Configurar e solucionar problemas de junção de clusters para ILS

Contents

Introduction

Este documento descreve os possíveis métodos de configuração para unir Clusters para Serviço de Pesquisa Intercluster (ILS) e também a análise de log para solucionar problemas em cada um dos métodos.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

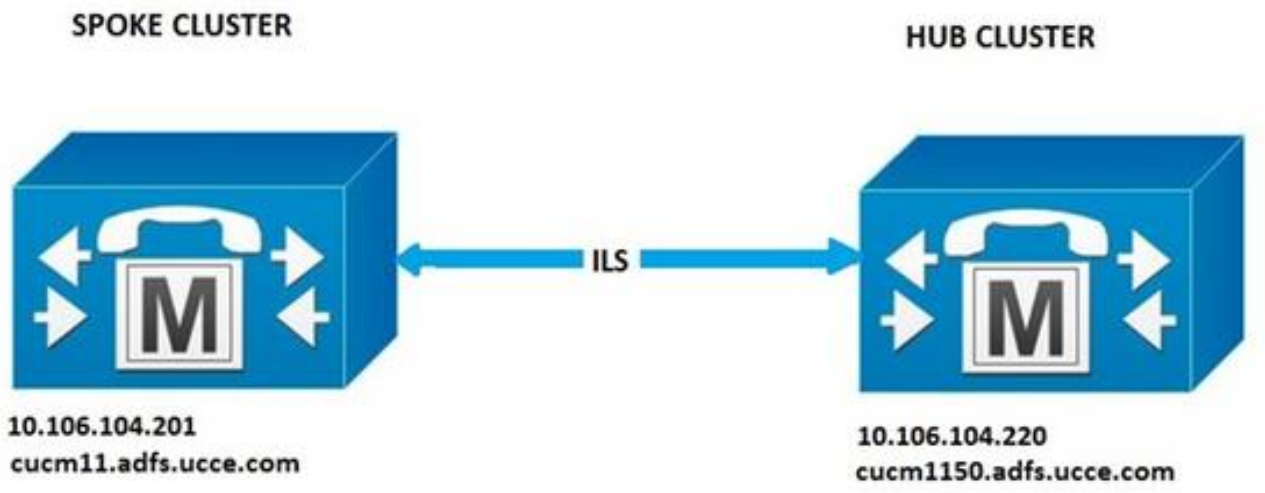
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager (CUCM) versão 11.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de Rede



Configurações

Método 1. Usando a autenticação de senha entre clusters

Faça login na página de administração do CUCM, navegue para **Advanced Features > ILS Configuration**.
Na janela Configuração de ILS, marque a caixa de seleção **Usar senha**.

Gerencie as senhas e pressione **Salvar**. A senha deve ser a mesma em todos os clusters na rede ILS.

Método 2. Usando a autenticação TLS entre clusters

Para usar esse método, assegure-se de que todos os clusters que fazem parte da rede ILS importaram os clusters remotos Certificados Tomcat em sua confiança de tomcat.

Na Administração do CUCM, navegue para **Recursos avançados > Configuração do ILS**. Na janela Configuração de ILS, marque a caixa de seleção **Usar certificados TLS** em Autenticação de ILS.

Método 3. Usar TLS com autenticação de senha entre clusters.

A vantagem desse método é que não há necessidade de importar os Certificados Tomcat entre os clusters para estabelecer a conexão TLS se ela for assinada pela Autoridade de Certificação Externa (CA). Esse método está disponível no CUCM 11.5 e posterior.

Para usar esse método, certifique-se de que todos os clusters que fazem parte da rede ILS tenham os certificados tomcat assinados por uma CA externa e o certificado raiz desta CA esteja presente em tomcat-trust. Além disso, a senha deve ser a mesma em todos os clusters na rede ILS.

Na Administração do CUCM, navegue até **Advanced Features > ILS Configuration** em ILS Authentication, marque a caixa de seleção **Use TLS Certifications** e **Use Password**.

Método 4. Alternar para Autenticação TLS depois que o cluster é associado à autenticação Senha.

Essa é outra maneira de usar o TLS sem importar os certificados Tomcat entre os clusters se eles forem assinados por CA externa. Isso é útil para versões anteriores a 11.5 do CUCM em que o

método 3 não é suportado.

Para usar esse método, certifique-se de que todos os clusters que fazem parte da rede ILS tenham os certificados tomcat assinados por uma CA externa e o certificado raiz desta CA esteja presente em tomcat-trust.

Ingresse no cluster primeiro usando a Autenticação de senha. No Cisco Unified CM Administration, navegue para **Advanced Features > ILS Configuration**. Em Autenticação ILS, marque a caixa de seleção **Usar senha**. Gerencie as senhas. Click Save.

A senha deve ser a mesma no lado do cliente e do servidor no momento de ingressar no cluster.

Depois que a Conexão for estabelecida, altere o método de autenticação para TLS. Na Administração do CUCM, navegue até **Advanced Features > ILS Configuration**. Na janela Configuração de ILS, marque a caixa de seleção **Usar certificados TLS** em Autenticação de ILS.

Verificar

O registro bem-sucedido pode ser visto em clusters ILS e catálogos importados do plano de discagem global em

Recursos avançados > Configuração de ILS

Os detalhes do cluster remoto são listados usando o comando ***run sql select * de remotecluster***

```
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:
```

Troubleshoot

Defina o nível de rastreamento de depuração do Cisco Intercluster Lookup Service como detalhado.

Localização do Rastreamento: ativelog /cm/trace/ils/sdl/

A análise de log para cenários de Êxito e Falha para cada método de registro ILS com exemplo é explicada.

Análise de log para registro ILS do método 1

Registros spoke bem-sucedidos no hub usando autenticação de senha entre clusters

Trecho de log do hub:

```
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
```

Trecho de log do Spoke:

```
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
```

Falou para Tentar se Registrar no Hub, mas falhou devido à incompatibilidade de senha

DecryptData falhou e o alarme ILSPwdAuthenticationFailed nos registros do Hub indica a incompatibilidade da senha.

Trecho de log do hub:

```
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
```

> **Note**: O erro também é o mesmo em todos os métodos sempre que a conexão falha devido a uma incompatibilidade de senha.

Análise de log para registro ILS do método 2

Registros spoke com êxito no hub usando autenticação TLS

Trecho de log do hub:

```
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
```

Trecho de log do Spoke:

```
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
```

A conexão falha porque o certificado Tomcat do hub não é importado no Spoke

O log do Spoke indica que a verificação de certificado do hub falhou.

Trecho de log do Spoke:

```
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)
```

A conexão falha porque o certificado Tomcat do spoke não é importado no hub

Os registros do hub indicam que a conexão está fechada como nem o certificado do spoke na loja local, nem o FQDN no vetor de informações do peer.

Trecho de log do hub:

```
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
```

Análise de log para registro ILS do método 3

Registros spoke com êxito no hub usando TLS com autenticação de senha

Trecho de log do hub:

```
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
```

Trecho de log do Spoke:

```
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
```

A conexão falha porque o certificado Tomcat do spoke é autoassinado

Logs do hub indicam falha na verificação do certificado para o certificado autoassinado do spoke.

Trecho de log do hub:

```
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
```

A conexão falha porque o certificado Tomcat do hub é autoassinado

Os registros do Spoke indicam falha de verificação de certificado para certificado autoassinado do hub.

Trecho de log do Spoke:

```
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
```

> **Note**: O erro visto nesse caso também é o mesmo quando o hub e o spoke se autoinscreveram.

Análise de log para registro ILS do método 4

O spoke registra com êxito no hub ao alternar para Autenticação TLS a partir da conexão estabelecida usando Autenticação de senha.

FQDN do cluster remoto apresentado no PeerInfoVetor, pois a conexão já está estabelecida com o método de autenticação de senha. Ao alternar para TLS a partir do método de autenticação de senha, o erro "X509_STORE_get_by_subject failed" é impresso nos registros, pois o certificado tomcat não é importado cruzadamente. Mas a conexão ainda é aceita usando TLS, pois "FQDN está em PeerInfoVetor".

Trecho de log do hub:

```
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]
```

Trecho de log do Spoke:

```
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
```

A conexão falha porque o hub tem o certificado autoassinado ao alternar para a autenticação TLS da conexão estabelecida usando a Autenticação de senha.

Os registros do Spoke indicam falha na verificação do certificado para o certificado autoassinado do hub.

Trecho de log do Spoke:

```
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
```

A conexão falha como Spoke possui certificado autoassinado ao alternar para a autenticação TLS da conexão estabelecida usando a Autenticação de senha.

Os registros do hub indicam falha na verificação do certificado para o certificado autoassinado do spoke

Trecho de log do hub:

```
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
```