CPPM v6.9.5 及以上版本做 cluster 的相关注意点-202108

背景描述：

CPPM 从 V6.8.0 版本开始（V6.8.9 除外），做 cluster 集群时，Pub 和 Sub 需要先相互信任 HTTPs 证书的前提下，才能让 Sub 成功地加入到 Cluster 集群。而在 V6.8.9 和 V6.9.5 版本上，支持系统初始化后默认证书下的 Cluster 建立，但是如果我们在建立 Cluster 集群之前，已经各自系统分别创建了自签 HTTPs 和 Database 证书的话，那还能正常地完成 Cluser 集群的创建吗？

原因：

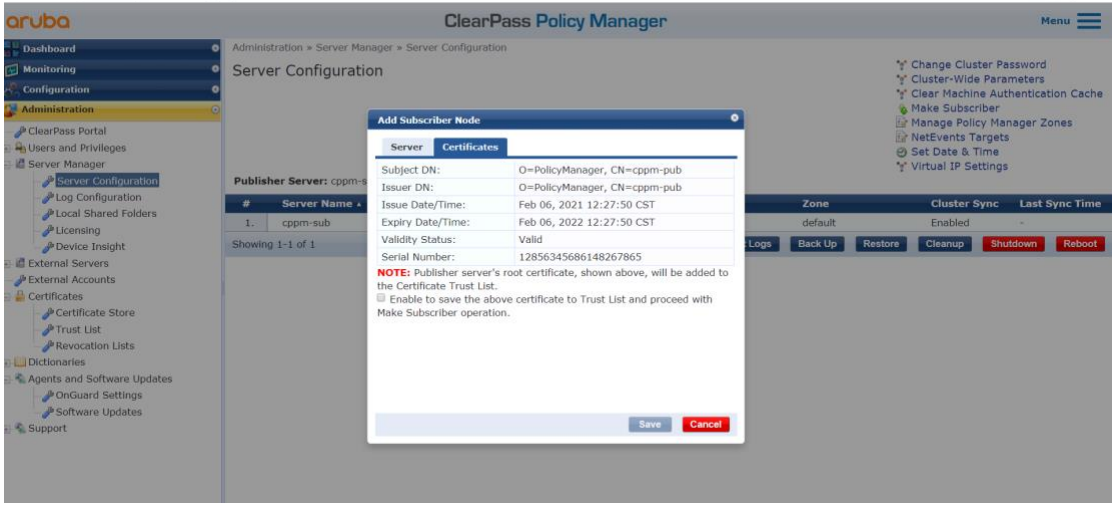
V6.8.X（V6.8.9 除外），CPPM 建立 Cluster 集群之前，需要 HTTPs 证书的相互信任，而新版本不需要事先信任 HTTPs 证书，使用系统初始化后的默认证书，直接可以建立 Cluster 集群，反而如果我们 Pub 和 Sub 节点各自创建了自签 Database 证书后，Cluser 集群是无法建立成功的，那如何解决？

解决办法：

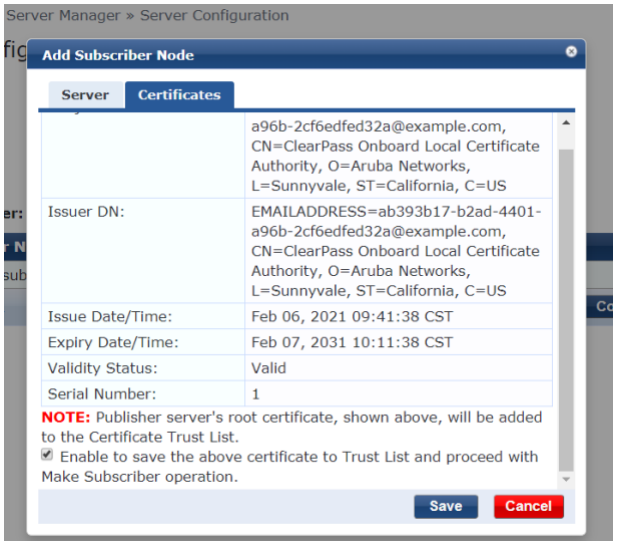
在 v6.9.5 及以上版本（含 V6.8.9），HTTPs 证书使用系统默认的或者各自创建自签的证书都可以完成 Cluster 集群创建，但是 Database 证书要么保持系统初始化默认的（不能采用系统创建自签的 Database 证书），要么就是由 Pub Onboard CA 来统一签发给 Pub 和 Sub（签发的时候，创建 CSR 时，要求 CN=mgmt-ip 或者 SAN DNS:mgmt.-ip），就是不能采用各自节点分别独立创建 Database 自签证书的方式。

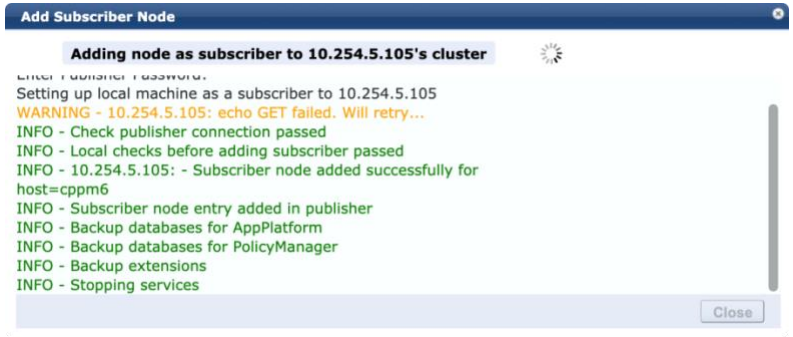
相关的详细测试步骤：

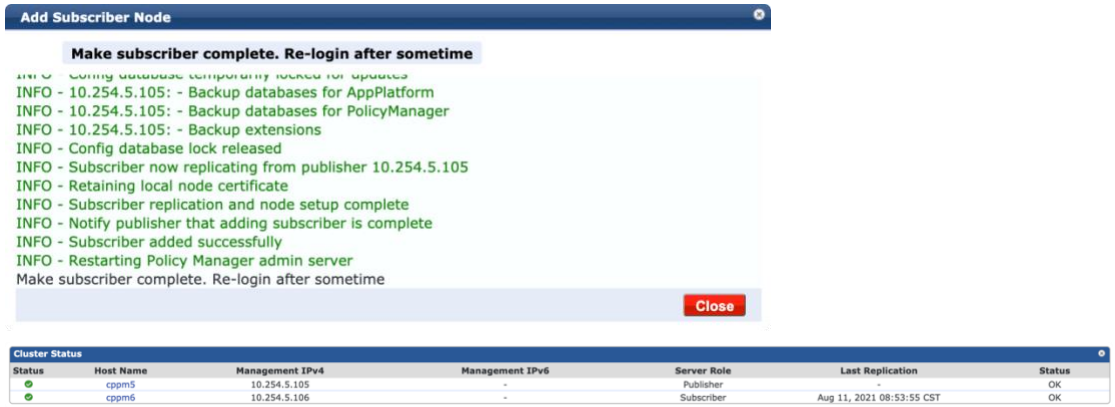
1） Pub 和 Sub 采用系统初始化后的默认证书（注意，这里不是后来创建的自签证书），做 Cluster 成功（直接将 Sub 加入到 Pub 中）。



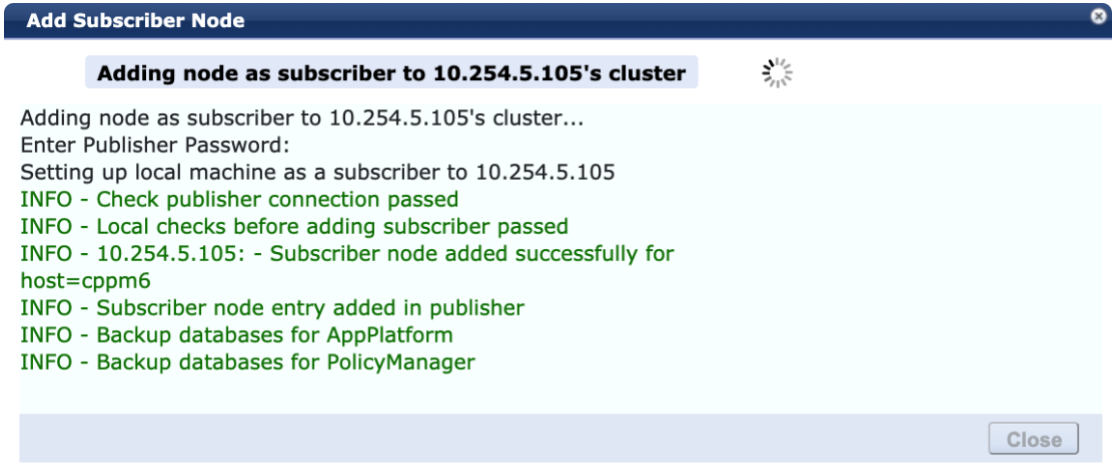
需要勾选 enable to save the above certificate to Trust List and proceed with Make Subscriber operation 选项。


Server Manager » Server Configuration
Add Subscriber Node
Server
Certificates
a96b-2cf6edfed32a@example.com, CN=ClearPass Onboard Local Certificate Authority, O=Aruba Networks, L=Sunnyvale, ST=California, C=US
Issuer DN:
EMAILADDRESS=ab393b17-b2ad-4401-a96b-2cf6edfed32a@example.com, CN=ClearPass Onboard Local Certificate Authority, O=Aruba Networks, L=Sunnyvale, ST=California, C=US
Issue Date/Time:
Feb 06, 2021 09:41:38 CST
Expiry Date/Time:
Feb 07, 2031 10:11:38 CST
Validity Status:
Valid
Serial Number:
1
NOTE: Publisher server's root certificate, shown above, will be added to the Certificate Trust List.
Enable to save the above certificate to Trust List and proceed with Make Subscriber operation.
Save
Cancel

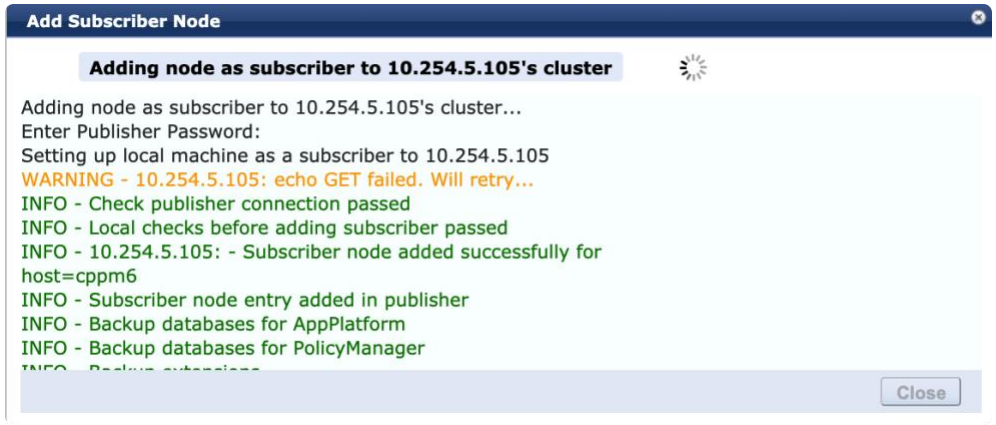

Add Subscriber Node
Adding node as subscriber to 10.254.5.105's cluster
Setting up local machine as a subscriber to 10.254.5.105
WARNING - 10.254.5.105: echo GET failed. Will retry...
INFO - Check publisher connection passed
INFO - Local checks before adding subscriber passed
INFO - 10.254.5.105: - Subscriber node added successfully for host=cppm6
INFO - Subscriber node entry added in publisher
INFO - Backup databases for AppPlatform
INFO - Backup databases for PolicyManager
INFO - Backup extensions
INFO - Stopping services
Close

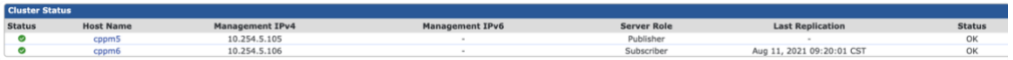


2） Pub 和 Sub 采用 Pub Onboard CA 来签发一张 HTTPs 证书，参考 arubase.club（https://arubase.club/archives/5509 ）网站介绍步骤。而 Database 证书仍然保持系统默认（注意这里不能是创建的自签证书），仍然可以完成 Cluster 集群设置。

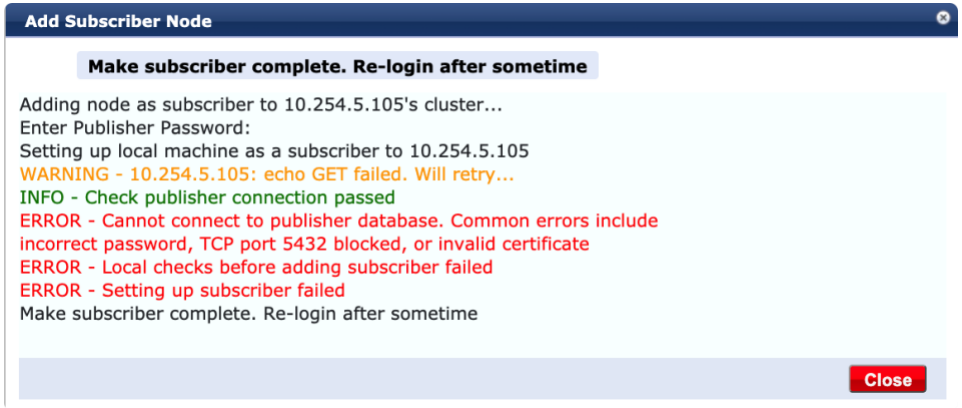


3） Pub 和 Sub 各自独立创建自签 HTTPs 证书，但是 Database 证书仍然是系统默认自带的。Cluster 集群可以成功建立。

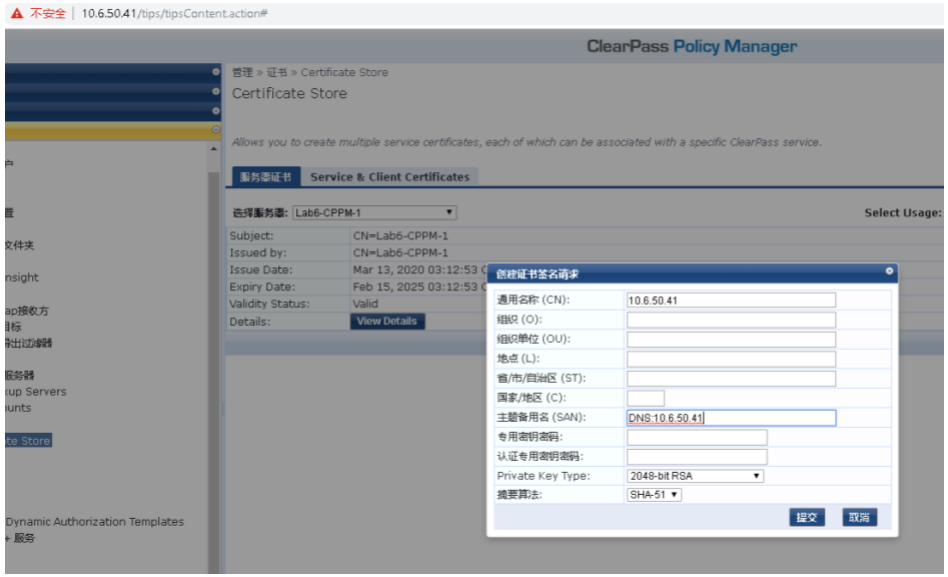




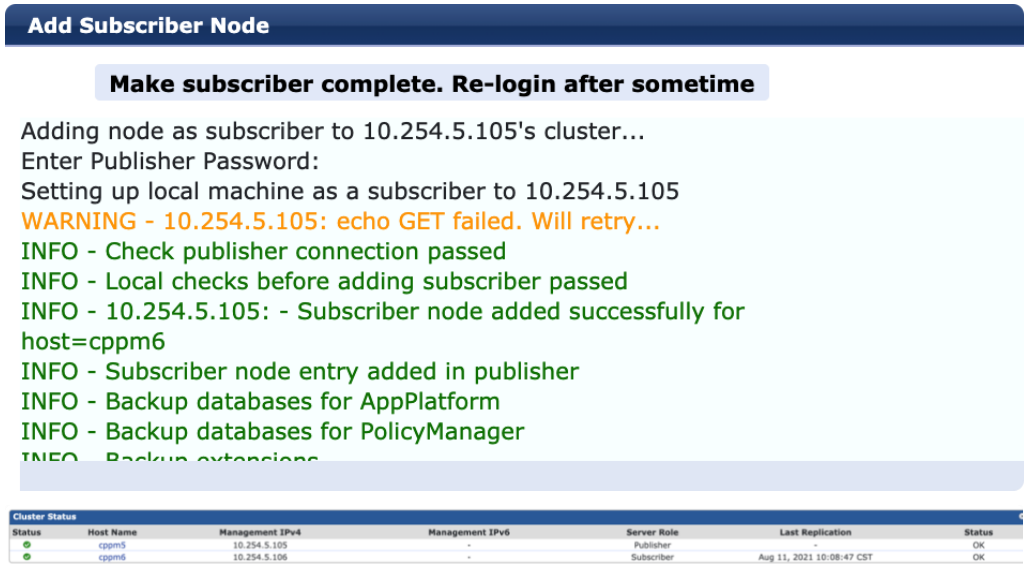
4） Pub 和 Sub 各自分别创建自签 HTTPs 证书，各自分别创建自签 Database 证书(CN=hostname 和 SAN=空，都是默认的)。 Cluster 建立不成功，其实是因为你自签了 Database 的证书，所以就出问题。



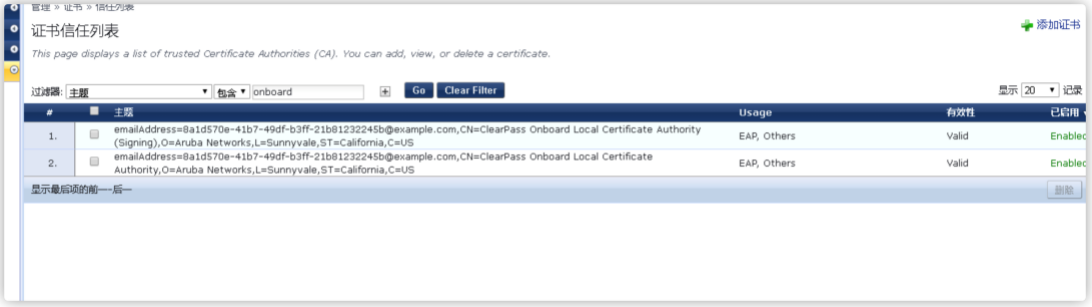
5） Pub 和 Sub 各自分别创建自签的 HTTPs 证书，然后 Database 证书都由 Pub Onboard CA 来统一签发。
（签发的时候，创建 CSR 时，要求 CN=mgmt-ip or SAN DNS:mgmt.-ip）
那么 Cluster 集群也是成功建立的。

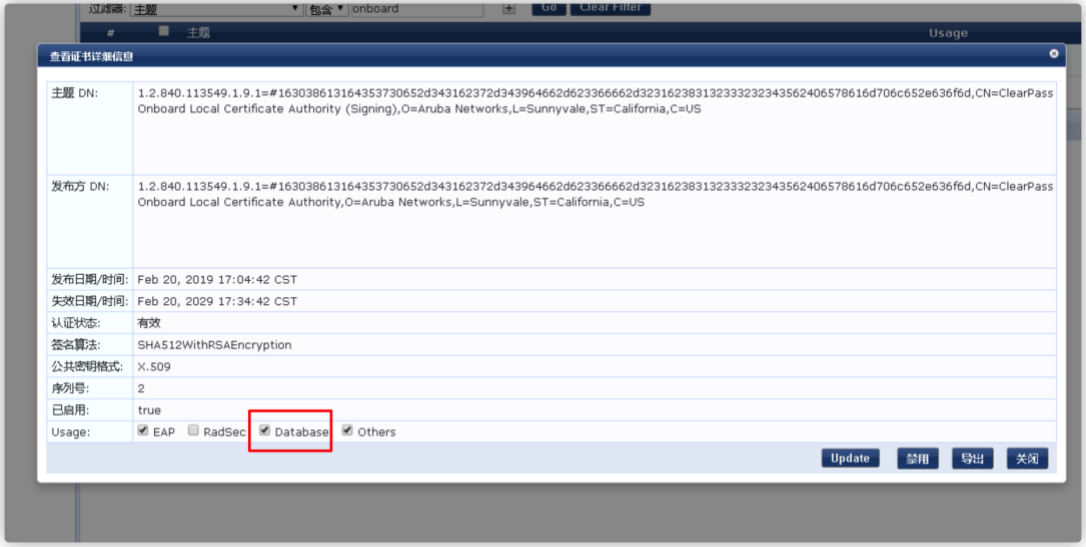


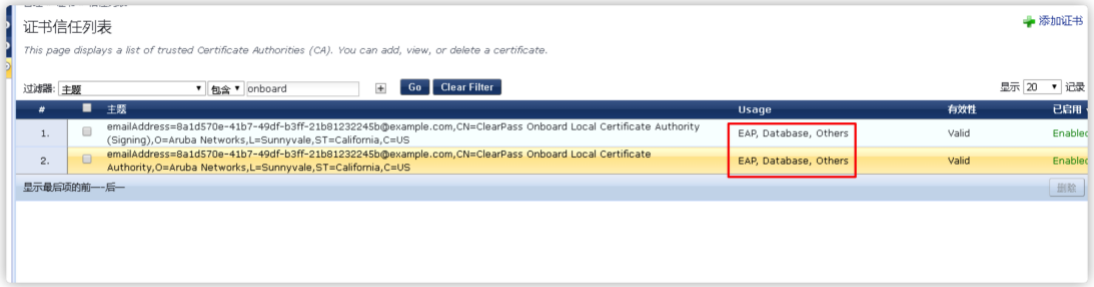
clearpass 6.9.6 自签 HTTPs 证书和 Pub Onboard CA 签发 Database 证书（CN:<MGMT-IP> or SAN:DNS:<MGMT-IP> ），可以成功创建 Cluster 集群。



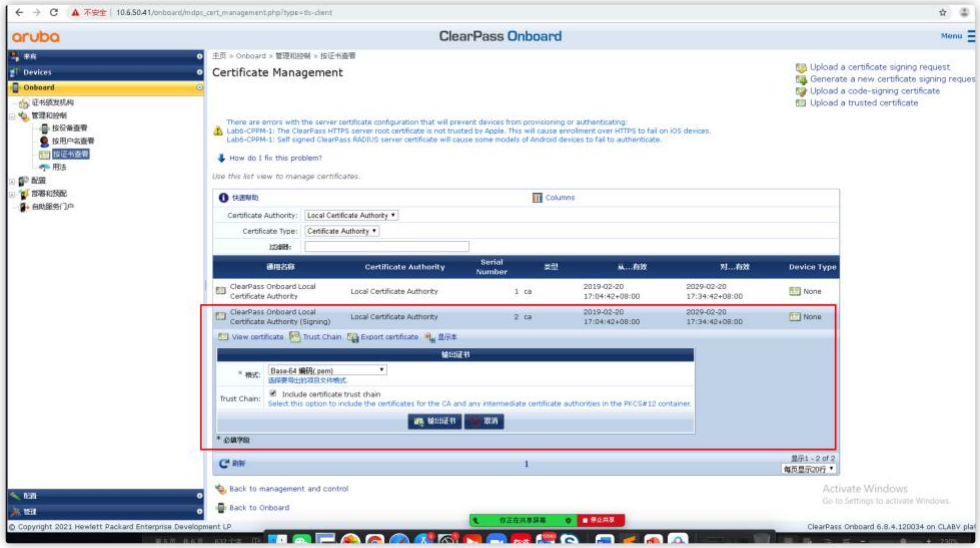
在导入到 Pub 时，需要在 Trust list 中找到两张 Onboard CA，修改 usage 类型，增加 Database，然后再将签发好的 database 证书导入到 Pub，需要系统重启一次


管理 » 证书 » 信任列表
证书信任列表
添加证书
This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.
过滤器: 主题 包含 onboard Go Clear Filter
显示 20 记录
主题 Usage 有效性 已启用
1. emailAddress=8a1d570e-41b7-49df-b3ff-21b81232245b@example.com,CN=ClearPass Onboard Local Certificate Authority (Signing),O=Aruba Networks,L=Sunnyvale,ST=California,C=US EAP, Others Valid Enabled
2. emailAddress=8a1d570e-41b7-49df-b3ff-21b81232245b@example.com,CN=ClearPass Onboard Local Certificate Authority,O=Aruba Networks,L=Sunnyvale,ST=California,C=US EAP, Others Valid Enabled
显示最后项的前一后一
删除

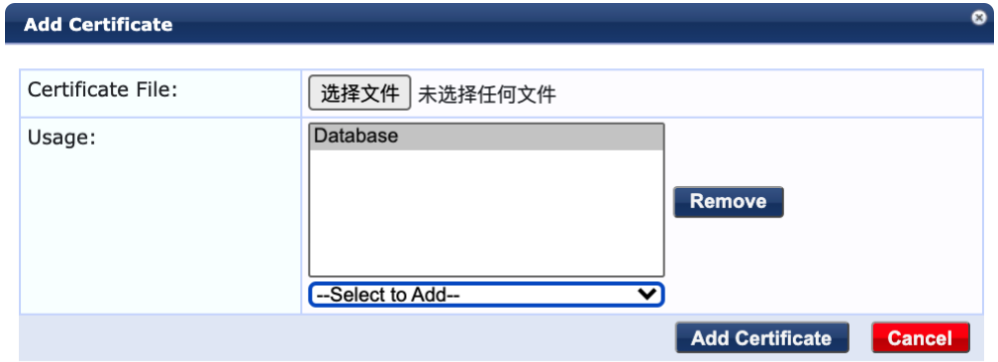

查看证书详细信息
主题 DN: 1.2.840.113549.1.9.1=#16303861316435373065 2d343162372d343964662d623366662d323162383132333232343562406578616d706c652e636f6d,CN=ClearPass Onboard Local Certificate Authority (Signing),O=Aruba Networks,L=Sunnyvale,ST=California,C=US
发布方 DN: 1.2.840.113549.1.9.1=#16303861316435373065 2d343162372d343964662d623366662d323162383132333232343562406578616d706c652e636f6d,CN=ClearPass Onboard Local Certificate Authority,O=Aruba Networks,L=Sunnyvale,ST=California,C=US
发布日期/时间: Feb 20, 2019 17:04:42 CST
失效日期/时间: Feb 20, 2029 17:34:42 CST
认证状态: 有效
签名算法: SHA512WithRSAEncryption
公共密钥格式: X.509
序列号: 2
已启用: true
Usage: EAP RadSec Database Others
Update 禁用 导出 关闭



在导入 Sub 前，需要先在 Pub CPPM onboard 上，将 onboard local certificate authority（signing）这张证书导出，格式选择.pem，包括 Trust Chain。



然后到 Sub 上，在证书的 Trust Isit 中，导入上面的证书，同时要选择 usage=Database



最后将签发好的 Database 证书导入到 Sub，需要系统重启一次

创建 Cluster 和相关证书方式的总结:

证书	系统初始化默认的自带方式	创建自签方式	采用 Pub Onboard CA 签发
HTTPs	可以 Cluster	可以 Cluster	可以 Cluster
Database	可以 Cluster	不可以 Cluster	可以 Cluster，但是创建 CSR 时，要求 CN=mgmt-ip or SAN DNS:mgmt.-ip

Honggang 还发现一个问题的提示 TIPS:

在 Pub 和 Sub 的受信任根证书 Trusted list 列表中，如果有多个其他 Onboard CA Root 证书的 usage 里也有选择 Database 的，需要先去掉，仅保留签发当前 Database 证书的 Onboard CA root 证书里添加 usage=Database 用途。honggang 认为多个 CA 根证书用途都指向 Database，可能会导致根证书出错，未经证实，但是可以值得注意。

另外提醒，在 v6.9.0 下，如果不打 path5 及以上的补丁，默认证书下，直接做 Cluster，那么会报下面的错误：

添加订阅者节点
Make subscriber complete. Re-login after sometime
正在将节点作为订阅者添加到 192.168.134.210 的群集...
Enter Publisher Password:
Setting up local machine as a subscriber to 192.168.134.210
WARNING - 192.168.134.210: echo GET failed. Will retry...
WARNING - 192.168.134.210: echo GET failed. Will retry...
ERROR - Publisher connection failed
ERROR - Connection to publisher failed. Please check that:
ERROR - 1) Publisher IP address and cluster password is valid and synchronized
ERROR - 2) Publisher is up and accessible from this machine
ERROR - 3) License is active
ERROR - Setting up subscriber failed
Make subscriber complete. Re-login after sometime