Configurar a função TACACS personalizada para o Nexus 9K usando o ISE 3.2

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Diagrama de Rede
Etapa 1: Configurar o Nexus 9000
Etapa 2. Configurar o Identity Service Engine 3.2
Verificar
Troubleshooting

Introdução

Este documento descreve como configurar uma função Nexus personalizada para TACACS via CLI em NK9.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- TACACS+
- ISE 3.2

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O arquivo de imagem do Cisco Nexus9000, NXOS é: bootflash:///nxos.9.3.5.bin
- Identity Service Engine versão 3.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Requisitos de licenciamento:

Cisco NX-OS - O TACACS+ não requer licença.

Cisco Identity Service Engine - Para novas instalações do ISE, você tem uma licença de período de avaliação de 90 dias que tem acesso a todos os recursos do ISE. Se você não tiver uma licença de avaliação, para usar o recurso ISE TACACS, você precisará de uma licença de Administrador de dispositivo para o Nó do servidor de política que faz a autenticação.

Após a autenticação dos usuários de administração/help desk no dispositivo Nexus, o ISE retorna a função desejada do shell do Nexus.

O usuário atribuído com essa função pode executar a solução básica de problemas e devolver determinadas portas.

A sessão TACACS que obtém a função Nexus deve ser capaz de usar e executar somente os próximos comandos e ações:

- Acesso para configurar o terminal para SOMENTE executar interfaces desligadas e sem desligamento a partir de 1/1-1/21 e 1/25-1/30
- ssh
- SSH6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Enable

Configurar

Diagrama de Rede



Diagrama de Componentes de Fluxo

Etapa 1: Configurar o Nexus 9000

1. Configuração AAA.



Aviso: depois que você habilita a autenticação TACACS, o dispositivo Nexus pára de usar a autenticação local e começa a usar a autenticação baseada em servidor AAA.

Nexus9000(config)# feature tacacs+ Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample Nexus9000(config)# tacacs-server key 0 "Nexus3xample" Nexus9000(config)# aaa group server tacacs+ IsePsnServers Nexus9000(config-tacacs+)# server <Your ISE IP> Nexus9000(config)# aaa authentication login default group IsePsnServers local

2. Configure a função personalizada com os requisitos especificados.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#
                          description Can perform basic Toubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown
vlan policy deny
interface policy deny
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/1
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/2
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/3
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/4
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/5
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/6
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/7
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/8
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/8
                                      permit interface Ethernet1/9
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/10
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/11
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/12
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/13
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/14
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/15
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/16
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/17
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/18
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/19
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/20
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/21
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/22
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/25
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/26
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/27
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/28
                                      permit interface Ethernet1/29
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/30
```

Copy complete.

Etapa 2. Configurar o Identity Service Engine 3.2

1. Configure a identidade usada durante a sessão do Nexus TACACS.

A autenticação local do ISE é usada.

Navegue até a guia Administration > Identity Management > Groups e crie o grupo do qual o usuário precisa fazer parte, o grupo de identidade criado para esta demonstração é iseUsers.

=	С	isc	o ISE		Administr	ation • Identity Ma	anagement			A Evaluation Mode 29 [Days	Q	0	P	٩
lde	ntitie	es	Groups	External Ide	entity Sources	Identity Source	Sequences	Settings							
	Ident EQ	tity G	iroups		User Identity Grou	ups > New User Identity JP	Group								
			Endpoint Ident	tity Groups	* Name	iseUsers									
		Ð	User Identity (Groups	Description										
								ubmit	Cancel						

Criando um grupo de usuários

Clique no botão Submit.

Em seguida, navegue até a guia Administração > Gerenciamento de identidades > Identidade.

Pressione o botão Add.



Criação de usuário

Como parte dos campos obrigatórios, comece com o nome do usuário, o nome de usuário isisicool é usado neste exemplo.

Network Access Users List >	> New Network Access User	
$^{\vee}$ Network Access	User	
* Username	iseiscool	
Status	Z Enabled 🗸	
Account Name Alias		
Email		

Nomeando o usuário e criando-o

A próxima etapa é atribuir uma senha ao nome de usuário criado, VainillaISE97 é a senha usada nesta demonstração.

\vee Passwords							
Password Type:	Internal Users						
Password Lifetime	:						
With Expiration ① Password will expire in 60 days							
O Never Expires							
	Password		Re-Enter Password				
* Login Password				Generate Password	()		
Enable Password				Generate Password	()		

Atribuição de senha

Por fim, atribua o usuário ao grupo criado anteriormente, que, nesse caso, é iseUsers.

∨ Use	er Groups	
:	iseUsers	<u>·</u> 🗊 🕂

2. Configure e Adicione o Dispositivo de Rede.

Adicione o dispositivo NEXUS 9000 à Administração do ISE > Recursos de rede > Dispositivos de rede

Clique no botão Add para iniciar.

Netv	work	Devices				
						Selected 0
🖉 Edit	+ Add	Duplicate	للے Import	스 Export 🗸	🔒 Generate PAC	🗑 Delete 🗸
	Name	∧ IP/Mask	Profile N	ame	Location	Туре

Página Dispositivo de acesso à rede

Insira os valores do formulário, atribua um nome ao NAD que está sendo criado e um IP do qual o NAD entra em contato com o ISE para a conversação TACACS.

≡ Cisco ISE	Work Centers ·	Device Administration	A (valuation Mode 27 Days	Q	0	6	٥
Overview Identities	User Identity Groups Ext Id	Sources Network Resour	ces Policy Elements	More \vee				
Network Devices	Network Devices List > New Netw	vork Device						
Network Device Groups	Network Devices							
Default Devices		_						
TACACS External Servers	Name NEXUS98	<						
TACACS Server Sequence	Description Nexus De	vice For TACACS						
	IP Address 🗸 * IF	P: A.B.C.D / 32						
	Device Profile Cisco							
	Model Name							
	Software Version							
	Network Device Group							

Configurar dispositivo de rede

As opções suspensas podem ser deixadas em branco e podem ser omitidas; essas opções destinam-se a categorizar seus NADs por local, tipo de dispositivo, versão e, em seguida, alterar o fluxo de autenticação com base nesses filtros.

Em Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings.

Adicione o segredo compartilhado que você usou em sua configuração NAD para esta

demonstração, o Nexus3xample é usado nesta demonstração.



seção de configuração de TACACS

Salve as alterações clicando no botão Submit.

3. Configuração do TACACS no ISE.

Verifique novamente se a PSN configurada no Nexus 9k tem a opção Device Admin habilitada.



Observação: Habilitar o Device Admin Service NÃO causa uma reinicialização no ISE.



Verificação do recurso PSN Device Admin

Isso pode ser verificado no menu do ISE Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services.

• Crie um perfil TACACS, que retorne a assistência técnica de função para o dispositivo Nexus se a autenticação for bem-sucedida.

No menu ISE, navegue até Workcenters > Device Administration > Policy Elements > Results >

TACACS Profiles e clique no botão Add.

≡ Cisco ISE	Work Centers · Device Ad	ministration	Evaluation Mode 27 Days	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Overview Identities User	Identity Groups Ext Id Sources	Network Resources	Policy Elements More 🗸	
Conditions >	TACACS Profiles			
Network Conditions				
Results 🗸 🗸		Rows/Page	$\begin{array}{c} \mathbf{e} \underline{4} \mathbf{\checkmark} \langle \langle 1 /1 \rangle \rangle \\ \hline \end{array}$	Go 4 Total Rows
Allowed Protocols	$\mathcal G$ Add Duplicate Trash \checkmark Edit			
TACACS Command Sets				
TACACS Profiles	Name	Type Description		
	Default Shell Profile	Shell Default Shell Profile		
	Deny All Shell Profile	Shell Deny All Shell Profile	6	

Perfil TACACS

Atribua um Nome e, opcionalmente, uma descrição.



Nomeando o perfil Tacacs

Ignore a seção Exibição de Atributo de Tarefa e navegue até a seção Exibição Bruta.

E insira o valor shell:roles="helpdesk".

≡ Cisco ISE	Work Centers · Device Administration	🛕 Evaluation Mode 27 Days Q 🕜 🔎 🚳
Overview Identities	User Identity Groups Ext Id Sources Network Resources	Policy Elements More ~
	Name	
Conditions	> Nexus Helpdesk	
Network Conditions	> Description	
Results	 This TACACS profile will be sent if the user is part of the helpdesk team 	
Allowed Protocols	group	
TACACS Command Sets		
TACACS Profiles	Task Attribute View Raw View	
	Profile Attributes	
	shell:roles="helpdesk"	
	Cancel	Save

Adicionando atributo de perfil

Configure o conjunto de políticas que inclui a política de autenticação e a política de autorização.

No menu do ISE, acesse Work Centers > Device Administration > Device Admin Policy Sets.

Para fins de demonstração, o conjunto de políticas padrão é usado. No entanto, outro conjunto de políticas pode ser criado, com condições para corresponder a cenários específicos.

Clique na seta no final da linha.

≡ Ci	sco	ISE		Work Cer	nters · Devic	e Adm	inistration			🛕 Evalua	ation Mode 2	7 Days	Q @	Q	٥
Overview	v	Identities	User Identity	Groups	Ext Id Source	es	Network Resource	es	Policy Elem	ents	More 🗸				
Policy S	Sets								Reset	Reset	Policyset Hi			Save	
(+ s	Status	Policy Set N	ame	Description		Condit	tions	Allow	ed Protocols	Server	Sequence	Hits	Actions	s Viev	N
Q															
	0	Default		Tacacs Default	policy set			Defa	ault Device Adn				ŝ	>]
												Reset		Save	

Página Conjuntos de Políticas de Administração de Dispositivos

Uma vez dentro da configuração do conjunto de políticas, role para baixo e expanda a seção Authentication Policy.

Clique no ícone Add.

Para este exemplo de configuração, o valor do Nome é Autenticação interna e a condição escolhida é o IP do dispositivo de rede (Nexus) (substitua o A.B.C.D.). Esta política de Autenticação usa o Repositório de Identidades de Usuários Internos.

≡ Cisco ISE	Work Centers · Device Administration	A Evaluation Mode 27 Days	Q Q 🖓 🕸
Overview Identities User Identity	Groups Ext Id Sources Network Resources	Policy Elements More \vee	
+ Status Rule Name	Conditions	Use	Hits Actions
Q Search			
Internal Authentication	P Network Access Device IP Address EQUALS A.B.C.D	Internal Users	 ¢
S Default		All_User_ID_Stores > Options	

Política de autenticação

Veja como a condição foi configurada.

Selecione Network Access > Device IP address Dictionary Attribute.

Conditions Studio								Ø
Library		Edi	tor					
Search by Name			Network	Access Device IP Address				8
	L O t 후		t attribute for o	ondition				
: EAP-MSCHAPv2		•			Q	1	Ŀ	Save
🗄 📄 EAP-TLS			Dictionary	Attribute	ID	Info		
			All Dictionaries 🗡	Attribute	ID			
		₽	DEVICE	Device Type				
		₽	DEVICE	Model Name				
			DEVICE	Network Device Profile				
		₽	DEVICE	Software Version				
		₽	Network Access	Device IP Address				
		₽	Network Access	NetworkDeviceName				
								Use

Substitua o comentário <Nexus IP address> pelo IP correto.

Conditions Studio								?	
Library		Editor							~
Search by Name			Network Access	Device IP Address				0	⊗
♥ ☶ □ ▲ ◎ ᇁ ▣ ☞ ☞	9 t 😤	P	Equals 🗸	<nexus address="" ip=""></nexus>					
EAP-MSCHAPv2							i address		
🗄 📑 EAP-TLS							ate Sav	8	
				NEW	NDOR				
						Close	Use		

Adicionando o filtro IP

Clique no botão Use.

Essa condição é atingida apenas pelo dispositivo Nexus configurado, no entanto, se a finalidade for ativar essa condição para uma grande quantidade de dispositivos, uma condição diferente deverá ser considerada.

Em seguida, navegue até a seção Política de autorização e expanda-a.

Clique no ícone + (sinal de adição).

	Cisco I	SE			Work Centers • [Device Ad	ministration			🛕 Evaluation Mode 27 Days Q 🔗 ᇩ						
Over	view I	Identitie	s User Identi	ty Groups	Ext Id Sources	Networ	k Resources	Policy Elem	ents D	evice Admin Poli	cy Sets	More	e ~			
	Statu	is Polic	y Set Name	Descript	ion (Conditions				Allowed F	Protocols /	Server	Seque	nce	Hits	
	Q Se															
	(🔊 De	fault	Tacacs	Default policy set					Default	Device Adr					
	> Authen	tication F	Policy (2)													
	> Authori	ization Po	licy - Local Except	tions												
	> Authorization Policy - Global Exceptions															
	\vee Authori	ization Po	licy (1)													
						Results										
	(+ S	tatus F	tule Name	Cond	litions		Command Sets	8	She	ell Profiles			Hits	Actio	ons	
	(Q §															
							+									
		છ ા	Pefault				DenyAllComma	unds		eny All Shell Profile				ŝ		

Seção de política de autorização

Neste exemplo, NEXUS HELP DESK como o nome da política de autorização foi usado.

V Authorization Policy (1)											
		Results									
🕂 Status Rule Name	Conditions	Command Sets		Shell Profiles		Hits	Actions				
Q Search											
NEXUS HELP DESK	Retwork Access-Device IP Address EQUALS A.B.C.D			Nexus Helpdesk	∞ ~+		ĝ				
🥪 Default		DenyAllCommands		Deny All Shell Profile			ŝ				
					Reset		Save				

Estúdio de condição para Diretiva de Autorização

A mesma condição que foi configurada na Diretiva de Autenticação é usada para a Diretiva de Autorização.

Na coluna Perfis de shell, o perfil configurado antes de Nexus Helpdesk foi selecionado.

Por fim, clique no botão Save.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Na GUI do ISE, navegue para Operations > TACACS > Live Logs, identifique o registro que corresponde ao nome de usuário usado e clique no Live Log Detail do evento de autorização.



Log ao vivo do TACACS

Como parte dos detalhes que este relatório inclui, ele pode ser encontrado em uma seção Resposta, onde você pode ver como o ISE retornou o valor shell:roles="helpdesk"

Despense	{Author-Reply-Status=PassRepl;
Response	AVPair=shell:roles=" helpdesk" ; }

Resposta Detalhada do Log ao Vivo

No dispositivo Nexus:

Nexus9000 login: iseiscool Password: VainillaISE97

Nexus9000# conf t Enter configuration commands, one per line. End with CNTL/Z. Nexus9000(config)# interface ethernet 1/23 % Interface permission denied

Nexus9000(config)# ? interface Configure interfaces show Show running system information end Go to exec mode exit Exit from command interpreter

Nexus9000(config)# role name test % Permission denied for the role

Nexus9000(config)#

Nexus9000(config)# interface loopback 0
% Interface permission denied

Nexus9000(config)# Nexus9000# conf t

Nexus9000(config)# interface ethernet 1/5 Notice that only the commands allowed are listed. Nexus9000(config-if)# ?

no Negate a command or set its defaults show Show running system information shutdown Enable/disable an interface end Go to exec mode exit Exit from command interpreter

```
Nexus9000(config-if)# cdp
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#
```

Troubleshooting

 Verifique se o ISE pode ser acessado a partir do dispositivo Nexus.Nexus9000# ping <Your ISE IP>

```
PING <Seu IP ISE> (<Seu IP ISE> 56 bytes de dados
64 bytes de <seu IP ISE> : icmp_seq=0 ttl=59 time=1,22 ms
64 bytes de <seu IP ISE> : icmp_seq=1 ttl=59 time=0,739 ms
64 bytes de <seu IP ISE> : icmp_seq=2 ttl=59 time=0,686 ms
64 bytes de <seu IP ISE> : icmp_seq=3 ttl=59 time=0,71 ms
64 bytes de <seu IP ISE> : icmp_seq=4 ttl=59 time=0,72 ms
```

- Verifique se a porta 49 está aberta entre o ISE e o dispositivo Nexus. Nexus9000# telnet <Seu IP ISE> 49 Tentando <seu IP ISE> ... Conectado a <seu IP ISE> .
 O caractere de escape é '^]'.
- Use estas depurações:

debug tacacs+ all

Nexus9000#

Nexus9000# 2024 Abr 19 22:50:44.199329 tacacs: event_loop(): chamando process_rd_fd_set 2024 Abr 19 22:50:44.199355 tacacs: process_rd_fd_set: chamada de retorno para fd 6 2024 Abr 19 22:50:44.199392 tacacs: fsrv não consumiu opcode 8421 2024 Abr 19 22:50:44.199406 tacacs: process_implicit_cfs_session_start: inserindo... 2024 Abr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: saindo; estamos no estado de distribuição desabilitada 2024 Abr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: informando para id de sessão de aaa 0 2024 Abr 19 22:50:44.199438 tacacs: process_aaa_tplus_request:Verificando o estado da porta mgmt0 com servergroup IsePsnServers 2024 Abr 19 22:50:44.199451 tacacs: tacacs_global_config(4220): inserindo ... 2024 Abr 19 22:50:44.199466 tacacs: tacacs_global_config(4577): GET_REQ... 2024 Abr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): recuperado o valor de retorno da operação de configuração global do protocolo:SUCCESS 2024 Abr 19 22:50:44.208045 tacacs: tacacs global config(4716): REQ:num server 0 2024 Abr 19 22:50:44.208054 tacacs: tacacs_global_config: REQ:num group 1 2024 Abr 19 22:50:44.208062 tacacs: tacacs_global_config: REQ:num timeout 5 2024 Abr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0 2024 Abr 19 22:50:44.208078 tacacs: tacacs_global_config: REQ:num encryption_type 7 2024 Abr 19 22:50:44.208086 tacacs: tacacs_global_config: return retval 0 2024 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info é preenchido em

aaa_req, então Usando servergroup IsePsnServers

2024 Abr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: inserindo para grupo de servidores, índice 0

2024 Abr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ para índice de grupo de servidor de protocolo:0 nome:

2024 Abr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = no such pss key

2024 Abr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: chamando pss2_getkey 2024 Abr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ got Protocol server group index:2 name:IsePsnServers

2024 Abr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: obteve de volta o valor de retorno da operação do grupo de protocolo:SUCCESS

2024 Abr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: return retval 0 for Protocol server group:IsePsnServers

2024 Abr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Group IsePsnServers encontrado. o vrf correspondente é padrão, source-intf é 0

2024 Abr 19 22:50:44.208224 tacacs: process_aaa_tplus_request: verificando mgmt0 vrf:management em relação a vrf:default do grupo solicitado

2024 Abr 19 22:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080

2024 Abr 19 22:50:44.208272 tacacs: process_aaa_tplus_request:global_src_intf : 0, src_intf local é 0 e vrf_name é padrão

2024 Abr 19 22:50:44.208286 tacacs: create_tplus_req_state_machine(902): informando para id de sessão de aaa 0

2024 Abr 19 22:50:44.208295 tacacs: contagem de máquina de estado 0

2024 Abr 19 22:50:44.208307 tacacs: init_tplus_req_state_machine: informando para id de sessão de aaa 0

2024 Abr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx is NULL deve ser se autor e teste

2024 Abr 19 22:50:44.208327 tacacs: tacacs_servergroup_config: inserindo para grupo de servidoresIsePsnServers, índice 0

2024 Abr 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ para índice de grupo de servidor de protocolo:0 name:IsePsnServers

2024 Abr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: inserindo para grupo de servidores IsePsnServers

2024 Abr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS 2024 Abr 19 22:50:44.208382 tacacs: find_tacacs_servergroup: saindo para grupo de servidores O índice IsePsnServers é 2

2024 Abr 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ:

find_tacacs_servergroup error 0 for Protocol server group IsePsnServers

2024 Abr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS 2024 Abr 19 22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ got Protocol server group index:2 name:IsePsnServers

2024 A2024 Abr 19 22:52024 Abr 19 22:52024 Abr 19 22:5 Nexus9000#

• Executar uma captura de pacote (para ver os detalhes do pacote, você deve alterar as

preferências do Wireshark TACACS+ e atualizar a chave compartilhada usada pelo Nexus e ISE)

No.		Time		Sc De	Protocol		Length	Info				
	66	22:25:08.7	757401		TACACS+		107	R: Aut	horizati	on		
>	Transmi	ssion Cont	rol Proto	col.	Src Port: 4	9. Dst Po	rt: 5886	3. Sea:	1. Ack:	90. Ler	1: 41	
~	TACACS+							-,	-,	,		
	Major Minor Type: Seque > Flags Packe Encry > Decry Au Se Da Ar Ar	r version: r version: Authoriza ence number s: 0x00 (En ion ID: 113 et length: ypted Reply ypted Reply ypted Reply th Status: rver Msg lu ta length: g count: 1 g[0] lengt g[0] value	TACACS+ 0 ition (2) : 2 icrypted p 16115821 29 7 PASS_REP ength: 0 0 h: 22 : shell:r	oayloa PL (Øx Poles=	nd, Multipl 02) "helpdesk"	e Connect:	ions)					

Pacote de autorização TACACS

• Verifique se a chave compartilhada é a mesma no ISE e no Nexus. Isso também pode ser verificado no Wireshark.

CACS+

Major version: TACACS+ Minor version: 1 Type: Authentication (1) Sequence number: 1 Flags: 0x00 (Encrypted payload, Multiple Connections) Session ID: 232251350 Packet length: 43 **Encrypted Request** Decrypted Request Action: Inbound Login (1) Privilege Level: 1 Authentication type: PAP (2) Service: Login (1) User len: 9 User: iseiscool Port len: 1 Port: 0 Remaddr len: 12 Remote Address: Password Length: 13 Password: VainillaISE97

Pacote de autenticação

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.