

XMPP の復元力の設定

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](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Meeting Server (CMS) 上で Extensible Messaging and Presence Protocol (XMPP) の復元力を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- XMPP復元力の前にデータベースクラスタリングを設定する必要があります。これは、データベースクラスタリングを設定するためのリンクです

<https://www.cisco.com/c/en/us/support/docs/conferencing/meeting-server/210530-Configure-Cisco-Meeting-Server-Call-Brid.html>

- CMS で Callbridge コンポーネントを設定する必要があること
- XMPP の復元力を設定するには、少なくとも 3 の XMPP ノードを使用すること
- 設定が復元力モードの場合、展開内の XMPP サーバが同じ設定でロードされること
- 自己署名、認証局 (CA) 署名付き証明書に関する理解
- 必要なドメイン ネーム サーバ (DNS)
- 証明書の生成に必要なローカル認証局またはパブリック認証局

注：実稼働環境では自己署名付き証明書は推奨されません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

- CMS

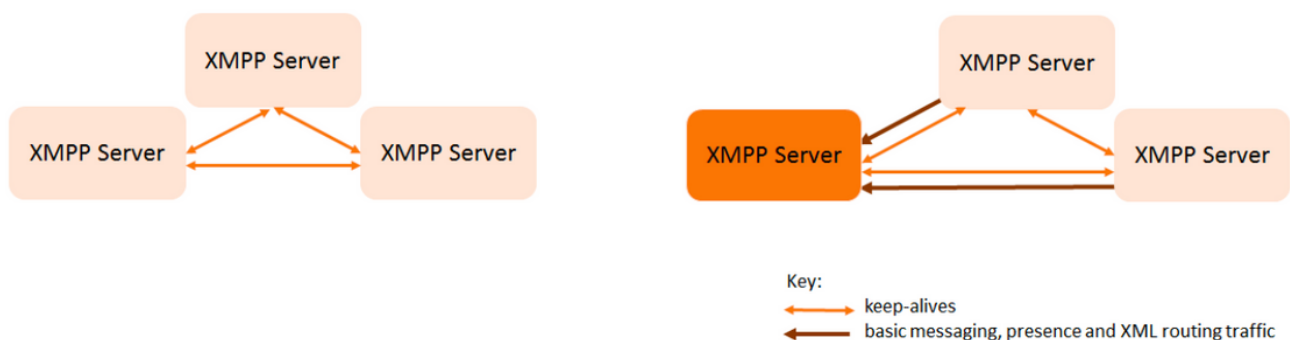
- メインボード管理プロセッサ (MMP) 用の PuTTY セキュア シェル (SSH) 端末エミュレーション ソフトウェア
- Firefox、Chrome などの Web ブラウザ

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実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

次の図に、XMPP メッセージおよびルーティング トラフィックの交換を示します。



コンフィギュレーション

この XMPP の復元力の導入例では、3 つの XMPP サーバを使用し、最初に設定します。

注： XMPP の復元力がすでに展開されている場合は、すべてのサーバをリセットすることをお勧めします。

XMPP サーバはキープアライブ メッセージを使用して互いを監視して、リーダーを選出します。XMPP メッセージは、任意のサーバに送信できます。上記の図に示すように、メッセージはリーダー XMPPサーバに転送されます。XMPP サーバは継続的に互いを監視します。リーダーに障害が発生した場合は、新しいリーダーが選出され、他の XMPP サーバは新しいリーダーにトラフィックを転送します。

ステップ 1： XMPP コンポーネント用の証明書を生成します。

CSR を生成し、次のコマンドを使用して、必要に応じてローカル認証局またはパブリック認証局を介して対応する証明書を生成します。

`pki csr <key/cert basename>`

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

ステップ2：上記のCSRを使用し、ローカル認証局を使用して証明書を生成します。VCS 証明書ガイド (付録 5、32 ページ) を使用して、Microsoft 認証局を使用して証明書を生成することがで

きます。

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

WINSOCP/SFTP サーバを使用して、3つのノードすべてに証明書をアップロードします。証明書がアップロードされているかどうかを確認するには、MMP/SSH で次のコマンドを使用します。

コマンドにより、WLC CLI で明確に示されます。pki list

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

注：ラボでは、3つのすべての XMPP ノード用に1つの証明書が使用されます。

ステップ3：XMPP コンポーネントを使用するように CMS を設定します。

```
cb1> xmpp domain tptac9.com
cb1>xmpp listen a
cb1>xmpp certs abhiatl.key abhiatl.cer certatl.cer
```

*certatl.cer= CA certificate

ヒント：CAが証明書バンドルを提供する場合は、バンドルを証明書に別のファイルとして含めます。証明書バンドルは、ルートCA証明書とチェーン内のすべての中間証明書のコピーを保持する単一のファイル(拡張子.pem、.cer、.crt)です。証明書は、証明書バンドル内で順番に配置されている必要があります(ルートCA証明書が最後)。外部クライアント(たとえば Web ブラウザや XMPP クライアント)に対しては、セキュア接続を設定するときに、XMPP サーバは証明書と証明書バンドルをそれぞれ提示する必要があります。

証明書のバンドルが必要な場合、上記のコマンドは次のようになります。

```
cb1> xmpc 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

3つの証明書を3つのXMPPノード用に使用する場合は、証明書をバンドルする必要があります。

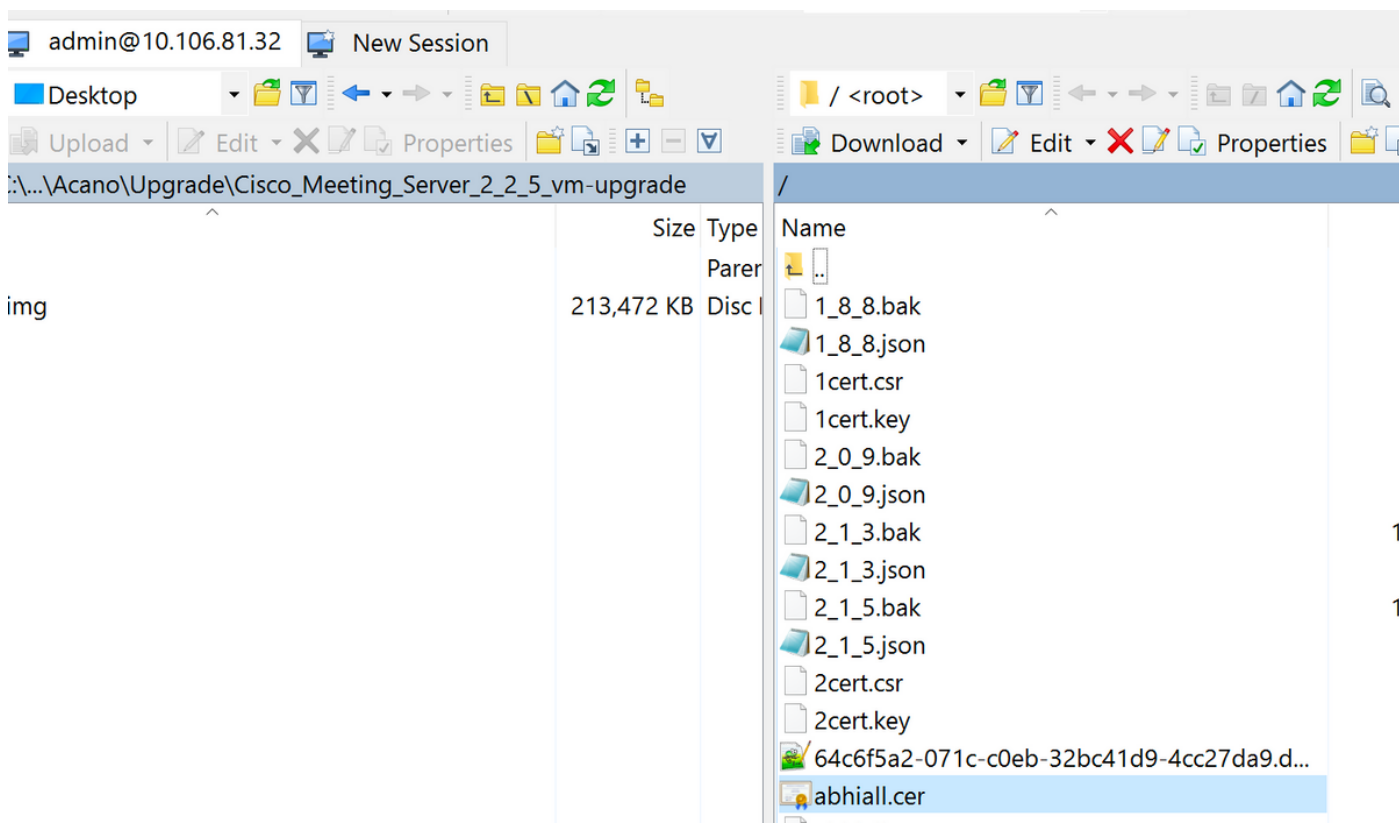
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

このドキュメントでは、単一の証明書 **abhiall.cer** を使用します。

証明書の詳細については、次のガイドを参照してください。

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

ステップ 4：XMPPコンポーネントを実行するすべてのCMSにSFTPで証明書をアップロードします。



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

ラボでは、xmpp クラスタは **abhiall.cer** を信頼します。

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

ステップ 5 : XMPP サーバに Call Bridge を追加します。

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

秘密が生成されます。これにより、XMPP サーバが **cb1** という名前の Call Bridge に接続できるように設定されます。

注 : ドメイン、Call Bridge 名、および秘密が生成されます。この情報は、後で Call Bridge から XMPP サーバへのアクセスを (Call Bridge が XMPP サーバに認証の詳細を提示できるようにするために) 設定するときに必要なになります

上記のコマンドを使用して、他の Call Bridge を同じ xmpp ノードに追加します。

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

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

注 : 各コールブリッジには一意の名前を付ける必要があります。XMPP サーバに追加された Call Bridges の詳細をメモしていない場合は、次のコマンドを使用します。xmpp callbridge list

```
cb1> xmpp disable
```

これにより、XMPPサーバ ノードが無効化されます。

ステップ 6 : XMPP クラスタを有効化します。

```
cb1> xmpp cluster enable
```

このノード上の XMPP クラスタを初期化します。このコマンドにより、1 つのノード xmpp クラスタが作成され、他のノード (xmpp サーバ) がこのクラスタに参加します。

```
cb1> xmpp cluster initialize
```

このノードを再び有効化します。

```
cb1>xmpp enable
```

ステップ 7 : 2 番目の XMPP ノードに Call Bridges を追加し、クラスタに参加させます。

このノードに各 Call Bridge を追加します。そのためには、最初の XMPP サーバ ノードから同じ Call Bridge 名と秘密を使用して、Call Bridge を追加する必要があります。これを行うには、次のコマンドを使用します。

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

Call Bridge の秘密を入力します。

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

秘密を確認するには、`xmpp call bridge list` コマンドを実行してください。これにより、最初のノードで生成されたすべての秘密が一覧表示されます。

```
[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
```

すべての Call Bridge 秘密を 2 番目のノードに追加したら、次のコマンドを実行します。

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

cluster : 最初のノードの IP アドレスまたはドメイン名です。

ステップ 8 : 3 番目の XMPP ノードに Call Bridges を追加し、クラスタに参加させます。

このノードに各 Call Bridge を追加します。そのためには、最初の XMPP サーバ ノードから同じ Call Bridge 名と秘密を使用して、Call Bridge を追加する必要があります。これを行うには、次のコマンドを使用します。

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

Call Bridge の秘密を入力します。

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

ここで、秘密を確認します。xmpp callbridge list コマンドを実行できます。このコマンドにより、最初のノードで生成されたすべての秘密が一覧表示されます。

```
[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
```

すべての Call Bridge 秘密がこのノードに追加されたら、次の手順を実行します。

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

cluster : 最初のノードの IP アドレスまたはドメイン名です。

ステップ 9 : クラスタ内の XMPP サーバの認証の詳細を使用して各 Call Bridge を設定します。これにより、Call Bridge が XMPP サーバにアクセスできるようになります。

[Webadmin] > [Configuration (設定)] > [General (全般)] に移動して、次を入力します。

1. 一意の Call Bridge 名を追加します。ドメイン部分は必要ありません。
2. XMPP サーバドメイン tptac9.com を入力します。
3. XMPP サーバのサーバアドレス。この Call Bridge が同じ場所に配置されている XMPP サーバのみを使用するようにするか、DNS が設定されていない場合は、このフィールドを設定します。同じ場所に配置されている XMPP サーバを使用すると、遅延が軽減されます。
4. この Call Bridge が XMPP サーバ間でフェールオーバーできるようにするには、このフィー

ルドを空のままにします。その場合は、DNS エントリを設定する必要があります。

Status ▾ Configuration ▾ Logs ▾

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"/>

ドメイン ネーム サーバ (DNS) を使用して、Call Bridge と XMPP サーバ間で接続する場合は、クラスタ内の各 XMPP サーバの DNS A レコードに解決するために、xmpp クラスタ用の DNS SRV レコードを設定する必要があります。DNS SRV レコードの形式は次のとおりです。
`_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.
```

上記の例では、**ポート 5223 が指定されています (5223 がすでに使用されている場合は、別のポートを使用します)**。

それぞれの Call Bridge に対して使用される共有秘密です。たとえば、上記のスクリーンショットの例では、

Cb1 秘密は次のとおりです。

Callbridge : cb1

ドメイン : tptac9.com

秘密 : kvgP1SRzWVabhiPVAb1

同様に cb2 と cb3 についても、3 のすべての Call Bridge **cb1**、**cb2**、**cb3** に対して上記の手順を繰り返します。

上記の手順を実行したら、3 つのすべての Call Bridge でクラスタのステータスを確認してください。

確認

`cb1>> xmpp cluster status` コマンドを実行して、xmpp クラスタの現在の状態を取得します。クラスタに障害が発生している場合、このコマンドは、この Meeting Server のみで実行されている xmpp サーバの統計情報を返します。このコマンドを使用して、接続の問題を診断します。

次の図に、ノード (1 つはリーダーの 10.106.81.30、残りの 2 つはフォロワー) を示します。


```
[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
```

同様に、残りの2つのノードでステータスを確認します。

第2ノードの場合

```
[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> █
```

第3ノードの場合

```
[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
```

トラブルシューティング

XMPP の復元力が正常に設定されました。xmpp の復元力を使用するときに、問題が発生する場合があります。

シナリオ 1：DNS 設定を確認したところ、スクリーンショットのエラーが DNS の問題を示している。

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

System status

Uptime	1 day, 17 hours, 41 minutes
Build version	2.2.5
XMPP connection	failed to connect to due to DNS error (28 seconds ago)
Authentication service	registered for 1 day, 17 hours, 41 minutes
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

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

Recent errors and warnins

これらのエラーが表示されている場合は、SRV レコードの設定を確認します。

XMPP の復元力では、Call Bridge が接続する XMPP サーバは DNS 経由で制御されます。この選択は、DNS の優先順位と指定されている重みに基づいています。Call Bridge は、一度に 1 つの

XMPP サーバにのみ接続します。すべてのトラフィックはマスターに転送されるため、すべての Call Bridge が同じ XMPP サーバに接続する必要はありません。ネットワークの問題により、Call Bridge が XMPP サーバへの接続を失った場合、Call Bridge は別の XMPP サーバに再接続しようとします。接続可能なすべての XMPP サーバに接続されるように Call Bridge を設定する必要があります。

クライアント接続を有効化するには、WebRTC クライアント、`_xmpp-client._tcp` レコードの使用が必要です。一般的な展開では、これはポート 5222 に解決されます。LAN 内では、コア サーバが直接ルーティング可能な場合、コア サーバで実行される XMPP サービスに解決できます。

以下に、いくつかの例を示します。`_xmpp-client._tcp.tptac9.com` は、これらの SRV レコードを持つことができます。

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

XMPP サーバ ノード用の DNS レコードの設定に関するアドバイス。XMPP の復元力のために、Call Bridge と XMPP サーバ間で接続するための DNS が必要です。また、クラスタ内の各 XMPP サーバの DNS A レコードを解決するには `xmpp` クラスタ用の DNS SRV レコードを設定する必要があります。DNS SRV レコードの形式は次のとおりです。`_xmpp-component._tcp.tptac9.com`

3 つの `xmpp` サーバの設定に従って、3 つのすべてのサーバに解決するレコードを示します。

```
_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
```

この例では、ポート 5223 が指定されています。5223 がすでに使用されている場合は、それ以外のポートも使用できます。ただし、使用されるポートを開く必要があります。

シナリオ2. CMSステータスページに認証失敗が表示される場合。

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

認証の失敗は、共有秘密が入力されていないか、誤って入力されている場合に表示されます。共有秘密が入力されていることを確認します。忘れた場合、および手元にメモがない場合は、サーバに SSH 接続して、次のコマンドを実行します。`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
```

このドキュメントでは、xmpp の復元力の設定について説明しています。そのため、3つのサーバのすべてでこのコマンドを実行して、生成された秘密がすべてのサーバで同じであることを確認します。図に示すように、サーバcb1で確認でき、使用されている共有秘密はcb3に反映されているものと同じです。他のサーバを確認した後、入力されたcb1の秘密が正しくないと判断されず。

シナリオ3. xmppクラスタステータスでXMPPノードのエントリが重複しています。

次の出力は、ノード 10.61.7.91:5222 のエントリの重複を示しています。

```
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)
```

注意：リセットする前に、クラスタからxmppノードを削除することをお勧めします。ノードがクラスタに存在するときはそのノードでXMPPリセットを実行し、既存のXMPPクラスタにそのノードを再参加させた場合、xmppクラスタステータスでステータスを確認すると、そのノードの重複エントリが作成されます。

これにより、復元力の設定に問題が発生する可能性があります。障害が報告されています。

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

次のガイドの 94 ページを確認してください。

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