

ILSのクラスタ参加の設定とトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[方法1.クラスタ間でのパスワード認証の使用](#)

[方法2.クラスタ間でのTLS認証の使用](#)

[方法3.クラスタ間でパスワード認証を使用するTLS](#)

[方法4.クラスタがパスワード認証に参加した後にTLS認証に切り替える。](#)

[確認](#)

[トラブルシュート](#)

[方法1のILS登録用ログ分析](#)

[クラスタ間のパスワード認証を使用したスポークのハブへの登録](#)

[スポークからハブへの登録が試行されるが、パスワードの不一致により失敗する](#)

[方法2のILS登録用ログ分析](#)

[スポークがTLS認証を使用してハブに正常に登録される](#)

[ハブのTomcat証明書がスポークにインポートされないため、接続が失敗する](#)

[スポークのTomcat証明書がハブにインポートされないため、接続が失敗する](#)

[方法3のILS登録用ログ分析](#)

[パスワード認証によるTLSを使用してスポークがハブに正常に登録される](#)

[スポークのTomcat証明書が自己署名であるため、接続が失敗する](#)

[ハブのTomcat証明書が自己署名であるため、接続が失敗する](#)

[方法4のILS登録用ログ分析](#)

[Spoke Registers Successfully to the Hub when switching to TLS Authentication from the established connection using Password Authentication.」](#)

[パスワード認証を使用して確立された接続からTLS認証に切り替えると、ハブに自己署名証明書があるため、接続が失敗します。](#)

[パスワード認証を使用して確立された接続からTLS認証に切り替えると、スポークに自己署名証明書があるため、接続が失敗します。](#)

概要

このドキュメントでは、クラスタ間検索サービス(ILS)のクラスタに参加するための可能な設定方法と、それぞれの方法をトラブルシューティングするためのログ分析について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

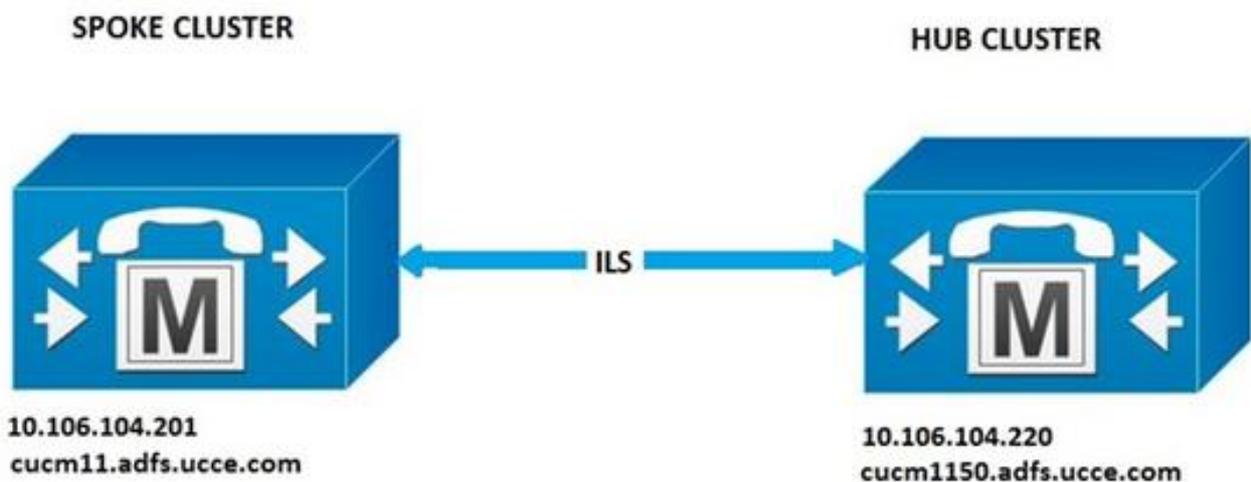
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Unified Communications Manager (CUCM) バージョン 11.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク図



設定

方法1. クラスタ間でのパスワード認証の使用

[CUCM Administration] ページにログインし、[Advanced Features] > [ILS Configuration] に移動します。

[ILS 設定 (ILS Configuration)] ウィンドウで、[パスワードを使用 (Use Password)] チェックボックスをオンにします。

パスワードを管理し、[Save] をクリックします。パスワードは、ILS ネットワーク内のすべてのクラスタで同じである必要があります。

ILS Authentication

Use TLS Certificates

Use Password

Password *

Confirm Password *

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

方法2. クラスタ間でのTLS認証の使用

この方法を使用するには、ILSネットワークの一部となるすべてのクラスタが、そのtomcat-trustにリモートクラスタTomcat証明書をインポートしていることを確認します。

CUCM Administrationで、[Advanced Features] > [ILS Configuration]に移動します。[ILS Configuration]ウィンドウで、[ILS Authentication]の下の[Use TLS Certificates]チェックボックスをオンにします。

ILS Authentication

Use TLS Certificates

Use Password

Password *

Confirm Password *

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

方法3. クラスタ間でパスワード認証を使用するTLS。

この方法の利点は、外部認証局(CA)によって署名されている場合、クラスタ間でTomcat証明書をクロスインポートしてTLS接続を確立する必要がないことです。この方法は、CUCM 11.5以降で使用できます。

この方法を使用するには、ILSネットワークの一部となるすべてのクラスタに、外部CAによって署名されたtomcat証明書があり、このCAのルート証明書がtomcat-trustにあることを確認します。また、パスワードはILSネットワーク内のすべてのクラスタで同じである必要があります。

CUCM Administrationで、[Advanced Features] > [ILS Configuration]に移動し、[ILS Authentication]で[Use TLS Certificates]および[Use Password]チェックボックスをオンにします。

ILS Authentication

Use TLS Certificates

Use Password

Password *

Confirm Password *

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

方法4. クラスタがパスワード認証に参加した後にTLS認証に切り替える。

これは、外部CAによって署名されている場合に、クラスタ間でTomcat証明書をクロスインポートせずにTLSを使用するもう1つの方法です。これは、方法3がサポートされていない11.5よりも前のCUCMバージョンで役立ちます。

この方法を使用するには、ILSネットワークの一部となるすべてのクラスタに、外部CAによって署名されたtomcat証明書があり、このCAのルート証明書がtomcat-trustにあることを確認します。

まず、パスワード認証を使用してクラスタに参加します。Cisco Unified CM Administrationで、[Advanced Features] > [ILS Configuration]に移動します。[ILS Authentication]の下の[Use Password]チェックボックスをオンにします。パスワードを管理します。[Save] をクリックします。

パスワードは、クラスタ加入時のクライアント側とサーバ側で同じである必要があります。



The screenshot shows the 'ILS Authentication' configuration window. The 'Use Password' checkbox is checked, while 'Use TLS Certificates' is unchecked. There are two password input fields, both containing masked characters. A note at the bottom states: 'Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"'

接続が確立されたら、認証方式をTLSに変更します。CUCM Administrationで、[Advanced Features] > [ILS Configuration]に移動します。[ILS設定(ILS Configuration)]ウィンドウで、[ILS認証(ILS Authentication)]の下の[TLS証明書を使用(Use TLS Certificates)]チェックボックスをオンにします。



The screenshot shows the 'ILS Authentication' configuration window. The 'Use TLS Certificates' checkbox is checked, while 'Use Password' is unchecked. There are two password input fields, both containing masked characters. A note at the bottom states: 'Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"'

確認

正常な登録は、の[ILSクラスタ(ILS Clusters)]および[グローバルダイヤルプランインポート済みカタログ(Global DialPlan Imported Catalogs)]で確認できます。

[拡張機能(Advanced Features)] > [ILS設定(ILS Configuration)]



Cluster ID/Name	Last Contact Time	Role	Advertised Route String	Last USN Data Received	USN Data Synchronization Status	Action
2	-	Hub (Local Cluster)	com1150.adfs.uccs.com	-	Up to date	Disconnect
1	8/26/16 5:06 PM	Spoke	cucm11.adfs.uccs.com	8/26/16 5:06 PM	Up to date	Disconnect

リモートクラスタの詳細は、コマンド `run sql select * from remotecluster` を使用して表示されます

```
admin:run sql select * from remotecluster
pkid                fullyqualifiedname  clusterid description version
=====
5edbbe9-d72b-4cd1-8f8e-93ab32cb58da cucm11.adfs.uccs.com 1          11.5.1.10000 (4)
admin:
```

トラブルシューティング

Cisco Intercluster Lookupサービスのデバッグトレースレベルをdetailedに設定します。

トレースの場所 : activelog /cm/trace/ils/sdl/

各ILS登録方法の成功シナリオと失敗シナリオのログ分析とその例について説明します。

方法1のILS登録用ログ分析

クラスタ間のパスワード認証を使用したスポークのハブへの登録

ハブからのログスニペット :

```
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
```

スポークからのログスニペット :

```
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
```

スポークからハブへの登録が試行されるが、パスワードの不一致により失敗する

DecryptDataが失敗し、HubログのILSPwdAuthenticationFailedアラームがパスワードの不一致を示します。

ハブからのログスニペット :

```
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：パスワードの不一致が原因で接続が失敗した場合も、他の方法と同じエラーが発生します。

方法2のILS登録用ログ分析

スポークがTLS認証を使用してハブに正常に登録される

ハブからのログスニペット：

```
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
```

スポークからのログスニペット：

```
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
```

ハブのTomcat証明書がスポークにインポートされないため、接続が失敗する

スポークからのログは、ハブの証明書検証が失敗したことを示します。

スポークからのログスニペット：

```
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)
```

スポークのTomcat証明書がハブにインポートされないため、接続が失敗する

ハブからのログは、ローカルストアのスポークの証明書でも、ピア情報ベクターのFQDNでもない接続が閉じられていることを示します。

ハブからのログスニペット：

```
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のILS登録用ログ分析

パスワード認証によるTLSを使用してスポークがハブに正常に登録される

ハブからのログスニペット :

```
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 succeeded
```

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

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

```
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
```

スポークからのログスニペット :

```
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
```

スポークのTomcat証明書が自己署名であるため、接続が失敗する

ハブからのログは、スポークの自己署名証明書の証明書検証の失敗を示します。

ハブからのログスニペット :

```
00000103.000 |09:44:16.896 |AppInfo |[1, 600, 17, 1]: HandleSSL error - 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]: HandleSSL error - Certificate verification failed for 10.106.104.201:52124
```

```
00000106.000 |09:44:16.896 |AppInfo |[1, 600, 17, 1]: HandleSSL error - 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
```

ハブのTomcat証明書が自己署名であるため、接続が失敗する

スポークからのログは、ハブの自己署名証明書の証明書検証障害を示します。

スポークからのログスニペット :

```
00000064.000 |12:44:19.641 |AppInfo |[1, 600, 17, 1]: HandleSSL error - 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]: HandleSSL error - Certificate verification failed for 10.106.104.220:7501
```

```
00000067.000 |12:44:19.641 |AppInfo |[1, 600, 17, 1]: HandleSSL error - 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：この場合に表示されるエラーは、ハブとスポークの両方が自己署名している場合も同じです。

方法4のILS登録用ログ分析

Spoke Registers Successfully to the Hub when switching to TLS Authentication from the established connection using Password Authentication.」

接続がパスワード認証方式で既に確立されているため、PeerInfoVectorに表示されるリモートクライアントのFQDN。パスワード認証方式からTLSに切り替えると、tomcat証明書がクロスインポートされないため、ログに「X509_STORE_get_by_subject failed」エラーが出力されます。ただし、「FQDNはPeerInfoVectorに含まれる」ため、TLSを使用して接続が引き続き受け入れられます。

ハブからのログスニペット :

```
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]
```

スポークからのログスニペット :

```
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
```

TLS認証に切り替えるとハブに自己署名証明書があるため接続が失敗する 設定します。

スポークからのログは、ハブの自己署名証明書の証明書検証の失敗を示します。

スポークからのログスニペット :

```
00000151.000 |12:29:18.600 |AppInfo |[1, 600, 17, 2]: HandleSSLSError - 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]: HandleSSLSError - Certificate verification failed for 10.106.104.220:7501
```

TLS認証に切り替えたときにスポークに自己署名証明書があるため、接続が失敗する 設定します。

ハブからのログは、スポークの自己署名証明書の証明書検証の失敗を示します

ハブからのログスニペット :

```
00000089.000 |09:32:27.365 |AppInfo |[1, 600, 17, 1]: HandleSSLSError - 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]: HandleSSLSError - Certificate verification failed for 10.106.104.201:41295
```