

集成指南

# 目录

简介	3
安全加入 – IEEE 802.1AR/802.1X	4
初始认证	4
配置	4
生产网络	4
配置 HPE Aruba Networking	5
配置 Axis	16
安全网络操作 – IEEE 802.1AE MACsec	19
HPE Aruba Networking ClearPass Policy Manager	20
HPE Aruba Networking 接入交换机	24
旧版板载 – MAC 身份验证	25
HPE Aruba Networking ClearPass Policy Manager	25
HPE Aruba Networking 接入交换机	33

### 简介

### 简介

本集成指南旨在概述如何在 HPE Aruba Networking 网络中加入和操作 Axis 设备的理想实践配置。配置使用现代安全标准和协议,如 IEEE 802.1X、IEEE 802.1AR、IEEE 802.1AE 和 HTTPS。

建立适当的网络集成自动化可以节省时间和财力。当将 Axis 设备管理应用程序与 HPE Aruba Networking 基础设施和应用结合使用时,它可以消除不必要的系统复杂性。以下是将 Axis 设备和软件与 HPE Aruba Networking 基础设施相结合时可以获得的一些优势**:** 

- 通过移除设备分级网络,尽可能地降低系统复杂性。
- 通过添加自动化入网流程和设备管理来节省成本。
- 利用 Axis 设备提供的零接触网络安全控制。
- 通过应用 HPE 和 Axis 专业知识来提高整体网络安全性。

在开始配置之前,必须准备好网络基础设施以安全地验证 Axis 设备的完整性。这允许在整个入网过程中逻辑网络之间进行软件定义的平滑过渡。在进行配置之前,有必要了解以下方面的知识:

- 通过 HPE Aruba Networking 管理企业网络 IT 基础设施,包括 HPE Aruba Networking 接入交换机和 HPE Aruba Networking ClearPass Policy Manager。
- 现代网络访问控制技术和网络安全策略的专业知识。
- 有关 Axis 产品的基本知识是必要的,但将在整个指南中提供。

#### 安全加入 – IEEE 802.1AR/802.1X

### 安全加入 - IEEE 802.1AR/802.1X



初始认证

连接 Axis Edge Vault 支持的 Axis 设备,以根据网络对设备进行身份验证。设备使用 IEEE 802.1AR Axis 设备 ID 证书通过 IEEE 802.1X 网络访问控制来验证自身身份。

为了授予网络访问权限,ClearPass Policy Manager 会验证 Axis 设备 ID 以及其他设备特定的指纹。MAC 地址和运行 AXIS OS 等信息用于做出基于策略的决策。

Axis 设备使用符合 IEEE 802.1AR 的 Axis 设备 ID 证书针对网络进行身份验证。

Axis 设备使用符合 IEEE 802.1AR 的 Axis 设备 ID 证书针对 HPE Aruba Networking 网络进行身份验证。

- 1 Axis 设备 ID
- 2 IEEE 802.1x EAP-TLS 网络身份验证
- 3 接入交换机(验证器)
- 4 ClearPass 策略管理器

### 配置

身份验证之后,Axis 设备将进入安装了AXIS Device Manager 的调配网络(VLAN201)。通过 AXIS Device Manager,可以执行设备配置、安全强化和 AXIS OS 更新。为了完成设备配置,新的客户特定生 产级证书将上传到设备上以用于 IEEE 802.1X 和 HTTPS。

身份验证成功后,Axis 设备将进入配置网络进行配置。

- 1 接入开关
- 2 配置网络
- 3 ClearPass 策略管理器
- 4 设备管理应用

#### 安全加入 - IEEE 802.1AR/802.1X

#### 生产网络

为 Axis 设备配置新的 IEEE 802.1X 证书会触发新的身份验证尝试。ClearPass Policy Manager 验证新 证书并决定是否将 Axis 设备移至生产网络中。

设备配置后, Axis 设备离开配置网络并尝试针对网络重新进行身份验证。

- 1 Axis 设备 ID
- 2 IEEE 802.1x EAP-TLS 网络身份验证
- 3 接入交换机(验证器)
- 4 ClearPass 策略管理器

重新验证后, Axis 设备移至生产网络(VLAN 202)。在该网络中, Video Management System (VMS) 连接到 Axis 设备并开始运行。

Axis 设备被授予对生产网络的访问权限。

- 1 接入开关
- 2 生产网络
- 3 ClearPass 策略管理器
- 4 视频管理系统

### 配置 HPE Aruba Networking

#### HPE Aruba Networking ClearPass Policy Manager

ClearPass Policy Manager 为跨多供应商的有线、无线和 VPN 基础设施的 IoT、BYOD、企业设备、员工、承包商和访客提供基于角色和设备的安全网络访问控制。

#### 可信证书存储配置

- 1. 从 axis.com 下载 Axis 特定的 IEEE 802.1AR 证书链。
- 2. 将 Axis 特定的 IEEE 802.1AR 根 CA 和中间 CA 证书链上传到受信任的证书存储中。
- 3. 启用 ClearPass Policy Manager 以通过 IEEE 802.1X EAP-TLS 对 Axis 设备进行身份验证。
- 4. 在使用字段中选择 EAP。这些证书用于 IEEE 802.1X EAP-TLS 身份验证。

### 安全加入 - IEEE 802.1AR/802.1X



将特定于 Axis 的 IEEE 802.1AR 证书上传到 ClearPass Policy Manager 的可信证书存储区。

ClearPass Policy Manager - Arub × +					~	- 0 ×
← → C ▲ Inte säker   https://172.25.2	201.120/tips/tips	Content.action#tipsCertTrustList.action			lê 🕯	r 🛛 🛎 E
aruba			ClearPass Policy Manager			Menu 📕
Dashboard	• Adminis	ration » Certificates » Trust List				
Monitoring	• Certif	icate Trust List				🛶 Add
Configuration	• This pag	e displays a list of trusted Certificate Au	uthorities (CA). You can add, view, or delete a certificate	e.		
- 🎤 ClearPass Portal	Filter: S	ubject 🗸 contains 🗸	axis device 🛨 Go Clear Filter		Show	20 v records
🕀 🔒 Users and Privileges		Subject 🔹		Usage	Validity	Enabled
Berver Manager     Bervers	1.	CN=Axis device ID Root CA RSA	A,O=Axis Communications AB	EAP	Valid	Enabled
- P External Accounts	2.	CN=Axis device ID Root CA ECC	C,O=Axis Communications AB	EAP	Valid	Enabled
🖃 🚆 Certificates	3.	CN=Axis device ID Intermediate	e CA RSA 2,0=Axis Communications AB	EAP	Valid	Enabled
- Dertificate Store	4.	CN=Axis device ID Intermediate	e CA RSA 1,0=Axis Communications AB	EAP	Valid	Enabled
- January List	5.	CN=Axis device ID Intermediate	e CA ECC 2,0=Axis Communications AB	EAP	Valid	Enabled
- Je Revocation Lists	6.	CN=Axis device ID Intermediate	e CA ECC 1,0=Axis Communications AB	EAP	Valid	Enabled
Agents and Software Updates	Showing	1-6 of 6				Delete
in na support						
© Copyright 2022 Hewlett Packard Enterprise	Development I	P Nov	25, 2022 08:48:50 CET	ClearPass Policy Manager 6.9.12.13	5929 on CLABV (Trial	Version) platform

ClearPass Policy Manager 中的可信证书存储包含特定于 Axis 的 IEEE 802.1AR 证书链。

#### 网络设备/组配置

- 1. 将受信任的网络访问设备(例如 HPE Aruba Networking 访问交换机)添加到 ClearPass Policy Manager。ClearPass Policy Manager 需要知道网络中的哪些接入交换机用于 IEEE 802.1X 通信。
- 使用网络设备组配置将多个可信网络访问设备分组。对受信任的网络访问设备进行分组可以 更轻松地进行策略配置。
- 3. RADIUS 共享密钥需要与特定交换机 IEEE 802.1X 配置相匹配。

### 安全加入 – IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub × +							~	-		<
← → C ▲ Inte säker   https://172.2	5.201.120/tips/tipsContent.action#t	ipsNetworkDevices.action					E	? ☆ [	a 🔹	
aruba		(	ClearPass Po	olicy Manag	er			P	1enu 🚍	
Dashboard	O Configuration » Network	k » Devices								
Monitoring	• Network Device	s					*	Add		
& Configuration	0							Import Export A		
- 🛱 Service Templates & Wizards							•	Discoven	ed Devic	!S
- 🛱 Services	A Network Access Devic	e (NAD) must belong to the	global list of devices i	n the ClearPass dat	abase in order to connect	to ClearPass.				
Authentication										
Dentity     Posture	Filter: Name	✓ contains ✓		+ Go Clear I	ilter		5	show 20	✓ record	:ls
Enforcement	# 🗖 Name	<u>۸</u>	IP or Subnet A	ddress	Device Groups		Description			
E-+Network							Сору	Export	Delet	
Devices										
Provy Targets										
- Ö Event Sources										
- 🛱 Network Scan										
- 🛱 Policy Simulation										
Administration		Day 20	0000 00-01-17 CET			Class Dellas Mass	6 0 10 106000 0 404	(Toisly) (see	in a lab	
© copyright 2022 newlett Packard Enterpris	e Development LP	Dec 28, .	1022 09.01:17 CET			Clearedss Policy Plana	ger 0.5.12.150929 00 CLABV	, mai vers	ion) placi	10

ClearPass Policy Manager 中的可信网络设备接口。

Q ClearPass Policy Manager - Arub × +				~ - O X
← → C ▲ Inte säker   https://172.2	5.201.120/tips/tipsContent.action#			🖻 🖈 🔲 😩 :
aruba		ClearPass Policy Manager		Menu 🗮
Dashboard	O Configuration » Network » Devices			
Monitoring	<ul> <li>Network Devices</li> </ul>			🐥 Add
Configuration				Export All
- 🛱 Service Templates & Wizards				Discovered Devices
- C Services	A Add Device		•	
Authentication	Device SNMP Read Settings SNM	IP Write Settings CLI Settings OnConnect Enforcement A	ttributes	
Posture	Fi Name:	SW04		Show 20 V records
Enforcement	IP or Subnet Address:	172 25 200 13		Description
- + Network		(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or	r 2001:db8:a0b:12f0::1/64)	
Device Groups	Description:			
Proxy Targets				
- 🛱 Event Sources	RADIUS Shared Secret:	verify:		
- Q Network Scan	TACACS+ Shared Secret:	Verify:		
and the state of t	Vendor Name:	Aruba		
	Enable RADIUS Dynamic Authorization:	0		
	Enable RadSec:			
			Add Cancel	
Administration	0			
Copyright 2022 Hewlett Packard Enterpris	e Development LP De	ec 28, 2022 09:02:18 CET	ClearPass Policy Manager	6.9.12.136929 on CLABV (Trial Version) platform

在 ClearPass Policy Manager 中将 HPE Aruba Networking 接入交换机添加为可信网络设备。请 注意,RADIUS 共享密钥必须与特定交换机 IEEE 802.1X 配置匹配。

### 安全加入 - IEEE 802.1AR/802.1X



配置了一台受信任网络设备的 ClearPass Policy Manager。



ClearPass Policy Manager 中的可信网络设备组接口。

### 安全加入 - IEEE 802.1AR/802.1X

C todals blagtered it i +							
	O ClearPass Policy Manager - Arub × +						~ - 🗆 X
Charles     Configuration > Return's - Device Group        Configuration > Return's - Device (O)     Permat:   Configuration > Devices (O) <td>← → C ▲ Inte säker   https://172.25.201.</td> <td>.120/tips/tipsContent.action#</td> <td></td> <td></td> <td></td> <td></td> <td>e ☆ □ ≗ :</td>	← → C ▲ Inte säker   https://172.25.201.	.120/tips/tipsContent.action#					e ☆ □ ≗ :
Configuration + Detroits + Device Groups   Mathemotoring   Bandia Template & Wizards   Device Groups function   Referity   Prost   Postrie   Postrie   Postrie   Postrie   Postrie   Device Groups function   Vertee Groups function   Postrie   Po	aruba			ClearPass Policy N	/lanager		Menu 🗮
Mathiadianation   Carriade Transfels & Mitzards   Carriade Transfels & Mitzards <td< td=""><td>Dashboard</td><td>o Configuration » Netwo</td><td>k » Device Groups</td><td></td><td></td><td></td><td></td></td<>	Dashboard	o Configuration » Netwo	k » Device Groups				
Configuration       O evice Groups function         Configuration       Device Groups function         Configuration       Configuration	Monitoring	<ul> <li>Network Device</li> </ul>	Add New Device Group				🗭 Add
C Services Completes & Wizerds C Services C Services C Services C Services C Retrort Scan C Retrort Sca	Configuration	0	Name:	Switches			Limport Export All
<pre>     the starting starting start start starts start sta</pre>	- 🗘 Service Templates & Wizards	Device Groups function	Description:	Access Switches		nent profiles.	
Identity   Ident	- 🙀 Services						-1 00 1
Administration	🗟 🗕 Identity	Filter: Name	Format:	O Subnet			Show 20 V records
Administration       Administration	🗈 🖶 Posture	# Name		<ul> <li>Regular Expression</li> <li>List</li> </ul>			
Concises     Concise Concupation     Concise     Concis     Concise     Concise     Concise     Concise     Concise     C	Enforcement     Network		Available Devices (0)		Selected Devices (1)		Export Delete
<ul> <li>Powies Groups</li> <li>Grown Targets</li> <li>Grown Sources</li> <li>Policy Simulation</li> <li>Policy Simulation</li> <li>Model (172:25:200:13)</li> </ul>	Devices			Filter	Filter		
C Frox Targets     C Ford Sources     C Administration	- Device Groups				SW04 [172.25.200.13]		
Administration     Administration     O	Proxy Targets						
Concel	- Network Scan						
Administration O	- Delicy Simulation						
Administration							
Administration 0							
Administration 0							
Administration 0							
Administration •							
Administration 0							
Administration 0							
Administration 0							
Administration o					Save		
Administration o					Save		
	🗿 Administration	0					
g Lopyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 U9:U5:28 CE1 ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform	Copyright 2022 Hewlett Packard Enterprise De	evelopment LP	Dec 2	8, 2022 09:05:28 CET		ClearPass Policy Manager 6.9.12.136929 on C	LABV (Trial Version) platform

将受信任的网络访问设备添加到 ClearPass Policy Manager 中的新设备组中。

Q ClearPass Policy Manager - Arub × +		✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.1	20/tips/tipsContent.action#	@ ☆ □ ≗ :
aruba	ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration > Network > Device Groups	
Monitoring •	Network Device Groups	Add
Service Templates & Wizards     Services     Authentication     O Identity	Device Group "Switches" added successfully Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.	
Posture	Filter: Name V contains V 🕢 Go Clear Filter	Show 20 🗸 records
🗈 🔹 Enforcement	# ■ Name ▲ Format Description	
- © Devices - © Devices Groups - © Proxy Targets - © Event Sources - © Network Scan - © Policy Simulation	Showing 1-1 of 1	Export Delete
Administration © Copyright 2022 Hewlett Packard Enterprise Dev	elopment LP Dec 28, 2022 09:05:43 CET ClearPass Policy Manager 6.9.12.136929 on C	:LABV (Trial Version) platform

ClearPass Policy Manager 已配置网络设备组,其中包括一个或多个受信任的网络设备。

#### 设备指纹配置

Axis 设备可以通过网络发现分发设备特定信息,例如 MAC 地址和设备软件版本。使用此信息在 ClearPass Policy Manager 中创建、更新或管理设备指纹。在这里,您还可以根据 AXIS OS 版本授 予或拒绝访问权限。

- 1. 转往管理 > 词典 > 设备指纹。
- 2. 选择现有的设备指纹或创建新的设备指纹。

### 安全加入 - IEEE 802.1AR/802.1X

3. 设置设备指纹设置。

Q ClearPass Policy Manager - Arub: × +								~ - 🗆 X
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tips	sContent.action#tip	psFingerprintDictionary.action					🖻 🖈 🔲 😩 :
aruba			C	learPass Poli	cy Manager			Menu 🗮
Dashboard O Common Monitoring O Configuration O Administration O	Adminis	tration » Dictiona e Fingerpri	aries » Device Fingerprints nts					<ul> <li>Add</li> <li>Import Custom Fingerprints</li> <li>Export Custom Fingerprints</li> </ul>
Administration     ClearPass Portal     ClearPass Portal     Autors and Privileges     Server Manager     External Accounts     Certificates     Dictionaries     Particular Counts     Particular     Particular Counts     Particular     Particular     Particul	This page Filter: F 1. 2. 3. 4. Showing	e lists all the de amily Cotegory Network Can Network Can Server 3 1-4 of 4	vice Ingerprints recognized B Update Device Fingerprints Category: Family: Name: Custom Rules-1 Name LUDP System Descrif 3. SNMP System Descrif 3. SNMP System Descrif	y the Profiler module. 1 Network Camera Axis Axis Axis Matches Operator contains_all otion not_contains ption not_contains	These fingerprints are update provide the second s	Delete Rule	Updates page. Name AXIS OS version unsupported AXIS OS version supported Axis Network Camera Axis Print Server	Show 20 v records
© Copyright 2022 Hewlett Packard Enterprise Deve	lopment l	LP	Nov 25, 20	022 08:50:09 CET			ClearPass Policy Manager 6.9.12.1369	929 on CLABV (Trial Version) platform

ClearPass Policy Manager 中的设备指纹配置。运行除 10.12 之外的其他 AXIS OS 版本的 Axis 设备均被视为不受支持。

Q ClearPass Policy Manager - Arub × +								✓ - □ ×
← → C ▲ Inte säker   https://172.25.201.12	0/tips/tip:	sContent.action#ti	psFingerprintDictionary.action					🖻 🖈 🔲 😩 :
aruba			C	ClearPass Pol	icy Manager			Menu 🗮
Dashboard O	Adminis	stration » Dictions	aries » Device Fingerprints nts					Add
Administration •	This pag	ge lists all the de	vice fingerprints recognized	by the Profiler module.	These fingerprints are upd	ated from the Software L	Ipdates page.	Export Custom Fingerprints
/# ClearPass Portal 	Filter: [	amily	Update Device Fingerprint Category:	Network Camera	T	•	Name	Show 20 👻 records
<ul> <li>External Servers</li> <li>PExternal Accounts</li> <li>Certificates</li> </ul>	1. 2.	Network Can Network Can	Family: Name:	Axis AXIS OS version sup	port V		AXIS OS version unsupported AXIS OS version supported	
	3. 4.	Network Can Server	Custom Rules- 1 Name Host MAC Vendor	Matche Operator contains all	s (ALL ) Value	Delete Rule	Axis Network Camera Axis Print Server	
TACACS + Services  Toxice Engraphics  Toxice Engraphics  Toxice Engraphics  Toxice Engraphics  Toxice Server Actions  Toxice Server Actions  Toxice Server Servers  Toxice Se	Showing	g 1-4 of 4	LLDP System Descri     SNMP System Descri	ption contains	10.12 10.12			
© ♣ Agents and Software Updates © ♣ Support			"Note: 0 Rule(s) will be de	leted	Update Delete Fing	erprint Close		
Copyright 2022 Hewlett Packard Enterprise Deve	lopment	LP	Dec 05, 2	022 09:05:39 CET		(	ClearPass Policy Manager 6.9.12.136	929 on CLABV (Trial Version) platform

ClearPass Policy Manager 中的设备指纹配置。在上例中,运行AXIS OS 10.12的 Axis 设备被视为受支持。

有关 ClearPass Policy Manager 收集的设备指纹的信息可以在端点部分找到。

- 1. 转往配置 > 身份 > 端点。
- 2. 选择要浏览的设备。

注

#### 安全加入 - IEEE 802.1AR/802.1X

3. 单击设备指纹选项。

默认情况下,SNMP 在 Axis 设备中处于禁用状态,并从HPE Aruba Networking 接入交换机收集。

ClearPass Policy Manager - Arub × +							× -	□ ×
← → C ▲ Inte säker   https://172.25.201.1	120/tips/tipsConter	nt.action#tipsEndpoin	ts.action				፼ ☆ [	3 😩 E
aruba			ClearPass Polic	y Manager	3		P	ienu 🔳
E Bashboard O	Configuration a	» Identity » Endpoin	nts					
Monitoring O	Endpoints	;					*	Add
Configuration								Export All
- 🛱 Service Templates & Wizards	This page au	Edit Endpoint				orth with a network to which it is		
- 🛱 Services	connected (e	Endpoint At	ributes Device Fingernrints					
Authentication	O Select AL		induces bencer ingerprints	1	Construction and the second	_		
Single Sign-On (SSO)	Filter: MAC A	MAC Address	B8-A4-4F-30-42-EA	IP Address	172.25.201.233			
- C Local Users	Filter: MAC A	Description		Static IP	FALSE			
Endpoints Filte	Filter: MAC A			Hostname	axis-b8a44f3042ea		Show 20	✓ records
- C Static Host Lists		Status	O Known client	Device Category	Network Camera	ly Status	Profiled	
- Role Mappings	1. C		Unknown client	Device OS Family	AXIS	Unknown	Yes	
Posture	2. 🗆		O Disabled client	Device Name	AX13 03 Version suppor	Unknown	Yes	
Enforcement	з. С	MAC Vendor	Axis Communications AB	Added At	Dec 28, 2022 14:50:45 CET	Unknown	Yes	
💽 📲 Network	4. C	Added by	Policy Manager	Fromed by	Policy Manager	Unknown	Yes	
- O Network Scan	Showing 1-4	Online Status	Not Available	Last Promed At	Dec 29, 2022 00:10:23 CET	ger Server Action ] Update Fingerprin		
- Q Policy Simulation		Connection Type	Unknown					
					Save	cel		
						_		
Administration 0								
© Copyright 2022 Hewlett Packard Enterprise Dev	elopment LP		Dec 29, 2022 08:28:03 CET		c	ClearPass Policy Manager 6.9.12.136929 on CL	ABV (Trial Vers	ion) platform

由 ClearPass Policy Manager 配置的 Axis 设备。

ClearPass Policy Manager - Arub × +						~ -	
← → C ▲ Inte säker   https://172.25.201.	120/tips/tipsContent	t.action#tipsEndpoints.action				፼ ☆ [	1 😩 E
aruba			ClearPass Policy Manager			M	lenu 🔳
Deshboard     Deshboard     Deshboard     Configuration     Configuration     Services     Services     Services     Services     Services     Single Sign-On (SSO)     Deal Users     Origonal Users	Configuration - Endpoints This page au connected (e Select AL Filter: MACA Filter: MACA Filter: MACA Filter: MACA Showing 1-4	Identity = Endpoints Edit Endpoint Endpoint Attributes CDP Device Description: DHCP Option55: DHCP Option60: DHCP Option8: Host MAC Vendor; LDP System Description: SNMP Device Type: SNMP Device Type: SNMP System Description:	Device Fingerprints Endpoint Fingerprint Details Endpoint Fingerprint Details 1,3,6,12,15,28,42,66,119 AXI5,Panoramic Camera,P3727-PLE,10,12,130 33,57,55,12,60,61 AXIS P3727-PLE Panoramic Camera 10,12,130 axis-b8a44f3042ea Host AXIS P3727-PLE Panoramic Camera 10,12,130	о 	th with a network to which it is Status Unknown Unknown Unknown uknown ar Server Action	Show (20) Profiled Yes Yes Export	Add Import Export All
Copyright 2022 Hewlett Packard Enterprise Dev	velopment LP		Dec 29, 2022 08:28:24 CET	ClearPass I	Policy Manager 6.9.12.136929 on CLA	BV (Trial Vers	ion) platform

配置文件的 Axis 设备的详细设备指纹。请注意,默认情况下,Axis 设备中禁用 SNMP。 LLDP、CDP 和 DHCP 特定的发现信息由处于出厂默认状态的 Axis 设备共享,并由 HPE Aruba Networking 接入交换机中继到 ClearPass Policy Manager。

安全加入 - IEEE 802.1AR/802.1X

#### 强制配置文件配置

强制配置文件用于允许 ClearPass Policy Manager 将特定 VLAN ID 分配给交换机上的访问端口。这是一 个基于策略的决策,适用于设备组"交换机"中的网络设备。必要的强制配置文件数量取决于将使用的 VLAN 数量。在我们的设置中,共有三个 VLAN(VLAN 201、202、203)与三个强制配置文件相关。

配置完 VLAN 的强制文件后,就可以配置实际的强制策略了。ClearPass Policy Manager 中的强制策略配置定义是否根据四个示例策略配置文件授予 Axis 设备访问 HPE Aruba Networking 网络的权限。

ClearPass Policy Manager - Arub × +								~	-	
← → C ▲ Inte säker   https://172.25.201.1	120/tips/	/tipsContent	action#tip	osEditEnforcementPro	file.action%3FcontextData%3D3004			Ŀ	☆ [	3 😩 E
aruba					ClearPass Policy Manager				м	1enu 🔳
Dashboard	Conf	iguration »	Enforcen	nent » Profiles » Edi	t Enforcement Profile - Allow_VLAN_201					
Monitoring O	Enf	orceme	nt Pro	files - Allow	VLAN 201					
Configuration O	Su	mmary	Profile	Attributes						
- 🛱 Service Templates & Wizards	Profi	ile:								
Authentication	Nam	e:		Allow_VLAN_20	L.					
🗉 🖳 Identity	Desc	ription:								
Posture	Туре	с.		RADIUS						
B Enforcement	Actio	on:		Accept						
- Profiles	Devi	ce Group L	ist;	1. Switches						
	Attri	ibutes:								
- 🛱 Network Scan		Туре			Name		Value			
-Q Policy Simulation	1.	Radius: I	ETF		Session-Timeout	=	10800			
	2.	Radius:I	ETF		Termination-Action	-	RADIUS-Request (1)			
	з.	Radius: II	ETF		Tunnel-Type	=	VLAN (13)			
	4.	Radius:II	ETF		Tunnel-Medium-Type	-	IEEE-802 (6)			
	5.	Radius: I	ETF		Tunnel-Private-Group-Id	=	201			
				and the officer						
Administration O	<	Back to En	forceme	nt Profiles				Сору	Save	Cancel
© Copyright 2022 Hewlett Packard Enterprise Dev	elopme	ent LP		0	Dec 28, 2022 09:08:57 CET		ClearPass Policy Manager 6.9.12.136929	on CLABV (T	rial Vers	ion) platform

允许访问 VLAN 201 的强制配置文件示例。

<ul> <li>Configuration &gt; Enforce</li> <li>Enforcement Pc</li> <li>Summary Enforce</li> <li>Enforcement:</li> <li>Name:</li> </ul>	ClearPass Policy Manager ement * Policies - Edit - Axis Radius policy plicies - Axis Radius policy ement Rules		Menu
Configuration > Enforce     Enforcement Pc     Summary Enforce     Enforcement:     Name:	ement » Policies » Edit - Axis Radius policy Dicies - Axis Radius policy ment Rules		
Enforcement Po     Summary Enforce     Enforcement:     Name:	olicies - Axis Radius policy ment Rules		
Summary Enforce	Rules		
Enforcement: Name:			
Name:			
	Axis Radius policy		
Description:			
Enforcement Type:	RADIUS		
Default Profile:	Allow_VLAN_203		
Rules:			
Rules Evaluation Algori	ithm: First applicable		
Conditions		Actions	
1. AND (Certificate:Issuer AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate AND (Certificate	-CN_CONTAINS Axis device ID Intermediate CA) Essence - Equivals. Axis Communications AB) Essubject-E Equils. Suis Communications AB) Essubject-E Equils. SE) Essubject-E Equils. SE) Exclient-Nac-Address-Nobellim. Equil.25 % (Certificate:Subject-serialNumber))	Allow_VLAN_201	
2. AND (Certificate AND (Certificate AND (Authorizat	-CN CONTAINS Production CA Certificate) a:Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim})) tion:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported)	Allow_VLAN_201	
3. AND (Certificate AND (Certificate AND (Authorizat	-CN CONTAINS Production CA certificate) a:Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim}) tion:[Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202	
< Back to Enforcem	nent Policies	2	py Save Cance
	Certificate: Issue Certificate:	Description:       Enforcement Type:       RADIUS         Default Porfile:       Allow_VLAN_203         Description:         Bulse Evaluation Algorithm: First applicable         Continue         Contrindue:Subject-C	Description:     RADIUS       Enforcement Type:     RADIUS       Defail Profile:     Allow_VLAN_203       Nules:     Rules:       Rules:     Rules:       Rules:     Actions       Condition:     First applicable       AMD (Conflicate:Subject-CONCAVINS Axis device ID Intermediate CA) AMD (Conflicate:Subject-O EQUALS Axis Communications AB) AMD (Conflicate:Subject-CONCAVINS Axis advice ID Intermediate CA) AMD (Conflicate:Subject-CONCAVINS Axis Communications AB) AMD (Conflicate:Subject-CONCAVINS Axis Communications AB) AMD (Conflicate:Subject-CONCAVINS Stophace) EQUALS Axis Communications AB) AMD (Conflicate:Subject-CONCAVINS Stophace) EQUALS Stophace Address-NoDelim (QUALS Stophace) AMD (Conflicate:Subject-CONCAVINS Stophace)     Allow_VLAN_201 AMD (Conflicate:Subject-CONCAVINS Stophace) AMD (Conflicate:Subject-CONCAVINS Stophace)     Allow_VLAN_201 AMD (Conflicate:Subject-CONCAVINS Stophace)       3.     AMD (Conflicate:Subject-CONCAVINS Stophace)     Allow_VLAN_201 AMD (Conflicate:Subject-CONCAVINS Stophace)       4.     AMD (Conflicate:Subject-CONCAVINS Stophace)     Allow_VLAN_202 AMD (Conflicate:Subject-CONCAVINS Stophace)       5.     AMD (Conflicate:Subject-CONCAVINS Stophace)     Allow_VLAN_202 AMD (Conflicate:Subject-CONCAVINS Stophace)       6.     Back to Enforcement Policies     Control AND Conflicate Address AND AND Conflicate)

ClearPass Policy Manager 中的强制策略配置。

#### 安全加入 - IEEE 802.1AR/802.1X

四项强制策略及其行动如下:

拒绝网络访问

当未进行 IEEE 802.1X 网络访问控制认证时,网络将被拒绝访问。

访客网络(VLAN 203)

如果 IEEE 802.1X 网络访问控制身份验证失败,则 Axis 设备将被授予访问受限、隔离网络的权限。 需要对设备进行手动检查以采取适当的措施。

配置网络(VLAN 201)

Axis 设备被授予对配置网络的访问权限。这是为了通过以下方式提供 Axis 设备管理功 能: AXIS Device Manager 和 AXIS Device Manager Extend。它还可以使用 AXIS OS 更新、生产级证书 和其他配置来配置 Axis 设备。以下条件已由 ClearPass Policy Manager 验证:

- Axis 设备的 AXIS OS 版本。
- 设备的 MAC 地址与供应商特定的 Axis MAC 地址方案与 Axis 设备 ID 证书的序列号属性相匹配。
- Axis 设备 ID 证书是可验证的,并且与 Axis 特定属性(例如颁发者、组织、位置及国家/地区)相匹配。

#### 生产网络 (VLAN 202)

Axis 设备被授予访问 Axis 设备应在其中运行的生产网络的权限。从配置网络(VLAN 201)内完成设备置备后,将授予访问权限。以下条件已由 ClearPass Policy Manager 验证:

- 设备的 MAC 地址与供应商特定的 Axis MAC 地址方案与 Axis 设备 ID 证书的序列号属性相匹配。
- Axis 设备的 AXIS OS 版本。
- 生产级证书可由受信任的证书存储区验证。

#### 认证方式配置

在身份验证方法中,定义了 Axis 设备如何尝试针对网络进行身份验证。理想的身份验证方法应为 IEEE 802.1X EAP-TLS,因为支持 Axis Edge Vault 的 Axis 设备默认启用了 IEEE 802.1X EAP-TLS。

### 安全加入 - IEEE 802.1AR/802.1X

O ClearPass Policy Manager - Arub × +							~ - O X
← → C ▲ Inte säker   https://17	2.25.201.120/tips/tips	Content.action#tipsAuthM	ethods.action				🖻 🛧 🔲 😩 :
aruba			ClearPas	s Policy Manager			Menu 🗮
Dashboard	O Configur	ation » Authentication »	Methods				
Monitoring	• Authe	entication Method	ls				Add A Import Export All
- 🛱 Service Templates & Wizards - 🙀 Services - 🔒 Authentication	As a first	t step in the service-bas	Edit Authentication Method		r device against an authentication source.	Show 20 V records	
- 🛱 Methods	Filter: N	Name A	Name:	is FAP TI S		Description	Show 20 Theorem
- Q Sources	1.	[Allow All MAC A	Description: De	fault settings for EAP-TLS	_	Default settings for Allow All MAC-AUTH	
E Bosture	2.	[Aruba EAP GTC				EAP-GTC method to use with Aruba EAP-GTC plugin for Windows	
🗈 🔹 Enforcement	3.	[Authorize]				Default settings for Authorize	
🗈 📫 Network	4.	Axis EAP TLS	Type: EA	P-TLS		Default settings for EAP-TLS	
- O Network Scan	5.	CHAP]	1	Method Details		Default settings for CHAP	
- La Policy Simulation	6.	EAP FAST]	Session Resumption:	Enable		Default settings for EAP-FAST	
	7.	EAP GTC]	Session Timeout:	6 hours		Default settings for EAP-GTC	
	8.	EAP MD5]	Authorization Required:	Enable		Default settings for EAP-MD5	
	9.	EAP MSCHAPv2	Certificate Comparison:	Do not compare 🗸 🗸		Default settings for EAP-MSCHAPv2	
	10.	EAP PEAP]	Verify Certificate using OCSP:	None 🗸		Default settings for EAP-PEAP	
	11.	EAP PEAP Public	Override OCSP URL from Client	:: 🗆 Enable		Default settings for EAP-PEAP-Public	
	12.	EAP PEAP With	OCSP URL:			EAP-PEAP with Fast Reconnect disabled; recommen-	ded for Onboard
	13.	EAP PWD]				Default settings for EAP-PWD	
	14.	EAP TLS]		Copy Save	Cancel	Default settings for EAP-TLS	
	15.	EAP TLS With C	(			EAP-TLS with OCSP enabled; recommended for Onb	oard
	16.	EAP TTLS]		EAP-TTLS		Default settings for EAP-TTLS	
	17.	[MAC AUTH]		MAC-AUTH		Default settings for MAC-AUTH	
	18.	[MSCHAP]		MSCHAP		Default settings for MSCHAP	
	19.	[PAP]		PAP		Default settings for PAP	
© Copyright 2022 Hewlett Packard Enterp	20. Drise Development L	P Issol	Dec 28, 2022 09:43:30	PAP		Default settings for SSO ClearPass Policy Manager 6.9.12.136929	• on CLABV (Trial Version) platform

ClearPass Policy Manager 的身份验证方法接口,其中定义了 Axis 设备的 EAP-TLS 身份验证方法。

#### 设备配置

在服务界面中,配置步骤合并为一项服务,用于处理 HPE Aruba Networking 网络中 Axis 设备的身 份验证和授权。

ClearPass Policy Manager - Arub × +					×	- 0	×		
← → C ▲ Inte säker   https://172.25.201.12	20/tips/	/tipsContent.action#tip	osEditService.action%3FcontextData%3D3001		l		0 E		
orubo			ClearPass Polic		Menu	=			
Dashkaard 0	Conf	inuration » Services	» Edit - Avie 802 1X Wired	-,					
	C	nuises Auris C							
	Ser	vices - Axis d	02.1X Wired						
Configuration	Su	mmary Service	Authentication Roles Enforcement						
- Criservices	Nam	e:	Axis 802.1X Wired						
Authentication	Description:		To authenticate users to any wired network via 802.1X.						
- 🕀 Posture	Type		802.1X Wired						
Enforcement	Statu	us:	Enabled						
- Q Network Scan	Moni	itor Mode:	Enable to monitor network access without enforcement						
- 🛱 Policy Simulation	More	Options:	Authorization Posture Compliance Audi	it End-hosts 🗌 Profile Endpoints 🗌 Accounting	] Proxy				
	Service Rule								
	Matcl	hes 🔿 ANY or 🖲 .	ALL of the following conditions:						
		Туре	Name	Operator	Value				
	1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)	63	Ť		
	2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	92)	Ŧ		
	з.	Click to add							
Administration 0	< 8	Back to Services			Disable Copy Sa	ve Car	icel		
Copyright 2022 Hewlett Packard Enterprise Deve	elopme	ent LP	Dec 28, 2022 09:41:27 CET		ClearPass Policy Manager 6.9.12.136929 on CLABV (Tria	Version) p	alatform		

创建了专用的 Axis 服务,将 IEEE 802.1X 定义为连接方法。

### 安全加入 - IEEE 802.1AR/802.1X

ClearPass Policy Manager - Arub × +					× − □ ×
← → C ▲ Inte säker   https://172.25.201.12	20/tips/tipsContent.action#tips	EditService.action%3FcontextData%3D3001			@☆□
aruba		ClearPass	Policy Manager		Menu 📕
Dashboard	Configuration » Services »	Edit - Axis 802.1X Wired			
Monitoring O	Services - Axis 80	2.1X Wired			
🖧 Configuration 📀	Summary Service	Authentication Roles Enforcement			
Corvice Templates & Wizards     Corvice     Corv	Authentication Methods:	Axis EAP TLS Select to Add-	Move Up 1 Move Down 1 Remove View Details Modify Move Up 1 Move Down 1 Remove View Details Modify Notify	Add Ne Add N	w Authentication Method
	Strip Username Rules:	Enable to specify a comma-separated lis	t of rules to strip username prefixes or suffixes		
	Service Certificate:	Select to Add 🗸			View Certificate Details
Administration 0	Back to Services			Disable Copy	Save Cancel
© Copyright 2022 Hewlett Packard Enterprise Deve	elopment LP	Dec 28, 2022 09:41:41 CE	r	ClearPass Policy Manager 6.9.12.136929 on CLA	BV (Trial Version) platform



Q ClearPass Policy Manager - Arub × +			✓ - □ ×
← → C ▲ Inte säker   https://172.25	5.201.120/tips/tipsContent.action#tip	psEditService.action%3FcontextData%3D3001	🖻 🕁 🔲 🛓 :
aruba		ClearPass Policy Manager	Menu 📕
Dashboard	• Configuration » Services	» Edit - Axis 802.1X Wired	
Monitoring	<ul> <li>Services - Axis 8</li> </ul>	02.1X Wired	
🝰 Configuration	Summary Service	Authentication Roles Enforcement	
🛱 Service Templates & Wizards	Use Cached Results:	Use cached Roles and Posture attributes from previous sessions	
Qr Services     Authentication	Enforcement Policy:	Axis Radius policy V Modify	Add New Enforcement Policy
Identity		Enforcement Policy D	etails
Posture     Sefereement	Description:		
A Network	Default Profile:	Allow_VLAN_203	
- 🛱 Network Scan	Rules Evaluation Algorith	m: first-applicable	
	Conditions		Enforcement Profiles
	(Certificate:Issue AND (Certifica 1. AND (Certifica AND (Certifica AND (Certifica AND (Certifica AND (Contect	er-CN COMTAINS Axis device ID Intermediate CA) terisSuep-C PCUALS Axis Communications AB) tersSubject- CPCUALS Axis Communications AB) tersSubject- CPCUALS und tersSubject- CPCUALS SE) ion:Client-MacAddress-Nobelim EQUALS %{Certificate:Subject-serialNumber})	Allow_VLAN_201
	(Certificate:Issu 2. AND (Certifica AND (Authoriz	er-CN CONTAINS Production CA Certificate) te:Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim}) ation:[Endpoints Repository]:Device Name <i>EQUALS</i> AXIS OS version unsupported	Allow_VLAN_201
	(Certificate:Issue 3. AND (Certifica AND (Authoriz	er-CN CONTAINS Production CA certificate) te:Subject-CN CONTAINS %{Connection:Client-Mac-Address-NoDelim}) ation:[Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202
	Back to Services		Disable Copy Save Cancel
Administration	e Development I P	Dec 28, 2022 09:51:01 CET	ClearPass Policy Manager 6.9.12.136929 op CLABV (Trial Version) platform

在尾部步骤中,将之前创建的强制策略配置到服务。

#### HPE Aruba Networking 接入交换机

Axis 设备可以直接连接到支持 PoE 的接入交换机,也可以通过兼容的 Axis PoE 中跨连接。要将 Axis 设 备安全地接入 HPE Aruba Networking 网络,需要将接入交换机配置为 IEEE 802.1X 通信。Axis 设备将 IEEE 802.1x EAP-TLS 通信中继到充当 RADIUS 服务器的 ClearPass Policy Manager。

注

还为 Axis 设备配置了 300 秒的定期重新验证,以提高整体端口访问安全性。

#### 安全加入 - IEEE 802.1AR/802.1X

请参阅以下 HPE Aruba Networking 接入交换机的全局和端口配置示例。

radius-server 主机 MyRADIUSIPAddress 密钥"MyRADIUSKey"

AAA 身份验证端口访问 eap-radius AAA 端口访问验证器 18-19 AAA 端口访问验证器 18 reauth-period 300 AAA 端口访问验证器 19 reauth-period 300 AAA 端口访问验证器处于活动状态

配置 Axis

#### Axis 网络设备

支持 Axis Edge Vault 的 Axis 设备制造时带有安全设备标识,称为 Axis 设备 ID。Axis 设备 ID 基于国际 IEEE 802.1AR 标准,该标准定义了一种通过 IEEE 802.1X 进行自动化、安全设备识别和网络接入的方法。



Axis 设备在制造时带有符合 IEEE 802.1AR 标准的 Axis 设备 ID 证书,用于可信设备身份服务

1 Axis 设备 ID 密钥基础设施(PKI)

2 Axis 设备 ID

Axis 设备的安全元件提供的受硬件保护的安全密钥库在出厂时就预配了设备单独的证书和相应的密钥 (Axis 设备 ID),可在全局范围内证明 Axis 设备的真实性。*Axis Product Selector* 可用于了解哪些 Axis 设备支持 Axis Edge Vault 和 Axis 设备 ID。

1	<b>`</b>
-	_
1	T
	_

Axis 设备的序列号是其 MAC 地址。

		AXIS Q1656 Box Camera	0 🛱 🛈 🖪	:
🔁 Status				
□ Video	~	Certificates		
PTZ		+ Add certificate	-a 💌	
📥 Audio	~			
Recordings		Name Ty	/pe	
🛠 Apps		Axis device ID ECC-P256 (802.1AR)	ient-server	
🕸 System	^	Axis device ID RSA-2048 (802.1AR) CI	ient-server	
Date and time				
Network		Axis device ID RSA-4096 (802.1AR)	ient-server	
Security	1	Axis device ID Intermediate CA ECC 2		

处于出厂默认状态的 Axis 设备的证书存储以及 Axis 设备 ID。

### 安全加入 - IEEE 802.1AR/802.1X

符合 IEEE 802.1AR 标准的 Axis 设备 ID 证书包含有关序列号的信息和其他 Axis 供应商特定信息。该信息 由 ClearPass Policy Manager 使用以进行分析和决策以授予网络访问权限。请参阅以下可从 Axis 设 备 ID 证书获取的信息



国家/地区	SE
位置	隆德
发行人组织	Axis Communications AB
发行人通用名称	Axis 设备 ID 中介
组织	Axis Communications AB
常用名称	Axis-b8a44f279511-eccp256-1
序列号	b8a44f279511

通用名称由 Axis 公司名称、设备序列号和所使用的加密算法(ECC P256、RSA 2048、RSA 4096)组合 而成。自 AXIS OS 10.1(2020–09)起,默认情况下启用 IEEE 802.1X,并预先配置 Axis 设备 ID。这使 得 Axis 设备能够在支持 IEEE 802.1X 的网络上对自身进行身份验证。

		AXIS Q1656 Box Camera	😗 🖙 🕼 🖪 🗄
⊠ Status	~	IEEE 802.1x     Connecting	
PTZ	~	Client certificate ① EAPOL Version     Axis device ID RSA-2048 (802.1AR)	
<ul> <li>Recordings</li> </ul>	Ŷ	CA certificates () 2 No CA certificate selected •	
System	^	EAP Identity axis-b8444f27a03a	
Date and time Network			
Security			Save

Axis 设备处于出厂默认状态,启用 IEEE 802.1X 并预先选择 Axis 设备 ID 证书。

#### **AXIS Device Manager**

AXIS Device Manager 和 AXIS Device Manager Extend 可在网络上以经济高效的方式配置和管理多个 Axis 设备。AXIS Device Manager 是一款基于 Microsoft Windows® 的应用程序,可以本地安装在网络 中的计算机上,而 AXIS Device Manager Extend 则依赖云基础设施进行多站点设备管理。两者都为 Axis 设备提供简单的管理和配置功能,例如:

- 安装 AXIS OS 更新。
- 应用网络安全配置,例如 HTTPS 和 IEEE 802.1X 证书。

安全加入 – IEEE 802.1AR/802.1X

• 配置特定设备的设置,例如图像设置等。

安全网络操作 – IEEE 802.1AE MACsec

安全网络操作 – IEEE 802.1AE MACsec



IEEE 802.1AE MACsec(媒体访问控制安全)是一种定义明确的网络协议,它以加密方式保护网络第 2 网络层上的点对点以太网链路。它确保两个主机之间数据传输的机密性和完整性。

IEEE 802.1AE MACsec 标准描述了两种操作模式:

- 手动配置预共享密钥/静态 CAK 模式
- 自动主会话/动态 CAK 模式使用 IEEE 802.1X EAP-TLS



在 AXIS OS10.1(2020–09)及更高版本, IEEE 802.1X 对于与 Axis 设备 ID 兼容的设备, 默认启用。在 AXIS OS 11.8 及更高版本,我们使用自动动态模式支持 MACsec IEEE 802.1X 默认情况下启用 EAP-TLS。当您使用出厂默认值连接 Axis 设备时,IEEE 802.1X 执行网络身份验证,成功后还会尝试 MACsec 动态 CAK 模式。

安全存储的 Axis 设备 ID (1) 是与 IEEE 802.1AR 兼容的安全设备身份,用于通过 IEEE 802.1X EAP-TLS 基于端口的网络访问控制 (2) 对 网络(4、5)进行身份验证。通过 EAP-TLS 会话,自动交换 MACsec 密钥以建立安全链路 (3),从而保护从 Axis 设备到HPE Aruba Networking 接入交换机的网络流量。

### 安全网络操作 – IEEE 802.1AE MACsec

IEEE 802.1AE MACsec 要求 HPE Aruba Networking 接入交换机和 ClearPass Policy Manager 配置准备。 无需在 Axis 设备上进行配置即可允许 IEEE 802.1AE通过 EAP--TLS 进行 MACsec 加密通信。

如果 HPE Aruba Networking 接入交换机不支持使用 EAP-TLS 的 MACsec,则可以使用预共享密钥模 式并手动配置。

HPE Aruba Networking ClearPass Policy Manager

Q app20 × +									~	-		×
← → C ▲ Inte säker   https://172.25	.201.120/tips,	/tipsCo	ontent.action#	tipsRoles.action					e i	¥ L	1.8	1
aruba				C	learPass	Policy Manager	r			м	enu	
Dashboard	O Configu	ration	» Identity »	Roles								
Monitoring	Roles	5								-	Add	
& Configuration	0									*	Impor	
- 🎝 Service Templates & Wizards - 🎝 Services	Roles e	xist in	dependently	of an individual service	and can be acce	essed globally through the	role-mapping policy o	f any service.		-	Expor	
E 🖴 Authentication	Filter:	Name		✓ contains ✓		Go Clear	r Filter		Show	20	♥ red	cords
- Cources	#		Name 🔺			Description						
🕞 🚨 Identity	1.		[AirGroup v	/1]		Role for an AirGroup	protocol version 1 rec	quest				-
- 🛱 Single Sign-On (SSO)	2.		[AirGroup v	[2]		Role for an AirGroup	protocol version 2 rec	quest				
- 🛱 Local Users	3.		[Aruba TAC	ACS+ read-only Admin	1	Default role for read	I-only access to Aruba	device				
- C Endpoints	4.		[Aruba TAC	ACS+ root Admin1		Default role for root	access to Aruha devic					
C Relea	5.		AxisDevi	Edit Role								
- Q Role Mappings	6.		[BYOD O	Role ID:	3001			age their own provisioned devices				
🖃 🕀 Posture	7.		[Contrac	Name:	AxisDevice	1						
- 🗘 Posture Policies	8.		[Device I	Description:				their devices, for use with MAC authenticat	ion and Airo	Group	sharing	g.
- Audit Servers	9.		[Employe	beberpeen								
- CAgentless OnGuard	10.		[Guest]									
	11.		[MAC Ca				A					
- C Profiles	12.		[Onboard				Save Cancel					
🖃 📲 Network	13.		[Onboard					:d				
- 🗘 Devices	14.		[Onboard i	DS]		Role for an iOS device	ce being provisioned					
- C Device Groups	15.		[Onboard ii	PadOS]		Role for an iPadOS d	device being provisione	ed				
- O Proxy Targets	16.		[Onboard L	inux]		Role for Linux device	e being provisioned					
- Prevent Sources	17.		[Onboard n	nacOS]		Role for a macOS de	evice being provisioned	1				
- Delicy Simulation	18.		[Onboard V	Vindows]		Role for a Windows of	device being provision	ed				
	19.		[Other]			Default role for anot	ther user or device					
	20.		[TACACS+	API Admin]		API administrator ro	le for Policy Manager A	Admin				-
	Showin	g 1-20	) of 25 🕨 🕨									
👰 Administration	0											
				0+26								

添加 Axis 设备的角色名称。该名称是接入交换机配置中的端口访问角色名称。

#### 角色和角色映射策略

### 安全网络操作 - IEEE 802.1AE MACsec



为之前创建的 Axis 设备角色添加 Axis 角色映射策略。设备映射到 Axis 设备角色需要定 义的条件。如果不满足条件,设备成为 [Guest] 角色的一部分。

默认情况下,Axis 设备使用 EAP 身份格式"axis-serialnumber"。Axis 设备的序列号是其 MAC 地址。例如"axis-b8a44f45b4e6"。

### 安全网络操作 - IEEE 802.1AE MACsec

设备配置



将之前创建的 Axis 角色映射策略添加到将 IEEE 802.1X 定义为 Axis 设备加入的连接方法的服务中。

### 安全网络操作 - IEEE 802.1AE MACsec



将 Axis 角色名称作为条件添加到现有策略定义中。

### 安全网络操作 - IEEE 802.1AE MACsec

### 强制文件

Q app20 × +						~ -	o x
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsContent.action	#tipsEditEnforcementProfile.action%3Fconte	extData%3D3004			€ \$	🗆 😩 E
aruba		ClearPass	Policy Manager				Menu 🚍
Dashboard 0	Configuration » Enforcer	nent » Profiles » Edit Enforcement Profile	- Allow_VLAN_201				
Monitoring 0	Enforcement Pro	files - Allow VI AN 201					
Configuration O	Cummany Drofile	Attributor					
- Ö Service Templates & Wizards	Summary Prome	Attributes					
- 🛱 Services	Profile:						
🖃 🗣 Authentication	Name:	Allow_VLAN_201					
- 🛱 Methods	Description:						
- 🛱 Sources	Type:	RADIUS					
E- Q Identity	Action:	Accept					
Single Sign-On (SSO)	Device Group List:	1. Switches					
- Local Users	Attributes:						
- A Static Host Lists	Attributes.						
Roles	Туре	Name			value		
- 🛱 Role Mappings	1. Radius:IETF	Session-1	Imeout	=	10800		
🖃 🕂 Posture	2. Radius:IETF	Terminati	on-Action	=	RADIUS-Request (1)		
- 🛱 Posture Policies	3. Radius:IETF	Tunnel-Ty	rpe	=	VLAN (13)		
- 🛱 Audit Servers	4. Radius:IETF	Tunnel-M	edium-Type	=	IEEE-802 (6)		
Agentless OnGuard	5. Radius:IETF	Tunnel-Pr	ivate-Group-Id	=	201		
Senforcement     Policies	6. Radius:Aruba	Aruba-Us	er-Role	=	AxisDevice		
Profiles							
- + Network							
- O Devices							
- 🛱 Device Groups							
- 🛱 Proxy Targets							
C Event Sources							
- 🛱 Network Scan							
- 🋱 Policy Simulation							
	K Back to Enforcement	nt Profiles			Co	oy Save	Cancel
🐉 Administration 🛛 🛛 🛛 🛛 🛛 🔮							
Converight 2022 Howlett Packard Enterprise D	ovelenment I B	Oct 26, 2022 05:12:21	UTC		ClearDass Believ Manager 6 11 2 252204 op Cl	ABV (Trial Vo	and an A set of a set

将 Axis 角色名称作为属性添加到在 IEEE 802.1X 加入服务中分配的强制配置文件。

# HPE Aruba Networking 接入交换机

除了中描述的安全登录配置之外,参考下面 HPE Aruba Networking 接入交换机的端口配置示例进行配 置 IEEE 802.1AE MACsec。

macsec 策略 macsec-eap cipher-suite gcm-aes-128

端口访问角色 AxisDevice 关联 macsec-policy macsec-eap 验证模式客户端模式

AAA 身份验证端口访问 dot1x 身份验证器 macsec mkacak-length 16 启用

#### 旧版板载 – MAC 身份验证

#### 旧版板载 – MAC 身份验证

您可以使用 MAC 身份验证绕过(MAB)来板载不支持 IEEE 802.1AR的 Axis 设备,使用 Axis 设备 ID 证书进行注册,以及在出厂默认状态下启用 IEEE 802.1X。如果 802.1X 板载失败,ClearPass Policy Manager 会验证 Axis 设备的 MAC 地址并授予对网络的访问权限。

MAB 需要接入交换机和 ClearPass Policy Manager 配置准备。在 Axis 设备上,无需配置即可允 许 MAB 载入。

HPE Aruba Networking ClearPass Policy Manager

#### 强制政策

ClearPass Policy Manager 中的强制策略配置定义是否根据以下两个示例策略条件授予 Axis 设备访问 HPE Aruba Networking 网络的权限。

<b>Q</b> app20 × +			✓ – □ Х
← → C ▲ Inte säker   https://172.25.2	201.120/tips/tipsContent.action	#tipsEditService.action%3FcontextData%3D3006	ie 🛧 🛛 😩 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	Configuration » Services	» Edit - Axis 802.1X Wired - Mac Authentication	
Monitoring (	Services - Axis 8	02.1X Wired - Mac Authentication	
Sconfiguration	Summary Service	Authentication Roles Enforcement	
	Summary Service Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions (Date:Day-of-We 1. AND (Date:The Connect) AND (Connect)	AUTIENTICATION     ROLES     EINORCEMENT       Use cached Roles and Posture attributes from previous sessions     Axis MAC Authentication Policy     Modify       Enforcement I     [     [       [Deny Access Profile]	Add New Enforcement Policy Policy Details Enforcement Profiles Allow_VLAN_203
Administration	Back to Services  Pevelopment LP	Oct 26, 2023 05:15:57 UTC	Enable Copy Save Cancel

#### 拒绝网络访问

当 Axis 设备不符合配置的强制策略时,它会被拒绝访问网络。

访客网络(VLAN 203)

如果满足以下条件, Axis 设备将被授予访问受限、隔离网络的权限:

- 这是周一到周五之间的一个工作日
- 时间为 09:00 至 17:00

旧版板载 – MAC 身份验证

• MAC 地址供应商与 Axis Communications 匹配。

由于 MAC 地址可能被欺骗,因此不会授予对常规配置网络的访问权限。我们建议您仅使用 MAB 进行 初始启动,并进一步手动检查设备。

#### 来源配置

在来源界面中,创建一个新的身份验证源,仅允许手动导入的 MAC 地址。

Q app20 × +				v - L X
← → C ▲ Inte säker   https://172.25.20	1.120/tips/tipsCo	ntent.action#tipsAuthSources.action		ie 🛧 🖬 🛓 :
aruba		Clea	rPass Policy Manager	Menu 🗮
Dashboard 0	Configuration	» Authentication » Sources		
Monitoring 0	Authentic	ation Sources		🚽 Add
& Configuration	Additioned			A Import
A Service Templates & Wizards	An authentic	tion source is the identity store (Astive 5	inesten, IDAD directory, etc.) assignt which use	Export All
- I'l Services	An autientica	cion source is the identity store (Active L	mectory, LDAP unectory, etc.) against which use	rs and devices are authenticated.
Authentication			Co. Clear Filter	Show 20 w records
- 🛱 Methods	Filter: Name	✓ contains ✓		
- 🛱 Sources	#	Name 🔺	Туре	Description
🖃 🚨 Identity	1. 🗆	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
—🛱 Single Sign-On (SSO)	2.	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
- C Local Users	3. 🗆	[Endpoints Repository]	Local SOL DB	Authenticate endpoints against Policy Manager local database
- Static Host Liete	4	[Guest Device Repository]	Local SQL DB	Authenticate quest devices against Policy Manager local database
- Roles	5 0	[Guest Liser Repository]	Local SQL DB	Authenticate quest users against Policy Manager local database
Role Mappings	6 0	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
🖃 🖶 Posture	7	[Local User Repository]	Local SQL DB	Authenticate years against Policy Manager local year database
- 🛱 Posture Policies	•	[Ophoard Davisos Repository]	Local SQL DB	Authenticate Ophoard devices against Policy Manager local database
- 🛱 Audit Servers	a. U	[Control of the president ]		Authenticate Unboard devices against Policy Manager secial Legin database
- 🛱 Agentless OnGuard	9. 0	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
Enforcement	10.	[Time Source]	LOCAL SQL DB	Authorization source for implementing various time functions
- I Policies	11. U	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions
Network	Showing 1-11	of 11		Copy Export Delete
Devices				
- Device Groups				
— 🛱 Proxy Targets				
- 🛱 Event Sources				
- 🗘 Network Scan				
- 🛱 Policy Simulation				
🖉 Administration 🛛 🛛 🛛 🛛				
© Copyright 2023 Hewlett Packard Enterprise D	evelopment LP	Oct 31, 2023	09:13:53 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

# 旧版板载 – MAC 身份验证

• app20 × +			✓ - □ X
← → C ▲ Inte säker   https://172.25	5.201.120/tips/tipsContent.action#	tipsAddAuthSource.action	년 ☆ 🛛 💄 :
aruba		ClearPass Policy Manager	Menu 🗮
Dashboard	o Configuration » Authentic	ation » Sources » Add	
Monitoring	<ul> <li>Authentication Set</li> </ul>	ources	
& Configuration	Conoral Static Host	licte Summany	
- 🛱 Service Templates & Wizards	Name:		
- C Services	Description:	MAC addresses of Avis devices in use	
- Authentication	Description.	THE BUILESSES OF AKIS GETTES IN USE.	
Sources			
- Q Identity	Type:	Static Host List	
- 🛱 Single Sign-On (SSO)	Use for Authorization:	Enable to use this Authentication Source to also fetch role mapping attribu	ites
- 🗘 Local Users	Authorization Sources:		
- C Endpoints		Remove	
- D Static Host Lists		View Details	
Role Mappings		×	
- 🕀 Posture			
- C Posture Policies			
- Audit Servers			
- Agentiess OnGuard			
- Dicies			
Profiles			
- 🛱 Devices			
- C Device Groups			
- IC Proxy largets			
- Network Scan			
- C Policy Simulation			
100 8			
	K Back to Authenticat	ion Sources	Next → Save Cancel
Administration	0		
© Copyright 2023 Hewlett Packard Enterpris	e Development LP	Oct 31, 2023 09:21:23 UTC	ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

旧版板载 – MAC 身份验证

Q app20 × +					✓ - □ X
← → C ▲ Inte säker   https://172.25.20	01.120/tips/tipsContent.action#				ie 🖈 🛛 😩 i
aruba		ClearP	ass Policy Manager		Menu 🗮
Dashboard     O     Monitoring     O     Service Templates & Wizards     Services	Configuration » Authentical Authentication Sof General Static Host Li MAC Address Host Lists:	tion » Sources » Add UFCES sts Summary			Add New Static Host List
Authentication     Authenti		Add Static Host List          Name:       Description:         Host Format:       Host Format:         Host Entries       # Address         1.       Bs-A4-4F-45-B4-E6         2.       Bs-A4-4F-45-B4-E6         3.       Bs-A4-4F-45-B4-E6         Address:       Description:	Axis devices	ि में में में Save Host	
Administration Q	Back to Authentication	on Sources			Next → Save Cancel
© Copyright 2023 Hewlett Packard Enterprise D	Development LP	Oct 31, 2023 09:2	20:18 UTC	CI	learPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

创建了包含 Axis MAC 地址的静态主机列表。

旧版板载 – MAC 身份验证



### 设备配置

在服务界面中,配置步骤合并为一项服务,用于处理 HPE Aruba Networking 网络中 Axis 设备的身 份验证和授权。

# 旧版板载 – MAC 身份验证

← → C ▲ Inte säker   https://172	.25.201.120/tip	s/tipsCo	ontent.action	#tipsServices.action			B	* 🛛 😩
aruba				ClearPass Policy	Manager			Menu
Dashboard	• Config	uratior	n » Services					
	0 Com							👍 Add
Configuration	Serv	ices						🛓 Import
Convice Templates & Witards	This				A start and a start and			🙎 Export
Services	i nis p	age sno	ows the curi	ent list and order of services that ClearPass follows	ouring authentication and	authorization.		
Authentication	Cilhant	Mana			Go Clear Filter	Hit Count for Current hour	Sho	w 20 ¥ reco
- 🛱 Methods	Filter:	Name		contains      temperature	Clear Tilter		5110	V ZO V TECO
- 🛱 Sources	#	-	Order 🔺	Name	Туре	Template	Hit Count	Status
Q Identity	1.	U	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	0
— 🛱 Single Sign-On (SSO)	2.		2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	0
- 🛱 Local Users	з.		3	Test_Service	RADIUS	802.1X Wired	0	0
- 🛱 Endpoints	4.		4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	0
Static Host Lists	5.		5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	0	0
Role Manalage	6.		6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	0
Posture	7.		7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	0
Posture Policies	8.	0	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	0
- Q Audit Servers	9.		9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	õ
Agentless OnGuard	Chaud		-6.0			Deer		unnet ] [ Date
🔹 Enforcement	Snowl	Showing 1-9 of 9 Reor				der copy E	xport Dele	
- 🛱 Policies								
- 🛱 Profiles								
- Devices								
- O Device Groups								
- O Proxy Targets								
- C Event Sources								
A Deline Circulation								
- Le Policy Simulation								
Administration	0							
and the second se								

旧版板载 – MAC 身份验证



创建了将 MAB 定义为连接方法的专用的 Axis 服务。

旧版板载 – MAC 身份验证

Q app20 × +				×	- 🗆 X
← → C ▲ Inte säker   https://172.25.201	1.120/tips/tipsContent.action#t	ipsEditService.action%3FcontextData%3D3006		E	2 🖈 🔲 😩 :
aruba		ClearPass Pol	icy Manager		Menu 🗮
Dashboard 0	Configuration » Services »	Edit - Axis 802.1X Wired - Mac Authenticatio	'n		
Monitoring O	Services - Axis 80	2.1X Wired - Mac Authenticat	ion		
Configuration O	Summary Service	Authentication Roles Enforcement			
Configuration  Confi	Authentication Methods: Authentication Sources:	[Allow All MAC AUTH] Select to Add	Move Up † Move Down 1 Remove View Details Modify Move Down 1 Remove View Details Modify to findes to strip username prefixes or suf-	Add New / Add New /	Authentication Method
	Back to Services			Disable Copy	Save Cancel
Administration 0		0.4.21.2022.00.22.00.170		ClassBase Balling Manager ( 11 0 05000 )	(Total Mandala) atot
Copyright 2023 Hewlett Packard Enterprise De	evelopment LP	Oct 31, 2023 09:22:22 UTC		ClearPass Policy Manager 6.11.2.252294 on CLABV	(Trial Version) platform

将预先配置的 MAC 认证方法配置到服务中。此外,还会选择先前创建的包含 Axis MAC 地址列表的身份验证源。

Axis Communications 使用以下 MAC 地址 OUI:

- B8:A4:4F:XX:XX:XX
- AA:C8:3E:XX:XX:XX
- 00:40:8C:XX:XX:XX

旧版板载 – MAC 身份验证



在尾部步骤中,之前创建的强制策略配置到服务。

### HPE Aruba Networking 接入交换机

除了中描述的安全登录配置之外,请参阅以下 HPE Aruba Networking 接入交换机的端口配置示例以允许 MAB。

 AAA 端口访问验证器 18 发送周期 5

 AAA 端口访问验证器 19 发送周期 5

 AAA 端口访问验证器 18 上限请求数 3

 AAA 端口访问验证器 19 上限请求数 3

 AAA 端口访问验证器 19 上限请求数 3

 AAA 端口访问验证器 19 客户端限制 1

 AAA 端口访问验证器 19 客户端限制 1

 AAA 端口访问验证器 19 客户端限制 1

 AAA 端口访问基于 mac 的 18-19

 AAA 端口访问 18 身份验证顺序验证器基于 mac

 AAA 端口访问 19 auth-order 验证器基于 mac

 AAA 端口访问 19 身份验证优先级验证器基于 mac

 AAA 端口访问 19 身份验证优先级验证器基于 mac

集成指南
HPE Aruba Networking
© Axis Communications AB, 2023 – 2024