# 針對ISE 2.x配置Prime 3.1 TACACS身份驗證

### 目錄

<u>簡介</u> <u>需求</u> <u>設定</u> <u>Prime配置</u> <u>ISE 組態</u> <u>疑難排解</u>

# 簡介

本文檔介紹如何配置Prime基礎設施以通過ISE 2.x的TACACS進行身份驗證。

# 需求

思科建議您瞭解以下主題的基本知識:

- •身分識別服務引擎 (ISE)
- Prime基礎架構

# 設定

Cisco Prime網路控制系統3.1

Cisco Identity Service Engine 2.0或更高版本。

(附註:ISE僅支援從版本2.0開始的TACACS,但是可以將Prime配置為使用Radius。如果您希望將 Radius與較舊版本的ISE或第三方解決方案配合使用,Prime除了TACACS還包括Radius屬性清單。 )

### Prime配置

'導航到以下螢幕:管理/使用者/使用者、角色和AAA,如下所示。

在此之後,選擇TACACS+伺服器頁籤,然後選擇右上角的Add TACACS+伺服器選項並選擇go。

在下一個螢幕上,TACACS伺服器條目的配置可用(此操作必須針對每個單獨的TACACS伺服器完 成)

AAA Mode Settings	Add TACACS+ Server		
Active Sessions	IP Address		
Change Password	The second secon		
ocal Password Policy	* Port	49	
ADIUS Servers	Shared Secret Format	ASCII	
SSO Server Settings	* Shared Secret		0
SSO Servers	* Confirm Shared Secret		
ACACS+ Servers	* Retransmit Timeout	5 (secs)	
Jser Groups	* Retries	1	
Jsers	Authentication Type	PAP •	
	Local Interface IP	192.168.10.154	•

在這裡,您需要輸入伺服器的IP地址或DNS地址以及共用金鑰。另請注意您要使用的本地介面 IP,因為稍後需要在ISE中將此相同的IP地址用於AAA客戶端。

以便完成Prime上的配置。您需要在AAA mode settings頁籤下的Administration / Users / Users , Roles & AAA下啟用TACACS。

(附註:建議選中Enable fallback to Local選項,該選項包含ONLY on no server response或On no response or failure選項(特別是在測試配置時)

Administration / Users / U	Users, Roles & AAA	00
AAA Mode Settings	AAA Mode Settings	
Active Sessions	AAA Mode @ CLocal RADIUS SSO	
Change Password	C Enable fallback to Local ONLY on no server respon:	
ocal Password Policy		
RADIUS Servers	Save	
SSO Server Settings		
SSO Servers		
ACACS+ Servers		
Jser Groups		
Jsers		
	Administration / Users / 1 AAA Mode Settings Active Sessions Change Password Local Password Policy ADIUS Servers SSO Server Settings SSO Servers FACACS+ Servers Jser Groups Jsers	Administration / Users / Users, Roles & AAA   AdA Mode Settings   AAA Mode Settings   AAA Mode Settings   AAA Mode @   Local @RADIUS @TACACS+   © SSO   Change Password Policy   .ocal Password Policy   ADIUS Servers   SSO Servers   SSO Servers   CACACS+ Servers   Jser Groups

#### ISE 組態

在工作中心/裝置管理/網路資源/網路裝置/新增Prime配置為ISE上的AAA客戶端

dentity Services Engine	Home   Context Visibil	ity > Operations	▶ Policy      ▶ Administrat	ion - Work Centers		License Warning 🔺		
Network Access     Guest Access	► TrustSec ► BYOD ►	Profiler   Posture	- Device Administration					
Overview Identities User Identities	ity Groups Ext Id Sources	▼Network Resources	Network Device Groups	Policy Elements	Device Admin Policy Sets	Reports Settings		
Network Devices	Network Devices						Selected 0   Total	• <del>8</del> & _
TACACS External Servers	🖊 Edit 🕂 Add 🕞 Du	plicate 😭 Import 🚱	Export Generate PAC	🔀 Delete		Show All		- 8
TACACS Server Sequence	Name 🔺 IP	/Mask Profile N	lame	Location	Туре		Description	
interfee center coquentes				No data avai	ilable			

輸入Prime伺服器的資訊。您需要包括的屬性包括Name(名稱)、IP address(IP地址),為 TACACS和Shared Secret(共用金鑰)選擇選項。您可能還希望新增裝置型別,特別是為 Prime,以便稍後作為授權規則或其他資訊的條件使用,但這是可選的。

Notwork Davisor	Network Devices List > New Network Device	
	Network Devices	
Default Devices	' Name	
IACACS External Servers	Description	
TACACS Server Sequence		
	* IP Address: / 32	
	* Davies Brafile the Circa - (D)	
	Model Name 👻	
	Software Version	
	* Network Device Group	
	Device Type All Device Types Set To Default	
	Location All Locations Set To Default	
	RADIUS Authentication Settings	
	☑ ▼TACACS Authentication Settings	
	Shared Secret Show	
	Enable Single Connect Mode	
	<ul> <li>Legacy Cisco Device</li> <li>TACACS Draft Compliance Single Connect Support</li> </ul>	
	□ → SNMP Settings	
	Advanced TrustSec Settings	
	Submit Cancel	

然後建立TACACS配置檔案結果以將所需的屬性從ISE傳送到Prime,以提供正確的訪問級別。導航 至Work Centers/Policy Results/Tacacs Profiles並選擇Add選項。

dentity Services Engine	Home	<ul> <li>Operations</li> </ul>	Policy      Guest	Access	► Administration	✓ Work Centers	1	License Wa	arning 🔺	0	2	\$
TrustSec     Tevice Administration												
Overview   Identities User Identity	Groups	Network Resource	ces Network Device	Groups	Policy Conditions		Device Admin Policy Sets	Reports	Settings			
TACACS Command Sets	TAC/	ACS Profiles			Rov	vs/Page 6 v	∢ ∢ (1)/1 ► ►	Go 6 To	tal Rows			
	CF	Refresh 🕂 Add	Duplicate 🛛 🗂 Tr	rash 👻 (	🕑 Edit			🔻 Filter 🕶	¢			
		Name			Description							

配置名稱,並使用Raw View選項在Profile attributes框中輸入屬性。屬性將來自初級伺服器本身。

diale Identity Services Engine	Home > Operations >	Policy Guest Access	► Administration	✓ Work Centers		License Warning 🔺	۹ 0	4 O
TrustSec     Tevice Administration								
Overview Identities User Identity	Groups   Network Resource	Network Device Groups	Policy Conditions		Device Admin Policy Sets	Reports Settings		
C TACACS Command Sets	TACACS Profiles > New							
TACACS Profiles	TACACS Profile	Namet						
		Name						
		Description						
	Task Attribute Vi	Raw View						
	Profile Attributes							
	l							
						Cancel	Submit	

獲取管理/使用者/使用者、角色和AAA螢幕下的屬性,然後選擇使用者組頁籤。在此,您可以選擇要 提供的組訪問許可權級別。在本示例中,通過在左側選擇適當的「任務清單」來提供管理員訪問許 可權。

#### Administration / Users / Users, Roles & AAA ★

000

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP	6	Task List
Local Password Policy	Config Managers		8	Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita	6	Task List
SSO Server Settings	Monitor Lite		8	Task List
	NBI Credential			Task List
SSU Servers	NBI Read		8	Task List
FACACS+ Servers	NBI Write		6	Task List
Jser Groups	North Bound API		1	Task List
Users	Root	root		Task List
	Super Users		8	Task List
	System Monitoring		6	Task List
	User Assistant		8	Task List
	User Defined 1		6	Task List
	User Defined 2		0	Task List
	User Defined 3		6	Task List
	User Defined 4			Task List
	mDNS Policy Admin		A	Task List

#### Administration / Users / Users, Roles & AAA A -000 Task List AAA Mode Settings O Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server. RADIUS Custom Attributes © If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS TACACS+ Custom Attributes Active Sessions Change Password NCS:role0=Admin role0=Admin role0=Admin task0=Discovery Schedule Privilege task1=Mesh Reports task2=Saved Reports List task3=Monitor Menu Access task4=Device WorkCenter task5=Inventory Menu Access task6=Add Device Access task6=Add Device Access NCS:task0=Discovery Schedule Privilege NCS:task1=Hesh Reports NCS:task2=Saved Reports List NCS:task3=Monitor Menu Access NCS:task4=Device WorkCenter NCS:task5=Inventory Menu Access NCS:task5=Inventory Menu Access NCS:task5=Inventory Menu Access Local Password Policy **RADIUS Servers SSO Server Settings** taskG=Add Device Access task7=Config Audit Dashboard task8=Usom NetFlow Reports task9=Apic Controller Read Access task10=Configuration Templates Read Access task12=High Availability Configuration task13=View Job task14=Incidents Alarms Events Access task15=TAC Case Management Tool task16=Configure Autonomous Access Point Templates NCS:task6=Add Device Access NCS:task7=Config Audit Dashboard NCS:task8=Custom NetFlow Reports NCS:task8=Configuration Templates Read Access NCS:task10=Configuration Templates Read Access NCS:task11=Alarm Policies Edit Access NCS:task12=High Availability Configuration NCS:task13=View Job NCS:task13=View Job NCS:task15=TAC Case Management Tool NCS:task15=TAC Case Management Tool NCS:task15=CAC figure Autonomous Access Point Templates SSO Servers TACACS+ Servers User Groups Users NCS:task19=LONTIgure Autonomous Access .. Templates NCS:task17=Import Policy Update NCS:task18=PNP Profile Read-Write Access NCS:task19=SSO Server AAA Mode MCGLebck20ellang Reputer Access Templates task17=Import Policy Update task18=PnP Profile Read-Write Access task19=SSO Server AAA Mode task20=Alarm\_Repuser\_Access

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

### 然後將其貼上到ISE上的配置檔案的原始檢視部分。

sco Ide	ntity Services	Engine	Home	<ul> <li>Operations</li> </ul>	Policy	Guest Access	Administration	✓ Work Centers		License W	/arning 🔺			
TrustSe	c • Device A	dministration												
verview	Identities	User Identity	Groups	Network Reso	ources Net	work Device Groups	Policy Conditions		Device Admin Policy Sets	Reports	Settings			
		G	THO	ACC Destine - New	12									
ACS C	ommand Sets		IAC	ACS Promes > Nev	W									
CS PI	rofiles		TAC	ACS Profile										
					Na	ime * Prime								
					Descri	ption								
				Task Attribut	te View	Raw View								
			Prof	file Attributes										
			ro	le0=Admin									-	1
			ta	sk0=Discovery §	Schedule P	rivileae								
			ta	sk1=Mesh Repo	orts	9								
			ta	sk2=Saved Rep	orts List									
			ta	sk3=Monitor Me	nu Access									
			ta	sk4=Device Wor	rkCenter									
			ta	sk5=Inventory N	Aenu Acces	s								
			ta	sk6=Add Device	Access									
			ta	sk7=Config Aud	it Dashboa	rd								
			ta	sk8=Custom Ne	tFlow Repo	orte								
			ta	sko-Caston Ne	aller Dead /	Arcase								
			ta	sk10-Configura	tion Tomple	tes Boad Access								
			la	skild-Connyural	lates Edit A	iles Redu Access								
			ta	sk11=Alarm Poll	Icles Edit A	ccess								
			ta	sk12=High Avail	lability Con	iguration								
			ta	sk13=View Job									-	
											Cancel	Su	hmit	
														-

### 虛擬域自定義屬性是必需的。根域資訊可在Prime Administration -> Virtual Domains下找到。

										Virtual Do	main RO	JOT-DOMAIN	I   ro	ot 🔻 🛛
cisco Infrastructure	≪d 💌 M	Ionitor 🔻	Configuration	•	Inventory	<ul> <li>Map</li> </ul>	s •	Services	•	Reports	Ac	iministration	1 🗶	
Administration > Virtual Domains Virtual Domains	Virtual Domains ROOT-DOM	> ROOT-D	OMAIN											
Virtual Domains	Virtual domains Infrastructure, their assigned	s are logica you can co part of the	I groupings of configure virtual configure virtual context.	levice Iomai	s and are us ins. Virtual de	ed to contr omain filter	ol who s allow	o can admir w users to c	iister onfigi	a group. Afte ure devices,	r you a view ali	add devices arms, and g	to Prime enerate	reports
ROOT-DOMAIN	* Name Email Address	ROOT-DO	NIAMO			Time Zo Descript	ne [· ion [	Select Tin ROOT-DOM	ne Zo AIN	ne		• 		
	Submit	Cancel												

### Prime虛擬域名稱必須新增為屬性virtual-domain0="virtual domain name"

dentity Services Engine	Home	y → Operations	▶ Policy	Administration	✓ Work Centers		
Network Access     Guest Access	TrustSec     BYOD     H	Profiler Posture	- Device Adm	inistration + Pas	siveID		Click have to do wireless setup F
Overview Identities User Identities	ity Groups Ext Id Sources	Network Resource	es · Policy El	ements Device A	dmin Policy Sets	Reports Settings	Click here to do wireless setup to
0	TACACS Profiles > Prime	Access:					
Conditions	TACACO Profile	ALLESS					
Network Conditions	IACACS FIOIL	Name	Drime Assess				
✓ Results		Name	Phine Access				
Allowed Dretecole		Description					
TACACS Command Sets							
TACACS Profiles	Task Attribute	View Raw V	ew				
	Profile Attributes						
	task162=Monitor Mo task163=Context Av task164=Voice Diag task165=Configure U task166=RRM Dash task167=Swim Dele task168=Theme Ch task168=Inpert Poli task170=Design End task170=Design End task171=Planning N task172=Pick and U task172=Fick and U task174=Ack and U task175=Ack and U task176=Auto Provisi virtual-domain0=RO	abbility Devices vare Reports nostics Choke Points board te anger Access cy Update dpoint Site Associ lode npick Alerts Menu Access nack Security Inde nack Alerts sioning OT-DOMAIN	ation Access x Issues				Ň

完成此操作後,您需要做的只是建立一個規則以分配在上一步中「工作中心/裝置管理/裝置管理策略 集」下建立的外殼配置檔案

(附註:「條件」因部署而異,但是您可以將「裝置型別」專門用於Prime或其他型別的過濾器(例 如Prime的IP地址)作為「條件」之一,以便此規則可以正確地過濾請求)

-dudu Identity Services Engine Home	Context Visibility + Operations + Policy + Administration + Work Centers License Warning 🔺 🔍	0 1 0
Network Access     Guest Access     TrustSec	BYOD      Profiler      Posture      -Device Administration	
Overview Identities User Identity Groups E	Ent Id Sources + Network Resources Network Device Groups + Policy Elements Device Admin Policy Sets Reports Settings	
Policy Sets Search policy names & descriptions. Search policy names & descriptions. Second Se	Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page Status Name Description Default Tacacs_Default Regular ® Proxy Sequence ✓ Authentication Policy Default Rule (if no match) : Allow Protocols : Default Device Admin and use : Internal Users	Edt   •
Save Order Reset Order	Authorization Policy     Exceptions (0)     Standard	
	Status         Rule Name         Conditions (identity groups and other conditions)         Command Sets         Shell Profiles           Prime Rule         If         DEVICE:Device Type EQUALS All Device         then         PermitAll AND         Prime           Types#Prime         If no matches, then         Select Profile(s)         Deny All Shell Profile         Profile	Edt) • Edt) •

此時,配置應該已完成。

# 疑難排解

如果此配置不成功,並且在Prime上啟用本地回退選項,您可以通過刪除Prime的IP地址強制從 ISE進行故障轉移。這將導致ISE不響應並強制使用本地憑證。如果本地回退配置為對拒絕執行,則 本地帳戶仍可正常工作並提供對客戶的訪問許可權。

如果ISE顯示成功的身份驗證並且匹配正確的規則,但是Prime仍拒絕請求,您可能需要仔細檢查屬 性在配置檔案中是否正確配置,並且沒有傳送其他屬性。