

Konfigurieren des Cisco Meeting Server Call Bridge-Datenbank-Clusters

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Teil 1: Zertifikaterstellung](#)

[Teil 2. Konfiguration der Anrufbrücke](#)

[Netzwerkdiagramm](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Schritte zum Konfigurieren des DB-Clustering (DB) auf Cisco Meeting Server (CMS) oder Acano Call Bridges (CB) beschrieben.

Voraussetzungen

Anforderungen

- Cisco empfiehlt, dass Sie über mindestens 3 CMS-Knoten verfügen, um einen funktionsfähigen DB-Cluster erstellen zu können.

Hinweis: Es wird empfohlen, eine ungerade Anzahl von DB-Cluster-Knoten zu verwenden, da dies für die Master-Auswahl und den aktiven Failover-Mechanismus wichtig ist. Ein weiterer Grund hierfür ist, dass der Master-DB-Knoten der Knoten ist, der Verbindungen zu den meisten DB-Knoten im Cluster aufweist. Es können maximal 5 Knoten in einem DB-Cluster vorhanden sein.

- Port 5432 auf Firewall geöffnet

Hinweis: Der DB-Cluster-Master überwacht Port 5432 auf Verbindungen von den Client-Knoten. Wenn also eine Firewall (FW) zwischen den Knoten vorhanden ist, stellen Sie sicher, dass dieser Port geöffnet wird.

Verwendete Komponenten

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

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

Es gibt zwei Arten von Zertifikaten für das DB-Clustering:

1. Kunde: Das Clientzertifikat als Name suggest wird von den DB-Clients für die Verbindung mit dem DB-Server (Master) verwendet. Dieses Zertifikat muss die Zeichenfolge postgres in seinem Feld Common Name (CN) enthalten.
2. Server: Das Serverzertifikat als Name suggest wird vom DB-Server für die Verbindung mit der Postgres-DB verwendet.

Teil 1: Zertifikaterstellung

1. Stellen Sie eine Verbindung mit einer Secure Shell (SSH) mit den Admin-Anmeldeinformationen für den Server-MMP her.
2. Zertifikatsanforderung (Certificate Signing Request, CSR) erstellen:

a) Für das Datenbankecluster-Clientzertifikat:

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

Beispiel: `pki csr datenbank ecluster_client CN:postgres`

b) Für das Datenbankecluster-Serverzertifikat:

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

Beispiel: `pki csr datenbank ecluster_server CN:vngtpres.aca`

3. Senden Sie die CSRs an Ihre Zertifizierungsstelle (Certificate Authority, CA), um sie signieren zu lassen. Stellen Sie sicher, dass die CA Ihnen die Root-Zertifizierungsstellenzertifikate (und alle dazwischenliegenden Zertifizierungsstellenzertifikate) bereitstellt.
4. Laden Sie die signierten Zertifikate, die Root-Zertifizierungsstelle (und alle dazwischenliegenden Zertifizierungsstellen) mithilfe eines SFTP-Clients (z. B. WinSCP) auf alle DB-Knoten hoch.

Hinweis: Die CN für Teil A muss Postgres sein, und Teil B kann der Domänenname der Anrufbrücke sein. Einträge für Betreffalternativen Namen (SAN) sind nicht erforderlich.

Teil 2. Konfiguration der Anrufbrücke

Führen Sie auf der CB-Karte, die die Master-DB ausführt, die folgenden Schritte aus:

1. Um die zu verwendende Schnittstelle auszuwählen, geben Sie den Befehl ein:

Datenbank Cluster localnode a

Dadurch kann Schnittstelle "a" für das DB-Clustering verwendet werden.

2. Definieren Sie die Client-, Server- und Root-CA-Zertifikate sowie die privaten Schlüssel, die vom DB-Cluster mit den folgenden Befehlen verwendet werden:

Datenbank-Cluster-Zertifikate <client_key> <client_crt> <ca_crt>

Datenbank-Cluster-Zertifikate <server_key> <server_crt> <client_key> <client_crt> <ca_crt>

Hinweis: Dieselben Client- und Serverzertifikate können für andere CB-Knoten in Clustern verwendet werden, wenn Sie die privaten Schlüssel und Zertifikate über die anderen Knoten kopieren. Dies ist möglich, da die Zertifikate keine SAN-Verbindung mit einer bestimmten Anrufbrücke enthalten. Es wird jedoch empfohlen, für jeden DB-Knoten individuelle Zertifikate zu besitzen.

3. Initialisieren Sie diese DB auf der lokalen Zentralbank als Master für diesen DB-Cluster:

Datenbank-Cluster initialisieren

4. Führen Sie auf den CallBridges, die Teil der geclusterten DB wären und die DB-Slaves werden, diesen Befehl aus, nachdem Sie die Schritte 1 und 2 für Teil 2 abgeschlossen haben:

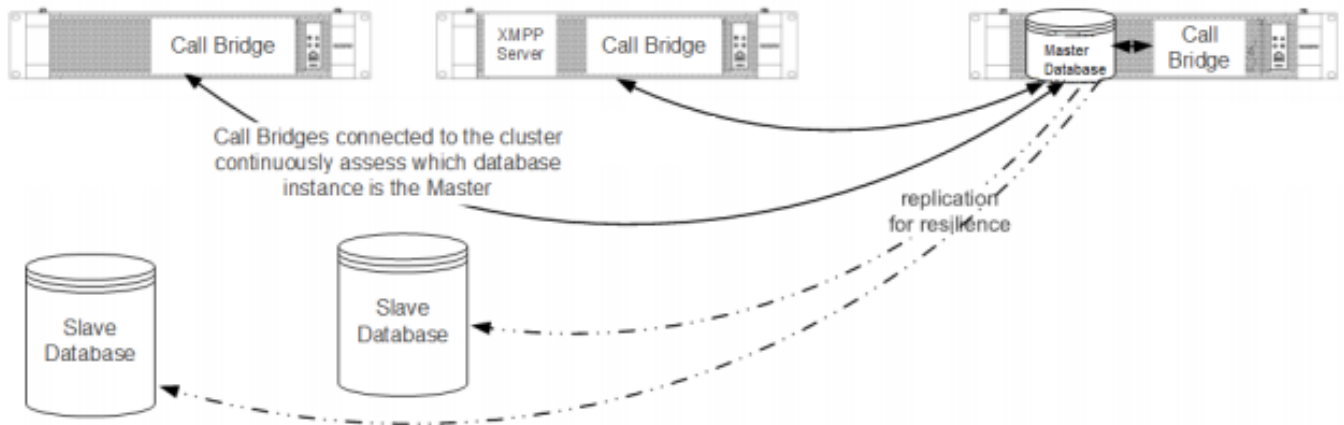
Datenbank-Cluster-Verbindung <IP-Adresse der Master-Zentralbank>

Beispiel: **database cluster join <10.48.36.61>**

Dadurch wird die DB-Synchronisierung initiiert und die DB vom Master-Peer kopiert.

Hinweis: Die lokale DB, die existierte, bevor der Befehl **Datenbankcluster join** initiiert wurde, existiert weiter, bis der Knoten aus der geclusterten DB entfernt wird. Solange sich der Knoten im DB-Cluster befindet, wird seine lokale DB nicht verwendet.

Netzwerkdiagramm



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um den Cluster-DB-Status zu überprüfen, führen Sie diesen Befehl für einen der Knoten im DB-Cluster aus:

Datenbankclusterstatus

Die Ausgabe ähnelt:

```
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)
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Verwenden Sie diesen Befehl in der CLI, um die aktuellen Protokolle zum DB-Clustering anzuzeigen:

Syslog folgen

Protokollausgaben für die DB enthalten in der Regel die Postgre-Zeichenfolge, z. B.:

```
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
```

Der [CMS-Protokollsammler](#) bietet eine einfache und benutzerfreundliche Benutzeroberfläche zum Erfassen von Protokollen vom CMS-Server.

Hier einige typische DB-Probleme und -Lösungen:

Problem: DB-Schemafehler auf einem Nicht-Master-Peer

```
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)
```

Lösung:

1. Führen Sie zuerst diesen Befehl aus, um den Fehler zu beheben:

Datenbankclusterklarer Fehler

2. Mit diesem Befehl wird das DB-Schema aktualisiert:

Datenbankcluster-Upgrade_schema

3. Überprüfen Sie anschließend den Status des DB-Clustering mit:

Datenbankclusterstatus

Die Protokollausgabe ähnelt der folgenden:

```
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
```

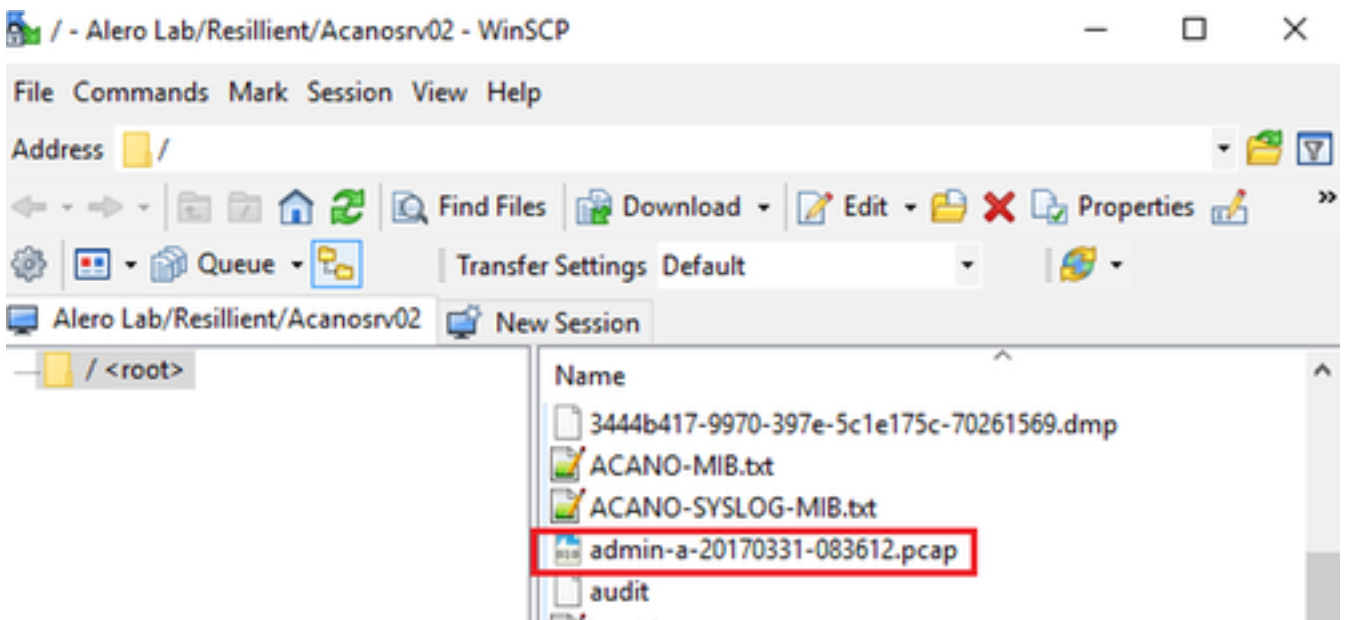
Problem: Peer-Knoten können keine Verbindung zum DB-Master-Knoten herstellen

```
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?|
```

Lösung:

Verwenden Sie diese Schritte, um Ablaufverfolgungen zu erfassen, um Verbindungsprobleme zu beheben:

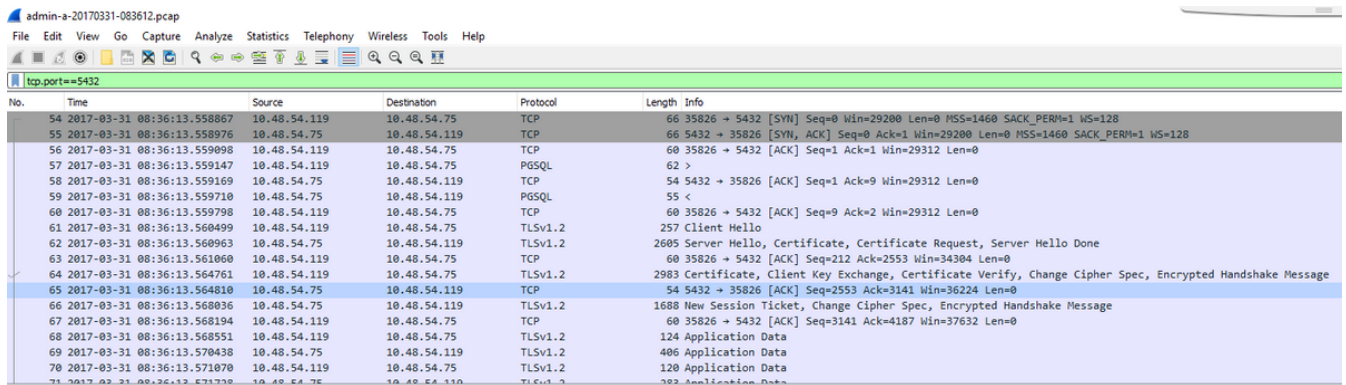
1. Führen Sie den Befehl `pcap <interface>` auf dem Nicht-Master-Knoten (Slave) aus, und beenden Sie die Erfassung nach einigen Minuten mit **Strg-C**.
2. Stellen Sie eine Verbindung mit einem SFTP-Client (Secure File Transfer Protocol) zum Server her, und laden Sie die `.pcap`-Datei aus dem Stammverzeichnis herunter:



3. Öffnen Sie die Erfassungsdatei in Wireshark, und filtern Sie auf Port 5432 mit `tcp.port==5432`, um den Datenverkehr zwischen dem Nicht-Master-Peer und dem DB-Master zu überprüfen.
4. Wenn kein Rückverkehr vom Server erfolgt, blockiert wahrscheinlich eine Firewall den Port zwischen dem logischen Standort der beiden Server.

Nachfolgend finden Sie eine typische Paketerfassung aus einer funktionierenden Verbindung zwischen Client und Server:

In diesem Beispiel ist die IP-Adresse des Clients 10.48.54.119 und der Server 10.48.54.75.



The screenshot shows a network packet capture tool interface with a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main window displays a list of captured packets. The filter is set to 'tcp.port==5432'. The packet list includes:

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	TCP	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	TCP	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	TCP	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 08:36:13.571338	10.48.54.75	10.48.54.119	TLSv1.2	382	Application Data

Zugehörige Informationen

Weitere Informationen zur Fehlerbehebung sowie weitere Fragen zum Datenbank-Clustering finden Sie in den häufig gestellten Fragen unter den folgenden Links:

- [Warum muss ich sie bei der Clustering von Datenbankservern an verschiedenen Standorten platzieren?](#)
- [Wir haben einen Datenbank-Cluster, und ich sehe einen Datenbankfehler oder eine Warnung im Protokoll. Was soll ich tun?](#)
- [Mindestens ein Datenbankserver ist nicht verbunden oder befindet sich im Synchronisierungsstatus. Was soll ich tun?](#)
- [Was kann ich tun, wenn keine Master-Datenbank vorhanden ist?](#)
- [Verschieben der Master-Datenbank](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)