Introduction

This document describes the possible configuration methods to join Clusters for Intercluster Lookup Service (ILS) also log analysis to troubleshoot each the methods.

Prerequisites

Requirements

There are no specific requirements for this document.
Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager (CUCM) Version 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.

Configure

Network Diagram

![Network Diagram](image)

Configurations

Method 1. Using Password Authentication between Clusters

Log in to CUCM Administration Page, navigate to Advanced Features > ILS Configuration. In the ILS Configuration window, check the Use Password check box.

Manage the passwords then hit Save. The password must be same across all clusters in the ILS network.

![ILS Authentication](image)

Method 2. Using TLS Authentication between Clusters

To use this method, ensure that all clusters that to be a part of ILS Network have imported the
remote clusters Tomcat Certificates in its tomcat-trust.

In CUCM Administration, navigate to Advanced Features > ILS Configuration. In the ILS Configuration window, check the Use TLS Certificates check box under ILS Authentication.

**Method 3. Use TLS with Password Authentication between Clusters**

The advantage of this method is that no need to cross import the Tomcat Certificates between the clusters to establish the TLS connection if it’s signed by External Certificate Authority(CA). This method is available from CUCM 11.5 and later.

To use this method, ensure that all clusters that to be a part of ILS Network have the tomcat certificates signed by an External CA and the root certificate of this CA is present in tomcat-trust. Also, the password must be same across all clusters in the ILS network.

In CUCM Administration, navigate to Advanced Features > ILS Configuration Under ILS Authentication, check the Use TLS Certificates and Use Password check box.

**Method 4. Switching to TLS Authentication after cluster is joined with Password authentication.**

This is another way to use TLS without cross importing the Tomcat Certificates between the clusters if it’s signed by External CA. This is useful for CUCM versions prior 11.5 where method 3 is not supported.

To use this method, ensure that all clusters that to be a part of ILS Network have the tomcat certificates signed by an External CA and the root certificate of this CA is present in tomcat-trust.

Join the cluster first using the Password Authentication. In Cisco Unified CM Administration, navigate to Advanced Features > ILS Configuration. Under ILS Authentication, check Use Password check box. Manage the Passwords. Click Save.

The password must be same in client and server side at the time of joining the cluster.
Once the Connection is established, change the authentication method to TLS. In CUCM Administration, navigate to Advanced Features > ILS Configuration. In the ILS Configuration window, check the Use TLS Certificates check box under ILS Authentication.

![ILS Authentication](image)

Verify

Successful registration can be seen under ILS Clusters and Global DialPlan Imported Catalogs in Advanced Features > ILS Configuration

![ILS Clusters and Global DialPlan Imported Catalogs](image)

Remote cluster details are listed using command `run sql select * from remotecluster`

```
admin:run sql select * from remotecluster
```

Troubleshoot

Set the debug trace level for Cisco Intercluster Lookup Service to detailed.

Location for the Trace : activelog /cm/trace/ils/sdl/

The log analysis for Success and Failure scenarios for each ILS registration methods with example ar explained.

Log Analysis for ILS Registration for Method 1

Spoke Registers Succesfully to the Hub using Password Authentication between Clusters

Log Snippet from Hub:

Log snippet from Spoke:

Spoke to Tries to Register to Hub but it fails due to the password mismatch

DecryptData failed and ILSPwdAuthenticationFailed alarm in the Hub logs indicates the mismatch
of the password.

Log snippet from 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: The error is same in rest of the methods too whenever connection fails due to password mismatch.

Log Analysis for ILS Registration for Method 2

Spoke Registers Successfully to the Hub using TLS Authentication

Log snippet from 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

Log Snippet from Spoke:

Connection Fails as Tomcat Certificate of the Hub is not imported in Spoke

Log from Spoke indicates that the Certificate Verification for the Hub is failed.

Log snippet from Spoke:

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

Connection Fails as Tomcat Certificate of the Spoke is not imported in Hub

Logs from the hub indicates that connection is closed as neither Certificate of the Spoke in local store nor FQDN in the peer info vector.

Log Snippet from 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,
Log Analysis for ILS Registration for Method 3

Spoke Registers Successfully to the Hub using TLS with Password Authentication

Log snippet from 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
```

Log snippet from Spoke:

```
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
```

Connection Fails as Tomcat Certificate of the Spoke is Self Signed

Logs from Hub Indicates Certificate Verification failure for Self-Signed Certificate of the Spoke.

Log Snippet from 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
```

Connection Fails as Tomcat Certificate of the Hub is Self Signed


Log Snippet from Spoke:

```
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: The error seen in this case is also same when both hub and spoke have self signed.

Log Analysis for ILS Registration for Method 4

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

FQDN of the remote cluster presented in the PeerInfoVector as the connection is already established with password authentication method. When switching to TLS from password authentication method, “X509_STORE_get_by_subject failed” error is printed in the logs since tomcat certificate is not cross imported. But, the connection still accepted using TLS since “FQDN is in PeerInfoVector”.

Log snippet from 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
```

Log snippet from Spoke:

```
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
```

Connection Fails as Hub has Self Signed Certificate when switching to TLS Authentication from the established connection using Password Authentication.


Log snippet from Spoke:

```
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
```

Connection Fails as Spoke has Self Signed Certificate when switching to TLS Authentication from the established connection using Password Authentication.

Logs from Hub indicates Certificate Verification failure for Self-Signed Certificate of the Spoke.

Log snippet from 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
```