How to renew expired database cluster certificates in Cisco Meeting Server (CMS)

Contents

Introduction

This document describes how to renew expired (client and server) certificates on database cluster on Cisco Meeting Server (CMS).

Prerequisites

Components Used

Cisco Meeting Server

Background Information

Certificate (client and server) used to create a database cluster on Cisco Meeting Server comes with an expiry date.

Once the certificate expires, database nodes in cluster stops talking to each other. Certificates cannot be renewed on CMS database cluster nodes unless cluster is removed using CLI command **"database cluster remove".**
Certificates are tied to DB servcies which does not let us make any changes, unless a cluster is torndown and certificates are disengaged.

Configure

Network Diagram
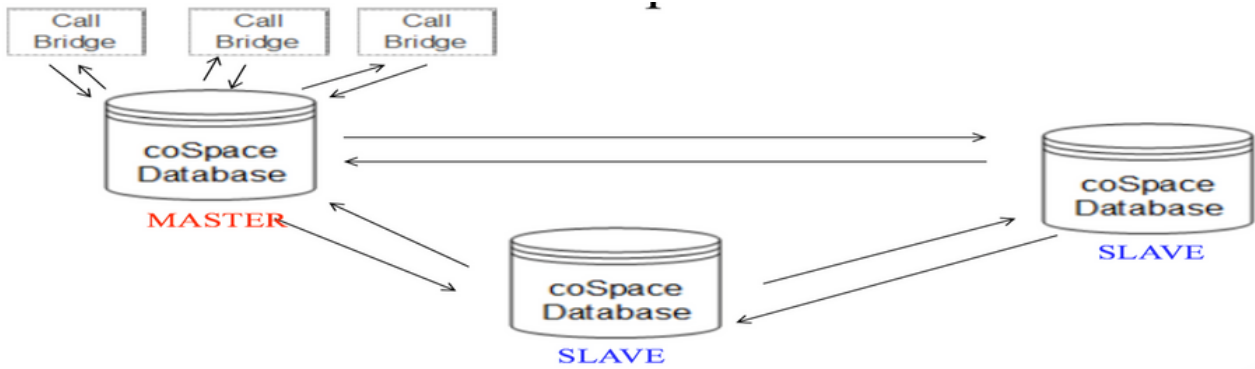
Procedure Overview

Step 1. Take a backup of CMS Nodes in the cluster

Step 2. Fetch the backup file from cms via FTP and store on local pc.

Step 3. Remove database cluster node from cluster.

Step 4. Update the certificates.

> **Note**: Try to give same certificate file name as used earlier (which got expired). You may need to remove old expired certificates from Cisco Meeting Server for new one to take affect.

Step 5. Create cluster again database cluster initialize.

Step 6. Follow process to create cluster.

> **Note**: Above procedure to follow on all slaves and then at last update on master nodes

Configuration Procedure

Step 1. In the output of **"database cluster status"** Certificate shows expired for CMS database cluster.

```
cms2> database cluster status
Status                    : Disabled
Node in use               : None

Interface                 : a

Certificates
  Server Key              : dbclusterserver.key
  Server Certificate      : dbclusterserver.cer (expired)
  Client Key              : dbclusterclient.key
  Client Certificate      : EXPRSVR.cer (expired)
  CA Certificate          : CA.cer
```

Step 2. Verify certificate expiry by running "**pki inspect <cert name>**" command

```
cms2> pki inspect EXPRSVR.cer
Checking ssh public keys...not found
Checking user configured certificates and keys...found
File contains a PEM encoded certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            11:02:ce:3b:00:06:00:00:00:a7
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=uctplab, CN=uctplab-TPWIN2008R2DC-CA
        Validity
            Not Before: Mar  9 08:47:17 2015 GMT
            Not After : Mar  9 08:57:17 2017 GMT
        Subject: C=IN, ST=KA, L=BLR, O=Cisco, OU=TAC, CN=VCScMRA.S.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

Caution: We cannot update the certificate when database cluster is active. We need to remove the node from cluster. If an attempt is made to update certificate while cluster is active. Following error is noticed

```
ROOTEXPRSVR.cer
cms2> database cluster certs dbclusterserver.key  dbclusterserver.cer EXPRSVR.cer cmscore2.key CAVD.cer
ERROR: Cannot change certificates when clustering enabled.
  Disable clustering on this node first
cms2>
cms2>
cms2>
cms2>
cms2>
```
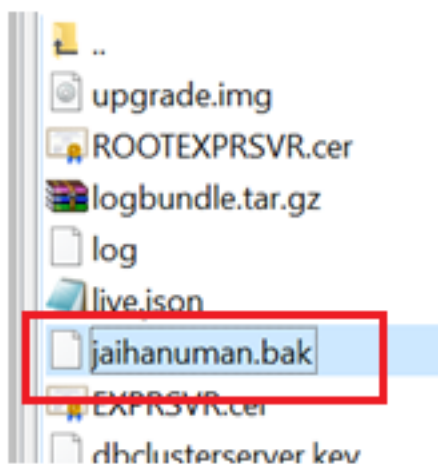
Step 3. Create a backup file on the node by runinng backup **snapshot <filename>**

```
Usage:
    backup snapshot <name>
    backup rollback <name>
    backup list
cms2> backup snapshot jaihanuman
jaihanuman.bak ready for download
cms2>
cms2>
cms2>
```

Step 4. Login to FTP client and pull the file on local PC.
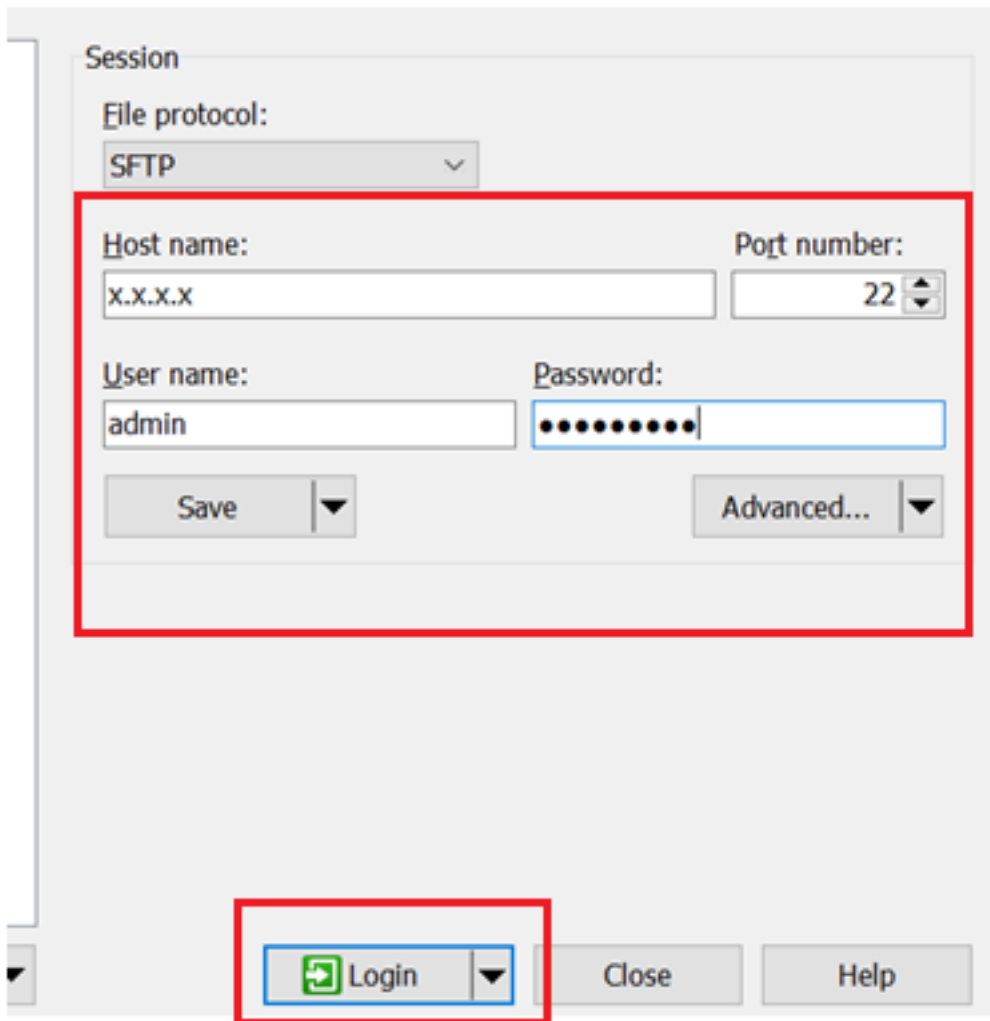
Step 5. Pull the .bak file from cms to local PC

Step 6. Run command to remove the node from database cluster. "**database cluster remove"**

Note:Press **"Y"** in caps. lower case "y" wont proceed.

Step 7. Node is detaching from cluster

Step 8. Node has been removed from database cluster.

```
cms2> database cluster status
Status                          : Disabled
Node in use                     : None

Interface                       : a

Certificates
   Server Key                   : dbclusterserver.key
   Server Certificate           : dbclusterserver.cer (expired)
   Client Key                   : dbclusterclient.key
   Client Certificate           : EXPRSVR.cer (expired)
   CA Certificate               : CA.cer

Last command                    : 'database cluster remove' (Success)
```

Step 9. Update new certificates files for databse cluster. Database cluster would need client and server certificate.

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

```
cms2> .key dbclusterserver.cer dbclusterclient.key dbclusterclient.cer CAVD.cer
Certificates updated
cms2>
cms2>
```

Step 10. Add node to the database cluster again.

```
cms2> database cluster initialize
WARNING!!!
Are you sure you wish to initialize this node as a new database cluster? (Y/n)
 The contents of this node's database will become the master version of the data
base in the new cluster.
 The callbridge and web administration will restart at the end of this procedure
.
```

Step 11. New certificate files have been updated.

```
cms2> database cluster status
Status                      : Enabled

Nodes:
    10.106.85.75 (me)       : Connected Master
Node in use                 : 10.106.85.75

Interface                   : a

Certificates
    Server Key              : dbclusterserver.key
    Server Certificate      : dbclusterserver.cer
    Client Key              : dbclusterclient.key
    Client Certificate      : dbclusterclient.cer
    CA Certificate          : CAVD.cer

Last command                : 'database cluster initialize' (Success)
```

Step 12. Add the node to the database cluster master.

```
cms2> database cluster join 10.106.85.73
WARNING!!!
Are you sure you wish to join this node to an existing database cluster? (Y/n)
 The contents of this node's database will be destroyed!
 The callbridge and web administration will restart at the end of this procedure.
 NOTE: This node is already in a cluster.
 Knowledge of all nodes in the old cluster will be removed
```

Step 13. Database cluster is good again with updated certificates

```
cms2> database cluster status
Status                      : Enabled

Nodes:
    10.106.85.73            : Connected Master
    10.106.85.74            : Connected Slave ( In Sync )
    10.106.85.75 (me)       : Connected Slave ( In Sync )
Node in use                 : 10.106.85.73

Interface                   : a

Certificates
    Server Key              : dbclusterserver.key
    Server Certificate      : dbclusterserver.cer
    Client Key              : dbclusterclient.key
    Client Certificate      : dbclusterclient.cer
    CA Certificate          : CAVD.cer

Last command                : 'database cluster join 10.106.85.73' (Success)

cms2>
```