Configurar a resiliência do XMPP

Contents

Introduction

Este documento descreve como configurar o Extensible Messaging e Presence Protocol (XMPP) no Cisco Meeting Server (CMS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O clustering do banco de dados deve ser configurado antes da resiliência de XMPP. Este é o link para configurar o cluster do banco de dados

https://www.Cisco.com/c/en/us/support/docs/Conferencing/Meeting-Server/210530-Configure-Cisco-Meeting-Server-Call-Brid.HTML

- O Componente de Callbridge deve estar configurado no CMS
- A Cisco recomenda que você tenha pelo menos 3 nós XMPP para configurar a resiliência de XMPP
- Quando a instalação está no modo resiliente, os servidores XMPP em uma implantação são carregados com a mesma configuração
- Compreensão de certificados autoassinados e por Autoridade de certificado (CA)
- Domain Name Server (DNS) exigido
- Énecessário uma autoridade de certificado local ou pública para gerar certificados

Note: Usar certificados autoassinados não é recomendado para o ambiente de produção

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

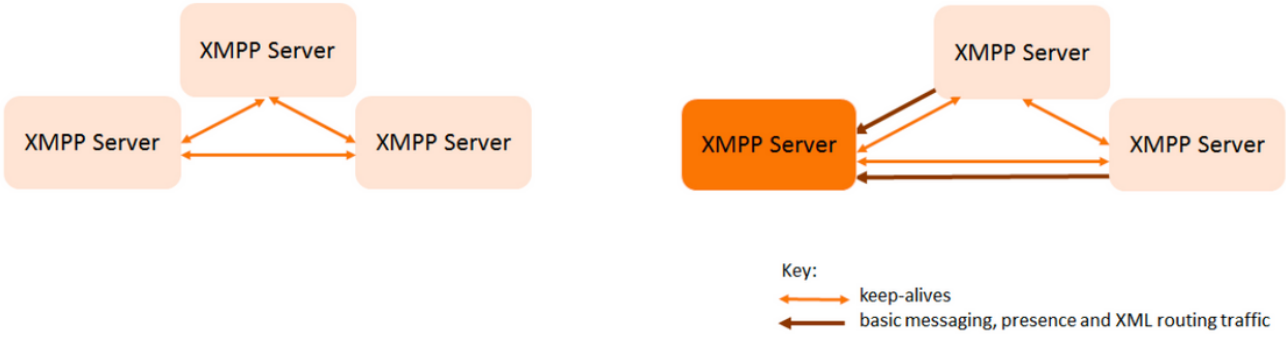
- CMS
- Software de emulação de terminal puTTY Secure Shell (SSH) para o processador de gerenciamento de placa-mãe (MMP)
- Um navegador da Web, como o Firefox, Chrome

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.

Configurar

Diagrama de Rede

Essa imagem mostra a troca de mensagens XMPP e roteamento do tráfego.



Configuração

Este exemplo de implantação de resiliência XMPP usa três servidores XMPP e configura-a pela primeira vez.

> **Note**: Se a resiliência XMPP já estiver instalada, então, é recomendável redefinir todos os servidores.

Os servidores XMPP usam mensagens de manutenção de funcionamento para monitorar uns aos outros e eleger um líder. As mensagens XMPP podem ser enviadas para qualquer servidor. Como mostrado na imagem anterior, as mensagens são encaminhadas para o servidor XMPP líder. Os servidores XMPP continuarão a monitorar uns aos outros, se o líder falhar, então, um novo líder é eleito e os outros servidores XMPP encaminham o tráfego para o novo líder.

Etapa 1. Gerar certificados para o componente XMPP.

Gere CSR e, em seguida, emita esse comando para gerar o certificado correspondente por meio de autoridade de certificação local/público, conforme necessário

pki csr <key/cert basename>

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

Etapa 2. Use CSR acima e gere o certificado usando a autoridade de certificado local. Você pode

usar o guia Certificado VCS para gerar certificados usando a Autoridade de certificado da Microsoft, Apêndice 5, página 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

Carregue o certificado em todos os 3 nós usando o servidor WINSCP/SFTP. Para verificar se os certificados carregados usam um comando em MMP/SSH

comando: Lista de PKI

```
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: No laboratório, um certificado é usado para todos os 3 nós XMPP.

Etapa 3. Configure o CMS para usar o componente XMPP.

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

*certall.cer= CA certificate
```

Tip: Se sua CA fornece um pacote de certificado, inclua o pacote como um arquivo separado ao certificado. Um pacote de certificado é um único arquivo (com uma extensão de PEM, **.cer ou .crt) mantendo uma cópia do certificado de CA de raiz e toda a cadeia de certificados intermediários.** Os certificados precisam estar na sequência com o certificado da CA raiz sendo última no pacote certificado. Os clientes externos (por exemplo, navegadores

da web e clientes XMPP) exigem o certificado e o pacote de certificado a ser apresentado pelo servidor XMPP, respectivamente, ao configurar uma conexão segura.

Quando o pacote de certificados é necessário. O comando acima seria

```
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
```

Ao usar 3 certificados de 3 nós XMPP respectivos. Certifique-se de agrupar os certificados

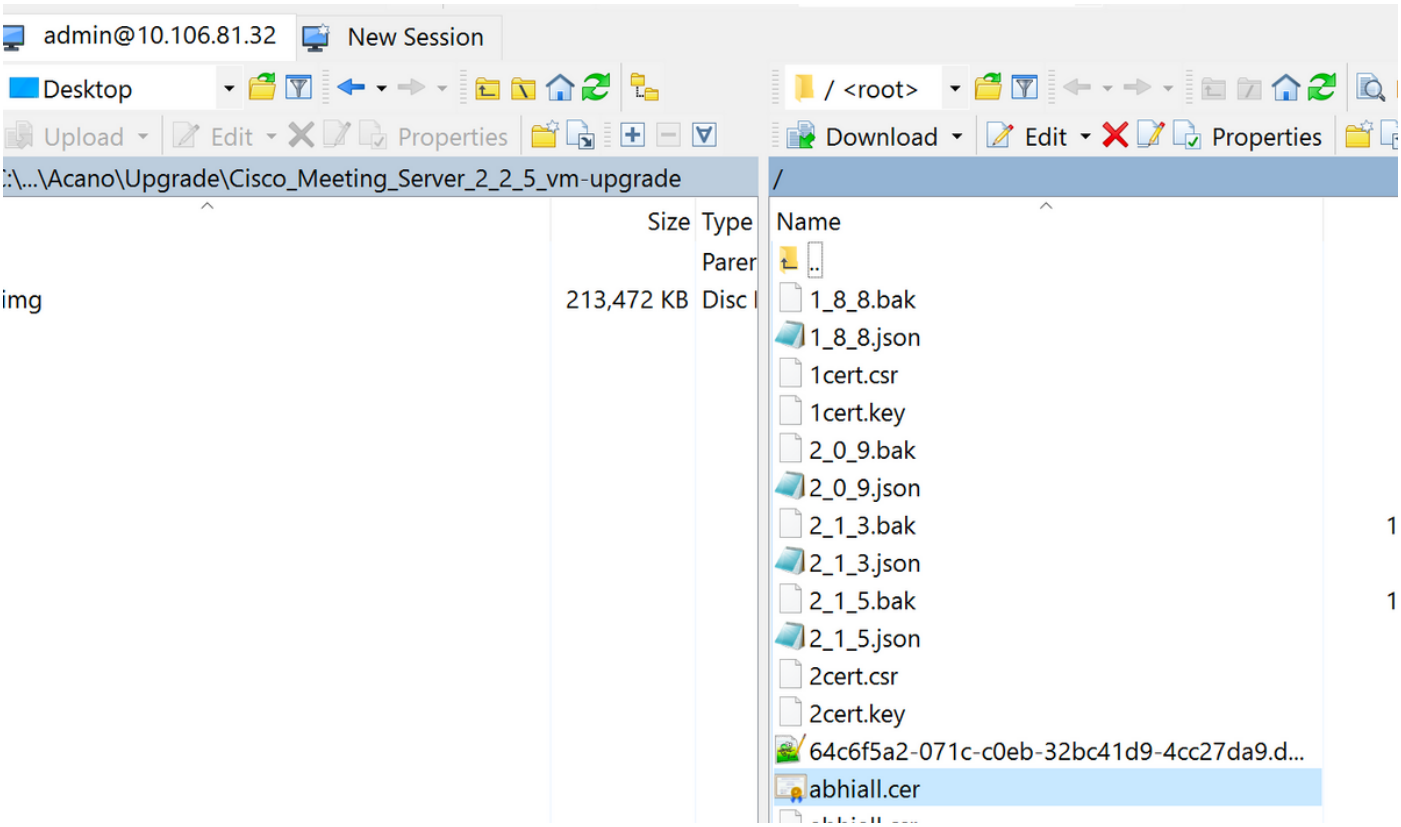
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

Um único certificado **abhiall.cer** é usado no documento.

Consulte este guia para conhecer mais detalhes sobre certificados

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

Etapa 4. Carregue certificados por meio do SFTP para todo o CMS, que executa o componente XMPP.



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

No laboratório xmpp cluster trust **abhiall.cer**

cb1 >> xmpp cluster trust abhiall.cer

Etapa 5. Adicionar Call Bridges ao servidor XMPP.

cb1 > xmpp callbridge add cb1

Um segredo é gerado, isto configura o servidor XMPP para permitir conexões com a **Call Bridgechamada cb1**.

> **Note**: O domínio, o nome de Call Bridge e o segredo são gerados, você precisará dessa informação mais tarde quando configurar o acesso da Call Bridge para o servidor XMPP (de modo que a Call Bridge apresente os detalhes de autenticação para o servidor XMPP)

O comando acima é usado para adicionar outras Call Bridges ao mesmo nó xmpp.

cb1> xmpp callbridge add cb2

cb1> xmpp callbridge add cb3

> **Nota**:Cada ponte de chamada deve ter um **nome exclusivo**. Se você ainda não observou os detalhes para as Call Bridges que adicionou para o servidor XMPP, então, use o **comando: xmpp callbridge list**

cb1> xmpp disable

Isso desabilita o nó de servidor XMPP

Etapa 6. Ative o cluster XMPP.

cb1> xmpp cluster enable

Inicialize o cluster XMPP neste nó. Esse comando cria um **cluster xmpp de 1 nó**, os outros nós (servidores xmpp) estão associados a este cluster.

cb1> xmpp cluster initialize

Ative novamente este nó

cb1> xmpp enable

Passo 7. Adicione Call Bridges ao segundo nó XMPP e junte-o a um cluster.

Adicione cada Call Bridge a esse nó. Isso requer que a Call Bridge a ser adicionada use o mesmo nome e segredo da Call Bridge do primeiro nó de servidor XMPP. Isso é obtido usando o comando:

cb2>> xmpp callbridge add-secret cb1

Insira um segredo da Call Bridge

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

Para verificar o segredo execute o comando **xmpp call bridge list**. Ele lista todos os segredos gerados no primeiro nó.

```
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
```

Depois de adicionar todos os o segredo de Call Bridges ao segundo nó.

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

Cluster: é o Endereço IP ou nome do domínio do primeiro nó

Etapa 8. Adicione Call Bridges ao terceiro nó XMPP e junte-o a um cluster.

Adicione cada Call Bridge a esse nó. Isso requer que a Call Bridge a ser adicionada use o mesmo nome e segredo da Call Bridge do primeiro nó de servidor XMPP. Isto é feito por meio deste comando:

cb3>> xmpp callbridge add-secret cb1

Insira um segredo da Call Bridge

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

Agora verifique o segredo. Você pode executar o comando **xmpp callbridge list**. O comando lista todos os segredos gerados no primeiro nó.

```
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
```

Depois que todos os segredos da Call Bridge forem adicionados a esse nó execute essas etapas.

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

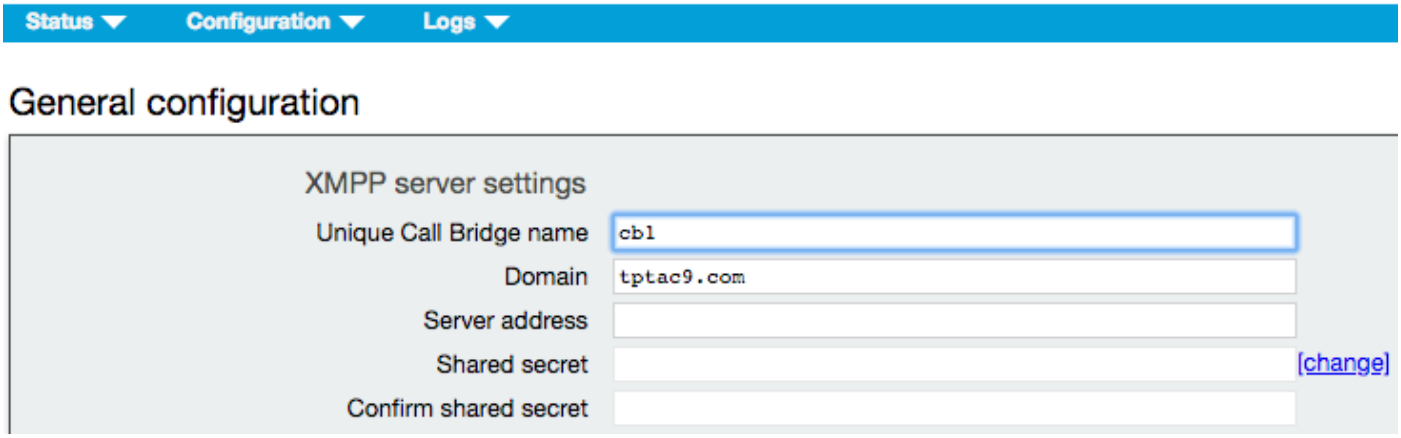
Cluster: é o Endereço IP ou nome do domínio do primeiro nó

Etapa 9. Configure cada Call Bridge com os detalhes de autenticação dos servidores XMPP no cluster. Isso permite que as Call Bridges de chamada acessem os servidores XMPP.

Navegue até **Webadmin > Configuração > Geral e insira:**

1. Adicione o nome da Call Bridge exclusiva, nenhuma parte do domínio é obrigatória.
2. Digite o domínio para o servidor XMPP tptac9.com
3. Endereço do servidor XMPP. Defina este campo se você quiser que essa Call Bridge use somente um servidor XMPP colocalizado, ou você não tiver um DNS configurado. O uso do servidor XMPP colocalizado reduz a latência.
4. Deixe este campo em branco para permitir que essa Call Bridge faça failover entre

servidores XMPP, isso requer que as entradas do DNS sejam configuradas.



Se você planeja usar o Domain Name Server (DNS) para se conectar entre Call Bridges e servidores XMPP, também precisa configurar um registro SRV do DNS para o cluster xmpp, a fim de resolver o registro de DNS A de cada um dos servidores XMPP no cluster. O formato do registro SRV DNS é: **_xmpp-components._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.
```

O exemplo acima especifica a **porta 5223(use outra porta, se 5223 já estiver sendo usada).**

o segredo compartilhado usado para a respectiva Call Bridge. Por exemplo, nas capturas de tela acima

O segredo Cb1 é

Callbridge: cb1

Domínio: tptac9.com

Segredo: **kvgP1SRzWVabhiPVAb1**

Da mesma forma para cb2 e cb3, repita essas etapas para todas as 3 Call Bridges **cb1, cb2 e cb3**.

Depois que você executa estas etapas, verifique o status do cluster em todos as três Call Bridges

Verificar

Execute **cb1>> xmpp cluster status**, esse comando para obter um relatório sobre o estado em tempo real do cluster xmpp. Se o cluster falhar, esse comando retorna as estatísticas do servidor xmpp, executado somente no Servidor do Meeting. Use esse comando para tentar diagnosticar problemas de conectividade e ajudar nesse processo.

Essa imagem mostra os nós, um como líder 10.106.81.30 e os dois restantes como Seguidores.

```
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
```

Da mesma forma, verifique o status nos dois nós restantes.

No segundo nó

```
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>
```

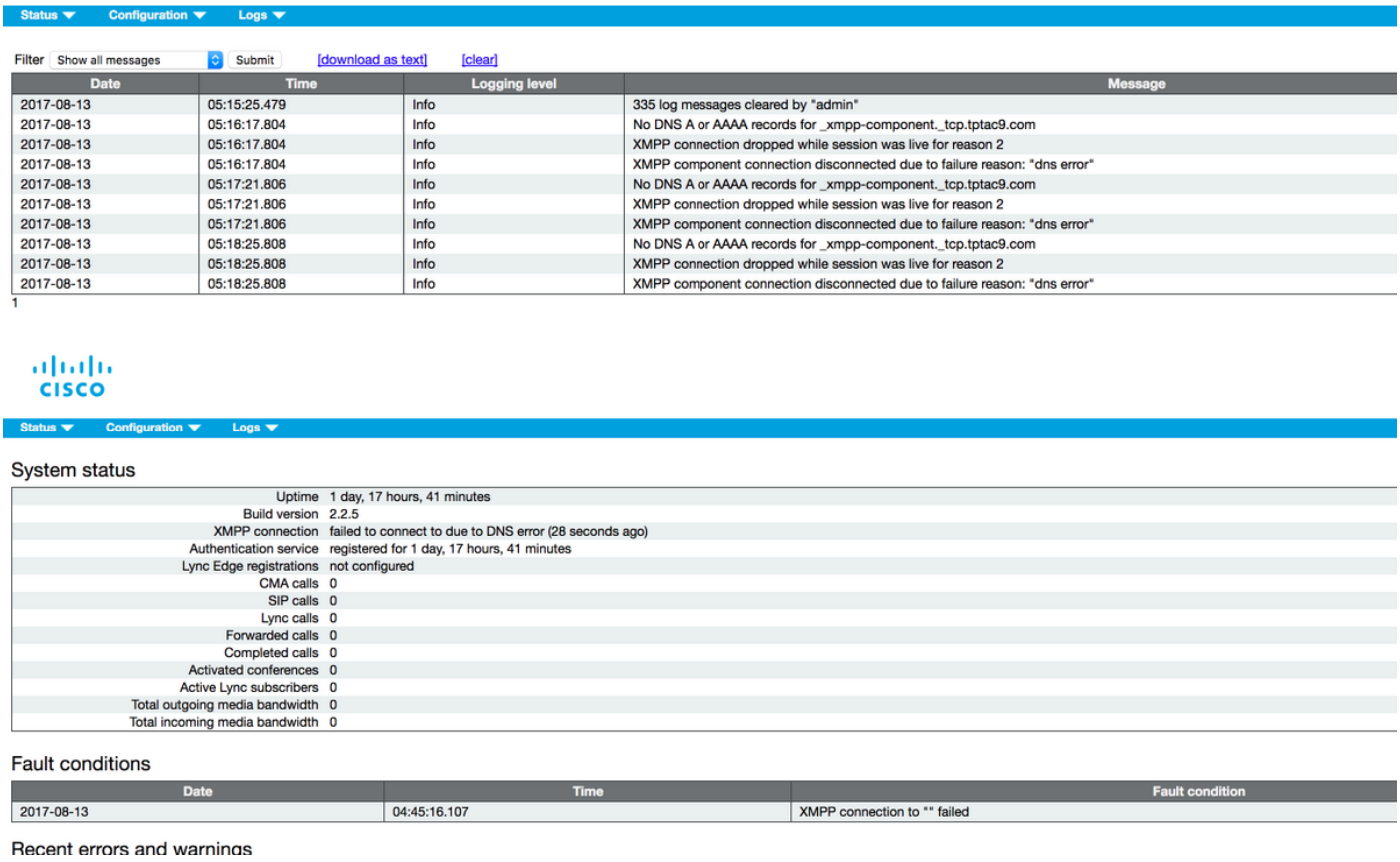
No terceiro nó

```
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
```

Troubleshoot

A resiliência XMPP foi configurada com êxito. Pode haver problemas ao usar a resiliência xmpp.

Cenário 1. Verificado se há configuração DNS, os erros nas capturas de tela apontam para problemas de 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 esses erros forem observados, verifique a configuração de registros SRV.

Na resiliência XMPP, o servidor XMPP conectado a uma Call Bridge é controlado por meio de DNS. Essa opção se baseia na prioridade do DNS e no peso dado. Uma Call Bridge apenas se conecta a um servidor XMPP por vez. Não há nenhuma exigência que todas as Call Bridges se

conectem ao mesmo servidor XMPP desde que todo o tráfego seja encaminhado para o mestre. Se houver um problema de rede na perda de conexão da Call Bridge para o servidor XMPP, a Call Bridge tenta se reconectar a outro servidor XMPP. A Call Bridge deve ser configurada para qualquer servidor XMPP ao qual possa se conectar.

Para ativar conexões de cliente, uso do cliente WebRTC, é necessário um registro **_xmpp-client._tcp .** Em uma implantação típica, ele é resolvido para a **porta 5222**. Dentro, a LAN, se o servidor do núcleo for roteável diretamente, poderá resolver para o serviço XMPP que é executado no servidor núcleo.

Por exemplo: **_xmpp-client._tcp.tptac9.com pode ter esses registros de SRV:**

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

conselho sobre como configurar registros de DNS para os nós do servidor XMPP. Para a resiliência de XMPP, você precisa usar o DNS para se conectar entre Call Bridges e servidores XMPP e também precisa configurar um registro SRV do DNS para o cluster xmpp, a fim de resolver o registro de DNS A de cada um dos servidores XMPP no cluster. O formato do registro SRV do DNS é: **_xmpp-component._tcp.tptac9.com**

De acordo com a configuração discutida para 3 servidores xmpp, o registro que resolve a todos os três servidores são mostrados

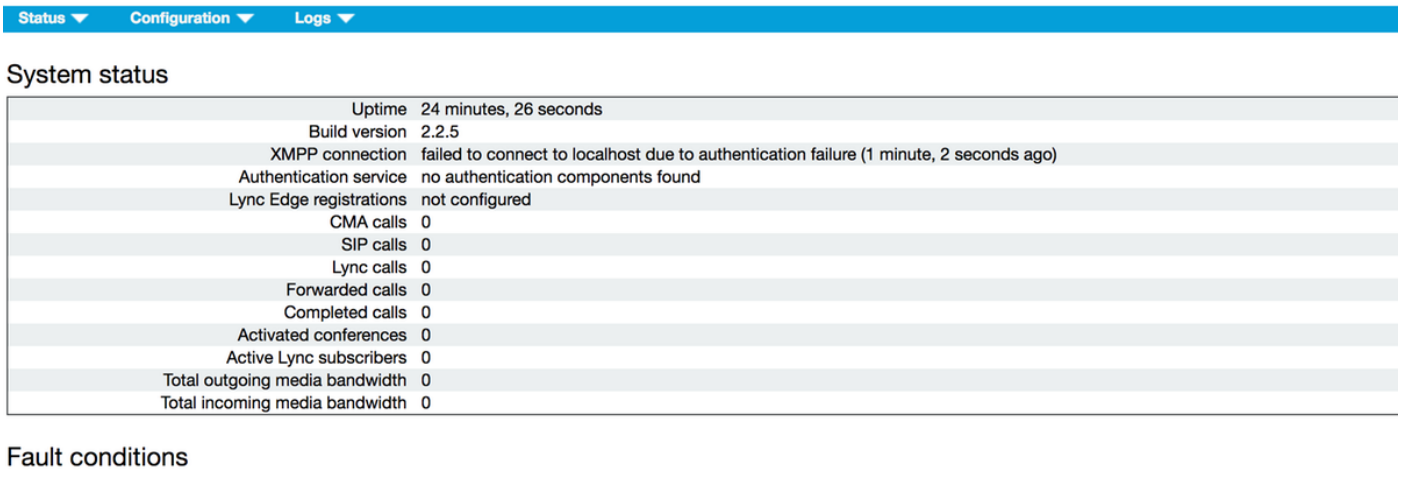
_xmpp-component._tcp.tptac9.com. 86400 IN SRV 0 0 5223 cb1.tptac9.com

_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

O exemplo especifica a porta 5223, mas qualquer outra porta pode ser usada se a 5223 já estiver sendo usada. No entanto, garanta que a porta esteja aberta.

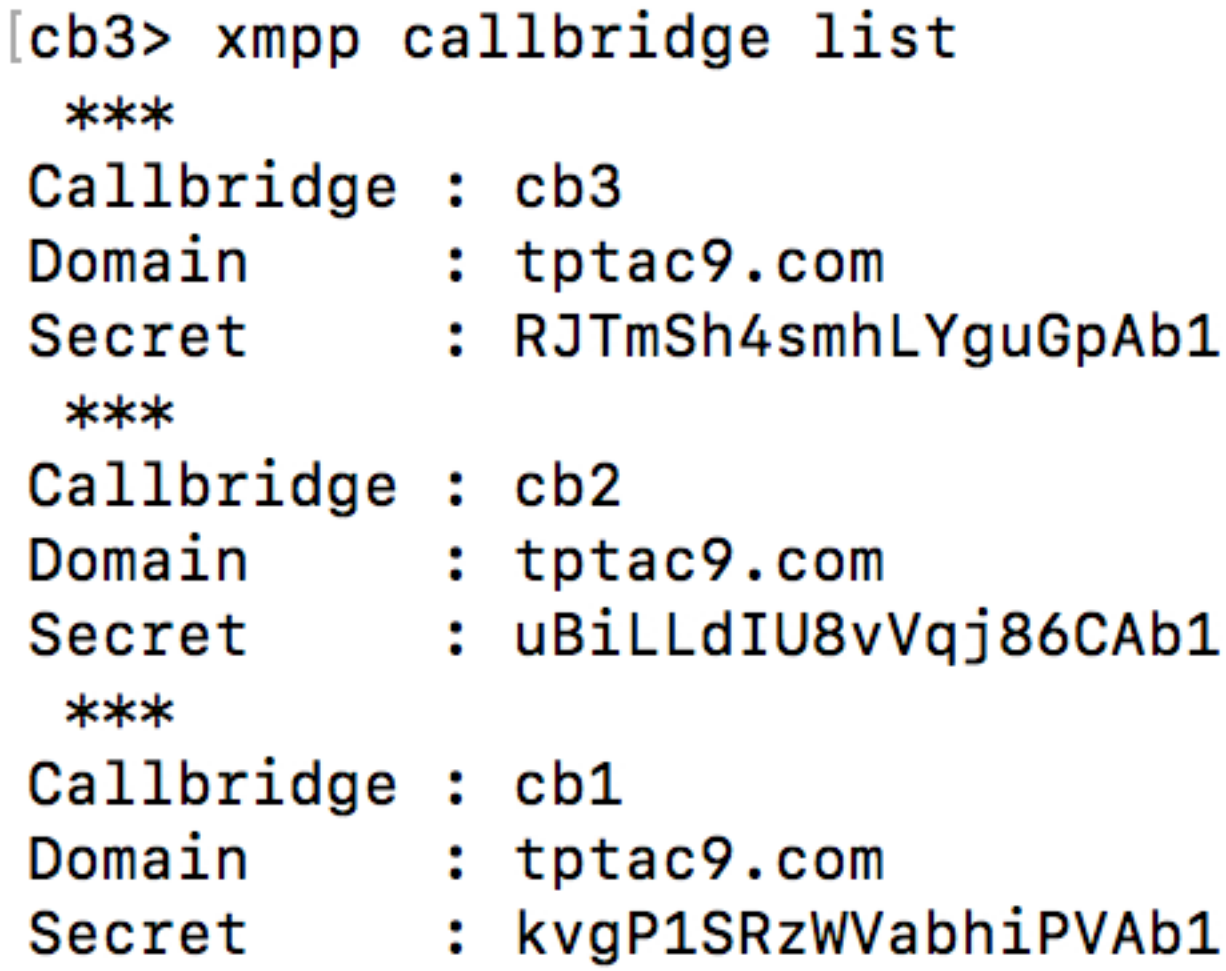
Cenário 2. Quando a página de status do CMS mostra **falha na autenticação.**



A **falha na autenticação é principalmente observada quando o segredo compartilhado não é inserido ou ele é inserido incorretamente.** Certifique-se de que o segredo compartilhado tenha sido inserido, se tiver esquecido e não tenha como lembrar. Faça SSH para o servidor e execute esse **comando: 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
```



O documento descreve a configuração de resiliência do xmpp. Portanto, execute o comando em todos os 3 servidores para garantir que os segredos gerados sejam iguais em todos os servidores. Como mostra a imagens, ele pode ser visto no servidor **cb1**, o segredo compartilhado usado é o mesmo que está sendo refletido para **cb3**. Depois de verificar em outros servidores, conclui-se que o segredo inserido para **cb1 está incorreto.**

Cenário 3. No status de cluster xmpp, **entradas duplicadas de nós XMPP.**

Essa saída mostra a entrada duplicada do nó **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)
```

> **Cuidado**: é recomendável remover os nós xmpp do cluster antes de redefini-los. Se a redefinição do XMPP é executada em um nó enquanto ele ainda está em cluster e, em seguida, ele se une novamente ao nó do cluster XMPP existente, ele cria uma entrada duplicada daquele nó quando o status é verificado por meio de status do cluster xmpp.

Isso pode causar problemas em uma configuração resiliente. Um defeito foi gerado

https://BST.cloudapps.Cisco.com/bugsearch/bug/CSCvi67717

Verifique a página 94 do guia abaixo

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