CSM TACACS-Integration mit ISE

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfiguration Netzwerkdiagramm Authentifizierungsverfahren ISE-Konfiguration CSM-Konfiguration Überprüfung Fehlerbehebung

Einführung

In diesem Dokument wird das Verfahren zur Integration von Cisco Security Manager (CSM) in Identity Services Engine (ISE) für die Authentifizierung von Administratoren-Benutzern mit dem TACACS+-Protokoll beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CSM-Server, Version 4.22
- ISE Version 3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Standardmäßig verwendet der Cisco Security Manager (CSM) einen Authentifizierungsmodus namens CiscoWorks, um Benutzer lokal zu authentifizieren und zu autorisieren. Um über eine zentralisierte Authentifizierungsmethode zu verfügen, können Sie die Cisco Identity Service Engine über das TACACS-Protokoll verwenden.

Konfiguration

Netzwerkdiagramm



Authentifizierungsverfahren

Schritt 1: Melden Sie sich mit den Anmeldeinformationen des Admin-Benutzers bei der CSM-Anwendung an.

Schritt 2: Authentifizierungsprozess-Trigger und die ISE validiert die Anmeldeinformationen lokal oder über Active Directory.

Schritt 3: Sobald die Authentifizierung erfolgreich war, sendet die ISE ein Genehmigungspaket, um den Zugriff auf den CSM zu autorisieren.

Schritt 4: Der CSM ordnet den Benutzernamen der lokalen Benutzerrollenzuweisung zu.

Schritt 5: Die ISE zeigt ein erfolgreiches Authentifizierungs-Live-Protokoll an.

ISE-Konfiguration

Schritt 1: Wählen Sie das Symbol für drei LeitungenNavigieren Sie in der linken oberenEcke zu Administration > Network Resources > Network Devices (Verwaltung >Netzwerkressourcen > Netzwerkgeräte).

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	k Devices							
	/ Lot + A	6d Duplicate 🕁 Import e 🗠 IP/Mask Profile N	the Export → A Generate PA	C Delete V Type	Description				

Schritt 2: Wählen Sie die Schaltfläche +Hinzufügen, und geben Sie die korrekten Werte für den Namen und die IP-Adresse des Netzwerkzugriffsgeräts ein. Aktivieren Sie anschließend das Kontrollkästchen TACACS Authentication Settings (TACACS-Authentifizierungseinstellungen), und definieren Sie einen gemeinsamen geheimen Schlüssel. Wählen Sie die Schaltfläche Senden.

Network Devices No	twork Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC	Managers E	idemal MOM Location Services
Network Devices	Notwork Devices Link 3: New Network Device		
Default Device Device Security Settings	Network Devices * Name CDM422 Description		
	Nework Device Group Loceion Al Locations Set To Deflawit #10C Is #950C Device Set To Deflawit Device Note Al Device Types Set To Deflawit V RADIUS Authentication Settings V TACACS Authentication Settings Device Snape Covers Male		
	Inducts Drat Compared Single Connect Support SNMP Settings Advanced TrustSec Settings		
			Submit Cancel
		=	
chritt 3: W	ählen Sie das Symbol für drei Leitungen		Navigieren Sie in der linken oberen

Ecke zu Administration > Identity Management > Groups (Verwaltung > Identitätsverwaltung > Gruppen).

Cisco ISE	Administration - Identity Management					
antities Groups External Iden	tity Sources Identity Source Sequences	Settings				
Identity Groups EQ < 20 Control Contro	User Identity Groups					
> C Endpoint Identity Groups	🖉 Edit 🕂 Add 👔 Delete 🗸 🕁 Import	▲ Export ∨				
> User Identity Groups	Name	Description				
	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group				
	C A 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				
	SOWN ACCOUNTS (default)	Default OWN ACCOUNTS (default) User Group				

Schritt 4: Navigieren Sie zum Ordner Benutzeridentitätsgruppen, und wählen Sie die Schaltfläche +Hinzufügen aus. Definieren Sie einen Namen, und wählen Sie die Schaltfläche Senden.

Identities	Groups	External Ide	ntity Sources	Identity Source Sequer	nces Settings			
Identity Gr EQ	oups		User lo	lentity Groups	5			
< 18	8	٥					Selected 0 Total 10 🔗	٢
> 🗖 E	Indpoint Identi	ty Groups	🖉 Edit 🛛 🕂	Add 🏮 Delete 🗸 🕁	j Import 🔥 Export 🖂		ai \sim	V
> 🗖 (Jser Identity G	roups	Na	me	∧ Description			
			0 4	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default)	User Group		
			0 🐇	CSM Admin				
			0 🐇	CSM Oper				

Hinweis: In diesem Beispiel werden Gruppen für CSM-Admin und CSM-Oper-Identität erstellt. Sie können Schritt 4 für jeden Administratorbenutzer-Typ im CSM wiederholen.

Schritt 5: Wählen Sie das Symbol für drei Leitungen und navigieren Sie zu Administration > Identity Management >Identities. Wählen Sie die Schaltfläche +Hinzufügen, legen Sie Benutzername und Kennwort fest, und wählen Sie dann die Gruppe aus, der der Benutzer angehört. In diesem Beispiel werden die csmadmin- und csmoper-Benutzer erstellt und jeweils CSM Admin- bzw. CSM Oper-Gruppe zugewiesen.

lentities Groups Ext	amal identity Sources Identity Source Sequences Settings	
	Network Access Dama Cet 5: considers	
Mercul Network Scen Res		
	✓ Network Access User	
	Tares considerin	
	Status 🖸 Drobled 🗸	
	Enal	
	✓ Passwords	
	And and have a second stars of the	
	Passad Tge Interactions V	
	Password Re-Errar Password	
	*Logit Password ······ Generate Password	0
	Committee	~
		0
	V User Information	
	First North	
	LastAure	
	V Account Options	
	Description d	
	Charge paerward on hext login	
	 Account Disable Policy 	
	Onable account # data acceeds 2021-06-16 (symp-mm-dd)	
	V User Groups	
	E CSW Admin v - +	

Identities Gr	roups Ext	ernal Identity Sourc	es Identity Source Sequences	Settings			
Users Latest Manual Network S	Scan Res	Network	Access Users				
						Selected 0 Total 2 🧭	۲
		🖉 Edit 🕂 Ada	🛞 Change Status \vee 🛛 🕁 Import	🚯 Export \vee 🛛 🚦 Delete	✓ Duplicate	All V	Y
		Statue	Name	ption First Name I	Last Name Email Address	User Identity Grou Ad	
		🗌 🗧 Enal	led 1 csmadmin			CSM Admin	
		🗌 🗧 Enal	led 1 csmoper			CSM Oper	

Schritt 6: Auswählenund navigieren Sie zu Administration > System > Deployment.Wählen Sie den Hostnamen-Knoten aus, und aktivieren Sie den Device Admin Service.



Hinweis: Im Fall einer verteilten Bereitstellung wählen Sie den PSN-Knoten aus, der TACACS-Anforderungen behandelt.

Schritt 7: Wählen Sie das Symbol für drei Zeilen aus, und navigieren Sie zu Administration > Device Administration > Policy Elements (Verwaltung > Geräteverwaltung > Richtlinienelemente). Navigieren Sie zu Ergebnisse > TACACS-Befehlssätze. Wählen Sie +Schaltfläche hinzufügen, definieren Sie einen Namen für den Befehlssatz, und aktivieren Sie den Befehl Zulassen für alle Befehle, die nicht unter dem Kontrollkästchen aufgeführt sind. Wählen Sie Senden aus.

E CISCO ISE			work Centers -	Device Administration			and a c	200	φ
Overview Identiti	es	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More \sim		
onditions	>	TACACS Command Sets Command Set	> New						
etwork Conditions	>	Maria							
esults	~	Permit all							
Allowed Protocols									
TACACS Command Sets		Description							
TACACS Profiles									
		Commands							
		Permit any command that	t is not listed below	•					
		+ Add 🛛 Trash 🗸	🖉 Edit 🔷 Move Up	o 💛 Move Down					
		Grant	Command	Arguments					
		No data found.							
								_	_

Schritt 8: Wählen Sie in der linken oberen Ecke das Symbol für drei Zeilen aus, und navigieren Sie zu Administration (Verwaltung) > Device Administration (Geräteverwaltung) > Device Admin Policy

Sets (Geräte-Admin-Richtliniensätze). Auswählen unter "Policy Sets title" (Titel für Richtliniensätze) einen Namen definieren und die +Schaltfläche in der Mitte auswählen, um eine neue Bedingung hinzuzufügen.

Policy	Sets				Reset Reset Policyset Hitcounts	ave
۲	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions	View
Q	Search					\supset
	۰	CSM Administrators		+	Select from list \sim +	>
	۰	Default	Tacacs Default policy set		Default Device Admin 🛛 🗠 + o 🎊	•

Schritt 9: Wählen Sie im Fenster Bedingung die Option Attribut hinzufügen aus, und wählen Sie dann Netzwerkgerät-Symbol gefolgt von der IP-Adresse des Netzwerkzugriffsgeräts aus. Wählen Sie Attributwert aus, und fügen Sie die CSM-IP-Adresse hinzu. Wählen Sie Nach Beendigung verwenden aus.

Conditions Studio						
Library	Editor					
Search by Name	Ģ	Network Access-D	evice IP Address	5		8
		Equals 🧹	10.88.243.	42		
No conditions found - reset filters.		Set to 'Is not'			Duplicate	Save
			NEW	AND OR		
					Close	Use

Schritt 10: Wählen Sie im Abschnitt Zulassen von Protokollen die Option Gerätestandardadministrator aus. Wählen Sie Speichern

Policy Sets					Reset	Reset Policyset Hit	tcounts		Save
🔶 Status	Policy Set Name	Description	Con	ditions	Allowed Protoco	ls / Server Sequence	Hits	Actions	View
Q Search									
۲	CSM 4.22		ę	Network Access-Device IP Address EQUALS 10.88.243.42	Default Device	Admin 🛛 🗠 +	0	ŝ	>

Schritt 11: Wählen Sie den Pfeil nach rechts aus Authentifizierungs- und Autorisierungsrichtlinien

Symbol des Policy Set zum Definieren von

Schritt 12: Auswählen unter dem Titel der Authentifizierungsrichtlinie einen Namen definieren und in der Mitte das + auswählen, um eine neue Bedingung hinzuzufügen. Wählen Sie im Fenster Bedingung die Option Attribut hinzufügen aus, und wählen Sie dann Netzwerkgerät-Symbol gefolgt von der IP-Adresse des Netzwerkzugriffsgeräts aus. Wählen Sie Attributwert aus, und fügen Sie die CSM-IP-Adresse hinzu. Wählen Sie Nach Beendigung verwenden aus

Schritt 13: Wählen Sie Interne Benutzer als Identitätsspeicher aus, und wählen Sie Speichern aus.

∨ Authen/	tication	n Policy (1)					
🕣 S	tatus	Rule Name	c	onditions	Use	Hits	Actions
Q	Search						
					Internal Users \odot \checkmark		
	0	CSM Authentication	5	2 Network Access-Device IP Address EQUALS 10.88.243.42	> Options		₹ĝ}

Hinweis: Der Identitätsspeicher kann in einen AD-Speicher geändert werden, wenn die ISE einem Active Directory hinzugefügt wird.

Schritt 14: Auswählen definieren Sie unter dem Titel der Autorisierungsrichtlinie einen Namen, und wählen Sie in der Mitte die +-Schaltfläche aus, um eine neue Bedingung hinzuzufügen. Wählen Sie im Fenster Bedingung die Option Attribut hinzufügen aus, und wählen Sie dann das Identitätsgruppensymbol gefolgt von Interner Benutzer aus: Identitätsgruppe. Wählen Sie die CSM-Administratorgruppe aus, und wählen Sie Verwenden aus.

ibrary		Editor					0
Search by Name			InternalUser-Identity	Group			
• III () * 0 F I I ()	8 0 1 0 t 🕈	4	Equals 🗸	User Identity	Groups:CSM Admin +		ш
EAP-MSCHAPv2	o		Set to 'Is not'			Duplicate	Save
🗄 📑 EAP-TLS	٥			NEW AI	ND OR		
Guest_Flow	٥						
B Network_Access_Authent	lication_ ()						

Schritt 15: Wählen Sie unter "Befehlssatz" die Option Gesamten in Schritt 7 erstellten Befehlssatz zulassen aus, und wählen Sie dann Speichern aus.

Wiederholen Sie die Schritte 14 und 15 für die Gruppe CSM Oper.

V Authoriz	ation	Policy (3)								
					Results					
🕒 Sta	atus	Rule Name	c	onditions	Command Sets		Shell Profiles		Hits	Actions
Q s	earch									
	•	CSM Oper	۶	8. InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all ×	~+	Select from list	~+	0	ŵ
	•	CSM. Admin	۶	8. InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$\text{Permit all} \times$	~+	Select from list	~+	0	(2)
	•	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>a</u> ~+	0	(2)

Schritt 16 (optional). Wählen Sie in der linken oberen Ecke drei Zeilen-Symbol aus, und wählen Sie Administration > System>Maintenance>Repository aus, wählen Sie +Add, um ein Repository hinzuzufügen, das zum Speichern von TCP-Dump-Dateien für die Fehlerbehebung verwendet wird.

Schritt 17 (optional). Definieren Sie einen Projektnamen, ein Protokoll, einen Servernamen, einen Pfad und Anmeldeinformationen. Wählen Sie abschließend **Senden** aus.

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

CSM-Konfiguration

Schritt 1: Melden Sie sich mit dem lokalen Administratorkonto bei der Cisco Security Manager Client-Anwendung an. Navigieren Sie im Menü zu **Extras > Sicherheitsmanager-Verwaltung.**

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



Schritt 2: Aktivieren Sie das Kontrollkästchen unter Native RBAC Parameters. Wählen Sie Speichern und Schließen

5	Cisco Security Manager - Administration	_ _ ×
API AVS AUSLIN AUSLIN AUSLIN AUSLIN AUSLIN COS Setings COS Setings Configuration Archive CS-MARS CSM Moble Customize Desktop Debug Options Debug Options Device Communication Rule Exercision Taile Over User Section	Server Security Use the bottoms below to cross launch the Server Security Tools within Common Services. AAA Setup Certificate Setup Single Sign On Local User Setup System Identity Setup Notive RBAC Parameters Biotive RBAC Parameters Biotive RBA	Save Reset Restore Defaults

Schritt 3: Wählen Sie im Menü Datei > Senden aus. Datei > Senden.

Hinweis: Alle Änderungen müssen gespeichert werden, falls Konfigurationsänderungen erforderlich sind.

Schritt 4: Navigieren Sie zu CSM Management UI, geben Sie <u>https://<enter_CSM_IP_Address ein,</u> und wählen Sie Server Administration aus.



Hinweis: Die Schritte 4 bis 7 zeigen die Prozedur zur Definition der Standardrolle für alle Administratoren, die nicht auf der ISE definiert sind. Diese Schritte sind optional.

Schritt 5: Validieren Sie, ob der Authentifizierungsmodus auf CiscoWorks Local (Lokal) und Online-BenutzerID (Online-Benutzer-ID) festgelegt ist, ist das lokale Administratorkonto, das auf CSM erstellt wurde.

cisco Cis	co Security Mana	ger						admin Logout About Feedback
Home Server # 1	Software Center •							
								17 Apr 2021, 14
Common Services	Home							
Auto Refresh	, nome	Version: 4.2.2						Last Undated: Sat Apr 17 14:11:20 PDT 2021
	Security		Beckup			Recent	ly Completed Jobs	
Automatication Made	Cincellinden Local	Backup Schedule	Not Scheduled	Job k5	Job Type	Status	Description	Completed At
	COLUMN COLO			1001,1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
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
lippie Size on Made	Electricity			1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
ingle sign on wood	00000	Recent Backup Status	Not found or unable to detect	1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sal Apr 10 05:00:56 PDT 2021
								More.
	System Taska		Inline Users		Management Tax	ka l		Reports
ocal User Setup				Schedule Back	kup		Permission Rep	tox
Multi-Server Trust Management Configure Single Sign-On		Number of Online users		Check for Soft	ware Updates		Log File Status	
		Handa of Crime and F		Check for Dev	ice Updates		Process Status	Status Compared At 41 Stat Apr 17 05 015 59 PDT 2021 42 Pri Apr 16 05:05 29 PDT 2021 43 Thu Apr 15 05:05 39 PDT 2021 44 Wind Apr 16 05:05 29 PDT 2021 45 Ture Apr 13 05:00 54 PDT 2021 46 Mon Apr 12 05:00 54 PDT 2021 41 Bun Apr 13 05:00 56 PDT 2021 42 Stat Apr 10 05:00 56 PDT 2021 43 Bun Apr 10 05:00 56 PDT 2021 44 Stat Apr 10 05:00 56 PDT 2021 45 Stat Apr 10 50:00 56 PDT 2021 46 Stat Apr 10 50:00 56 PDT 2021 47 Stat Apr 10 50:00 56 PDT 2021 48 Stat Apr 10 50:00 56 PDT 2021 49 Stat Apr 10 50:00 56 PDT 2021
VAA Mode Setup				Collect Server Information System		System Audit L		
			admin					
		Online User k8(s)	Send Message					

Schritt 6: Navigieren Sie zu Server, und wählen Sie Einzelserver-Management aus.

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	,				
Single Sig	Processes Backup	,				
	Log Rotation					
	Collect Server information					
	Selftest					
	Notify Users					
	Job Browser					
	Resource Browser					
Local Lieo	System Preferences					
Multi-Serv	CS Log Configurations					
Configure	DiskWatcher Configuration					
AAA Mode	e Setuo					

Schritt 7: Wählen Sie Role Management Setup (Rollenverwaltungs-Setup) aus, und wählen Sie die Standardberechtigung aus, die alle Admin-Benutzer bei der Authentifizierung erhalten. In diesem Beispiel wird der Netzwerkadministrator verwendet. Wählen Sie anschließend die Standardeinstellung aus.

cisco Security Manager					
Roles Roles Roles Approver Approver Roles Network Administrator Roles Roles	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			
	Role Management Setup Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Rol	Role Management Setup Roles Roles Roles Roles Roles Role Role Role			

Schritt 8: Wählen Sie Server > AAA Mode Setup Role (Servermodus > AAA-Modus-Setup-Rolle) aus und wählen Sie dann TACACS+-Option aus. Wählen Sie schließlich Change aus, um ISE-Informationen hinzuzufügen.

uļu cis	Cisco Security Manager
Home	Server Software Center
Commo Auto	Security Single-Server Management Multi-Server Trust Management Cisco.com Connection Management AAA Mode Setup
Authoriza Single Si	at Admin Processes 9 Backup
	Log Rotation Collect Server information Selftest
	Notify Users Job Browser Resource Browser
Local Us Multi-Ser Configur	CS Log Configurations DiskWatcher Configuration

cisco Cisco Security Manager
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

Schritt 9: Definieren Sie ISE-IP-Adresse und -Schlüssel. Optional können Sie die Option auswählen, die allen lokalen Authentifizierungsbenutzern oder nur einem Benutzer erlaubt, wenn die Anmeldung fehlschlägt. In diesem Beispiel ist der Nur-Admin-Benutzer als Fallbackmethode zulässig. Wählen Sie **OK**, um die Änderungen zu speichern.

		-
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	כ



Schritt 10: Wählen Sie Server > Einzelserver-Management aus, wählen Sie dann Lokales Benutzer-Setup aus, und wählen Sie Hinzufügen aus.

cisc	cisco Cisco Security Manager						
Home	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						
Circle Circ	Processes						
Single Sig	Backup						
	Log Rotation						
	Collect Server information						
	Selftest						
	Notify Users						
	Job Browser						
	Resource Browser						
Localities	System Preferences						
Local Use	CS Log Configurations						
Multi-Serv	DiskWatcher Configuration						
Configure							

cisco Cisco Security	Manager
Home Server * Software Center *	
Navigator	Local User Setup
Browser-Server Security mode setup Local User Policy Setup Local User Setup	Showing 206 records
Certificate Setup	2. Adrian.Lotean 3. Adrian.Richards 4. ahchenstein
	5. Aida.Aguitar 6. Alaric.Castain 7. alem.weldehimanot
	Andrew.OConnor
	11. armand.smith 12. Bernard.Alston
	13. bhess 14. Bil.Mason 15. bil.nash
	16. Billy Vaughan 17. bpiotnik
	18 Brother Loren

Schritt 11: Definieren Sie in Schritt 5 im ISE-Konfigurationsabschnitt denselben Benutzernamen und dasselbe Kennwort, das für die ISE erstellt wurde. In diesem Beispiel werden Rollen für die Autorisierung von Aufgaben csmoper und Help Desk verwendet. Wählen Sie OK, um den Administrator-Benutzer zu speichern.

semame:	csmoper			
assword:			Verify Password:	
mail:				
Authorization Type				
elect an option: O Full Aut	horization Ο Ena	able Task Au	thorization C Enable Device Authority	orization
Roles		Device	level Authorization	
Help Desk		Not Ap	plicable	
Approver				
Network Operator				
Network Administrator				
System Administrator				
Super Admin				
Security Administrator				
Security Approver				
_ Secondy Approver				
OK Cancel				
Con Cancer				

Überprüfung

Benutzeroberfläche des Cisco Security Manager-Clients

Schritt 1: Öffnen Sie einen neuen Fensterbrowser, und geben Sie <u>https://<enter_CSM_IP_Address</u> ein. Verwenden Sie im Abschnitt zur ISE-Konfiguration den Benutzernamen und das Kennwort **csmadmin**, der in Schritt 5 erstellt wurde.



Erfolgreiche Anmeldung beim Versuch kann in ISE TACACS-Live-Protokollen überprüft werden

E Cisco ISE			0	perations • TA	CACS		Evaluation Mode 39 Days	9	D 58	٥
Live Logs										
ට Refresh රා Export To 🗸						Refresh Show Every 3 seconds V Later	it 20 records 🗸	Last 3	hours Filter V	•
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Ne	twork D	evic.
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	Ne	etwork Dev	vice N
Apr 17, 2021 02:34:54.1		ò	csmadmin	Authentic	CSM 4.22 >> Default		ise30	CS	M422	
Last Updated: Sat Apr 17 202	09:37:58 0	MT-0500 (C	entral Daylight T	ime)				Recor	ds Show	n: 1

Cisco Security Manager Client-Anwendung

Schritt 1: Melden Sie sich mit dem Helpdesk-Administratorkonto bei der Cisco Security Manager Client-Anwendung an.

	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 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.	11.

Erfolgreiche Anmeldung beim Versuch kann in ISE TACACS-Live-Protokollen überprüft werden

ve Logs								
📿 Refresh 🖞 Export To 🗸						Refresh Every 3 seconds 🗸	Show Latest 20 records v	Within Last 3 hours →
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic
×		~	Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device

Schritt 2: Wählen Sie im Menü CSM-Client-Anwendung Extras > Sicherheitsmanager-Verwaltung, eine Fehlermeldung weist darauf hin, dass ein Mangel an Berechtigungen angezeigt werden muss.

🔒 Device 🗵 Neo 🔅 Pokcy 🚔 P	ky Bundle	Device Properties	0	6 🖲 🔁	Q %					9	inarch All Categories	CISCO
nter: -rene - v	Healt	Packet Cut Of Band Changes Packet Capture Witand Ping TraceRaute and MiLookup			De e	rployment () Fait 2 0	Nanager Fanding 2 O	Pasa: 0		Device State Octical 3 O Warring 3 O Korr	wi 8	
8:	0 a s	Wal.								Last Updat	e Time: 17 Apr 2021 00	LIE PM PDT d
1 () A		Show Containment Inventory Status Catalyst Summary Info Apply IPS Update Paniaw Configuration		d Alerta O O	Cannectio 0 0	on State 0 0	Deployment Qa • Qa •	Additional Information	39 Address 199, 134, 215, 3 199, 139, 210, 3 199, 139, 210, 9	Yest Donain goul-stuo varih-Suada.gov goul-stuo varvas 3 vada.gov goul-stuo varvas 11. vada.go	2- Turpe to Search Target 05 Heraton 9-9(2) 9-9(2) 9-9(2) 9-9(2)	Running 051 5.9(2)40 5.9(2)40 5.9(2)40
Publics	9	Backup Security Manager Diagnostics		-	•	0	6.0 6.0		199, 139, 233, 30 199, 139, 235, 4 199, 139, 235, 4	gu Latur varias 42.000, go gu Latur varias 42.000 gu Latur varias 4.000 gu Latur varias 4.000	9.900 9.900	9.9(2)40 9.9(2)40 9.9(2)40
no device adexifed	90	Satus-usefo-Suada.gev 0 Satus-usere: 2 usda.gev 0	0	•	•	0	8. 8.		199, 134, 215, 5 199, 139, 210, 5	qui sta varie i unta gov qui sta vavae i unta gov	9.9(2) 9.9(2)	8.9(2)40 8.9(2)40
				Error	- In	nsuffi	cient P	rivileges				x
You do r Please o If your A	ot have ontact y AA mod	sufficient privileges to our system administrato le is ACS, privileges are le is non-ACS, privileges	perfo or and gran	rm this o d have to ted via / granted	hem g ACS c via 1	ation. grant y configur (CiscoW	ou additi ration. /orks Hon	onal privileges. 1epage > Serve	er > Single-5	ierver Management > L	.ocal User Se	tup".

Schritt 3: Wiederholen Sie die Schritte 1 bis 3 mit dem csmadmin-Konto, um zu überprüfen, ob diesem Benutzer die entsprechenden Berechtigungen erteilt wurden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Kommunikationsvalidierung mit dem TCP-Dump-Tool auf der ISE

Schritt 1. Melden Sie sich bei der ISE an, navigieren Sie zum Symbol für drei Zeilen in der linken oberen Ecke, und wählen Sie Operations > Troubleshoot > Diagnostic Tools (Vorgänge > Fehlerbehebung > Diagnosetools) aus.

Schritt 2: Wählen Sie unter Allgemeine Tools die Option TCP-Dumps und dann Add+ aus. Wählen Sie Hostname, Network Interface File Name, Repository und optional einen Filter aus, um nur den Kommunikationsfluss der CSM-IP-Adresse zu erfassen. Wählen Sie Speichern und Ausführen

Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Downlo	oad Logs Debug Wizard	
General Tools	Add TCP Dump	
General Ioons	Add TCP Dumo packet for monitoring on a network interface and troubleshoot problems on the network as they appear.	
RADIUS Authentication Troubl	The set of the particular international and the termination of termination o	
Execute Network Device Com	Host Name *	
Evaluate Configuration Validat	ise30 V	
Posture Troubleshooting		
Agentiess Posture Troublesho	Network Interface *	
EndPoint Debug	GigabitEthernet 0 V 0	
TCP Dump		
Session Trace Tests		
	Filter	
	ip host 10.88.243.42	
TrustSec Tools >		
	E.g: ip host 10.77.122.123 and not	
	10.177.122.119	
	File Name	
	CSM_Tshoot	
	Nuppository VMRepository V	
	File Size	
	Mb	
	Limit to	
	File(c)	
	Time Lief	
	Minute(s)	
	Promisrulus Mode	
	Cancel Save Save and	Run

Schritt 3: Melden Sie sich bei der CSM-Clientanwendung oder der Client-Benutzeroberfläche an, und geben Sie die Administratoranmeldeinformationen ein.

Schritt 4: Wählen Sie auf der ISE die Schaltfläche Stopp aus, und überprüfen Sie, ob die pcap-Datei an das definierte Repository gesendet wurde.

₿ Re	efresh + Add	0 Edit	🗍 Trash 🗸 🕨 Start	$igodot$ Stop $\ \pm$ Downloa	d		$\nabla \mathbf{r}$	Filter 🗸 🐵
	Host Name		Network Interface	Filter	File Name	Repository	File S	Number o
	ise30.ciscoise.lab		GigabitEthernet 0	ip host 10.88.243	3.42 CSM_Tshoot	VMReposit	100	1

File Commands Tools Favorites Options Help Image: Add Image: Add	
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX ↑	
↑ 🗱 CSM_Tshoot.zip - ZIP archive, unpacked size 1,166 bytes	
Name Size Packed Type Modified CRC32	
- File folder	
CSM_Tshoot.pcap 1,166 556 PCAP File 4/17/2021 3:29 8A27888D	

Schritt 5: Öffnen Sie die pcap-Datei, um die erfolgreiche Kommunikation zwischen CSM und ISE zu überprüfen.

					CSM_Tshoot.pcap
4 🔳	1 🖉 🛞	S 🕺 🗋 🚍	९ 🗰 🗯 🚞	Ŧ ± 🗔	📃 a a a II
Apply :	a display filter	<¤/>			Expression +
No.	Time	Source	Destination	Protocol	Length Info
r 3	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	2 0.000130	10.122.112.4	10.88.243.42	TCP	66 49 - 55740 [SYN, ACK] Seg=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	8 0.065680	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1 5	0.101272	10.88.243.42	10.122.112.4	TACACS+	97 Q: Authentication
	5 0.101352	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0
0	0.10/185	10.122.112.4	10.88.243.42	TACACS+	81 R: Authentication
	0.203012	10.88.243.42	10.122.112.4	TACACCA	00 55/40 + 49 (ALK) Sed=44 ACK=28 Win=60048 Len=0
	0.220350	10.00.243.42	10.122.112.4	TCP	60 (2) AUTOFILICATION 54 (5) - 55746 [J(Y] Con-78 Jok-78 Win-20112 Lon-8
10	0.311136	10.122.112.4	10.88.243.42	TACACS+	72 Ri Authentication
11	0.311193	10,122,112,4	10.88,243,42	TCP	54 49 - 55748 [FIN, ACK] Segr46 Ack=78 Win=29312 Len=8
12	2 0.375973	10.88.243.42	10.122.112.4	TCP	60 55740 - 49 [ACK] Seg=70 Ack=47 Win=66048 Len=0
13	8 0.400651	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [FIN, ACK] Seg=70 Ack=47 Win=66048 Len=0
- 14	0.400724	10.122.112.4	10.88.243.42	TCP	54 49 → 55740 [ACK] Seq=47 Ack=71 Win=29312 Len=0
Erana	6: 01 huter	on wire (649 hits)	91 butes centured (6	AB hite)	1
Ether	met II, Src:	Vmware_a4:0d:c6 (00	1:50:56:a4:0d:c6). Dst	: Cisco 1f:21:	45 (00:14:6a:1f:21:45)
Inter	met Protocol	Version 4, Src: 10.	122.112.4, Dst: 10.88	.243.42	
Trans	mission Cont	rol Protocol, Src Po	ort: 49, Dst Port: 557	40, Seq: 1, Ac	:k: 44, Len: 27
TACAC	S+				
Ma	jor version:	TACACS+			
Mi	nor version:	0			
Tyj	pe: Authentic	cation (1)			
Se	quence number	ri Z	Itiala Connetions)		
> FU	ags: exee (Er	norypted payload, Mu 10057030	(tiple connections)		
	ssion ID: 301	15			
0000 0	NO 14 6a 1f 2	1 45 00 50 56 a4 0	d c6 88 88 45 88 ···	1 · ! E · P V · · · · · E	E -
0 7	CSM_Tshoot.pca	ø			 Packets: 14 - Displayed: 14 (100.016) Profile: Default

Wenn in der pcap-Datei keine Einträge angezeigt werden, überprüfen Sie Folgendes:

- 1. Der Device Administration Service ist auf ISE-Knoten aktiviert.
- 2. Die richtige ISE-IP-Adresse wurde zur CSM-Konfiguration hinzugefügt.
- 3. Falls sich eine Firewall in der Mitte befindet, überprüfen Sie, ob Port 49 (TACACS) zulässig ist.