配置 XMPP 恢复能力

目录

简介

本文档介绍如何设置思科 Meeting Server (CMS) 上的可扩展消息传送和网真协议 (XMPP) 的恢复能力。

先决条件

要求

Cisco 建议您了解以下主题：

- 必须在XMPP恢复能力之前设置数据库群集。这是设置数据库群集的链接
https://www.cisco.com/c/en/us/support/docs/conferencing/meeting-server/210530-Configure-Cisco-Meeting-Server-Call-Brid.html

- CMS 上必须配置有 Callbridge 组件
- 思科建议您至少有 3 个 XMPP 节点再设置 XMPP 的恢复能力
- 当在“复原”模式下设置时，部署中的 XMPP 服务器都加载有相同的配置
- 对证书自签名、证书授权机构 (CA) 签名有一定的了解
- 必须使用域名服务器 (DNS)
- 需要本地证书授权机构或公共证书授权机构生成证书

注意：不建议在生产环境下使用自签名证书

使用的组件

本文档不限于特定的软件和硬件版本。

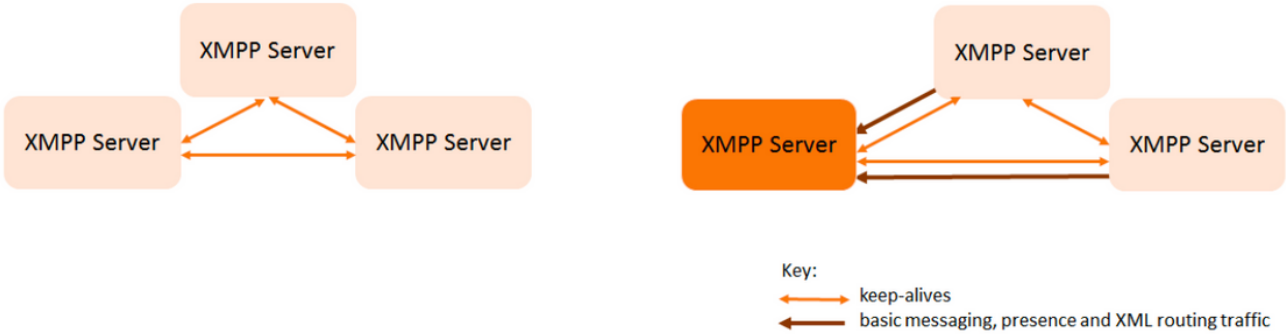
- CMS
- 主板管理处理器 (MMP) 的PuTTY 安全外壳 (SSH) 终端仿真软件
- Firefox 和 Chrome 等 Web 浏览器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图

下图显示 XMPP 消息交换和路由流量。



配置

此 XMPP 恢复能力部署示例使用三个 XMPP 服务器，并且是第一次进行配置。

注意：如果之前部署过 XMPP 恢复能力，则建议重置所有服务器。

XMPP 服务器使用保持连接消息彼此监听和选择主服务器。XMPP 消息可以发送到任何服务器。如上图所示，消息转发到 XMPP主服务器。XMPP 服务器继续彼此监听，如果主服务器发生故障，则选择一个新的主服务器，其他 XMPP 服务器会将流量转发到主服务器。

第 1 步： 为 XMPP 组件生成证书。

生成 CSR，然后使用此命令通过所需的本地证书授权机构/公共证书授权机构生成相应的证书

pki csr <密钥/证书基本名称>

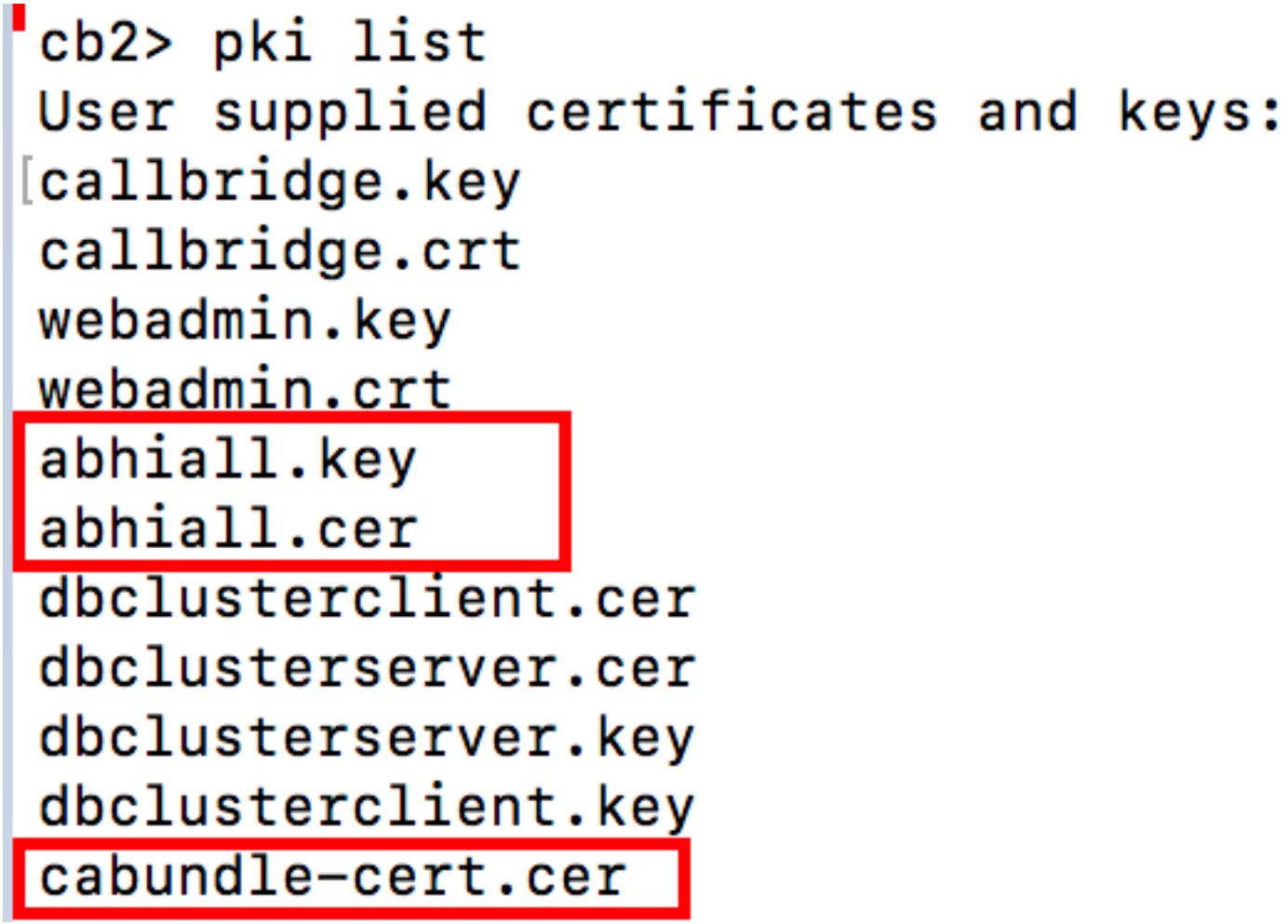
```
cb1> pki csr abhiall CN:tptac9.com subAltName:cb1.tptac9.com,cb2.tptac9.com,cb3
```

步骤2.使用上述CSR并使用本地证书颁发机构生成证书。您可以使用 VCS 证书指南通过 Microsoft 证书授权机构生成证书（ 第 32 页附录 5 ）

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

使用 WINSCP/SFTP 服务器将证书上传到所有 3 个节点。要检查是否已上传证书，在 MMP/SSH 上使用以下命令

指令：pki list



注意：在实验中，所有 3 个 XMPP 节点使用一个证书。

第 3 步： 配置 CMS 以使用 XMPP 组件。

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

*certall.cer= CA certificate
```

提示：如果CA提供证书捆绑包，则将捆绑包作为单独的文件包含到证书中。证书捆绑包是一个文件(扩展名为.pem、.cer或.crt)，其中包含根CA证书和链中所有中间证书的副本。证书捆绑包中的证书有一定的顺序，其中根 CA 证书位于最后。在设置安全连接时，外部客户端（例如 Web 浏览器和 XMPP 客户端）要求 XMPP 服务器分别提供证书和证书捆绑包。

当需要证书捆绑包时，上述命令将是

```
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
```

当 3 个各自的 XMPP 节点使用 3 个证书时，请确保捆绑证书

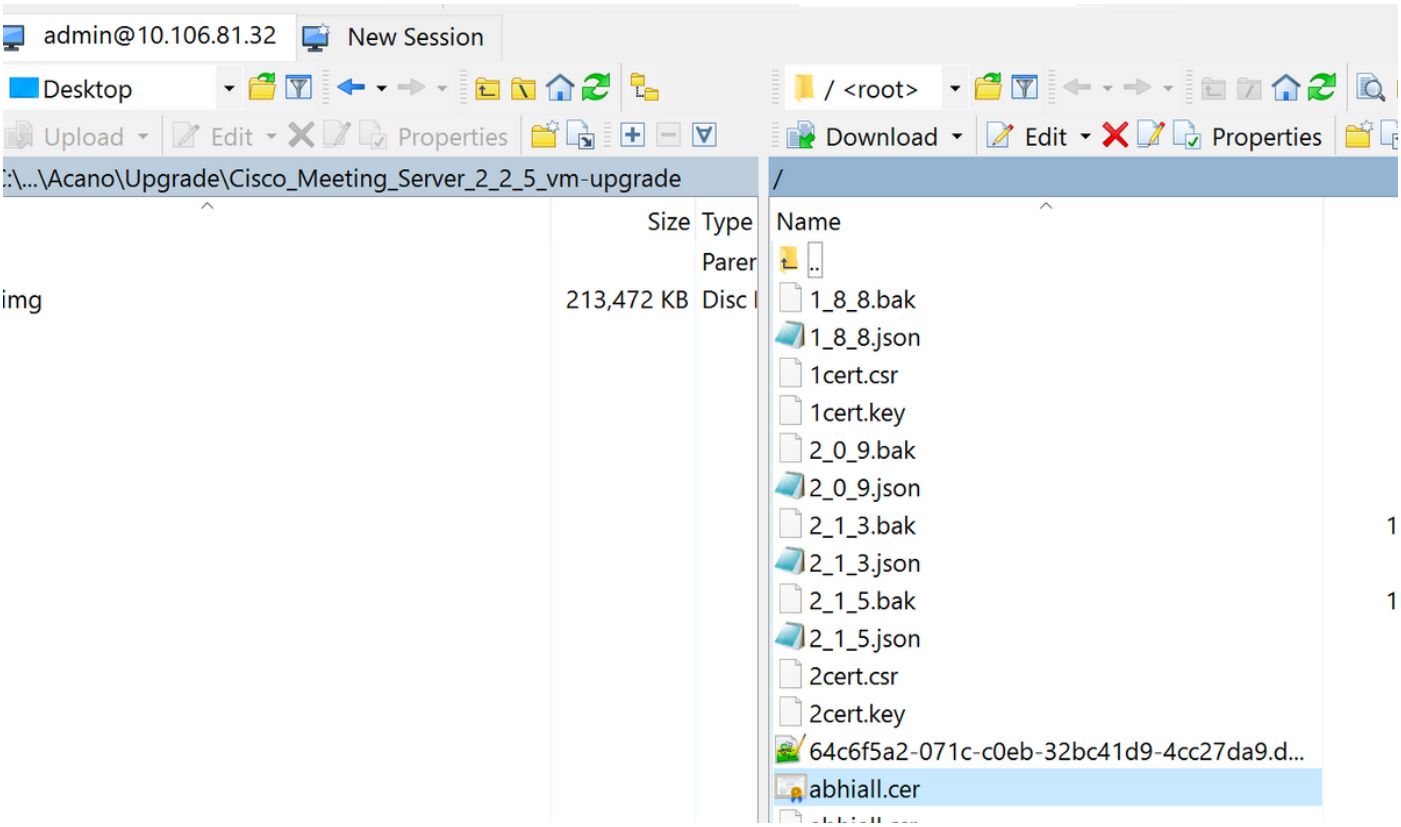
```
xmppserver1.crt + xmppserver2.crt + xmppserver3.crt= xmpp-cluster-bundle.crt
```

本文档中使用一个证书 **abhiall.cer**。

请参阅以下指南获取有关证书的详细信息

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

第 4 步： 通过 SFTP 的证书将证书上传至运行 XMPP 组件的所有 CMS。



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

在实验室中，XMPP 集群信任 **abhiall.cer**

cb1>>xmpp cluster trust abhiall.cer

第 5 步： 将呼叫网桥添加到 XMPP 服务器。

cb1> xmpp callbridge add cb1

生成密钥，这将配置 XMPP 服务器允许连接名为 **cb1 的呼叫网桥**。

> **注意：**生成域、呼叫网桥名称和密钥，您稍后会在配置呼叫网桥到 XMPP 服务器的访问权限（以便呼叫网桥向 XMPP 服务器提供身份验证详细信息）时需要此信息

上述命令用于向同一 XMPP 节点添加其他呼叫网桥。

cb1> xmpp callbridge add cb2

cb1> xmpp callbridge add cb3

> **注意**：每个呼叫网桥必须有**唯一名称**。如果您尚未几下添加到 XMPP 服务器的呼叫网桥的详细信息，请使用以下**命令：xmpp callbridge list**

cb1> xmpp disable

这将禁用 XMPP 服务器节点

第 6 步： 启用 XMPP 集群。

cb1> xmpp cluster enable

在此节点上初始化 XMPP 集群。此命令会创建 **1 个节点的 XMPP 集群**，其他节点（XMPP 服务器）加入此集群。

cb1> xmpp cluster initialize

重新启用此节点

cb1>xmpp enable

第 7 步： 将呼叫网桥添加到第二个 XMPP 节点并将其加入集群。

向此节点添加每个呼叫网桥。这要求使用第一个 XMPP 服务器节点提供的同一呼叫网桥名称和密钥添加呼叫网桥。使用以下命令可以实现上述操作：

cb2>> xmpp callbridge add-secret cb1

输入呼叫网桥的密钥

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

药查看密钥，请运行 xmpp call bridge list 命令。它会列出第一个节点上生成的所有密钥。

将所有呼叫网桥密钥添加到第二个节点后。

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

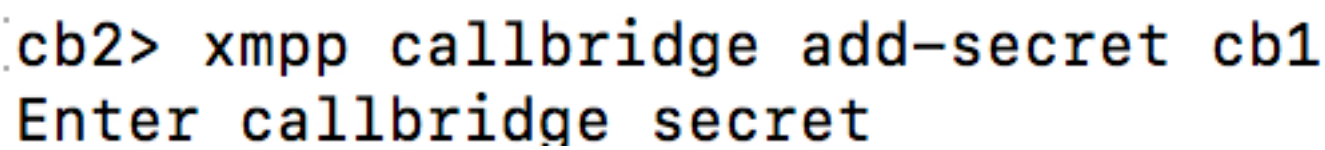
集群：是第一个节点的 IP 地址或域名

第 8 步： 将呼叫网桥添加到第三个 XMPP 节点并将其加入集群。

向此节点添加每个呼叫网桥。这要求使用第一个 XMPP 服务器节点提供的同一呼叫网桥名称和密钥添加呼叫网桥。使用以下命令可以实现上述操作：

cb3>> xmpp callbridge add-secret cb1

输入呼叫网桥的密钥



现在查看密钥。您可以运行 xmpp callbridge list 命令。此命令会列出第一个节点上生成的所有密钥。

```
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
```

将所有呼叫网桥密钥添加到此节点后执行以下步骤。

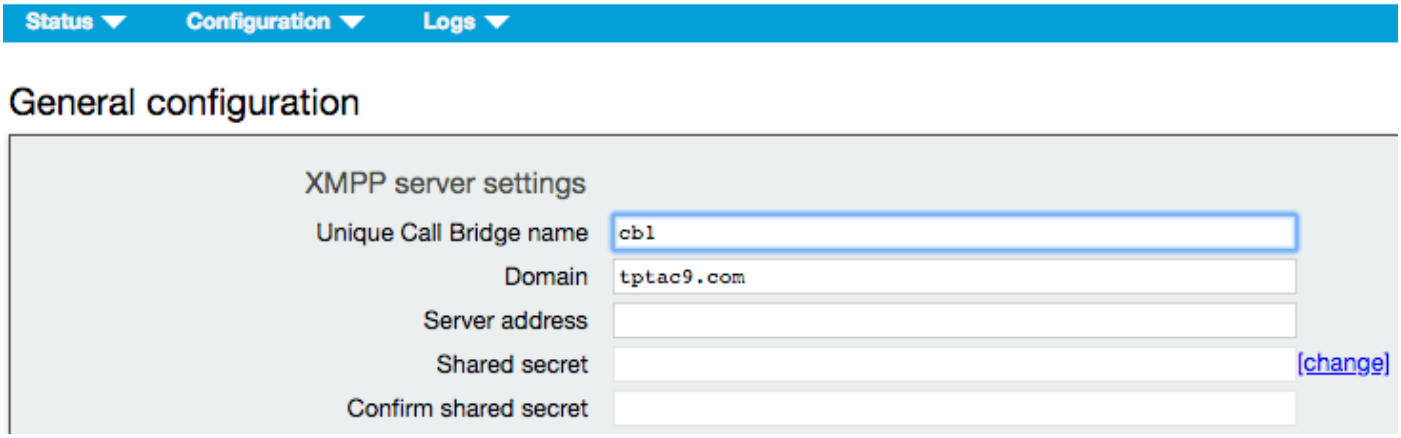
```
cb3>> xmpp disable
cb3>> xmpp cluster enable
cb3>> xmpp enable
cb3>> xmpp cluster join <cluster>
```

集群：是第一个节点的 IP 地址或域名

第 9 步： 使用集群中 XMPP 服务器的身份验证详细信息配置每个呼叫网桥。这可让呼叫网桥访问 XMPP 服务器。

导航至 **Webadmin > 配置 > 常规并输入以下信息**：

1. 添加唯一的呼叫网桥名称，不需要域名部分。
2. 输入 XMPP 服务器域的域名 tptac9.com
3. XMPP 服务器的服务器地址。如果您希望此呼叫网桥仅使用同一个位置的 XMPP 服务器，或者未配置 DNS，则设置此字段。使用同一位置的 XMPP 服务器可减少延迟。
4. 将此字段留空可让此呼叫网桥在 XMPP 服务器之间进行故障切换，这需要设置 DNS 条目。



如果您打算使用域名服务器 (DNS) 连接呼叫网桥和 XMPP 服务器，还需要为 XMPP 集群设置 DNS SRV 记录，以便解析到集群中每个 XMPP 服务器的 DNS A 记录。DNS SRV 记录的格式为：**_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.
```

上面的示例指定使用**端口 5223（如果已使用 5223，则使用其他端口）。**

各自呼叫网桥使用的共享密钥。例如，在上述屏幕截图中

Cb1 密钥为

Callbridge：cb1

域：tptac9.com

密钥：**kvgP1SRzWVabhiPVAb1**

cb2 和 cb3 与此类似，对于所有 3 个呼叫网桥 **cb1、cb2 和 cb3** 重复这些步骤。

执行这些步骤后，请在所有三个呼叫网桥上检查集群的状态

验证

运行 **cb1>> xmpp cluster status**，此命令可获取有关 XMPP 集群的实时状态。如果集群发生故障，此命令会返回 XMPP 服务器（仅运行在此 Meeting Server 上）的统计信息。使用此命令可尝试帮助诊断连接问题。

下图显示节点，一个是主节点 10.106.81.30，其他两个是从属节点。

```
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
```

同样，在其他两个节点上检查状态。

在第二个节点上

```
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>
```

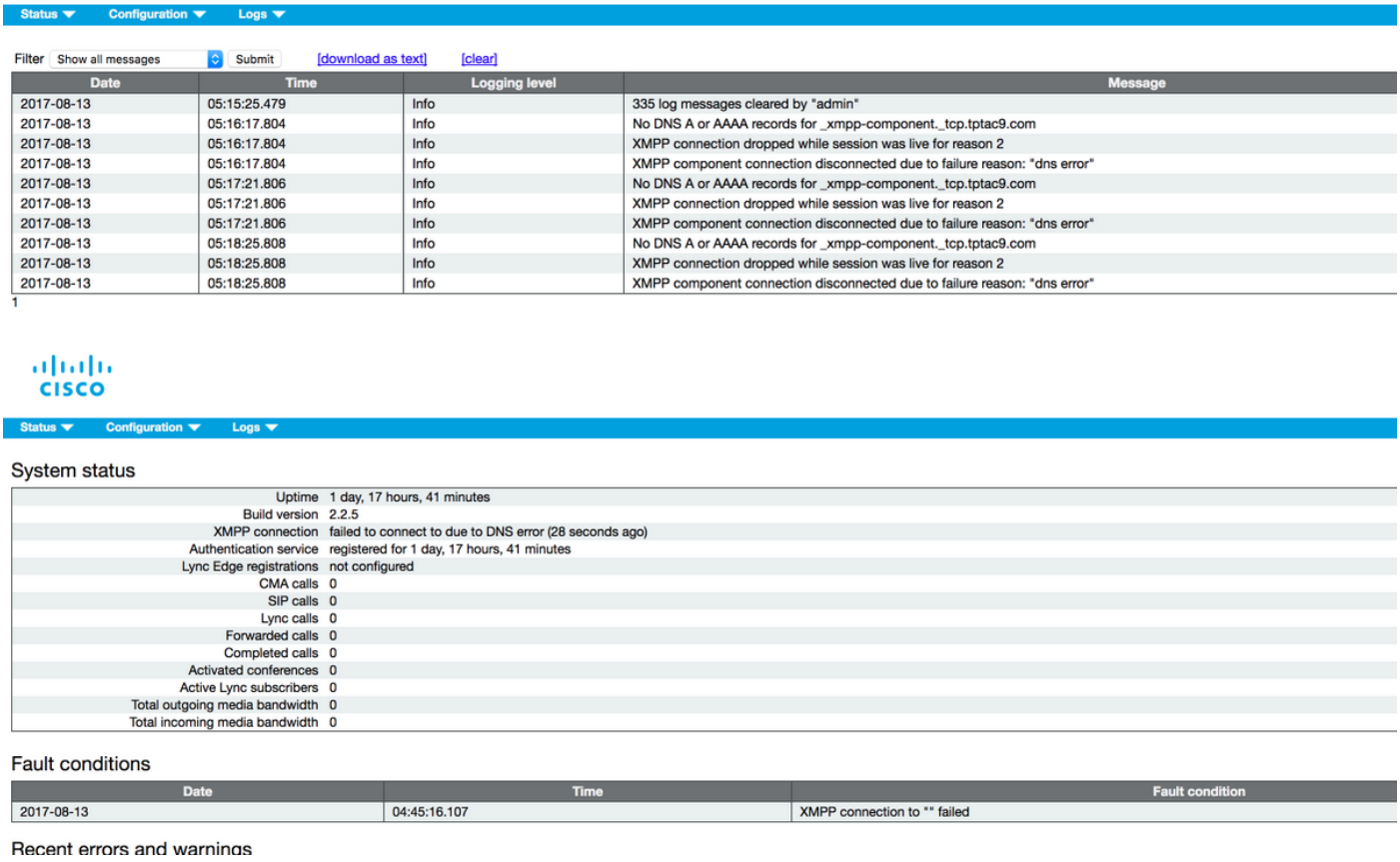
在第三个节点上

```
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
```

故障排除

XMPP 恢复能力已成功设置。使用 XMPP 恢复能力时可能会出现问题。

场景 1： 检查 DNS 配置，屏幕截图上的错误表示出现了 DNS 问题。



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

cisco

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

如果看到这些错误，请检查 SRV 记录的配置。

在 XMPP 恢复能力中，呼叫网桥连接的 XMPP 服务器通过 DNS 进行控制。此选项基于给定的 DNS 优先级和权重。呼叫网桥一次仅连接一台 XMPP 服务器。不要求所有呼叫网桥都连接到同一台 XMPP 服务器，因为所有流量都会转发到主服务器。如果某个网络问题导致呼叫网桥到 XMPP 服务器的连接中断，呼叫网桥会尝试重新连接到其他 XMPP 服务器。必须为可以连接呼叫网桥的任

何 XMPP 服务器配置呼叫网桥。

要启用客户端连接（使用 WebRTC 客户端），需要使用 **_xmpp-client._tcp 记录。**在典型部署中，其解析为**端口 5222**。在局域网内部，如果核心服务器可直接路由，则可解析为核心服务器上运行的 XMPP 服务。

例如：**_xmpp-client._tcp.tptac9.com 可以有以下 SRV 记录：**

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

有关为 XMPP 服务器节点设置 DNS 记录的建议。为了实现 XMPP 恢复能力，您需要使用 DNS 连接呼叫网桥和 XMPP 服务器，还需要为 XMPP 集群设置 DNS SRV 记录，以便解析到集群中每个 XMPP 服务器的 DNS A 记录。DNS SRV 记录的格式为：**_xmpp-component._tcp.tptac9.com**

根据针对 3 台 XMPP 服务器讨论的设置，可解析为所有三台服务器的记录如下所示

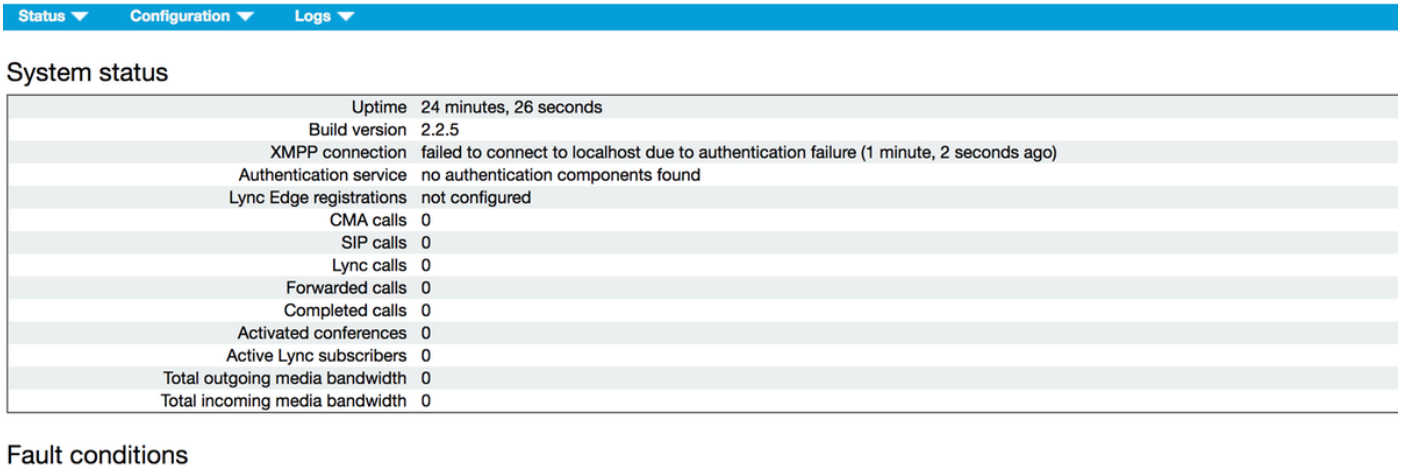
_xmpp-component._tcp.tptac9.com.86400 IN SRV 0 0 5223 cb1.tptac9.com

_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

在此示例中指定的端口是 5223，如果已在使用 5223，也可以使用任何其他端口。但是，请确保必须打开所使用的端口。

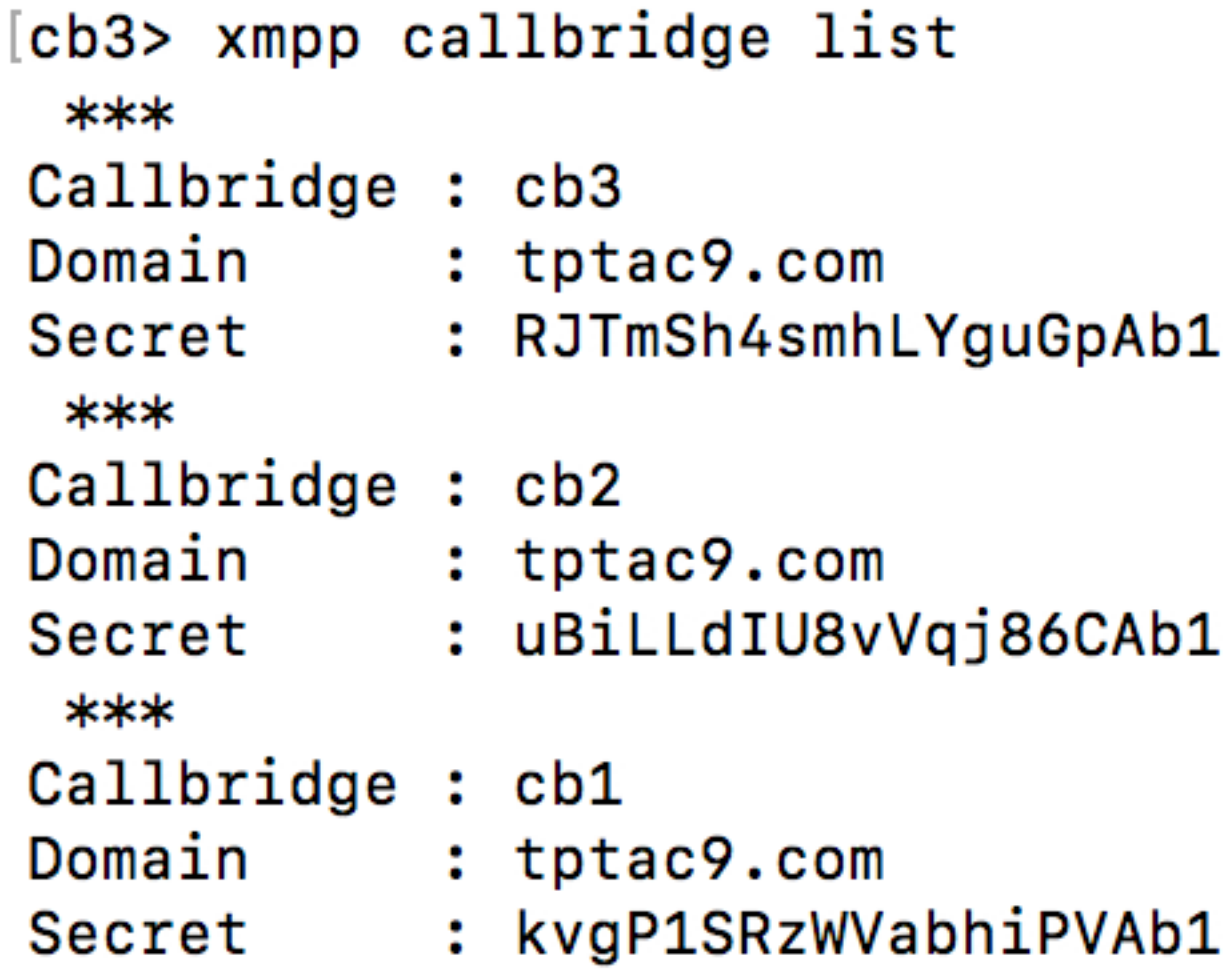
场景2.当CMS状态页显示身份验证**失败时。**



如果未输入共享密钥或输入不正确，我们通常会看到**身份验证失败。**请确保已输入共享密钥，如果忘记密钥或者不方便获取密钥，请使用 SSH 登录服务器，然后运行此**命令：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
```



本文档介绍 XMPP 恢复能力设置。因此，在所有 3 台服务器上运行命令，确保所有服务器上生成的密钥相同。如图所示，在服务器**cb1**上可以看到它，所使用的共享密钥与反映给**cb3**的共享密钥相同。在您检查其他服务器后，会断定为**cb1**输入的密钥不正确。

场景3.在XMPP节点的xmpp集**群状态**重复条目。

此输出显示节点 **10.61.7.91:5222 的重复条目**

```
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**：建议在重置xmpp节点之前从群集中删除这些节点。如果在仍位于集群中的节点上执行 XMPP 重置，然后将节点重新加入到现有 XMPP 集群中，那么当通过 XMPP 集群状态检查状态时，就会创建此节点的重复条目。

这样会导致恢复能力设置出现问题。发现缺陷

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

请查看以下指南的第 94 页

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