Configura resilienza XMPP

Sommario

Introduzione

In questo documento viene descritto come configurare Extensible Messaging and Presence Protocol (XMPP) Resiliency su Cisco Meeting Server (CMS).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Il clustering del database deve essere impostato prima della resilienza XMPP. Questo è il collegamento per l'impostazione del clustering del database

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

- Il componente Callbridge deve essere configurato in CMS
- Cisco consiglia di avere almeno 3 nodi XMPP per poter configurare la resilienza XMPP
- Quando l'installazione è in modalità Resilient, i server XMPP all'interno di una distribuzione vengono caricati con la stessa configurazione
- Informazioni sui certificati autofirmati, firmati da CA
- DNS (Domain Name Server) richiesto
- Per generare certificati è necessaria un'Autorità di certificazione locale o pubblica

Nota: L'utilizzo di certificati autofirmati non è consigliato per l'ambiente di produzione

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

- CMS

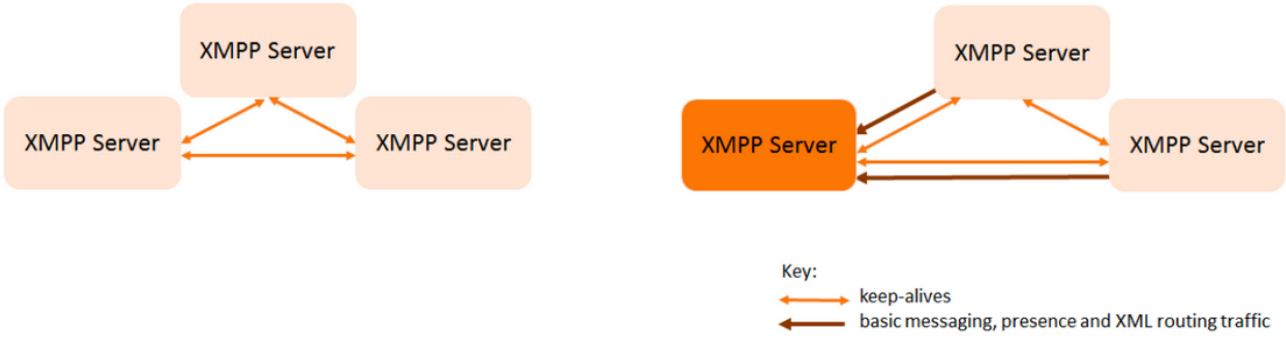
- Software di emulazione terminale PuTTy Secure Shell (SSH) per MMP (Mainboard Management Processor)
- Un browser web come Firefox, Chrome

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Questa immagine mostra lo scambio di messaggi XMPP e il traffico di routing.



Configurazione

In questo esempio di distribuzione della resilienza XMPP vengono utilizzati tre server XMPP che vengono configurati per la prima volta.

> **Nota:** Se la resilienza XMPP è già stata distribuita, si consiglia di reimpostare tutti i server.

I server XMPP utilizzano messaggi keep-alive per monitorare gli altri server e selezionare un coordinatore. I messaggi XMPP possono essere inviati a qualsiasi server. Come mostrato nell'immagine precedente, i messaggi vengono inoltrati al server XMPP Leader. I server XMPP continuano a monitorarsi l'un l'altro, se il Leader si guasta viene selezionato un nuovo Leader e gli altri server XMPP inoltrano il traffico al nuovo Leader.

Passaggio 1. Generare certificati per il componente XMPP.

Generare CSR, quindi eseguire questo comando per generare il certificato corrispondente tramite Autorità di certificazione locale/Autorità di certificazione pubblica, come richiesto

pki csr <nome base chiave/certificato>

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

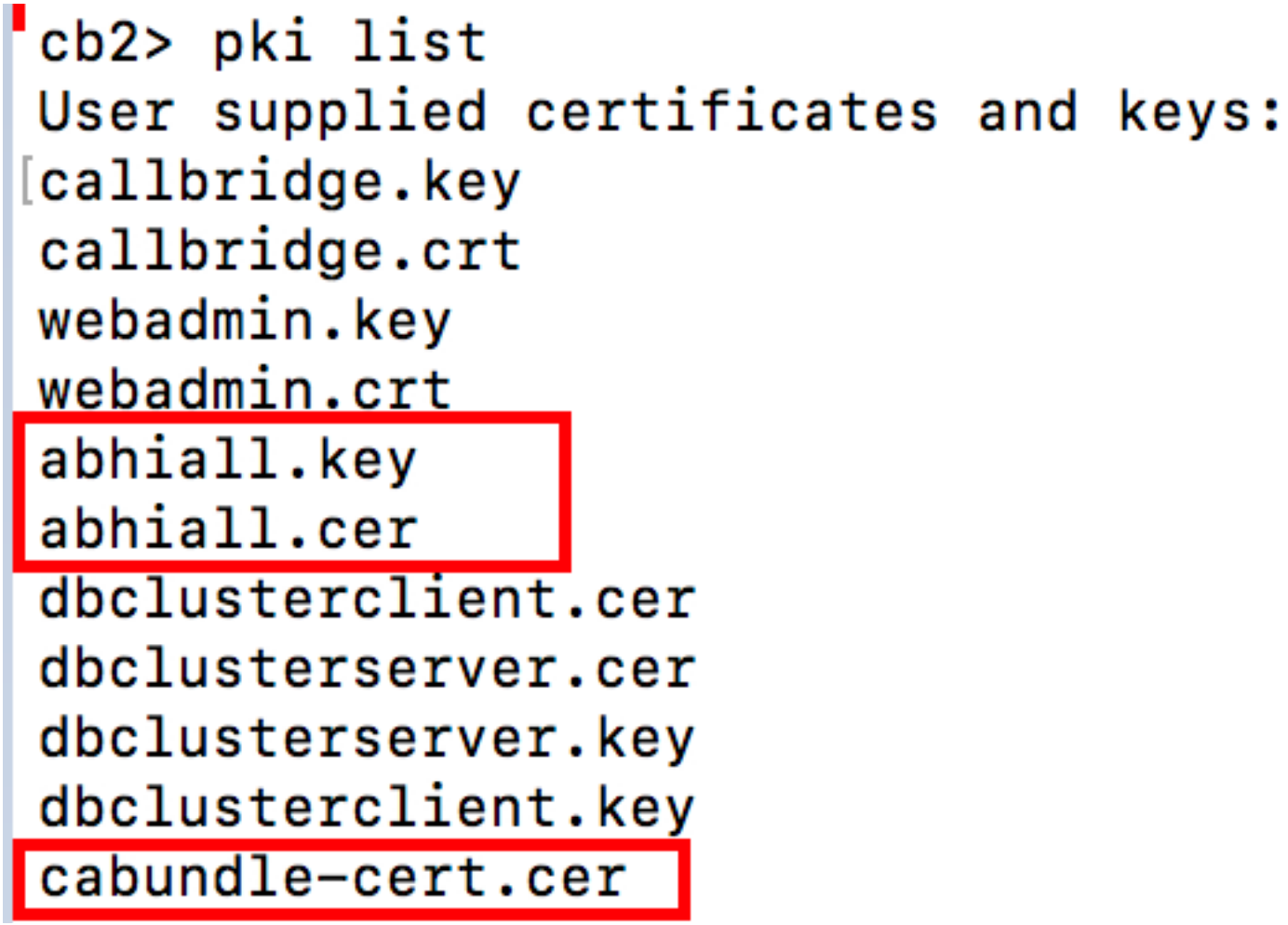
Passaggio 2. Utilizzare il CSR precedente e generare il certificato utilizzando l'autorità di certificazione locale. È possibile utilizzare la guida al certificato VCS per generare certificati

utilizzando Microsoft Certificate Authority, Appendice 5 pagina 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

Caricare il certificato su tutti e tre i nodi utilizzando il server WINSCP/SFTP. Per verificare se i certificati da caricare utilizzano un comando su MMP/SSH

comando: elenco pki



Nota: In lab, viene utilizzato un certificato per tutti e tre i nodi XMPP.

Passaggio 3. Configurare CMS per l'utilizzo del componente XMPP.

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

*certall.cer= CA certificate
```

Suggerimento: Se la CA fornisce un bundle di certificati, includere il bundle come file separato al certificato. Un bundle di certificati è un singolo file (con estensione **.pem**, **.cer** o**.crt**) che contiene una copia del certificato della CA radice e tutti i certificati intermedi della catena. I certificati devono essere in sequenza e il certificato della CA radice deve essere l'ultimo nel bundle dei certificati. I client esterni (ad esempio i browser Web e i client XMPP) richiedono che il certificato e il pacchetto di certificati siano presentati rispettivamente dal

server XMPP, durante la configurazione di una connessione protetta.

Quando è richiesto un bundle di certificati. Il comando precedente sarebbe

```
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
```

Quando si utilizzano 3 certificati per 3 nodi XMPP rispettivi. Assicurati di raggruppare i certificati

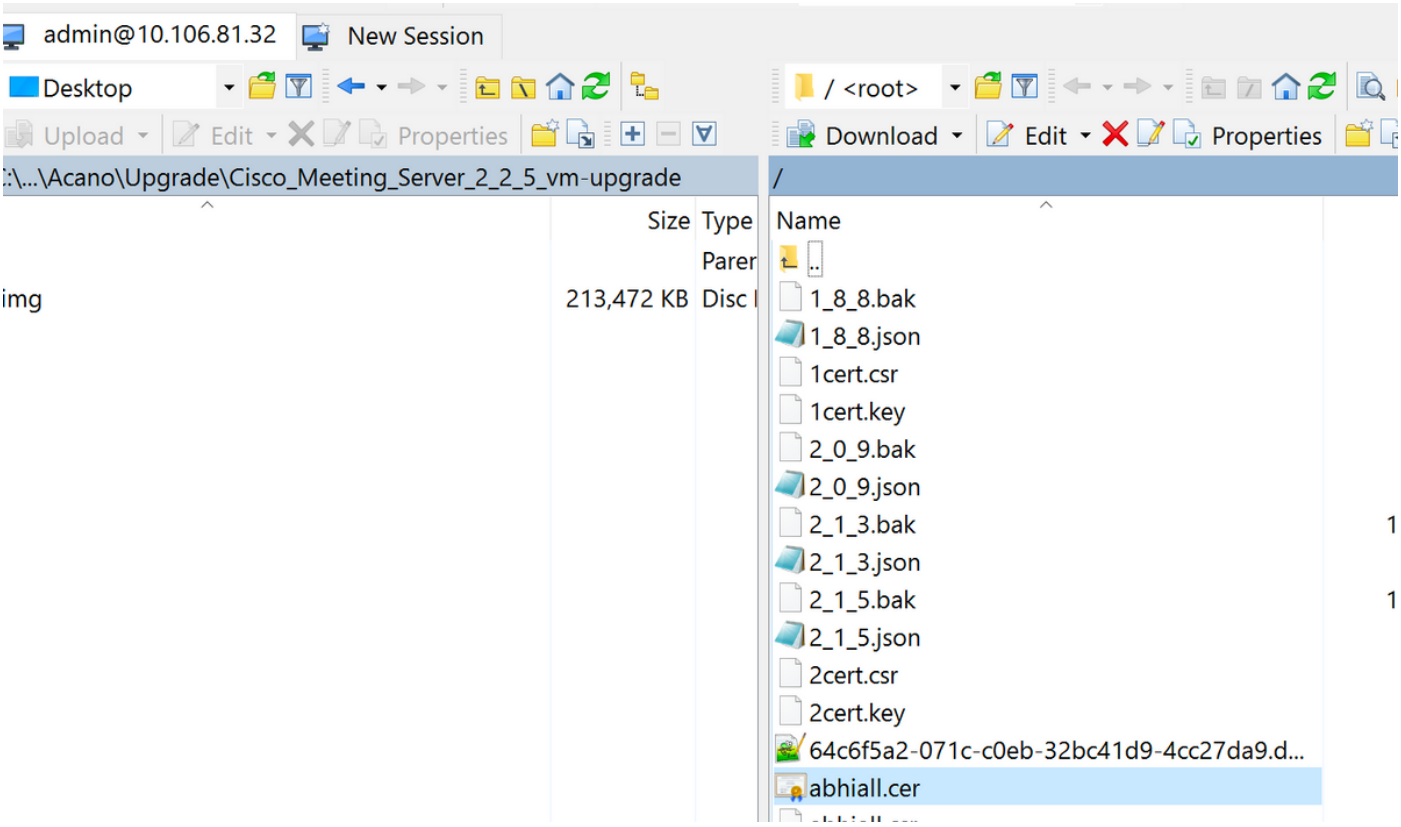
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

Nel documento viene utilizzato un singolo certificato **abhiall.cer**.

Fare riferimento a questa guida per ulteriori dettagli sui certificati

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

Passaggio 4. Caricare i certificati tramite SFTP in tutti i CMS, che eseguono il componente XMPP.



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

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

cb1>>trust cluster xmpp abhiall.cer

Passaggio 5. Aggiungere i bridge di chiamate al server XMPP.

cb1> xmpp callbridge add cb1

Viene generato un segreto. In questo modo il server XMPP viene configurato per consentire le connessioni con il **bridge di chiamate** denominato **cb1**.

> **Nota:** Il dominio, il nome e il segreto del bridge di chiamate vengono generati. Queste informazioni sono necessarie in seguito quando si configura l'accesso del bridge di chiamate al server XMPP (in modo che il bridge di chiamate presenti i dettagli di autenticazione al server XMPP)

Il comando precedente viene utilizzato per aggiungere altri bridge di chiamate allo stesso nodo xmpp.

cb1> xmpp callbridge add cb2

cb1> xmpp callbridge add cb3

> **Nota**:ogni bridge di chiamate deve avere un **nome univoco**. Se non sono già stati annotati i dettagli dei bridge di chiamata aggiunti al server XMPP, utilizzare il **comando: elenco callbridge xmpp**

cb1> disattivazione xmpp

In questo modo viene disattivato il nodo del server XMPP

Passaggio 6. Abilitare il cluster XMPP.

cb1> abilitazione cluster xmpp

Inizializzare il cluster XMPP in questo nodo. Con questo comando viene creato un **cluster xmpp a 1 nodo** e gli altri nodi (server xmpp) vengono uniti a questo cluster.

cb1> inizializzazione cluster xmpp

Riattiva nodo

cb1>abilitazione xmpp

Passaggio 7. Aggiungere i bridge di chiamata al secondo nodo XMPP e aggiungerlo a un cluster.

Aggiungere ogni bridge di chiamate a questo nodo. È quindi necessario aggiungere il bridge di chiamate utilizzando lo stesso nome e segreto del bridge di chiamate del primo nodo del server XMPP. Per ottenere questo risultato, usare questo comando

cb2>> xmpp callbridge add-secret cb1

Immettere il segreto del bridge di chiamate

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

Per verificare il segreto, eseguire il comando **xmpp call bridge list**. Vengono elencati tutti i segreti generati nel primo nodo.

```
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
```

Dopo aver aggiunto tutti i bridge di chiamata al secondo nodo.

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

Cluster: è l'indirizzo IP o il nome di dominio del primo nodo

Passaggio 8. Aggiungere i bridge di chiamata al terzo nodo XMPP e aggiungerlo a un cluster.

Aggiungere ogni bridge di chiamate a questo nodo. È quindi necessario aggiungere il bridge di chiamate utilizzando lo stesso nome e segreto del bridge di chiamate del primo nodo del server XMPP. A tale scopo, utilizzare il comando

cb3>> xmpp callbridge add-secret cb1

Immettere il segreto del bridge di chiamate

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

Ora per controllare il segreto. È possibile eseguire il comando **xmpp callbridge list**. Il comando elenca tutti i segreti generati sul primo nodo

```
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
```

Dopo l'aggiunta di tutti i segreti del bridge di chiamate a questo nodo, eseguire la procedura seguente.

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

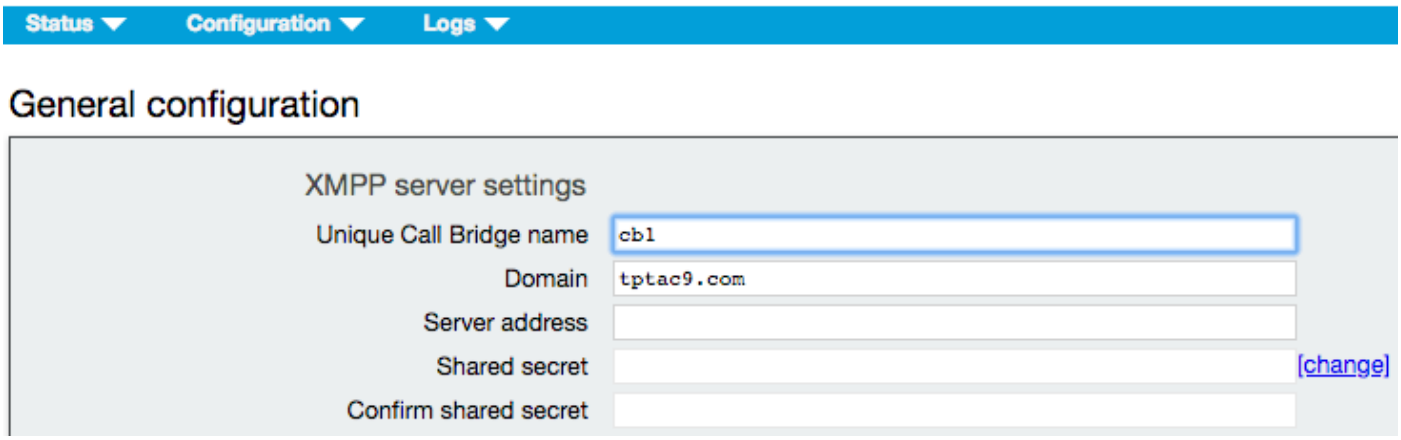
Cluster: è l'indirizzo IP o il nome di dominio del primo nodo

Passaggio 9. Configurare ogni bridge di chiamate con i dettagli di autenticazione dei server XMPP nel cluster. Ciò consente ai bridge di chiamate di accedere ai server XMPP.

Passare a **Webadmin > Configurazione > Generale** e immettere quanto segue:

1. Aggiungere un nome di bridge di chiamate univoco. Non è richiesta alcuna parte del dominio.
2. Immettere il dominio per il dominio del server XMPP tptac9.com
3. Indirizzo server del server XMPP. Impostare questo campo se si desidera che il bridge di chiamate utilizzi solo un server XMPP nella stessa posizione oppure se non si dispone di DNS configurato. L'utilizzo del server XMPP nella stessa posizione riduce la latenza.

4. Lasciare vuoto questo campo per consentire al bridge di chiamate di eseguire il failover tra server XMPP. È necessario configurare le voci DNS.



Se si intende utilizzare il DNS (Domain Name Server) per la connessione tra i bridge di chiamata e i server XMPP, è inoltre necessario configurare un record DNS SRV per il cluster xmpp per risolvere il record A DNS di ogni server XMPP nel cluster. Il formato del record DNS SRV è: **_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.
```

Nell'esempio precedente viene specificata la **porta 5223** (utilizzare un'altra porta se la porta 5223 è già in uso).

il segreto condiviso utilizzato per il rispettivo Call Bridge. Ad esempio, nelle schermate precedenti

Il segreto Cb1 è

Callbridge: cb1

Dominio: tptac9.com

Secret: **kvgP1SRzWVabhiPVAb1**

Analogamente, per cb2 e cb3, ripetere questi passaggi per tutti i 3 ponti di chiamata **cb1, cb2 e cb3**.

Dopo aver eseguito questi passaggi, controllare lo stato del cluster su tutti e tre i bridge di chiamate

Verifica

Eseguire **cb1>> xmpp cluster status** per ottenere un report sullo stato attivo del cluster xmpp. Se il cluster ha esito negativo, questo comando restituirà le statistiche del server xmpp, che viene eseguito solo in questo Meeting Server. Utilizzare questo comando per diagnosticare i problemi di connettività.

Nell'immagine vengono mostrati i nodi, uno come Leader 10.106.81.30 e gli altri due come 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
```

Analogamente, controllare lo stato sugli altri due nodi.

Sul secondo nodo

```
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>
```

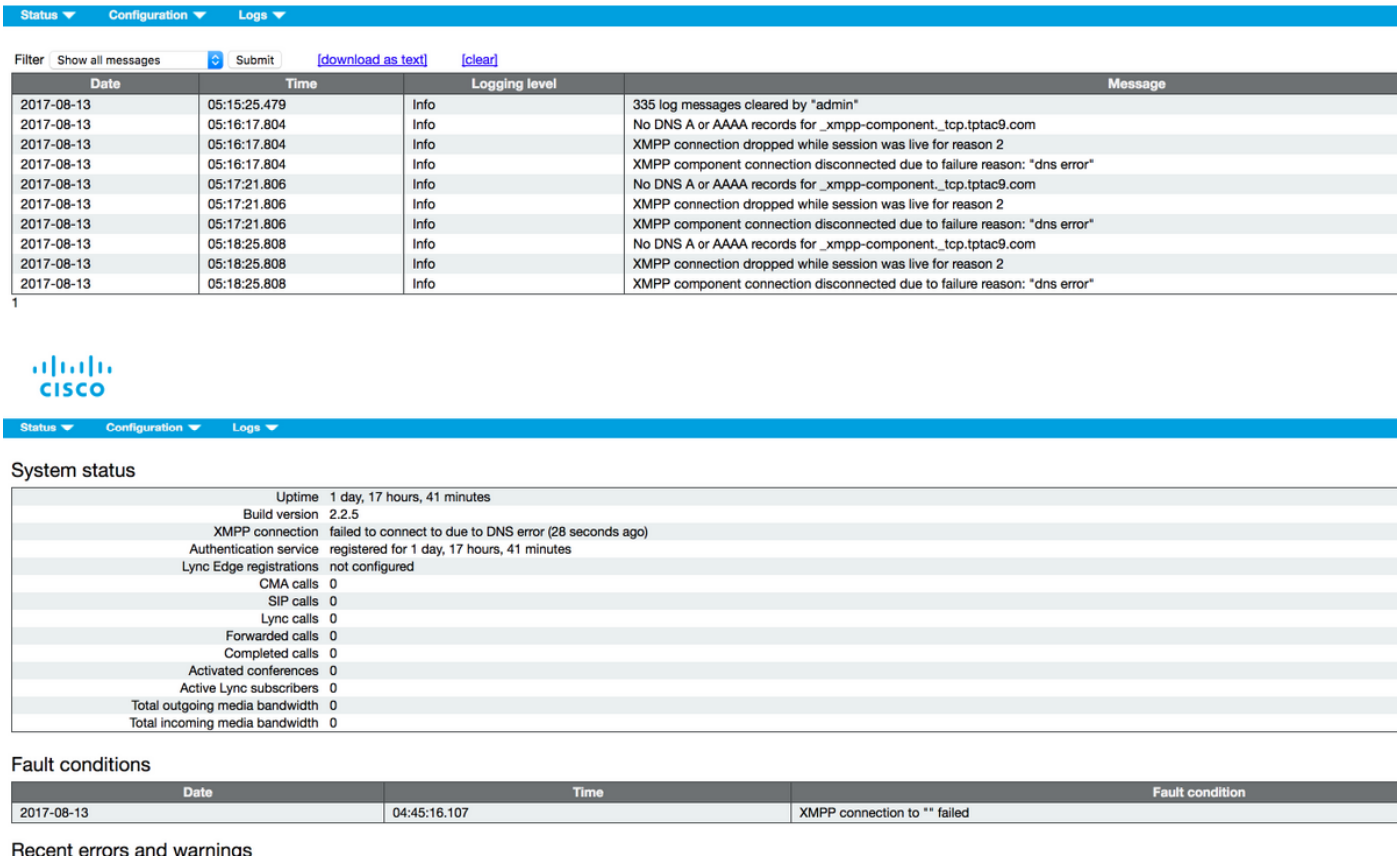
Sul terzo nodo

```
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
```

Risoluzione dei problemi

Configurazione resilienza XMPP completata. L'utilizzo della resilienza xmpp potrebbe causare problemi.

Scenario 1. Dopo aver verificato la configurazione DNS, gli errori negli screenshot indicano i problemi relativi al DNS.



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

Se vengono rilevati questi errori, controllare la configurazione per i record SRV.

Nella resilienza XMPP, il server XMPP a cui si connette un bridge di chiamate è controllato tramite DNS. Questa scelta si basa sulla priorità e sul peso DNS forniti. Un bridge di chiamate si connette

a un solo server XMPP alla volta. Non è necessario che tutti i bridge di chiamate si connettano allo stesso server XMPP poiché tutto il traffico viene inoltrato al master. Se a causa di un problema di rete il bridge di chiamate perde la connessione al server XMPP, tenta di riconnettersi a un altro server XMPP. Il bridge di chiamate deve essere configurato su qualsiasi server XMPP a cui può connettersi.

Per abilitare le connessioni client, utilizzare il client WebRTC, un record **_xmpp-client._tcp**. In un'implementazione tipica, viene risolto nella **porta 5222**. All'interno, la LAN, se il server principale è direttamente instradabile, può risolversi nel servizio XMPP, che viene eseguito sul server principale.

Ad esempio: **_xmpp-client._tcp.tptac9.com** può avere i seguenti record SRV:

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

consigli sulla configurazione dei record DNS per i nodi server XMPP. Ad esempio, la resilienza XMPP necessaria al DNS per la connessione tra i bridge di chiamate e i server XMPP sarà inoltre necessario impostare un record DNS SRV per il cluster xmpp per risolvere il record A DNS di ogni server XMPP nel cluster. Il formato del record DNS SRV è: **_xmpp-component._tcp.tptac9.com**

In base alla configurazione descritta per 3 server xmpp, viene visualizzato il record che risolve tutti e tre i server

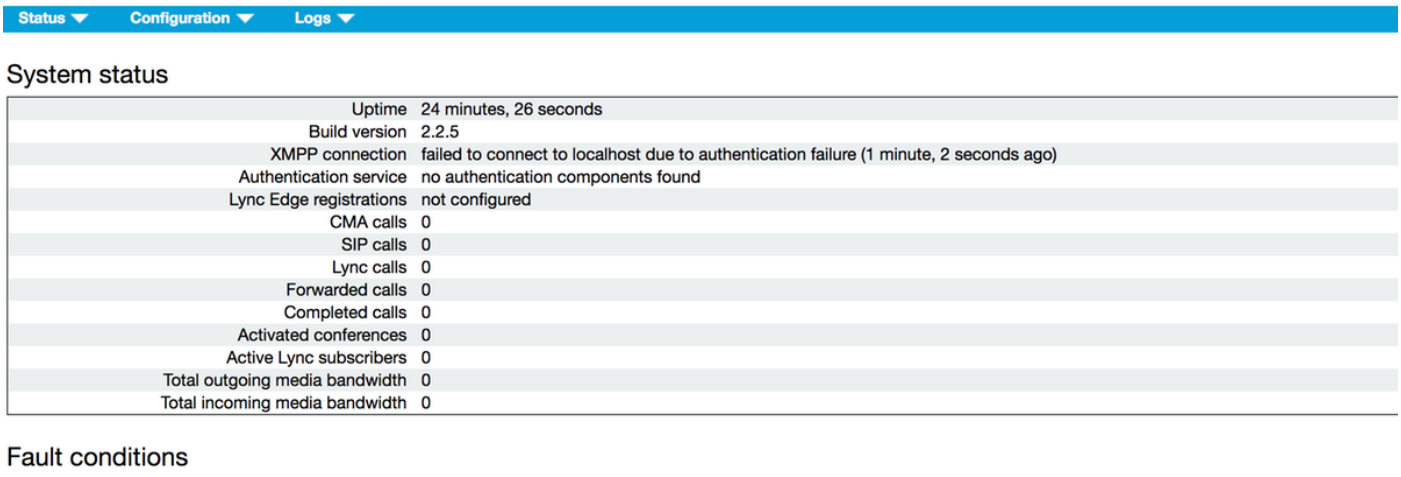
_xmpp-component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb1.tptac9.com

_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

Nell'esempio viene specificata la porta 5223. È possibile utilizzare qualsiasi altra porta se la porta 5223 è già in uso. Accertarsi tuttavia che la porta utilizzata sia aperta.

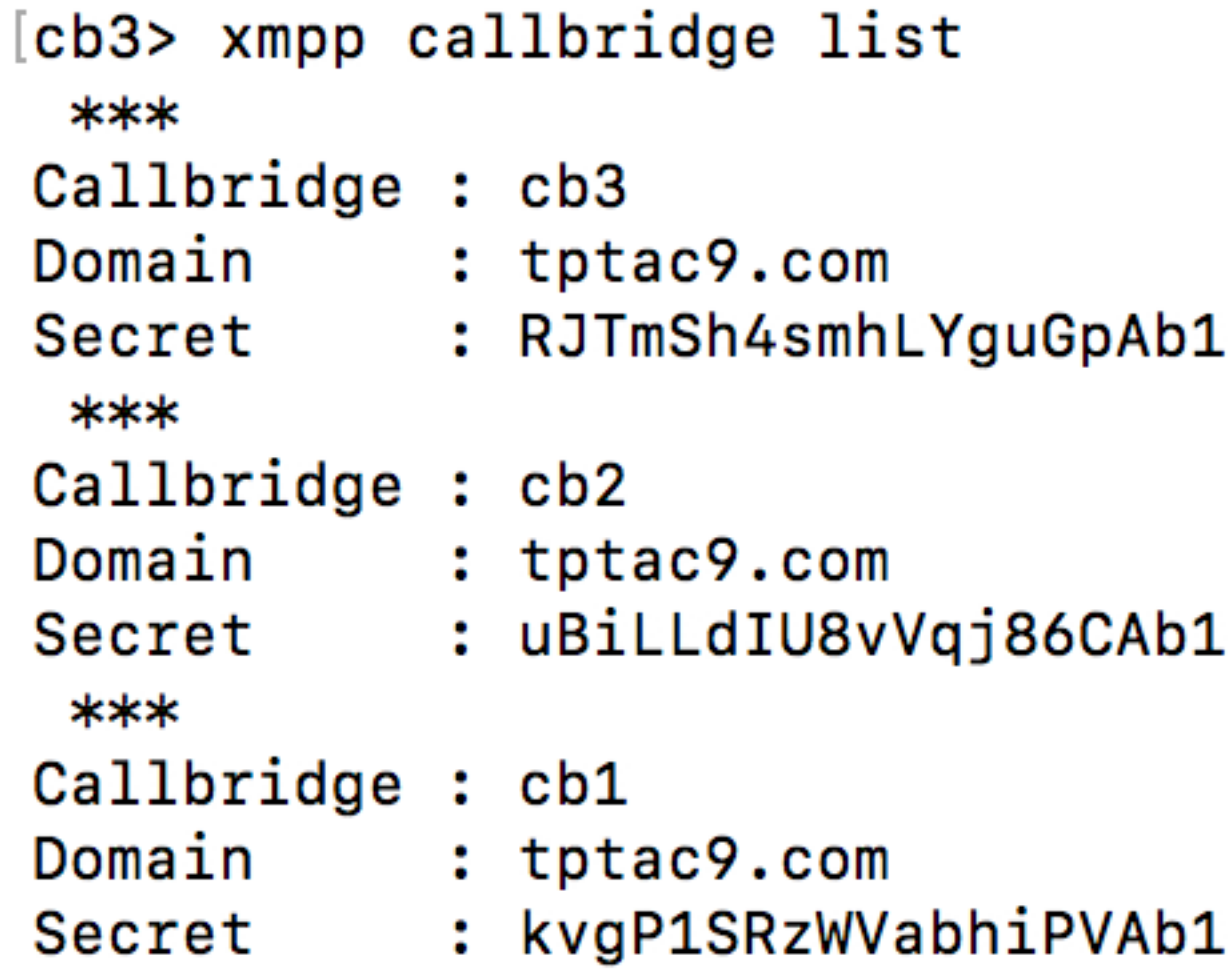
Scenario 2. Quando la pagina di stato CMS mostra un **errore di autenticazione.**



L'**errore di autenticazione** si verifica principalmente quando il segreto condiviso non viene immesso o immesso in modo non corretto. Verifica che il segreto condiviso sia inserito, se dimenticato e se non lo hai a portata di mano. Collegare il supporto SSH al server ed eseguire questo **comando: elenco callbridge xmpp**

```
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
```



Nel documento viene descritta l'impostazione della resilienza xmpp. Eseguire quindi il comando su tutti e 3 i server per verificare che i segreti generati siano gli stessi in tutti i server. Come illustrato nelle immagini, può essere visualizzato sul server **cb1**, il segreto condiviso utilizzato è lo stesso che viene riflesso per **cb3**. Dopo aver controllato su altri server, si conclude che il segreto immesso per **cb1** non è corretto.

Scenario 3. In stato cluster xmpp **voci duplicate** di nodi XMPP.

Questo output mostra la voce duplicata del nodo **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)
```

> **Attenzione**: si consiglia di rimuovere i nodi xmpp dal cluster prima di reimpostarli. Se la reimpostazione di XMPP viene eseguita su un nodo mentre si trova ancora nel cluster e quindi si aggiunge nuovamente il nodo al cluster XMPP esistente, viene creata una voce duplicata del nodo quando viene verificato lo stato tramite lo stato del cluster XMPP.

Ciò può causare problemi in una configurazione resiliente. È stato rilevato un difetto

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

Consultare la pagina 94 della guida riportata di seguito

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