LAB GUIDE

Secure RADIUS in AOS-CX

.

.

a Hewlett Packard

1

.

.

.

!!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

Secure RADIUS in AOS-CX	•••••••••••••••••••••••••••••••••••••••
Lab Objective	
Lab Overview	
Lab Network Lavout	
Lab Tasks	
Task 1 - Lab setup	
Task 2 – Switch Configuration	
Task 3 – ClearPass Configuration	
Task 4 – Client Verification and Troubleshooting	
Appendix A – Completed Switch Configuration	
Appendix B – EVE-NG ClearPass Installation	

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 Guide SNMP in AOS-CX

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.
- 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 EVENG 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).
- 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.

```
Lab Guide
                                                                                      SNMP in AOS-CX
       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.

Lab Guide SNMP in AOS-CX 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-labl)# import terminal ta-profile labdemo
password Specify the password to decrypt the imported data.
 <cr>
SwitchA(config-cert-labl)# 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 local-cert https-server, syslog-client	installed installed	n/a n/a	radsec-client captive-portal, est-client, hsc,

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'.

oduna	ClearPass Policy Manager						
	You have 50 day(s) to activate the product						
	Admin Login						
	Usernane:			 			
	Passeval			 			
	Log In			 	• • •		•
				 	•••) • •) • •	
				 	• • •		•
Figure 5. ClearPass Login Screen				 			
		• • • • • • • • • • • • • • • • •		 			•
4. Navigate to "Configuration \rightarrow Network	→ Devices" and click on Devices, ther	ו click on "Add"	• • • • • • •	 	• • •		•
aruba	ClearPass Policy Manager	Menu		 			

aruba	ClearPass Policy Manager		Menu	•		•	
Dashboard 0	Configuration » Network » Devices					-	
Monitoring Q	Network Devices		🛖 Add				ļ
Contiguration			Export All	• •		•	
Service Templates & Wizards			Discovered Devices				
Q Services	A Network Access Device (NAD) must belong to the global list of devices in the Clear ClearDaws	rPass database in order to connect	(10				
- Authentication	- Setterm P. Marter				- 0	۰	•
- C Sources	Ellar Nama W costalar W	Til Co. Clear Filter	sheer 20 M month				
🗉 🚨 Identity	concains *	Go Clear Pitter	SHOW 20 + HECOIDS				
🕣 📅 Posture	# IP or Subnet Addre	ss Description					
Enforcement			Copy Export Defete				
- Q Policies							
- I Promes							
Devices							
Device Groups							
- 🗘 Proxy Targets							
- CE Event Sources							
Q Network Scan							
- LD Policy Simulation							

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.

Name:	(~
	lab1				
IP or Subnet Address:	10.10.0.254				
	(e.g., 192.168.1	.10 or 192.168.1.1/24	or 192.168.1.1-20 or 1	2001:db8:a0b:12f0::1)	
Description:					
RADIUS Shared Secret:			Verify:	1 + + + + + + + + + + + + + + + + + + +	
TACACS+ Shared Secret:	(Verify:		
Vendor Name:	Aruba	*			
Enable RADIUS Dynamic Authorization:					
Enable RadSec:					

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 \rightarrow Enforcement \rightarrow Profiles \rightarrow 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.

aruba		ClearPass Policy Manager	Menu 🚞
Dashboard O	Configuration = Enforcement	nt = Profiles = Add Enforcement Profile	
Configuration	Protile Attributes	Summary	
Service Templates & Wizards Services	Template:	Aruba RADIUS Enforcement	
Authentication Q identity	Name:	AOS-CX_ENFORCEMENT_PROFILE	
Posture B Enforcement Q Policies	Description:		
- O Profiles	туре:	RADIUS	
	Action:	Accept C Reject C Drop	
- Q Policy Simulation	Device Group List:	Visor Details Visor Details Middly	Add New Device Group
		Select- V	
	Sack to Enforcement	Profiles	Next - Save Cancel

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.

aruba			Clea	rPass Policy M	anager	r			Menu
Dashboard 0	0	onfiguration = Enforce	ment > Profiles =	Add Enforcement Profile					
Monitoring 0	E	Inforcement Pr	ofiles						
Configuration		Profile Attributes	Summary						
Service Templates & Wizards		Туре		Name			Value		
- Q Services	1.	Radius:Aruba		Aruba-User-Role (1)	*		User1	*	<u> </u>
2 identity	2.	Click to add							
Posture									
a Enforcement									

Figure 10. Aruba User Role Attribute creation

9. In ClearPass, click on Configuration \rightarrow Services, then click on "Add".

aruba				ClearPass	Policy M	lanager				Menu	\equiv						
Deshboard 0	Config	unation »	Service	9						_							
wantoring O	Serv	ices								Ad	1						
Scontiguration C										2 Exp	ont All						
© Service Templates & Wizards	This p	age shov	is the cu	ment list and order of service	s that ClearPass	්බේටහය ක්යාගල කැණ	ensis	ation and authorization.									
Authentication	Filter:	Name		✓ contains	*		÷.	Go Clear Filter	show	20 ~	ecords	•	•				
Sources			Orde	 Name 		Type		Template	-	State					-		
G Identity	L	0	1	[Policy Manager Admin N Service]	ietwork Login	TACACS		TACACS+ Enforcement		0		•	•	•	•	• •	
a Enforcement	2.		2	(AirGroup Authorization S	iervice]	RADIUS		RADIUS Enforcement (G	eneric)	0		•	•	•	•		
Q Policies	3.	0	3	[Aruba Device Access Se	rvice]	TACACS		TACACST Enforcement		0		•	• •	•	•	0 0	
- @ Profiles	4.	0	4	[Guest Operator Logins]		Application		Aruba Application Authen	cation	0		•	•	•	•		
- Network	5.	0	5	linsight Operator Logins!		Application		Aruba Application Author	ication	0							
- Q Devices	а.	0		Device Registration Disc	onnect]	WEDAUTH		Web-based Authentication		0							
Device Groups	7.	0	7	ADS-CX MACAUTH		RADIUS		MAC Authentication		0		•	• •				
C mont Science	Chevelo					270 C			100	20001	-	•	• •	•	•	•	
Ph Network Scan	Sidiat	ig 1-7 01	-					Rootcar	and the second	short 1 1 r	e ivia	•	• •	•	•	0 0	
D Policy Simulation																	



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

aruba		ClearPass Policy M	lanager		Menu	=
Dashboard 0	Configuration + 1	Services × Add				
Monitoring 0	Services					
Configuration O	Service Au	thentication Roles Enforcement Summary				
Service Templates & Wizards Services	Туре:	MAC Authentication	~			
 Q Identity 	Name:	AOS-CX_MACAUTH				
Posture BEnforcement Network	Description:	MAC-based Authentication Servio				
Q Network Scan	Monitor Mode:	Enable to monitor network acces	is without enforcement			
- Q Policy Simulation	More Options:	Authorization O Audit End-h	osts 🗍 Profile Endpoints 🗍	Accounting Proxy		
			Service Rule			
	Matches O	ALL of the following conditions:				
	Туре	Name	Operator	Value		
	1. Radius:IET	F NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)	99	ŧ
	2. Radius:IET	F Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	Ra	
	3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	Ra	
	4. Click to ack	£				
	& Back to Sen	vices		Next - Save	Can	cel
👰 Administration 🔹 💿				JEN JEN		

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).

aruba		ClearPass Policy Manager	Menu 🚞
Dashboard G	Configuration + Services + A Services	dd	
Configuration	Service Authentication	Roles Enforcement Summary	
Service Templates & Wizards Service Service Authentication density Possure Enforcement Network Network Scan	Authentication Methods:	[Allow All MAC AUTH] A Move Dow Hemove View Deter Modify -Select to Add-	Add New Authentication Method
- 22 Policy Simulation	Authentication Sources:	[Endpoints Repository] [Local SQL DB] Move Li Move De Remov View De Modifi -Select to Add- V	Add New Authentication Source ver zaits y
	Strip Username Rules:	Enable to specify a comma-separated list of rules to strip	username prefixes or suffixes

	Service Authentication Use Cached Results:	Roles Enforcement	Summary	ributes	hom pre	vious se	ssions	• • •			0 0 1	
-	Service Authentication	Roles Enforcement	Summary		Uncy	•••	• • •	• • •		• • •	5 0 0 1	
	Services		V Emoreen		Uncy	•••	• • •	• • •				
					Uncy	••••	• • •	• • •	• • •			
2. ⊢rom	the "Enforcement" tan) CIICK ON "Add New	/ Entorcom	nont L								
0 5	4h - "Enferrence" (- h		· • •	• • •		• • •	• • •	• • •	•••			
igure 13.	ClearPass MAC Auth	entication Sources	0 0 0 3 0 0	• • •	 	•••	• • •	• • •	•••	• • •		
			• • •	•••	• • • • • • • •	•••	•••	• • •	•••	• • ·		
									• • •	0 0		SNMP in AOS-
				• • • •	• • • •	• • •	• • •	•••	•••	••		Lab Gui
) 0 0 0) 0 0 0	•••	 		• • •			•••		

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".

aruba		ClearPass Policy Manager Menu	
Deshboard 0	Configuration + Enforcement	nt » Policies » Add	
Monitoring O	Enforcement Polic	ies	
Configuration	Enforcement Rules	Summary	
 Service Templates & Wizards Services 	Name:	AOS-CX_ENFORCEMENT	
Authentication Q Identity Posture	Description:		
Enforcement	Enforcement Type:	RADIUS O TACACS+ O WEBAUTH (SNMP/Agent/CLI/CoA) O Application O Event	
Network	Default Profile:	[Deny Access Profile] View Details Modify Add New Enforcement Profile	le

Figure 15. Adding a new Enforcement Policy

14. Click on "Add Rule".

Configuration » Enforcement »	icies » Add	
Enforcement Policies		
Enforcement Rules S	ary.	
Rules Evaluation Algorithm:	Select first match 🔘 Select all matches	
Enforcement Policy Rules:		
Conditions	Actions	
	Add Rule Copy Rule Move Up 1. Move Down 4. Edit Rule Rem	ove 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.

	Conditions		
Match ALL of the following	ng conditions:		
Туре	Name Operator	Value	
Connection Circk to sold]	Citers-Mac-Address-Colon EQUALS	00:50:79:66:58:04	B ₂ a
k	Enforcement Profiles		
Profile Names	[RADIUS] ADS-CX_ENFORCEMENT_PROFILE Move Up 1 Move Down Permove		
	-telert to add-		

Figure 17. Adding a rule to an enforcement policy

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

aruba		ClearPass Policy	Vlanager	Menu				
Dashb d	Administration » Certific	ates » Certificate Store						
Monitoring Configuration	Certificate Store		Create Se	elf-Signed Certificate ertificate Signing Reques				
Administration	Allows you to create mu	Itiple service certificates, each of which can	be associated with a specific ClearPass					
CreatPlass Portal CreatPlass Portal Server Manager P Server Configuration Change Configuration	Server Certificates	Service & Client Certificates						
- Decal Shared Folders	Select Server: LAB-	Select Usage: Radsec Server Certifica	a •					
Device Insight	Issued bu:	Chatmelab AD CA DC-tmelab DC-	L=IUSEVINE, ST=La, C=US					
External Servers	Issue Date:	Apr 08, 2021 21:24:52 PDT	Apr 08, 2021 21:24:52 PDT					
External Accounts	Expiry Date:	Mar 28, 2022 18:23:08 PDT						
Certificate Store	Validity Status:	Valid	Valid					
Provide Sold	Details:	View Details		Export				

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.

Create Certificate Signing Reques	đ.	•
Common Name (CN):	10.10.0.105	
Organization (O):		
Organizational Unit (OU):		
Location (L):		
State (ST):		
Country (C):		
Subject Alternate Name (SAN):		
Private Key Password:		
Verify Private Key Password:		
Private Key Type:	2048-bit RSA Y	
Digest Algorithm:	SHA- Y	
	Submit	Cancel

Figure 17. RadSec Certificate form

18. Copy the CSR file or copy and paste the contents to the Certificate Authority to be signed.	Lab Guide SNMP in AOS-CX
Create Certificate Signing Request	•
Copy and paste the following content into the web form in the enrollment process	
BEGIN CERTIFICATE REQUEST	0 0
END CERTIFICATE REQUEST	
Download CSR Close	
Figure 18 PadSac Cartificate Signing Paguest Output	

- 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.

aruba		ClearPass Policy	Manager	Menu
Dashb rd 0	Administration » Certificate	es » Certificate Store		
Monitoring O	Certificate Store	Create Self-Signed Certificate		
Configuration O				Create Centricate Signing Request
Administration	Allows you to create multip	le service certificates, each of which ca	n be associated with a specific Clear	Pass
ClearPass Portal ClearPass P	Server Certificates	ervice & Client Certificates		
- & Log Configuration - & Local Shared Folders	Select Server: LAB-CP	• (10.10.0.105)	Select Usage:	RadSec Server Certifica 🗸
Licensing	Subject:	CN=10.10.0.105, OU=aruba, O=tm	3, L=roseville, ST=ca, C=us	
- JP Device Insight	Issued by:	CN=tmelab-AD-CA, DC=tmelab, DC)=net	
External Servers	Issue Date:	Apr 08, 2021 21:24:52 PDT		
P External Accounts	Expiry Date:	Mar 28, 2022 18:23:08 PDT		
Certificate Store	Validity Status:	Valid		
J Trust List	Details:	View Details		
Prevocation Lists				Export

Figure 19. Certificate Import

• • • • •	• • • •	• • • •	• • • •	• • • •	• • • • •		• • • •		Lab Guide SNMP in AOS-CX
		-				•		۰	

Certificate Type:	Server Certificate	
Server:	LAB-CP (10.10.0.105) V	
Usage:	RadSec Server Certificate 🗸	
Upload Method:	Upload Certificate and Use Saved Private Key 🗸	
Certificate File:	Browse No file selected.	

Figure 20. Signed RadSec Certificate Import Wizard

20.	Verify that the TLS connection is working between switch and ClearPa	ass using the	e c	om	m	and	d "s	ho	w r	adi	us	se	rve	er c	leta	ail".	•	•••	•	•••	• •	
	SwitchA# show radius-server detail	• • •	•	•••	•	•••	•••	•	•••	•••	• •	•••	•••	•	•••	•••	•	•••	•	•••	• •	
	****** Global RADIUS Configuration ******	•	•	•••	•	•••	•••	•	• •	•••	• •	•••	•••	•	•••	•••	•	•••	•	•••	•••	
	Shared-Secret: None			•	•	••	•••	•	•••	• •	• •	•••	•••	•	•••	• •	• •	•••	•	•••	• •	
	Timeout: 5	n switch and ClearPass using the command "show radius-server detail". *******																				
	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 Info	ormation *****
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.

								SNI	Lab Guide	
Га	sk 4 – Clie	nt Verification an	d Troubleshoo	ting		, , , , , , , , , , , , , , , , , , ,	- 0 0 L 0 0			
۱.	Open the sw	itch console and run th	e command "show	port-access clien	ts". You sh	ould se	e output	like the fol	lowing:	
	Switch-A#	show port-acc cl	ients				0 0 0 L 0 0 0 0			
Port Access Clients					0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	6 C		
	Status coo	des: d device-mod	e	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	• • • •	
	Port	MAC-Address	Onboarding Method	Status	Role			0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		,) o o o o o o o
		00:50:79:66:68:	04 mac-auth	Success	Userl			• • • • • •) • • • } • • •

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 \rightarrow Access Tracker. A successful authentication should appear as in Figure 15.

aruba				ClearPa	ss Policy Manage	r		Menu
Dashtourd								
Monitoring	Auto Refresh							
HELINE Monitoring	The Act	cess Tracker page p	rowides a rea	s-time display of per-session	access activity on the selected se	rver or domain,		
Accounting	T P	W Requests]		[]] LAB_CP_1 (10.10	0.0.105)	tast 1 day befor	e Today	Edit
System Monitor Profiler and Network Scan	Filter	Request ID	~	contains v	Go Go	Clear Filter		Show 20 v record
Event Viewer		Server	_	Source	Username	Service	Login Status	Request Timestamp +
Data Filters	1.	10 10 0 105		RADIUS	005079666804	AOS-CX_MACAUTH	ACCEPT	2021/04/07 16:43:40
Blackisted Users	2.	10 10 0 105		RADIUS	005079666804	ADS-CX_MACAUTH	ACCEPT	2021/04/07 16:42:40
		And the second s						Concerns and the second s

Figure 21. Successful Authentication in ClearPass Access Tracker

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

13. 10.10.0.105 RADIUS 005079666804 AOS-CX_MACAUTH REJECT 2022/04/06 18:51:37

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.

Request Details		•
Summary	Input Output Alena	
Error Code:	206	
Error Category	Authentication failure	
Error Message	Access denied by policy	
Alerts for this	Request	
RADIUS (En App	dpoints Repository] - localhast: User not found. ilied 'Reject' profile	

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.



```
Lab Guide
SNMP in AOS-CX
```

Appendix A – Completed Switch Configuration

```
SwitchA
SwitchA# show run
Current configuration:
1
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname SwitchA
user admin group administrators password ciphertext
AQBapWb/pjC9oE4MgWhwh9WkLL6NvS/EmwGKRxWt+OIQnNheYgAAABUKjRX/cKs2auHA+4U7ALtGRO0awqp4SK4gK47gGVK
nVWLCAroltQ1NSeGnpZ/9yca734cQ6EokP6J0AWUCHaD2rF2rHwKiU5onKgbFhyY
9PSOIsyCjfPSrDEuCSpqs7T6w
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
1
ļ
L
1
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----
        MIIDYzCCAkuqAwIBAqIQZiDAdPhWQqNE3PpMDBcTBjANBqkqhkiG9w0BAQsFADBE
        MRMwEOYKCZImiZPyLGOBGRYDbmV0MRYwFAYKCZImiZPyLGOBGRYGdG11bGFiMRUw
        EwYDVQQDEwx0bWVsYWItQUQtQ0EwHhcNMTcwMzI5MDExMzA4WhcNMjIwMzI5MDEy
        MzA4WjBEMRMwEQYKCZImiZPyLGQBGRYDbmV0MRYwFAYKCZImiZPyLGQBGRYGdG11
        bGFiMRUwEwYDVQQDEwx0bWVsYWItQUQtQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
        DwAwggEKAoIBAQDrdqdR2QQm4Lo3i/X9bvTu41cf3sVFzPFn727z1grYySXWtyvW
        M3Jzf6P3FsqQzrsaP+QhlNsYMTrY2Yiccm7C9gNshpx95elzXsZ2TBP88qoUPD9F
        jH42YgnqAN61+opmct8aRgSJhTtKv+WEolVtLgL9/CL3zmvmbpz3oyYjF9W31esp
        D52BeEbPqsBrALbYQypxJJLonZuueM7ePhSYbPnbrGuV8M9BiDyEyQ870UYGqq7J
        krwjrer+BKYFIxqJQDHbY96ozbaUScv8nOylpUrH56r3jT5Xn05JDdOIJvBKniYK
        ZxIK+m4Mv2XS0zxuZBG1F1YD1/bcQ353jazbAgMBAAGjUTBPMAsGA1UdDwQEAwIB
        hjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQuBjOz0LpCALxkgy9bWbziV+1D
        UDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAydVR86YZez9N
        uIvJOftLczu0y3YfGoA5PK88Yv3TSMv+qxK5yiceU2HkV3PvVeCXyN9Nn9EUKLJ8
        87/BqDTsNKKD20axHNk/w2p518LY6g/Y8t3N84gXx3439+GezBdlxznEmWAhebAQ
        /JMnp+aD9Xhw9tgGeDXMB/GIhx0PCK22VbRUoDeZP3o+LmdB2f0dqhfN8+e20Mpz
        AGsBGGEJJWqOKSUkHC25Jkl0RfyymdxuWEflHofbF2DjSWheR023A5dA6a5WkxTV
        7WxwC8ekitnlY5BT2ZHV1LXLUsqvuN3j8G2+yvYiS6Z/da3ORb6Grm79sqZpz1KZ
        XWjU/zVxBO==
        -----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
```

	$b \circ \circ$	
	Lab Guide	
	SNMP in AOS-CX	
	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
aaa authentication port-access mac-au		
onchio		
ellable		
interface 1/1/1		
no shutdown	· · · · · · · · · · · · · · · · · · ·	
no routing		
vlan access 1)	
aaa authentication port-access cl	ient-limit 5	
aga authentication port-access ma	z-auth	
enable		
interface 1/1/9		
no shutdown	· · · · · · · · · · · · · · · · · · ·	
no routing	V 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
vlan access 10		••
interface vlan 10		•••
ip address 10.10.0.254/24	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	•••
-		• •
•		• •
!		• •
!		• •
1		
·	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	• •
nulps-server vri 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.

<u>Steps</u>

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.

Do you want to configure system date t	ime information? [y[n]: y								
Please select the date time configurat	ion options.								
1) Set date time manually 2) Set date time by configuring MT	P servers								
Enter the option or press any key to quit: 1 Enter the system date in 'yyyy-mm-dd' format: 2021-04-05 Enter the system time in 'HH:NM:SS' format: 11:40:00									
Do you want to configure the timezone?	'[yin]: y								
Please identify a location so that tim Please select a continent or ocean.	e zone rules can be set correctly.	9) Indian Ocean							
2) Americas	6) Atlantic Ocean	10) Pacific Ocean							
3) Antarctica	7) Australia	11) guit							
4) Arctic Ocean	8) Europe	TTA JOYO							
40									

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.

Configuration Summary		
Hostname Hostname Management Port IP Address Management Port Subnet Mask Management Port Gateway Data Port IP Address Data Port Gateway Management Port IPv6 Address/Prefix length Management Port IPv6 Gateway Data Port IPv6 Address/Prefix length Data Port IPv6 Address/Prefix length Data Port IPv6 Address/Prefix length		 LAB_CP 18.18.0.190 255.255.255.0 18.18.0.254 (not configured)
Frimary DNS Secondary DNS System Date System Time Timezone FIPS Mode		: 0.0.8.0 : 0.0.8.0 : <not configured=""> : 2021-04-05 11:40:00 : 'America/Los_Angeles' : False</not>
Proceed with the configuration [y[Y]/n[N]/q[Q] y[Y] to continue n[N] to start over again q[Q] to quit]	
Enter the choice:		

Figure 27. ClearPass Configuration Confirmation



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

			•	۰.																	
Add License		6	•	٠																	
			•	•	•																
License Key:			0 0 0	•		• • •															
			•	٠	•		•	٠													
Terms and Condition	ns:		•	٠	•		•	٠	•	•											
	de Tre End Heer Ceffrence Licence Agreement	*	•	•	•		•	•	•	•											
Aruba Netwo	ks, Inc. End-Oser Soltware License Agreement		•		•			•	•		•										
(Agreement			2						•												
IMPORTANT																					
YOU SHOULD C	REFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF																				
ANY SOFTWAR	PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR							•	•												
AIRWAVE WIRE	ESS (COLLECTIVELY, "ARUBA"), INSTALLATION OR USE OF SUCH SOFTWAR		•	•	•			•	•	• •		•	•			•	• •				•
PROGRAMS SH	LI BE DEEMED TO CONFIRM YOUR ACCEPTANCE OF THESE TERMS. IF THESE	-	•	•	•			•	•	• •		•	•	• •		•	•				•
PROGRAMS SH	LE BE BEENED TO CONTINUT FOR ACCEPTANCE OF THESE TERMS. IF THESE	_	•	•	•	• •	•	•	•	• •	•	•	•	• •	•	•	•			•	•
I agree to the abo	e terms and conditions.			•	•	• •	•	•	•	• •		•	•	• •		•	•				•
		_		•	•	• •	•	•	•	• •	•	•	•	• •	•	•	• •		• •		٠
	Add License Can	el	•	٠	•	• •	•	٠	•	• •	•	•	•		•	•	• •	0.0	• •	•	۰
			•	۰	•	• •	•	۰	•	• •	•	•	•	• •	•	٠	• •		• •		٠
	1000	0 0 0	•	٠	•	• •	•	٠	•	• •	•	•	•	• •	•	۰	0 0	5 0	• •		٠
	N 0.0 (• •	٠	•	• •	•	•	•	• •		0	•	• •		0	•	9 0		1.0	•
																					-

Figure 28. ClearPass Platform License entry

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

Adminis	Sion = Server Manager	Licensing								
Licensing										
The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.										
Licen	se Summary Servers	Applications								
Cluster	License Summary									
	License Type	Total Count	Used Count	Updated At						
1	Onboard	0	0	2021/04/07 17:45:05						

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