aruba
a Hewlett Packard
Enterprise company

CPPM 6.8 - CLUSTER CONFIGURATION USING CERTIFICATES

VERSION 1.0

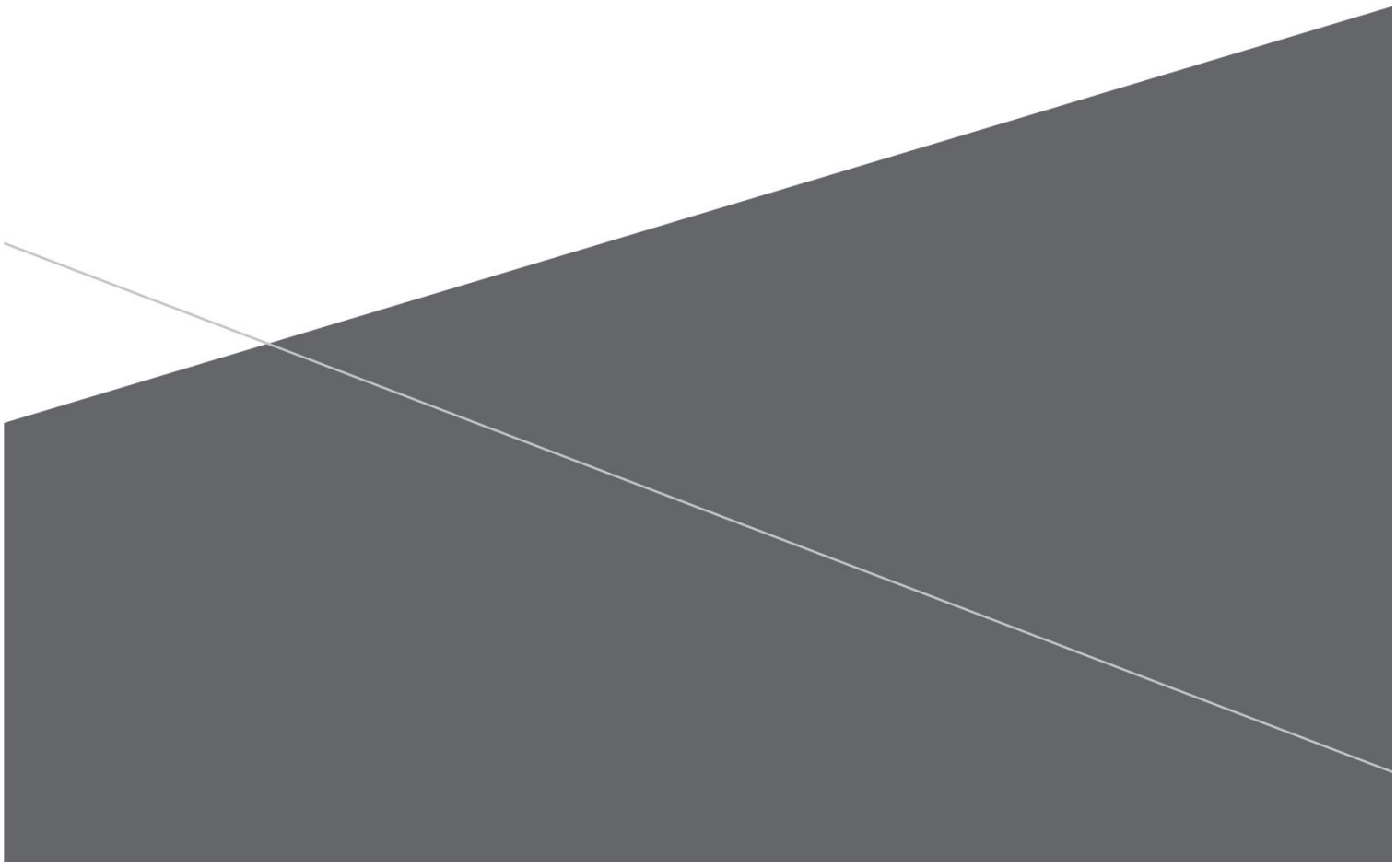


Table of Contents

Certificate role in cluster configuration in 6.8

In 6.8, for enhance cluster security introduce https and database server certificate which role play vital role between cluster nodes.

Https server Certificate validation – It is mandatory that nodes (subscriber's) should trust https certificate of publisher node. It should be present in CPPM nodes trust list before configure cluster.
In order to adhere best practice https server certificate is signed by public Certificate Authority, which includes all nodes FQDN name in subject alternate name (SAN) field.

Database server Certificate – This is new certificate type in 6.8 to enhance security in the cluster replication between the cluster's nodes. It should be present in CPPM nodes (subscriber's) trust list before configuration cluster.

In order to adhere best practice, do not use self-sign CPPM database server certificate instead of that signed database severe certificate by internal/external Certificate Authority.

HTTPS Server certificate

Step -1 CSR Generation

Generate CSR from Publisher CPPM node & Subscriber nodes and sign with Root CA server

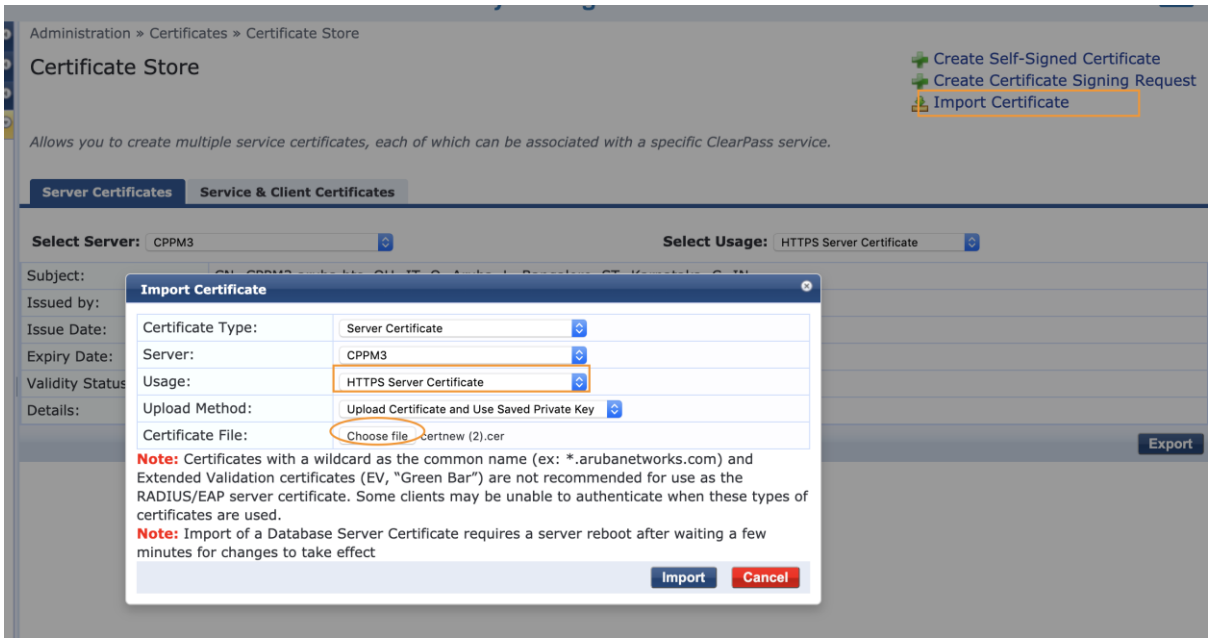
Administration » Certificates » Certificate Store

Note: -
1. Adhere best practice use public signed https certificate.

2. We could also use internal root CA server for sign https certificate (only useful for Lab environment)

Step -2 Import signed certificate

Login on Publisher and import the public signed certificate - Administration » Certificates » Certificate Store



Step -3 Import certificate in subscriber trust list

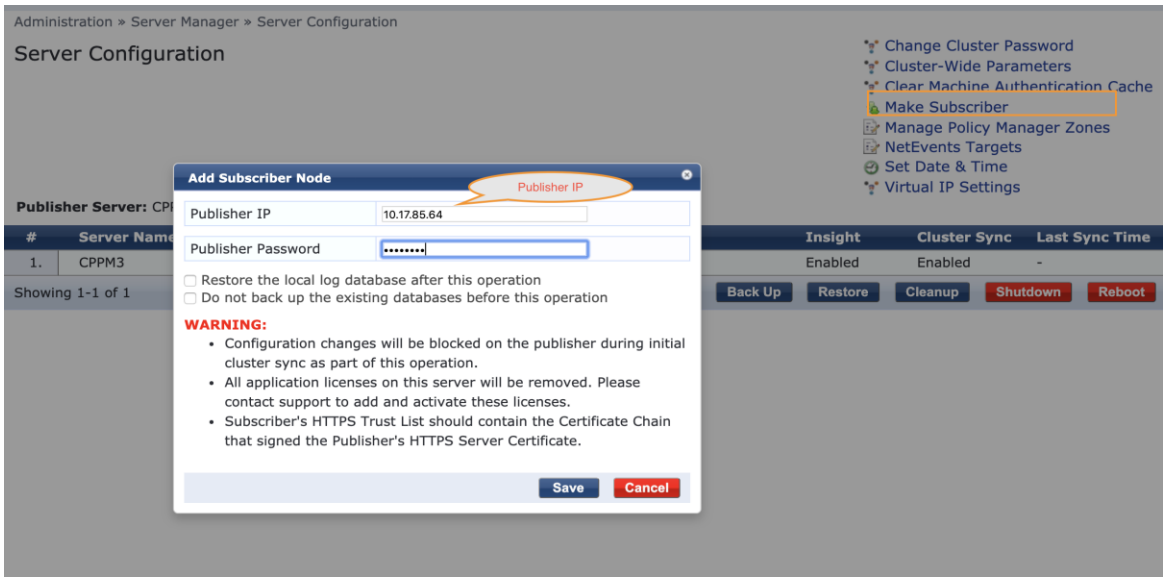
Login on subscriber's node and import publisher https server certificate in the trust list - Administration » Certificates » Trust List >> Add

Note: -

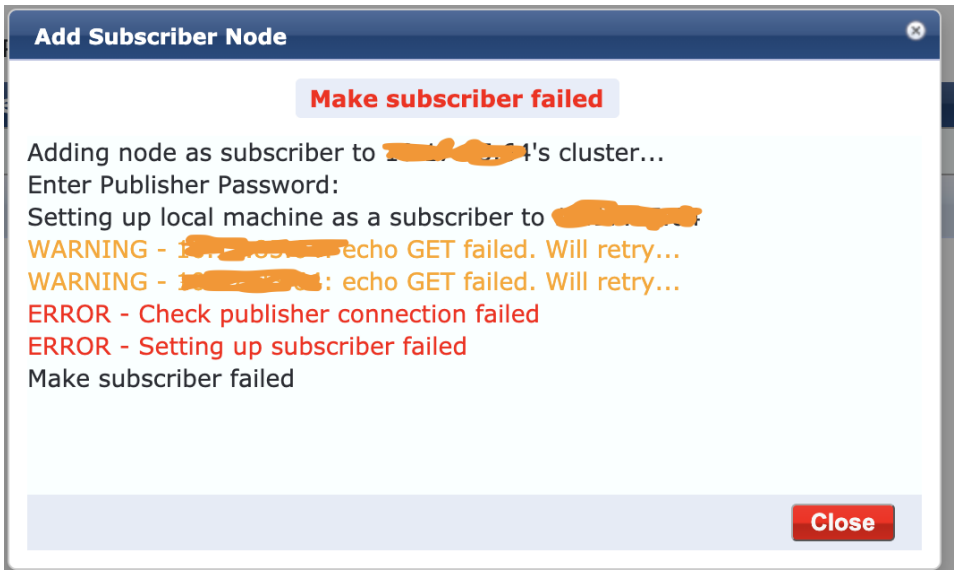
1. Root CA chain should be in trust list before import cert.
2. When generate CSR private key does save in CPPM database. which does expire after 15 days, after expired private key we can't recover private key

Step -4 Configure cluster

Login on CPPM node (subscriber) and joining the node in the cluster



If publisher CPPM node https certificate is not trust list of subscriber node failed with below error.



Database Server certificate

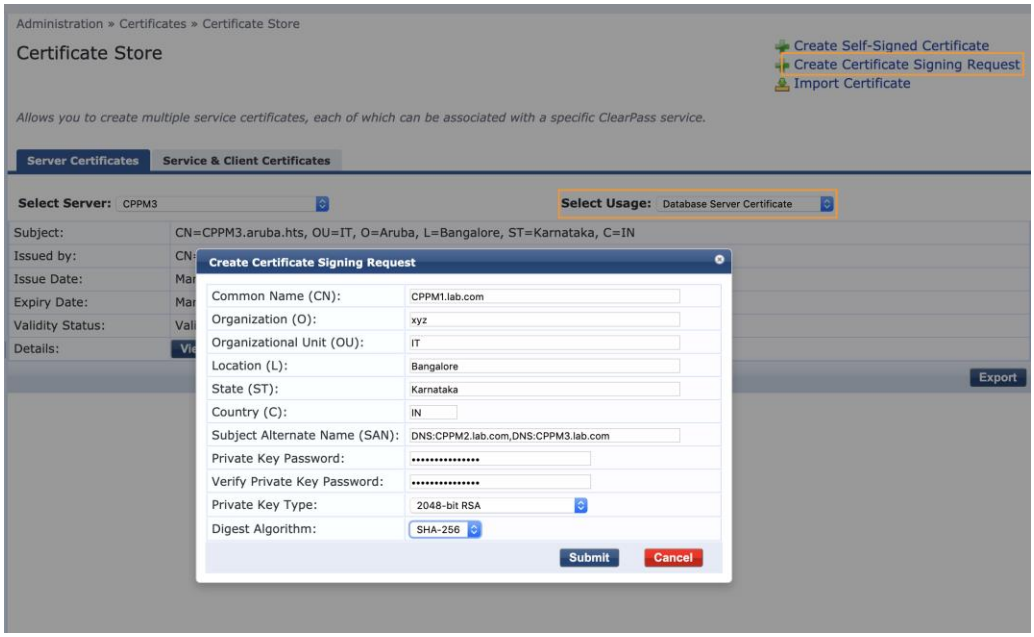
This is new feature introduce in 6.8, This provides customers an ability to import a certificate signed by the Certificate Authority of their choice hence enhancing security between the cluster members.

Note: - In 6.8, database server certificate support only 1 year. This was fixed in 6.8.1 where the default Database certificate validity was increased back to 5 years.

Import DB server certificate

Step -1 CSR Generation

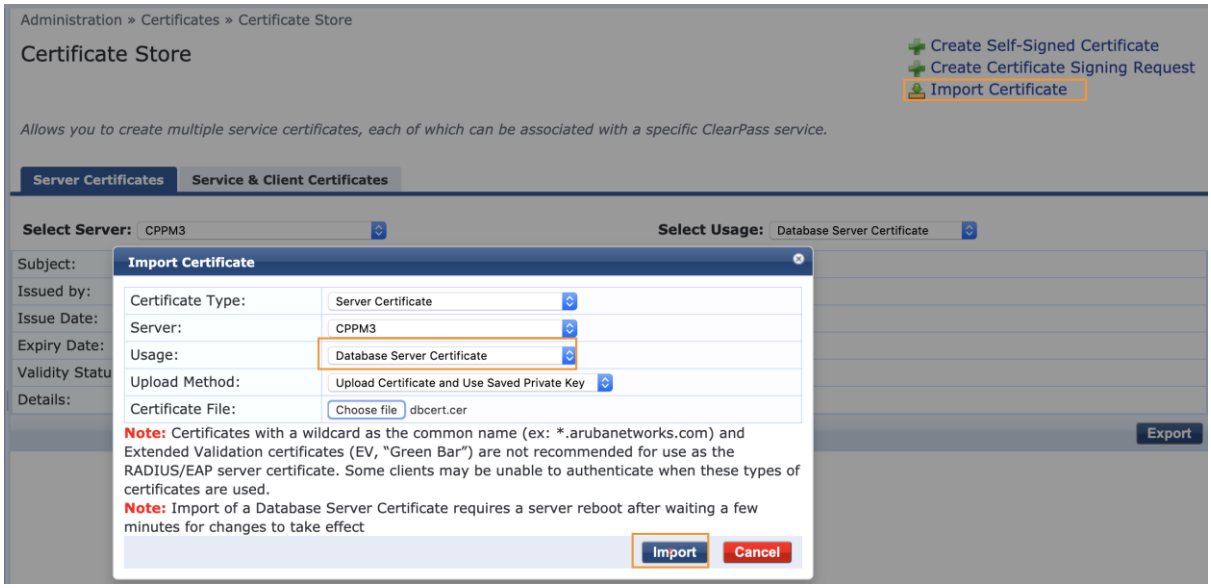
Generate CSR from CPPM UI - Administration » Certificates » Certificate Store (select usage – Database server certificate)



Step -2 Import certificate

Login on Publisher, after signed the certificate by Certificate Authority, need to import database server certificate on CPPM node.

Administration » Certificates » Certificate Store



Step -3 Import certificate in subscriber trust list

Login on subscriber's node and import publisher database server certificate in the trust list - Administration » Certificates » Trust List >> Add