## ClearPass 6.8以上版本Cluster集群配置证书信任问题

### 开启Cluster集群注意事项

从ClearPass 6.8开始，建立集群和删除集群时增加了对Publisher和Subscriber HTTPs证书的校验。当Subscriber添加到Publisher时Subscriber会校验Publisher的HTTPs证书是否被信任，当在Publisher上删除Subscriber时，Publisher会校验Subscriber的HTTPs证书是否被信任，当证书校验不通过时会提示WARNING - 10.X.50.41: echo GET failed. 并且无法成功创建集群或者删除集群。

针对此情况，有两种解决方式：

1. 在ClearPass的CLI下通过命令将ClearPass转换为Subscriber，并通过设置参数来忽略对Publisher证书的校验，通过此方式可以成功将Subscriber加入到Publisher，但是在Publisher上通过命令删除Subscriber时无法通过设置参数来忽略对Subscriber证书的校验，所以会导致删除Subscriber失败；此方式不推荐

[appadmin@Lab5-CPPM-1]# **cluster make-subscriber -V -i 10.X.50.41**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \*

\* 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: **aruba123**

Setting up local machine as a subscriber to 10.1.50.41

INFO - Check publisher connection passed

INFO - Local checks before adding subscriber passed

INFO - 10.1.50.41: - Subscriber node added successfully for host=Lab5-CPPM-1

[appadmin@Lab5-CPPM-1]# cluster make-subscriber --h

ERROR: Invalid command-line argument

Usage:

make-subscriber -i <IP Address> [-l] [-b] [-V]

-i <IP Address> -- Publisher IP Address

-l -- Restore the local log database after this operation

-b -- Skip generating a backup before this operation

**-V -- Do not verify publisher certificate**

1. 分别在Publisher和Subscriber上创建证书签名请求CSR，通过CA（这里采用ClearPass Onboard）签发HTTPs证书，分别在Publisher和Subscriber上导入HTTPs证书，并在证书信任列表中导入对方的证书链。推荐采用此方式。

### 通过ClearPass Onboard给Publisher节点签发HTTPs证书

这里统一采用Publisher节点的Onboard给Publisher和Subscriber签发HTTPs证书。

**Publisher节点：**

1. 创建证书签名请求。打开Publisher ClearPass管理页面，打开 管理 -> 证书 -> Certificate Store ，点右上角的 创建证书签名请求 链接，创建一个新的证书签名请求。

* 通用名称（CN）：LabX-CPPM-1
* 专用密钥密码：aruba123
* 认证专用密码密码：aruba123

点“提交”按钮，在弹出的窗口中点“Download CSR”按钮下载CSR文件

手机截图图社交软件的信息

描述已自动生成

手机屏幕截图

描述已自动生成 社交网站的手机截图

描述已自动生成

1. 上传证书签名请求并生成HTTPS证书。在ClearPass Policy Manager页面的右上角点Menu图标手机屏幕的截图

   描述已自动生成，选择Onboard进入Onboard管理页面。打开 Onboard -> 证书颁发机构，点右边的Local Certificate Authority，选择 证书，点右上角的 Upload a certificate signing request 链接，在证书签名请求页面，

* Certificate Signing Request：点“选择文件”按钮打开刚才下载的CSR文件
* Certificate Type：HTTPS
* Approval：勾选Issue this certificate immediately
* Expiration： 1800天

点“Submit Certificate Signing Request”按钮提交

手机屏幕截图

描述已自动生成

社交网站的手机截图

描述已自动生成

社交网站的手机截图

描述已自动生成

手机屏幕截图

描述已自动生成

1. 导出HTTPS证书。在Certificate Type中选择HTTPS，点下面的LabX-CPPM-1证书，选择Export certificate，

* 格式：Base-64编码（.pem）
* Trust Chain：勾选Include certificate trust chain

点“输出证书”按钮导出证书

社交网络的手机截图

描述已自动生成

社交网络的手机截图

描述已自动生成

1. 导入HTTPS服务器证书，在ClearPass Onboard页面的右上角点Menu图标手机屏幕的截图

   描述已自动生成，选择Policy Manager进入ClearPass Policy Manager管理页面。打开 管理 -> 证书 -> Certificate Store ，点右上角的 导入服务器证书 链接，

* Certificate Type：服务器证书
* Usage：HTTPS Server Certificate
* 证书文件：点“选择文件”按钮选择刚才下载的证书文件

点“导入”按钮

手机屏幕截图

描述已自动生成

手机截图图社交软件的信息

描述已自动生成

手机屏幕截图

描述已自动生成

### 通过ClearPass Onboard给Subscriber节点签发HTTPs证书

这里统一采用Publisher节点的Onboard给Publisher和Subscriber签发HTTPs证书。

**Subscriber节点：**

1. 在Subscriber节点创建证书签名请求。打开Subscriber ClearPass管理页面，打开 管理 -> 证书 -> Certificate Store ，点右上角的 创建证书签名请求 链接，创建一个新的证书签名请求。

* 通用名称（CN）：LabX-CPPM-1
* 专用密钥密码：aruba123
* 认证专用密码密码：aruba123

点“提交”按钮，在弹出的窗口中点“Download CSR”按钮下载CSR文件

手机截图图社交软件的信息

描述已自动生成

手机屏幕截图

描述已自动生成 社交网站的手机截图

描述已自动生成

**Publisher节点：**

1. 在Publisher节点的Onboard中上传Subscriber节点的证书签名请求并生成HTTPS证书。打开Publisher ClearPass管理页面，通过在ClearPass Policy Manager页面的右上角点Menu图标手机屏幕的截图

   描述已自动生成，选择Onboard进入Onboard管理页面。打开 Onboard -> 证书颁发机构，点右边的Local Certificate Authority，选择 证书，点右上角的 Upload a certificate signing request 链接，在证书签名请求页面，

* Certificate Signing Request：点“选择文件”按钮打开刚才下载的CSR文件（Subscriber节点的CSR文件）
* Certificate Type：HTTPS
* Approval：勾选Issue this certificate immediately
* Expiration： 1800天

点“Submit Certificate Signing Request”按钮提交

手机屏幕截图

描述已自动生成

社交网站的手机截图

描述已自动生成

社交网站的手机截图

描述已自动生成

手机屏幕截图

描述已自动生成

1. 导出HTTPS证书。在Certificate Type中选择HTTPS，点下面的Subscriber节点的LabX-CPPM-1证书，选择Export certificate，

* 格式：Base-64编码（.pem）
* Trust Chain：勾选Include certificate trust chain

点“输出证书”按钮导出证书

手机截图图社交软件的信息

描述已自动生成

社交网站的手机截图

描述已自动生成

**Subscriber节点：**

1. Subscriber节点导入证书信任列表，未导入证书信任列表时无法导入通过Publisher Onboard签发的HTTPs证书。打开Subscriber ClearPass管理页面，打开 管理 -> 证书 -> 信任列表，点右上角的 添加证书 链接，导入刚才创建的Subscriber节点的HTTPs证书（里面包含证书信任关系）。

* 证书文件：点“选择文件”按钮选择刚才下载的证书文件（Subscriber节点的证书文件）
* Usage：Others

点“添加证书”按钮

手机截图图社交软件的信息

描述已自动生成

手机屏幕截图

描述已自动生成

1. Subscriber节点导入HTTPS服务器证书。打开 管理 -> 证书 -> Certificate Store ，点右上角的 导入服务器证书 链接，

* Certificate Type：服务器证书
* Usage：HTTPS Server Certificate
* 证书文件：点“选择文件”按钮选择刚才下载的证书文件（Subscriber节点的证书文件）

点“导入”按钮

手机截图图社交软件的信息

描述已自动生成

手机屏幕截图

描述已自动生成

Publisher和Subscriber的HTTPs证书导入成功后，即可正常生成和删除Subscriber操作，具体操作步骤可以参考ClearPass基础实验手册