

Configurar o cluster do banco de dados da Call Bridge do Cisco Meeting Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Parte 1. Criação de certificado](#)

[Parte 2. Configuração do Call Bridge](#)

[Diagrama de Rede](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas para configurar o clustering do banco de dados (DB) no Cisco Meeting Server (CMS) ou nas pontes de chamada do Acano (CB).

Prerequisites

Requirements

- A Cisco recomenda que você tenha pelo menos 3 nós CMS para criar um cluster de DB viável

Note: É recomendável ter um número ímpar de nós de cluster de banco de dados, pois é importante para a seleção mestre e o mecanismo de failover ativo. Outra razão para isso é que o nó mestre de banco de dados seria o nó que tem conexões com a maioria do banco de dados no cluster. Você pode ter um máximo de 5 nós em um cluster DB.

- Porta 5432 aberta no firewall

Observação: o mestre do cluster de banco de dados escuta na porta 5432 conexões dos nós do cliente, portanto, se houver um firewall (FW) entre os nós, certifique-se de que essa porta esteja aberta.

Componentes Utilizados

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

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Há dois tipos de certificados para o cluster DB:

1. Cliente: O certificado do cliente, como o nome sugere, é usado pelos clientes DB para se conectar ao servidor DB (Master). Este certificado deve conter a sequência de caracteres, pôsteres, no campo Nome Comum (CN).
2. Servidor: O certificado do servidor, como o nome sugere, é usado pelo servidor DB para se conectar ao DB do postgres.

Parte 1. Criação de certificado

1. Conecte-se com um Shell Seguro (SSH) com as credenciais de administrador ao MMP do servidor.
2. Gerar solicitação de assinatura de certificado (CSR):

a. Para o certificado de cliente de cluster de banco de dados:

```
pki csr <key/cert basename> CN:postgres
```

Por exemplo: **pki csr databasecluster_client CN:postgres**

b. Para o certificado do servidor de cluster de banco de dados:

```
pki csr <key/cert basename> CN:<domainname>
```

Por exemplo: **pki csr databasecluster_server CN:vngtpres.aca**

3. Envie os CSRs à autoridade de certificação (CA) para que eles sejam assinados. Certifique-se de que a AC fornece a você os certificados CA raiz (e qualquer CA intermediária).
4. Carregue os certificados assinados, os certificados CA raiz (e qualquer CA intermediária) em todos os nós DB usando um cliente SFTP (Secure File Transfer Protocol) (por exemplo, WinSCP).

Note: O CN da parte A deve ser de pôsteres e a parte B pode ser o nome de domínio da ponte de chamada, não são necessárias entradas de nome alternativo de assunto (SAN).

Parte 2. Configuração do Call Bridge

No BC que executa o BD mestre, siga estas etapas:

1. Para selecionar a interface a ser usada, digite o comando:

nó local do cluster de banco de dados a

Isso permite que a interface "a" seja usada para o agrupamento de DB.

2. Defina os certificados cliente, servidor e raiz ca, bem como as chaves privadas a serem usadas pelo cluster DB com estes comandos:

```
database cluster certs <client_key> <client_crt> <ca_crt>
```

```
database cluster certs <server_key> <server_crt> <client_key> <client_crt> <ca_crt>
```

Note: Os mesmos certificados de cliente e servidor podem ser usados em outros nós CB para serem agrupados quando você copia as chaves privadas e os certificados para os outros nós. Isso é possível porque os certificados não contêm SAN vinculando-os a uma ponte de chamada específica. No entanto, é recomendável ter certificados individuais para cada nó DB.

3. Inicialize este banco de dados no CB local como mestre para este cluster de banco de dados:

inicialização do cluster de banco de dados

4. Nas CallBridges que seriam parte do banco de dados clusterizado e se tornariam os escravos do banco de dados, execute este comando depois de concluir as Etapas 1 e 2 para a Parte 2:

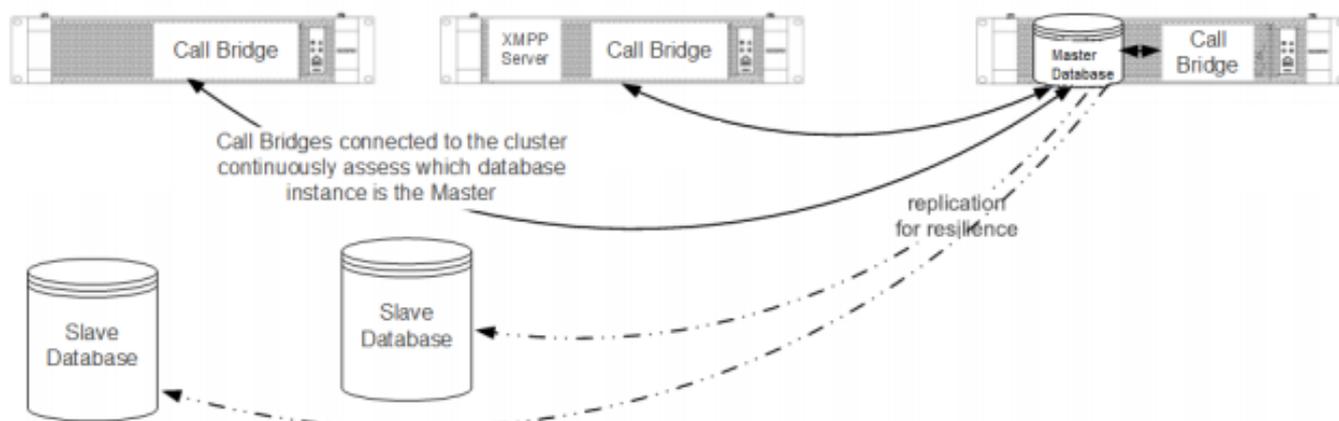
associação do cluster de banco de dados <endereço IP do CB mestre>

Por exemplo: **associação de cluster de banco de dados <10.48.36.61>**

Isso inicia a sincronização do banco de dados e copia o banco de dados do peer mestre.

Note: O banco de dados local que existia antes do início do comando de **união de cluster de banco de dados**, continua a existir até que o nó seja removido do banco de dados clusterizado. Enquanto o nó estiver no cluster DB, seu DB local não será usado.

Diagrama de Rede



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para verificar o status do banco de dados clusterizado, execute este comando em qualquer um dos nós no cluster DB:

status de cluster de banco de dados

A saída é semelhante a:

```
Status                : Enabled
Nodes:
  10.48.36.61          : Connected Master
  10.48.36.118         : Connected Slave ( In Sync )
  10.48.36.182 (me)    : Connected Slave ( In Sync )
Node in use           : 10.48.36.61

Interface              : a

Certificates
Server Key              : dbclusterserver.key
Server Certificate      : dbclusterserver.cer
Client Key              : dbclusterclient.key
Client Certificate      : dbclusterclient.cer
CA Certificate          : vngtpRootca.cer
Last command           : 'database cluster join 10.48.36.61' (Success)
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Use este comando, na CLI, para exibir os logs atuais relacionados ao cluster de BD:

syslog siga

As saídas de log do DB geralmente contêm a string de postgres, exemplos como a seguir:

```
Mar 30 12:39:04 local0.warning DBMaster postgres[20882]: [2-7] #011SQL statement "INSERT INTO
domains(domain_id, domain_name, tenant_id, target, priority, passcode_separator) VALUES
(inp_domain_id, inp_domain_name, inp_tenant_id, existing_target, inp_priority,
inp_passcode_separator)"
Mar 30 12:39:04 local0.warning DBMaster postgres[20882]: [2-8] #011PL/pgSQL function
create_or_update_matching_domain(boolean,uuid,text,boolean,uuid,integer,integer,integer,text)
line 61 at SQL statement
Mar 30 12:39:04 local0.warning DBMaster postgres[20882]: [2-9] #011SQL statement "SELECT * FROM
create_or_update_matching_domain(TRUE, inp_domain_id, inp_domain_name, TRUE, inp_tenant_id,
inp_target_true, 0, inp_priority, inp_passcode_separator)"
Mar 30 12:39:04 local0.warning DBMaster postgres[20882]: [2-10] #011PL/pgSQL function
create_matching_domain(uuid,text,uuid,integer,integer,text) line 3 at SQL statement
```

O [coletor de registros CMS](#) oferece uma interface de usuário (UI) fácil e fácil de usar para coletar registros do servidor CMS.

Aqui estão alguns problemas típicos de BD e soluções:

Problema: Erro de esquema de BD em um peer não mestre

```
ERROR          : Couldn't upgrade the schema
Status         : Error

Nodes:
  10.48.54.75   : Connected Master
  10.48.54.76   : Connected Slave ( In Sync )
  10.48.54.119 (me) : Connected Slave ( In Sync )
Node in use    : 10.48.54.75

Interface      : a

Certificates
  Server Key       : dbclusterServer.key
  Server Certificate : dbserver.cer
  Client Key       : dbclusterClient.key
  Client Certificate : dbclient.cer
  CA Certificate    : Root.cer

Last command    : 'database cluster upgrade_schema' (Failed)
```

Solução:

1. Primeiro, execute este comando para limpar o erro:

erro de limpeza de cluster de banco de dados

2. Seguido por este comando para atualizar o esquema DB:

database cluster upgrade_schema

3. Em seguida, verifique o status do cluster de BD com:

status de cluster de banco de dados

Os registros mostram uma saída semelhante a esta:

```
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: Upgrading schema with connect line
'connect_timeout=4 user=postgres host=127.0.0.1 port=9899 sslmode=verify-ca
sslcert=/srv/pgsql/client.crt sslkey=/srv/pgsql/client.key sslrootcert=/srv/pgsql/ca.crt '

Mar 30 11:22:45 user.notice acanosrv05 schema_builder: Using database name 'cluster'
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: schema build on database cluster
complete
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: Using CiscoSSL 1.0.1u.4.13.322-fips
(caps 0x4FABFFFF)
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: Using 0x1000115F
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: INFO      : Waiting for database cluster
to settle...
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: INFO      : Database cluster settled
Mar 30 11:22:45 user.notice acanosrv05 schema_builder: Schema upgrade complete
Mar 30 11:22:45 user.info acanosrv05 dbcluster_watcher: Operation Complete
```

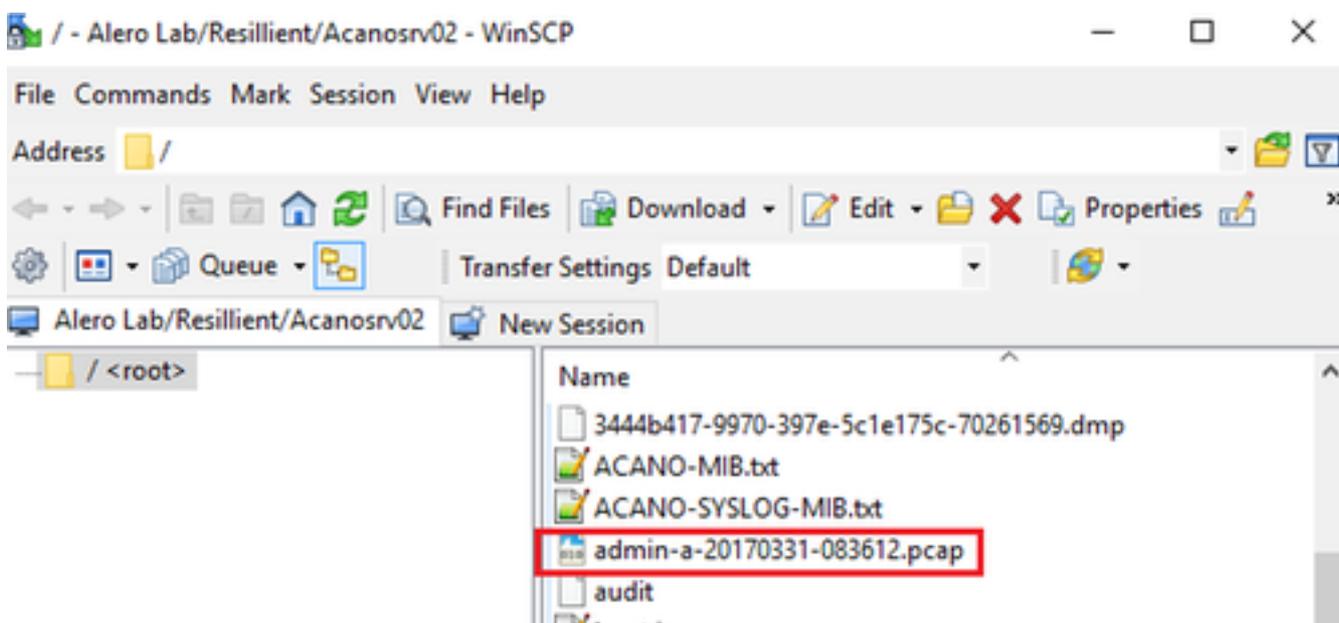
Problema: Os nós de peer não podem se conectar ao nó mestre de DB

```
Mar 31 10:16:59 user.info acanosrv02 sfpool: Health check 10.48.54.119: error (up = 1): could
not connect to server: Connection refused|#011Is the server running on host "10.48.54.119" and
accepting|#011TCP/IP connections on port 5432?|
```

Solução:

Siga estes passos para coletar rastreamentos para solucionar problemas de conexão:

1. Execute o comando **pcap <interface>** no nó não-mestre (escravo) e, após alguns minutos, pare a captura com **Ctrl-C**.
2. Conecte-se com um cliente Secure File Transfer Protocol (SFTP) ao servidor e faça o download do arquivo **.pcap** do diretório raiz:



3. Abra o arquivo de captura no Wireshark e filtre na porta 5432 com **tcp.port==5432** para verificar o tráfego entre o peer não mestre e o mestre de DB.

4. Se não houver tráfego de retorno do servidor, é provável que um FW esteja bloqueando a porta entre o local lógico dos dois servidores.

Aqui está uma captura típica de pacotes de uma conexão em funcionamento entre o cliente e o servidor:

Neste exemplo, o IP do cliente é 10.48.54.119 e o servidor é 10.48.54.75.

The screenshot shows a Wireshark capture of network traffic filtered by 'tcp.port==5432'. The capture shows a sequence of packets related to a TLS handshake. The first packet is a SYN from the client to the server. The second packet is a SYN, ACK from the server to the client. The third packet is an ACK from the client to the server. The fourth packet is a Client Hello from the client to the server. The fifth packet is a Server Hello, Certificate, Certificate Request, Server Hello Done from the server to the client. The sixth packet is an ACK from the client to the server. The seventh packet is a Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message from the server to the client. The eighth packet is a New Session Ticket, Change Cipher Spec, Encrypted Handshake Message from the server to the client. The ninth packet is an ACK from the client to the server. The tenth packet is Application Data from the client to the server. The eleventh packet is Application Data from the server to the client. The twelfth packet is Application Data from the client to the server.

No.	Time	Source	Destination	Protocol	Length	Info
54	2017-03-31 08:36:13.558867	10.48.54.119	10.48.54.75	TCP	66	35826 → 5432 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
55	2017-03-31 08:36:13.558976	10.48.54.75	10.48.54.119	TCP	66	5432 → 35826 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
56	2017-03-31 08:36:13.559098	10.48.54.119	10.48.54.75	TCP	60	35826 → 5432 [ACK] Seq=1 Ack=1 Win=29312 Len=0
57	2017-03-31 08:36:13.559147	10.48.54.119	10.48.54.75	PGSQL	62	>
58	2017-03-31 08:36:13.559169	10.48.54.75	10.48.54.119	TCP	54	5432 → 35826 [ACK] Seq=1 Ack=9 Win=29312 Len=0
59	2017-03-31 08:36:13.559710	10.48.54.75	10.48.54.119	PGSQL	55	<
60	2017-03-31 08:36:13.559798	10.48.54.119	10.48.54.75	TCP	60	35826 → 5432 [ACK] Seq=9 Ack=2 Win=29312 Len=0
61	2017-03-31 08:36:13.560499	10.48.54.119	10.48.54.75	TLSv1.2	257	Client Hello
62	2017-03-31 08:36:13.560963	10.48.54.75	10.48.54.119	TLSv1.2	2605	Server Hello, Certificate, Certificate Request, Server Hello Done
63	2017-03-31 08:36:13.561060	10.48.54.119	10.48.54.75	TCP	60	35826 → 5432 [ACK] Seq=212 Ack=2553 Win=34304 Len=0
64	2017-03-31 08:36:13.564761	10.48.54.119	10.48.54.75	TLSv1.2	2983	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
65	2017-03-31 08:36:13.564810	10.48.54.75	10.48.54.119	TLSv1.2	54	5432 → 35826 [ACK] Seq=2553 Ack=3141 Win=36224 Len=0
66	2017-03-31 08:36:13.568036	10.48.54.75	10.48.54.119	TLSv1.2	1688	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
67	2017-03-31 08:36:13.568194	10.48.54.119	10.48.54.75	TCP	60	35826 → 5432 [ACK] Seq=3141 Ack=4187 Win=37632 Len=0
68	2017-03-31 08:36:13.568551	10.48.54.119	10.48.54.75	TLSv1.2	124	Application Data
69	2017-03-31 08:36:13.570438	10.48.54.75	10.48.54.119	TLSv1.2	406	Application Data
70	2017-03-31 08:36:13.571070	10.48.54.119	10.48.54.75	TLSv1.2	120	Application Data
71	2017-03-31 08:36:13.571330	10.48.54.75	10.48.54.119	TLSv1.2	382	Application Data

Informações Relacionadas

Para obter mais informações sobre como solucionar problemas e outras perguntas sobre clustering de bancos de dados, consulte as Perguntas frequentes nestes links:

- [Quando agrupar servidores de banco de dados, por que preciso colocá-los em locais diferentes?](#)
- [Temos um cluster de banco de dados e vejo um erro ou aviso de banco de dados no log. O que devo fazer](#)
- [Um ou mais servidores de banco de dados não estão conectados ou no estado "Sincronizar". O que devo fazer](#)
- [O que faço se não houver um banco de dados mestre?](#)
- [Como faço para mover o banco de dados mestre](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)