

# Configurer le cluster de base de données Cisco Meeting Server Call Bridge

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Partie 1. Création de certificat](#)

[Partie 2. Configuration du pont d'appel](#)

[Diagramme du réseau](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit les étapes à suivre pour configurer le clustering de base de données (DB) sur Cisco Meeting Server (CMS) ou les ponts d'appels Acano (CB).

## Conditions préalables

### Conditions requises

- Cisco recommande de disposer d'au moins 3 noeuds CMS pour pouvoir créer un cluster de base de données viable

**Note:** Il est recommandé d'avoir un nombre impair de noeuds de cluster de base de données car il est important pour la sélection principale et le mécanisme de basculement actif. Une autre raison à cela est que le noeud de base de données maître serait le noeud qui a des connexions à la plus grande partie de la base de données dans le cluster. Vous pouvez avoir un maximum de 5 noeuds dans un cluster de base de données.

- Port 5432 ouvert sur pare-feu

**Remarque :** le maître du cluster de base de données écoute sur le port 5432 les connexions à partir des noeuds clients, donc s'il y a un pare-feu (FW) entre les noeuds, assurez-vous que ce port est ouvert.

## Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configuration

Il existe deux types de certificats pour le clustering de base de données :

1. Client : Le certificat client, comme son nom l'indique, est utilisé par les clients DB pour se connecter au serveur DB (maître). Ce certificat doit contenir la chaîne, les postgres, dans son champ Nom commun (CN).
2. Serveur : Le certificat du serveur, comme son nom l'indique, est utilisé par le serveur de base de données pour se connecter à la base de données postgres.

### Partie 1. Création de certificat

1. Connectez-vous à Secure Shell (SSH) avec les informations d'identification admin au serveur MMP.
2. Générer une demande de signature de certificat (CSR) :

a. Pour le certificat client de la base de données :

```
pki csr <clé/nom de base du certificat> CN : postgres
```

Par exemple : **pki csr databasecluster\_client CN : postgres**

b. Pour le certificat du serveur de base de données :

```
pki csr <nom de base de clé/certificat> CN : <nom de domaine>
```

Par exemple : **pki csr databasecluster\_server CN : vngtpres.aca**

3. Envoyez les CSR à votre autorité de certification (CA) pour les faire signer. Assurez-vous que l'autorité de certification vous fournit les certificats d'autorité de certification racine (et toute autorité de certification intermédiaire).
4. Téléchargez les certificats signés, les certificats d'autorité de certification racine (et toute autorité de certification intermédiaire) sur tous les noeuds de base de données à l'aide d'un client SFTP (Secure File Transfer Protocol) (par exemple WinSCP).

**Note:** Le CN de la partie A doit être des messages et la partie B peut être le nom de domaine du pont d'appel, aucune entrée de nom de remplacement de sujet (SAN) n'est requise.

### Partie 2. Configuration du pont d'appel

Sur la CB qui exécute la base de données principale, procédez comme suit :

1. Pour sélectionner l'interface à utiliser, entrez la commande suivante :

**cluster de base de données localnoeud a**

Cela permet " interface un " à utiliser pour le clustering de base de données.

2. Définissez les certificats ca client, serveur et racine ainsi que les clés privées à utiliser par le cluster de base de données avec les commandes suivantes :

**certs de cluster de base de données <clé\_client> <crt\_client> <crt\_ca>**

**certs de cluster de base de données <clé\_serveur> <crt\_serveur> <clé\_client> <crt\_client>  
<crt\_ca>**

**Note:** Les mêmes certificats client et serveur peuvent être utilisés sur d'autres noeuds CB à mettre en cluster lorsque vous copiez les clés privées et les certificats sur les autres noeuds. Cela est possible car les certificats ne contiennent aucun SAN les liant à un pont d'appel spécifique. Cependant, il est recommandé d'avoir des certificats individuels pour chaque noeud de base de données.

3. Initialisez cette base de données sur la BC locale en tant que maître pour ce cluster de base de données :

**initialisation du cluster de base de données**

4. Sur les ponts d'appel qui feraient partie de la base de données en cluster et deviendraient les esclaves de la base de données, exécutez cette commande après avoir terminé les étapes 1 et 2 pour la partie 2 :

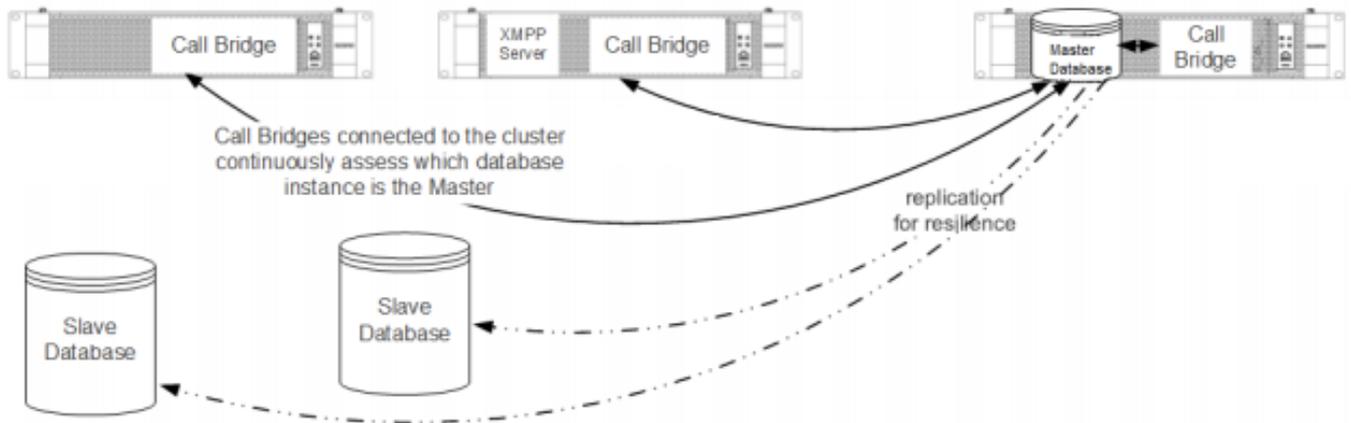
**jointure de cluster de base de données <adresse IP CB principale>**

Exemple : **jointure de cluster de base de données <10.48.36.61>**

Ceci initie la synchronisation de la base de données et copie la base de données à partir du pair principal.

**Note:** La base de données locale qui existait avant l'exécution de la commande **de jointure de cluster de base de données** continue d'exister jusqu'à ce que le noeud soit supprimé de la base de données en cluster. Aussi longtemps que le noeud est dans le cluster de base de données, sa base de données locale n'est pas utilisée.

**Diagramme du réseau**



## Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Pour vérifier l'état de la base de données en cluster, exécutez cette commande sur l'un des noeuds du cluster de base de données :

### état du cluster de base de données

La sortie est similaire à :

```
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)
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Utilisez cette commande, sur l'interface de ligne de commande, pour afficher les journaux actuels relatifs au clustering de base de données :

### suivi syslog

Les sorties du journal de la base de données contiennent généralement la chaîne postgres, par exemple :

```

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

```

Le [collecteur de journaux CMS](#) fournit une interface utilisateur simple et conviviale pour collecter les journaux à partir du serveur CMS.

Voici quelques problèmes et solutions de base de données typiques :

**Problème : Erreur de schéma de base de données sur un homologue non maître**

```

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)

```

**Solution :**

1. Exécutez d'abord cette commande pour effacer l'erreur :

**erreur d'effacement du cluster de base de données**

2. Suivez cette commande pour mettre à niveau le schéma de base de données :

**database cluster upgrade\_schema**

3. Vérifiez ensuite l'état du cluster DB avec :

**état du cluster de base de données**

Les journaux affichent une sortie similaire à celle-ci :

```

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
```

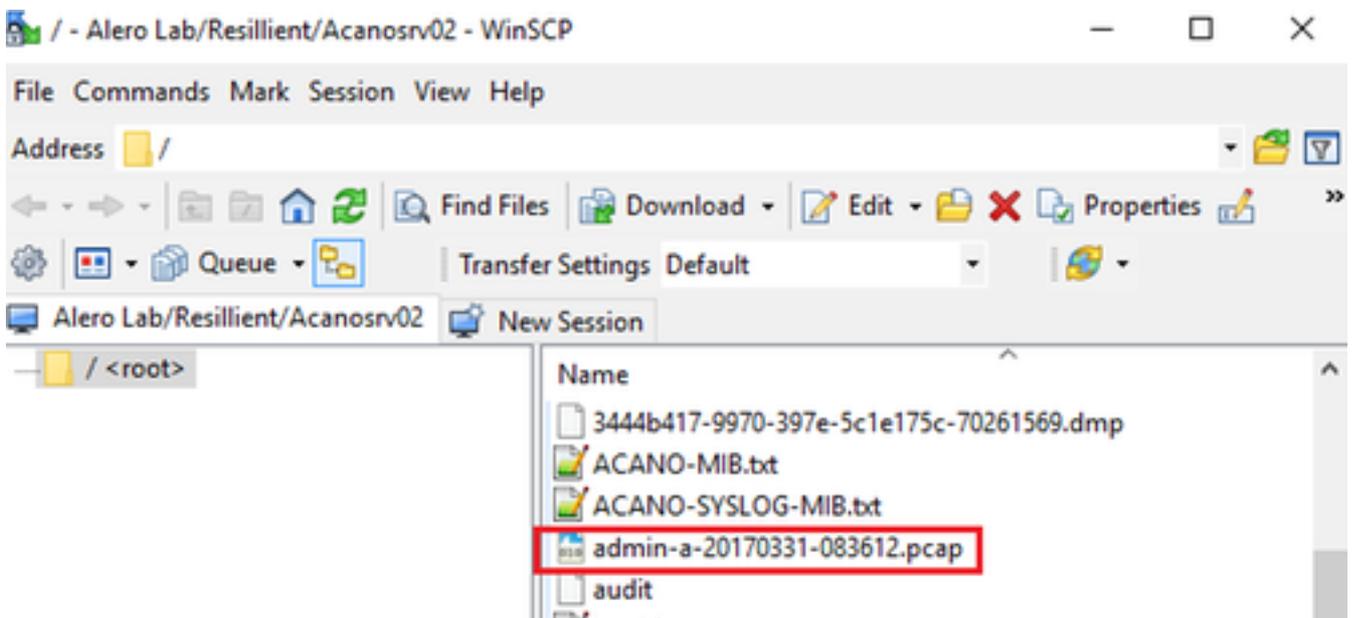
**Problème : Noeuds homologues ne pouvant pas se connecter au noeud maître de la base de données**

```
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?|
```

**Solution :**

Utilisez ces étapes pour collecter les traces afin de résoudre les problèmes de connexion :

1. Exécutez la commande **pcap <interface>** sur le noeud non maître (esclave) et, après quelques minutes, arrêtez la capture avec **Ctrl-C**.
2. Connectez-vous avec un client SFTP (Secure File Transfer Protocol) au serveur et téléchargez le fichier **.pcap** à partir du répertoire racine :



3. Ouvrez le fichier de capture sur Wireshark et filtrez sur le port 5432 avec **tcp.port==5432** pour vérifier le trafic entre le pair non maître et le maître de la base de données.
4. S'il n'y a pas de trafic de retour du serveur, il est probable qu'un pare-feu bloque le port entre l'emplacement logique des deux serveurs.

Voici une capture de paquets typique d'une connexion opérationnelle entre le client et le serveur :

Dans cet exemple, l'adresse IP du client est 10.48.54.119 et le serveur est 10.48.54.75.

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	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 08:36:13.571730	10.48.54.75	10.48.54.119	TLSv1.2	382	Application Data

## Informations connexes

Pour plus d'informations sur la résolution des problèmes et d'autres questions sur la mise en grappe de bases de données, reportez-vous à la FAQ dans les liens suivants :

- [Lors de la mise en grappe de serveurs de base de données, pourquoi dois-je les placer sur différents emplacements ?](#)
- [Nous avons un cluster de base de données, et je vois une erreur de base de données ou un avertissement dans le journal. Que dois-je faire](#)
- [Un ou plusieurs serveurs de base de données ne sont pas connectés ou dans l'état « Sync ». Que dois-je faire](#)
- [Que faire en l'absence de base de données principale](#)
- [Comment déplacer la base de données principale](#)
- [Support et documentation techniques - Cisco Systems](#)