FIELD ADVISORY

CLUSTERING IN 6.8

CERTIFICATE VALIDATIONS

ClearPass Policy Manager 6.8 introduced additional flexibility to customers who would like to use their own certificates to secure the database. To facilitate this change, some of the controls that were previously implemented automatically within the system have been moved to require administrator actions prior to creating clusters. Customers who have created their clusters prior to 6.8.0 upgrades are not impacted by these changes as the system will automatically account for them when all members are upgraded as a cluster. However, customers who are creating a new cluster in 6.8 have to understand the nuances associated with this feature.

The process of clustering ClearPass Policy Manager nodes requires 2 certificate validations.

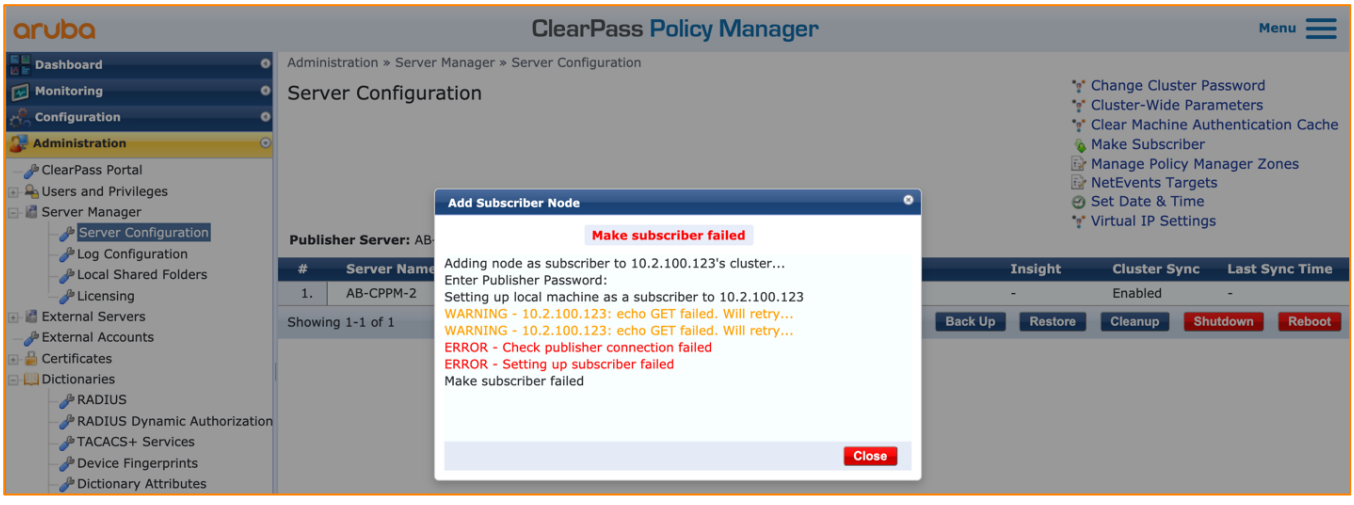
a. HTTPS certificate validation

b. Database certificate validation

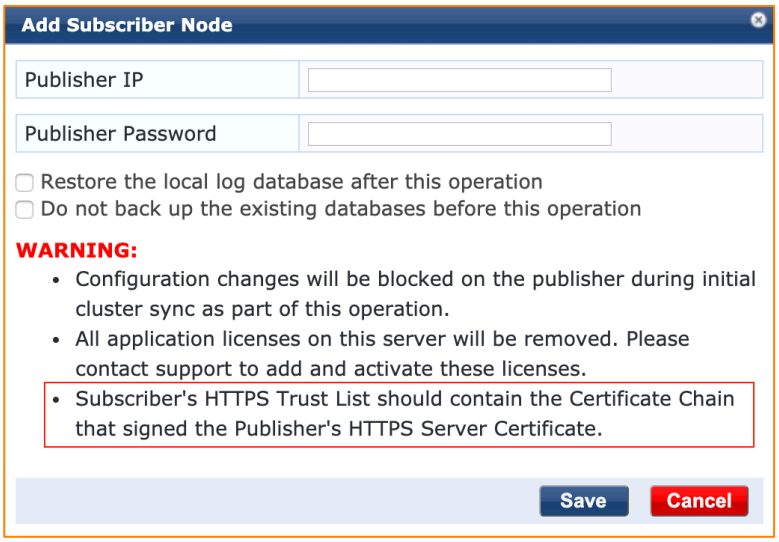
The nodes within the cluster communicate with each other over HTTPS. The subscriber nodes also replicate their database with the Publisher node in the cluster. In order to adhere with the best security practices, it is mandatory that the nodes validate the trust using certificates before exchanging the data. 6.8 also mandates the validation of HTTPS certificate between cluster nodes.

HTTPS CERTIFICATE VALIDATION

A self-signed HTTPS certificate is installed upon a fresh install of a ClearPass server. Hence an attempt to add a subscriber node with the default HTTPS certificate fails with the following error.



A WARNING is shown on the UI when an attempt to add a subscriber node to the cluster is made as highlighted below

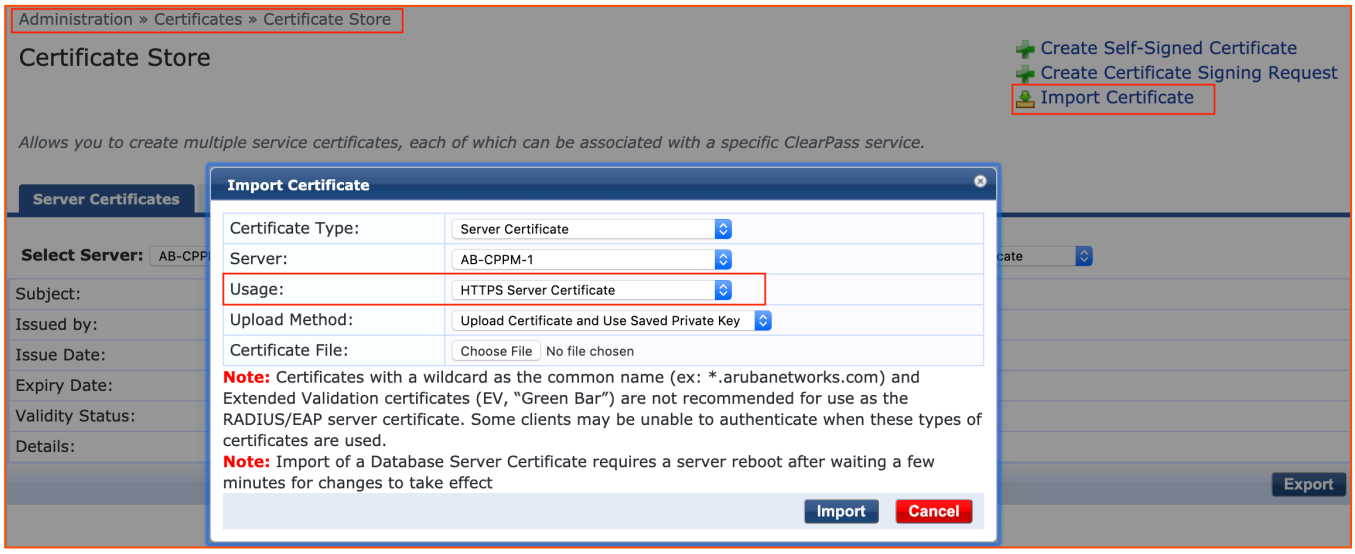


Hence, to create a cluster in 6.8, there are 2 approaches. In production environments, one must follow the first approach where the HTTPS certificate is signed by a public Certificate Authority (CA). The second approach should be avoided at all costs and only be used in LAB scenarios.

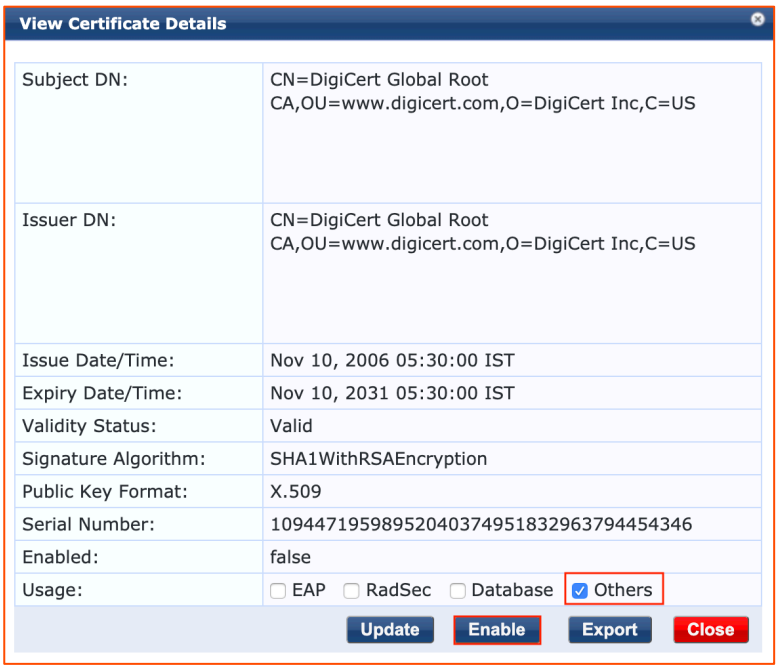
HTTPS CERTIFICATE SIGNED BY PUBLIC CA

1. In this approach, the ClearPass Policy Manager (CPPM) nodes are signed by a Public Certificate Authority. A wildcard certificate or a certificate containing the FQDN for all the nodes in the cluster within the Subject Alternate Name (SAN) signed by a known Public Certificate Authority can be used.

   This certificate needs to be imported under **Administration > Certificates > Certificate Store**. Click on **Import Certificate**.



2. Ensure the entire chain including the Root and Intermediates of the Signing Certificate Authority (CA) are enabled in the Trust list of the Publisher. To enable a trusted CA, navigate to **Administration > Certificates > Trust List**. Enable the CA to be trusted for "**Usage = Others**".



HTTPS CERTIFICATE VALIDATION IGNORED USING CLI

Again, this method is not recommended as it completely ignores trust validation for the nodes joining the cluster

Login to the CLI of the ClearPass Policy Manager node to be added as a subscriber using the appadmin credentials. Once logged in, issue the command as shown below:

```
[appadmin@AB-CPPM-2]# cluster make-subscriber -i <Publisher IP> -V

******************************************************
*                                                    *
* WARNING: Executing this command will make the current*
* machine a subscriber to the publisher host specified.*
* Current configuration and application licenses     *
* installed (if any) on this node will be lost when the*
* operation is complete.                             *
*                                                    *
* Configuration changes will be blocked on the       *
* publisher during initial cluster sync as part of   *
* this operation.                                   *
*                                                    *
* Do not close the shell or interrupt this command   *
* execution.                                         *
*                                                    *
******************************************************
```

```
Continue? [y|n]: y

Enter Publisher Password:
Setting up local machine as a subscriber to 10.1.1.2
INFO - Check publisher connection passed
INFO - Local checks before adding subscriber passed
INFO - 10.1.1.2: - Subscriber node added successfully for host=AB-CPPM-2
INFO - Subscriber node entry added in publisher
INFO - Backup databases for AppPlatform
INFO - Backup databases for PolicyManager
INFO - Backup extensions
INFO - Stopping services
INFO - Dropped existing databases for Policy Manager
INFO - Create database and schema for Policy Manager
INFO - Local database setup done for Policy Manager databases
INFO - Subscriber password changed
INFO - Syncing up initial data...
INFO - Config database temporarily locked for updates
INFO - 10.1.1.2: - Backup databases for AppPlatform
INFO - 10.1.1.2: - Backup databases for PolicyManager
INFO - 10.1.1.2: - Backup extensions
INFO - Config database lock released
INFO - Subscriber now replicating from publisher 10.1.1.2
INFO - Retaining local node certificate
INFO - Subscriber replication and node setup complete
INFO - Notify publisher that adding subscriber is complete
INFO - Subscriber added successfully
INFO - Restarting Policy Manager admin server
```

DATABASE CERTIFICATE VALIDATION

In 6.8, an ability to import a custom Database certificate was exposed in the UI. This provides customers an ability to import a certificate signed by the Certificate Authority of their choice hence enhancing security between the cluster members.

Historically, when a customer upgraded a major version of ClearPass the Database certificates were regenerated for 5 years. For instance, an upgrade from 6.6 to 6.7 will regenerate the certificate with the validity of 5 years. In 6.8, these certificates were generated only for a year. Hence a new install of 6.8 or an upgrade from any previous version to 6.8 will always generate a Database certificate with a validity of 1 year. This is a very short duration for production environments. This was fixed in 6.8.1 where the default Database certificate validity was increased back to 5 years. However, Database certificates regenerated in 6.8.1 could not handle the trust relationship between the nodes with the default certificates. This would often result in UI errors shown in red "Error in processing request. Please retry...". The issue of trust between these certificates was fixed with the hotfix for 6.8.1.

The summary of the above paragraph is that if a cluster is being upgraded from any version to 6.8.1, the automatic Database certificate trust handling is broken and hence the cluster is affected. Adding the hotfix should fix this issue thereby ensuring the cluster nodes trust the Database certificates of the member nodes hence restoring normalcy as far as cluster operations are concerned.

Note: A change in DB certificate will only be applicable after a reboot of the node.

SUMMARY

Cluster Upgrade/Update	DB Cert Validation	HTTPS Cert Validation
6.7.X to 6.8.0	Automatic validation. Default certificate valid only for **1 year**.	Automatic validation. Upload a public signed HTTPS certificate **(recommended)**
6.8.0 to 6.8.1	Certificate validation fails.	Uses the same trust as available in 6.8.0.
6.8.1 to (6.8.1 + Hotfix) or 6.8.2	Automatic validation. Default certificate valid for **5 years**.	Uses the same trust as available in 6.8.0.
Clustering in a new install		
6.8.0	Automatic validation. Default certificate valid only for **1 year**.	HTTPS certificate signed by Public Certificate Authority **(recommended)** OR Use CLI to ignore trust **(Lab only)**
6.8.1 or 6.8.1 + Hotfix or 6.8.2	Automatic validation. Default certificate valid for **5 years**.	HTTPS certificate signed by Public Certificate Authority **(recommended)** OR Use CLI to ignore trust **(Lab only)**

Adding a new node to an upgraded cluster should be treated the same as clustering in a new install.

FAQ

1. What happens to my cluster when I upgrade from 6.7 to 6.8.0?

   Clustering will not be affected. However, database certificate validity will only be 1 year. Hence it needs to be replaced within the validity timeframe.

2. What is the behavior upon an update from 6.8.0 to 6.8.1?

   The Database certificate even though generated for 5 years will fail automatic validation. 6.8.1 should not be used without the hotfix for a cluster setup.

3. What happens to a cluster when the certificate expires?

   Expiration of HTTPS certificate does not affect the existing cluster. Expiration of DB certificate will break the cluster.

4. I had created a cluster on 6.8.1, the cluster seems to have broken. The issue seems to persist even after applying the hotfix.

   Contact Aruba support.