Integração de TACACS CSM com ISE

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Diagrama de Rede Procedimento de autenticação Configuração do ISE Configuração do CSM Verificar Troubleshoot

Introduction

Este documento descreve o procedimento para integrar o Cisco Security Manager (CSM) ao Identity Services Engine (ISE) para autenticação de usuários administradores com o TACACS+ Protocol.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CSM Server versão 4.22
- ISE versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Por padrão, o Cisco Security Manager (CSM) usa um modo de Autenticação chamado CiscoWorks para autenticar e autorizar usuários localmente, a fim de ter um método de autenticação centralizado, você pode usar o Cisco Identity Service Engine através do protocolo TACACS.

Configurar

Diagrama de Rede



Procedimento de autenticação

Etapa 1. Faça login no aplicativo CSM com as credenciais do Usuário Admin.

Etapa 2. O processo de autenticação dispara e o ISE valida as credenciais localmente ou através do Ative Diretory.

Etapa 3. Quando a autenticação for bem-sucedida, o ISE envia um pacote de permissão para autorizar o acesso ao CSM.

Etapa 4. O CSM mapeia o nome de usuário com a atribuição de função de usuário local.

Etapa 5. O ISE mostra um registro ao vivo de autenticação bem-sucedido.

Configuração do ISE

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue até Administration > Network Resources > Network Devices (Administração > Recursos de rede > Dispositivos de rede).

E Cisco ISE	E Administration - Network Resources							
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services	
Network Devices Default Device	Networ	k Devices						
	0 tot + A	dd 🜔 Duplicate 🕁 Import	ර Export ~ ලි Generate PM	0 Delete V	Providelar			
	Name	e 🗠 IP/Mask Profile N	ame Location	Туре	Description			

Etapa 2. Selecione o botão **+Adicionar** e insira os valores corretos para Network Access Device Name (Nome do dispositivo de acesso à rede) e IP Address (Endereço IP), verifique a caixa de

seleção TACACS Authentication Settings (Configurações de autenticação TACACS) e defina um segredo compartilhado. Selecione o botão Enviar.

Number Number
Entres Single Convect More
Sub-M Cancel

Etapa 3. Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue até **Administration > Identity Management > Groups**.

E Cisco ISE	Administration • Identity Ma	anagement
entities Groups External Ide	entity Sources Identity Source Sequences	Settings
Identity Groups	User Identity Groups	
Endpoint Identity Groups	🖉 Edit 🕂 Add 🌘 Delete 🗸 🕁 Import	🟦 Export 🖂
 > In Dentity Groups > In User Identity Groups 	Name	∧ Description
	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	Default Employee User Group
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
	GuestType_Contractor (default)	Identity group mirroring the guest type
	GuestType_Daily (default)	Identity group mirroring the guest type
	GuestType_SocialLogin (default)	Identity group mirroring the guest type
	GuestType_Weekly (default)	Identity group mirroring the guest type
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Etapa 4. Navegue até a pasta **Grupos de Identidades do Usuário** e selecione o botão **+Adicionar**. Defina um nome e selecione o botão **Enviar**.

Identities	Groups	External Ide	ntity Sources	Identity Source Sequence	es Settings	
Identity Gr EQ	roups		User lo	lentity Groups		
< 18	8	0				Selected 0 Total 10 🖉 🧔
	Endpoint Identi	ity Groups	0 Edit +	Add 🌔 Delete 🗸 🕁 ir	nport 🏦 Export 🖂	all \sim $~$ ∇
> 🗖 (User Identity G	iroups	Nar	ne	∧ Description	
			0 4	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group	
			0 😤	CSM Admin		
			0 😤	CSM Oper		

Note: Este exemplo cria grupos Admin CSM e Oper Identity CSM. Você pode repetir a Etapa 4 para cada tipo de usuário administrativo no CSM

Etapa 5. Selecione o ícone de três linhas e navegue até **Administration > Identity Management >Identities.** Selecione o botão **+Adicionar**, defina o nome de usuário e a senha e selecione o grupo ao qual o usuário pertence. Neste exemplo, cria os usuários **csmadmin** e **csmoper** e atribuídos ao CSM Admin e ao CSM Oper group respectivamente.

Manager Concern For		
dentities unsups Ext	mail identity Sources Identity Source Sequences Settings	
	Nervent Access Users List () considers	
ne Meruel Network Scen Res	 Network Access User *Nerw containin Sona Contai) o) o
	User Information Proclame Lastnere Account Options	
	Charge paerward in Hod togin	
	Deside account if data encents 2021-06-16 Gymmers-dd)	
	V User Groups	

Identities Groups Ex	xternal 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 $-\nabla$
	Status Name	s User Identity Grou Ad
	Enabled 1 csmadmin	CSM Admin
	Enabled 1 csmoper	CSM Oper

Etapa 6. Selecionare navegue até Administration > System > Deployment(Administração > Sistema > Implantação). Selecione o nó do nome de host e ative o DeviceAdmin Service



Note: Em caso de implantação distribuída, selecione o nó PSN que lida com solicitações TACACS

Passo 7. Selecione o ícone de três linhas e navegue até Administration > Device Administration > Policy Elements (Administração > Administração de dispositivo > Elementos de política). Navegue até Results > TACACS Command Sets (Resultados > Conjuntos de comandos TACACS). Selecione +Adicionar botão, defina um nome para o conjunto de comandos e ative o comando Permitir qualquer que não esteja listado abaixo da caixa de seleção. Selecione Submit.

E CISCO ISE			Work Centers -	Device Administration			e months of a	28	Ŷ
Overview Identitie	S	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More \sim		
Conditions	>	TACACS Command Sets Command Set	> New						
etwork Conditions	>	Name							
lesults	~	Permit all							
Allowed Protocols									
TACACS Command Sets		Description							
TACACS Profiles									
		Commands							
		Permit any command that	t is not listed below	2					
		+ Add 🛛 Trash 🗸	CEdit 🔷 Move U	o 💛 Move Down					
		Grant	Command	Arguments					
		No data found.							
								_	_

Etapa 8. Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue até

Administration->Device Administration->Device Admin Policy Sets. Selecionar localizado abaixo do título Conjuntos de políticas, defina um nome e selecione o + botão no meio para adicionar uma nova condição.

Policy	Sets				Reset	Policyset Hite	counts		Save
۲	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Serve	er Sequence	Hits	Actions	View
Q	Search								
	۰	CSM Administrators		+	Select from list	~+		(2)	>
	۰	Default	Tacacs Default policy set		Default Device Admin	<u>a ~</u> +	0	¢3>	•

Etapa 9. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Dispositivo de rede** seguido do endereço IP do dispositivo de acesso à rede. Selecione **Attribute Value** e adicione o endereço IP do CSM. Selecione **Usar** uma vez concluído.

Conditions Studio						
Library	Editor					
Search by Name		Network Access-D	evice IP Address			
	ę	Equals 🗸	10.88.243.42			
No conditions found - reset filters.		Set to 'Is not'			Duplicate	Save
			NEW A	ND OR		
					Close	Use

Etapa 10. Na seção permitir protocolos, selecione Device Default Admin. Selecione Salvar

Policy Sets					Reset	Reset	Policyset Hit	counts)	Save
🔶 Status Policy	y Set Name	Description	Con	ditions	Allowed Protoc	ols / Serve	r Sequence	Hits	Actions	View
Q Search										
CSM 4	.22		Ŗ	Network Access-Device IP Address EQUALS 10.88.243.42	Default Device	Admin	∞ ~+	0	ŵ	>

Etapa 11. Selecione a set	a para a direita
políticas de autenticação	e autorização

ícone do Conjunto de políticas para definir

Etapa 12. Selecionar localizado abaixo do título da política de autenticação, defina um nome e selecione o + no meio para adicionar uma nova condição. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Dispositivo de rede** seguido do endereço IP do dispositivo de acesso à rede. Selecione **Attribute Value** e adicione o endereço IP do CSM. Selecione **Usar** uma vez concluído

Etapa 13. Selecione Usuário interno como o repositório de identidade e selecione Salvar

\vee Authe	nticatio	n Policy (1)					
۲	Status	Rule Name	Cor	ditions	Use	н	its Actions
Q	Search						
					Internal Users	a ~	
	0	CSM Authentication		Network Access-Device IP Address EQUALS 10.88.243.42	> Options		(\$)

Note: O repositório de identidades pode ser alterado para o repositório do AD se o ISE estiver associado a um Ative Diretory.

Etapa 14. Selecionar localizado abaixo do título da política de autorização, defina um nome e selecione o + botão no meio para adicionar uma nova condição. Na janela Condição, selecione adicionar um atributo e selecione o ícone **Grupo de Identidade** seguido por **Usuário Interno: Grupo de Identidades**. Selecione o grupo de administração do CSM e selecione **Usar**.

ibrary	1	Editor				
Search by Name			InternalUser-Identity	yGroup		
	8 0 1 0 t 🕈	4	Equals 🗸	User Identity Groups:CSM Ac	dmin × 🗸 🗸	
EAP-MSCHAPv2	o		Set to 'Is not'		Duplicate	ave
EAP-TLS	٥			NEW AND OR		
Guest_Flow	0					
Betwork_Access_Authen	ntication_ ()					

Etapa 15. Em Conjunto de comandos, selecione Permitir todos os conjuntos de comandos criados na Etapa 7 e selecione **Salvar**

Repita as etapas 14 e 15 para o grupo de trabalho do CSM

Author	ization	Policy (3)								
					Results					
⊕ s	Status	Rule Name	Con	ditions	Command Sets		Shell Profiles		Hits	Actions
Q	Search									
	•	CSM Oper	A	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	${\rm Permit\ all\ }\times$	~+	Select from list	~+	0	(2)
	0	CSM. Admin	я.	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$Permit\;all\;\times$	~+	Select from list	~+	0	(2)
	0	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	∞ ~+	0	錼

Etapa 16 (Opcional). Selecione o ícone de três linhas localizado no canto superior esquerdo e Selecione **Administração>Sistema>Manutenção>Repositório**, selecione **+Adicionar** para adicionar um repositório usado para armazenar o arquivo de despejo de TCP para fins de solução de problemas.

Etapa 17 (Opcional). Defina um nome de repositório, um protocolo, um nome de servidor, um caminho e credenciais. Selecione **Submit** quando terminar.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup	Click here to do visibility setup Do not show this again.
Patch Management		Repository List > /	Add Repository					
Repository		Repository Co	onfiguration	n				
Operational Data Pur	ging	* Repository Ca * Repository Nam * Protocol Location * Server Name * Path Credentials * User Name * Password	re VMRepor FTP ~ 10.122.1 / cisco	12.137				

Configuração do CSM

Etapa 1. Faça login no aplicativo Cisco Security Manager Client com a conta de administrador local. No menu, navegue até **Ferramentas > Administração do Security Manager**

	Cisco Security Manager Version 4.22.0 Service Pack 1
	Server Name 10.88.243.42 V Username admin Password ••••••
© 2020 Cisco Systems, Inc. Cisco, Cisco Syst	ems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or



Etapa 2. Marque a caixa em Native RBAC Parameters. Selecione Salvar e Fechar

Etapa 3. No menu, selecione Arquivo > Enviar. Arquivo > Enviar.

Note: Todas as alterações devem ser salvas, caso sejam feitas alterações na configuração, elas precisam ser enviadas e implantadas.

Etapa 4. Navegue até CSM Management UI e digite <u>https://<enter_CSM_IP_Address</u> e selecione **Server Administration.**



Note: As etapas 4 a 7 mostram o procedimento para definir a função padrão para todos os administradores que não estão definidos no ISE. Estas etapas são opcionais.

Etapa 5. Valide se o modo de autenticação está definido como **CiscoWorks Local** e **Online** userID é a conta de administrador local criada no CSM.

cisco Cisc	co Security Mana	ger						admin Logout About Feedbac
Home Server * S	Software Center *							
								17 Apr 2021, 14
ommon Services	Home							
Auto Refresh		Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021
	Security		Backup			Recent	ly Completed Jobs	
uthentication Mode	Ciscol/Works Local	Backup Schedule	Not Scheduled	Job ki	Job Type	Status	Description	Completed At
				1001,1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
uthorization 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
unio Tino on Mada	Standaloga			1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
nge agrion wooe		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 Tasks		Inline Users		Management Tax	ka l		Reports
cel User Setup				Schedule Back	kup		Permission Rep	of
ulti-Server Trust Manage	Internet	Mumber of Online upon		Check for Soft	ware Updates		Log File Status	
Configure Single Sign-On		Harrison of Shine alloy		Check for Dev	ice Updates		Process Status	
AA Mode Setup				Collect Server	Information		System Audit L	
			admin					-
		Online User (d(s)	Send Message					

Etapa 6. Navegue até Servidor e selecione Gerenciamento 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	Ċ
Authorizat	Admin	,
Single Sig	Processes	
Siligie Sig	Backup	2
	Log Rotation	
	Collect Server information	
	Selftest	
	Notity Users	
	Job Browser	
	System Preferences	
Local Use	CS Log Configurations	
Multi-Serv	DiskWatcher Configuration	
Configure	Disktratorior Configuration	
AAA Mode	e Setuo II	

Passo 7. Selecione Configuração de gerenciamento de função e selecione o privilégio padrão que todos os usuários admin recebem na autenticação. Para este exemplo, é usado o Network Administrator. Depois de selecionada, selecione **definir como padrão.**

cisco Cisco Security Man	nager		
Home Server * Software Center *			
Navigator Browser-Server Security mode setup Local User Policy Setup Local User Setup Role Management Setup Certificate Setup	Role Management Setup	Image: Description Default Roles Approver Role Image: Desk Role Help Desk Role Image: Desk Role Network Administrator Role Image: Desk Role Network Operator Role Image: Desk Role Security Administrator Role Image: Desk Role Security Administrator Role Image: Desk Role Super Administrator Role Image: Desk Role Super Administrator Role Image: Desk Role Image: Desk Role Image: Desk Role Super Administrator Role Image: Desk Role Image: Desk Role Image: Desk Role <th>econds</th>	econds

Etapa 8. Selecione **Server>AAA Mode Setup Role (Função de configuração do modo AAA)** e selecione a opção **TACACS+**; finalmente selecione **change (alterar)** para adicionar informações do ISE.

ulu cis	co Cisco Security Manager
Home	Server Software Center
Commo	Security Single-Server Management Multi-Server Trust Management Cisco.com Connection Management AAA Mode Setup
Authoriza Single Si	t Admin Processes Backup
	Log Rotation Collect Server information Selftest
	Notify Users Job Browser Resource Browser
Local Us Multi-Ser Configure	System Preferences CS Log Configurations DiskWatcher Configuration

cisco Cisco Security M	lanager
Home Server V Software Center V	
Authentication Mode Setup	
AAA Mode Setup	
Select a Type: ACS O Local RBAC	
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

Etapa 9. Defina o endereço IP e a chave do ISE, opcionalmente, você pode selecionar a opção para permitir todos os usuários de autenticação local ou apenas um usuário se o login falhar. Para este exemplo, o único usuário admin é permitido como método de fallback. Selecione **Ok** para salvar as alterações.

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	
	 Allow all Local Authentication users to fal Authentication login. 	lback to the Local
Login fallback options:	 Only allow the following user(s) to fallbac Authentication login if preceding login fails: 	k to the Local
	admin	(comma separated)
	Allow no fallbacks to the Local Authentica	ation login.
		OK Cancel



Etapa 10. Selecione Server> Single Server Management, selecione Local User Setup e selecione add.

ului cisco	Cisco Security Manager	
Home S	Server v Software Center v	
Commo	Single Server Management	
Auto R	Multi-Server Trust Management	
	Cisco com Connection Management	
	AAA Mode Setup	
Authentica		
Authorizat	Admin	
	Processes	
Single Sig	Backup	
	Log Rotation	
	Collect Server information	
	Selftest	
	Notify Users	
	Job Browser	
	Resource Browser	
Local Lise	System Preferences	
Multi-Sec	CS Log Configurations	
Configure	DiskWatcher Configuration	
AAA Mode S	lature II	

cisco Cisco Security	Manager
Home Server * Software Center *	
Navigator	Local User Setup
Browser-Server Security mode setup Local User Policy Setup	Showing 206 records
Local User Setup Role Management Setup Certificate Setup	1. Aaron Logen 2. Adrian Lotrean
	Annan Kohanas Annan Kohanas Annan Kohanas Annan Kohanas Annan Kohanas Annan Kohanas
	Alariz Castain
	A determine of the second
	10. Anwar Khan 11. armand amith
	12. Bernard Alston 13. bhess
	14. Bill.Mason 15. bill.nash
	16. Billy Vaughan 17. bplotnik
	+a Bredier Ionzan t Select items then take an Import Users Export Users Edit Delete Add Modily My Profile

Etapa 11. Defina o mesmo nome de usuário e senha criados no ISE na etapa 5 na seção de configuração do ISE, as **funções de autorização de tarefas do Help Desk e** do **cliente** são usadas neste exemplo. Selecione **OK** para salvar o usuário admin.

sername:	csmoper			
assword:			Verify Password:	٦
nail:				
uthorization Type				
elect an option: Full A	uthorization 📀 E	hable Task Au	uthorization C Enable Device Authorization	'n
Koles		Device	level Authorization	ר
Help Desk		Not Ap	oplicable	
Approver				
Network Operator				
Network Administrator	·			
System Administrator	I			
Super Admin	I			
Security Administrator				
Conucley Accession				
Security Approver				
				-
OK Cancel				
OK Cancel				

Verificar

IU do cliente do Cisco Security Manager

Etapa 1. Abra um novo navegador de janela e digite <u>https://<enter_CSM_IP_Address</u>, use **csmadmin** username e password criados na etapa 5 na seção de configuração do ISE.



O login bem-sucedido na tentativa pode ser verificado nos registros ao vivo do ISE TACACS

E Cisco ISE			0	perations • TA	CACS	^	Evaluation Mode 39 Days	Q	0 73	0
Live Logs										
영 Refresh : 쇼 Export To 🗸						Refresh Show Every 3 seconds V Later	st 20 records 🗸	Within Last	3 hours	~ •
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	,	ietwork l	Devic.
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	_	Network D	evice N
Apr 17, 2021 02:34:54.1		6	csmadmin	Authentic	CSM 4.22 >> Default		ise30	c	SM422	
Last Updated: Sat Apr 17 2021	09:37:58 0	MT-0500 (C	entral Daylight T	ime)				Rece	ords Show	vn: 1

aplicativo do Cisco Security Manager Client

Etapa 1. Faça login no aplicativo Cisco Security Manager Client com a conta de administrador do helpdesk.

	8
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	
© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or Its affiliates in the U.S. and certain other countries.	

O login bem-sucedido na tentativa pode ser verificado nos registros ao vivo do ISE TACACS

ve Logs								
⊘ Refresh 🖞 Expert To ∨						Refresh Every 3 seconds 🗸	Show Latest 20 records 🗸	Within Last 3 hours →
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic
			Identify		Juthentication Policy	Authorization Dalicy	ise Node	Network Device
×		~	internary			Participation Porcy		CHECKLER DETTER

Etapa 2. No menu do aplicativo cliente CSM, selecione **Tools > Security Manager Administration**, uma mensagem de erro indica que falta de privilégio deve aparecer.

🎒 Device 🔀 Neo 🔅 Pokcy 😹	hiky Bunde	Device Properties		60	e e 6	à 🗞	9	Search AE Categories	CISCO				
Devices		Packet Capture Witard Ping TraceRaute and Millock IP Intelligence	- up			0eg	ployment P Fait 8 😐	Nenager Fending 2 0	Paan: 0		Device State © Critical 0 © Warning 0 © Norr Last Upde	nel 8 No Tene: 17 Apr 2021 03	S I TON POL
Nekies		Store Containment Inventory Satura Cetalyst Sureaman Info Apply PS Updera Preview Configuration Backup Security Manager Diagnestics Security Manager Administration Security Manager Manager Manager Manager Security Manager Manager Manager Manager Manager Security Manager Ma	. • 6en 0 (1	Alerta C	emector e e e e e e e	n Sute 0 0 0 0 0 0 0 0	Deployment Go Go Go Go Go Go Go Go Go Go Go	Addisonal Information	9 Address 199, 134, 215, 3 199, 139, 234, 3 199, 139, 238, 3 199, 139, 238, 3 199, 139, 238, 4 199, 139, 238, 4 199, 139, 238, 4 199, 139, 238, 5	Heat Domain and share works Cardin gov and share works Cardin gov and share works Clusking and share works Clusking ov and share works Clusking ov	Q- from to Search Target 05 Fersion 9.9(2) 9	Running 05 5.9(2)40 5.9(2)40 5.9(2)40 5.9(2)40 5.9(2)40 5.9(2)40 6.9(2)40 8.9(2)40
You do Please If your	not have contact y	sufficient privilege our system adminis e is ACS, privileges	s to per trator a are gra	form and h	Error n this o have th d via A	- In perat	tion. grant y	ou addition.	rivileges				×

OK

Etapa 3. Repita as etapas 1 a 3 com a conta **csmadmin** para validar se as permissões apropriadas foram fornecidas a este usuário.

Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

Validação de comunicação com a ferramenta TCP Dump no ISE

Etapa 1. Faça login no ISE e navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione **Operations>Troubleshoot>Diagnostic Tools (Operações > Solucionar problemas > Ferramentas de diagnóstico).**

Etapa 2. Em Ferramentas gerais, selecione TCP Dumps e selecione Add+ (Adicionar+). Selecione o nome do host, o nome do arquivo da interface de rede, o repositório e, opcionalmente, um filtro para coletar somente o fluxo de comunicação do endereço IP do CSM. Selecione Salvar e executar

Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Down	load Logs Debug Wizard
	Add TCP Dump
General Tools ~	Add 75% Points parties for maniparian on a setterative and travitienters excitizence on the astrony as they appear
RADIUS Authentication TroubI	Add IGP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
Execute Network Device Com	Host Name *
Evaluate Configuration Validat	ise30 V
Posture Troubleshooting	
Apentiess Posture Troublesho	No. of Control of Cont
Endering Datus	Retwork Interface *
TCP Dump	
Tor builty	
Session Trace Tests	Filter
	ip host 10.88.243.42
TrustSec Tools >	
	li.
	E.g: (p host 10.77,122,123 and not 10.177,122,119
	Ele Name
	CSM_Tshoot
	Repository
	VMRepository V
	File Size 100 0 0
	105
	mu -
	1 0 0
	Eadel
	Time Limit
	S O O
	Minute(s)
	Demission Moda
	Cancel Save and Run

Etapa 3. Faça login no aplicativo cliente CSM ou na IU do cliente e digite as credenciais de administrador.

Etapa 4. No ISE, selecione o botão **Stop (Parar**) e verifique se o arquivo pcap foi enviado ao repositório definido.

C Re	fresh + Add	0 Edit	🔋 Trash 🗸 🕨 Start	$igodot$ Stop $\ \pm$ Download			∏ F	Filter 🗸 🐵
	Host Name		Network Interface	Filter	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 Extract To Image: Test Image: Test	ST CSN	1_Tshoot.zip (or	nly 20 days left to b	uy a license	e)		-	
Add Extract To Test View Delete Find Wizard Info ViewsScan Comment SFX	File Co	ommands To	ols Favorites O	ptions He	elp			
↑ Image: CSM_Tshoot.zip - ZIP archive, unpacked size 1,166 bytes Name Size Packed Type Modified CRC32 Image: Provide the folder File folder	Add	Extract To	Test View	Delete	Eind Wa	rd Info VirusScan Comment SFX		
Name Size Packed Type Modified CRC32	Υ.	CSM_Tsh	oot.zip - ZIP archive	e, unpackee	d size 1,166 bytes			
- File folder	Name	^	Size	Packed	Туре	Modified CRC32		
					File folder			
CSM_Tshoot.pcap 1,166 556 PCAP File 4/17/2021 3:29 8A27888D	CSM	Tshoot.pcap	1,166	556	PCAP File	4/17/2021 3:29 8A27888D		

Etapa 5. Abra o arquivo pcap para validar a comunicação bem-sucedida entre o CSM e o ISE.

					CSM_Tshoot.pcap
	1 🧶 🛞	S 🛛 🗋	९ 🗰 🗯 🛅	Ŧ 🗶 🗔	📃 Q, Q, Q, II
Apply	a display filter	<#/>			Expression +
No.	Time	Source	Destination	Protocol	Lengt? Info
r 3	1 0.000000	10.88.243.42	10.122.112.4	TCP	66 55740 → 49 [SYN, ECN, CWR] 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
	9 0.1012/2 5 0.101262	10.88.243.42	10.122.112.4	TACACS+	97 Q: AUTHONICATION 54 AD _ 55740 (AVV) Concl Acked4 Win=20212 Lone0
	5 8.187185	10.122.112.4	10.88.243.42	TACACS+	81 R: Authentication
	7 0.203012	10,88,243,42	10,122,112,4	TCP	60 55740 - 49 [ACK] Seg=44 Ack=28 Win=66048 Len=0
1	8 0.220350	10.88.243.42	10.122.112.4	TACACS+	88 Q: Authentication
	9 0.259963	10.122.112.4	10.88.243.42	TCP	54 49 → 55740 [ACK] Seq=28 Ack=70 Win=29312 Len=0
10	0.311136	10.122.112.4	10.88.243.42	TACACS+	72 R: Authentication
1	1 0.311193	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [FIN, ACK] Seq=46 Ack=70 Win=29312 Len=0
1	2 0.375973	10.88.243.42	10.122.112.4	TCP	60 55740 - 49 [ACK] Seq=70 Ack=47 Win=66048 Len=0
1	4 0.400051	10.88.245.42	10.122.112.4	TCP	56 55/40 - 49 [FIN, ALK] Sequid Ackiel/ Minibole3 Leneo
> Frame	e 6: 81 bytes	on wire (648 bits),	81 bytes captured (6	48 bits)	
Ether	rnet II, Src:	Vmware_a4:0d:c6 (00	0:50:56:a4:0d:c6), Dst	: Cisco_1f:21:4	45 (00:14:6a:1f:21:45)
Inter	rnet Protocol	Version 4, Src: 10.	122.112.4, Dst: 10.88	243.42 10 Coor 1 Act	kr 44 Jan 27
TACA	SHISSION CONT CS+	rot protocot, src pe	ort: 49, 0st Port: 55/	we, sed: I, MCM	1: 44, Len: 2/
Ma Mi Ty	jor version: nor version: pe: Authenti-	TACACS+ 0 cation (1)			
> F1 Se	ags: 0x00 (Er ssion ID: 38	ncrypted payload, Mu 19957939	ltiple Connections)		
0000	14 6a 1f 2	1 45 00 50 56 a4 0	d c6 88 88 45 88 ···	j · ! E · P V · · · · · E	
07	CSM_Tshoot.pca	φ			 Packets: 14 - Displayed: 14 (100.0%) Profile: Default
-					

Se nenhuma entrada for exibida no arquivo pcap, valide o seguinte:

- 1. O serviço de administração de dispositivos está ativado no nó ISE
- 2. O endereço IP correto do ISE foi adicionado na configuração do CSM
- 3. No caso de um firewall estar no meio, verifique se a porta 49 (TACACS) é permitida.