XMPP-Ausfallsicherheit konfigurieren

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie XMPP-Ausfallsicherheit (Extensible Messaging and Presence Protocol) auf Cisco Meeting Server (CMS) einrichten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Das Datenbank-Clustering muss vor der XMPP-Ausfallsicherheit eingerichtet werden. Dies ist der Link zum Einrichten von Datenbank-Clustering

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

- Die Callbridge-Komponente muss auf dem CMS konfiguriert werden.
- Cisco empfiehlt, dass Sie über mindestens 3 XMPP-Knoten verfügen, um XMPP-Ausfallsicherheit einrichten zu können.
- Wenn sich das Setup im ausfallsicheren Modus befindet, werden die XMPP-Server in einer Bereitstellung mit derselben Konfiguration geladen
- Verständnis der selbstsignierten Zertifikate, Zertifizierungsstelle (Certificate Authority, CA)-signiert
- Domänennamenserver (DNS) erforderlich
- Von einer lokalen Zertifizierungsstelle oder einer öffentlichen Zertifizierungsstelle angefordert, Zertifikate zu generieren

> **Hinweis**: Die Verwendung von selbstsignierten Zertifikaten wird in der Produktionsumgebung nicht empfohlen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

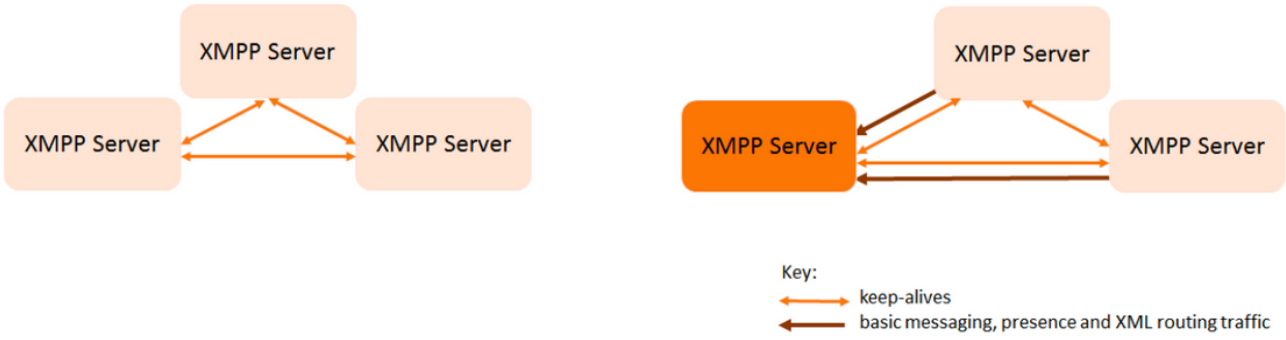
- CMS
- PuTTY Secure Shell (SSH) Terminal-Emulationssoftware für Mainboard Management Processor (MMP)
- Einen Webbrowser wie Firefox, Chrome

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm

Dieses Bild zeigt den Austausch von XMPP-Nachrichten und den Routing-Verkehr.



Konfiguration

In diesem Beispiel wird bei der Bereitstellung der XMPP-Ausfallsicherheit drei XMPP-Server verwendet, die zum ersten Mal konfiguriert werden.

> **Hinweis**: Wenn zuvor eine XMPP-Ausfallsicherheit bereitgestellt wurde, wird empfohlen, alle Server zurückzusetzen.

XMPP-Server verwenden Keepalive-Nachrichten, um sich gegenseitig zu überwachen und einen Leader auszuwählen. XMPP-Nachrichten können an jeden Server gesendet werden. Wie im vorherigen Bild gezeigt, werden Nachrichten an den Leader XMPP-Server weitergeleitet. Die XMPP-Server überwachen einander weiter. Wenn der Leader ausfällt, wird ein neuer Leader ausgewählt, und die anderen XMPP-Server leiten Datenverkehr an den neuen Leader weiter.

Schritt 1: Generieren von Zertifikaten für XMPP-Komponenten.

Erstellen Sie CSR, und geben Sie dann den Befehl ein, um bei Bedarf ein entsprechendes Zertifikat über die Local Certificate Authority/Public Certificate Authority zu generieren.

pki csr <key/cert basename>

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

Schritt 2: Verwenden Sie den obigen CSR, und generieren Sie Zertifikate mithilfe der lokalen Zertifizierungsstelle. Sie können den VCS-Zertifikatsleitfaden verwenden, um Zertifikate mithilfe der Microsoft Certificate Authority zu generieren, Anhang 5, Seite 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

Laden Sie das Zertifikat auf alle 3 Knoten mithilfe des WINSCP/SFTP-Servers hoch. Um zu überprüfen, ob Zertifikate hochgeladen werden, verwenden Sie den Befehl MMP/SSH

Befehl: Pki-Liste

```
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
```

Hinweis: Im Labor wird ein Zertifikat für alle 3 XMPP-Knoten verwendet.

Schritt 3: Konfigurieren von CMS zur Verwendung der XMPP-Komponente

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

*certall.cer= CA certificate
```

Tipp: Wenn Ihre Zertifizierungsstelle ein Zertifikatpaket bereitstellt, fügen Sie das Paket als

separate Datei zum Zertifikat hinzu. Ein Zertifikatspaket ist eine einzelne Datei (mit einer Erweiterung von **.pem**, **.cer** oder**.crt**) mit einer Kopie des Zertifikats der Root-Zertifizierungsstelle und aller Zwischenzertifikate in der Kette. Die Zertifikate müssen in Übereinstimmung mit dem Zertifikat der Stammzertifizierungsstelle als letztes im Zertifikatpaket vorliegen. Externe Clients (z. B. Webbrowser und XMPP-Clients) erfordern, dass das Zertifikats- und Zertifikatspaket beim Einrichten einer sicheren Verbindung vom XMPP-Server jeweils präsentiert wird.

Wenn ein Zertifikatspaket erforderlich ist. Der obige Befehl lautet

```
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
```

Bei Verwendung von 3 Zertifikaten für 3 entsprechende XMPP-Knoten. Stellen Sie sicher, dass die Zertifikate gebündelt werden.

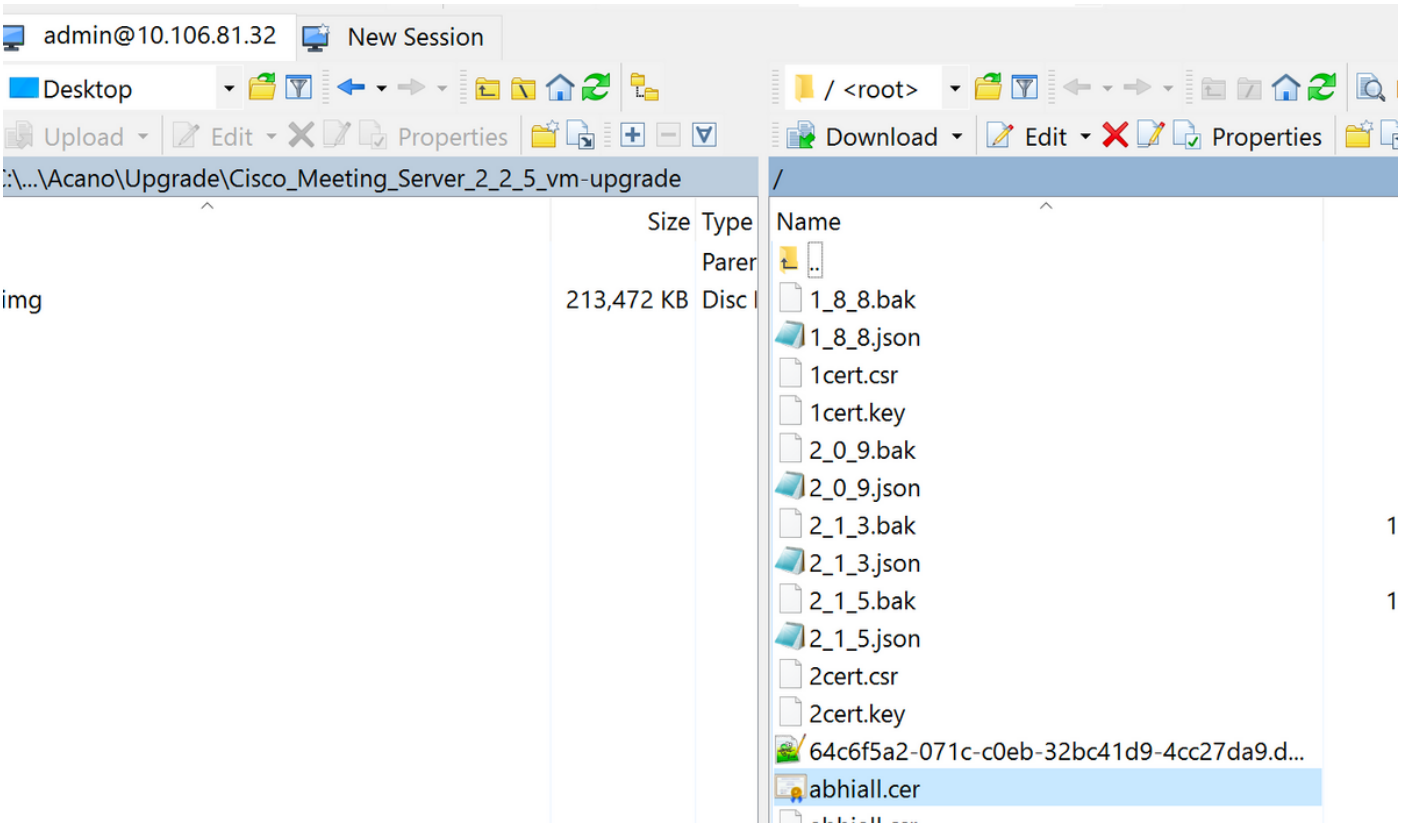
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

Im Dokument wird ein einziges Zertifikat **abhiall.cer** verwendet.

Weitere Einzelheiten zu Zertifikaten finden Sie in diesem Leitfaden.

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

Schritt 4: Hochladen von Zertifikaten über SFTP auf das gesamte CMS, das die XMPP-Komponente ausführt.



cb1>> xmpp cluster trust xmpp-cluster-bündeln.crt

Im Labor xmpp cluster trust **abhiall.cer**

cb1>>xmpp cluster trust abhiall.cer

Schritt 5: Hinzufügen von Anrufbrücken zum XMPP-Server.

cb1> xmpp callbridge add cb1

Es wird ein geheimer Schlüssel generiert, der den XMPP-Server so konfiguriert, dass Verbindungen mit der **Call Bridge** mit dem Namen **cb1** zugelassen werden.

> **Hinweis**: Die Domäne, der Name der Anrufbrücke und der geheime Schlüssel werden generiert. Sie benötigen diese Informationen später, wenn Sie den Zugriff der Anrufbrücke auf den XMPP-Server konfigurieren (sodass die Anrufbrücke dem XMPP-Server die Authentifizierungsdetails vorlegt).

Der obige Befehl wird verwendet, um demselben xmpp-Knoten weitere Anrufbrücken hinzuzufügen.

cb1> xmpp callbridge add cb2

cb1> xmpp callbridge add cb3

> **Hinweis**: Jede Anrufbrücke muss einen **eindeutigen Namen** haben. Wenn Sie noch nicht die Details für die Gesprächsbrücken angegeben haben, die Sie dem XMPP-Server hinzugefügt haben, verwenden Sie den **Befehl: xmpp callbridge-Liste**

cb1> xmpp deaktivieren

Dadurch wird der XMPP-Serverknoten deaktiviert.

Schritt 6: Aktivieren Sie XMPP-Cluster.

cb1> xmpp-Cluster aktivieren

Initialisieren Sie den XMPP-Cluster auf diesem Knoten. Mit diesem Befehl wird ein **XMPP-Cluster mit einem Knoten** erstellt, die anderen Knoten (xmpp-Server) sind diesem Cluster verbunden.

cb1> xmpp-Cluster initialisieren

Aktivieren Sie diesen Knoten erneut.

cb1>xmpp enable

Schritt 7: Fügen Sie dem zweiten XMPP-Knoten Anrufbrücken hinzu, und schließen Sie ihn einem Cluster an.

Fügen Sie diesem Knoten jede Anrufbrücke hinzu. Dazu muss die Anrufbrücke mit demselben Namen und geheim vom ersten XMPP-Serverknoten hinzugefügt werden. Dies wird mithilfe dieses Befehls erreicht

cb2>> xmpp callbridge add-secret cb1

Rufbrücke geheim eingeben

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

Um den geheimen Schlüssel zu überprüfen, führen Sie den Befehl **xmpp call bridge list aus**. Es listet alle auf dem ersten Knoten generierten geheimen Daten auf.

```
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
```

Nachdem Sie alle Anrufbrücken geheim zum zweiten Knoten hinzugefügt haben.

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

Cluster: ist die IP-Adresse oder der Domänenname des ersten Knotens.

Schritt 8: Fügen Sie dem dritten XMPP-Knoten Anruf-Bridges hinzu, und schließen Sie ihn einem Cluster an.

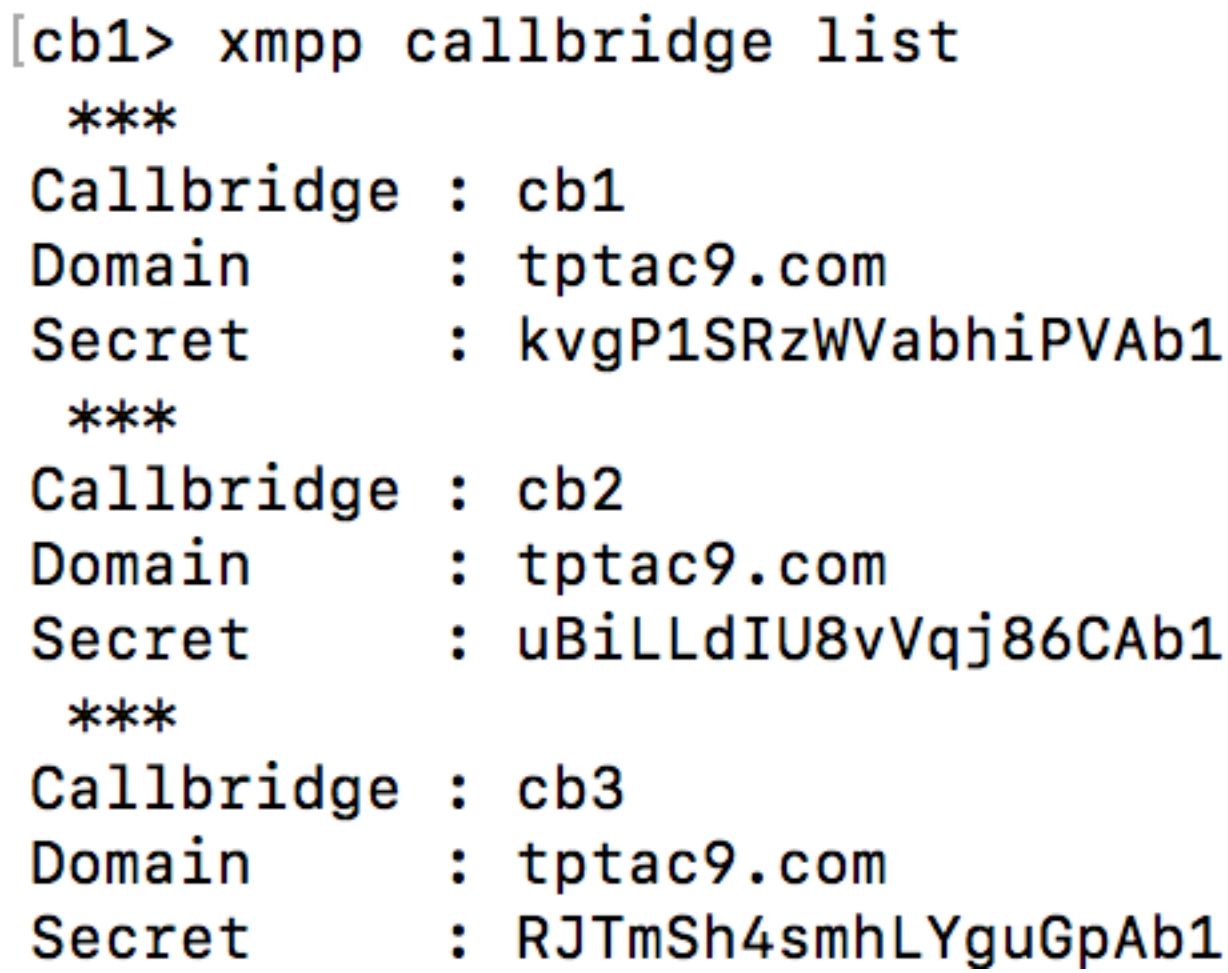
Fügen Sie diesem Knoten jede Anrufbrücke hinzu. Dazu muss die Anrufbrücke mit demselben Namen und geheim vom ersten XMPP-Serverknoten hinzugefügt werden. Dies wird mithilfe des Befehls

cb3>> xmpp callbridge add-secret cb1

Rufbrücke geheim eingeben

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

Jetzt um das Geheimnis zu überprüfen. Sie können den Befehl **xmpp callbridge list** ausführen. Der Befehl listet alle auf dem ersten Knoten generierten geheimen Daten auf.



Führen Sie die folgenden Schritte aus, nachdem diesem Knoten alle Call Bridge-Geheimnisse hinzugefügt wurden.

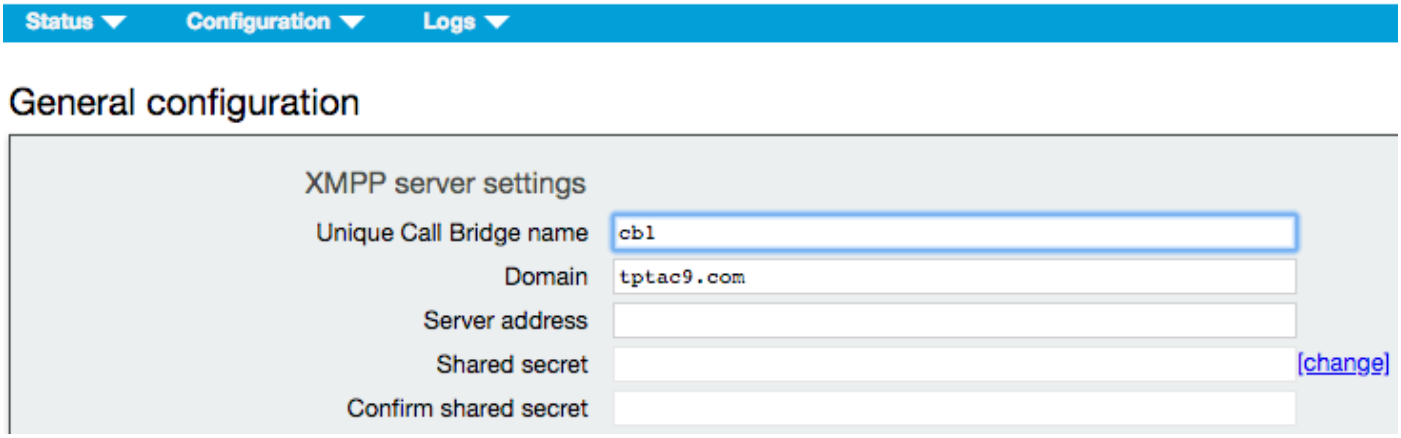
```
cb3>> xmpp disable
cb3>> xmpp cluster enable
cb3>> xmpp enable
cb3>> xmpp cluster join <cluster>
```

Cluster: ist die IP-Adresse oder der Domänenname des ersten Knotens.

Schritt 9: Konfigurieren Sie jede Anrufbrücke mit den Authentifizierungsdetails der XMPP-Server im Cluster. Dadurch können die Call Bridges auf die XMPP-Server zugreifen.

Navigieren Sie zu **Webadmin > Configuration > General**, und geben Sie Folgendes ein:

1. Fügen Sie einen eindeutigen Namen für die Anrufbrücke hinzu. Es ist kein Domänenteil erforderlich.
2. Geben Sie die Domäne für den XMPP-Server tptac9.com ein.
3. Serveradresse des XMPP-Servers. Legen Sie dieses Feld fest, wenn diese Anrufbrücke nur einen am gleichen Standort befindlichen XMPP-Server verwenden soll oder Sie keinen DNS konfiguriert haben. Die Verwendung des am gleichen Standort befindlichen XMPP-Servers reduziert die Latenz.
4. Lassen Sie dieses Feld leer, damit diese Anrufbrücke ein Failover zwischen XMPP-Servern ermöglicht. Dies erfordert die Einrichtung der DNS-Einträge.



Wenn Sie planen, den Domain Name Server (DNS) für die Verbindung zwischen Call Bridges und XMPP-Servern zu verwenden, müssen Sie auch einen DNS SRV-Datensatz für den xmpp-Cluster einrichten, um den DNS A-Datensatz jedes der XMPP-Server im Cluster aufzulösen. Das Format des DNS SRV-Datensatzes ist: **_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.
```

Im obigen Beispiel wird **Port 5223** angegeben (einen anderen Port verwenden, wenn bereits 5223 verwendet wurde).

den gemeinsamen geheimen Schlüssel, der für die jeweilige Anrufbrücke verwendet wird. Zum Beispiel in den obigen Screenshots

Cb1 geheim

Callbridge: cb1

Domäne: tptac9.com

geheim: **kvgP1SRzWVabhiPVAb1**

Wiederholen Sie diese Schritte ähnlich für cb2 und cb3 für alle 3 Call Bridges **cb1,cb2 und cb3**.

Wenn Sie diese Schritte ausgeführt haben, überprüfen Sie den Status des Clusters aller drei Anruf-Bridges.

Überprüfen

Führen Sie **cb1>> xmpp Cluster-Status aus**, dieser Befehl, um einen Bericht über den Live-Status des xmpp-Clusters abzurufen. Wenn der Cluster ausfällt, gibt dieser Befehl die Statistiken des xmpp-Servers zurück, der nur auf diesem Meeting-Server ausgeführt wird. Verwenden Sie diesen Befehl, um zu versuchen, Verbindungsprobleme zu diagnostizieren.

Dieses Bild zeigt die Knoten, eine als Leader 10.106.81.30 und die anderen zwei als 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
```

Überprüfen Sie auf ähnliche Weise den Status auf den anderen beiden Knoten.

Auf dem zweiten Knoten

```
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>
```

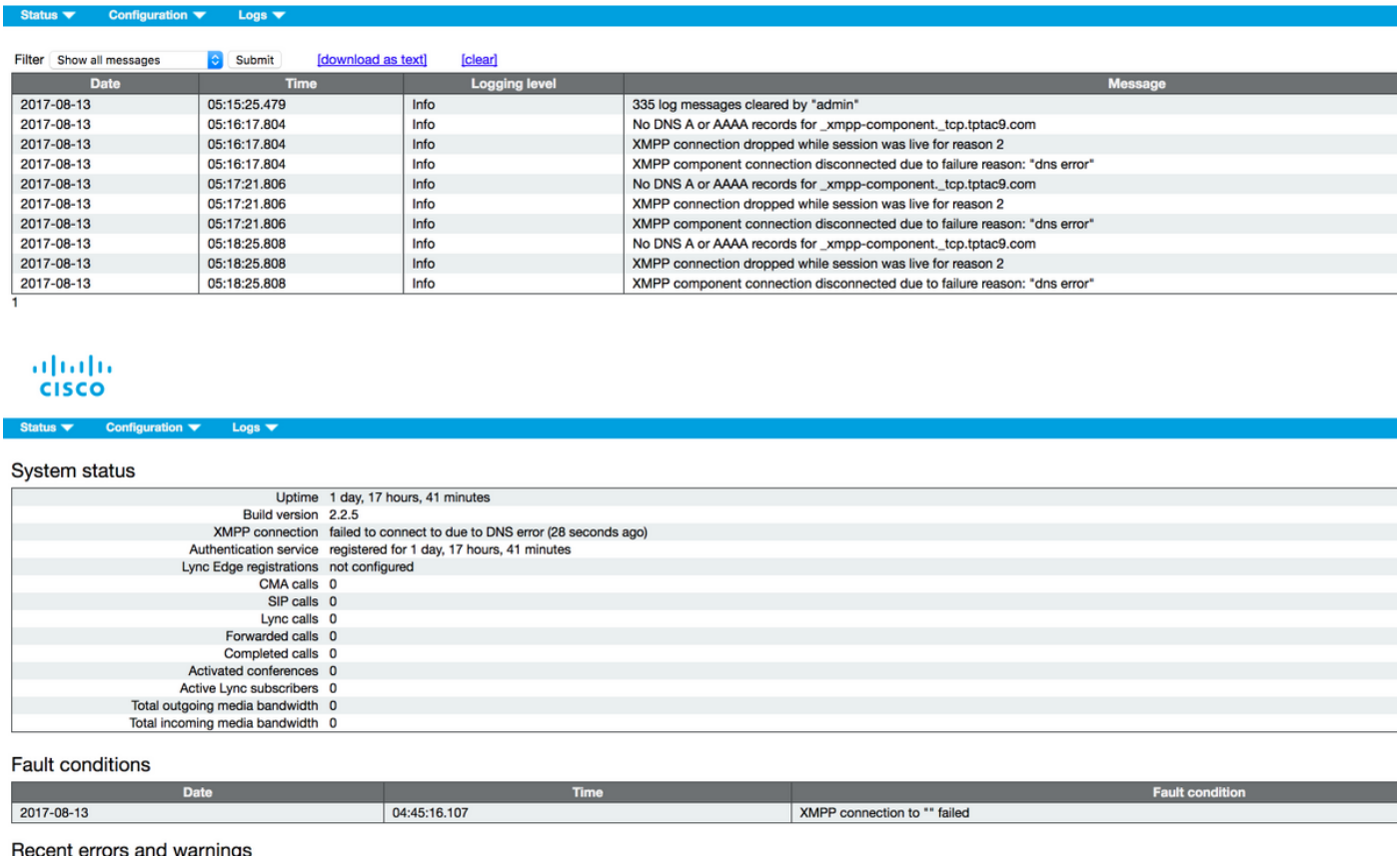
Auf drittem Knoten

```
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
```

Fehlerbehebung

XMPP-Ausfallsicherheit wurde erfolgreich eingerichtet. Bei der Verwendung von xmpp-Ausfallsicherheit können Probleme auftreten.

Szenario 1. Nach DNS-Konfiguration gesucht, zeigen die Fehler in den Screenshots auf die DNS-Probleme.



Status Configuration Logs

Filter Show all messages Submit [download as text] [clear]

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"

1

Status Configuration Logs

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 warnings

Wenn diese Fehler auftreten, überprüfen Sie die Konfiguration auf SRV-Datensätze.

In der XMPP-Ausfallsicherheit wird der XMPP-Server, mit dem eine Anruf-Bridge verbunden ist, über DNS gesteuert. Diese Auswahl basiert auf der angegebenen DNS-Priorität und -Gewichtung.

Eine Anruf-Bridge ist jeweils nur mit einem XMPP-Server verbunden. Es ist nicht erforderlich, dass alle Call Bridges eine Verbindung zum gleichen XMPP-Server herstellen, da der gesamte Datenverkehr an den Master weitergeleitet wird. Wenn ein Netzwerkproblem dazu führt, dass die Verbindung der Call Bridge zum XMPP-Server unterbrochen wird, versucht die Call Bridge, erneut eine Verbindung zu einem anderen XMPP-Server herzustellen. Die Call Bridge muss für jeden XMPP-Server konfiguriert werden, mit dem sie eine Verbindung herstellen kann.

Um Client-Verbindungen zu aktivieren, ist die Verwendung des WebRTC-Clients, eines **_xmpp-client._tcp-**Datensatzerforderlich. Bei einer typischen Bereitstellung wird die Lösung auf **Port 5222** aufgelöst. Im Inneren kann das LAN, wenn der Core-Server direkt routbar ist, zum XMPP-Dienst aufgelöst werden, der auf dem Core-Server ausgeführt wird.

Beispiel: **_xmpp-client._tcp.tptac9.com** kann folgende SRV-Datensätze enthalten:

_xmpp-client._tcp tptac9.com 86400 IN SRV 10 50 522 cb1. tptac9.com

Hinweise zur Einrichtung von DNS-Datensätzen für die XMPP-Serverknoten. Für XMPP-Ausfallsicherheit benötigen Sie DNS, um eine Verbindung zwischen Call Bridges und XMPP-Servern herzustellen. Außerdem müssen Sie einen DNS SRV-Datensatz für das xmpp-Cluster einrichten, um den DNS A-Eintrag jedes der XMPP-Server im Cluster aufzulösen. Das Format des DNS SRV-Datensatzes ist: **_xmpp-Component_tcp.tptac9.com**

Wie bei der Konfiguration für 3 xmpp-Server beschrieben, wird der Datensatz angezeigt, der auf alle drei Server aufgelöst wird.

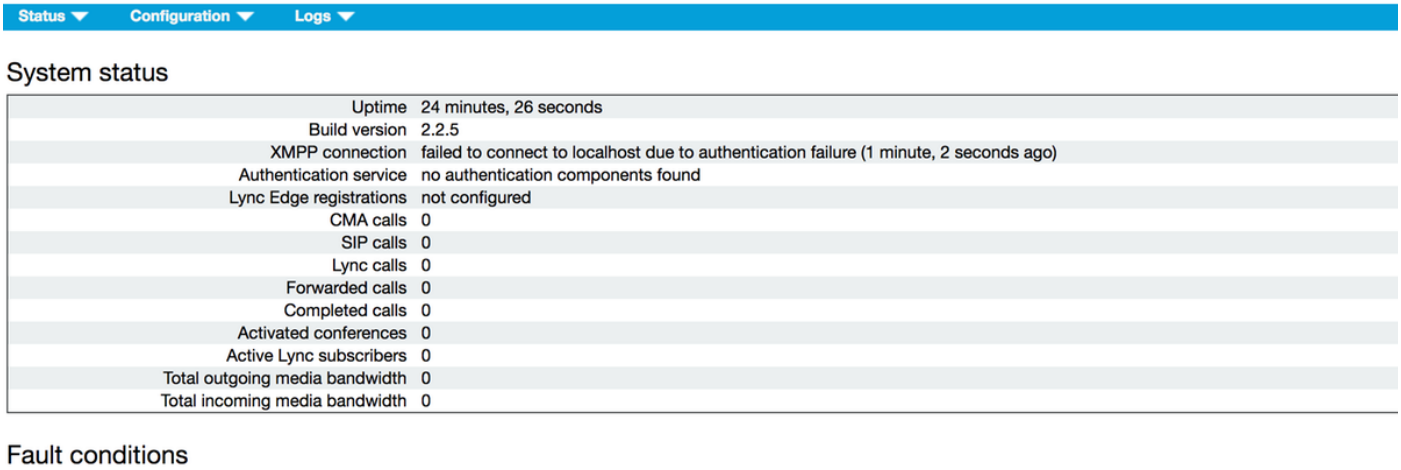
_xmpp-Component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb1.tptac9.com

_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

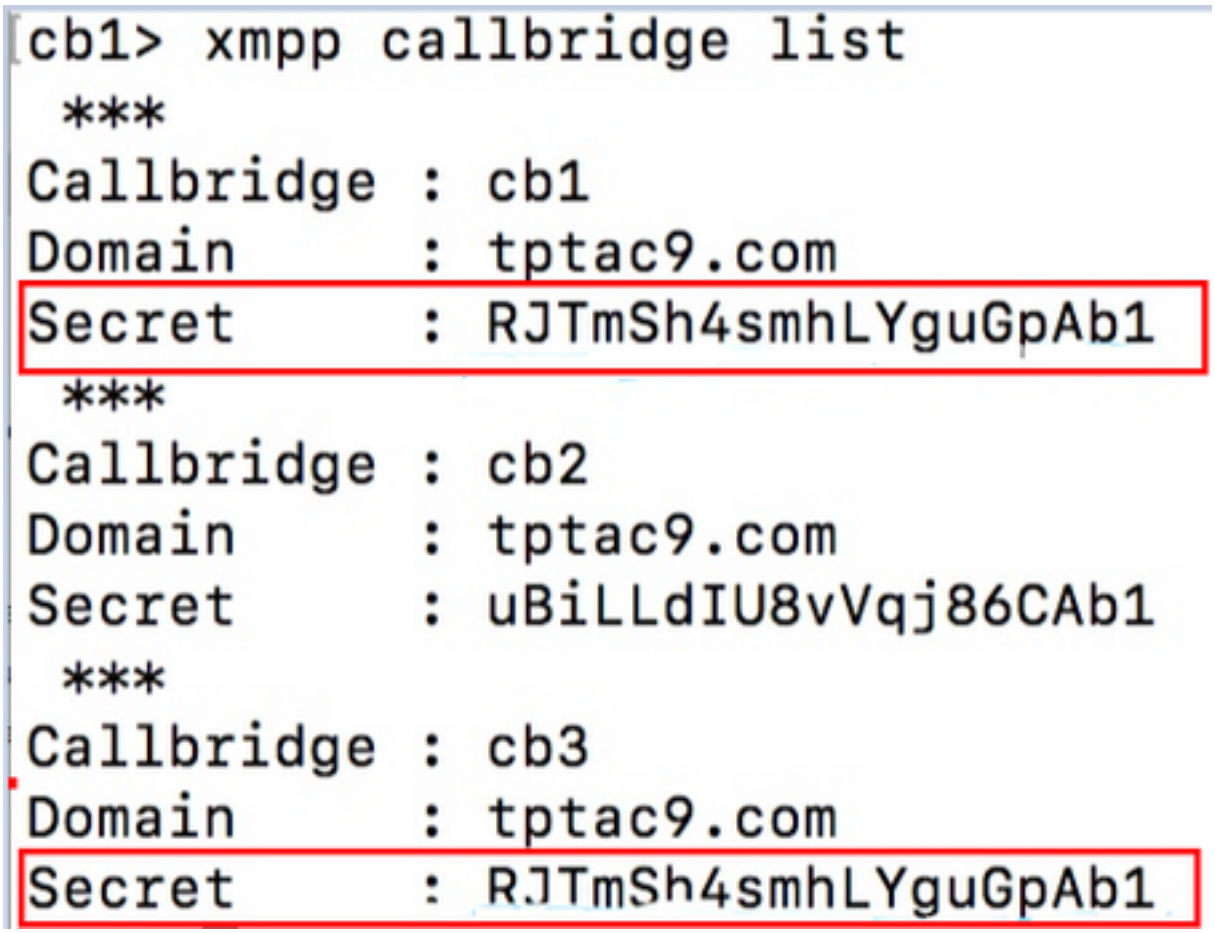
Im Beispiel wird der Port 5223 angegeben. Wenn der Port 5223 bereits verwendet wird, können auch andere Ports verwendet werden. Stellen Sie jedoch sicher, dass der verwendete Port geöffnet werden muss.

Szenario 2. Wenn die CMS-Statusseite einen **Authentifizierungsfehler** anzeigt.

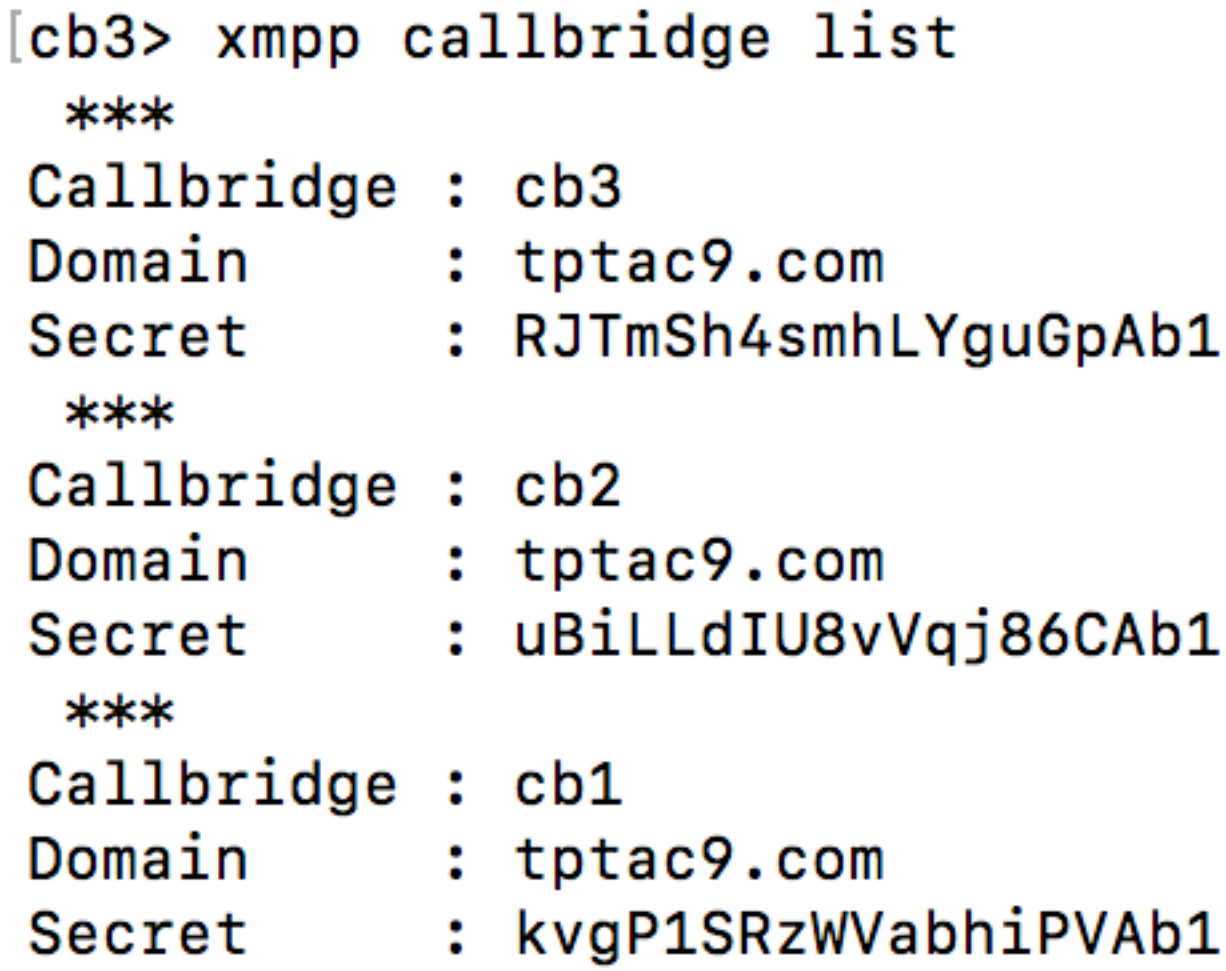


Der **Authentifizierungsfehler** tritt meistens dann auf, wenn entweder der gemeinsam verwendete geheime Schlüssel nicht eingegeben oder falsch eingegeben wird. Bitte stellen Sie sicher, dass

der geheime Schlüssel eingegeben wird, falls Sie ihn vergessen haben und nicht praktisch sind. Führen Sie den folgenden **Befehl** aus: **xmpp callbridge-Liste**




```
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
```



Das Dokument beschreibt die Einrichtung der xmpp-Ausfallsicherheit. Führen Sie den Befehl daher auf allen drei Servern aus, um sicherzustellen, dass die generierten Geheimnisse auf allen Servern gleich sind. Wie die Bilder zeigen, kann es auf dem Server **cb1** gesehen werden, ist der verwendete geheime Schlüssel derselbe wie der, der für **cb3** reflektiert wird. Nach der Überprüfung anderer Server wird der Schluss gezogen, dass der eingegebene geheime Schlüssel für **cb1** falsch ist.

Szenario 3. In xmpp Cluster-Status **doppelte Einträge** von XMPP-Knoten.

Diese Ausgabe zeigt den doppelten Eintrag des Knotens **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)
```

> **Vorsicht**: Es wird empfohlen, XMPP-Knoten aus dem Cluster zu entfernen, bevor Sie sie zurücksetzen. Wenn XMPP-Reset auf einem Knoten ausgeführt wird, während er sich noch im Cluster befindet, und dann wieder dem vorhandenen XMPP-Cluster beitritt, wird ein doppelter Eintrag dieses Knotens erstellt, wenn der Status über den xmpp-Cluster-Status überprüft wird.

Dies kann bei einer ausfallsicheren Konfiguration zu Problemen führen. Es wurde ein Fehler ausgelöst.

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

Bitte lesen Sie Seite 94 des nachstehenden Leitfadens.

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