

Configurez et dépannez joindre des batteries pour l'Is

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Méthode 1. Utilisant l'authentification de mot de passe entre les batteries](#)

[Méthode 2. Utilisant l'authentification de TLS entre les batteries](#)

[Méthode 3. TLS d'utilisation avec l'authentification de mot de passe entre les batteries.](#)

[La méthode 4. commutant au TLS l'authentification après batterie est jointe avec l'authentification de mot de passe.](#)

[Vérifiez](#)

[Dépannez](#)

[Analyse de log pour l'inscription Is à la méthode 1](#)

[Le rai s'enregistre avec succès au hub utilisant l'authentification de mot de passe entre les batteries](#)

[A parlé aux essais pour s'enregistrer au hub mais il échoue en raison de la non-concordance de mot de passe](#)

[Analyse de log pour l'inscription Is à la méthode 2](#)

[Le rai s'enregistre avec succès au hub utilisant l'authentification de TLS](#)

[La connexion échoue car le certificat de Tomcat du hub n'est pas importé dans le rai](#)

[La connexion échoue car le certificat de Tomcat du rai n'est pas importé dans le hub](#)

[Analyse de log pour l'inscription Is à la méthode 3](#)

[Le rai s'enregistre avec succès au hub utilisant le TLS avec l'authentification de mot de passe](#)

[La connexion échoue car le certificat de Tomcat du rai est individu signé](#)

[La connexion échoue car le certificat de Tomcat du hub est individu signé](#)

[Analyse de log pour l'inscription Is à la méthode 4](#)

[Le rai s'enregistre avec succès au hub en commutant au TLS Authentification de la connexion établie utilisant l'authentification de mot de passe.](#)

[La connexion échoue car le hub a le certificat signé d'individu en commutant au TLS Authentification de la connexion établie utilisant l'authentification de mot de passe.](#)

[La connexion échoue comme le rai a le certificat signé d'individu en commutant au TLS Authentification de la connexion établie utilisant l'authentification de mot de passe.](#)

Introduction

Ce document décrit les méthodes possibles de configuration pour joindre des batteries pour le service de consultation d'Intercluster (Is) se connectent également l'analyse au troubleshoot

chaque les méthodes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

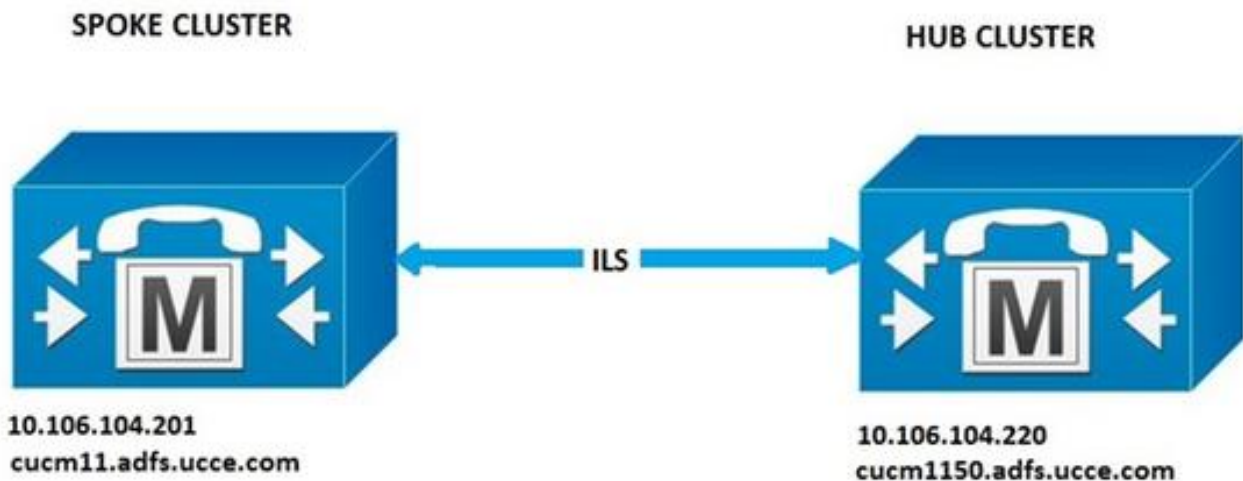
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 11.5 de Cisco Unified Communications Manager (CUCM)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Diagramme du réseau



Configurations

Méthode 1. Utilisant l'authentification de mot de passe entre les batteries

Ouvrez une session à la page de gestion CUCM, naviguez vers la **fonctionnalité avancée > la configuration ILS**.

Dans la fenêtre de configuration ILS, cochez la case de **mot de passe d'utilisation**.

Gérez la **sauvegarde de hit** de mots de passe puis. Le mot de passe doit être même à travers

toutes les batteries dans le réseau IIs.

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"

Méthode 2. Utilisant l'authentification de TLS entre les batteries

Pour utiliser cette méthode, assurez-vous que toutes les batteries que pour être une partie de réseau IIs ont importées le distant groupe des Certificats de Tomcat en sa Tomcat-confiance.

Dans la gestion CUCM, naviguez vers la **fonctionnalité avancée > la configuration IIs**. Dans la fenêtre de configuration IIs, cochez la case de **Certificats de TLS d'utilisation** sous l'authentification IIs.

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"

Méthode 3. TLS d'utilisation avec l'authentification de mot de passe entre les batteries.

L'avantage de cette méthode est qu'aucun besoin de croiser l'importation que Tomcat délivre un certificat entre les batteries pour établir la connexion de TLS si elle a signé par Certificate Authority(CA) externe. Cette méthode est fournie par CUCM 11.5 et plus tard.

Pour utiliser cette méthode, assurez-vous que toutes les batteries que pour être une partie de réseau IIs ont les Certificats de chat ont signé par un CA externe et le certificat racine de ce CA est présente en Tomcat-confiance. En outre, le mot de passe doit être même à travers toutes les batteries dans le réseau IIs.

Dans la gestion CUCM, naviguez vers la **fonctionnalité avancée > la configuration IIs** sous l'authentification IIs, cochez les **Certificats de TLS d'utilisation** et la case de **mot de passe d'utilisation**.

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"

La méthode 4. commutant au TLS l'authentification après batterie est jointe avec l'authentification de mot de passe.

C'est une autre manière d'utiliser le TLS sans croix important les Certificats de Tomcat entre les batteries s'il a signé par CA externe. C'est utile pour les versions antérieurement 11.5 CUCM où la méthode 3 n'est pas prise en charge.

Pour utiliser cette méthode, assurez-vous que toutes les batteries que pour être une partie de réseau Ils ont les Certificats de chat ont signé par un CA externe et le certificat racine de ce CA est présente en Tomcat-confiance.

Joignez la batterie d'abord utilisant l'authentification de mot de passe. Dans la gestion de Cisco Unified CM, naviguez vers la **fonctionnalité avancée > la configuration Ils**. Sous l'authentification Ils, case de **mot de passe d'utilisation de** contrôle. Gérez les mots de passe. Cliquez sur **Save**.

Le mot de passe doit être même dans le côté de client et serveur au moment de joindre la batterie.



The screenshot shows the 'ILS Authentication' configuration window. The 'Use Password' checkbox is checked, and the 'Use TLS Certificates' checkbox is unchecked. There are two password input fields, one for 'Password' and one for 'Confirm Password', 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"'

Une fois que la connexion est établie, changez la méthode d'authentification au TLS. Dans la gestion CUCM, naviguez vers la **fonctionnalité avancée > la configuration Ils**. Dans la fenêtre de configuration Ils, cochez la case de **Certificats de TLS d'utilisation** sous l'authentification Ils.



The screenshot shows the 'ILS Authentication' configuration window. The 'Use TLS Certificates' checkbox is checked, and the 'Use Password' checkbox is unchecked. There are two password input fields, one for 'Password' and one for 'Confirm Password', 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"'

Vérifiez

L'enregistrement réussi peut être vu sous des batteries Ils et des catalogues importés par DialPlan globaux dedans

Fonctionnalité avancée > configuration Ils



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.occ.com	-	Up to date	Disconnect
1	8/26/16 5:06 PM	Spoke	cucm11.adfs.occ.com	8/26/16 5:06 PM	Up to date	Disconnect

Des détails distants de batterie sont répertoriés utilisant le **passage SQL de** commande **choisi * du remotecuster**

```

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

```

Dépannez

Placez le niveau de suivi de débogage pour le service de consultation de Cisco Intercluster à détaillé.

Emplacement pour le suivi : `activelog /cm/trace/ils/sdl/`

L'analyse de log pour des scénarios de succès et échec pour des méthodes de chaque enregistrement Ils avec l'exemple AR expliquées.

Analyse de log pour l'inscription Ils à la méthode 1

Le rai s'enregistre avec succès au hub utilisant l'authentification de mot de passe entre les batteries

Extrait de log de 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

```

Extrait de log de rai :

```

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

```

A parlé aux essais pour s'enregistrer au hub mais il échoue en raison de la non-concordance de mot de passe

DecryptData a manqué et l'alarme d'ILSPwdAuthenticationFailed dans les logs de hub indique la

non-concordance du mot de passe.

Extrait de log de 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
```

Remarque: L'erreur est même dans le reste des méthodes trop toutes les fois que la connexion échoue en raison de la non-concordance de mot de passe.

Analyse de log pour l'inscription Ils à la méthode 2

Le rai s'enregistre avec succès au hub utilisant l'authentification de TLS

Extrait de log de 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
```

Extrait de log de rai :

```
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
```

La connexion échoue car le certificat de Tomcat du hub n'est pas importé dans le rai

Le log du rai indique que la vérification de certificat pour le hub est manquée.

Extrait de log de rai :

```
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
```

La connexion échoue car le certificat de Tomcat du rai n'est pas importé dans le hub

Les logs du hub indiquent que la connexion n'est fermée pendant que ni certificat du rai dans la mémoire locale ni FQDN dans le vecteur de l'information de pair.

Extrait de log de 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

Analyse de log pour l'inscription Ils à la méthode 3

Le rai s'enregistre avec succès au hub utilisant le TLS avec l'authentification de mot de passe

Extrait de log de 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

Extrait de log de rai :

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

La connexion échoue car le certificat de Tomcat du rai est individu signé

Les logs du hub indique la panne de vérification de certificat pour le certificat Auto-Signer du rai.

Extrait de log de 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

La connexion échoue car le certificat de Tomcat du hub est individu signé

Les logs du rai indique le faulure de vérification de certificat pour le certificat Auto-Signer du hub.

Extrait de log de rai :

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

Remarque: L'erreur vue dans ce cas est également même quand les deux le hub and spoke ont l'individu signé.

Analyse de log pour l'inscription Ils à la méthode 4

Le rai s'enregistre avec succès au hub en commutant au TLS Authentication de la connexion établie utilisant l'authentification de mot de passe.

Le FQDN de la batterie de distant présentée dans le PeerInfoVector comme connexion est déjà établi avec la méthode d'authentification de mot de passe. En commutant au TLS de la méthode d'authentification de mot de passe, « X509_STORE_get_by_subject a manqué » l'erreur est imprimée dans les logs puisque le certificat de chat n'est pas croisé importé. Mais, la connexion reçue toujours utilisant le TLS puisque le « FQDN est dans PeerInfoVector ».

Extrait de log de 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
```

Extrait de log de rai :

```
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
```

La connexion échoue car le hub a le certificat signé d'individu en commutant au TLS Authentication de la connexion établie utilisant l'authentification de mot de passe.

Les logs du rai indique la panne de vérification de certificat pour le certificat Auto-Signer du hub.

Extrait de log de rai :

```
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
```

La connexion échoue comme le rai a le certificat signé d'individu en commutant au TLS Authentication de la connexion établie utilisant l'authentification de mot de passe.

Les logs du hub indique la panne de vérification de certificat pour le certificat Auto-Signer du rai

Extrait de log de 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
```