Intégration de CSM TACACS à ISE

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Diagramme du réseau Procédure d'authentification Configuration ISE Configuration CSM Vérification Dépannage

Introduction

Ce document décrit la procédure d'intégration de Cisco Security Manager (CSM) avec Identity Services Engine (ISE) pour l'authentification des utilisateurs administrateurs avec le protocole TACACS+.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur CSM version 4.22
- ISE version 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Par défaut, Cisco Security Manager (CSM) utilise un mode d'authentification appelé CiscoWorks pour authentifier et autoriser les utilisateurs localement, afin d'avoir une méthode d'authentification centralisée que vous pouvez utiliser Cisco Identity Service Engine via le protocole TACACS.

Configuration

Diagramme du réseau



Procédure d'authentification

Étape 1.Connectez-vous à l'application CSM avec les informations d'identification de l'utilisateur Admin.

Étape 2. Le processus d'authentification se déclenche et ISE valide les informations d'identification localement ou via Active Directory.

Étape 3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour autoriser l'accès au CSM.

Étape 4. CSM mappe le nom d'utilisateur avec l'affectation du rôle d'utilisateur local.

Étape 5. ISE affiche un journal en direct d'authentification réussi.

Configuration ISE

Étape 1. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et accédez à **Administration > Network Resources > Network Devices**.

E Cisco ISE		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	Network	k Devices									
Device Security Settings	Øtot + A Name	dd Duplicate 🕁 Import e 🔿 IP/Mask Profile N	the Deport → A Generate PW	C Delete V Type	Description						

Étape 2. Cliquez sur le bouton +Ajouter et entrez les valeurs appropriées pour le nom du périphérique d'accès réseau et l'adresse IP, puis vérifiez la case TACACS Authentication Settings et définissez un secret partagé. Sélectionnez le bouton Soumettre.

Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Servers NAC Managers External MDM Location Services
Natarofk Devices	Network Device Ltd: > Rev Relative Device
Default Device Device Security Settings	Network Devices
	* Name CSM422
	Description
	E #Addesix v *P1 10.85.243.42 / 32 @+
	* Device Profile as Owner w ID
	Nudel Name
	Sofware Version
	* Network Device Group
	Location All Locations 🗸 Set To Default
	In IPSEC Device V Set To Default
	Levice Types V Set To Default
	RADIUS Authentication Settings
	TACACS Authentication Settings
	David Secret Show
	theter tinge Convect Note
	Lapay Crash Service TACACS Draft Compliance Single Connect Support
	SNMP Settings
	Advanced TrustSec Settings
	A AND CONTRACTOR

Étape 3. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et accédez à **Administration > Identity Management > Groups.**

Cisco ISE		Administration · Identity Ma	anagement
entities Groups External Ider	ntity Source	Identity Source Sequences	Settings
Identity Groups	User	Identity Groups	
< 22 Ø			
> 🗀 Endpoint Identity Groups	/ Edit	+ Add 👩 Delete 🗸 🕁 Import	t 📩 Export 🗸
> 🛅 User Identity Groups		Name	∧ Description
		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
		A Employee	Default Employee User Group
		GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
		EuestType_Contractor (default)	Identity group mirroring the guest type
		F GuestType_Daily (default)	Identity group mirroring the guest type
		A GuestType_SocialLogin (default)	Identity group mirroring the guest type
		A GuestType_Weekly (default)	Identity group mirroring the guest type
		VWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Étape 4. Accédez au dossier Groupes d'identités utilisateur et sélectionnez le bouton +Ajouter. Définissez un nom et sélectionnez le bouton Soumettre.

dentities Groups External Iden	ty Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 28 Ø		Selected 0 Total 10 🔗 🚷
> 🗀 Endpoint Identity Groups	🖉 Edit 🕂 Add 🏮 Delete 🗸 🕁 Import 🛧 Export 🗸	$\sim 10^{-10}$
> 🛅 User Identity Groups	Name Description	
	ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	CSM Admin	
	CSM Oper	

Note: Cet exemple montre comment créer des groupes CSM Admin et CSM Oper Identity. Vous pouvez répéter l'étape 4 pour chaque type d'utilisateurs Admin sur CSM

Étape 5. Sélectionner l'icône des trois lignes et accédez à Administration > Identity Management > Identities. Cliquez sur le bouton +Ajouter et définissez le nom d'utilisateur et le mot de passe, puis sélectionnez le groupe auquel appartient l'utilisateur. Dans cet exemple, crée les utilisateurs csmadmin et csmoper et affectés respectivement aux groupes CSM Admin et CSM Oper.

dentities Groups Ex	amal Identity Sources Identity Source Sequences Settings	
	Narwork Acons Gum Unt () considers	
n Merual Network Scan Res	✓ Network Access User * New containin Sons © Enelled ∨ Enel ✓ Passwords Passwords *Lopit Password *Lopit Password Transe Transe Transe	0
	V User Information Free Name Last Name Vectorate Cescopton	
	Charge passward on nor login Charge passward on nor login Account Disable Policy Deable account 6 data access 2021-36-16 (yyyu-me-at) V User Groups	
	E <u>COM Admin</u> <u>v</u> – +	

Latest Manual Network Scan Res	Network Access Users									
								Selected 0 Total 2	ø	٥
	0 Edit	+ Add	🛞 Change Status 🚿	import ريلي 🗸	🖞 Export 🗸 🛛 🗍	Delete 🗸 📋 Dv	plicate		• ~	Υ.
		Status	Name	∧ Description	n First Na	me Last Name	Email Address	User Identity Grou A	d	
		Enabled	2 csmadmin					CSM Admin		
		Enabled	2 csmoper					CSM Oper		

_	

Étape 6. Sélectionner et accédez à **Administration > System > Deployment.** Sélectionnez le noeud de nom d'hôte et activez le **service d'administration de périphérique**



Note: En cas de déploiement distribué, sélectionnez le noeud PSN qui gère les requêtes TACACS.

Étape 7. Sélectionnez l'icône des trois lignes et accédez à Administration > Device Administration > Policy Elements. Accédez à Résultats > Jeux de commandes TACACS. Cliquez sur le bouton +Ajouter, définissez un nom pour le jeu de commandes et activez la commande Permit any qui n'est pas répertoriée sous la case à cocher. Sélectionnez Submit.

Cisco ISE			Work Centers -	Device Administration		Evaluation Mod	: 19 Days Q (0)	58 Ø
Overview Identitie	'S	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More ${\scriptstyle \curlyvee}$	
onditions	>	TACACS Command Sets Command Set	> New					
twork Conditions	>	Name						
sults	~	Permit all						
Allowed Protocols								
TACACS Command Sets		Description						
TACACS Profiles		Commands		1				
		Permit any command that	t is not listed below	0				
		+ Add 🔋 Trash 🗸	🖉 Edit 🔿 Move U	p 💛 Move Down				
		Grant	Command	Arguments				
		No data found						
		rea casa touno.						

Étape 8. Sélectionnez l'icône de trois lignes située dans le coin supérieur gauche et accédez à

Administration->Administration des périphériques->Jeux de stratégies d'administration des

périphériques. Sélectionner situé sous le titre Jeux de stratégies, définissez un nom et sélectionnez le bouton + au milieu pour ajouter une nouvelle condition.

Policy	/ Sets			Reset Reset Policyset Hitcounts	Save	
۲	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits	Actions View
0) Search					
	۰	CSM Administrators		+	Select from list \sim +	<u>نې</u>
	۰	Default	Tacacs Default policy set		Default Device Admin $@>+$ o	

Étape 9. Sous Condition, sélectionnez Ajouter un attribut, puis sélectionnez **Network Device** Icon, suivi de Network Access device IP address. Sélectionnez **Attribute Value** et ajoutez l'adresse IP CSM. Sélectionnez **Utiliser** une fois terminé.

.

Conditions Studio				
Library	Editor			
Search by Name		Network Access-De	vice IP Address	0
	ę	Equals 🗸	10.88.243.42	
No conditions found - reset filters.		Set to 'Is not'		Duplicate
			NEW AND OR	
				Close Use

Étape 10. Dans la section Allow protocols, sélectionnez Device Default Admin. Sélectionnez Save (enregistrer)

Policy	Sets						Reset	set Policyset Hit	counts		Save
۲	Status	Policy Set Name	Description	Co	nditions		Allowed Protocols / S	erver Sequence	Hits	Actions	View
Q	Search										
	0	CSM 4.22		ę	Network Acce Address EQU	ISS-Device IP IALS 10.88.243.42	Default Device Admi	n <u>∞</u> ~+	0	ŵ	•

Étape 11. Sélectionner la flèche droite d'authentification et d'autorisation

icône du jeu de stratégies pour définir les stratégies

Étape 12. Sélectionner situé sous le titre de la stratégie d'authentification, définissez un nom et sélectionnez le + au milieu pour ajouter une nouvelle condition. Sous Condition, sélectionnez Ajouter un attribut, puis sélectionnez **Network Device** Icon, suivi de Network Access device IP address. Sélectionnez **Attribute Value** et ajoutez l'adresse IP CSM. Sélectionner **Utiliser** une fois terminé

Étape 13. Sélectionnez Utilisateurs internes comme magasin d'identité et sélectionnez Enregistrer

✓ Authe	nticatio	n Policy (1)					
•	Status	Rule Name	Co	nditions	Use	Hits	Actions
Q	Search						
					Internal Users	a ~	
	0	CSM Authentication		Network Access-Device IP Address EQUALS 10.88.243.42	> Options		(2)

Note: Le magasin d'identités peut être modifié en magasin AD si ISE est joint à Active Directory.

_	
_	
_	
_	

Étape 14. Sélectionner situé sous le titre de la stratégie d'autorisation, définissez un nom et sélectionnez le bouton + au milieu pour ajouter une nouvelle condition. Sous la fenêtre Condition, sélectionnez Ajouter un attribut, puis sélectionnez l'icône **Groupe d'identités** suivie de **Utilisateur interne : Groupe d'identités.** Sélectionnez le groupe d'administration CSM et sélectionnez **Utiliser**.

orony	E	ditor					
Search by Name			InternalUser-Identity	Group			
	E O 1 O E 🕈	*	Equals 🗸	User Identity	Groups:CSM Adm	in × 🗸	
EAP-MSCHAPv2	٥		Set to 'Is not'			Duplicate	Save
EAP-TLS	٥			NEW A	ND OR		
Guest_Flow	٥						
Network_Access_Authen Passed	tication_ ()						

Étape 15. Sous Jeu de commandes, sélectionnez Autoriser tout jeu de commandes créé à l'étape 7, puis sélectionnez **Enregistrer**

Répétez les étapes 14 et 15 pour le groupe CSM Oper

V Authori	ization	Policy (3)								
					Results					
🕣 s	tatus	Rule Name	Con	ditions	Command Sets		Shell Profiles		Hits	Actions
(Q :	Search									
	•	CSM Oper	A	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	$\left \text{Permit all} \times \right $	\sim +	Select from list	~+	0	{
	0	CSM. Admin	. А.	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$Permit all \times$	~+	Select from list	~+	0	{\$}
	0	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>a</u> ~+	0	{ĝ}

Étape 16 (Facultatif). Sélectionnez l'icône de trois lignes située dans le coin supérieur gauche et sélectionnez **Administration>Système>Maintenance>Référentiel**, sélectionnez **+Ajouter** pour ajouter un référentiel utilisé pour stocker le fichier de vidage TCP à des fins de dépannage.

Étape 17 (Facultatif). Définissez un nom de référentiel, un protocole, un nom de serveur, un chemin d'accès et des informations d'identification. Sélectionnez **Soumettre** une fois terminé.

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				

Configuration CSM

Étape 1. Connectez-vous à l'application Client Cisco Security Manager avec le compte d'administrateur local. Dans le menu, accédez à Outils > Administration de Security Manager

		6
		Cisco Security Manager Version 4.22.0 Service Pack 1
		Server Name 10.88.243.42 V Username admin
		Password ••••••• Default View Configuration Manager v Login Help
© 2020 Cisco Sys its affiliates in th	tems, Inc. Cisco, Cisco Systems e U.S. and certain other countries	and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or Cisco



Étape 2. Cochez la case sous Paramètres RBAC natifs. Sélectionnez Enregistrer et Fermer

3	Cisco Security Manager - Administration	_ _ X
	Server Security Use the buttons 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 visit not available in Local User Database	Save Reset Restore Defaults

Étape 3. Dans le menu, sélectionnez Fichier > Soumettre. Fichier > Soumettre.

Note: Toutes les modifications doivent être enregistrées, en cas de modifications de configuration, elles doivent être soumises et déployées.

Étape 4. Accédez à CSM Management UI et tapez <u>https://<enter_CSM_IP_Address</u> et sélectionnez Administration du serveur.



Note: Les étapes 4 à 7 montrent la procédure permettant de définir le rôle par défaut de tous les administrateurs qui ne sont pas définis sur ISE. Ces étapes sont facultatives.

Étape 5. Valider le mode d'authentification est défini sur CiscoWorks Local et Online userID est le compte d'administrateur local créé sur CSM.

Home Server • S	co Security Manag	er						edmin Logout About Freedback
								17 Apr 2021, 14
Common Services	Home	Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021
	Security		Backup			Recent	y Completed Jobs	
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job 15 1001.1370	Job Type SystemCheckUtility	Status Succeeded	Description SysCheckTest	Completed At Sat Apr 17 05:01:56 PDT 2021
uthorization Mode	CiscoWorks Local Standaione	Last Backup Completed at	Not found or unable to detect	1001.1369	SystemCheckUtility SystemCheckUtility	Succeeded Succeeded	SysCheckTest SysCheckTest	Fri Apr 16 05:00:58 PDT 2021 Thu Apr 15 05:00:57 PDT 2021
		Contract Concept Contract		1001.1367	SystemCheckUtility SystemCheckUtility	Succeeded	SysCheckTest SysCheckTest	Wed Apr 14 05:00:55 PDT 2021 Tue Apr 13 05:00:54 PDT 2021
				1001.1366	SystemCheckUtility SystemCheckUtility	Succeeded	SysCheckTest SysCheckTest	Mon Apr 12 05:00:56 PDT 2021 Sun Apr 11 05:00:55 PDT 2021
				1001.1363	systemCneckOsity	Succeeded	Syscheoktest	Sal Apr 10 05:00 56 PDT 2021 More
	System Tasks		wine Users		Management Tax	•		Reports
ocal User Setup Auti-Server Trust Manage Configure Single Sign-On	ment	Number of Online users	()	Schedule Back Check for Soft Check for Dev	kup ware Updates loe Updates		Permission Rep Log File Status Process Status	of
www.wooe.oegup		Online User Id(s)	admin Send Message	Conect Server	romation		System Aude Lo	9

Étape 6. Accédez à Serveur et sélectionnez Gestion à serveur unique

ulu cisc	cisco 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	,		
Cinala Cia	Processes			
Single Sig	Backup	2		
	Log Rotation			
	Collect Server information			
	Selftest			
	Notify Users			
	Job Browser			
	Resource Browser			
Local Use	System Preterences			
Multi-Serv	DiskWatcher Configuration			
Configure	Diskwatcher Conliguration			
AAA Mode	Setup			

Étape 7. Sélectionnez Configuration de la gestion des rôles et sélectionnez le privilège par défaut que tous les utilisateurs admin reçoivent lors de l'authentification. Dans cet exemple, Network Administrator est utilisé. Une fois sélectionné, sélectionnez **défini par défaut.**

cisco Cisco Security Mar	ager		
Home Server * Software Center *			
Navigator	Role Management Setup		
Browser-Server Security mode setup			Showing 8 percents
Local User Policy Setup	Roles	Description	Default Roles
Local User Setup	1. Approver	Approver Role	
Kole Management Setup Certificate Setup	2. Help Desk	Help Desk Role	
	3. Network Administrator	Network Administrator Role	R
	4. Network Operator	Network Operator Role	
	5. Security Administrator	Security Administrator Role	
	6. C Security Approver	Security Approver Role	
	7. 🖸 Super Admin	Super Admin Role	
	8. O System Administrator	System Administrator Role	
	Add Edit Delete Copy I Export	Import I Set as default Clear default	

Étape 8. Sélectionnez Serveur>Rôle de configuration du mode AAA, puis sélectionnez TACACS+, enfin sélectionnez modifier pour ajouter des informations ISE.

ii)ii cise	 Cisco Security Manager
Home	Server Software Center
Common Auto R Authentics Authorizat	Security Single-Server Management Multi-Server Trust Management Cisco.com Connection Management AAA Mode Setup Admin
Single Sig	Processes Backup Log Rotation Collect Server information Selftest Notify Users Job Browser Resource Browser
Local Use Multi-Serv Configure	System Preferences CS Log Configurations DiskWatcher Configuration

cisco Cisco Security Manager	
Home Server Software Center	
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+	
Chang	0

Étape 9. Définissez l'adresse IP ISE et la clé, si vous le souhaitez, vous pouvez sélectionner l'option permettant d'autoriser tous les utilisateurs d'authentification locale ou un seul utilisateur si la connexion échoue. Dans cet exemple, l'utilisateur Only admin est autorisé comme méthode de secours. Sélectionnez **OK** pour enregistrer les modifications.

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 🙁 False
	 Allow all Local Authentication users to fallback to the Local Authentication login.
Login fallback options:	 Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails:
	admin (comma separated)
	 Allow no fallbacks to the Local Authentication login.
	OK Cancel



Étape 10. Sélectionnez Server> Single Server Management, puis sélectionnez Local User Setup et sélectionnez 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	Palua	

ululu cisco Cisco Securit	v Manager
Home Server * Software Center *	, managor
Navigator	Local User Setup
Browser-Server Security mode setup	Showing 206 record
Local User Policy Setup	
Local User Setup	Advantagen
Certificate Setup	Addas Bichante
	5 Attractor
	A Mark Castain
	7 alam unitabilitared
	A alter stiened
	Action Conner
	10. Preservan
	12 Remark Alter
	15 North
	16. bilash
	16 Bit/Junhan
	17 beldnik
	18 Bradian Israel
	tSelect items then take an Import Users Export Users Edt Delete Add Modify My Profile

Étape 11. Définissez le même nom d'utilisateur et le même mot de passe créés sur ISE à l'étape 5 sous la section Configuration ISE, les **rôles csmoper** et d'**autorisation des tâches du centre d'assistance** sont utilisés dans cet exemple. Sélectionnez OK afin d'enregistrer l'utilisateur admin.

semame:	csmoper			
assword:			Verify Password: ••	
mail:				
uthorization Type			-	
elect an option: O Full Auth	orization 💿 En	able Task Au	thorization 💿 Enab	le Device Authorization
Roles		Device	level Authorization	
Help Desk		Not Ap	plicable	
Approver				
Network Operator				
Network Administrator				
System Administrator				
Super Admin				
Security Administrator				
Cocurity Approver				
Security Approver				
OK Cancel				
OR Conver				

Vérification

Interface utilisateur du client Cisco Security Manager

Étape 1. Ouvrez un nouveau navigateur de fenêtre et tapez <u>https://<enter_CSM_IP_Address</u>, utilisez csmadmin nom d'utilisateur et mot de passe créés à l'étape 5 dans la section de configuration ISE.



La tentative de connexion réussie peut être vérifiée sur les journaux en direct ISE TACACS

E Cisco ISE			c	Operations • TAI	CACS	A 1	Ivaluation Mode 39 Days	0.0	Ø 0
Live Logs									
🕄 Refresh 🖞 Disport To 🗸						Refresh Show Lates	t 20 records 🗸	Ulthin Last 3 hours	· ·
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network	k Devic.
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	Network	Device N
Apr 17, 2021 02:34:54.1		6	csmadmin	Authentic	CSM 4.22 >> Default		ise30	C5M422	
Last Updated: Sat Apr 17 2021	09:37:58 0	GMT-0500 (C	entral Daylight 1	Time)				Records Sh	own: 1

Application client Cisco Security Manager

Étape 1. Connectez-vous à l'application Client Cisco Security Manager avec le compte d'administration du centre d'assistance.

	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.	•

La tentative de connexion réussie peut être vérifiée sur les journaux en direct ISE TACACS

le Logs								
ට Refresh ්ර Export To 🗸						Refresh Every 3 seconds 🗸	Show Latest 20 records 🗸	Within Last 3 hours
Longed Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	lse Node	Network Devic
cogged time								
×		~	Identity		Juthentication Policy	Authorization Policy	Ise Node	Network Device

Étape 2. Dans le menu de l'application cliente CSM, sélectionnez Outils > Administration du gestionnaire de sécurité, un message d'erreur indique un manque de privilège.

🎒 Device 🔀 Neo 🔅 Policy 🚔 P	ky Bunde	Device Properties	66	9 🖗 🖗	6.6					9	Search All Categories	CISCO
Ner: -rore - v	Healt 0	Packet Capture Witard Packet Capture Witard Ping TraceRoute and NiLockup			Orgal © 1	loyment P fait 0 0	tenager Fending 8 - O	Paan: 0		Device State © Critical 3 © Warring 3 © Korn	w1	
8 - A Constant 8 - Constant	0 a 🛔	Pinteligence								Leet Updet	e Time: 17 Apr 2021 00	LIB PM PDT B
* () 4		Show Containment Inventory Status Catalyst Summary Info Apply IPS Update	-	Alerta 0	Connection 0	Sale 0	Deployment Que	Additional Information	D Address 199, 134, 215, 3 199, 139, 215, 3	risat.Donain qui situs vanto 3 vado.gov qui situs vanno 3 vado.gov	C- have to Search Target OS Hension 9.9(2) 9.9(2)	Running CS 5.9(2)40 5.9(2)40
	2	Preview Configuration Backup Security Manager Discretifict			:	0	8. 8.		199, 139, 215, 9 199, 139, 215, 10 199, 134, 215, 4	gin 1 alus varvas 11. uslauga gin 1 alus varvas 12. uslauga gin 2 alus varvas 12. uslauga	v 9.900 v 9.900 9.900	5.9(2)40 5.9(2)40 5.9(2)40
Publies	9 ad 9 ad 9 ad	Security Manager Administration Inter-unite-Scanin-gev 0 Inter-unite-Scanin-gev 0	0	:	:	0	6 6 6		1998, 5398, 243, 4 1998, 5394, 215, 5 1998, 539, 245, 5	igna) atur varvar 3 unda gin gua) atur varte 3 unda gin gua) atur varvar 2 unda gin	9.9(2) 9.9(2) 9.9(2)	8.9(2)40 8.9(2)40 8.9(2)40
				Error	r - Ins	suffic	ient P	rivileges				x
You do r Please o If your / If your /	ot have ontact ye AA mode AA mode	sufficient privileges to p our system administrato e is ACS, privileges are e is non-ACS, privileges	r and grant are g	m this (have t ted via / granted	operati hem gr ACS co via "C	ion. rant y nfigur iscoW	ou additi ation. orks Hon	onal privileges. Jepage > Serve	er > Single-5	ierver Management > L	ocal User Se	tup".

Étape 3. Répétez les étapes 1 à 3 avec le compte **csmadmin** pour valider les autorisations appropriées ont été fournies à cet utilisateur.

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Validation de la communication avec l'outil TCP Dump sur ISE

Étape 1.Connectez-vous à ISE et accédez à l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez Operations>Troubleshoot>Diagnostic Tools.

Étape 2. Sous Outils généraux, sélectionnez Dumps TCP puis sélectionnez Ajouter+. Sélectionnez Hostname, Network Interface File Name, Repository et éventuellement un filtre pour collecter uniquement le flux de communication d'adresse IP CSM. Sélectionnez Enregistrer et exécuter

Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Down	nload Logs Debug Wizard
	Add TCP Dump
General Tools	Add TAD Dump packet for mechanism on a second interface and productions are the advant as the second
RADIUS Authentication Troubl	Add IL-> 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	
Agentiess Posture Troublesho	Natural Interface
EndBoird Debug	GigableEthernet 0 V 0
TCP Dump	
Session Trace Tests	
Session made resta	Filer
	ip host 10.88.243.42
TrustSec Tools	
	F or in bost 10.77 122 123 and not
	10,177,122,119
	File Name
	CSM_Tshoot
	Nepository VMRepository V
	File Size
	100 0
	Mb
	Fields
	Time Linit
	5 0
	Minute(s)
	Promiscuous Mode
	Cancel Save and Run

Étape 3. Connectez-vous à l'application cliente CSM ou à l'interface utilisateur du client et saisissez les informations d'identification d'administrateur.

Étape 4. Sur ISE, sélectionnez le bouton Arrêter et vérifiez que le fichier pcap a été envoyé au référentiel défini.

C Re	fresh + Add	0 Edit	📋 Trash 🗸 🕨 Start	$igodot$ Stop $\ \pm$ Download			$\nabla \mathbf{r}$	Filter 🗸 🐵
	Host Name		Network Interface	Filter	File Name	Repository	File S	Number o
	ise30.ciscoise.lab		GigabitEthernet 0	ip host 10.88.243.4	2 CSM_Tshoot	VMReposit	100	1

💶 CSM_Tshoot.zip (/	only 20 days left to bu	y a license)		-	
File Commands T	lools Favorites Opt	tions Help			
Add Extract Te	Test View	Delete Find	Wizard Info VirusScan Comment SFX		
1 CSM_Tsi	hoot.zip - ZIP archive,	unpacked size 1,166 by	ytes		
Name	Size	Packed Type	Modified CRC32		
		File folder			
CSM_Tshoot.pcap	1,166	556 PCAP File	4/17/2021 3:29 8A27888D		
CSM_IShoot.pcap	1,100	550 PCAP File	4/11/2021 3:29 8A2/8880		

Étape 5. Ouvrez le fichier pcap pour valider la communication réussie entre CSM et ISE.

• •	•				CSM_Tshoot.pcap
	📕 🙋 🛞	🖸 🕺 🗂 🚞	९ 🗰 👄 🚞	Ŧ 🗶 🗔	📃 Q Q Q 🎹
Ap	ply a display filter	<೫/>			📼 🔹 Expression 🔸
No.	Time	Source	Destination	Protocol	Lengt/ Info
e	1 0.000000	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 55748 → 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 0.101362	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0
	6 0.107185	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] Seq=44 Ack=28 Win=66048 Len=0
	8 0.220350	10.88.243.42	10.122.112.4	TACACS+	80 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
	11 0.311193	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) Seq=70 Ack=47 Win=66048 Len=0
	13 0.400051	10.88.243.42	10.122.112.4	TOP	00 55740 4 49 [FIN, ACK] Segura Acki47 Winibo048 Lenia
> Fr	ame 6: 81 bytes	on wire (648 bits),	, 81 bytes captured (6	48 bits)	
> Et	hernet 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)
> Ir	ternet Protocol	Version 4, Src: 10.	.122.112.4, Dst: 10.88	.243.42	
> Tr	ansmission Cont	rol Protocol, Src Po	ort: 49, Dst Port: 557	40, Seq: 1, Ack	k: 44, Len: 27
~ T/	CACS+				
	Major version:	TACACS+			
	Minor version:	0			
	Type: Authentic	cation (1)			
	Sequence number	r: 2			
>	Flags: 0x00 (Er	ncrypted payload, Mu	iltiple Connections)		
	Session ID: 381	19957939			
0000	00 14 6a 1f 2	1 45 00 50 56 a4 0	d c6 88 88 45 88 ···	1 · ! E · P V · · · · · E	
-					
0	CSM Taboot oca				Packets: 14 - Displayed: 14 (100,016) Profile: Default

Si aucune entrée n'est affichée sur le fichier pcap, validez les éléments suivants :

- 1. Le service Administration des périphériques est activé sur le noeud ISE
- 2. L'adresse IP ISE correcte a été ajoutée à la configuration CSM
- 3. Si un pare-feu est au milieu, vérifiez que le port 49 (TACACS) est autorisé.