

Configurer la résilience XMPP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document explique comment paramétrer la résilience du protocole Messagerie et présence extensibles (XMPP) sur le serveur de réunion Cisco (CMS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Les grappes de base de données doivent être configurées avant la résilience XMPP. Ceci est le lien pour le paramétrage des grappes de base de données

https://www.cisco.com/c/fr_ca/support/docs/conferencing/meeting-server/210530-configure-cisco-meeting-server-call-brid.html

- Le composant de pont d'appel doit être configuré sur CMS
- Cisco recommande que vous ayez au moins 3 nœuds XMPP pour être en mesure de configurer la résilience XMPP
- Quand la configuration est en mode résilience (Resilient mode), les serveurs XMPP dans un déploiement sont chargés avec la même configuration
- Comprendre les certificats autosignés et signés par une Autorité de certification (CA)
- Serveur de nom de domaine (DNS) obligatoire
- Obligatoire : une autorité de certification locale ou une autorité de certification publique pour générer des certificats

Note: L'utilisation de certificats autosignés n'est pas recommandée pour un environnement de production

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

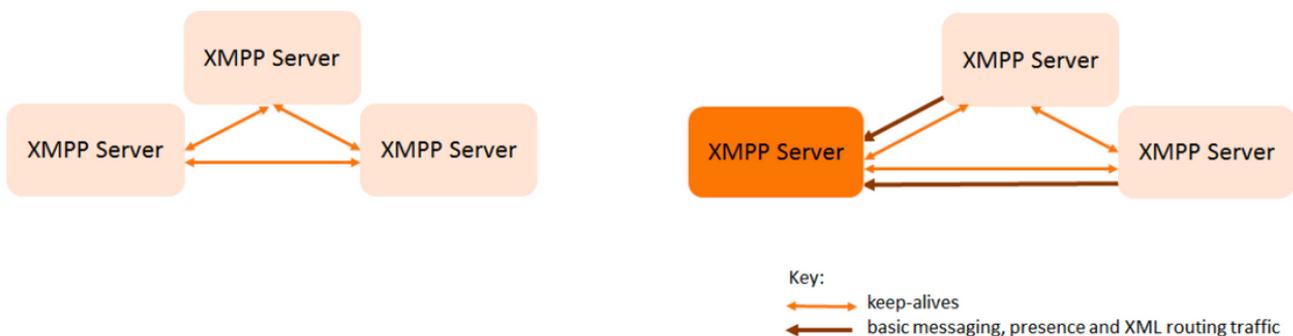
- CMS
- Logiciel d'émulation de terminal PuTTY Secure Shell (SSH) pour le processeur de gestion principal (Mainboard Management Processor ou MMP)
- Un navigateur Web comme Firefox ou Chrome

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.

Configuration

Diagramme du réseau

Cette image affiche l'échange de messages XMPP et le trafic de routage.



Configuration

Cet exemple de déploiement de résilience XMPP utilise trois serveurs XMPP et la configure pour la première fois.

Note: Si la résilience XMPP est déjà déployée, il est alors recommandé de réinitialiser tous les serveurs.

Les serveurs XMPP utilisent des messages keep-alive pour se surveiller entre eux et élire un Leader. Les messages XMPP peuvent être envoyés à n'importe quel serveur. Comme indiqué dans l'image précédente, les messages sont transférés vers le serveur XMPP Leader. Les serveurs XMPP continuent à se surveiller entre eux, et si le Leader tombe en panne, un nouveau Leader est élu et les autres serveurs XMPP commencent à transférer le trafic vers le nouveau Leader.

Étape 1. Générer des certificats pour le composant XMPP.

Générez la demande de signature de certificat (DSC), puis vous pourrez utiliser cette commande pour générer le certificat correspondant par l'intermédiaire de l'autorité de certification locale ou publique au besoin

```
pki csr <key/cert basename>
```

```
cb1> pki csr abhiall CN:tptac9.com subAltName:cb1.tptac9.com,cb2.tptac9.com,cb3
```

Étape 2. Utilisez la DSC ci-dessus et générez le certificat à l'aide de l'autorité de certification locale. Vous pouvez utiliser le guide de certificat VCS pour générer des certificats à l'aide de Microsoft Certificate Authority, annexe 5, page 32

https://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-8/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-8.pdf

Téléversez le certificat sur les trois nœuds à l'aide du serveur WINSFTP/SFTP. Pour vérifier si les certificats sont en cours de téléversement, utilisez une commande sur MMP/SSH

commande : pki list

```
cb2> pki list
User supplied certificates and keys:
[callbridge.key
callbridge.crt
webadmin.key
webadmin.crt
abhiall.key
abhiall.cer
dbclusterclient.cer
dbclusterserver.cer
dbclusterserver.key
dbclusterclient.key
cabundle-cert.cer
```

Note: Dans le laboratoire, un seul certificat est utilisé pour les trois nœuds XMPP.

Étape 3. Configurez CMS pour utiliser le composant XMPP.

```
cb1> xmpp domain tptac9.com
cb1>xmpp listen a
cb1>xmpp certs abhiall.key abhiall.cer certall.cer
```

*certall.cer= CA certificate

Astuce : Si votre autorité de certification fournit un ensemble de certificats, alors incluez

l'ensemble en tant que fichier distinct du certificat. Un ensemble de certificats est un fichier unique (avec comme extension `.pem`, `.cer` ou `.crt`) qui contient une copie du certificat de l'autorité de certification racine et de tous les certificats intermédiaires dans la chaîne. Les certificats doivent être en ordre, le certificat de l'autorité de certification racine étant en dernier dans l'ensemble de certificats. Les clients externes (par exemple les navigateurs Web et les clients XMPP) nécessitent que le certificat et l'ensemble de certificats soient présentés par le serveur XMPP respectivement, lors du paramétrage d'une connexion sécurisée.

Lorsqu'un ensemble de certificats est nécessaire. La commande ci-dessus serait

```
cb1> xmpp certs abhiall.key abhiall.cer certallbundle.cer
```

```
certallbundle.cer= CA certificate + Intermediate CA + Intermediate CA1 + Intermediate CA2 +....  
+ Intermediate CAn + Root CA
```

where n is an integer

Lorsque vous utilisez trois certificats pour trois nœuds XMPP respectifs. Veuillez vous assurer de grouper les certificats dans un ensemble

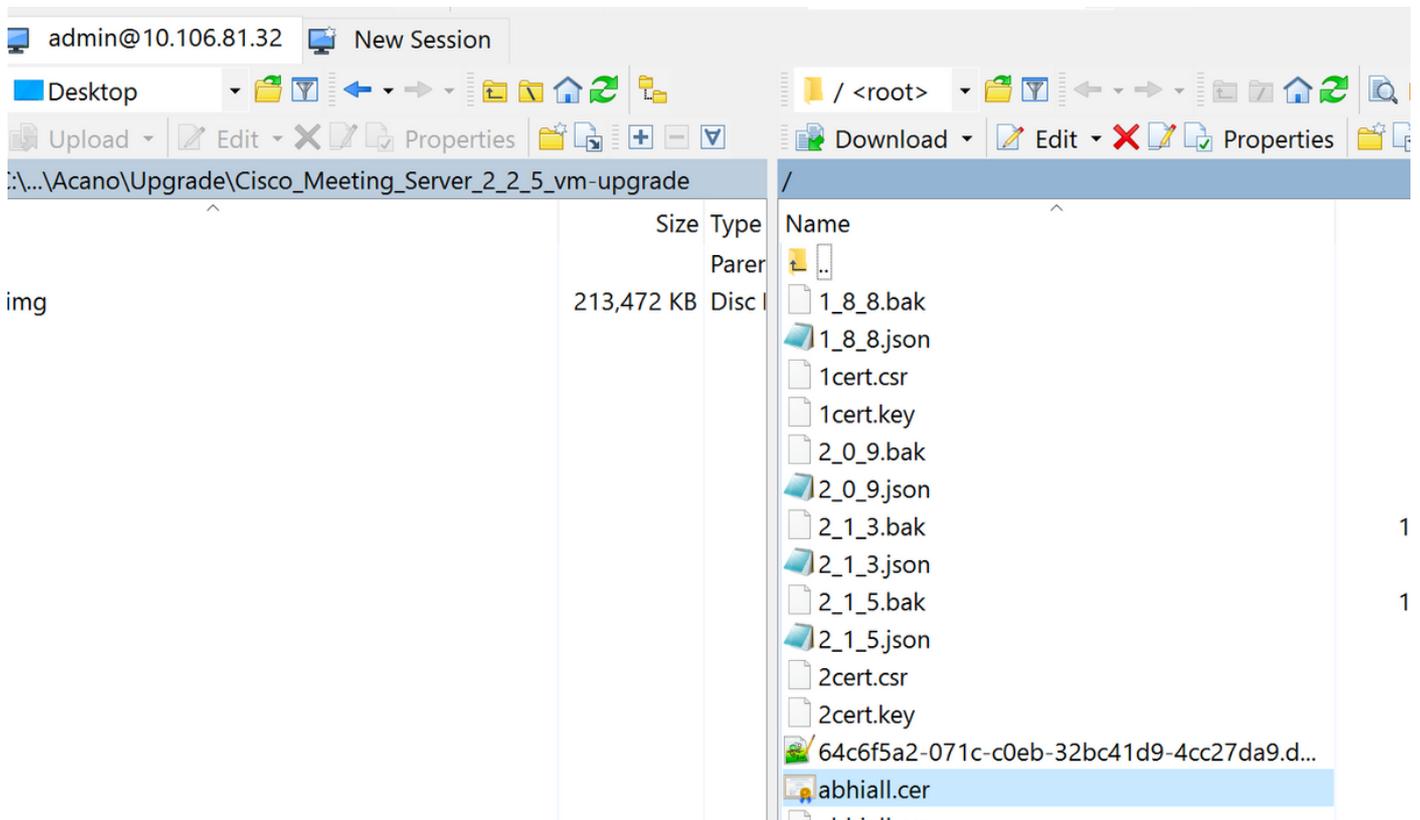
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

Un certificat unique, **abhiall.cer**, est utilisé dans le document.

Veuillez vous reporter à ce guide afin d'en savoir plus sur les certificats

https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Scalable-and-Resilient-Deployments-2-2.pdf

Étape 4. Téléchargez des certificats via SFTP vers tous les CMS, qui exécutent le composant XMPP.



```
cb1>> xmpp cluster trust xmpp-cluster-bundle.crt
```

In lab xmpp cluster trust **abhiall.cer**

```
cb1>>xmpp cluster trust abhiall.cer
```

Étape 5. Ajoutez des ponts d'appels au serveur XMPP.

```
cb1> xmpp callbridge add cb1
```

Un secret est généré, ceci configure le serveur XMPP pour permettre les connexions avec le **pont d'appel nommé cb1**.

Note: Le domaine, le nom du pont d'appel et le secret sont générés, vous aurez besoin de cette information plus tard lorsque vous configurerez l'accès du pont d'appel au serveur XMPP (afin que le pont d'appel puisse présenter les détails d'authentification au serveur XMPP)

La commande ci-dessus est utilisée pour ajouter d'autres ponts d'appel au même nœud XMPP.

```
cb1> xmpp callbridge add cb2
```

```
cb1> xmpp callbridge add cb3
```

Remarque : chaque pont d'appel doit avoir un **nom unique**. Si vous n'avez pas déjà pris en note les détails des ponts d'appel que vous avez ajoutés au serveur XMPP, utilisez la commande : **xmpp callbridge list**

```
cb1> xmpp disable
```

Cela désactive le nœud de serveur XMPP

Étape 6. Activez le cluster XMPP.

```
cb1> xmpp cluster enable
```

Initialisez la grappe XMPP sur ce nœud. Cette commande crée une **grappe xmpp à un nœud**, les autres nœuds (serveurs XMPP) sont joints à cette grappe.

```
cb1> xmpp cluster initialize
```

Réactivez ce nœud

```
cb1>xmpp enable
```

Étape 7. Ajoutez des ponts d'appel au deuxième nœud XMPP et joignez-le à un cluster.

Ajoutez chaque pont d'appel à ce nœud. Cela nécessite que le pont d'appel soit ajouté en utilisant le même nom de pont d'appel et le même secret que le premier nœud de serveur XMPP. Cela s'effectue avec cette commande

```
cb2>> xmpp callbridge add-secret cb1
```

Entrez le secret du pont d'appel

```
cb2> xmpp callbridge add-secret cb1
Enter callbridge secret
_
```

Pour vérifier le secret, veuillez exécuter la commande **xmpp call bridge list**. Elle répertorie tous les secrets générés sur le premier nœud.

```

[cb1> xmpp callbridge list
***
Callbridge : cb1
Domain     : tptac9.com
Secret     : kvgP1SRzWVabhiPVAb1
***
Callbridge : cb2
Domain     : tptac9.com
Secret     : uBiLLdIU8vVqj86CAb1
***
Callbridge : cb3
Domain     : tptac9.com
Secret     : RJTmSh4smhLYguGpAb1

```

Ensuite, vous ajoutez tous les secrets des ponts d'appel au deuxième nœud.

```

cb2>> xmpp disable
cb2>> xmpp cluster enable
cb2>> xmpp enable
cb2>> xmpp cluster join <cluster>

```

Grappe : est l'adresse IP ou le nom de domaine du premier nœud

Étape 8. Ajoutez des ponts d'appel au troisième nœud XMPP et joignez-le à un cluster.

Ajoutez chaque pont d'appel à ce nœud. Cela nécessite que le pont d'appel soit ajouté en utilisant le même nom de pont d'appel et le même secret que le premier nœud de serveur XMPP. Ceci s'effectue en utilisant la commande

```
cb3>> xmpp callbridge add-secret cb1
```

Entrez le secret du pont d'appel

```

[cb2> xmpp callbridge add-secret cb1
Enter callbridge secret

```

Maintenant, pour vérifier le secret. Vous pouvez exécuter la commande `xmpp callbridge list`. Cette commande répertorie tous les secrets générés sur le premier nœud.

```
[cb1> xmpp callbridge list
***
Callbridge : cb1
Domain     : tptac9.com
Secret     : kvgP1SRzWVabhiPVAb1
***
Callbridge : cb2
Domain     : tptac9.com
Secret     : uBiLLdIU8vVqj86CAb1
***
Callbridge : cb3
Domain     : tptac9.com
Secret     : RJTmSh4smhLYguGpAb1
```

Une fois que tous les secrets des ponts d'appel ont été ajoutés à ce nœud, procédez comme suit.

```
cb3>> xmpp disable
cb3>> xmpp cluster enable
cb3>> xmpp enable
cb3>> xmpp cluster join <cluster>
```

Grappe : est l'adresse IP ou le nom de domaine du premier nœud

Étape 9. Configurez chaque pont d'appel avec les détails d'authentification des serveurs XMPP du cluster. Cela permet aux ponts d'appel d'accéder aux serveurs XMPP.

Naviguez jusqu'à **Webadmin > Configuration > General (Webadmin > Configuration > Générale)** et entrez les éléments suivants :

1. Ajoutez un nom de pont d'appel unique, aucune partie domaine requise.
2. Entrez le domaine pour le domaine de serveur XMPP tptac9.com
3. Adresse du serveur pour le serveur XMPP. Configurez ce champ si vous souhaitez que ce pont d'appel n'utilise qu'un serveur XMPP colocalisé, ou si vous n'avez pas configuré le DNS. L'utilisation d'un serveur XMPP colocalisé réduit la latence.
4. Laissez ce champ vide pour autoriser ce pont d'appel à basculer entre les serveurs XMPP; cela nécessite que les entrées DNS soient configurées.

General configuration

XMPP server settings	
Unique Call Bridge name	<input type="text" value="cb1"/>
Domain	<input type="text" value="tptac9.com"/>
Server address	<input type="text"/>
Shared secret	<input type="text"/> [change]
Confirm shared secret	<input type="text"/>

Si vous prévoyez utiliser le serveur de nom de domaine (DNS) pour la connexion entre les ponts d'appel et les serveurs XMPP, vous devez également configurer un enregistrement DNS SRV pour que la grappe XMPP mène à l'enregistrement A DNS de chacun des serveurs XMPP dans la grappe. Le format de l'enregistrement SRV DNS est : `_xmpp-component._tcp`.

```
_xmpp-component._tcp.example.com. 86400 IN SRV 0 0 5222 xmppserver1.example.com, _xmpp-  
component._tcp.example.com. 86400 IN SRV 0 0 5223 xmppserver2.example.com, _xmpp-  
component._tcp.example.com. 86400 IN SRV 0 0 5223 xmppserver3.example.com.
```

L'exemple ci-dessus spécifie **5223** comme port (utiliser un autre port si 5223 est déjà utilisé).

le secret partagé utilisé pour le pont d'appel respectif. Par exemple, dans les captures d'écran ci-dessus

Le secret de cb1 est

Pont d'appel : cb1

Domaine : tptac9.com

Secret : kvgP1SRzWVabhiPVA**1**

D'une façon semblable pour cb2 et cb3, répétez ces étapes pour les trois ponts d'appel, **cb1**, **cb2** et **cb3**.

Après avoir effectué ces étapes, veuillez vérifier l'état de la grappe sur les trois ponts d'appel

Vérification

Exécutez la commande **cb1>> xmpp cluster status** pour obtenir un rapport sur l'état en direct de la grappe XMPP. Si la grappe échoue, alors cette commande rapporte les statistiques du serveur XMPP, qui n'est en cours d'exécution que sur ce serveur de réunion. Utilisez cette commande vous aider à diagnostiquer les problèmes de connectivité.

Cette image affiche les nœuds, l'un comme Leader 10.106.81.30 et les deux autres comme Follower.

```
[cb1> xmpp cluster status
State: FOLLOWER
List of peers
10.106.81.30:5222 (Leader)
10.106.81.31:5222
10.106.81.32:5222
Last state change: 2017-Aug-13 11:37:
Key file           : abhiall.key
Certificate file   : abhiall.cer
Trust bundle       : abhiall.cer
```

De même, vérifiez l'état des deux nœuds restants.

Sur le deuxième nœud

```
[cb2> xmpp cluster status
State: FOLLOWER
List of peers
10.106.81.30:5222 (Leader)
10.106.81.32:5222
10.106.81.31:5222
Last state change: 2017-Aug-13 07:27:58
Key file           : abhiall.key
Certificate file   : abhiall.cer
Trust bundle       : abhiall.cer
cb2> █
```

Sur le troisième nœud

```
[cb3> xmpp cluster status
State: LEADER
List of peers
10.106.81.32:5222
10.106.81.31:5222
10.106.81.30:5222 (Leader)
Last state change: 2017-Aug-13 07:28:05
Key file           : abhiall.key
Certificate file   : abhiall.cer
Trust bundle       : abhiall.cer
```

Dépannage

La résilience XMPP a été configurée avec succès. Des problèmes pourraient survenir lors de l'utilisation de la résilience XMPP.

Scénario 1. Vérifiées pour la configuration DNS, les erreurs dans les captures d'écran pointent vers les problèmes DNS.

Date	Time	Logging level	Message
2017-08-13	05:15:25.479	Info	335 log messages cleared by "admin"
2017-08-13	05:16:17.804	Info	No DNS A or AAAA records for _xmpp-component_tcp.tptac9.com
2017-08-13	05:16:17.804	Info	XMPP connection dropped while session was live for reason 2
2017-08-13	05:16:17.804	Info	XMPP component connection disconnected due to failure reason: "dns error"
2017-08-13	05:17:21.806	Info	No DNS A or AAAA records for _xmpp-component_tcp.tptac9.com
2017-08-13	05:17:21.806	Info	XMPP connection dropped while session was live for reason 2
2017-08-13	05:17:21.806	Info	XMPP component connection disconnected due to failure reason: "dns error"
2017-08-13	05:18:25.808	Info	No DNS A or AAAA records for _xmpp-component_tcp.tptac9.com
2017-08-13	05:18:25.808	Info	XMPP connection dropped while session was live for reason 2
2017-08-13	05:18:25.808	Info	XMPP component connection disconnected due to failure reason: "dns error"



Date	Time	Fault condition
2017-08-13	04:45:16.107	XMPP connection to ** failed

Fault conditions

Recent errors and warnins

Si ces erreurs sont détectées, vérifiez la configuration des enregistrements SRV.

En résilience XMPP, le serveur XMPP auquel un pont d'appel se connecte est géré par DNS. Ce choix est basé sur la priorité DNS et le poids donnés. Un pont d'appel ne se connecte qu'à un seul

serveur XMPP à la fois. Il n'y a aucune exigence pour que tous les ponts d'appel se connectent au même serveur XMPP, car tout le trafic est transféré au principal. Si un problème de réseau fait en sorte qu'un pont d'appel perde sa connexion au serveur XMPP, le pont d'appel tente de se reconnecter à un autre serveur XMPP. Le pont d'appel doit être configuré sur n'importe quel serveur XMPP auquel il peut se connecter.

Afin d'activer les connexions de clients, l'utilisation du client WebRTC, un enregistrement **_xmpp-client._tcp** est requis. Sur un déploiement standard, il mène au port **5222**. À l'intérieur du réseau local, si le serveur central est directement routable, il peut mener au service XMPP, qui est en exécution sur le serveur central.

Exemple : **_xmpp-client._tcp.tptac9.com** peut avoir ces enregistrements SRV :

_xmpp-client._tcp. tptac9.com 86400 IN SRV 10 50 5222 cb1. tptac9.com

conseils sur le paramétrage d'enregistrements DNS pour les nœuds de serveur XMPP. Pour la résilience XMPP où vous nécessitez le DNS pour la connexion entre les ponts d'appel et les serveurs XMPP, vous devez également configurer un enregistrement DNS SRV pour que la grappe XMPP mène à l'enregistrement A DNS de chacun des serveurs XMPP dans la grappe. Le format de l'enregistrement DNS SRV est : **_xmpp-component._tcp.tptac9.com**

Selon la configuration abordée pour trois serveurs XMPP, l'enregistrement qui mène aux trois serveurs est démontré

_xmpp-component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb1.tptac9.com

_xmpp-component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb2.tptac9.com

_xmpp-component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb3.tptac9.com

L'exemple spécifie le port 5223, mais n'importe quel autre port peut également être utilisé si 5223 est déjà utilisé. Cependant, vous devez vous assurer que le port utilisé soit ouvert.

Scénario 2. La page d'état CMS affiche un **échec d'authentification**.

Status	Configuration	Logs
System status		
Uptime	24 minutes, 26 seconds	
Build version	2.2.5	
XMPP connection	failed to connect to localhost due to authentication failure (1 minute, 2 seconds ago)	
Authentication service	no authentication components found	
Lync Edge registrations	not configured	
CMA calls	0	
SIP calls	0	
Lync calls	0	
Forwarded calls	0	
Completed calls	0	
Activated conferences	0	
Active Lync subscribers	0	
Total outgoing media bandwidth	0	
Total incoming media bandwidth	0	

Fault conditions

L'échec d'authentification s'affiche dans la plupart des cas parce que le secret partagé n'a pas été entré ou a été entré de façon incorrecte. Veuillez vous assurer que le secret partagé est entré. Si vous l'avez oublié ou que vous ne l'avez pas à portée de main; Veuillez accéder au serveur par SSH et exécuter cette commande : **xmpp callbridge list**

```
[cb1> xmpp callbridge list
```

```
***
```

```
Callbridge : cb1
```

```
Domain : tptac9.com
```

```
Secret : RJTmSh4smhLYguGpAb1
```

```
***
```

```
Callbridge : cb2
```

```
Domain : tptac9.com
```

```
Secret : uBiLLdIU8vVqj86CAb1
```

```
***
```

```
Callbridge : cb3
```

```
Domain : tptac9.com
```

```
Secret : RJTmSh4smhLYguGpAb1
```

```
[cb1> xmpp callbridge list
```

```
***
```

```
Callbridge : cb1
```

```
Domain : tptac9.com
```

```
Secret : kvgP1SRzWVabhiPVAb1
```

```
***
```

```
Callbridge : cb2
```

```
Domain : tptac9.com
```

```
Secret : uBiLLdIU8vVqj86CAb1
```

```
***
```

```
Callbridge : cb3
```

```
Domain : tptac9.com
```

```
Secret : RJTmSh4smhLYguGpAb1
```

```
[cb3> xmpp callbridge list
```

```
***
```

```
Callbridge : cb3  
Domain     : tptac9.com  
Secret     : RJTmSh4smhLYguGpAb1
```

```
***
```

```
Callbridge : cb2  
Domain     : tptac9.com  
Secret     : uBiLLdIU8vVqj86CAb1
```

```
***
```

```
Callbridge : cb1  
Domain     : tptac9.com  
Secret     : kvgP1SRzWVabhiPVAb1
```

Le document décrit le paramétrage de la résilience XMPP. De ce fait, exécutez la commande sur les trois serveurs pour vous assurer que les secrets générés sont identiques sur tous les serveurs. Comme le montre l'image, on peut observer que pour le serveur **cb1**, le secret partagé est le même que celui qui s'affiche pour **cb3**. Après avoir vérifié les autres serveurs, on peut conclure que le secret entré pour **cb1** est incorrect.

Scénario 3. Dans l'état de la grappe XMPP, on retrouve des **entrées dupliquées des nœuds XMPP**.

Cette sortie affiche l'entrée dupliquée du nœud **10.61.7.91:5222**

```
cb1> xmpp cluster status
```

```
State: LEADER
```

```
List of peers
```

```
10.61.7.91:5222
```

```
10.61.7.91:5222
```

```
10.59.103.71:5222
```

```
10.59.103.70:5222 (Leader)
```

Attention : il est recommandé de supprimer les nœuds xmpp du cluster avant de les réinitialiser. Si la réinitialisation XMPP est exécutée sur un nœud pendant qu'il est toujours dans la grappe et que le nœud est joint à nouveau à la grappe XMPP existante, cela crée une entrée dupliquée de ce nœud lorsque l'état est vérifié par l'entremise de l'état de la grappe XMPP.

Cela peut entraîner des problèmes dans une configuration en résilience. Une défaillance a été soulevée

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvi67717>

Vérifiez la page 94 du guide ci-dessous

https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-3/Cisco-Meeting-Server-2-3-Scalable-and-Resilient-Deployments.pdf