# Integración de CSM TACACS con ISE

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Diagrama de la red Procedimiento de autenticación Configuración de ISE Configuración de CSM Verificación Troubleshoot

### Introducción

Este documento describe el procedimiento para integrar Cisco Security Manager (CSM) con Identity Services Engine (ISE) para la autenticación de usuarios administradores con el protocolo TACACS+.

### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- protocolo TACACS.

#### **Componentes Utilizados**

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

- Servidor CSM versión 4.22
- ISE versión 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Antecedentes

De forma predeterminada, Cisco Security Manager (CSM) utiliza un modo de autenticación denominado CiscoWorks para autenticar y autorizar a los usuarios de forma local, con el fin de disponer de un método de autenticación centralizado, puede utilizar Cisco Identity Service Engine a través del protocolo TACACS.

## Configurar

### Diagrama de la red



#### Procedimiento de autenticación

Paso 1. Inicie sesión en la aplicación CSM con las credenciales del usuario administrador.

Paso 2. El proceso de autenticación desencadena e ISE valida las credenciales localmente o a través de Active Directory.

Paso 3. Una vez que la autenticación se realiza correctamente, ISE envía un paquete de permiso para autorizar el acceso al CSM.

Paso 4. CSM asigna el nombre de usuario con la asignación de rol de usuario local.

Paso 5. ISE muestra un registro en directo de autenticación exitoso.

#### Configuración de ISE

Paso 1. Seleccione el icono de tres líneas se encuentra en la esquina superior izquierda y navegue hasta Administración > Recursos de red > Dispositivos de red.

E Cisco ISE			Admi	nistration - Network Resource	15		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services
Network Devices Default Device	Network	k Devices					
Device Security Settings	0 tat + 44	6d 🚺 Duplicate 🕁 Import	ත් Export 🗸 👌 Generate PAG	Delete 🗸			
	Name	e 🗠 IP/Mask Profile N	ame Location	Туре	Description		

**Paso 2.** Seleccione el botón **+Add** e ingrese los valores adecuados para Network Access Device Name y IP Address, luego verifique la **casilla de verificación TACACS Authentication Settings** y defina un secreto compartido. Seleccione el botón **Enviar**.

Notaeth Devices Default Device Device Security Settings	Network Devices         CSM422           Description
Device Security Settings	Network Devices           * Name         CSM422           Description
	<u>Η</u> PAREN v *P1 1088243.42 <sup>f</sup> 32 Φx
	* Device Profile III. Decis VIII
	Sofware Version
	* Network Denvis Onus Linceton All Locations Us IMSCO Device Set Tis Detaunt Set Tis Detaunt Set Tis Detaunt
	A DUS Authentication Settings
	V TACACS Authentication Settings      Devel Scott      Trates Some Original      Show
	Ispacy Cest Device     InCACS Shall Compliance Single Connect Support
	V SNMP Settings     Advanced TrustSec Settings
	Submit Cancel

=

Paso 3. Seleccione el icono de tres líneasse encuentra en la esquina superior izquierday navegue hasta Administración > Administración de identidades > Grupos.

Cisco ISE	Administration · Identity Management					
entities Groups External Ide	ntity Sources Identity S	ource Sequences Settings				
Identity Groups	User Identity	Groups				
¢ 12 ¢						
> 🗀 Endpoint Identity Groups	🖉 Edit 🕂 Add 👩 D	slete 🗸 🕁 Import 🏠 Export 🗸				
> 🛅 User Identity Groups	Name	∧ Description				
		S (default) Default ALL_ACCOUNTS (default) User Group				
	Employee	Default Employee User Group				
	GROUP_ACCO	JNTS (default) Default GROUP_ACCOUNTS (default) User Group				
	GuestType_Co	tractor (default) Identity group mirroring the guest type				
	GuestType_Dai	ly (default) Identity group mirroring the guest type				
	GuestType_So	salLogin (default) Identity group mirroring the guest type				
	GuestType_We	ekly (default) Identity group mirroring the guest type				
		TS (default) Default OWN_ACCOUNTS (default) User Group				

Paso 4. Navegue hasta la carpeta Grupos de identidad de usuario y seleccione el botón +Agregar botón. Defina un nombre y seleccione el botón Enviar.

dentities	Groups External Id	entity Sources Ide	entity Source Sequences Settings	
Identity Gr ∃Q	oups	User Iden	ntity Groups	
< 18	o			Selected 0 Total 10 🧭 🧔
> 🗖 E	indpoint Identity Groups	🖉 Edit 🕂 Add	🔋 Delete 🗸 🚽 Import 🕐 Export 🗸	All $\sim$ 11A
> 🗖 (	Iser Identity Groups	Name	∧ Description	
		🗌 🏯 ALL_A	CCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
		🗌 🍕 CSM A	Idmin	
		🗌 🏘 сям с	)per	

**Nota:** Este ejemplo crea grupos de administración CSM y de identidad Oper CSM. Puede repetir el paso 4 para cada tipo de usuarios de administración en CSM

Paso 5. Seleccione el icono de tres líneas y navegue hasta Administración > Administración de identidades > Identidades. Seleccione el botón +Agregar y defina el nombre de usuario y la contraseña y, a continuación, seleccione el grupo al que pertenece el usuario. En este ejemplo, crea los usuarios csmadmin y csmoper y se asigna al grupo CSM Admin y CSM Oper respectivamente.

Jentities Groups E	stemal identity Sources Identity Source Sequences Settings	
	Nerverk Access Gains Gat 2 consultrin	
Warual Network Scan Res		
	✓ Network Access User	
	* Name (Diffadmin	
	Status 💆 Enabled 🗸	
	tral	
	✓ Passwords	
	Annual how immediate	
	Password Re-Errar Password	
	*Logit Password	0
	Frate Tensor	0
		0
	V User Information	
	First Norte	
	Last Name	
	V Account Options	
	Devrement A	
	Charge paerward on hool login	
	✓ Account Disable Policy	
	Orisidale account if data anceeds 2021-06-16 (systemet-add)	
	✓ User Groups	
	E CSM Admin v - +	

Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 2 🧭 🚳
	🖉 Edit 🕂 Add 🔅 Change Status 🗸 🕁 Import 🏠 Export 🗸 🏮 Delete 🗸 🍈 Duplicate	All $\sim$ $\gamma$
	Status Name	User Identity Grou Ad
	Enabled 1 csmadmin	CSM Admin
	Enabled 2 csmoper	CSM Oper

Paso 6. Seleccionary navegue hasta Administración > Sistema > Implementación.Seleccione el nodo de nombre de host y active Device Admin Service

=



**Nota:** En caso de implementación distribuida, seleccione el nodo PSN que gestiona las solicitudes TACACS

Paso 7. Seleccione el icono de tres líneas y navegue hasta Administración > Administración de dispositivos > Elementos de políticas. Vaya a Resultados > Conjuntos de Comandos TACACS. Seleccione +botón Agregar, defina un nombre para el conjunto de comandos y habilite la casilla de verificación Permitir cualquier comando que no aparezca en la siguiente lista. Seleccione Enviar.

■ Cisco ISE			Work Centers -	Device Administration		A Evaluation Mod	e 39 Days Q 💿	¢
Overview Identit	ties	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More $\vee$	
Conditions	>	TACACS Command Sets Command Set	> New					
Network Conditions	>	Name						
Results	~	Permit all						
Allowed Protocols								
TACACS Command Sets		Description						
TACACS Profiles				i.				
		Commands						
		Dennit any command that	is not listed below					
		Permit any command that	I IS FICK INSTRUCTION	-				
		+ Add 🛛 🔋 Trash 🗸	🖉 Edit 🔷 Move Uj	p 🖂 Move Down				
		Grant	Command	Arguments				
		No data found.						
							0	

Paso 8. Seleccione el icono de tres líneas situado en la esquina superior izquierda y navegue hasta Administración->Administración de dispositivos->Conjuntos de políticas de administración

**de dispositivos.** Seleccionar situado debajo del título Conjunto de políticas, defina un nombre y seleccione el botón + en el centro para agregar una nueva condición.

Policy	Sets				Reset CReset Policyset Hitcounts	ave
٠	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions	View
Q	Search					$\supset$
	٥	CSM Administrators		+	Select from list $\sim$ +	>
	۰	Default	Tacacs Default policy set		Default Device Admin $\otimes$ $\sim$ + • • §	•

**Paso 9.** En la ventana Condición, seleccione Add an attribute y luego seleccione **Network Device** Icon seguido de Network Access Device IP address. Seleccione **Valor de atributo** y agregue la dirección IP de CSM. Seleccione **Usar** una vez hecho.

Conditions Studio							
Library	Editor						-
Search by Name		Network Access-D	evice IP Address				8
	ę	Equals 🗸	10.88.243.	42			
No conditions found - reset filters.		Set to 'Is not'				Duplicate	Save
			NEW	AND	OR		
						Close	Use

Paso 10. En la sección Permitir protocolos, seleccione Device Default Admin. Seleccione Save (Guardar).

Policy Sets					Reset		Reset	Policyset Hit	counts		Save
Status	Policy Set Name	Description	Con	ditions	Allowed Pro	tocols	/ Serve	r Sequence	Hits	Actions	View
Q Search											
۰	CSM 4.22		ę	Network Access-Device IP Address EQUALS 10.88.243.42	Default Dev	vice A	dmin	∞ ~+	0	<u>نې</u>	>

**Paso 11.** Seleccione la flecha derecha autenticación y autorización

del conjunto de políticas para definir las políticas de

**Paso 12.** Seleccionar situado debajo del título de la política de autenticación, defina un nombre y seleccione el + en el centro para agregar una nueva condición. En la ventana Condición, seleccione Add an attribute y luego seleccione **Network Device** Icon seguido de Network Access Device IP address. Seleccione **Valor de atributo** y agregue la dirección IP de CSM. Seleccione **Usar** una vez hecho

Paso 13. Seleccione Usuarios Internos como Almacén de Identidades y Seleccione Guardar

🕒 Status Rule Name Conditions Use Hi	s Actions
Q Search	
Internal Users 🗷 🗸	
CSM Authentication Retwork Access-Device IP Address EQUALS 10.88.243.42 Options	{Ô}

**Nota:** El almacén de identidades se puede cambiar a almacén de AD si ISE se une a un directorio activo.

Paso 14. Seleccionar situado debajo del título de la política de autorización, defina un nombre y seleccione el botón + en el centro para agregar una nueva condición. En la ventana Condición, seleccione agregar un atributo y, a continuación, seleccione el icono Grupo de identidad seguido por Usuario interno: Grupo de identidad. Seleccione el grupo de administración de CSM y seleccione Usar.

ibrary	Ed	ditor				
Search by Name		InternalUser	IdentityGroup			
	8 0 1 0 t 🕈	# Equals	Vuser Ident	ity Groups:CSM Adm	in × 🗸 🗸	ш
EAP-MSCHAPv2	O	Set to 'Is not			Duplicate	Save
EAP-TLS	٥		NEW	AND OR		
Guest_Flow	0					
E Network_Access_Authent	lication_					

**Paso 15.** En Conjunto de comandos, seleccione Permitir todo el conjunto de comandos creado en el Paso 7 y, a continuación, seleccione **Guardar** 

Repita los pasos 14 y 15 para el grupo CSM Oper

Authorization	on Policy (3)								
				Results					
🕣 Statu	s Rule Name	Condition	ns	Command Sets		Shell Profiles		Hits	Actions
Q Sear	sh								
•	CSM Oper	유 Inte Iden	rnalUser-IdentityGroup EQUALS User ntity Groups:CSM Oper	$\text{Permit all} \times$	~+	Select from list	~+	0	{ĝ}
۰	CSM. Admin	유 Inte Iden	rnalUser-IdentityGroup EQUALS User ntity Groups:CSM Admin	$\text{Permit all} \times$	~+	Select from list	~+	0	{ô}
0	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>∞</u> ~+	0	{3

**Paso 16 (opcional).** Seleccione el icono de tres líneas situado en la esquina superior izquierda y Seleccione **Administration>System>Maintenance>Repository**, seleccione **+Add** para agregar un repositorio que se utilice para almacenar el archivo de volcado TCP con fines de resolución de problemas.

**Paso 17 (opcional).** Defina un nombre de repositorio, protocolo, nombre de servidor, ruta y credenciales. Seleccione **Enviar** una vez hecho.

Deployment	Licensing	Certificates L	ogging Maintenar	ce Upgrade	Health Checks	Backup	Click here to do visibility setup Do not show this again.
Patch Management		Repository List > Ad	dd Repository				
Repository		Repository Co	nfiguration				
Operational Data Pur	ging	* Repository Name * Protocol Location * Server Name	VMRepository FTP  10.122.112.137				
		* Path Credentials * User Name * Password	cisco				

### Configuración de CSM

Paso 1. Inicie sesión en la aplicación Cisco Security Manager Client con la cuenta de administrador local. En el menú, vaya a Herramientas > Administración del Administrador de seguridad

		•
	Cisco Security Manager Version 4.22.0 Service Pack 1	
	Server Name 10.88.243.42	
	Password ••••••• Default View Configuration Manager v Login Help	
© 2020 Cisco Systems, Inc. Cisco, Cisco System its affiliates in the U.S. and certain other countr	ns and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or les.	111



Paso 2. Marque la casilla en Parámetros RBAC nativos. Seleccione Guardar y Cerrar

5	Cisco Security Manager - Administration	X
APS     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     Costemps     Configuration Archive     Configuration Archive     Configuration Archive     Costanze Desktop     Debug Options     Debug Options     Debug Options     Debug Options     Debug Options     Dehuice Communication     Dervice Communication	Server Security         Use the buttors below to cross launch the Server Security Tools within Common Services.         AAA Setup         Certificate Setup         Single Sign On         Local User Setup         System Identity Setup         Native RBAC Parameters         W Blow logon for user ids not available in Local User Databaset	Save Restore Defaults

Paso 3. En el menú seleccione Archivo > Enviar. File > Submit (Archivo > Enviar).

**Nota:** Todos los cambios se deben guardar, en caso de que se produzcan cambios en la configuración, es necesario enviarlos e implementarlos.

Paso 4. Navegue hasta la interfaz de usuario de administración de CSM y escriba <u>https://<enter\_CSM\_IP\_Address</u> y seleccione Administración del servidor.



**Nota:** Los pasos 4 a 7 muestran el procedimiento para definir la función predeterminada para todos los administradores que no están definidos en ISE. Estos pasos son opcionales.

Paso 5. Validar el modo de autenticación se establece en CiscoWorks Local y Online userID es la cuenta de administración local creada en CSM.

cisco Cis	co Security Mana	ger						admin Logout About Feedback
Home Server * 1	Software Center ·							
								17 Apr 2021, 14.11
ommon Services	Home							
Auto Refresh		Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021
	Security		Beckup			Recent	ly Completed Jobs	
thentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job Id	Job Type	Status	Description	Completed At
				1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat.Apr 17 05:01:56 PDT 2021
thorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021
usia Eine on Made	Electricity			1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
die odbiou woos	00000	Recent Backup Status	Not found or unable to detect	1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat.Apr 10 05:00:56 PDT 2021
								More
	System Taska		Inline Users		Management Tax	ka l		Reports
cal User Setup				Schedule Back	up		Permission Rep	ot
15-Server Trust Manag	sment	Number of Online users		Check for Soft	ware Updates		Log File Status	
infigure Single Sign-On		Hander of Chine Gao's		Check for Dev	ice Updates		Process Status	
A Mode Setup				Collect Server	Information		System Audit L	
			admin					
		Online User kl(s)	Send Message					

Paso 6. Navegue hasta Servidor y seleccione Administración de Servidor Único

ciso	Cisco Security Manager	
Home	Server V Software Center V	
	Security	
Commo	Single-Server Management	
🗹 Auto R	Multi-Server Trust Management	
	Cisco.com Connection Management	
Authentica	AAA Mode Setup	
Authorizat	Admin	,
Cingle Cig	Processes	
Single Sig	Backup	2
	Log Rotation	
	Collect Server information	
	Selftest	
	Notify Users	
	Job Browser	
	Resource Browser	
Local Use	System Preferences	
Multi-Serv	CS Log Configurations	
Configure	DiskWatcher Configuration	
AAA Mode	e Setup	

**Paso 7.** Seleccione Role Management Setup (Configuración de administración de funciones) y seleccione el privilegio predeterminado que reciben todos los usuarios administradores tras la autenticación. Para este ejemplo, se utiliza Network Administrator. Una vez seleccionado, seleccione **set as default .** 

cisco Cisco Security M	lanager		
Home Server   Software Center			
Navigator Browser-Server Security mode setup Local User Policy Setup	Role Management Setup	Description	Showing 8 records Default Roles
Local User Setup Role Management Setup Certificate Setup	1. Approver 2. Help Desk	Approver Role Help Desk Role	
	3. Network Administrator     4. Network Operator	Network Administrator Role Network Operator Role	R
	5. Security Administrator	Security Administrator Role	
	7. Super Admin	Super Admin Role	
	System Administrator     Add Edit Delete Copy   Expo	System Administrator Role	

**Paso 8.** Seleccione **Servidor>Función de configuración del modo AAA** y luego seleccione la opción **TACACS+**, y finalmente seleccione **cambiar** para agregar información de ISE.



cisco Cisco Security Manager	
Home Server  Software Center  Uthentication Mode Setup AAA Mode Setup Select a Type: ACS Local RBAC Current Login Mode: Local Authentication Available Login Modules 1 Local Authentication	
Authentication Mode Setup	
AAA Mode Setur	
Caled a Time: ACC Local DBAC	
oelect a type. Hoo 😈 Local homo	
Current Login Mode: Local Authentication	
Available Login Modules	
1 Local Authentication	
2 Local NT System	
3 MS Active Directory	
4 RADIUS	
5 O TACACS+	
	Change

**Paso 9.** Defina la dirección IP y la clave de ISE; opcionalmente, puede seleccionar la opción para permitir a todos los usuarios de autenticación local o sólo a un usuario si falla el inicio de sesión. Para este ejemplo, se permite al único usuario administrador como método de reserva. Seleccione **Aceptar** para guardar los cambios.

Login Module Options		
Selected Login Module:	TACACS+	
Description:	Cisco Prime TACACS+ login module	
Server:	10.122.112.4	
Port:	49	
SecondaryServer:		
SecondaryPort:	49	
TertiaryServer:		
TertiaryPort:	49	
Key:		
Debug:	True O False	
	<ul> <li>Allow all Local Authentication users to fall Authentication login.</li> </ul>	lback to the Local
Login fallback options:	<ul> <li>Only allow the following user(s) to fallbac Authentication login if preceding login fails:</li> </ul>	k to the Local
	admin	(comma separated)
	<ul> <li>Allow no fallbacks to the Local Authentica</li> </ul>	ation login.
		OK Cancel



Paso 10. Seleccione Server> Single Server Management, luego seleccione Local User Setup y seleccione add.

uļu cisc	Cisco Security Manager	
Home	Server V Software Center V	
Commo	Security	
Commo	Single-Server Management	
Auto R	Multi-Server Trust Management	
	Cisco.com Connection Management	
Authentica	AAA Mode Setup	(
Authorizat	Admin	)
Single Sig	Processes	
	Los Retetion	-
	Collect Server information	
	Collect Server Information	
	Serrest	
	Notiny Users	
	Job Browser	
	Resource Browser	
Local Use	System Preferences	
Multi-Serv	CS Log Configurations	
Configure	DiskWatcher Configuration	
AAA Modo	Rahun	

ululu cisco Cisco Securit	Manager
Home Server * Software Center *	, manager
Navigator	Local User Setup
Browser-Server Security mode setup	Showing 206 records
Local User Policy Setup	t Carron loop
Local User Setup	
Certificate Setup	Adap Bishania
	5 Aits Ander
	A Alast Castan
	7. alem weldehimanot
	A alien sciencel
	Andrew OCenter
	10. Anwar Khan
	11. amandamith
	12. Bernard Alation
	13. bheas
	14. Bill Mason
	15. bill.nash
	16. Billy Vaughan
	17. D bpiotnik
	18 Brofier Issuen
	tSelect items then take an Import Users Export Users Edit Delete Add Modify My Profile

**Paso 11. En este ejemplo, se utilizan** los mismos nombres de usuario y contraseña creados en ISE en el paso 5 de la sección de configuración de ISE, **csmoper** y **funciones de autorización de tareas de Help Desk**. Seleccione **OK** para guardar el usuario administrador.

serriarite.	csmoper			
assword:			Verify Password:	
mail:				
uthorization Type				_
elect an option: Full A	Authorization 🔾 Ena	able Task Au	thorization Enable Device Authori	zation
Koles		Device	level Authorization	
Help Desk		Not Ap	plicable	
Approver				
Network Operator				
Network Administrato	e			
System Administrator				
Super Admin				
Security Administrato	r			
Security Approver				

### Verificación

Interfaz de usuario del cliente de Cisco Security Manager

**Paso 1.** Abra un nuevo navegador de ventanas y escriba <u>https://<enter\_CSM\_IP\_Address</u>, utilice el nombre de usuario y la contraseña **csmadmin** creados en el paso 5 en la sección de configuración de ISE.



El inicio de sesión exitoso se puede verificar en los registros en vivo de ISE TACACS

E Cisco ISE			С	perations • TA	CACS		Ivaluation Mode 39 Days	0020	
Live Logs									
ට Refresh රෝ Expert To 🗸						Refresh Show Every 3 seconds V Lates	t 20 records 🗸	Utbin Last 3 hours → ⊽ Filter → ⊕	
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic.	
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device N	
Apr 17, 2021 02:34:54.1		à	csmadmin	Authentic	CSM 4.22 >> Default		ise30	C5M422	
Last Updated: Sat Apr 17 202	09:37:58 0	GMT-0500 (C	entral Daylight T	lime)				Records Shown: 1	

aplicación Cisco Security Manager Client

**Paso 1.** Inicie sesión en la aplicación Cisco Security Manager Client con la cuenta de administrador del soporte técnico.

		0
	Cisco Security Manager Version 4.22.0 Service Pack 1	
	Server Name 10.88.243.42 V Username csmoper Password ••••••• Default View Configuration Manager V Login Help	
_	Its affiliates in the U.S. and certain other countries.	

El inicio de sesión exitoso se puede verificar en los registros en vivo de ISE TACACS

e Logs								
						Refresh Every 3 seconds 🗸	Show Latest 20 records 🗸	Within Last 3 hours
🖸 Refresh 🛛 🛈 Export To 🗸								V Filter V (
C Refresh ① Export To ∨	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	ise Node	V Filter V
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Vetwork Device

Paso 2. En el menú de aplicación del cliente CSM seleccione Herramientas > Administración del administrador de seguridad, un mensaje de error indica que debe aparecer la falta de privilegio.

Bones Rep Polcy And			0	6 🖷 🔁	Q % I					9	Search All Categories	CISCO
Devkes 💽 🖗	Healt	Heelt Packet Capture Waard Ping Tacket and Nilockup Ping Tacket and Nilockup			Dep	fai s 😐	lenager Fending 8 0	Paase 0		Orvice State O Critical 3 O Warning 3 O Nor	with the second second	
III - A Concentration	0 a 2	Pinteligence								LastUpd	te Time: 17 Apr 2021 00	LILI PN PDT
* <b>3</b> 4	Dup P	Show Containment Inventory Status Catalyst Summary Info Apply IPS Updata		d Aleta O	Connection 0	Sana O O	Deployment Qu 0 Qu 0	Additional Information	JP Address 199, 134, 215, 3 199, 139, 215, 3	ricat.Donain quel etus umfo-3 unde, gru quel etus umres 2 unde, gr	C)- fupe to Search Target 05 Version 9.9(2) v 9.9(2)	Running 05 5.9(2)40 5.9(2)40
	24	Preview Configuration Backup Security Manager Disonactics		:	:	0	8. 8.		199, 129, 210, 9 199, 139, 210, 30 199, 139, 215, 4	gel eta unen filosiag gel eta unen filosiag gel eta unen filosiage	N 9.900 N 9.900 9.900	5.5(2)40 5.5(2)40 5.5(2)40
Policies	9 1	Security Manager Administration Satus usefo Sustagev 0 Satus usero 2 use gev 0	0	:	:	0	8. 8.		199, 139, 218, 4 199, 139, 215, 5 199, 139, 215, 5	og also 6-meson ante Curg og also 6-meson ante Curg og also 6-meson ante Curg	9.900 9.900 9.900	8.9(2)40 8.9(2)40 8.9(2)40
				Erro	r - Ins	suffic	ient P	rivileges				×
You do Please of If your	ontact y	sufficient privileges to our system administrat e is ACS, privileges are e is non-ACS, privilege	perfo or and gran	rm this d have ted via	operat them gr ACS co	ion. rant y onfigur JiscoW	ou additi ation. orks Hor	onal privileges.	er > Sindle-5	ierver Management > I	ocal Liser Se	tuo".

**Paso 3.** Repita los pasos 1 a 3 con la cuenta **csmadmin** para validar los permisos adecuados que se han proporcionado a este usuario.

### Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Validación de la comunicación con la herramienta TCP Dump en ISE

**Paso 1.** Inicie sesión en ISE y desplácese al icono de tres líneas situado en la esquina superior izquierda y seleccione **Operaciones>Solución de problemas>Herramientas de diagnóstico.** 

**Paso 2. En General tools** seleccione **TCP Dumps** y luego **Add+.** Seleccione Nombre de host, Nombre de archivo de interfaz de red, Repositorio y opcionalmente un filtro para recopilar sólo el flujo de comunicación de dirección IP de CSM. Seleccione **Guardar y ejecutar** 

#### Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Downl	oad Logs Debug Wizard	
General Tools ~	Add TCP Dump	
RADIUS Authentication Troubl	Add TCP Dump packet for monitoring on a	network interface and troubleshoot problems on the network as they appear.
Execute Network Device Com		
Evaluate Configuration Melided	ise30	
Evaluate Competation Validat		
Posture Troubleshooting		
Agentiess Posture Troublesho	Network Interface *	
EndPoint Debug	GigabitEthernet 0	~ 0
TCP Dump		
Session Trace Tests		
	in bost 10.88.243.42	0
TrustSec Tools	10 HONE FOLDOLEHOLME	*
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		di.
	E.g. ip host 10.77.122.123 and not	
	10.177.122.119	
	File Name CSM_Tshoot	
	Repository	
	VMRepository	~ 0
	File Size	
	100	· ·
	M	b
	Limit to	0
	-	
	F 10(5	0
	5 C	0
	Minutale	
	Promiscuous Mode	
		Cancel Save and Due
		Cancer Save and Run

**Paso 3.** Inicie sesión en la aplicación cliente CSM o en la interfaz de usuario del cliente y escriba las credenciales de administrador.

**Paso 4.** En ISE, seleccione **el** botón **Detener** y verifique que el archivo pcap haya sido enviado al repositorio definido.

C Re	efresh + Add	0 Edit	🖞 Trash 🗸 🕨 Start	⊖ Stop	🛓 Download			∏ F	ilter 🗸 🐵
	Host Name		Network Interface	Fi	lter	File Name	Repository	File S	Number o
	ise30.ciscoise.lab		GigabitEthernet 0	ip	host 10.88.243.42	CSM_Tshoot	VMReposit	100	1

File       Commands       Tools       Favorites       Options       Help         Image: Add	
Image: Add Extract To       Image: View       Image:	
Name Size Packed Type Modified CRC32	
- File folder	
CSM_Tshoot.pcap 1,166 556 PCAP File 4/17/2021 3:29 8A27888D	

Paso 5. Abra el archivo pcap para validar la comunicación correcta entre CSM e ISE.

• •	•					CSM_Tshoot.pcap
		2 💿	S 🕺 🗋 💼	९ 🗰 🗯 🕾	Ŧ 🛓 🗔	📃 🤉 🤉 🗉
App	ily a dis	splay filter	<#/>			🖘 🔹 Expression 🔸
No.	T	ime	Source	Destination	Protocol	Length Info
r	1 0	666669	10.88.243.42	10.122.112.4	TCP	66 55740 → 49 [SYN, ECN, CMR] Seq=0 Win=8192 Len=0 MSS=1300 WS=256 SACK_PERM=1
	2 0	.000130	10.122.112.4	10.88.243.42	TCP	66 49 - 55740 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
	3 0	.065680	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=1 Ack=1 Win=66048 Len=0
	4 0	.101272	10.88.243.42	10.122.112.4	TACACS+	97 Q: Authentication
_	5 8	.101362	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0
	0 0	.10/185	10.122.112.4	10.00.243.42	TACALS+	61 K: Authentication
	2 0	2203012	10.00.243.42	10.122.112.4	TACACS+	98 0: Authonication
	9.8	259963	10.122.112.4	10.88.243.42	TCP	54 49 - 55748 [ACK] Sec.28 Ack=78 Win=2012 Len=8
	18 8	.311136	10,122,112,4	10.88.243.42	TACACS+	72 R: Authentication
100	11 8	.311193	10.122.112.4	10.88.243.42	TCP	54 49 → 55740 [FIN, ACK] Seg=46 Ack=70 Win=29312 Len=0
	12 0	.375973	10.88.243.42	10.122.112.4	TCP	60 55740 - 49 (ACK) Seg=70 Ack=47 Win=66048 Len=0
	13 0	.400651	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [FIN, ACK] Seq=70 Ack=47 Win=66048 Len=0
L	14 0	.400724	10.122.112.4	10.88.243.42	TCP	54 49 → 55740 [ACK] Seq=47 Ack=71 Win=29312 Len=0
> En	ane 6:	81 bytes	on wire (648 bits),	81 bytes captured (6	48 bits)	
> Et	hernet	t II, Src:	Vmware_a4:0d:c6 (00	:50:56:a4:0d:c6), Dst	: Cisco_1f:21:4	45 (00:14:6a:1f:21:45)
> In:	ternet	t Protocol	Version 4, Src: 10.	122.112.4, Dst: 10.88	.243.42	
> Tri > TA	ansmis CACS+	ssion Cont	rol Protocol, Src Po	rt: 49, Dst Port: 557	40, Seq: 1, Aci	k: 44, Len: 27
	Major	version:	TACACS+			
	Type:	Authentic	ation (1)			
	Seque	nce number	12	14/-1- C		
>	Sessi	: 0x00 (En on ID: 381	erypted payload, Mu 9957939	(tiple Connections)		
0000	88.1	1 Ionathi 14 6a 1f 2	15 1 45 88 58 56 a4 8	4 76 88 88 45 88	1. IF.P. VF	£.
0 7	C 64	M Taboot occur			1.16.9.4	Packets: M - Displayed: 14 (100.0%) . Dvollar Dafault
_						- research is and share of financial - Financial

Si no se muestra ninguna entrada en el archivo pcap, valide lo siguiente:

- 1. El servicio de administración de dispositivos está habilitado en el nodo ISE
- 2. La dirección IP de ISE correcta se ha agregado en la configuración de CSM
- 3. En el caso de un firewall se permite el puerto de verificación intermedio 49 (TACACS).