# CSM TACACS与ISE集成

## 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 背景置 配络图 身份验证过程 ISE配置 CSM配置 验证 批除

## 简介

本文档介绍将思科安全管理器(CSM)与身份服务引擎(ISE)集成的过程,以便管理员用户通过 TACACS+协议进行身份验证。

## 先决条件

#### 要求

Cisco 建议您了解以下主题:

- •思科安全管理器(CSM)。
- •身份服务引擎(ISE)。
- TACACS协议。

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- CSM服务器版本4.22
- ISE版本3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 背景信息

默认情况下,思科安全管理器(CSM)使用称为Ciscoworks的身份验证模式在本地对用户进行身份验

证和授权,以便采用集中式身份验证方法,您可以通过TACACS协议使用思科身份服务引擎。

## 配置

#### 网络图



#### 身份验证过程

步骤1.使用管理员用户的凭证登录CSM应用。

步骤2.身份验证过程触发,ISE在本地或通过Active Directory验证凭证。

步骤3.身份验证成功后,ISE发送允许数据包以授权对CSM的访问。

步骤4. CSM将用户名与本地用户角色分配映射。

步骤5. ISE显示成功的身份验证实时日志。

#### ISE配置

步骤1.选择三行图标 位于左上角,导航至Administration > Network Resources > Network Devices。 ■ Clace ISE Administration - Network Resources

			14011		00		
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					
Device Security Settings	/ Kat + A	dd 🚺 Duplicate 🕁 Import	스 Export 🗸 👌 Generate R/	iC 🔋 Delete 🗸			
	Nam	e 🗠 IP/Mask Profile I	Name Location	Туре	Description		

**步骤2.**选择+Add按钮,为Network Access Device Name和IP Address输入正确的值,然后验证 TACACS Authentication Settings复选框并定义共享密钥。选择"提**交"**按钮。

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 Mar	agement
dentities Groups External Ide	Identity Source Sequences	Settings
Identity Groups	User Identity Groups	
	🖉 Edit 🕂 Add 🍵 Delete 🗸 🕁 Import	▲ Export ∨
<ul> <li>See Endpoint Identity Groups</li> <li>User Identity Groups</li> </ul>	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

步骤4.导航至"用户身份组"文件夹,然后选择+Add按钮。定义名称并选择"提交"按钮。

Identities	Groups	External Ide	ntity Sources	Identity Source Seque	nces Settings		
Identity Gr EQ	oups		User	dentity Groups	6		
< 8	l .	٥				Selected 0 Total 10 💋 🗔	
> 🗖 6	indpoint Identity	y Groups	🖉 Edit 🚽	- Add 🌔 Delete 🗸 🕁	Import 🚯 Export 🖂	all $\sim$	
> 🖻 (	Jser Identity Gro	oups	N	lame	∧ Description		
				ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group		
				CSM Admin			
				CSM Oper			

**注意:**此示例创建CSM Admin和CSM Oper Identity组。您可以对CSM上的每种类型的Admin Users重复步骤4

**步骤5.**选择三行图标 并导航至Administration > Identity Management > Identities。选择 +Add按钮并定义用户名和密码,然后选择用户所属的组。在本示例中,分别创建csmadmin和 csmoper 用户并分别分配给CSM Admin和CSM Oper组。

		Administration - Identity Management
Identities Groups Ex	amal Identity Sources Identity Source Sequences Settings	
	Network Adonas Users Units > considerity	
teet Merael Neberth Scan Res	✓ Network Access User       * name     conadmin       Status        ■ Institut ✓       Status        ■ Institut ✓       Ensit        ■       ✓ Passwords        ■ Ensite ✓       Password        ■ Ensite ✓       *Login Password        ■ Ensite ✓       0x898 Password        ■ Ensite ✓       0x898 Password        ■ Ensite ✓       0x898 Password        ■ Ensite ✓	) o ) o
	User Information     Free Nome     Laschare	
	Account Options Description Charge paeaward in not tage	
	Account Disable Policy     Disable account if data exceeds 2021-06-16 (typy-mit-40)	
	V Liser Groups	

Identities	Groups	External Identit	y Sources	Identity Source Sequences	Settings					
Users Latest Manual Netv	work Scan Res	Netv	work A	ccess Users						
								Selected 0 Total 2	ø	٥
		0 Edit	+ Add	🛞 Change Status \vee 🛛 🕁 Import	🗄 Export 🗸 🛛 🚦 Del	ete 🗸 🔘 Dup	licate	A	• ~	7
			Status	Name ~ Descrip	ption First Name	Last Name	Email Address	User Identity Grou A	d	
		0	Enabled	2 csmadmin				CSM Admin		
		0	Enabled	1 csmoper				CSM Oper		



**步骤6.选**择

并导航至**管理>系统>部署。**选择主机名节点并启用设**备管理服务** 



注意:在分布式部署中,选择处理TACACS请求的PSN节点

**步骤7**.选择三行图标并导航至管理>**设备管理>策略元素。**导航至"**结果">"TACACS命令集"。**选择 +Add按钮,定义命令集的名称,并启用Permit any命令,该命令未列在复选框下。选择 Submit。

≡ Cisco ISE			Work Centers -	Device Administration		A Evaluation Mod	: 39 Days Q 💿		¢
Overview Identiti	es	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More $\vee$		
Conditions	>	TACACS Command Sets Command Set	> New						
Vetwork Conditions	>	Marrie							
Results	~	Permit all		_					
Allowed Protocols									
TACACS Command Sets		Description							
TACACS Profiles				é.					
		Commands							
		00111101100		_					
		Permit any command that	t is not listed below	0					
		+ Add 🔋 Trash 🗸	C Edit Move U	p 💛 Move Down					
		Grant	Command	Arguments					
		No data found.							
								_	

步骤8.选择左上角的三行图标,然后导航至Administration -> Device Administration -> Device

Admin Policy Sets。选择 <sup>1</sup>位于"策略集"标题下,定义名称,**然后选择**中间的+按钮以添加新条 件。

Policy Sets				Reset	Reset Policyset Hite	counts		Save
🕒 Status Polic	icy Set Name	Description	Conditions	Allowed Protocol	s / Server Sequence	Hits	Actions	View
Q Search								
😒 сѕм	Administrators		+	Select from list	~+		   	•
😒 Defa	sult	Tacacs Default policy set		Default Device A	dmin 👁 🖂 +	0	<u>ئې</u>	•

步骤9.在Condition窗口下,选择添加属性,然后选择Network Device Icon,后跟Network access device IP address。 选择Attribute Value并添加CSM IP地址。选择"完成后使用"。

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

#### **步骤10.在"允**许协议"部分下,选择"设**备默认管理"**。选择保存

•	Status	Policy Set Name	Description	Co	nditions	Allowed Protoco	ls / Server Sequence	Hits	Actions	Viev
Q	Search									
	0	CSM 4.22		Ģ	Network Access Device IP Address EQUALS 10.88,243.42	Default Device /	Admin 🛚 🙁 +	0	ŵ	>

"策略集"图标定义身份验证和授权策略

步骤13.选择Internal Users as the Identity Store并选择Save

✓ Auther	enticatio	n Policy (1)					
۲	Status	Rule Name	Con	ditions	Use	Hits	Actions
Q	Search						
					Internal Users	<b>a</b> ~	
	0	CSM Authentication		Network Access-Device IP Address EQUALS 10.88,243.42	> Options		{ĝ}

**注意:**如果ISE加入Active Directory,则身份库可更改为AD库。

**步骤14.选择**位于授权策略标题下,定义名称,**然后选择**中间的+按钮以添加新条件。在"条件"窗口下,选择添加属性,然后选择"身**份组"图标**,后跟"内**部用户:身份组。**选择CSM Admin Group,然后选择**Use**。

		Laitor				
Search by Name			InternalUser-Identity	Group		
• • • • • • • • • •	E C 1 O E 🕈	4	Equals 🗸	User Identity Groups:CSM Admin	×	
EAP-MSCHAPv2	٥		Set to 'Is not'		Duplicate	Save
EAP-TLS	٥			NEW AND OR		
: [] Guest_Flow	٥					
Hetwork_Access_Auther	ntication_					

步骤15.在"命令集"下,选择"允许在步骤7中创建的所有命令集",然后选择"保存"

#### 对CSM操作组重复步骤14和15

V Authorization Policy (3)									
				Results					
🕣 Status	Rule Name	Conditions		Command Sets		Shell Profiles		Hits	Actions
Q Searc	h								
٥	CSM Oper	A InternalUser- Identity Grou	IdentityGroup EQUALS User ps:CSM Oper	Permit all ×	~+	Select from list	~+	0	(2)
٥	CSM. Admin	A InternalUser- Identity Grou	IdentityGroup EQUALS User ps:CSM Admin	$Permit \; all \; \times$	~+	Select from list	~+	0	(2)
٥	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>∞</u> ~+	0	{\$}

#### 步骤 16 (可选)。 选择左上角的三行图标,然后选择

Administration>System>Maintenance>Repository,选择+Add以添加用于存储TCP转储文件以进行 故障排除的存储库。

步骤 17(可选)。 定义存储库名称、协议、服务器名称、路径和凭证。完成后选择"提交"。

De	eployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup	Click here to do visibility setup Do not show this again.
Patci	h Management		Repository List >	Add Repository					
Rep	ository		Repository (	Configuratio	n				
Oper	rational Data Pur	ging	* Repository Na * Protocol Location * Server Name		sitory				
			Credentials * User Name * Password	cisco					

#### CSM配置

步骤1.使用本地管理员帐户登录到Cisco Security Manager客户端应用。从菜单导航到工具>安全管理器管理

	8
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 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.	1)11 CO

File Edit View Policy Map M	Manage	Tools	Launch Help	
Sevice 🔀 Map 🗊 Policy 🖾 Poli	cy Bundle		Device Properties	٥
Devices A S	Davisar	P	Detect Out Of Band Changes	
vevices 🛛	Policy A	1	Packet Capture Wizard	
Filter : none 🗸		1	Ping, TraceRoute and NSLookup	
😪 cpu1-atus-uswas-2.usda.gov 🔥		۱ 😨	P Intelligence	
🔗 cpu1-atus-uswas-91.usda.gov		*	Wall	
cpu1-atus-uswas-92.usda.gov			Show Containment	
cpu2-atus-ussto-3.usda.gov	ſ		nventory Status	
© cpu2-atus-ussfo-3.usda.gov ≡			Catalyst Summary Info	hir
cpu3-atus-uswas-2.usda.gov			Apply IPS Update	
TAC-RECREATE.cisco.com				-11
TAC-RECREATE.cisco.com_adm		∞ !	Preview Configuration	_
C III >		1	Backup	
			Security Manager Diagnostics	•
Policies		20	Security Manager Administration	

步骤2.选中Native RBAC Parameters下的复选框。选择保存并关闭

步骤3.从菜单中选择"文件">"提交"。文件>提交。

**注意:**在配置更改时,必须保存所有更改,这些更改需要提交和部署。

**步骤4.导**航至CSM Management UI并键入<u>https://<enter\_CSM\_IP\_Address,然</u>后选择**Server** Administration。



**注意:**第4步到第7步显示了定义所有未在ISE上定义的管理员的默认角色的过程。这些步骤是 可选的。

**步骤5.验**证身份验证模式设置为CiscoWorks Local,**Online** userID是在CSM上创建的本地管理员帐 户。

Home         Server ★         Software Center ★           Common Services Home         Common Services Home         Last Update:           Auto Retriesh         Venion: 4.2.2         Last Update:           Methodation Mode         CiscoWorks Local         Backup Schedule         Not Scheduled           Undortation Mode         CiscoWorks Local         Backup Schedule         Not Scheduled           Imgle Sign-on Mode         Standaine         Not Scheduled         Not Scheduled           Recent Backup Status         Not found or unable to detect         1001:1326         SystemCheckUBity         Succeeded         SysCheckTest         Fil Apr 16 50:00           1001:1366         SystemCheckUBity         Succeeded         SysCheckTest         Werd Apr 16 05:00           1001:1366         SystemCheckUBity         Succeeded         SysCheckTest         Werd Apr 16 05:00           1001:1366         SystemCheckUBity         Succeeded         SysCheckTest         Werd Apr 10 05:00           1001:1366         SystemCheckUBity         Succeeded         SysCheckTest         Werd Apr 10 05:00	Logout About Feedback I
Common Services Home           Auto Refresh         Version: 42.2         Last Update:           Medication Mode         CasoWorks Local         Disclup Schedule         Not Scheduled         Disclup Schedule         Last Update:         Disclup Schedule         Not Scheduled         Disclup Schedule         Disclup Schedule         Disclup Schedule         Not Scheduled         Disclup Schedule         Disclup Schedule <thdisclup schedule<="" th=""> <thdisclup sched<="" th=""><th></th></thdisclup></thdisclup>	
Common Services Home Version: 4.2.2 Last Update: Auto Refresh Version: 4.2.2 Last Update: Last Update: Last Backup Status Ingle Sign-on Mode Standaine Version: Status Version: 4.2.2 Last Backup Status Version: 4.2.2 Version: 4.2.2 Version: 4.2.2 Last Backup Status Version: 4.2.2 Version: 4.2.2 Version: 4.2.2 Version: 4.2.2 Last Update: 4.2.2 Version: 4.2.2 Versio	17 Apr 2021, 14:11 P
Backer         Backer         Exactly         Last Updated           Muterification Mode         CiscoWorks Load         Not Schedule         Not Schedule         Not Schedule         Description         D	
Becurity         Backup         Backup         Backup         Recently Completed Jobs           Nuthenrication Mode         CiscoWorks Local         Not Schedule         Not Schedule         Job 3d         Job 7pe         Status         Description           Nuthorization Mode         CiscoWorks Local         Last Backup Completed at         Not found or unable to detect         Job 3d         Job 7pe         Status         Description           Ingle Sign on Mode         Stantaione         Recent Backup Status         Not found or unable to detect         1001.1306         System/Check/Jillity         Succeeded         SysCheckTest         The Apr 16 56 001           1001.1366         System/Check/Jillity         Succeeded         SysCheckTest         The Apr 16 56 001           1001.1366         System/Check/Jillity         Succeeded         SysCheckTest         The Apr 13 06:00           1001.1366         System/Check/Jillity         Succeeded         SysCheckTest         Twe Apr 13 06:00	Sat Apr 17 14:11:20 POT 2021 🛞
Backup Schedule         Not Schedule         Job 1d         Job 1d         Job 7pe         Status         Description           Nuthorization Mode         CiscoWorks Local         Last Backup Completed at         Not found or unable to detect         1001.1320         System/CheckUBity         Succeeded         SysCheckTest         File Apr 10 0610           Bingle Sign-on Mode         Status         Not found or unable to detect         1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Tile Apr 15 06 00           Not         Status         Not found or unable to detect         1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Tile Apr 16 06 00:           1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Tile Apr 16 06 00:           1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Wed Apr 14 06:00           1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Wed Apr 13 06:00           1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Tile Apr 13 06:00           1001.1368         System/CheckUBity         Succeeded         SysCheckTest         Tile Apr 13 06:00	
Nuthorization Mode CiscoWorks Local Leat Backup Completed at Not found or unable to detect 1001.1370 SystemCheck/3819 Succeeded SysCheck/Test Set Apr 17 05 05 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Wed Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 16 05 00 1001.1388 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Test Apr 13 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded SysCheck/Test Mod Apr 14 05 00 1001.1386 SystemCheck/3819 Succeeded	Completed At
Nuthorization Mode         CiscoWorks Local         Last Backup Completed at Not found or unable to detect         1001.1369         SystemCheck/UBIty         Succeeded         SystemCheck/UBIty           Single Sign-on Mode         Standatione         Recent Backup Status         Not found or unable to detect         1001.1369         SystemCheck/UBIty         Succeeded         SystCheck/Test         Thu Apr 16 05.00           Under Sign-on Mode         Standatione         Recent Backup Status         Not found or unable to detect         1001.1367         SystemCheck/UBIty         Succeeded         SystCheck/Test         Thu Apr 15 05.00           1001.1367         SystemCheck/UBIty         Succeeded         SystCheck/Test         Wed Apr 14 05.00           1001.1366         SystemCheck/UBIty         Succeeded         SystCheck/Test         Wed Apr 13 05.00           1001.1366         SystemCheck/UBIty         Succeeded         SystCheck/Test         Mon Apr 12 05.00	56 PDT 2021
Bingle Sign-on Mode         Standatione         Thu Apr 15 05:00           Bingle Sign-on Mode         Standatione         SystemCheck/Milly         Successed         SystCheckTest         Thu Apr 15 05:00           1001.1368         SystemCheck/Milly         Successed         SystCheckTest         Web Apr 16:00:00           1001.1366         SystemCheck/Milly         Successeded         SystCheckTest         Web Apr 16:00:00           1001.1366         SystemCheck/Milly         Successeded         SystCheckTest         Web Apr 16:00:00           1001.1366         SystemCheck/Milly         Successeded         SystCheckTest         Web Apr 16:00:00	58 PDT 2021
Recent Backup Status Not Bund or unable to detect 1001.1367 SystemCheck/381y Succeeded SysCheckTest Wed Apr 14 05:0 1001.1368 SystemCheck/381y Succeeded SysCheckTest Tue Apr 13 05:00 1001.1365 SystemCheck/381y Succeeded SysCheckTest Mon Apr 12 05:00	557 PDT 2021
1001.1366 SystemCheckU8ity Succeeded SysCheckTest Tue Apr 13 05 00 1001.1365 SystemCheckU8ity Succeeded SysCheckTest Mon Apr 12 05 00	0.55 PDT 2021
1001.1365 SystemCheckUtility Succeeded SysCheckTest Mon Apr 12 05 00	2:54 PDT 2021
	0.56 PDT 2021
1001.1364 SystemCheckUtility Succeeded SysCheckTest Sun Apr 11 05:00	2:55 PDT 2021
1001.1383 SystemCheckUtility Succeeded SysCheckTest Sat Apr 10 05:00	56 PDT 2021
	Hore
Bystem Tasks Online Usars Management Tasks Report	n .
Local User Setup Permission Report	
Multi-Server Trust Management Log File Status	
Configure Sinde Sign-On Check for Device Updates Process Status	
AAA Mode Setup	
admin	
Online User M(s)	

步骤6.导航至服务器并选择单服务器管理



**步骤7.选**择Role Management Setup并选择所有管理员用户在身份验证时接收的默认权限。在本例 中,使用网络管理员。选中后,选择**set作为默认值。** 

cisco Security Manager				
Home Server   Software Center				
Navigator Browser-Server Security mode setup Local User Policy Setup Local User Setup Role Management Setup Certificate Setup	Roles         1.       Roles         1.       Approver         2.       Help Desk         3.       Network Administrator         4.       Network Administrator         5.       Security Administrator         6.       Security Administrator         7.       Super Admin         8.       System Administrator	Description         Approver Role         Help Desk Role         Network Administrator Role         Security Administrator Role         Security Approver Role         Super Admin Role         System Administrator Role	Showing 8 records Default Roles	
	Add Edit Delete Copy   Expo	t Import I Set as default Clear default		

**步骤8.选**择服**务器> AAA模式设置角**色,然后**选择TACACS+**选项,最后选**择更改**以添加ISE信息。

uļu cisc	Cisco Security Manager	
Home	Server  Software Center	
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	
	System Preferences	
Local Use	CS Log Configurations	
Multi-Serv	DiskWatcher Configuration	
Configure		

ului cisc	<ul> <li>Cisco Security Manager</li> </ul>
Home	Server V Software Center V
Authent	ication Mode Setup
AAA Mode	9 Setup
Select a T	ype: ACS O Local RBAC
Current Lo	oin Mode: Local Authentication
Available	e Login Modules
10	Local Authentication
2 (	Local NT System
3 (	MS Active Directory
4 0	RADIUS
5 0	TACACS+
	Change

**步骤9.定**义ISE IP地址和密钥,或者,您可以选择允许所有本地身份验证用户或仅允许一个用户登 录失败的选项。在本例中,仅允许管理员用户作为回退方法。选择**确定**以保存更改。

Login Module Options		
Selected Login Module: Description:	TACACS+ Cisco Prime TACACS+ login module	
Server:	10.122.112.4	
Port:	49	
SecondaryServer:		
SecondaryPort:	49	
TertiaryServer:		
TertiaryPort:	49	
Key:		
Debug:	<ul> <li>True • False</li> <li>Allow all Local Authentication users to fallback to the Local Authentication login.</li> </ul>	al
Login fallback options:	<ul> <li>Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails:</li> </ul>	
	admin (comma separat	led)
	Allow no fallbacks to the Local Authentication login.	
	OK Canc	el

Login Module Change Summary	
Login Module changes updated.	
OK	

**步骤10.选**择Server> Single Server Management,**然**后选择Local User Setup并选择Add。

ululu cisco	Cisco Security Manager	
Home Se	rver <ul> <li>Software Center </li> </ul>	
Commo	Single-Server Management	
Auto R	Multi-Server Trust Management	
	Cisco.com Connection Management	
Authoptics	AAA Mode Setup	
Addienoca		
Authorizat	Admin	د
Single Sig	Processes	
Single Sig	Backup	2
	Log Rotation	
	Collect Server information	
	Selftest	
	Notify Users	
	Job Browser	
	Resource Browser	
	System Preferences	
Local Use	CS Log Configurations	
Multi-Serv	DiskWatcher Configuration	
Configure		
AAA Mada Sal	10	11

cisco Cisco Security I	Manager	
Home Server * Software Center *		
Navigator	Local User Setup	
Browser-Server Security mode setup		howing 206 records
Local User Policy Setup		
Local User Setup	1. O Amontogen	_
Certificate Setup	Z. Adhan.Lotean	
	3. Adren.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 Alaton	
	13. Dhess	
	14. DBILMason	
	15. bill.nash	
	16. Billy Vaughan	
	17. 🗋 bgilotnik	
	18 Bruffer Ianzan	
	*Select items then take an import Users Export Users Edit Delete Add M	odiły My Profile

**步骤11.在**ISE配置部分下定义步骤5中ISE上创建的相同用户名和密码,**csmoper**和**帮助台任务授**权 角色在本示例中使用。选择OK以保存管理员用户。

	csmoper			
assword:			Verify Password:	
mail:				
uthorization Type				
elect an option: Full	Authorization 💿 Ena	able Task Au	thorization C Enable Device Auth	norization
Roles		Device	level Authorization	
Help Desk		Not Ap	plicable	
Approver				
Network Operator				
Network Administrate	~			
Sustem Administrator				
System Administrator				
Super Admin				
Security Administrato	or 🖉			
Security Approver				

## 验证

#### 思科安全管理器客户端UI

**步骤1.**打开新窗口浏览器并键入<u>https://<enter\_CSM\_IP\_Address</u>,使用**csmadmin**用户名和密码在步 骤5中在ISE配置部分下创建。

## 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实时日志上验证尝试中的成功日志

E Cisco ISE			0	perations • TA	CACS		Evaluation Mode 39 Days	0 0 2	0
Live Logs									
ට Refresh ්රා Export To 🗸						Refresh Show Every 3 seconds V Late	est 20 records 🗸	Within Last 3 hours	× × 0
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network	Devic.
×		~	Identity		Authentication Policy	Authorization Policy	ise Node	Network D	evice N
Apr 17, 2021 02:34:54.1			csmadmin	Authentic	CSM 4.22 >> Default		ise30	C5M422	
Last Updated: Sat Apr 17 202	09:37:58 0	GMT-0500 (C	entral Daylight T	ime)				Records Sho	wn: 1

#### 思科安全管理器客户端应用

步骤1.使用帮助台管理员帐户登录到Cisco Security Manager客户端应用。

	Cisco Security Manager Version 4.22.0 Service Pack 1
	Server Name 10.88.243.42 V Username csmoper Password ••••••
© 2020 Cisco Systems, Inc. Cisco, Cisco Syste Its affiliates in the U.S. and certain other count	Default View Configuration Manager

#### 在ISE TACACS实时日志上验证尝试中的成功日志

e Logs								
Cl. Burlands - A. Francet To S						Refresh Every 3 seconds 🗸	Show Latest 20 records v	Within Last 3 hours
C wenter C export to 4								A human A 10
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic
Logged Time	Status	Details	<b>Identity</b>	Туре	Authentication Policy Justhentication Policy	Authorization Policy	Ise Node	Network Device

**步骤2.从**CSM客户端应用程序菜单中选择**Tools > Security Manager Administration**,必须显示一条 错误消息,指示权限不足。

•			Cisco Ser	curity	Manager	- Configu	ration N	fanager - cs	moper Connected to	10.88.243.42			- 0 X
File Edit View Policy Map	Manage	144	s Launch Help										ababa
🔒 Device 🗵 Neo 🔅 Policy 🔗 Po	icy Bunde		Device Properties	1	16 🖲 E	1 🔒 🗞 i	6 0				9	Search All Categories	CISCO.
Devices 💽 🗑	Healt	1	Packet Capture Wizard	- 6		Dep	loyment	Heneger			Device State		
Piter: -rone - v	00		Fing Tracellaste and NiLookup				fait ti 😐	Fending 5 0	Pasa: 0		O Critical D O Warning D O No	rmai B	
er die Lectrice 10 de Lectrice 10 de Al	0 a	ž	Pinteligence Wal Show Containment								LastUp	lete Time: 17 Apr 2021 03	LII PH POT
	N 789				Q: from to Search								
	Dag		inventory Status	1.1	ed Alerta	Connection	State	Deployment	Additional Information	3P Address	Host.Donain	Target 05 Version	Running OS 18
	2	5	Catalyst Summary Info	- 1	•			· · · ·		199, 134, 215, 3	grub-etus-usefe-3 usda.gr	v 9.9(2)	9.9(2)40
	8		Apply PS Update		•			- 6°		199, 139, 219, 3	cost etus varvas 2 xada g	w 9.900	9.9(2)40
	2	-4	Preview Configuration	- 1	•		0	· · · · ·		199, 139, 210, 9	geb alus vavas #Lusia.	prv 9.905	9.9(2)40
	9	10	Backup	-			0	- G •		199, 139, 213, 30	gebalus useas 42 usla.	prv 9.900	9-9(2)40
	2		Security Manager Diagnostics		•		0	Q. 0		199, 134, 215, 4	què etus varle-busda ge	v 9.900	9.9(2)40
Publics	2	14	Security Manager Administration		۰		0	0.0		199, 129, 213, 4	quid also verses il velle g	w 9.905	9.9(2)40
-      no device adected -	9	0131	rus-usefo-3-usela-gev 0	0	•		0	Q. 0		199, 134, 215, 5	qui eta orte-bata p	9.9(2)	8.9(2)40
	9	0.0	Aus-uswas-2 usela-gav 0	0	•		0	Q. 0		199, 139, 210, 5	qui-sta-unvar-Lucia.g	w 9.9(2)	8.9(2)40

1	Error - Insufficient Privileges	k
	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".	Î
	OK	

步骤3.使用csmadmin帐户重复步骤1到步骤3,以验证是否向此用户提供了适当的权限。

## 故障排除

本节提供可用于排除配置故障的信息。

在ISE上使用TCP转储工具进行通信验证

步骤1.登录ISE并导航至左上角的三行图标,然后选择"操作">"故障排除">"诊断工具"。

**步骤2.在"**常规**工具"**下,选**择"TCP转**储",然后**选择"添加+"。**选择Hostname、Network Interface File Name、Repository和过滤器(可选),以仅收集CSM IP地址通信流。选择**保存并运行** 

#### Clsco ISE

Operations · Troubleshoot

Alter A	Diagnostic Tools Downle	load Logs Debug Wizard
Add Advected for the Network Over Control of the Interform of the Interfor	General Tools 🗸 🗸	Add TCP Dump
Decket Nationalization         Patrices Stratus Nationalization         Decket Nationalization         Torbinalization	RADIUS Authentication TroubI	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
Partners   Ausress Partner Troublekaboring   Ausress Partner Troublekaboring   Torbing   Station Trace Tests     Partner   Station Trace Tests     Station Tests     Station Tests     Station Tests <td>Execute Network Device Com</td> <td>Kinst Name *</td>	Execute Network Device Com	Kinst Name *
Partice Tools       Image: Control Tools         To Poor       Image: Control Tool Tool Tool Tool Tool Tool Tool T	Evaluate Configuration Validat	ise30 V
Appenders Protuine Transcription   Torbinon   Torbinon </td <td>Posture Troubleshooting</td> <td></td>	Posture Troubleshooting	
Turbled Dates         Call Statistication           Tor Dure         Ggab Statistication           Season There Tests         Par           TextStee Tests         Call Statistication           Far         Call Statistication           Eg: to host 10.85.243.42         Call Statistication           Eg: to host 10.77.122.123 and not         Call Statistication           10.77.122.123 and not         Call Statistication           10.77.122.119         File State           File State         Coll State           10.77.122.123 and not         Call State           10.77.122.119         File State           File State         Call State           10.77.122.119         Call State           File State         Call State           10.77.122.119         Call State           File State         Call State           10.77.122.119         Call State           11.77.122.119         Call State           11.77.122.119         Call State           11.77.122.119         Call State	Agentiess Posture Troublesho	Material Interface.
Tore Trees         Treatise Tools         Face         ()         E::::::::::::::::::::::::::::::::::::	EndPoint Debug	GigabitEthernet 0 V O
Trace Tests         Testine Toin             Image:	TCP Dump	
Treatise Tools               File	Session Trace Tests	
Trustilee Tools     Image input 10.000.xels.ex     Image input 10.0		Filter
Eq: (p host 10.77.122.123 and not Eq: (p host 10.77.122.123 and not Eq: (p host 10.77.122.123 and not Ed: (SM_Tinhoo)	TrustSec Tools	D HORT IN OUTS AT AT
Eg: (p host 10.77.122.123 and not 10.177.122.119 File Name CSM_Tshoot Providency VMRepository CSM_Tshoot Providence CSM_Tshoot CSM_Tshoot Providence CSM_Tshoot Providence CSM_Tshoot Providence CSM_Tshoot Providence CSM_Tshoot Providence CSM_Tshoot Providence CSM_Tshoot Providence Providence CSM_Tshoot Providence Pr	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	h.
File Name         CSM_Tabloot         Recository         VMRepository         File Sare         100       Image         Mb         Limit to         1       Image         File(s)         File(s)         Minuta(s)         Image       Image         I		E.g: ip host 10.77.122.123 and not 10.177.122.119
Fie Name CSM_Tishool Repository VMRepository 0 Fie Size 10 0 M 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 Fie Size 10 0 0 0 0 0 0 0 0 0 0 0 0 0		TWO TY FINAL TOP
CSM_Tshoot Recository VMRepository • • • File Size 100 • • Mb Limit to 1 • • File(s) File(s) Time Limit 5 • • Minute(s) Minute(s) • • • •		File Name
Reconitory       Image: Constrained of the second of the sec		CSM_Tshoot
Recository       Image: Carcel         File Size       Image: Carcel         100       Image: Carcel         110       Image: Carcel		
VMRepository       Image: Save and Run         File Size       Image: Save and Run         100       Image: Save and Run		Reportiony
File Size 100 0 Mb 1 1 1 1 1 1 1 1 1 1 1 1 1		VMRepository V 0
File Size       Image: Constraint of the second of the secon		
Fie Size 100 Mb Limit to 1 Fie(s) Fie(s) Time Limit 5 Minute(s) Promiscuous Mode Cancel Save Save and Run		
Limit to 1 Diffection Time Limit 5 Minute(s) Promiscuous Mode Cancel Save Save and Run		File Size
Limit to 1		Mb
Limit to 1		
1 0 File(s) Time Limit 5 0 Minute(s) Promiscuous Mode Cancel Save Save and Run		Limit to
File(s) Time Limit 5 0 Minute(s) Promiscuous Mode Cencel Save Save and Run		1 0 0
Time Limit 5 0 Minute(s) Promiscuous Mode Cancel Save Save and Run		File(s)
Time Linit 5 Minute(s) Promiscuous Mode Cancel Save Save and Run		
Minute(s)  Promiscuous Mode  Cancel Save Save and Run		Time Linit 5 0
Promiscuous Mode  Cancel Save and Run		Minute(s)
Cancel Save and Run		Development Moda
Cancel Save and Run		
Cancel Save and Run		
		Cancel Save and Ru

#### 步骤3.登录CSM客户端应用或客户端UI并键入管理员凭证。

### 步骤4.在ISE上,选择Stop按钮并验证pcap文件是否已发送到定义的存储库。

C Refresh	+ Add 🖉 Edit	🔋 Trash 🗸 🕨 Start 🛛 🖂	Stop 🕘 Download			γr	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	uy a licens	e)					-	3
File Co	mmands Too	ols Favorites Op	tions H	elp						
Add	Extract To	Test View	Delete	Q Find	Wizard	Info Viru	Scan Commer	t SFX		
1	CSM_Tsho	oot.zip - ZIP archive	, unpacke	d size 1,166 b	ytes					
Name	^	Size	Packed	Туре		Modified	CRC32			
				File folder						
CSM.	Tshoot.pcap	1,166	556	PCAP File		4/17/2021 3:29	. 8A27888D			

#### 步骤5.打开pcap文件以验证CSM和ISE之间的成功通信。

••	•				CSM_Tshoot.pcap	
	<b>1</b>	ڭ 🕺 🗋 🚞	९ 🗰 🗯 🚞	Ŧ 🛓 🗔	📃 Q Q Q II	
App	ly a display filter .	<¤/>			📑 🔹 Expres	sion +
No.	Time	Source	Destination	Protocol	Length Info	
<b>r</b>	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=1	28
	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 0.101362	10.122.112.4	10.88.243.42	TACACCA	54 49 - 55/40 (ALK) Seq=1 ACK=44 W1n=29312 Len=0	
-	0 0.10/105	10.122.112.4	10.00.243.42	TALALS+	60 SS740 - 40 [ACK] Section Ack-20 Wig-SE040 Lecto	
	8 8.228358	10.88.243.42	10.122.112.4	TACACS+	88 D: Authentication	
	9 8,259963	10.122.112.4	10.88.243.42	TCP	54 49 → 55748 [ACK] Seg=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 0.400651	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	
> Erz	me 6: 81 byte:	s on wire (648 bits).	. 81 bytes captured (6	48 bits)	1	
Eth	ernet II, Src:	: Vmware_a4:0d:c6 (00	0:50:56:a4:0d:c6), Dst	: Cisco_1f:21:4	15 (00:14:6a:1f:21:45)	
> Int	ernet Protocol	l Version 4, Src: 10.	122.112.4, Dst: 10.88	.243.42		
> Tra	nsmission Cont ACS+	trol Protocol, Src Po	ort: 49, Dst Port: 557	40, Seq: 1, Ack	k: 44, Len: 27	
1	Major version:	TACACS+				
1	Minor version:	0				
	Type: Authenti	ication (1)				
	Sequence numbe	r: 2				
> 1	Flags: 0x00 (E	incrypted payload, Mu	ltiple Connections)			
	Session ID: 38	19957939				
6666	00 14 6a 1f	21 45 00 50 56 a4 0	d c6 88 88 45 88 ···	1 · ! E · P V · · · · · E		
0 7	CSM Tablet ec	10			Packets: 14 - Displayed: 14 (100.0%)	ofile: Default
-	eang should be				a montrer par a publicitation par (starte pa)	

如果pcap文件上未显示任何条目,请验证以下内容:

1. 设备管理服务在ISE节点上启用

2. CSM配置中已添加正确的ISE IP地址

3. 如果防火墙位于中间,请验证端口49(TACACS)是否允许。