# CSM TACACS與ISE整合

## 目錄

## 簡介

本檔案介紹將思科安全管理員(CSM)與身份服務引擎(ISE)相整合的過程,用於管理員使用者使用 TACACS+協定進行身份驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題:

- •思科安全管理員(CSM)。
- •身分識別服務引擎(ISE)。
- TACACS通訊協定。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- CSM伺服器版本4.22
- ISE版本3.0

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

## 背景資訊

預設情況下,思科安全管理器(CSM)使用稱為Ciscoworks的身份驗證模式在本地對使用者進行身份

驗證和授權,以便採用集中身份驗證方法,您可通過TACACS協定使用思科身份服務引擎。

### 設定

網路圖表



### 驗證程式

步驟1.使用管理員使用者的憑據登入CSM應用程式。

步驟2.身份驗證過程觸發和ISE在本地或通過Active Directory驗證憑證。

步驟3.身份驗證成功後,ISE傳送允許資料包以授權對CSM的訪問。

步驟4. CSM將使用者名稱與本地使用者角色分配進行對映。

步驟5. ISE顯示成功的身份驗證即時日誌。

ISE 組態

**步驟1.**選擇三行圖示 位於左上角,導航到**管理>網路資源>網路裝置。** 

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 Device Security Settings	Network	< Devices						
	Ø Edit + Ad	ld 🗋 Ovplicate 🕁 Import	💩 Export 🗸 👌 Generate PA	0 🔋 Delete 🗸				
	Name	A IP/Mask Profile N	lame Location	Туре	Description			

**步驟2.選擇+Add**按鈕並輸入網路訪問裝置名稱和IP地址的正確值,然後驗證**TACACS身份驗證設定** 覈取方塊並定義共用金鑰。選擇「Submit」按鈕。

Network Devices N	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services
Notwork Devices Default Device Device Security Settings	Network Devices Life > InverNetwork Device Network Devices * Name CDM422 Description
	E #ARRHS ~ *P: 1085243.42 / 32 @.
	träckt bruit Complexes Brige Convert Surgers     V SNMP Settings     V Advanced TrustSec Settings



E Cisco ISE	Administration • Identity Mana	agement
Identities Groups External Ide	ntity Sources Identity Source Sequences	Settings
Identity Groups	User Identity Groups	
< 🐮 🔅	🖉 Edit 🕂 Add 🌘 Delete 🗸 🕁 Import	û Export ∨
> 🛅 User Identity Groups	Name ^	Description
	ALL_ACCOUNTS (defauit)	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

步驟4.導航到User Identity Groups檔案夾,然後選擇+Add按鈕。定義名稱並選擇提交按鈕。

Identities	Groups	External Ide	ntity Sources	Identity Source Sequences Setting:	1	
Identity Gr EQ	oups		User Ic	entity Groups		
< 18	1	Φ			Selected 0 Total 10 🤗	0
> 🗖 E	indpoint Identity	Groups	0 Edit +	Add 🍵 Delete 🗸 🕁 Import 🟦 Export	✓ AII ✓	$\nabla$
> 🗖 (	Jser Identity Grou	ps	Nar	ne ^ Descrip	rtion	
			0 4	ALL_ACCOUNTS (default) Default	NLL_ACCOUNTS (default) User Group	
			0 4	CSM Admin		
			0 😤	CSM Oper		

**附註**:此示例建立CSM Admin和CSM Oper Identity組。您可以對CSM上每種型別的管理員使 用者重複步驟4

**步驟5.**選擇三行圖示 並導航到**管理>身份管理>身份。選擇+Add**按鈕並定義使用者名稱和密碼,然後選擇使用者所屬的組。在本示例中,分別建立csmadmin和csmoper使用者並分配給CSM Admin和CSM Oper組。

		summoration - toentry Management
Identities Groups E	temal Identity Sources Identity Source Sequences Settings	
**	Nerwork Address General General Consideration	
ant Mercad Helwork Scan Res	✓ Network Access User       * New constrain       State       State       © Enelled ∨       Enel       ✓ Passwords       Passed Type:       Internal bans       Y Lope Password       Trape Password       Trape Password       Cenerate Pass       Cenerate Pass       Trape Password	word O
	User Information     First Name     LastName	
	Account Options     Description     Charge deeward on text tops.	
	Account Disable Policy     Disable account if data access     2021-06-16     (vgv-mm-4d)	
	✓ User Groups	

Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
	🖉 Edik 🕂 Add 🛞 Change Status 🗸 🕁 Import 🕕 Export 🗸 🏮 Delete 🗸 📋 Du	Selected 0 Total 2 🧭 🧔 plicate All V 🏹
	Status Name	Email Address User Identity Grou Ad
	🔲 🔲 Enabled 👤 csmadmin	CSM Admin
	Enabled 1 camoper	CSM Oper

並導航到**管理>系統>部署。**選擇主機名節點並啟用Device Admin Service

**步驟6.選**擇



**附註**:如果是分散式部署,請選擇處理TACACS請求的PSN節點

**步驟7**.選擇三行圖示並導航到**管理>裝置管理>策略元素。導覽至Results > TACACS Command** Sets。選擇+Add按鈕,為Command Set定義名稱,並啟用Permit any command that not listed below覈取方塊。選擇**提交。** 

Overview Identiti	es	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More $\scriptstyle \lor$	
anditions	>	TACACS Command Sets Command Set	> New					
sults	``	Name Permit all						
TACACS Command Sets		Description						
		Commands Permit any command that	t is not listed below	5				
		+ Add 🛛 Trash 🗸	🖉 Edit 🔷 Move Up	Move Down				

步驟8.選擇位於左上角的三行圖示,然後導航到Administration -> Device Administration -> Device

Admin Policy Sets。選擇 🔛 位於Policy Sets標題下方,定義名稱並選擇中間的+按鈕以新增新條

ŀ	Ł	
T	Г	ο

Policy Sets				Reset	Reset Policyset Hit	counts		Save
Status	Policy Set Name	Description	Conditions	Allowed Protocols	/ Server Sequence	Hits	Actions	View
Q Search								$\supset$
٥	CSM Administrators		+	Select from list	~+		(2)	>
٥	Default	Tacacs Default policy set		Default Device A	dmin 🤕 🖂 +	0	贷	•

**步驟9.在**Condition(條件)視窗中,選擇add a attribute(新增屬性),然後選擇**Network Device** Icon(網路裝置圖示),後跟Network access device IP address(網路訪問裝置IP地址)。 選擇 **Attribute Value**並新增CSM IP地址。選擇**Use** once done。

I.

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

### 步驟10.在allow protocols部分下,選擇Device Default Admin。選擇保存

Policy Sets					Reset Policyset Hi	tcounts		Save
Status Policy Set Name	Description	Cor	nditions	Allowed Protoco	ls / Server Sequence	Hits	Actions	View
Q Search								
CSM 4.22		ę	Network Access-Device IP Address EQUALS 10.88.243.42	Default Device	Admin 🛚 🙁 +	0	贷	>

步驟11.選擇右箭頭

用於定義身份驗證和授權策略的策略集的圖示

**步驟12.選擇 ────** 位於身份驗證策略標題下方,定義名稱並選擇中間的+以新增新條件。在「條件」視窗中,選擇新增屬性,然後選擇**網路裝置**圖示,後跟網路訪問裝置IP地址。 選擇Attribute Value並新增CSM IP地址。選擇**使用一**次

步驟13.選擇Internal Users作為Identity Store並選擇Save

۲	Status	Rule Name	Con	ditions	Use	Hits	Actions
0	Search						
					Internal Users 🛛 🛇 🗸		
	CSM Authentication	Ģ	Network Access-Device IP Address EQUALS 10.88.243.42	> Options		₹ĝ}	

**附註**:如果ISE加入到Active Directory,可以將身份儲存更改為AD儲存。

步驟14.選擇 位於Authorization Policy標題下方,定義名稱並選擇中間的+按鈕以新增新條件。在「條件」視窗中,選擇新增屬性,然後選擇身份組圖示,後跟Internal User:身份組。選擇CSM Admin Group,然後選擇Use。

Conditions Studi	0					-
Library		Editor				
Search by Name			InternalUser-Identity	Group		0
Ŷ¤○♣♦₽₽₽₽₽₽	E @ 1 0 E 🕈	4	Equals 🗸	User Identity Groups:CSM Adr	min × 🗸	
# EAP-MSCHAPv2	0		Set to 'Is not'		Duplicate	Save
🗄 🗐 EAP-TLS	0			NEW AND OR		
: Guest_Flow	0					
E Network_Access_Authent	ication_ ()					

步驟15.在命令集下,選擇允許在第7步中建立的所有命令集,然後選擇保**存** 

### 對CSM Oper組重複步驟14和15

Authorized Authoriz	orization	Policy (3)								
					Results					
۲	Status	Rule Name	Cor	ditions	Command Sets		Shell Profiles		Hits	Actions
Q	Search									
	۰	CSM Oper	8	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	${\rm Permit \ all } \times$	~+	Select from list	~+	0	{ĝ}
	۲	CSM. Admin	8	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$\text{Permit all} \times$	~+	Select from list	<u> </u>	0	{ĝ}
	۲	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>∞</u> ~+	0	{Ô}

**第16步(可選)。** 選擇左上角的三行圖示並選擇**管理>系統>維護>儲存庫**,選擇+**新增**以新增用於 儲存TCP轉儲檔案以進行故障排除的儲存庫。

第17步(可選)。 定義儲存庫名稱、協定、伺服器名稱、路徑和憑據。選擇Submit once done。

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 (	Configuratio	n				
Operational Data Pur	ging							
		* Repository N	ame VMRepo	sitory				
		* Protocol	FTP	<u>&lt;</u>				
		Location						
		* Server Name	10.122.	112.137				
		* Path	1					
		Credentials						
		* User Name	cisco					
		* Password						

## CSM配置

**步驟1.**使用本地管理員帳戶登入到思科安全管理器客戶端應用程式。從選單導航到**工具>安全管理器 管理** 

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



步驟2.選中Native RBAC Parameters下的框。選擇儲存並關閉

3	Cisco Security Manager - Administration	_ <b>_</b> X
APS     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     Configuration Archive     Configuration Archive     Configuration Archive     Configuration Archive     Control Control     Debug Options     Debug Optins     Debug Options     Debug Options     D	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 Netwe RBAC Parameters W Blow logon for user ide not available in Local User Database	Save Reset Restore Defaults

步驟3.從選單中選擇文件>提交。「檔案」>「提交」。

**附註**:所有更改都必須儲存,以防配置更改需要提交和部署。

步驟4.導覽至CSM Management UI,鍵入<u>https://<enter\_CSM\_IP\_Address</u>,然後選擇Server Administration。



**附註**:第4步至第7步顯示了為ISE中未定義的所有管理員定義預設角色的過程。這些步驟是可 選的。

**步驟5.**驗證身份驗證模式設定為**CiscoWorks Local 並且Online** userID是在CSM上建立的本地管理員 帳戶。

cisco Ciso	co Security Mana	ger						admin Logout About Feedback
								17 Apr 2021, 14:11
ommon Services Z Auto Refresh	Home	Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021
	Security		Beckup			Recent	ly Completed Jobs	
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ki	Job Type	Status	Description	Completed At
Authorization 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
Single Sign-on Mode	Standalone	Recent Backup Status	Not found or unable to detect	1001.1368	SystemCheckUtility SystemCheckUtility	Succeeded	SysCheckTest SysCheckTest	Thu Apr 15 05:00:57 PDT 2021 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	Set Apr 10 05:00:56 PDT 2021
								More
	System Tasks		Inline Users		Management Tasl	ka l		Reports
Local User Setup Mul5-Server Trust Manage Configure Single Sign-On	ment	Number of Online users	¢	Schedule Back Check for Soft Check for Devi	up ware Updates ce Updates		Permission Rep Log File Status Process Status	ho
AAA MODE DAILUP		Online User Id(s)	admin Send Message	Coed Sever	normalion .		System Audit Li	9

步驟6.導覽至Server 並選擇Single-Server Management

ciso	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	,			
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	1			

**步驟7.選**擇Role Management Setup,並選擇所有管理員使用者在身份驗證時獲得的預設許可權。 在本示例中,使用Network Administrator。選中後,選擇**設定為預設值。** 

Home       Server *       Software Center *         Navigator       Browser-Server Security       Role       Management Setup         Local User Policy Setup       Roles       Description       Default Roles         Local User Setup       1.       Approver       Approver Role	cisco Cisco Security Ma	nager	
Navigator       Browser-Server Security       Role Management Setup       Showing 8 records         Local User Policy Setup       Roles       Description       Default Roles         Certificate Setup       1.       Approver       Approver Role       Imagement Setup         2.       Help Desk       Help Desk Role       Imagement Role       Imagement Role       Imagement Role         3.       Network Administrator       Network Operator Role       Imagement	Home Server * Software Center *		
6.     Security Approver     Security Approver Role       7.     Super Admin     Super Admin Role       8.     System Administrator     System Administrator Role	Home Server * Software Center * Navigator Browser-Server Security mode setup Local User Policy Setup Local User Setup Role Management Setup Certificate Setup	Role       Description         1.       Approver         2.       Help Desk         3.       Network Administrator         4.       Network Administrator         5.       Security Administrator         6.       Security Administrator         7.       Super Admin         8.       System Administrator         8.       System Administrator         9.       System Administrator	Showing 8 records Default Roles

**步驟8.選擇Sever>AAA Mode Setup Role**,然後選擇TACACS+選項,最後選擇change以新增ISE資 訊。

uļu cise	Cisco Security Manager
Home	Server  Software Center
Commo Auto R	Security Single-Server Management  Multi-Server Trust Management  Cisco.com Connection Management  AAA Mode Setup
Authorizat Single Sig	Admin 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 S	Security Manager
Home Server V Softwar	e Center ▼
Authentication Mode	Setup
AAA Mode Setup	
Select a Type: ACS O Lo	cal RBAC
Current Login Mode: Local Author	ntication
Available Login Modules	
1 Local Authenticatio	n
2 Local NT System	
3 MS Active Directory	1
4 RADIUS	
5 O TACACS+	
	Change

**步驟9.定**義ISE IP地址和金鑰(可選),您可以選擇允許所有本地身份驗證使用者的選項,或者在 登入失敗時僅允許一個使用者。在本示例中,僅管理員使用者被允許作為回退方法。選擇**確定**以儲 存更改。

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 Authentication login.</li> </ul>	o fallback to the Local
Login fallback options:	<ul> <li>Only allow the following user(s) to fall Authentication login if preceding login fail</li> </ul>	back to the Local ls:
	admin	(comma separated)
	Allow no fallbacks to the Local Auther	ntication login.
		OK Cancel



**步驟10.選擇Server> Single Server Management**,然後選擇Local User Setup並選擇add。

ului cisc	cisco Cisco Security Manager				
Home	Server V Software Center V				
	Security Single-Server Management Multi-Server Trust Management				
Authentica	Cisco.com Connection Management AAA Mode Setup				
Authorizat	Admin Processes				
Single Sig	Backup Log Rotation	2			
	Selftest Notify Users				
	Job Browser Resource Browser				
Local Use Multi-Serv	System Preferences CS Log Configurations				
Configure	DiskWatcher Configuration				

cisco Cisco Security Ma	anager
Home Server * Software Center *	
Navigator	Local User Setup
Browser-Server Security mode setup	Showing 206 records
Local User Policy Setup	Users 4
Local User Setup	1. AeronLogen
Role Management Setup	2. Adrian.Lotrean
	3. Adrian.Richards
	4. ahohenstein
	5. Aida Agular
	6. Alaric Castain
	7. alem.weldehimanot
	8. allen.spiegel
	9. Andrew.OConnor
	10. Anwar Khan
	11. armand.amith
	12. Bernard Alston
	13. bhess
	14. Bit.Mason
	15. bil.nash
	16. Billy Vaughan
	17. 🗇 bpiołnik
	18 Brodier Isrean
	*Select items then take an Import Users Export Users Edit Delete Add Modify My Profile

**步驟11.在**ISE配置部分的第5步中,定義在ISE上建立的相同使用者名稱和密碼,本示例使用 csmoper和Help Desk任務授權角色。選擇OK以儲存管理員使用者。

lsemame:	csmope	r	
Password:			Verify Password:
Email:			
Authorization Type Select an option: Full A	uthorization 🔾	Enable Task Au	thorization C Enable Device Authorization
Roles		Device	level Authorization
Help Desk		Not Ap	plicable
Approver			
Network Operator			
Network Administrato	r		
System Administrator			
Super Admin			
Security Administrato	·		
Security Approver			
<b></b>			

## 驗證

### 思科安全管理器客戶端UI

**步驟1.**開啟新視窗瀏覽器,在ISE配置部分下鍵入<u>https://<enter\_CSM\_IP\_Address</u>,使用 csmadmin在第5步中建立的使用者名稱和密碼。

## ahaha cisco 10.88.243.42 JavaScript: Enabled User ID: csmadmin Cookies: Password: ..... Enabled Login Help Browser: Supported Version **Cisco Security Manager** Copyright(c) 2006 - 2020 Cisco Systems, Inc. All rights reserved.

### 在ISE TACACS即時日誌上可以驗證登入嘗試是否成功

E Cisco ISE			C	perations • TA	CACS		Ivaluation Mode 39 Day	Q	0 73	0
Live Logs										
ට Refresh රා Export To 🗸						Refresh Show Every 3 seconds V Lates	t 20 records 🗸	Within Last 2	3 hours 7 Filter ~	•
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	N	letwork D	evic.
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	,	ietwork De	vice 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	GMT-0500 (C	entral Daylight 1	lime)				Reco	rds Show	m: 1

### 思科安全管理員使用者端應用程式

步驟1.使用服務檯管理員帳戶登入到思科安全管理器客戶端應用程式。

	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.	

### 在ISE TACACS即時日誌上可以驗證登入嘗試是否成功

/e Logs								
Cl. Belenak - di Fanant Ta 🗸						Refresh Every 3 seconds 🗸	Show Latest 20 records v	Within Last 3 hours ↓
C wanted C and a c								1 Failer A. 10-
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic
Logged Time	Status	Details	<b>Identity</b> Identity	Туре	Authentication Policy Justentication Policy	Authorization Policy	Ise Node	Network Devic

**步驟2.**從CSM客戶端應用程式選單中選擇「**工具」>「安全管理**器管理」,將顯示一條錯誤消息 ,指示必須缺少許可權。

•		Gisco Sec	urity	Manager	- Configu	ration N	lanager - cs	moper Connected to	10.88.243.42			- 0 X
File Edit View Policy Map 1 Bulleting International States of the State	Varage Ta ky Sunde	ds Laurch Help Device Properties	0	6 6 6						9	iearch All Categories	cisco
Devkes 💽 😥	Healt	Detect Out Of Band Changes Packet Capture Wizerd Ping TraceRoute and NSLockup			0eg	loyment fait 0 😐	Menager Fending 8 - O	Pasa: 0		Orvice State Octical 3 O Warring 3 O Korr	*1	
8 G Location 8 G Location 8 G Al	() () X 1996	P Intelligence Hel Show Containment	-							Last Upda	e Time: 17 Apr 2021 03 Qr: Type to Search	шармарт   🗗
	2	Inventory Status Catalyst Sommary Info Apply IFS Update		d Alerta B	Connection 0	State 0 0	Deployment Qa O	Additional Information	3P Address 199, 134, 215, 3 199, 139, 219, 3	ricat Donain goul et o vomb 3 unde gov goul et o vomen 3 unde gov	Target 05 Heraton 9.9(2) 9.9(2)	Running 0519 5.9(2)40 5.9(2)40
	94	Preview Configuration Backup		:	:	0	<i>8</i> .		199, 139, 215, 9 199, 139, 215, 10	geziatus volvas filvada ge geziatus volvas filvada ge	v 9.905 v 9.905	5.9(2H0 5.9(2H0
Publies	2 3	Security Manager Diagnetics Security Manager Administration	i	:	:	0	8		199, 139, 215, 4 199, 139, 215, 4	gu2 atus vaste 1 vada gev gu2 atus vaste 2 vada gev	9.9(2) 9.9(2)	9.9(2)40 9.9(2)40
• The service advectage	9 0.0	atus usero Susdeugev 0	0	•	•	0	17 e		199, 129, 210, 5	quil-atur unvan 2 unda gov	9.9(2)	8.9(2)40

1	Error - Insufficient Privileges	×
	You do not have sufficient privileges to perform this operation.	
	Please contact your system administrator and have them grant you additional privileges. If your AAA mode is ACS, privileges are granted via ACS configuration. If your AAA mode is non-ACS, privileges are granted via "CiscoWorks Homepage > Server > Single-Server Management > Local User Setup".	
	OK	

步驟3.使用csmadmin帳戶重複步驟1到3,以驗證已為此使用者提供了正確的許可權。

## 疑難排解

本節提供的資訊用於對組態進行疑難排解。

通過ISE上的TCP轉儲工具進行通訊驗證

步驟1.登入ISE並導航到位於左上角的三行圖示並選擇操作>故障排除>診斷工具。

步驟2. 在**General tools 下,選擇TCP Dumps ,然後選擇Add+。**選擇Hostname 、 Network Interface File Name 、 Repository ,也可以選擇過濾器以僅收集CSM IP地址通訊流**。**選擇**儲存並** 運行

#### Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Downlo	ad Logs Debug Wizard
General Tools $\checkmark$	Add TCP Dump
RADIUS Authentication Troubl Execute Network Device Com	Host Name *
Posture Troubleshooting Agentiess Posture Troublesho EndPoint Debug	Network Interface * GigabitEthernet 0 $\checkmark$ ()
TCP Dump	
Session Trace Tests	Filter ip host 10.88,243,42
TrustSec Tools >	li.
	E.g: ip host 10.77.122.123 and not 10.177.122.119
	Repository VMRepository V
	File Size 100 ©
	Limit to 1 File(s)
	Time Limit 5 0 Minute(s)
	Promiscuous Mode
	Cancel Save and Run

### 步驟3.登入CSM客戶端應用程式或客戶端UI並鍵入管理員憑據。

### 步驟4.在ISE上,選擇停止按鈕並驗證pcap檔案已傳送到定義的儲存庫。

C Refresh	+ Add 🖉	Edit 🛛 📋 Trash 🗸 🕨 Start	$igodot$ Stop $\ \pm$ Download			ΎF	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

SM CSM	_Tshoot.zip (or	nly 20 days left to be	y a licens	e)							-	;
File Co	mmands To	ols Favorites Op	tions He	elp								
Add	Extract To	Test View	Delete	Q Find	Wizard	(i) Info	VirusS	ican Comme	vt	SFX		
Ŷ	CSM_Tsho	oot.zip - ZIP archive	unpacke	d size 1,166 by	tes							
Name	^	Size	Packed	Туре	1	Modified		CRC32				
				File folder								
CSM_	Tshoot.pcap	1,166	556	PCAP File	4	4/17/2021 3	3:29	8A27888D				

### 步驟5.開啟pcap檔案驗證CSM和ISE之間的成功通訊。

Apply a c	lisplay filter			· ··· [30]	
1	and a second second second	<¤/>			Expression
1	Time	Source	Destination	Protocol	Lengt/ Info
	666666	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	8.865688	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	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	8.220350	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	8.311193	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [FIN, ACK] Seq=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	0.400551	10.88.243.42	10.122.112.4	TOP	00 55740 → 49 [FIN, ALK] Seq=70 Ack=47 Win=66048 Len=0
Frame ( Etherne	i: 81 bytes nt II, Src: nt Protocol ission Contr	on wire (648 bits), Vmware_a4:0d:c6 (00 Version 4, Src: 10, rol Protocol, Src Po	, 81 bytes captured (0 0:50:56:a4:0d:c6), Dst 122.112.4, Dst: 10.88 prt: 49, Dst Port: 557	48 bits) : Cisco_1f:21:4 J.243.42 40, Seq: 1, Ack	5 (00:14:6a:1f:21:45) 1: 44, Len: 27
Transm. TACACS		TACACS+			
Transm TACACS- Majo Mino Type Sequ > Flag	r version: r version: : Authentic ence number s: 0x00 (En	0 cation (1) r: 2 hcrypted payload, Mu	ltiple Connections)		
Transm TACACS- Majo Mino Type Sequ Sess	r version: r version: : Authentic ence number s: 0x00 (En ion ID: 381	0 cation (1) r: 2 hcrypted payload, Mu 19957939	ltiple Connections)		
Transm TACACS		TACACS+			

如果在pcap檔案中未顯示任何條目,則驗證以下內容:

- 1. 在ISE節點上啟用裝置管理服務
- 2. 在CSM配置中新增了正確的ISE IP地址
- 3. 如果防火牆位於中間,驗證允許連線埠49(TACACS)。