LAB GUIDE

Secure RADIUS in AOS-CX

!!IMPORTANT!!

THIS GUIDE ASSUMES THAT THE AOS-CX SWITCH SIMULATOR HAS BEEN INSTALLED AND WORKS IN GNS3 OR EVE-NG. PLEASE REFER TO GNS3/EVE-NG INITIAL SETUP LABS IF REQUIRED.

AT THIS TIME, EVE-NG DOES NOT SUPPORT EXPORTING/IMPORTING AOS-CX STARTUP-CONFIG. THE LAB USER SHOULD COPY/PASTE THE AOS-CX NODE CONFIGURATION FROM THE LAB GUIDE AS DESCRIBED IN THE LAB GUIDE IF REQUIRED.

TABLE OF CONTENTS

Lab Objective

This workshop will provide guidance on how to configure and validate Secure RADIUS (RadSec) in AOS-CX.

Lab Overview

The RADIUS protocol uses UDP as underlying transport layer protocol. RadSec is a protocol that supports RADIUS over TCP and TLS. In conventional RADIUS requests, security is a concern as the confidential data is sent using weak encryption algorithms. The access requests are in plain text includes information such as a username, IP address, and so on. The user password is an encrypted shared secret. As a result, eavesdroppers can listen to these RADIUS requests and collect confidential information. Data protection is necessary in roaming environments where the RADIUS packets travel across multiple administrative domains and untrusted networks.

The RadSec module secures the communication between the switch and RADIUS server using TLS connection. Using RADIUS over TLS provides users with the flexibility to host RADIUS servers across geographies and WAN networks. For enabling RADIUS security, a CLI option tls is provided with the command radius-server host, where TLS stands for Transport Layer Security.

Advantages:

- Secures the communication between the switch and RADIUS server using a TLS session.
- Provides flexibility and enhances security to host RADIUS servers across geographies and WAN networks.
- Uses digital certificates to authenticate both client and server connection.

Lab Network Layout

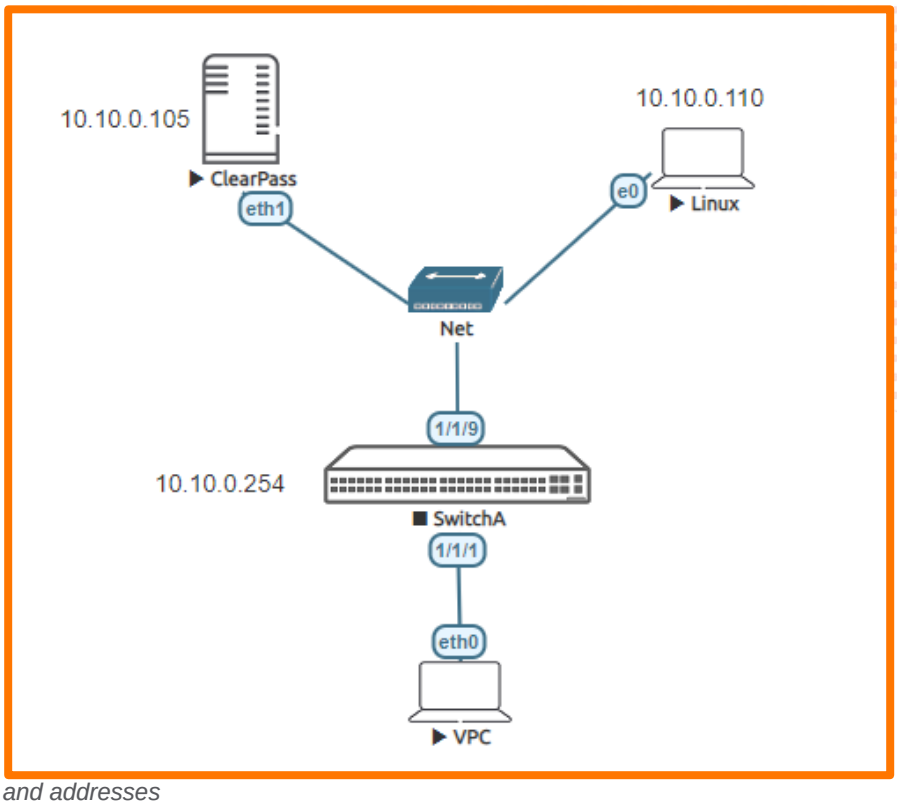

Figure 1. Lab topology and addresses

If using an external ClearPass, the topology would look like the example in Figure 2.

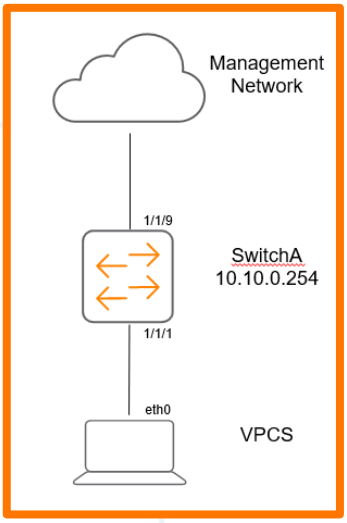

Figure 2. Example EVE-NG topology – external ClearPass

Lab Tasks

Task 1 - Lab setup

Note:

There are various ways to install a RADIUS server in EVE-NG. As this is an Aruba lab, ClearPass Policy Manager will be used. ***Refer to Appendix B*** to explore how to install ClearPass within EVE-NG, else you can point your EVE-NG instance and switch to the same network as the ClearPass server for RADIUS authentication. ClearPass will need to be accessible from a web browser to configure the enforcement policy if accessing outside of EVE-NG.

1. In GNS3/EVE-NG, create the topology as shown in Figure 1.
2. A Windows or Linux desktop will need to be pre-installed into EVE-NG to access ClearPass and configure. For the purposes of this lab, a customized EVE-NG Ubuntu server distribution was installed. Instructions on how to do this for EVE-NG environments can be found here:

   https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/
3. Install ClearPass into EVE-NG, if not using an external instance. Refer to Appendix B.
4. Start the devices.
5. Open the switch console and log in with the user “admin” and no password.
6. Change the password when prompted to the desired new password (ex: admin).
7. It is recommended as part of the lab to have a certificate authority available, either using Windows Server or ClearPass Onboard. It is recommended with ClearPass to have a publicly trusted certificate, however for this lab, Windows Server or OpenSSL can be used.

Task 2 – Switch Configuration

1. Change the switch hostname to SwitchA as shown in the topology

```
switch# configure
switch(config)# hostname SwitchA
SwitchA(config)#
```

2. On the switch, bring up the required uplink port.

```
SwitchA# configure
SwitchA (config)# int 1/1/9
SwitchA (config-if)# no shut
SwitchA (config-if)# no routing
```

3. Bring up the client port.

```
SwitchA# configure
SwitchA (config)# int 1/1/1
SwitchA (config-if)# no shut
SwitchA (config-if)# no routing
```

4. Configure the VLAN and gateway IP address that will be used for connectivity.

```
vlan 10
interface vlan 10
ip address 10.10.0.254/24
```

5. Configure the uplink port to be able to access the connectivity VLAN.

```
interface 1/1/9
no shutdown
no routing
vlan access 10
```

6. Validate the switch has connectivity to ClearPass.

```
Switch-A# ping 10.10.0.105
PING 10.10.0.105 (10.10.0.105) 100(128) bytes of data.
108 bytes from 10.10.0.105: icmp_seq=1 ttl=64 time=1.36 ms
108 bytes from 10.10.0.105: icmp_seq=2 ttl=64 time=2.17 ms
108 bytes from 10.10.0.105: icmp_seq=3 ttl=64 time=1.17 ms
108 bytes from 10.10.0.105: icmp_seq=4 ttl=64 time=1.05 ms
108 bytes from 10.10.0.105: icmp_seq=5 ttl=64 time=1.12 ms

--- 10.10.0.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.055/1.379/2.175/0.411 ms
```

7. From the configuration context, configure a local role on the switch using the `port-access role` command. This will be used to authenticate and test the RADIUS connection.

```
Switch-A(config)#
port-access role User1
poe-priority low
reauth-period 60
vlan access 10
```

Note: Ensure to add "`vlan access 10`" to test the client connectivity.

8. Configure the RADIUS Server (ClearPass) with tls enabled.

```
SwitchA(config)# radius-server host 10.10.0.105 tls
```

9. Create the Trusted Anchor Profile, which is the root or intermediate certificate from the Certificate Authority which does the digital signing of certificates. This is also used as the trusted root certificate for ClearPass. It is recommended to have a publicly trusted certificate for ClearPass installations, however for lab and demo purposes we can use Windows Server or OpenSSL to create a root certificate and to sign certificate requests.

```
SwitchA(config)#crypto pki ta-profile labdemo
```

10. Import the root certificate from the certificate authority that will be used for the lab.

```
SwitchA(config-ta-lab1)# ta-certificate import
Paste the certificate in PEM format below, then hit enter and ctrl+D:
SwitchA(config-ta-cert)#
```

Ensure the entire certificate is copied, including the last "end of certificate" message, and hit cntrl+D. Exit from the certificate context and validate the certificate was installed.

```
SwitchA(config)# show crypto pki ta-profile

TA Profile Name                 TA Certificate       Revocation Check
------------------------------- -------------------- ----------------
labdemo                         Installed, valid     disabled
```

11. Create the leaf certificate that will be used by the radsec client.

```
SwitchA(config)# crypto pki certificate labdemo
```

Create an request to sign the radsec client certificate.

```
SwitchA(config-cert-labdemo)# subject
Do you want to use the switch serial number as the common name (y/n)? n
Common Name: 10.10.0.105
Org Unit: tme
Org Name: aruba
Locality: roseville
State: ca
Country: us
SwitchA(config-cert-labdemo)# enroll terminal
You are enrolling a certificate with the following attributes:
Subject: C=us, ST=ca, L=roseville, OU=tme, O=aruba,
         CN=10.10.0.105
Key Type: RSA (2048)

Continue (y/n)? y

-----BEGIN CERTIFICATE REQUEST-----
<Certificate Contents>
-----END CERTIFICATE REQUEST-----
```

Note: Use the IP or FQDN of ClearPass in the common-name on the switch certificate signing request as well as on the ClearPass certificate signing request.

12. Sign the certificate with the chosen certificate authority. Copy the signed certificate back into the certificate profile as shown below. Ensure that cntrl+D is entered after certificate is entered.

```
SwitchA(config-cert-lab1)# import terminal ta-profile labdemo
  password  Specify the password to decrypt the imported data.
  <cr>
SwitchA(config-cert-lab1)# import terminal ta-profile labdemo
Paste the certificate in PEM format below, then hit enter and ctrl-D:
SwitchA(config-cert-import)#
```

Validate the certificate is installed correctly.

```
SwitchA(config)# show crypto pki certificate

Certificate Name                Cert Status    EST Status        Associated Applications
------------------------------- -------------- ----------------- ------------------------------
labdemo                         installed      n/a               none
local-cert                      installed      n/a               captive-portal, est-client, hsc,
https-server, syslog-client
```

Associate the certificate with the radsec application.

```
SwitchA(config)# crypto pki application radsec-client certificate labdemo
```

Verify the certificate is associated with RadSec.

```
SwitchA(config)# show crypto pki certificate

Certificate Name                Cert Status    EST Status        Associated Applications
------------------------------- -------------- ----------------- ------------------------------
labdemo                         installed      n/a               radsec-client
local-cert                      installed      n/a               captive-portal, est-client, hsc,
https-server, syslog-client
```

Task 3 – ClearPass Configuration

1. If running ClearPass from within the EVE-NG lab, open the Linux instance, log in using the credentials created in the Lab Setup Step 2 (default credentials - eve/eve).

Figure 3. Ubuntu Desktop in EVE-NG

2. Open the Firefox Web Browser in the Linux window and navigate to 10.10.0.105.

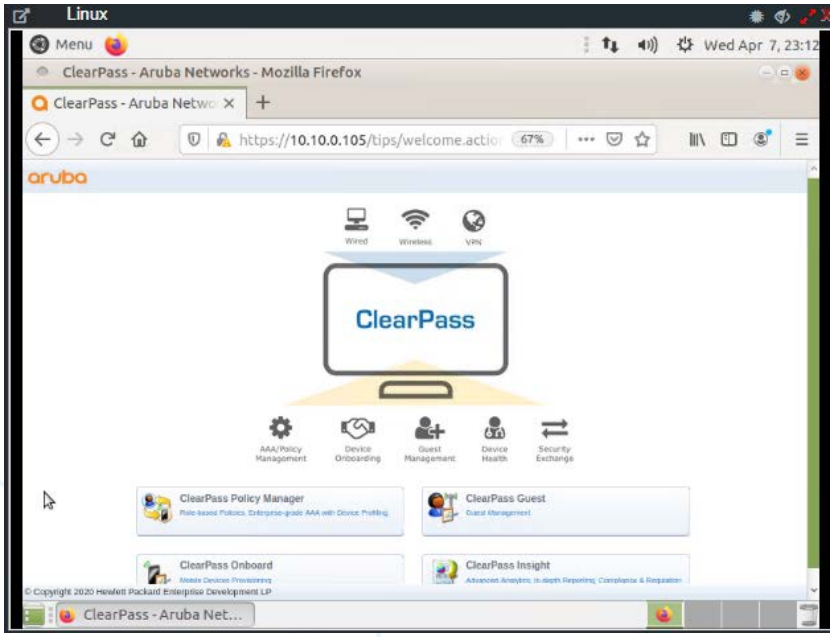

Figure 4. ClearPass Home Page in Ubuntu Window – EVE-NG

3. Click on the “ClearPass Policy Manager” Button and log into ClearPass with the following credentials, ‘admin/aruba123’.

Figure 5. ClearPass Login Screen

4. Navigate to “Configuration → Network → Devices” and click on Devices, then click on “Add”

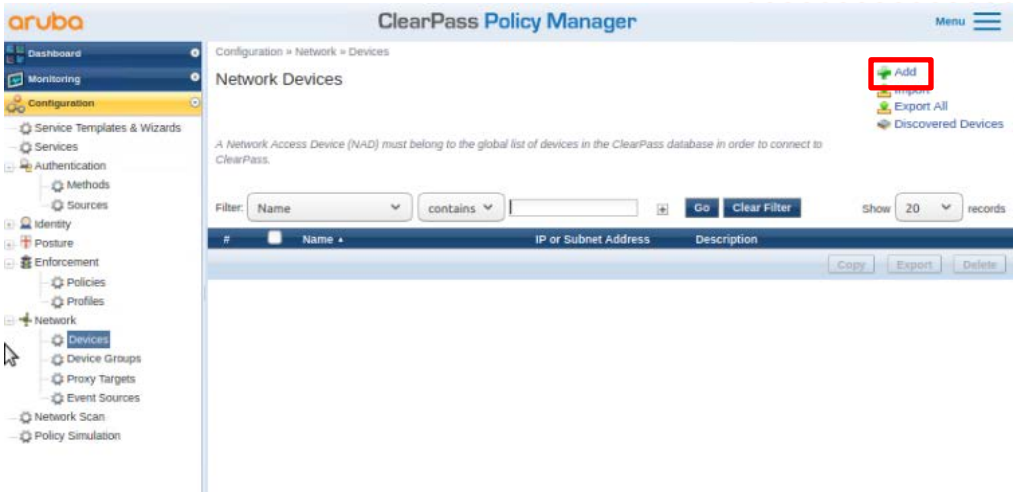

Figure 6. ClearPass Devices window

5. Enter the name of the Switch that will be identified as the authenticating device in ClearPass then enter the RADIUS key and confirm it. Ensure the RadSec check box is checked.

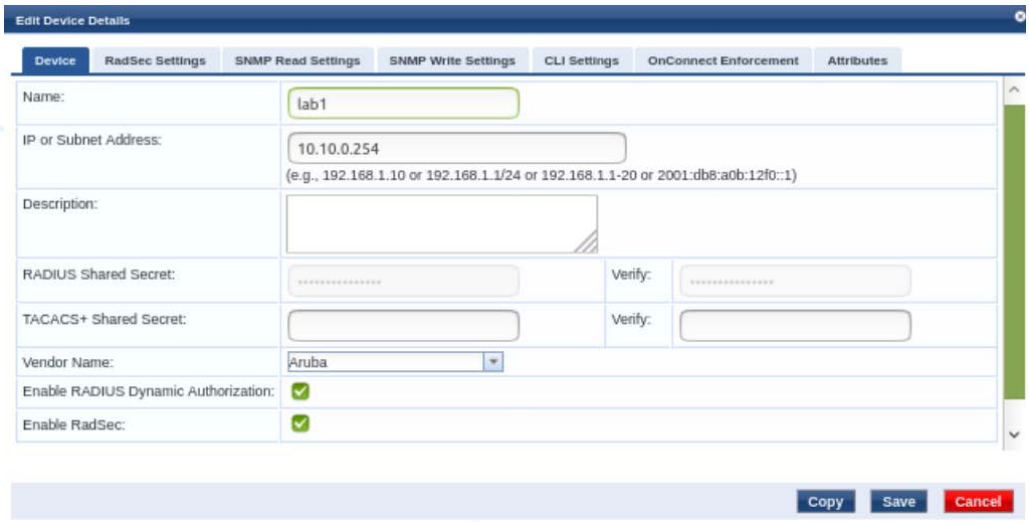

Figure 7. ClearPass Add Device Context

Note: The following steps are used to create a ClearPass Enforcement Policy for the purposes of this lab. For best practices in creating ClearPass enforcement policies in production environments, please refer to the ClearPass Policy Manager Documentation - https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/home.htm. Also note that this is using MAC Authentication. 802.1x can also be used but for the purposes of this lab.

6. Click on Configuration → Enforcement → Profiles → Add.

Figure 8. ClearPass Enforcement Profiles

7. Select the template “Aruba RADIUS Enforcement” and give the new profile a name (Ex: AOS-CX_ENFORCEMENT_PROFILE). Click Next.

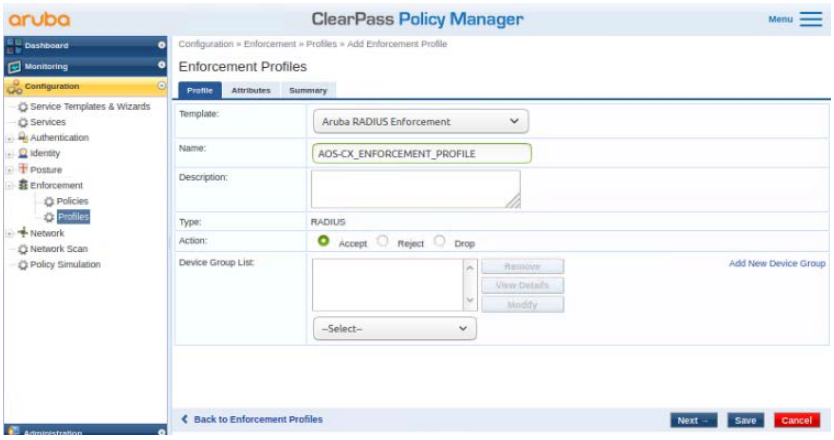

Figure 9. ClearPass Enforcement Profile creation

8. Select as type “Radius:Aruba”, Name “Aruba-User-Role”, and value as the value created in the switch setup, “User1”. Click the “Save” icon (floppy disk). Click Save.

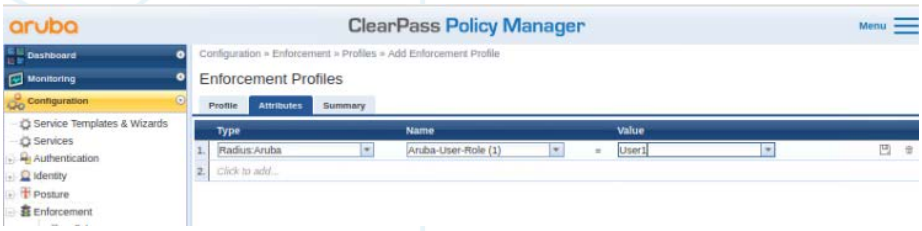

Figure 10. Aruba User Role Attribute creation

9. In ClearPass, click on Configuration → Services, then click on “Add”.

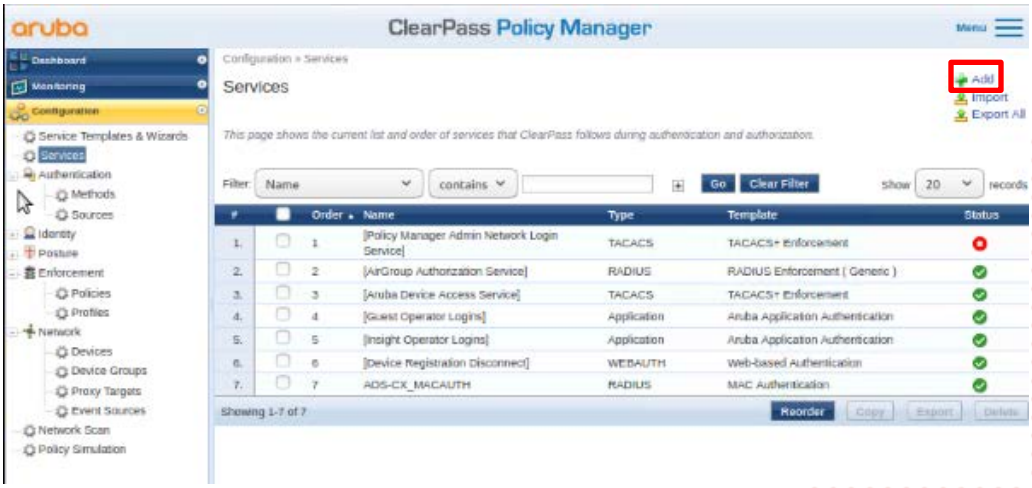

Figure 11. ClearPass Services

10. Select “MAC Authentication” from the drop down and give it a name (Ex: AOS-CX_MACAUTH). Click “Next”.

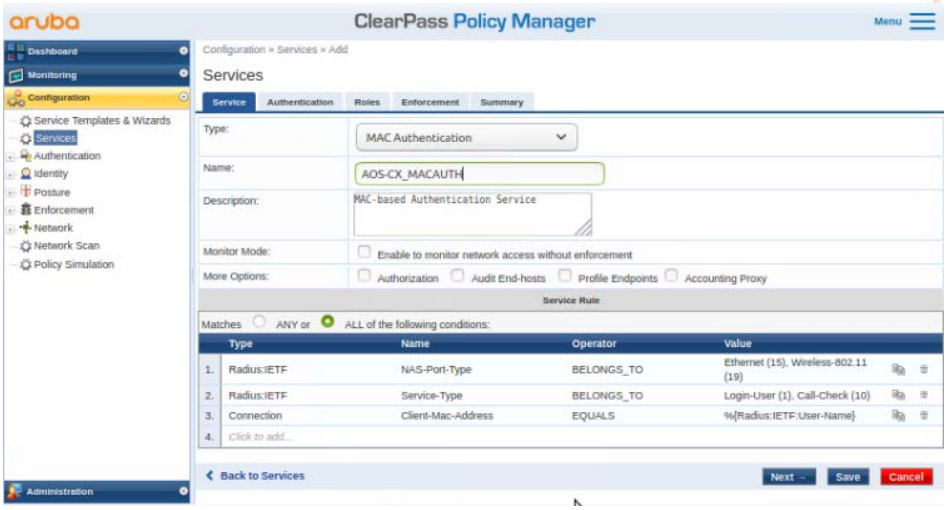

Figure 12. ClearPass MAC Authentication Service

11. Select “Endpoints Repository” from the “Authentication Sources” dropdown, then click “Next”. Click “Next” again to skip the configuration of roles (not needed for this lab).

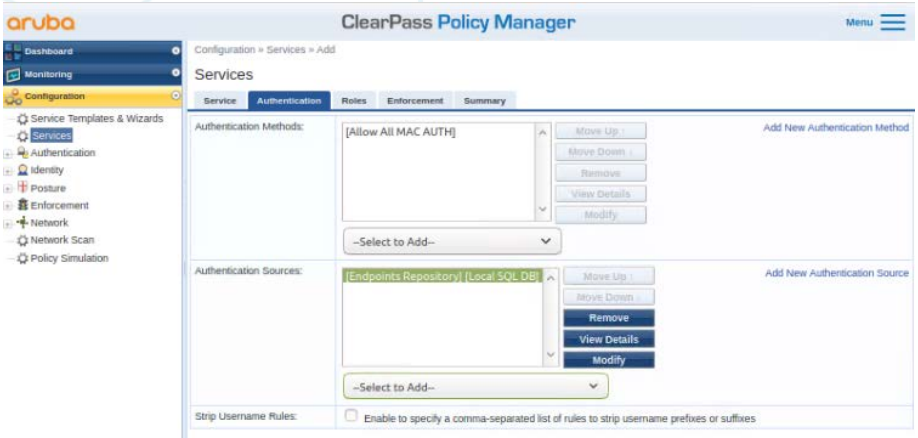

Figure 13. ClearPass MAC Authentication Sources

12. From the “Enforcement” tab, click on “Add New Enforcement Policy”.

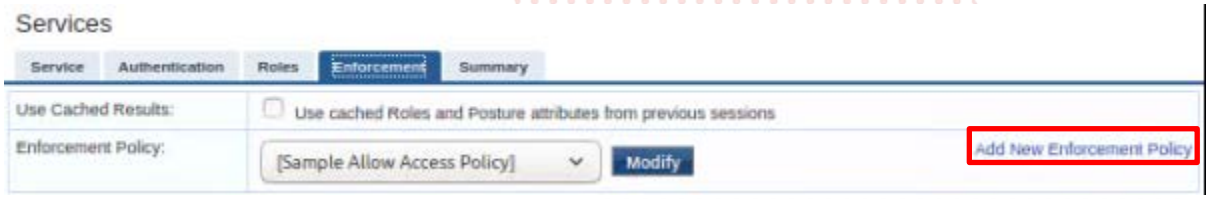

Figure 14. ClearPass Enforcement Policy

13. Give the new Enforcement Policy a name (Ex: AOS-CX_ENFORCEMENT) and select “Deny Access Profile” as the default profile. Click “Next”.

Figure 15. Adding a new Enforcement Policy

14. Click on “Add Rule”.

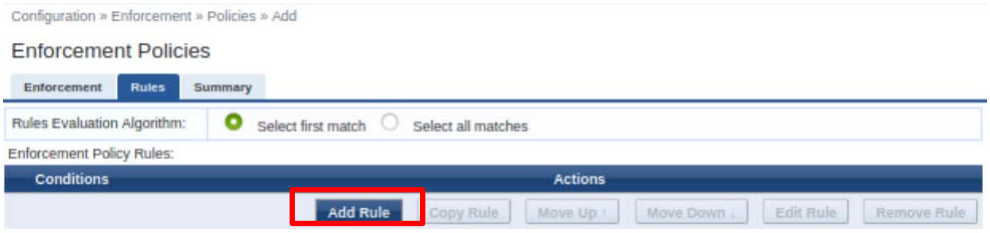

Figure 16. Adding a new Enforcement Policy

15. For the purposes of this lab, we will match on the client’s MAC address, this is the MAC address that was copied from the switch configuration. Enter the Type: Connection, Name: Client-Mac-Address-Colon, Operator: EQUALS, and Value as the client MAC Address previously retrieved. Click “Save” when finished.

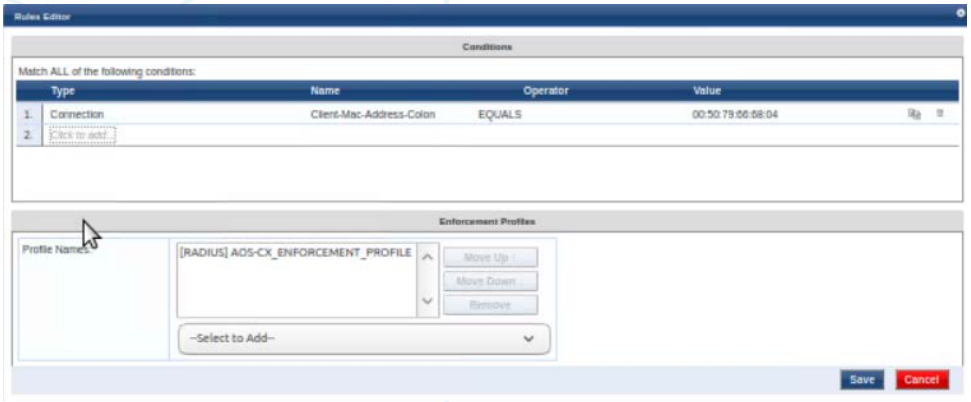

Figure 17. Adding a rule to an enforcement policy

16. Navigate in ClearPass to Administration → Certificates → Certificate Store. Select “RadSec Server Certificate”. Click on Create Certificate Signing Request.

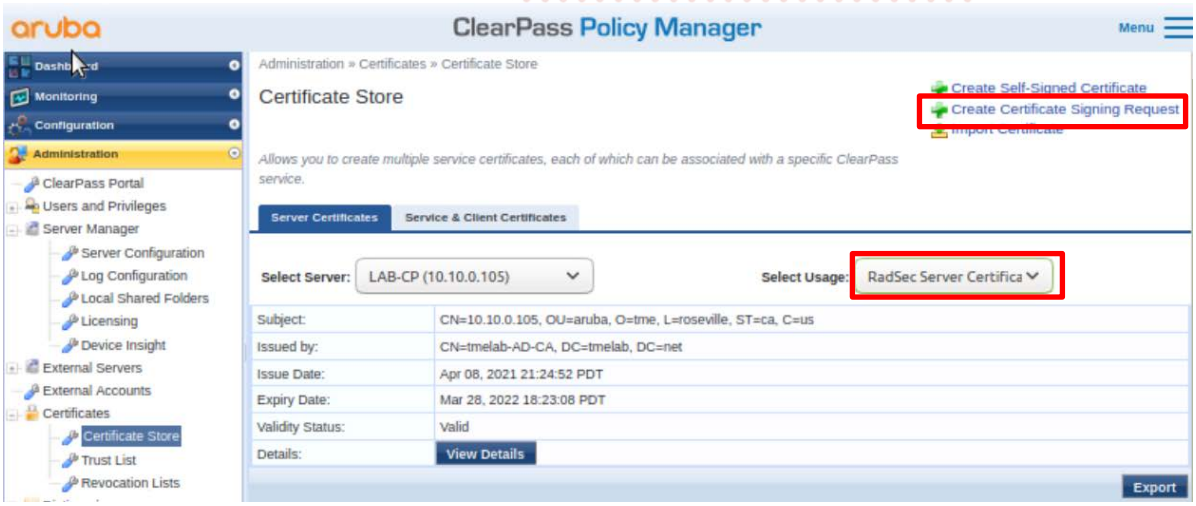

Figure 17. RadSec Certificate signing request

17. Fill in the certificate details that were also filled out on the switch certificate request. Ensure that the IP or FQDN of ClearPass is used as the Common Name of the Certificate.

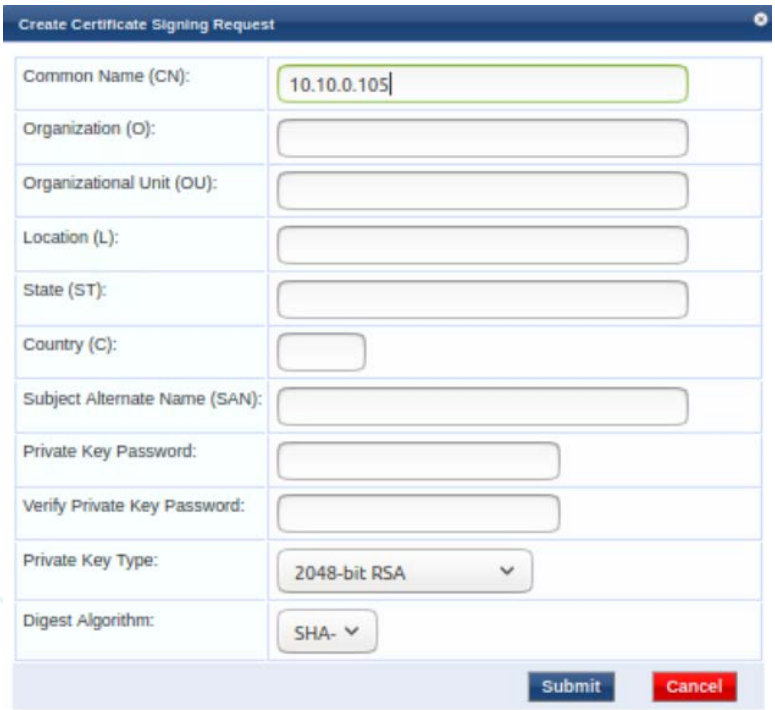

Figure 17. RadSec Certificate form

18. Copy the CSR file or copy and paste the contents to the Certificate Authority to be signed.

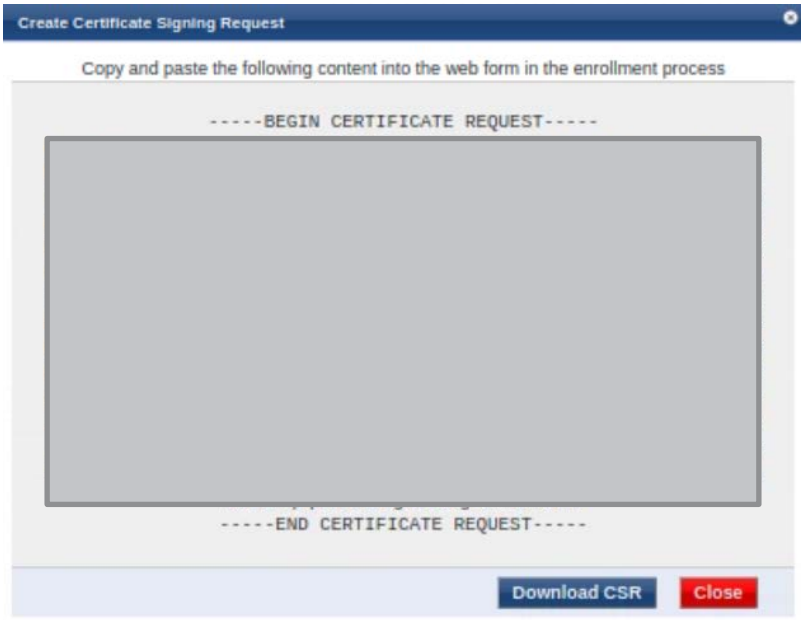

Figure 18. RadSec Certificate Signing Request Output

19. When the signed certificate is ready to be imported, click on “Import Certificate” link, then upload the signed certificate from the previous step.

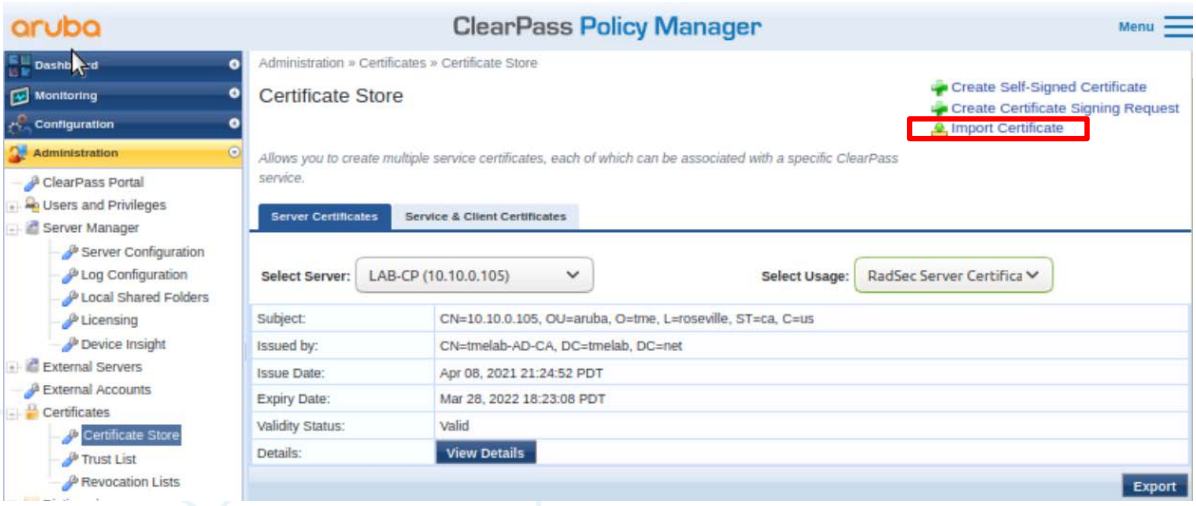

Figure 19. Certificate Import

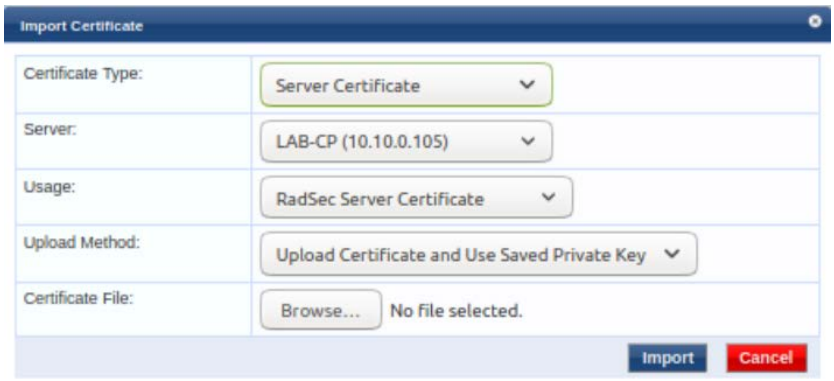

Figure 20. Signed RadSec Certificate Import Wizard

20. Verify that the TLS connection is working between switch and ClearPass using the command “show radius-server detail”.

```
SwitchA# show radius-server detail
******* Global RADIUS Configuration *******

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1

****** RADIUS Server Information ******
Server-Name              : 10.10.0.105
Auth-Port                : 2083
Accounting-Port          : 2083
VRF                      : default
TLS Enabled              : Yes
TLS Connection Status    : tls_connection_established
Timeout                  : 5
Auth-Type                : pap
Server-Group             : radius
Default-Priority         : 1
ClearPass-Username       :
ClearPass-Password       : None
Tracking                 : disabled
Tracking-Mode            : any
Reachability-Status      : unknown
Tracking-Last-Attempted  : N/A
Next-Tracking-Request    : N/A
```

If connection is not established, validate that the switch can reach the RADIUS server (ClearPass) as well as the certificates were installed correctly.

Task 4 – Client Verification and Troubleshooting

1. Open the switch console and run the command “show port-access clients”. You should see output like the following:

```
Switch-A# show port-acc clients

Port Access Clients

Status codes: d device-mode

--------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status      Role
                             Method
--------------------------------------------------------------------------------
  1/1/1    00:50:79:66:68:04 mac-auth       Success     User1
```

Note: If there is no client showing, check the access tracker in ClearPass to see if the authentication is successful. You can find that in Monitoring → Access Tracker. A successful authentication should appear as in Figure 15.

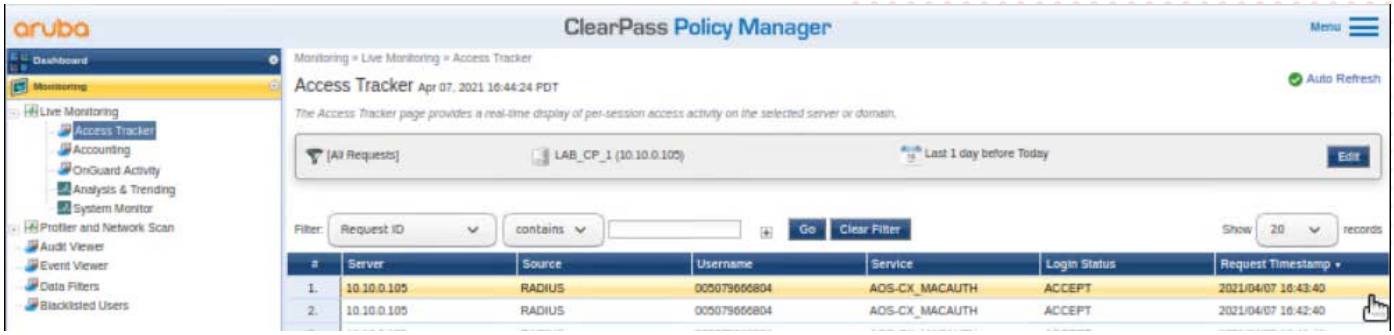

Figure 21. Successful Authentication in ClearPass Access Tracker

If the authentication were NOT successful, it would appear as a red line.

Figure 19. Unsuccessful Authentication in ClearPass Access Tracker

Click on the line and click on “Alerts” in the resulting window to see the reason why it was rejected.

Figure 22. Unsuccessful Authentication in ClearPass Access Tracker

Also ensure that the user role name on the switch matches what is in the Aruba-User-Role attribute configured in Step 15.

You have completed the lab!

Appendix A – Completed Switch Configuration

SwitchA

```
SwitchA# show run
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname SwitchA
user admin group administrators password ciphertext
AQBapWb/pjC9oE4MgWhwh9WkLL6NvS/EmwGKRxWt+OIQnNheYgAAABUKjRX/cKs2auHA+4U7ALtGRO0awqp4SK4gK47gGVK
nVWLCAro1tQ1NSeGnpZ/9yca734cQ6EokP6J0AWUCHaD2rF2rHwKiU5onKgbFhyY
9PSQIsyCjfPSrDEuCSpqs7T6w
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
radius-server host 10.10.0.105 tls
!
ssh server vrf default
ssh server vrf mgmt
crypto pki application radsec-client certificate labdemo
crypto pki ta-profile labdemo
    ta-certificate
        -----BEGIN CERTIFICATE-----
        MIIDYzCCAkugAwIBAgIQZiDAdPhWQqNE3PpMDBcTBjANBgkqhkiG9w0BAQsFADBE
        MRMwEQYKCZImiZPyLGQBGRYDbmV0MRYwFAYKCZImiZPyLGQBGRYGdG1lbGFiMRUw
        EwYDVQQDEwx0bWVsYWItQUQtQ0EwHhcNMTcwMzI5MDExMzA4WhcNMjIwMzI5MDEy
        MzA4WjBEMRMwEQYKCZImiZPyLGQBGRYDbmV0MRYwFAYKCZImiZPyLGQBGRYGdG1l
        bGFiMRUwEwYDVQQDEwx0bWVsYWItQUQtQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
        DwAwggEKAoIBAQDrdqdR2QQm4Lo3i/X9bvTu41cf3sVFzPFn727zlgrYySXWtyvW
        M3Jzf6P3FsqQzrsaP+QhlNsYMTrY2Yiccm7C9gNshpx95elzXsZ2TBP88qoUPD9F
        jH42YgnqAN61+opmct8aRgSJhTtKv+WEolVtLgL9/CL3zmvmbpz3oyYjF9W3lesp
        D52BeEbPqsBrALbYQypxJJLonZuueM7ePhSYbPnbrGuV8M9BiDyEyQ87OUYGgq7J
        krwjrer+BKYFIxqJQDHbY96ozbaUScv8nOylpUrH56r3jT5Xn05JDdOIJvBKniYK
        ZxIK+m4Mv2XS0zxuZBG1F1YDl/bcQ353jazbAgMBAAGjUTBPMAsGA1UdDwQEAwIB
        hjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQuBjOz0LpCALxkgy9bWbziV+1D
        UDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAydVR86YZez9N
        uIvJOftLczu0y3YfGoA5PK88Yv3TSMv+gxK5yiceU2HkV3PvVeCXyN9Nn9EUKLJ8
        87/BqDTsNKKD20axHNk/w2p5I8LY6g/Y8t3N84gXx3439+GezBdlxznEmWAhebAQ
        /JMnp+aD9Xhw9tgGeDXMB/GIhx0PCK22VbRUoDeZP3o+LmdB2fOdqhfN8+e2OMpz
        AGsBGGEJJWqOKSUkHC25Jkl0RfyymdxuWEflHofbF2DjSWheR023A5dA6a5WkxTV
        7WxwC8ekitnlY5BT2ZHV1LXLUsgvuN3j8G2+yvYiS6Z/da3ORb6Grm79sqZpzlKZ
        XWjU/zVxBQ==
        -----END CERTIFICATE-----
        END_OF_CERTIFICATE
debug radius all
vlan 1,10
interface mgmt
    no shutdown
    ip static 10.10.0.200/24
    default-gateway 10.10.0.254
port-access role User1
    vlan access 10
```

```
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access client-limit 5
    aaa authentication port-access mac-auth
        enable
interface 1/1/9
    no shutdown
    no routing
    vlan access 10
interface vlan 10
    ip address 10.10.0.254/24
!
!
!
!
!
https-server vrf mgmt
```

Appendix B – EVE-NG ClearPass Installation

Pre-Requisites:

- An Aruba Support Port account will be required to download the ClearPass OVA as well as EVAL licenses.

Steps

2. To first install the ClearPass OVA into the EVE-NG environment, follow the instructions at this link:

   https://www.eve-ng.net/index.php/documentation/howtos/howto-add-aruba-clearpass/

   This lab uses the latest ClearPass OVA v. 6.9.0, which can be downloaded from the Aruba Support Portal:

   https://asp.arubanetworks.com/downloads

3. Once installed, and the node is created in the EVE-NG lab file, follow the configuration steps for ClearPass. First login to ClearPass using the default credentials (appadmin/eTIPS123). Once entered, the configuration process will begin.

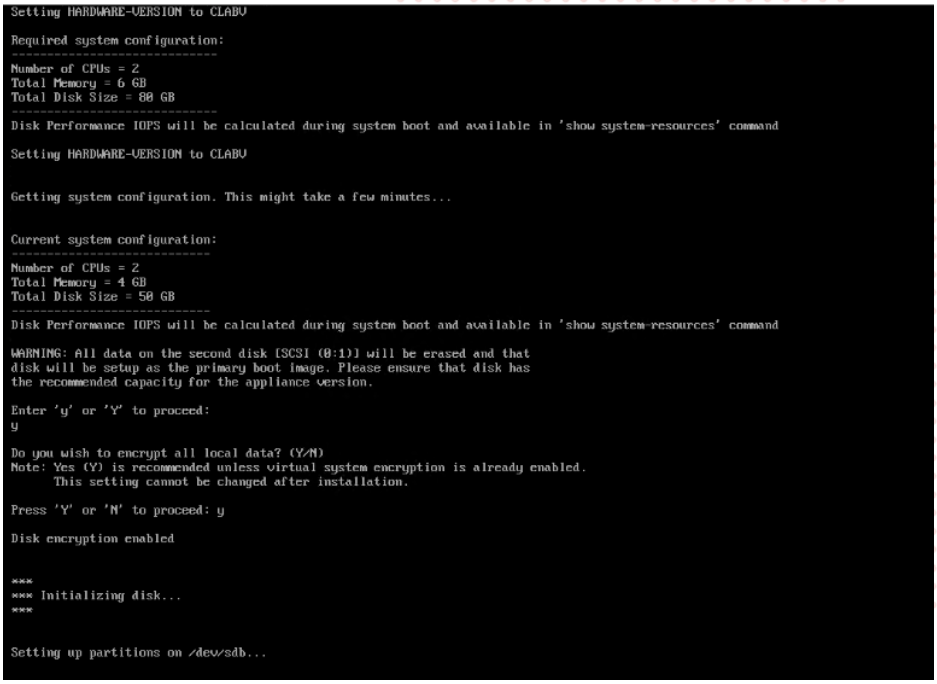

Figure 23. ClearPass Installation

Select the CLABV installation, click “Y” to proceed and “Y” to encrypt data.

4. Once prompted, enter the IP address as “10.10.0.105”, the mask as “255.255.255.0”, the gateway as “10.10.0.254”, and the DNS as “8.8.8.8” (not needed for this exercise). Configure a new password, this lab example used “aruba123”.

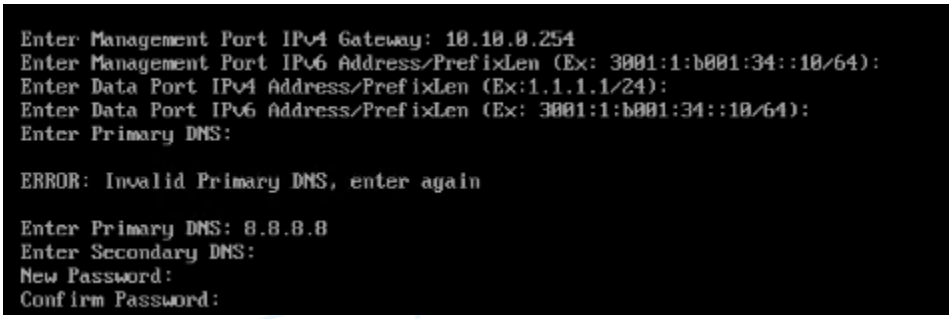

Figure 24. ClearPass IP Configuration

5. Configure the date and time manually as well as the time zone.

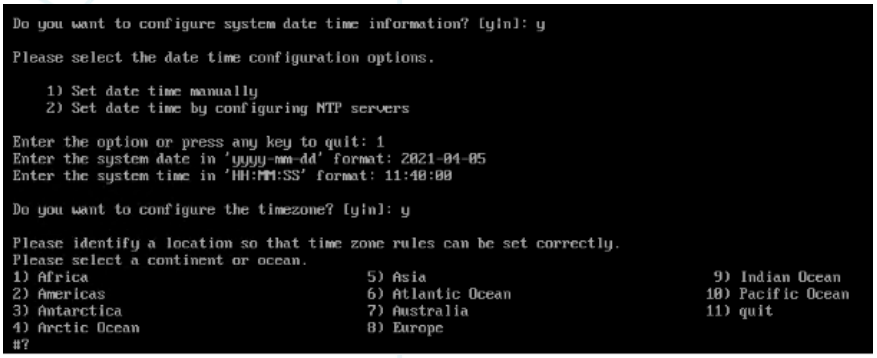

Figure 25. ClearPass Date and Time Configuration

6. Confirm the correct date, time, and time zone.

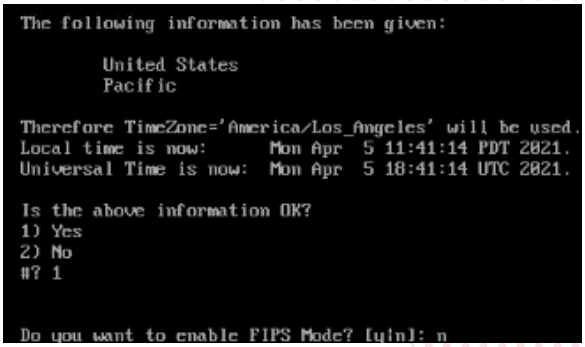

Figure 26. ClearPass Date and Time Settings Confirmation

7. Confirm the configured settings are correct. Press Y to save settings.

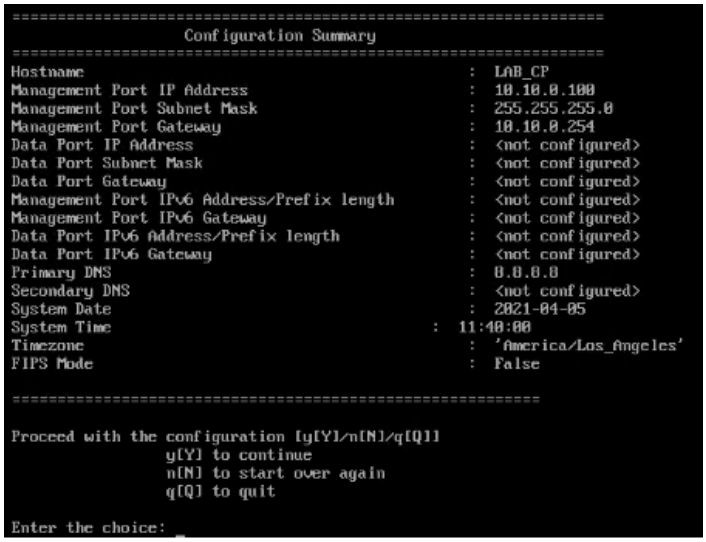

Figure 27. ClearPass Configuration Confirmation

8. ClearPass will then reboot and will then allow the user to log in to add licenses. Enter the platform license key retrieved from the Aruba Support Portal Licensing Management System - https://lms.arubanetworks.com/.

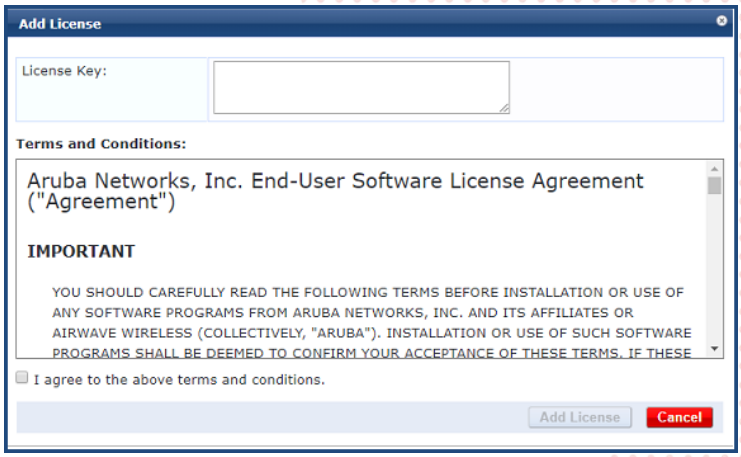

Figure 28. ClearPass Platform License entry

9. Once logged into ClearPass, enter the licensing section (Administration → Server Manager → Licensing). Click on "Add License".

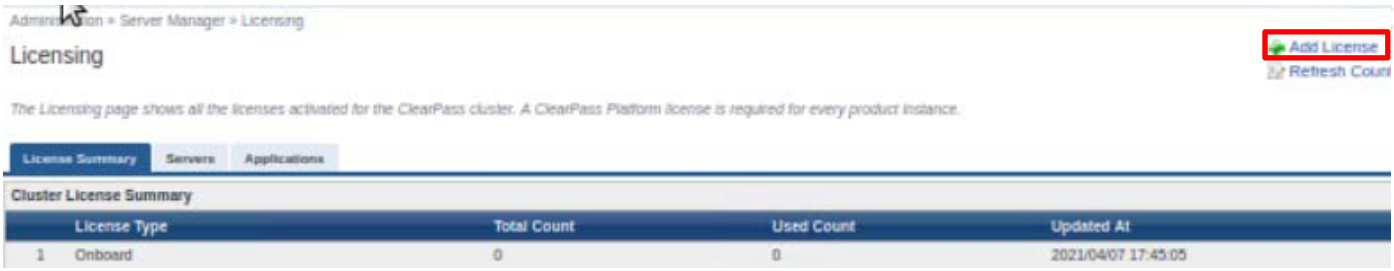

Figure 29. ClearPass Add New Server License

10. Add the new license and agree to the terms and conditions. ClearPass will then be ready to configure for authentication.

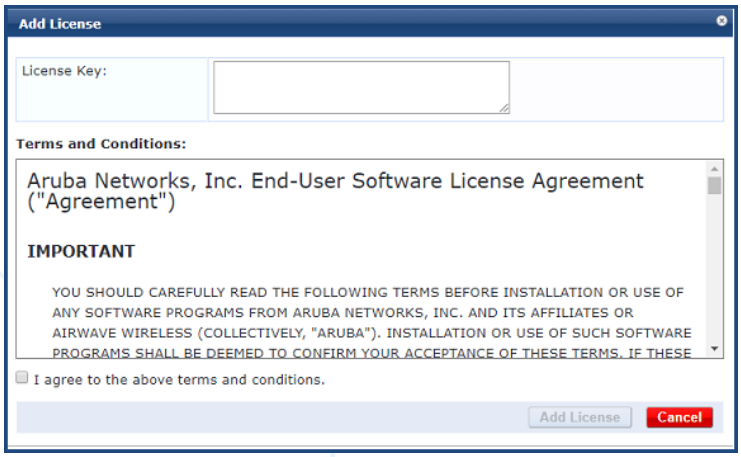

Figure 30. ClearPass Server license entry

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com