# Configuración del rol TACACS personalizado para Nexus 9K mediante ISE 3.2

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Paso 1: Configuración de Nexus 9000
Paso 2. Configuración de Identity Service Engine 3.2
Verificación
Troubleshoot

# Introducción

Este documento describe cómo configurar un rol personalizado de Nexus para TACACS a través de CLI en NK9.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- TACACS+
- ISE 3.2

## **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El archivo de imagen de Cisco Nexus 9000, NXOS es: bootflash:///nxos.9.3.5.bin
- Identity Service Engine versión 3.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

Requisitos de licencia:

Cisco NX-OS: TACACS+ no requiere licencia.

Cisco Identity Service Engine: para las instalaciones de ISE nuevas, dispone de una licencia de período de evaluación de 90 días que tiene acceso a todas las funciones de ISE. Si no dispone de una licencia de evaluación, para utilizar la función ISE TACACS necesita una licencia Device Admin para el nodo de Policy Server que realiza la autenticación.

Una vez que los usuarios de administración/soporte técnico se hayan autenticado en el dispositivo Nexus, ISE devuelve el rol de shell de Nexus deseado.

El usuario asignado a esta función puede llevar a cabo la resolución de problemas básica y rebotar determinados puertos.

La sesión TACACS que obtiene el rol Nexus solo debe poder utilizar y ejecutar los siguientes comandos y acciones:

- Acceso para configurar el terminal para que SÓLO ejecute las interfaces de apagado y no cierre de 1/1-1/21 y 1/25-1/30
- ssh
- ssh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Habilitar

# Configurar

Diagrama de la red



Diagrama de componentes de flujo

## Paso 1: Configuración de Nexus 9000

#### 1. Configuración AAA.



Advertencia: después de activar la autenticación TACACS, el dispositivo Nexus deja de utilizar la autenticación local y comienza a utilizar la autenticación basada en servidor AAA.

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. Configure el rol personalizado con los requisitos especificados.

```
Nexus9000(config)# role name helpdesk
                          description Can perform basic Toubleshooting and bounce certain ports
Nexus9000(config-role)#
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
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/1
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/2
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
                                      permit interface Ethernet1/8
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/9
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/10
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/11
                                      permit interface Ethernet1/12
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/13
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/14
                                      permit interface Ethernet1/15
Nexus9000(config-role-interface)#
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
                                      permit interface Ethernet1/27
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/28
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/29
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/30
```

Copy complete.

## Paso 2. Configuración de Identity Service Engine 3.2

1. Configure la identidad que se utiliza durante la sesión TACACS de Nexus.

Se utiliza la autenticación local de ISE.

Vaya a la pestaña Administration > Identity Management > Groups y cree el grupo del que el usuario debe ser parte; el grupo de identidad creado para esta demostración es iseUsers.

≡ Cisco ISE	Administration · Identity Management	🔺 Evaluation Mode 29 Days Q 🕜 🞜 🕸
Identities Groups External Ic	Ientity Sources Identity Source Sequences Setti	ings
Identity Groups	User Identity Groups > New User Identity Group	
< E	* Name iseUsers	
> 🛅 User Identity Groups	Description	
	Submit	Cancel

Creación de un grupo de usuarios

Haga clic en el botón Submit.

A continuación, vaya a la ficha Administration > Identity Management > Identity.

#### Presione el botón Add.

<b>≡ Cisco</b> ISE	Administration · Identity Management	🛕 Evaluation Mode 29 Days Q 🕜 ᇩ জ
Identities Groups Ext	ternal Identity Sources Identity Source Sequences Se	ettings
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 0 🦪 🚳
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🕧 Ex	port 🗸 📋 Delete 🗸 🗸 🗸 All 🗸 🏹
	Status Username A Description First I	Name Last Name Email Address User Identity Groups Adr
	No	data available

Creación de usuario

Como parte de los campos obligatorios, comience con el nombre del usuario, en este ejemplo se utiliza el nombre de usuario iseiscool.

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

Nombrar al usuario y crearlo

El siguiente paso es asignar una contraseña al nombre de usuario creado, VainillaISE97 es la contraseña utilizada en esta demostración.

nternal Users			
0 Dire in 60 days			
Ð			
Password		Re-Enter Password	
·····			Generate Password
			Generate Password
	nternal Users ire in <b>60 days</b> Password	nternal Users ine in 60 days Password 	nternal Users

Asignación de contraseña

Por último, asigne el usuario al grupo creado anteriormente, que en este caso es iseUsers.

∨ Use	er Groups		
:	iseUsers	~	1

2. Configure y agregue el dispositivo de red.

Agregue el dispositivo NEXUS 9000 a ISE Administration > Network Resources > Network Devices

Haga clic en el botón Add para comenzar.

Netv	work	Devices				
						Selected 0
🖉 Edit	+ Add	Duplicate	للي Import	🏦 Export 🗸	🔒 Generate PAC	💼 Delete 🗸
	Name	∧ IP/Mask	Profile N	ame	Location	Туре

Página Dispositivo de Acceso a Red

Introduzca los valores en el formulario, asigne un nombre al NAD que está creando y una IP desde la que el NAD se ponga en contacto con ISE para la conversación TACACS.

≡ Cisco ISE	Work Ce	enters · Device Adr	🛕 Eva	0	6	٥			
Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	More $\vee$				
Network Devices		New Network Device							
Network Device Groups	Network Devices								
Default Devices	Г								
TACACS External Servers	Name	NEXUS9K							
TACACS Server Sequence	Description N	lexus Device For TACA	cs						
	IP Address	~ * IP : A.E	3.C.D / 32 {						
	Device Profile	Cisco							
	Model Name								
	Software Version								
	Network Device Gre	oup							

Configurar dispositivo de red

Las opciones desplegables se pueden dejar en blanco y se pueden omitir; estas opciones están diseñadas para categorizar sus NAD por ubicación, tipo de dispositivo, versión y, a continuación, cambiar el flujo de autenticación basado en estos filtros.

En Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings .

Agregue el secreto compartido que utilizó en la configuración de NAD para esta demostración; en

esta demostración se utiliza Nexus3xample.



sección de configuración de TACACS

Guarde los cambios haciendo clic en el botón Submit.

3. Configuración de TACACS en ISE.

Compruebe dos veces que el PSN que ha configurado en el Nexus 9k tiene la opción Device Admin habilitada.



Nota: Habilitar el servicio Device Admin NO provoca un reinicio en ISE.



Comprobación de la función PSN Device Admin

Esto se puede verificar en el menú de ISE Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services.

• Cree un perfil TACACS que devuelva el servicio de asistencia al dispositivo Nexus si la autenticación es correcta.

En el menú de ISE, vaya a Workcenters > Device Administration > Policy Elements > Results >

TACACS Profiles y haga clic en el botón Add.

<b>≡ Cisco</b> ISE	Work Centers · Device Adr	ninistration	🛕 Evaluation Mode 27 Days Q 🕜 🞜 核			
Overview Identities Use	r Identity Groups Ext Id Sources	Network Resources	Policy Elements More $\vee$			
Conditions >	TACACS Profiles					
Network Conditions >						
Results ~		Rows/Page	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	Go 4 Total Rows		
Allowed Protocols	$egin{array}{ccc} egin{array}{ccc} Add \end{array} & Duplicate & Trash & \lor & Edit \end{array}$					
TACACS Command Sets	Name	Type Description				
TACACS Profiles						
	Default Shell Profile	Shell Default Shell Profile				
	Deny All Shell Profile	Shell Deny All Shell Profile	,			

Perfil TACACS

Asigne un nombre y, opcionalmente, una descripción.



Perfil de Tacacs de denominación

Omita la sección Vista de atributos de tarea y navegue hasta la sección Vista sin procesar.

E introduzca el valor shell:roles="helpdesk".

<b>≡ Cisco</b> ISE	Work Centers · Device Administration	🛕 Evaluation Mode 27 Days Q 🕜 🔎 🚳
Overview Identities	User Identity Groups Ext Id Sources Network Re	esources 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	a,oop O	
TACACS Command Sets		
TACACS Profiles	Task Attribute View Raw View	
	Profile Attributes	
	shell:roles=" helpdesk"	
		Cancel Save

Adición de atributos de perfil

Configure el conjunto de directivas que incluye la directiva de autenticación y la directiva de autorización.

En el menú de ISE, acceda a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

A modo de demostración, se utiliza el conjunto de políticas predeterminadas. Sin embargo, se puede crear otro conjunto de directivas, con condiciones para que coincida con escenarios específicos.

Haga clic en la flecha situada al final de la fila.

E Cisco ISE     Work Centers · Device Administration							🛕 Evalu	ation Mode 2	7 Days	୦ ୭	} ۹	\$	
Overview	Identitie	es User Iden	tity Groups	Ext Id Sources	Network Resourc	es Poli	icy Elem	ents	More 🗸				
Policy Set	s					Res	et	Reset	Policyset Hi			Save	
+ Sta	tus Policy	Set Name	Description	ı Co	nditions	Allowed P	rotocols	/ Server	Sequence	Hits	Actions	View	
Q Se													
e	Default		Tacacs Defau	It policy set		Default D	evice Adr				ŝ	>	
										Reset		Save	

Página Conjuntos de directivas de administración de dispositivos

Una vez dentro de la configuración del conjunto de políticas, desplácese hacia abajo y expanda la sección Política de autenticación.

Haga clic en el icono Add.

Para este ejemplo de configuración, el valor Name es Internal Authentication y la condición elegida es Network Device (Nexus) IP (sustituya el A.B.C.D.). Esta directiva de autenticación utiliza el almacén de identidad de usuarios internos.

	Cisco I	SE	Work Centers · Device Administration			🛕 Eva	luation Mode 27 Days	ର ଡ	) ,	<u> </u>
Ov	erview I	dentities User Identity	Groups	Ext Id Sources	Network Resources	Policy Elements	More 🗸			
	+ Status	Rule Name	Condition	15		Use		Hits	Actions	
	Q Searc									
						Internal Users				
		✓ Options								
	Internal Authentication				If Auth fail REJECT			- 0 -		
		Internal Authentication		P Network Access-Device IP Addr	ress EQUALS A.B.C.D	If User not four	nd		ŝ	
					If Process fail					
_						All_User_ID_Stor				
	0	Default				> Options			ŝ	

Política de autenticación

Así es como se configuró la condición.

Seleccione Network Access > Device IP address Dictionary Attribute.

Conditions Studio								0
Library		Edi	tor					
Search by Name			Network Ac	ccess-Device IP Address				×
	9 E 🕈							
EAP-MSCHAPv2		•	•	- 2	Q	1	ŧ.	Save
🗄 🖹 EAP-TLS			Dictionary	Attribute	ID	Info		
			All Dictionaries 🗡	Attribute	ID			
		₽	DEVICE	Device Type				
		₽	DEVICE	Model Name				
			DEVICE	Network Device Profile				
		₽	DEVICE	Software Version				
		₽	Network Access	Device IP Address				
		₽	Network Access	NetworkDeviceName				
								Use

Estudio de condición para la política de autenticación

Sustituya el comentario <dirección IP de Nexus> por la dirección IP correcta.

Conditions Studio								Ø	
Library		Editor							~
Search by Name			Network Acc	ess-Device IP Address					⊗
		Ģ	Equals 🗸	<nexus address="" ip=""></nexus>					
EAP-MSCHAPv2									
EAP-TLS								Save	
					AND OR				
							_		
						Close		Use	

Adición del filtro IP

Haga clic en el botón Use.

Esta condición solo la cumple el dispositivo Nexus configurado; sin embargo, si el propósito es

habilitar esta condición para una gran cantidad de dispositivos, se debe considerar una condición diferente.

A continuación, desplácese a la sección Directiva de autorización y expándala.

Haga clic en el icono + (más).

	Cisco	ISE				Work Centers	• Device A	dministration			<b>A</b> E	valuation Mode 27	7 Days O	0	6	9 E
Oven	view	Identi	ties	User Identit	y Groups	Ext Id Source	s Netw	ork Resources	Policy Eleme	ents	Device Admir	Policy Sets	More			
	Sta	atus P	olicy Se	et Name	Descri	ption	Conditions				Allo	wed Protocols	/ Server S	equen	ce	Hits
	Q															
		0	Default		Таса	cs Default policy set					De	fault Device Ad				0
	> Auth	enticatio	on Policy	ı (2)												
	> Auth	orization	Policy	- Local Excepti	ons											
	> Auth	orization	Policy	- Global Except	ions											
	$\vee$ Auth	orization	Policy	(1)												
								Results								
		Status	Rule	Name	Co	nditions		Command Sets			Shell Profiles			Hits	Actio	ons
	(0	Search														
								+								
		0	Defaul	lt				DenyAllComman	nds U		Deny All Shell				ŝ	

Sección de directiva de autorización

En este ejemplo se utilizó NEXUS HELP DESK como nombre de la política de autorización.

V Authorization Policy (1)										
		Results								
Ŧ Status Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions					
Q Search										
NEXUS HELP DESK	Retwork Access-Device IP Address EQUALS A.B.C.D		Nexus Helpdesk $\propto$ $\sim$ +		¢					
🥝 Default		DenyAllCommands	Deny All Shell Profile		ŝ					
			Reset		Save					

Estudio de condiciones para la directiva de autorización

La misma condición que se configuró en la directiva de autenticación se utiliza para la directiva de autorización.

En la columna Perfiles de shell, se selecciona el perfil configurado antes de Nexus Helpdesk.

Por último, haga clic en el botón Save.

# Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Desde la GUI de ISE, navegue hasta Operations > TACACS > Live Logs, identifique el registro que coincida con el nombre de usuario utilizado y haga clic en Live Log Detail del evento de autorización.

= Cisco ISE						Operations • TACACS	Operations - TACACS				ation Mode 11 Days Q	0 9 0
Live Lo	gs			/								
	Apr 19, 2024 10:25:08.7		R	iseiscool	Authorization		Default >> NEXUS HELP DESK	ISE PSN	NEXUS9K	«NEXUS IP»	Device Type#All	Location#All Loc.
	Apr 19, 2024 10:25:08.7			iselscool	Authentication	Default >> Internal Authentication		ISE PSN	NEXUS9K	<nexus ip=""></nexus>	Device Type#All	Location#All Loc.

Live Log de TACACS

Como parte de los detalles que incluye este informe, se puede encontrar la sección Respuesta, donde puede ver cómo ISE devolvió el valor shell:roles="helpdesk"

	Respon	se	{Author-Reply-Status=PassRepl; AVPair=shell:roles=" helpdesk" ; }							
	Respuesta deta	llada de Live Log								
En el dispositivo Nexus:										
	<pre>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 Show running system information end Go to exec mode exit Exit from command interpreter</pre>									
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)# ?

no Negate a command or set its defaults show Show running system information shutdown Enable/disable an interface end Go to exec mode exit Exit from command interpreter

Nexus9000(config-if)# cdp Nexus9000(config-if)# cdp enable % Permission denied for the role Nexus9000(config-if)#

# Troubleshoot

 Verifique que ISE sea accesible desde el dispositivo Nexus.Nexus9000# ping <Su IP de ISE>

PING <Su IP de ISE> (<Su IP de ISE>> 56 bytes de datos 64 bytes de <Su IP de ISE>: icmp\_seq=0 ttl=59 tiempo=1,22 ms 64 bytes de <Su IP de ISE>: icmp\_seq=1 ttl=59 tiempo=0,739 ms 64 bytes de <Su IP de ISE>: icmp\_seq=2 ttl=59 tiempo=0,686 ms 64 bytes de <Su IP de ISE>: icmp\_seq=3 ttl=59 tiempo=0,71 ms 64 bytes de <Su IP de ISE>: icmp\_seq=4 ttl=59 tiempo=0,72 ms

- Verifique que el puerto 49 esté abierto entre ISE y el dispositivo Nexus. Nexus9000# telnet <Su IP de ISE> 49 Intentando <Su IP de ISE>... Conectado a <Su IP de ISE> . El carácter de escape es '^]'.
- Utilice estas depuraciones:

debug tacacs+ all

Nexus9000#

Nexus9000# 2024 Apr 19 22:50:44.199329 tacacs: event\_loop(): calling process\_rd\_fd\_set 2024 19 de abril 22:50:44.199355 tacacs: process\_rd\_fd\_set: devolución de llamada de llamada para fd 6

2024 Apr 19 22:50:44.199392 tacacs: fsrv no consumió 8421 opcode

2024 Abr 19 22:50:44.199406 tacacs: process\_implicit\_cfs\_session\_start: introduciendo... 2024 Abril 19 22:50:44.199414 tacacs: process\_implicit\_cfs\_session\_start: salir; estamos en estado de distribución inhabilitada

2024 Apr 19 22:50:44.199424 tacacs: process\_aaa\_tplus\_request: introducción de aaa session id 0

2024 Apr 19 22:50:44.199438 tacacs: process\_aaa\_tplus\_request:Comprobando el estado del puerto mgmt0 con servergroup IsePsnServers

2024 19 de abril 22:50:44.199451 tacacs: tacacs\_global\_config(4220): introduciendo ...

2024 19 de abril 22:50:44.199466 tacacs: tacacs\_global\_config(4577): GET\_REQ...

2024 19 de abril 22:50:44.208027 tacacs: tacacs\_global\_config(4701): recuperó el valor devuelto de la operación de configuración de protocolo global:SUCCESS

2024 19 de abril 22:50:44.208045 tacacs: tacacs\_global\_config(4716): REQ:num server 0

2024 19 de abril 22:50:44.208054 tacacs: tacacs\_global\_config: REQ:num group 1

2024 Apr 19 22:50:44.208062 tacacs: tacacs\_global\_config: REQ:num timeout 5

2024 Abr 19 22:50:44.208070 tacacs: tacacs\_global\_config: REQ:num deadtime 0

2024 Abr 19 22:50:44.208078 tacacs: tacacs\_global\_config: REQ:num encryption\_type 7

2024 19 de abril 22:50:44.208086 tacacs: tacacs\_global\_config: devolviendo reval 0

2024 Apr 19 22:50:44.208098 tacacs: process\_aaa\_tplus\_request:group\_info se completa en aaa\_req, por lo que el uso de servergroup IsePsnServers

2024 Apr 19 22:50:44.208108 tacacs: tacacs\_servergroup\_config: introducción para el grupo de servidores, índice 0

2024 Abr 19 22:50:44.208117 tacacs: tacacs\_servergroup\_config: GETNEXT\_REQ for Protocol server group index:0 name:

2024 Abr 19 22:50:44.208148 tacacs: tacacs\_pss2\_move2key: rcode = 40480003 syserr2str = no hay tal clave pss

2024 Abr 19 22:50:44.208160 tacacs: tacacs\_pss2\_move2key: llamando a pss2\_getkey 2024 Abr 19 22:50:44.208171 tacacs: tacacs\_servergroup\_config: GETNEXT\_REQ got Protocol server group index:2 name:IsePsnServers

2024 Apr 19 22:50:44.208184 tacacs: tacacs\_servergroup\_config: recuperó el valor devuelto de la operación de grupo de protocolos:SUCCESS

2024 Apr 19 22:50:44.208194 tacacs: tacacs\_servergroup\_config: devolviendo el valor de retorno 0 para el grupo de servidores Protocol:IsePsnServers

2024 Abr 19 22:50:44.208210 tacacs: process\_aaa\_tplus\_request: Se encontraron IsePsnServers de grupo. el vrf correspondiente es el valor predeterminado, source-intf es 0

2024 19 de abril 22:50:44.208224 tacacs: process\_aaa\_tplus\_request: verificación de mgmt0 vrf:management contra vrf:default del grupo solicitado

19 de abril de 2024 22:50:44.208256 tacacs: process\_aaa\_tplus\_request:mgmt\_if 83886080 2024 Abr 19 22:50:44.208272 tacacs: process\_aaa\_tplus\_request:global\_src\_intf : 0, local src\_intf es 0 y vrf\_name es el valor predeterminado

2024 Apr 19 22:50:44.208286 tacacs: create\_tplus\_req\_state\_machine(902): introducción de aaa session id 0

2024 19 de abril 22:50:44.208295 tacacs: recuento de máquinas de estado 0

2024 Apr 19 22:50:44.208307 tacacs: init\_tplus\_req\_state\_machine: introducción de aaa session id 0

2024 Abr 19 22:50:44.208317 tacacs: init\_tplus\_req\_state\_machine(1298):tplus\_ctx es NULL debería ser si autor y prueba

2024 Apr 19 22:50:44.208327 tacacs: tacacs\_servergroup\_config: introducir para el grupo de servidores IsePsnServers, índice 0

2024 Abr 19 22:50:44.208339 tacacs: tacacs\_servergroup\_config: GET\_REQ para el índice de grupo de servidores de protocolo:0 name:IsePsnServers

2024 Apr 19 22:50:44.208357 tacacs: find\_tacacs\_servergroup: introducción para el grupo de servidores IsePsnServers

2024 Abr 19 22:50:44.208372 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = SUCCESS 2024 Abr 19 22:50:44.208382 tacacs: find\_tacacs\_servergroup: salir del grupo de servidores IsePsnServers index es 2 2024 Abr 19 22:50:44.208401 tacacs: tacacs\_servergroup\_config: GET\_REQ: find\_tacacs\_servergroup error 0 para el grupo de servidores de protocolo IsePsnServers 2024 Abr 19 22:50:44.208420 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = SUCCESS 2024 Abr 19 22:50:44.208433 tacacs: tacacs\_servergroup\_config: GET\_REQ got Protocol server group index:2 name:IsePsnServers 2024 A2024 19 do abril 22:52024 19 do abril 22:52024 19 do abril 22:5

2024 A2024 19 de abril 22:52024 19 de abril 22:52024 19 de abril 22:5 Nexus9000#

 Realizar una captura de paquetes (para ver los detalles del paquete, debe cambiar las preferencias de Wireshark TACACS+ y actualizar la clave compartida utilizada por Nexus e ISE)



Paquete de autorización TACACS

• Compruebe que la clave compartida es la misma en ISE y Nexus. Esto también se puede comprobar en Wireshark.

#### 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

Paquete de autenticación

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).