Configurazione e risoluzione dei problemi relativi all'unione di cluster per ILS

Sommario

Introduzione

In questo documento vengono descritti i possibili metodi di configurazione per unire i cluster per il servizio di ricerca intercluster (ILS) e l'analisi dei registri per risolvere i problemi relativi a ciascuno di essi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

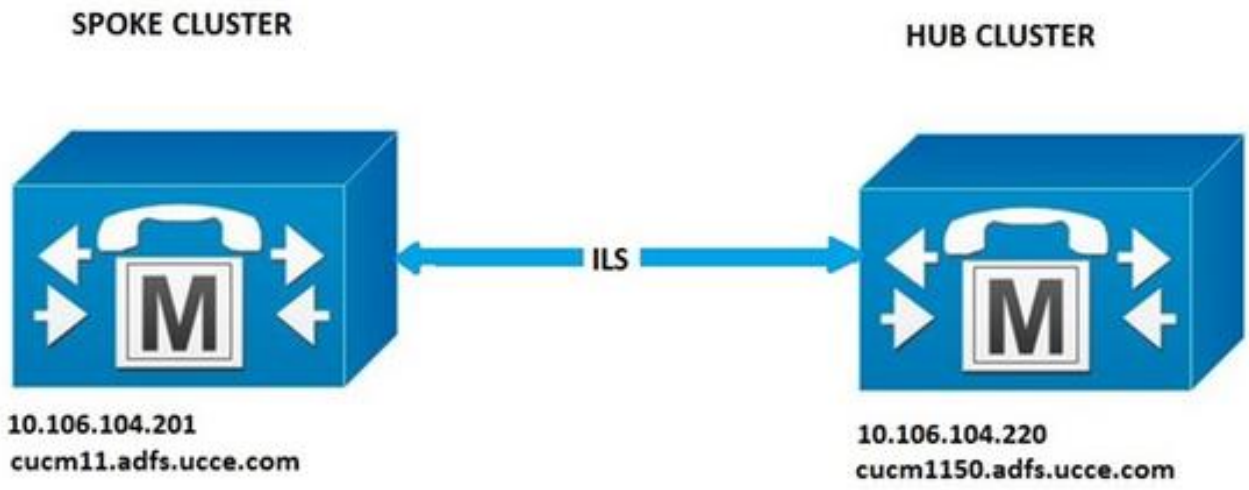
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Communications Manager (CUCM) versione 11.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

Metodo 1. Utilizzo dell'autenticazione tramite password tra cluster

Accedere alla pagina Amministrazione CUCM, selezionare **Funzioni avanzate > Configurazione ILS**.
Nella finestra Configurazione ILS selezionare la casella di controllo **Usa password**.

Gestire le password, quindi fare clic su **Salva**. La password deve essere la stessa per tutti i cluster nella rete ILS.

Metodo 2. Utilizzo dell'autenticazione TLS tra cluster

Per utilizzare questo metodo, verificare che tutti i cluster che devono far parte di ILS Network abbiano importato i certificati Tomcat dei cluster remoti nel relativo tomcat-trust.

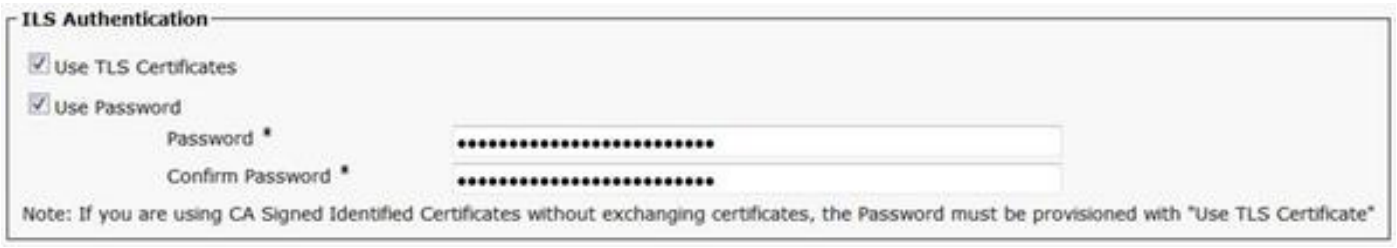
In Amministrazione CUCM passare a **Funzionalità avanzate > Configurazione ILS**. Nella finestra Configurazione ILS selezionare la casella di controllo **Usa certificati TLS** in Autenticazione ILS.

Metodo 3. Utilizzare TLS con autenticazione tramite password tra cluster.

Il vantaggio di questo metodo è che non è necessario importare i certificati Tomcat tra i cluster per stabilire la connessione TLS se è firmata da una CA (Certification Authority) esterna. Questo metodo è disponibile da CUCM 11.5 e versioni successive.

Per utilizzare questo metodo, verificare che tutti i cluster che fanno parte della rete ILS dispongano di certificati tomcat firmati da una CA esterna e che il certificato radice di questa CA sia presente in tomcat-trust. Inoltre, la password deve essere la stessa in tutti i cluster nella rete ILS.

In Amministrazione CUCM, selezionare **Funzioni avanzate > Configurazione ILS** In Autenticazione ILS, selezionare la casella di controllo **Usa certificati TLS** e **Usa password**.



Metodo 4. Passaggio all'autenticazione TLS dopo l'unione del cluster con l'autenticazione tramite password.

Questo è un altro modo per utilizzare TLS senza importare i certificati Tomcat tra i cluster se è firmato da una CA esterna. Ciò è utile per le versioni di CUCM precedenti alla 11.5 in cui il metodo 3 non è supportato.

Per utilizzare questo metodo, verificare che tutti i cluster che fanno parte della rete ILS dispongano di certificati tomcat firmati da una CA esterna e che il certificato radice di questa CA sia presente in tomcat-trust.

Eseguire il join del cluster utilizzando prima l'autenticazione tramite password. In Amministrazione Cisco Unified CM, selezionare **Funzioni avanzate > Configurazione ILS**. In Autenticazione ILS, selezionare la casella di controllo **Usa password**. Gestire le password. Fare clic su **Salva**.

La password deve essere la stessa sul lato client e server al momento dell'aggiunta al cluster.

Una volta stabilita la connessione, modificare il metodo di autenticazione in TLS. In Amministrazione CUCM, selezionare **Funzioni avanzate > Configurazione ILS**. Nella finestra Configurazione ILS selezionare la casella di controllo **Usa certificati TLS** in Autenticazione ILS.

Verifica

La corretta registrazione può essere verificata in Cluster ILS e Global DialPlan Imported Catalogs in

Funzioni avanzate > Configurazione ILS

I dettagli del cluster remoto vengono elencati utilizzando il comando ***run sql select * from 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:
```

Risoluzione dei problemi

Impostare il livello di traccia del debug per il servizio di ricerca tra cluster Cisco su Detailed.

Percorso della traccia: activelog /cm/trace/ils/sdl/

Viene illustrata l'analisi del log per gli scenari di esito positivo e negativo per ciascun metodo di registrazione ILS con l'esempio.

Analisi dei log per la registrazione ILS per il metodo 1

Registri spoke riusciti nell'hub utilizzando l'autenticazione tramite password tra cluster

Frammento di log dall'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
```

Frammento di registro da 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
```

Spoke to Tenta di eseguire la registrazione nell'hub, ma l'operazione non riesce a causa della mancata corrispondenza della password

DecryptData non riuscito. L'allarme ILSPwdAuthenticationFailed nei log hub indica la mancata corrispondenza della password.

Frammento di log dall'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
```

> **Nota:** L'errore è lo stesso nel resto dei metodi anche quando la connessione non riesce a causa di una mancata corrispondenza della password.

Analisi dei log per la registrazione ILS per il metodo 2

Registrazione Spoke completata nell'hub con autenticazione TLS

Frammento di log dall'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
```

Registra frammento di codice da 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
```

Connessione non riuscita perché il certificato Tomcat dell'hub non è importato in Spoke

Registra da spoke indica che la verifica del certificato per l'hub non è riuscita.

Frammento di registro da 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)
```

Connessione non riuscita perché il certificato Tomcat del spoke non è importato nell'hub

I registri dall'hub indicano che la connessione non è chiusa come certificato dello spoke nell'archivio locale né come FQDN nel vettore di informazioni peer.

Frammento di log dall'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
```

Analisi dei log per la registrazione ILS per il metodo 3

Registrazione Spoke completata nell'hub utilizzando TLS con autenticazione password

Frammento di log dall'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
```

Frammento di registro da 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
```

Connessione non riuscita perché il certificato Tomcat del raggio è autofirmato

Registri dall'hub Indica un errore di verifica del certificato per il certificato autofirmato del spoke.

Frammento di log dall'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
```

Connessione non riuscita perché il certificato Tomcat dell'hub è autofirmato

Registri da spoke indica un errore di verifica del certificato per il certificato autofirmato dell'hub.

Registra frammento di codice da 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
```

> **Nota:** L'errore rilevato in questo caso è lo stesso anche quando sia l'hub che lo spoke hanno la propria firma.

Analisi dei log per la registrazione ILS per il metodo 4

La funzionalità Spoke viene registrata correttamente nell'hub quando si passa all'autenticazione TLS dalla connessione stabilita utilizzando l'autenticazione tramite password.

FQDN del cluster remoto presentato in PeerInfoVector perché la connessione è già stabilita con il metodo di autenticazione tramite password. Quando si passa a TLS dal metodo di autenticazione tramite password, l'errore "X509_STORE_get_by_subject failed" viene stampato nei log poiché il certificato tomcat non viene importato. Tuttavia, la connessione è ancora accettata utilizzando TLS poiché "FQDN è in PeerInfoVector".

Frammento di log dall'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]
```

Frammento di registro da 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
```

Connessione non riuscita perché l'hub dispone di un certificato autofirmato quando si passa all'autenticazione TLS dalla connessione stabilita utilizzando l'autenticazione tramite password.

Registri da spoke indica un errore di verifica certificato per il certificato autofirmato dell'hub.

Frammento di registro da 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
```

La connessione non riesce perché il certificato autofirmato è attivo quando si passa all'autenticazione TLS dalla connessione stabilita utilizzando l'autenticazione tramite password.

Registri dall'hub indica un errore di verifica del certificato per il certificato autofirmato del spoke

Frammento di log dall'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
```