Autenticación de TACACS de la prima 3.1 de la configuración contra ISE 2.x

Contenido

Introducción Requisitos Configurar Configuración primera Configuración ISE Troubleshooting

Introducción

Este documento describe cómo configurar la infraestructura primera para autenticar vía el TACACS con ISE 2.x.

Requisitos

Cisco recomienda que usted tiene un conocimiento básico de estos temas:

- Identity Services Engine (ISE)
- Infraestructura primera

Configurar

Sistema de control de redes 3.1 de la prima de Cisco

Motor 2.0 del servicio de la identidad de Cisco o más adelante.

(Nota: El ISE soporta solamente el TACACS que comienza con la versión 2.0, sin embargo es posible configurar la prima para utilizar el radio. La prima incluye la lista de atributos de RADIUS además del TACACS si usted preferiría utilizar el radio, con una versión anterior del ISE o de una solución del otro vendedor.)

Configuración primera

Navigiate a la pantalla siguiente: La administración/usuarios, papeles y AAA de los usuarios según lo visto abajo.

Una vez que, selecciona el lengueta de los servidores TACACS+, después seleccione la opción del servidor del agregar TACACS+ en la esquina derecha superior y selecto vaya.

En la siguiente pantalla la configuración de la entrada del servidor TACACS está disponible (ésta

tendrá que ser hecha para cada servidor TACACS individual)

↑ Administration / Users	; / Users, Roles & AAA 🔺			0 0
AAA Mode Settings	Add TACACS+ Server			
Active Sessions	IP Address			
Change Password	The Name			
Local Password Policy	Divis Name			
RADIUS Servers	Shared Secret Format	ASCII		
SSO Server Settings	* Shared Secret		9	
SSO Servers	* Confirm Shared Secret			
TACACS+ Servers	* Retransmit Timeout	5 (secs)		
User Groups	* Retries	1		
Users	Authentication Type	PAP •		
	Local Interface IP	192.168.10.154 •		
	Save Cancel			

Aquí usted necesitará ingresar el IP Address o la dirección de DNS del servidor, así como la clave secreta compartida. También satisfaga observan el IP de la interfaz local que usted quisiera utilizar, como esta misma dirección IP necesita ser utilizada para el cliente AAA en el ISE después.

Para completar la configuración en la prima. Usted necesitará habilitar el TACACS bajo la administración/los usuarios/los usuarios, los papeles y el AAA bajo lengueta de las configuraciones de modo AAA.

(Nota: Se recomienda para marcar el retraso del permiso a la opción local, con SOLAMENTE en ninguna respuesta del servidor o encendido la ninguna opción de la respuesta o del error, especialmente mientras que prueba la configuración)

A	Administration / Users / U	sers, Roles & AAA \star	🗖 Q 🕲
ŀ	AAA Mode Settings	AAA Mode Settings	
ŀ	Active Sessions	AAA Mode @ _Local @RADIUS @TACACS+	©\$\$0
0	Change Password		
L	ocal Password Policy		
F	RADIUS Servers	Save	
5	SSO Server Settings		
	SSO Servers		
1	TACACS+ Servers		
L	Jser Groups		
U	Jsers		
_			

Configuración ISE

Configure la prima como cliente AAA en el ISE en los centros de trabajo/Device Administration (Administración del dispositivo) los dispositivos del /Network de los recursos del /Network/agregue



Ingrese la información para el servidor primero. Los atributos requeridos que usted necesita incluir son nombre, dirección IP, seleccionan la opción para el TACACS y el secreto compartido. Usted puede desear además agregar un tipo de dispositivo, específicamente para la prima, para utilizar después como condición para la regla de la autorización o la otra información, no obstante ésta es opcional.

Network Instruct default barles Default barles ACACS Statured Sequence Network Devices Image: Description	G	Natural Davies Link Result Burley	
Default Devices TACACS External Servers TACACS Server Sequence	Network Devices	Network Devices	
TACACS External Servers TACACS Server Sequence • Device Profile • Software Version • Network Device Group	Default Devices	' Name [
TACACS Server Sequence * IP Address: * Device Profile * Device Profile * Device Profile * Device Type * Network Device Group Device Type * Network Device Group Device Type Belice * RADIUS Authentication Settings * RADIUS Authentication Settings * Network Device * RADIUS Authentication Settings * NAP Settings * NAMP Settings * NAMP Settings * NAdvanced TrustSec Settings	TACACS External Servers	Description	
Perce Profile @ Cisco • 0 • Device Profile @ Cisco • 0 • Model Name • • Software Version • • • Network Device Group Device Type All Device Type ③ Set To Default. Location All Locations · Set To Default. • NADIUS Authentication Settings • TACACS Authentication Settings • TACACS Authentication Settings • TACACS Authentication Settings • Device Type Isings · Cisco Device · Ci	TACACS Server Sequence		
Device Profile Cisco • ① Model Name • Software Version • Software Version • Network Device Group Device Type Int Device Types • Set. To Default. Location Int Locations • Set. To Default. Location Int Locations • Set. To Default. • RADIUS Authentication Settings • RADIUS Authentication Settings • TACACS Authentication Settings • TACACS Authentication Settings • Legacy Cisco Device • Advanced TrustSec Settings • SIMMP Settings		I = 1P Address: / 32	
* Network Device Group Device Type All Device Types S Set To Default Location All Locations Set To Default • RADIUS Authentication Settings • TACACS Device • TACACS Device • Advanced TrustSec Settings		* Device Profile data Cisco ♥ ⊕ Model Name ♥ Software Version ♥	
Device Type All Device Types Location All Locations Image: ARDIUS Authentication Settings		* Network Device Group	
 RADIUS Authentication Settings TACACS Authentication Settings Shared Secret Show Enable Single Connect Mode Legacy Cisco Device TACACS Draft Compliance Single Connect Support SMMP Settings Advanced TrustSec Settings 		Device Type All Device Types Set To Default Location All Locations Set To Default	
 TACACS Authentication Settings Shared Secret Show Enable Single Connect Mode Legacy Cisco Device TACACS Draft Compliance Single Connect Support SNMP Settings Advanced TrustSec Settings 		RADIUS Authentication Settings	
Image: Strain		TACACS Authentication Settings Shared Secret Show Enable Single Connect Mode Legacy Cisco Device TACACS Draft Compliance Single Connect Support	
Advanced TrustSec Settings		SNMP Settings	
		Advanced TrustSec Settings	
		· · interfect record county	

Entonces cree un resultado del perfil TACACS para enviar los atributos requeridos del ISE para preparar, proporcionar el nivel correcto de acceso. Navegue a los centros de trabajo/a los resultados de la directiva/a los perfiles de Tacacs y seleccione la opción del agregar.

dentity Services Engine	Home	Operations	Policy Guest Access	► Administration	✓ Work Centers	1	License Wa	arning 🔺	Q,	0	±	ø
TrustSec Tevice Administration												
Overview Identities User Identit	Groups	Network Resources	Network Device Groups	Policy Conditions		Device Admin Policy Sets	Reports	Settings				
TACACS Command Sets	TACA	CS Profiles		Row	rs/Page 6 🔻	⊲ ⊲ 1 /1 ⊳ ₽	Go 6 To	ital Rows				
Monoo Homes	CR	efresh 🕂 Add	Duplicate 🗂 Trash 🗸	🕑 Edit			▼ Filter -	۰.				
		Name		Description								

Configure el nombre, y utilice la opción <u>sin procesar de la visión</u> para ingresar los atributos bajo el rectángulo de los atributos del perfil. Los atributos vendrán del servidor sí mismo de la cartilla.

dentity Services Engine	Home	Policy Guest Access	► Administration	✓ Work Centers		License Warning 🔺	९ 🔮	4 ¢
TrustSec Tevice Administration								
Overview Identities User Identity	Groups • Network Resou	rces Network Device Groups	Policy Conditions		Device Admin Policy Sets	Reports Settings		
C TACACS Command Sets	TACACS Profiles > New							
TACACS Profiles	TACACS Profile							
		Name						
		Description						
	Task Attribute	View Raw View						
	Profile Attributes							
	l							
						Cancel	Submit	

Consiga los atributos bajo la administración/los usuarios de los usuarios, los papeles y la pantalla AAA, y seleccione la lengueta de los grupos de usuarios. Aquí usted selecciona el nivel de grupo de acceso que usted desea proporcionar. En este admin de ejemplo el acceso es proporcionado seleccionando la lista de tareas apropiada en el lado izquierdo.

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
50 Seguere 033	NBI Credential			Task List
550 Servers	NBI Read		6	Task List
TACACS+ Servers	NBI Write		6	Task List
User Groups	North Bound API		1	Task List
Users	Root	root		Task List
	Super Users		8	Task List
	System Monitoring			Task List
	User Assistant		8	Task List
	User Defined 1		6	Task List
	User Defined 2			Task List
	User Defined 3		1	Task List
	User Defined 4			Task List
	mDNS Policy Admin			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=Nonitor Menu Access task4=Device NorkCenter task5=Turentory 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** task5=Add Device Access task7=Config Audit Dashboard task8=Custom NetFlow Reports task9=Apic Controller Read Access task10=Configuration Templates Read Access task11=Alarm Policies Edit 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:task17=Import Policy Update NCS:task18=PnP Profile Read-Write Access NCS:task18=SSO Server AAA Mode Templates Task17=Import Policy Update task18=PnP Profile Read-Write Access task19=SSO Server AAA Mode task20=Alarm Resusce Access • Virtual Domain custom attributes are mandatory. To add custom attri es related to Virtual Domains, please click here

Entonces pegúelos en la sección sin procesar de la visión del perfil en el ISE.

eisco	Identity Services	Engine	Home	Operations	▶ Policy	▶ Guest Access	Administration	✓ Work Centers		License Wa	arning 🔺				
▶ Trus	stSec • Device A	dministration													
Overv	iew Identities	User Identit	y Groups	Network Reso	urces Netw	ork Device Groups	Policy Conditions	✓ Policy Results	Device Admin Policy Sets	Reports	Settings				
		G													
TACAC	S Command Sets		TAC	ACS Profiles > Nev	t.										
TACAC	S Profiles		TAC	ACS Profile											
					Nan	ne * Prime									
					Descrip	tion									
				Task Attribute	e View	Raw View									
			Prof	ile Attributes											
			-	lo0=Admin									-	1	
			ta	sk0=Discovery S	chedule Pri	vilene									
			ta	sk1=Mesh Reno	rts	viiege									
			ta	sk2=Saved Repo	nts List										
			ta	sk3=Monitor Me	nu Access										
			ta	sk4=Device Wor	kCenter										
			ta	sk5=Inventory M	enu Access										
			ta	sk6=Add Device	Access										
			ta	sk7=Config Audi	t Dashboard	1									
			ta	sk8=Custom Net	Flow Repor	ts									
			ta	sk9=Anic Contro	ller Read Ar	rress									
			ta	sk10=Configurat	ion Templat	es Read Access									
			ta	sk11=Alarm Poli	ries Edit Acc										
			ta	sk12=High Avail	ability Confi	ruration									
			ta	sk13=View Job	ability coning	garadon									
			-									_			
											Cancel	Su	bmit		
													_		

Los atributos personalizados del dominio virtual son obligatorios. La información del Raíz-dominio se puede encontrar bajo administración primera - > los dominios virtuales.

uluulu, Cisco Prime								Virtual Dom	ain ROOT-DOMAII	N I	root 🔻
cisco Infrastructure	≪d 💌 M	onitor 🔻	Configuration	 Inventory 	 Maps 	 Servic 	es 🔻	Reports 🔻	Administration	n 🔻	
Administration > Virtual Domains Virtual Domains	Virtual Domains	> ROOT-DO	OMAIN								
Virtual Domains	Virtual domains Infrastructure, their assigned (s are logical you can co part of the	l groupings of dev nfigure virtual dor network only.	vices and are us mains. Virtual de	ed to control o omain filters a	who can adn Ilow users to	ninister config	a group. After ure devices, vie	you add devices ew alarms, and g	to Pr Jenera	ime ate reports
(= *) H * (\$\$ \$\$	* Name	ROOT-DO	MAIN		Time Zone	Select	Time Zo	ne	•		
ROOT-DOMAIN	Email Address				Description	ROOT-DO	MAIN				
	Submit	ancel									

El nombre del dominio virtual primero tiene que ser agregado como Domain Name del atributo virtual-domain0="virtual"

cisco identity Services Engine	Home → Context Visibility	Operations → Policy	Administration	✓ Work Centers		٩
Network Access Guest Access	TrustSec BYOD Pro	filer + Posture - Device	Administration + Pa	ssiveID		Click here to do wireless setup D
Overview Identities User Iden	ntity Groups Ext Id Sources	Network Resources Poli	cy Elements Device	Admin Policy Sets Rep	ports Settings	
Conditions	TACACS Profiles > Prime Ac	ccess				
Network Conditions	IACACS Profile	Name Prime Acce	is			
✓ Results		Description				
Allowed Protocols TACACS Command Sets		Description				
TACACS Profiles	Task Attribute Vie	ew Raw View				
	Profile Attributes					
	task162=Monitor Mobil task163=Context Awar task164=Voice Diagno task165=Configure Ch task166=RRM Dashbo task167=Swim Delete task168=Theme Chan task169=Import Policy task170=Design Endpt task170=Design Endpt task172=Pick and Unp task172=Pick and Unp task173=Configure Me task174=Ack and Unar task175=Ack and Unar task176=Auto Provisio	lity Devices re Reports stics oke Points aard ger Access Update point Site Association Acce de ick Alerts inu Access ck Security Index Issues ck Alerts ning	55			^

Una vez que eso se hace todos usted necesita hacer debe crear una regla para asignar el perfil del shell creado en el paso anterior, bajo los centros de trabajo/Device Administration (Administración del dispositivo)/directiva Admin del dispositivo fija

(Nota: Las "condiciones" variarán dependiendo del despliegue, no obstante usted puede utilizar el "tipo de dispositivo" específicamente para la prima u otro tipo de filtro tal como dirección IP de la prima, como una de "condicionan" de modo que esta regla filtre correctamente las peticiones)

-thete Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers License Warning Q	0 1 0
Network Access Guest Access TrustSec	BYOD Profiler Posture -Device Administration	
Overview Identities User Identity Groups	Ext Id Sources + Network Resources Network Device Groups + Policy Elements Device Admin Policy Sets Reports Settings	
Policy Sets Search policy names & descriptions.	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 Definit Tarcet. Definit	
Summary of Policies A list of all your policies	Regular ® Proxy Sequence ©	
Global Exceptions Rules across entire deployment	Authentication Policy Default Rule (if no match) Allow Protocols - Datault Davice Admin and use - Internet Linese	
Default Tacacs_Default		EOK *
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	Edit) •
	Tacacs_Detault if no matches, then Select Profile(s) Deny All Shell Profile	Edit) +

En este momento la configuración debe ser completa.

Troubleshooting

Si esta configuración es fracasada y si bajan el locales opción eran permiso en la prima, usted puede forzar un fall encima del ISE, quitando la dirección IP de la prima. Esto hará el ISE no responder y forzar el uso de las credenciales locales. Si el retraso local se configura para ser realizado en un rechazo, las cuentas locales todavía trabajarán y proporcionarán el acceso al cliente.

Si el ISE muestra una autenticación satisfactoria y está correspondiendo con la regla correcta sin embargo la prima todavía está rechazando la petición que usted puede desear para comprobar los atributos con minuciosidad se configura correctamente en el perfil y no se está enviando ningunos atributos adicionales.