使用ISE 3.2為Nexus 9K配置自定義TACACS角色

目錄

箇介

必要條件

需求

採用元件

背景資訊

設定

網路圖表

第1步:配置Nexus 9000

步驟2.配置身份服務引擎3.2

驗證

疑難排解

簡介

本文檔介紹如何透過NK9上的CLI為TACACS配置自定義Nexus角色。

必要條件

需求

思科建議您瞭解以下主題:

- TACACS+
- ISE 3.2

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Nexus9000, NXOS映像檔案為: bootflash:///nxos.9.3.5.bin
- 身分辨識服務引擎版本3.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

許可要求:

Cisco NX-OS - TACACS+不需要許可證。

思科身份服務引擎-對於新的ISE安裝,您擁有90天評估期許可證,可以訪問所有ISE功能,如果您 沒有評估許可證,為了使用ISE TACACS功能,您需要裝置管理員許可證用於執行身份驗證的策略 伺服器節點。

在管理員/幫助台使用者在Nexus裝置上進行身份驗證後,ISE返回所需的Nexus shell角色。

指定此角色的使用者可執行基本故障排除並退回某些埠。

獲得Nexus角色的TACACS會話必須能夠僅使用和運行以下命令和操作:

- 訪問配置終端,使其僅執行從1/1-1/21到1/25-1/30的關閉介面和不關閉介面
- ssh
- ssh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- 啟用

設定

網路圖表



流程元件圖表

第1步:配置Nexus 9000

1. AAA配置。



警告:啟用TACACS身份驗證後,Nexus裝置將停止使用本地身份驗證並開始使用基於 AAA伺服器的身份驗證。

Nexus9000(config)# feature tacacs+ Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample Nexus9000(config)# tacacs-server key 0 "Nexus3xample" Nexus9000(config)# aaa group server tacacs+ IsePsnServers Nexus9000(config-tacacs+)# server <Your ISE IP> Nexus9000(config)# aaa authentication login default group IsePsnServers local

2. 根據指定的需求設定自訂角色。

Nexus9000(config)# role name helpdesk Nexus9000(config-role)# description Can perform basic Toubleshooting and bounce certain ports Nexus9000(config-role)# rule 1 permit read Nexus9000(config-role)# rule 2 permit command enable *

```
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown
vlan policy deny
interface policy deny
                                      permit interface Ethernet1/1
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/2
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/3
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/4
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/5
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/6
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/7
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/8
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/8
                                      permit interface Ethernet1/9
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/10
                                      permit interface Ethernet1/11
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/12
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/13
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/14
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/15
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/16
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/17
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/18
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/19
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/20
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/21
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/22
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/25
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/26
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/27
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/28
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/29
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/30
```

Copy complete.

步驟 2.配置身份服務引擎3.2

1. 配置Nexus TACACS會話期間使用的標識。

使用ISE本地身份驗證。

導航到Administration > Identity Management > Groups頁籤並建立使用者需要加入的組,為此演示 建立的身份組為iseUsers。

≡	С	isco	ISE		Administr	ration • Identity Manageme	ent	A Evaluation Mode 29 Days	٩	0	Q	٩
lder	ntitie	es	Groups	External Id	entity Sources	Identity Source Sequence	es Settings					
I	denti	ity Gr	oups			ups > New User Identity Group						
	ΞQ				Identity Grou	up						
		19 10	ndpoint Ide	mtity Groups	* Name	iseUsers						
		Ξ.	Jser Identity	Groups	Description							
							Submit	Cancel				

建立使用者群組

按一下Submit按鈕。

然後導航到Administration > Identity Management > Identity頁籤。

按Add按鈕。



使用者建立

作為必填欄位的一部分,從使用者名稱開始,本示例中使用使用者名稱iseiscool。

Network Access Users List >	> New Network Access User	
✓ Network Access	User	
* Username	iseiscool	
Status	Z Enabled 🗸	
Account Name Alias		
Email		

下一步是為建立的使用者名稱分配密碼,VainillalSE97是本演示中使用的密碼。

imes Passwords						
Password Type:	Internal Users					
Password Lifetime	:					
 With Expiration Password will ex 	• With Expiration ① Password will expire in 60 days					
O Never Expires						
	Password		Re-Enter Password			
* Login Password				Generate Password	0	
Enable Password				Generate Password	()	

指定密碼

最後,將使用者分配到之前建立的組,在本例中為iseUsers。

∼ Us	er Groups		
:	iseUsers	<u> </u>	

命名使用者並建立使用者

2. 配置並增加網路裝置。

將NEXUS 9000裝置增加到ISE 管理>網路資源>網路裝置

按一下Add按鈕以開始。

Netv	work [Devices				
						Selected 0
🖉 Edit	+ Add	Duplicate	لى Import	스 Export 🗸	🔒 Generate PAC	💼 Delete 🗸
	Name -	^ IP/Mask	Profile N	ame	Location	Туре

在表單中輸入值,為正在建立的NAD分配名稱,並為TACACS通話從NAD與ISE聯絡的IP。

≡ Cisco ISE	Work Centers · Device A	dministration	► Evaluation Mode 27 Days Q ⑦					٢
Overview Identities	User Identity Groups Ext Id Sources	Network Resources	Policy Elements	More \vee				
Network Devices	Network Devices List > New Network Device							
Network Device Groups	Network Devices							
Default Devices								
TACACS External Servers	Name NEXUS9K							
TACACS Server Sequence	Description Nexus Device For TAC	CACS						
	IP Address 🗸 * IP :	A.B.C.D / 32						
	Device Profile Eisco							
	Model Name							
	Software Version							
	Network Device Group							

配置網路裝置

下拉選項可以保留為空白並可省略,這些選項旨在按位置、裝置型別和版本對您的NAD進行分類 ,然後根據這些過濾器更改身份驗證流程。

在Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings上。

增加您在此演示的NAD配置下使用的共用金鑰,此演示中使用Nexus3xample。

網路存取裝置頁面



TACACS配置部分

按一下Submit按鈕儲存更改。

3. ISE上的TACACS配置。

再次檢查您在Nexus 9k中配置的PSN是否啟用了Device Admin選項。



注意:啟用裝置管理服務不會導致ISE重新啟動。



PSN裝置管理功能檢查

可以在ISE選單Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services下檢查此情況。

• 建立一個TACACS配置檔案,如果身份驗證成功,它將角色幫助台返回給Nexus裝置。

從ISE選單,導航到工作中心>裝置管理>策略元素>結果> TACACS配置檔案,然後按一下增加按鈕

o

≡ Cisco ISE	Work Centers · Device Adn	ninistration	A Evaluation Mode 27 Days	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Overview Identities User	r Identity Groups Ext Id Sources	Network Resources	Policy Elements More ~	
Conditions >	TACACS Profiles			
Network Conditions				
Results ~		Rows/Page	$\frac{4}{2} \frac{\sqrt{2}}{2} \langle \langle 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ $	Go 4 Total Rows
Allowed Protocols	${\cal G}$ Add Duplicate Trash \vee Edit			
TACACS Command Sets				
TACACS Profiles	Name Name	Type Description		
	Default Shell Profile	Shell Default Shell Profile		
	Deny All Shell Profile	Shell Deny All Shell Profile		

TACACS配置檔案

指定「名稱」,並選擇性地指定摘要。

≡ Cisco ISE	Work Centers · Device Administration	🛕 Evaluation Mode 27 Days Q 🔗 🕫 🏟
Overview Identities	User Identity Groups Ext Id Sources Network Reso	ources Policy Elements More ~
Conditions	> TACACS Profiles > New TACACS Profile	
Network Conditions		
Results	∨ Nexus Helpdesk	
Allowed Protocols		
TACACS Command Sets		
TACACS Profiles	Description This TACACS profile will be sent if the	
	user is part of the helpdesk team	
	group	

命名Tacacs配置檔案

忽略任務屬性檢視部分並導航到原始檢視部分。

並輸入值shell : roles="helpdesk"。

≡ Cisco ISE	Work Centers · Device Administration	🛕 Evaluation Mode 27 Days 📿 🔗 🕫 🕸
Overview Identities	User Identity Groups Ext Id Sources Network Resources	Policy Elements More ~
	Name	
Conditions	> Nexus Helpdesk	
Network Conditions	> Description	
Results	This TACACS profile will be sent if the user is part of the helpdesk team group	
Allowed Protocols	group	
TACACS Command Sets		
TACACS Profiles	Task Attribute View Raw View	
	Profile Attributes	
	shell:roles=" helpdesk"	
	Cancel	Save

新增設定檔屬性

配置包含身份驗證策略和授權策略的策略集。

在ISE選單上,訪問Work Centers > Device Administration > Device Admin Policy Sets。

出於演示目的,使用預設策略集。但是,可以建立另一個策略集,並附帶條件以匹配特定方案。

按一下列尾的箭頭。

≡ (Cisco	ISE		Work Cer	nters · Device	Administratio	on		🛕 Evalua	ition Mode 2	' Days	Q Ø	9	٢
Overvi	ew	Identities	User Identity	Groups	Ext Id Sources	s Network	Resources	Policy Elem	ents	More \vee				
Policy	/ Sets							Reset	Reset	Policyset Hi	tcounts		Save	
	Status	Policy Set N	lame	Description	c	Conditions	Alle	owed Protocols	/ Server	Sequence	Hits	Actions	View	v
C	(Searc													
	0	Default		Tacacs Default	policy set		De	efault Device Adr				ŝ	>	
											Reset		Save	

Device Admin Policy Sets page -裝置管理原則集頁面

進入策略集配置後,向下滾動並展開Authentication Policy部分。

按一下Add圖示。

對於此配置示例,「名稱」值為內部身份驗證,選擇的條件為網路裝置(Nexus) IP(替換A.B.C.D.)。 此身份驗證策略使用內部使用者身份庫。

≡ Cisco ISE	Work Centers · Device Ad	dministration 🔒 🗈	raluation Mode 27 Days Q () 2 9 ¢
Overview Identities Us	ser Identity Groups Ext Id Sources	Network Resources Policy Elements	More \sim	
+ Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
		Internal Users	1	
		└ Options		
		If Auth fail REJECT		
S Internal Authenti	ication 🖳 Network Access-Device IP Ac	ddress EQUALS A.B.C.D If User not fo REJECT	und	ŝ
		If Process fai DROP	 <i> </i>	
		All_User_ID_St	ores //	-0-
🧭 Default		> Options		ŝ

身份驗證策略

以下是條件的配置方式。

選擇Network Access > Device IP address Dictionary Attribute。

Conditions Studio								e	•
Library		Edit	tor						
Search by Name			Network Ac	cess Device IP Address					⊗
	10 E 🕈		t attribute for co						
EAP-MSCHAPv2		Q	•	, 0	©	1	Ŀ	Save	
EAP-TLS			Dictionary	Attribute	ID	Info			
			All Dictionaries 🗡	Attribute	ID				
		Ð	DEVICE	Device Type					
		₽	DEVICE	Model Name					
		₽	DEVICE	Network Device Profil	e				
		₽	DEVICE	Software Version					
			Network Access	Device IP Address					
			Network Access	NetworkDeviceName					
								Use	

身份驗證策略的Condition studio

用正確的IP替換<Nexus IP地址>註釋。

Conditions Studio				0	>
Library	E	Editor			
Search by Name			Network Access Device IP Address	(8
	: 🕈	Ģ	Equals 🗸 <nexus address="" ip=""></nexus>		
E EAP-MSCHAPv2			Enter Valid IPV4 or IPV6 address		
🗄 📄 EAP-TLS			Set to 'Is not' Duplicate Set	ave	
			NEW AND OR		
			Close	е	

增加IP過濾器

按一下Use按鈕。

此條件僅由您配置的Nexus裝置滿足,但是,如果目的是為大量裝置啟用此條件,則必須考慮其他 條件。

然後導航到Authorization Policy部分並展開它。

按一下+ (加號)圖示。

=	Evaluation Mode 27 Da									?7 Days	۹ (0 5	0 4							
Over	view	Identi	ties	User Ide	ntity Gro	oups	Ext Id Sour	ces	Networ	k Resource	s Pol	licy Elem	ents	Device /	Admin Po	licy Sets	Μ	lore \vee		
	St	tatus P	olicy Se	t Name	D	escriptio	n	Cor	nditions						Allowed	Protocols	/ Serv	er Seque	nce	Hits
	Q																			
		0	Default			Tacacs D	efault policy set	t							Defaul	Device A	dmin			
	> Aut	henticatio	on Policy	(2)																
	> Aut	horizatior	Policy ·	- Local Exc	eptions															
	> Aut	horizatior	Policy	- Global Ex	ceptions															
	∨ Aut	horizatior	Policy	(1)																
										Results										
		Status	Rule	Name		Condit	ions			Command	Sets			Shell Profi	les			Hits	Acti	ions
	C	2 Searct																		
										+										
		0	Defaul	t					-	DenyAllCor	mmands		0+	Deny All	Shell Profi	e	0 +	- o	ŝ	}

在本示例中,使用了NEXUS HELP DESK作為授權策略的名稱。

V Authorization Policy (1)												
		Results										
🕂 Status Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions							
Q Search												
NEXUS HELP DESK	Network Access-Device IP Address EQUALS A.B.C.D		+ Nexus Helpdesk $ < > + $		ŵ							
🧭 Default		DenyAllCommands	⊢ _ Deny All Shell Profile		ŝ							
			Reset		Save							

授權策略的Condition studio

在身份驗證策略中配置的相同條件用於授權策略。

在Shell Profiles列中,選擇Nexus技術支援之前配置的配置檔案。

最後,按一下Save按鈕。

驗證

使用本節內容,確認您的組態是否正常運作。

從ISE GUI中,導航到操作> TACACS >即時日誌,辨識與所用使用者名稱匹配的記錄,然後按一下 授權事件的即時日誌詳細資訊。



TACACS即時日誌

作為此報告所包含詳細資訊的一部分,您可以找到響應部分,從中可以看到ISE如何返回值 shell : roles="helpdesk"

Response

{Author-Reply-Status=PassRepl; AVPair=shell:roles="helpdesk"; }

即時日誌詳細資訊響應

在Nexus裝置上:

Nexus9000 login: iseiscool Password: VainillaISE97 Nexus9000# conf t Enter configuration commands, one per line. End with CNTL/Z. Nexus9000(config)# interface ethernet 1/23 % Interface permission denied Nexus9000(config)# ? interface Configure interfaces Show running system information show end Go to exec mode Exit from command interpreter exit Nexus9000(config)# role name test % Permission denied for the role Nexus9000(config)# Nexus9000(config)# interface loopback 0 % Interface permission denied Nexus9000(config)# Nexus9000# conf t Nexus9000(config)# interface ethernet 1/5 Notice that only the commands allowed are listed. Nexus9000(config-if)# ? Negate a command or set its defaults no Show running system information show shutdown Enable/disable an interface Go to exec mode end Exit from command interpreter exit Nexus9000(config-if)# cdp Nexus9000(config-if)# cdp enable % Permission denied for the role

疑難排解

Nexus9000(config-if)#

驗證是否可從Nexus裝置訪問ISE。Nexus9000# ping <您的ISE IP> PING <您的ISE IP>(<您的ISE IP> 56資料位元組 來自<您的ISE IP>的64位元組:icmp_seq=0 ttl=59 time=1.22 ms 來自<您的ISE IP>的64位元組:icmp_seq=1 ttl=59 time=0.739 ms 來自<您的ISE IP>的64位元組:icmp_seq=2 ttl=59 time=0.686 ms 來自<您的ISE IP>的64位元組:icmp_seq=3 ttl=59 time=0.71 ms 來自<您的ISE IP>的64位元組:icmp_seq=3 ttl=59 time=0.71 ms 來自<您的ISE IP>的64位元組:icmp_seq=4 ttl=59 time=0.72 ms
驗證ISE和Nexus裝置之間的埠49是否已打開。 Nexus9000# telnet <您的ISE IP> 49

正在嘗試<您的ISE IP> ... 已連線到<您的ISE IP>。 逸出字元是'^]'。 • 使用以下調試:

debug tacacs+ all

Nexus9000編號

Nexus9000# 2024年4月19日22:50:44.199329 tacacs: event_loop():正在呼叫process_rd_fd_set 2024年4月19日22:50:44.199355 tacacs: process_rd_fd_set: calling callback for fd 6 2024年4月19日22:50:44.199392 tacacs: fsrv dnt使用8421操作碼 2024年4月19日22:50:44.199406 tacacs: process_implicit_cfs_session_start: entering... 2024年4月19日22:50:44.199414 tacacs: process implicit cfs session start:正在退出;我們處 於分發停用狀態 2024年4月19日22:50:44.199424 tacacs: process aaa tplus request: 輸入aaa session id 0 2024年4月19日22:50:44.199438 tacacs: process_aaa_tplus_request: 檢查伺服器組 IsePsnServers的mgmt0埠的狀態 2024年4月19日22:50:44.199451 tacacs: tacacs_global_config(4220): 輸入..... 2024年4月19日22:50:44.199466 tacacs: tacacs_global_config(4577): GET_REQ... 2024年4月19日22:50:44.208027 tacacs: tacacs global config(4701):已恢復全局協定配置操作 的返回值:SUCCESS 2024年4月19日22:50:44.208045 tacacs: tacacs_global_config(4716): REQ: num server 0 2024年4月19日22:50:44.208054 tacacs: tacacs_global_config: REQ: num group 1 2024年4月19日22:50:44.208062 tacacs: tacacs_global_config: REQ: num timeout 5 2024年4月19日22:50:44.208070 tacacs: tacacs_global_config: REQ: num deadtime 0 2024年4月19日22:50:44.208078 tacacs: tacacs_global_config: REQ: num encryption_type 7 2024年4月19日22:50:44.208086 tacacs: tacacs global config:返回retval 0 2024年4月19日22:50:44.208098 tacacs: process aaa tplus request: group info填充在 aaa_reg中,因此使用伺服器組IsePsnServers 2024年4月19日22:50:44.208108 tacacs: tacacs servergroup config: 輸入伺服器組,索引0 2024年4月19日22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ for Protocol server group index : 0 name : 2024年4月19日22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str =無此類pss金鑰 2024年4月19日22:50:44.208160 tacacs: tacacs_pss2_move2key:呼叫pss2_getkey 2024年4月19日22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ got Protocol server group index : 2 name : IsePsnServers 2024年4月19日22:50:44.208184 tacacs: tacacs_servergroup_config:返回協定組操作的返回值 : SUCCESS 2024年4月19日22:50:44.208194 tacacs: tacacs servergroup config:返回協定伺服器組的retval 0: IsePsnServers 2024年4月19日22:50:44.208210 tacacs: process_aaa_tplus_request: Group lsePsnServers found。對應的vrf為預設值,source-intf為0 2024年4月19日22:50:44.208224 tacacs: process_aaa_tplus_request: checking for mgmt0 vrf: management against vrf: default of requested group 2024年4月19日22:50:44.208256 tacacs: process_aaa_tplus_request: mgmt_if 83886080 2024年4月19日22:50:44.208272 tacacs: process_aaa_tplus_request: global_src_intf:0,本地 src intf為0, vrf name為預設值 2024年4月19日22:50:44.208286 tacacs: create_tplus_req_state_machine(902): 輸入aaa session id 0

2024年4月19日22:50:44.208295 tacacs:狀態機器計數0 2024年4月19日22:50:44.208307 tacacs: init_tplus_req_state_machine:輸入aaa session id 0 2024年4月19日22:50:44.208317 tacacs: init_tplus_req_state_machine(1298): tplus_ctx為 NULL。如果編寫和測試,它應該是 2024年4月19日22:50:44.208327 tacacs: tacacs_servergroup_config:正在輸入伺服器組 IsePsnServers,索引0 2024年4月19日22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ for Protocol server group index : 0 name : IsePsnServers 2024年4月19日22:50:44.208357 tacacs: find_tacacs_servergroup:輸入用於伺服器組 IsePsnServers 2024年4月19日22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str =成功 2024年4月19日22:50:44.208382 tacacs: find_tacacs_servergroup:正在退出伺服器組 IsePsnServers index is 2 2024年4月19日22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: find tacacs servergroup error 0 for Protocol server group IsePsnServers 2024年4月19日22:50:44.208420 tacacs : tacacs_pss2_move2key : rcode = 0 syserr2str =成功 2024年4月19日22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ got Protocol server group index : 2 name : IsePsnServers 2024年A2024年4月19日22:52024 4月19日22:52024 4月19日22:5 Nexus9000編號

 執行資料包捕獲(要檢視資料包詳細資訊,您必須更改Wireshark TACACS+首選項,並更新 Nexus和ISE使用的共用金鑰)

No.		Time	S c	De Protocol	Lengt	th Info			
	66	22:25:08.75	7401	TACACS+	:	107 R: Auth	norization		
> ~	Transmi TACACS+	ssion Contro	l Protocol	, Src Port: 4	9, Dst Port: 5	8863, Seq:	1, Ack: 90, Le	n: 41	
	Major Minor Type: Seque > Flags Sessi Packe Encry > Decry Au Se Da Ar Ar Ar	version: T version: 0 Authorizat ence number: s: 0x00 (Enc lon ID: 1136 et length: 2 vpted Reply vpted Reply th Status: F rver Msg ler ta length: 6 g count: 1 g[0] length: g[0] value:	ACACS+ ion (2) 2 rypted payl 115821 9 PASS_REPL (ngth: 0) 22 shell:role	load, Multiple 0x02) s="helpdesk"	Connections)				

TACACS授權封包

• 驗證ISE和Nexus端的共用金鑰是否相同。這也可以在Wireshark中檢查。

CACS+

Major version: TACACS+ Minor version: 1 Type: Authentication (1) Sequence number: 1 Flags: 0x00 (Encrypted payload, Multiple Connections) Session ID: 232251350 Packet length: 43 Encrypted Request Decrypted Request Action: Inbound Login (1) Privilege Level: 1 Authentication type: PAP (2) Service: Login (1) User len: 9 User: iseiscool Port len: 1 Port: 0 Remaddr len: 12 Remote Address: Password Length: 13 Password: VainillaISE97

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。