證書驗證失敗

來自集線器的日誌片段：

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