ACS 5.x: Autenticação TACACS+ e autorização de comando com base no exemplo de configuração de associação de grupo do AD

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Conventions Configuração Configurar o ACS 5.x para autenticação e autorização Configurar o dispositivo IOS Cisco para autenticação e autorização Verificar Informações Relacionadas

Introdução

Este documento fornece um exemplo de configuração de Autenticação TACACS+ e Autorização de Comando com base na associação de grupo do AD de um usuário com o Cisco Secure Access Control System (ACS) 5.x e posterior. O ACS usa o Microsoft Active Directory (AD) como um armazenamento de identidade externa para armazenar recursos, como usuários, máquinas, grupos e atributos.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

 O ACS 5.x é totalmente integrado ao domínio do AD desejado. Se o ACS não estiver integrado ao Domínio do AD desejado, consulte <u>ACS 5.x e posterior: Exemplo de</u> <u>Configuração de Integração com o Microsoft Ative Diretory</u> para obter mais informações para executar a tarefa de integração.

Componentes Utilizados

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

Cisco Secure ACS 5.3

• Software Cisco IOS[®] versão 12.2(44)SE6.

Observação: essa configuração pode ser feita em todos os dispositivos Cisco IOS.

Domínio do Microsoft Windows Server 2003

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configuração

Configurar o ACS 5.x para autenticação e autorização

Antes de iniciar a configuração do ACS 5.x para Autenticação e Autorização, o ACS deve ter sido integrado com êxito ao Microsoft AD. Se o ACS não estiver integrado ao Domínio do AD desejado, consulte <u>ACS 5.x e posterior: Exemplo de Configuração de Integração com o Microsoft Ative Diretory</u> para obter mais informações para executar a tarefa de integração.

Nesta seção, você mapeia dois grupos do AD para dois conjuntos de comandos diferentes e dois perfis do Shell, um com acesso total e outro com acesso limitado nos dispositivos Cisco IOS.

- 1. Faça login na GUI do ACS usando as credenciais de Admin.
- Escolha Users and Identity Stores > External Identity Stores > Ative Diretory e verifique se o ACS ingressou no domínio desejado e também se o status de conectividade é mostrado como connected.

Clique na guia Diretory Groups.

Users and Ide	Users and Identity Stores > External Identity Stores > Active Directory							
Genera	Directory Groups Directory	Attributes						
Connec	tion Details							
Activ	e Directory Domain Name:	MCS55.com						
Please s O User	specify the credentials used to joir name:	this machine to the Active Dir training	ectory Domain:					
Pass	word:							
Click on can sele	Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have successican select the Directory Groups and Directory Attributes to be available for use in policy rules.							
End Use V E V E	r Authentication Settings nable password change nable machine authentication nable Machine Access Restriction	ns						
Connec Joined	Connectivity Status Joined to Domain:mcs55.com Connectivity Status:CONNECTED							
Save Chan	ges Discard Changes	Clear Configuration						

3. Clique em Selecionar.

Users and Identity Stores > External Identity Stores > Active Directory
General Directory Groups Directory Attributes
Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click 'Select' to launch a dialog to select groups from the directory.
Selected Directory Groups:
Group Name
Add A Edit V Replace A Deselect Select Group Name
Example for group format : cisco.com/Users/Domain Users
• = Required fields
Save Changes Discard Changes Clear Configuration

4. Escolha os grupos que precisam ser mapeados para os perfis Shell e conjuntos de comandos na parte posterior da configuração. Click OK.

Exterr	nal User (Groups				•	
Search	Base DN	DC=MCS55,DC=com					
Search	Filter	G	Go				
	Group N	ame		Group Type			
	MCS55.c	com/Users/Domain Guests		GLOBAL	*		
	MCS55.d	om/Users/Network Admins		GLOBAL		E	
	MCS55.c	om/Users/Network Maintenance Team		GLOBAL			
	MCS55.c	com/Users/Schema Admins		UNIVERSAL	-		
OK	OK Cancel Database: Active Directory						
	Use * Searc	for wildcard search (i.e. admin*) ch filter applies to group name and not the fully qualified	l path.				

5. Clique em Save Changes.

Lisers and identity Stores > External identity Stores > Active Directory
Costs and rothing otores - External rothing otores - Marke birectory
General Directory Groups Directory Attributes
Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click 'Select' to launch a dialog to select groups from the directory.
Selected Directory Groups:
Group Name
MCS55.com/Users/Network Admins
MCS55.com/Users/Network Maintenance Team
Add A Edit V Replace A Deselect Select
Group Name
Example for group format : cisco.com/Users/Domain Users
P = Required fields
Read Changes Class Confermation
Save Changes Discaro Changes Clear Configuration

6. Escolha Access Policies > Access Services > Service Selection Rules e identifique o serviço de acesso, que processa a autenticação TACACS+. Neste exemplo, é Default Device Admin.

Access	Access Policies > Access Services > Service Selection Rules Single result selection () Rule based result selection							
Ser	vice Se	lection Po	olicy					
Filt	Filter: Status V Match if: Equals V Enabled V Clear Filter Go V							
		Status	Name	Protocol	Conditions		Results Service	Hit Count
1		0	Rule-1	match Tacacs			Default Device Admin	1
2	2	0	Rule-2	match Radius	4		Default Network Access	0

7. Escolha Access Policies > Access Services > Default Device Admin > Identity e clique em Select ao Iado de Identity Source.



8. Escolha AD1 e clique em OK.

Ident	iity Store		Showing 1-9 of 9	50	• per page 🤇	Go
Filter	: [Match if. 🚽 😡 🔻				
	Name 🔺	Description				
۲	AD1					
0	CN Usemanie	Predefined Certificate Authentication Profile				
0	DenyAccess					
O	Internal Hosts					
0	Internal Users					
0	LUAP	Domain Controller LUAP				
O	NAC Profiler	Default Entry for NAC Profiler				
0	safeword	THIS IS NOT USED nic 2011.11.22				
0	safeword-ias					
			🔣 💽 Page		1 of 1 🕩	
OK	Cancel					

9. Clique em Save Changes.

Access Policies > Access Services > Default Device Admin > Identity					
Single result selection O Rule based result selection					
Identity Source: AD1 Select					
Advanced Options					
Save Changes Discard Changes					

10. Escolha Access Policies > Access Services > Default Device Admin > Authorization e clique em Customize.

6	Coess Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy							
	Devic	e Adn	ninistrati	on Autho	rization Policy		_	
	Filter	Stat	us		Match if: Equals • Enabled •	Clear Filter	Go 🔻	
		121	Status	Name	Conditions	R	esults	Hit Count
		_			Compound Condition	Shell Profile	Command Sets	
			No data	to display	y			
			Default		If no rules defined or no enabled rule matches.	Permit Access	DenyAlCommands	1
	Create							
	Care Channel Discord Channel							
	Save	unang	es j U	iscard Ch	anges			

11. Copie AD1:ExternalGroups da seção Available to Seleted de Customize Conditions e depois mova o Perfil do Shell e os Conjuntos de Comandos da seção Available to Seleted de Customize Results. Agora clique em OK.

Customize Conditions			
Available:		Selected:	
ACS Host Name	_	AD1:ExternalGroups	A
Authentication Method			
Authentication Status			
Compound Condition	- <		
Device Filter			
Device IP Address			
Eap Authentication Method	>>		
Eap Tunnel Building Method			
End Station Filter	+		
Customize Results			
Available:		Selected:	
		Shell Profile	
		Command Sets	
	<		
	\gg		
OK Cancel			

12. Clique em Create para criar uma nova regra.

Acc Sta	ess F anda	olicies	s > Access licy <u>Exc</u>	s Services	> Default Device Admin > Authorization >Ilcy			
D	evic	e Adn	ninistrati	on Autho	rization Policy			
	Filter: Status • Match if: Equals • Enabled • Clear Filter Go •							
			Status	Name	Conditions AD1:ExternalGroups	R Shell Profile	command Sets	Hit Count
			No data	to displa	/			
	**		Default		If no rules defined or no enabled rule match	es. Permit Access	DenyAllCommands	0
	Create Duplicate Edit Delete A Move to Y Customize Hit Count							
s	Create Discard Changes							

13. Clique em Selecionar na condição AD1:ExternalGroups.

General Name: Rule-1	Status: Loobled		
Name. Pule-1	Status. Enabled		
The Customize bu conditions and res	tton in the lower right area ults are available here for u	of the policy rules screen cor use in policy rules.	ntrols which policy
Conditions			
AD1:LxtemalGroups:			
contains any 👻			
			A
			-
Select Deselect	Clear		
Results			
Shell Profile. Permit Access	Sele	act	
Command Sets:			
	<u>^</u>		
	+		
K Cancel			liel

14. Escolha o grupo ao qual você deseja conceder acesso total no dispositivo IOS Cisco. Click OK.

String	J Enum Definition	Showing 1-2 of 2 50 🔻 per page Go
Filter	- ■ Match if: ■ G0 ▼	
	Enum Name	•
V	MCS55.com/Users/Network Admins	
	MCS55.com/Users/Network Maintenance Team	
		< Page 1 of 1 ▶ ▶
ОК	Cancel	

15. Clique em Select no campo Shell Profile.

The Customize button in the lower right area of the policy right conditions and results are available here for use in policy ru	ules screen controls which policy ules.
Conditions Image: Conditions Image: Contains any	
MCS55.com/Users/Network Admins	×.
Select Deselect Clear	
Results Shell Profile: Permit Access Command Sets:	Ĩ
Select Deselect	
DK Cancel	lleip

16. Clique em Create para criar um novo Shell Profile para usuários com acesso total.

Shell	Profiles	Showing 1-2 of 2 50 🔹 per page Go
Filter:	✓ Match if: ✓ Go ▼	
	Name Description	
0	DenyAccess	
Ô	Permit Access	
Grea	te Duplicate Edit Delete	I ● Page 1 of 1 ▶ ▶
ОК	Cancel	Help

17. Forneça um Nome e Descrição (opcional) na guia Geral e clique na guia Tarefas comuns.

General Common Tasks Custom Attributes						
🌣 Name:	Full-Privilege					
Description:	To push default privilege 15 for IOS					
Required fields						

18. Altere Default Privilege e Maximum Privilege para Static com o Valor 15. Clique em Submit.

General Common	Tasks Custom Attributes
Privilege Level	
Default Privilege:	Static - Value 15 -
Maximum Privilege:	Static - Value 15 -
Shell Attributes	
Access Control List:	Not in Use 👻
Auto Command:	Not in Use 👻
No Callback Verify:	Not in Use 👻
No Escape:	Not in Use 👻
No Hang Up:	Not in Use 👻
Timeout:	Not in Use 🔻
Idle Time:	Not in Use 👻
Callback Line:	Not in Use 👻
Callback Rotary:	Not in Use 👻



19. Agora, escolha o Perfil do shell de acesso completo recém-criado (Privilégio completo neste exemplo) e clique em OK.

Shell	Profiles
Filter:	→ Match if: → Go ▼
	Name Description
\bigcirc	DenyAccess
۲	Full-Privilege To push default privilege 15 for IOS
۲	Permit Access
Crea	ate Duplicate Edit Delete
OK	Cancel

20. Clique em Selecionar no campo Conjuntos de Comandos.

The Customize button in the lower right area of the policy rules screen cor conditions and results are available here for use in policy rules.	ntrols which policy
Conditions Image: Conditions Image: Contains any	
MCS55.com/Users/Network Admins	*
Select Deselect Clear	
Results Shell Profile: Full-Privilege Select	E
Command Sets:	
OK Cancel	+

21. Clique em Create para criar um novo conjunto de comandos para usuários de Full-Access.

Command Sets	Showing 1-1 of 1 50 - per page Go				
Filter: Vatch if: Go 🔻					
Command Set Name Description					
DenyAllCommands					
Create Duplicate Edit Delete [File Operations Export M Page 1 of 1 P M					
OK Cancel	Help				

22. Forneça um Nome e verifique se a caixa de seleção ao lado de Permitir qualquer comando que não esteja na tabela abaixo está marcada. Clique em Submit.

Observação: consulte <u>Criação, Duplicação e Edição de Conjuntos de Comandos para</u> <u>Administração de Dispositivos</u> para obter mais informações sobre Conjuntos de Comandos.

		-	
Name:	Full-Access		
Description	1:		
2			
Permit any	command that is not in the table	pelow	
Grant	Command	Arguments	
		A	
Add A	Edit V Deplace A De	eta	
HUUM	Edit V Replace / De	1010	
Grant	Command	Arguments	
Permit	•		
	and/Arguments from Command S	et: DenyAllCommands -	
Select Comm			

23. Click OK.

Com	nand Sets
Filter	• Match if: • Go •
	Command Set Name Description
	DenyAllCommands
V	Full-Access
Crea	ate Duplicate Edit Delete File Operations Export
OK	Cancel

24. Click OK. Isso conclui a configuração da Regra-1.

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	•
Conditions Iml_AD1:ExternalGroups: contains any	
MCS55.com/Users/Network Admins	
Select Deselect Clear Results Shell Profile. Full-Privilage Command Sets: Select	
Full-Access	
	Help

25. Clique em Criar para criar uma nova Regra para usuários com acesso limitado.

E	Access Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization							
	Filter. Status Match if. Equals Enabled Clear Filter Go							
	Status Name Conditions AD1:ExternalGroups			R Shell Profile	esults Command Sets	Hit Count		
	1	1 🖸 \varTheta Rule_1 contains any (MCS55.com/Users/Network Admins)			Full-Privilege	Full-Access	0	
	** Default If no rules defined or no enabled rule matches.			Permit Access	DenyAllCommands	0		
	Creat	e •	Duplics	te • (Edit Delete 🔨 Move to 💟			Customize Hit Count
(Save (Crea	te s Di	scard Cha	nges			

26. Escolha AD1:ExternalGroups e clique em Select.

					4
General					
Name: Rule 2	Status:	Enabled -	0		
The Customize b conditions and re	utton in the lov sults are avail	wer right area o able here for us	f the policy rules screen cor se in policy rules.	ntrols which policy	
Conditions					
AD1.ExternalGroups.					
contains any -					
				^	
					≣
				T	
Select	Clear				
Results					
Shell Profile. Permit Acce	\$8	Sele	st.		
Command Sets:					
	-				
		1.61			
		Y			
					-
OK Cancel				_ l le	lp

27. Escolha o(s) grupo(s) ao(s) qual(is) você deseja conceder acesso limitado e clique em OK.

String Enum Definition					
Filter: Match if: Go					
Enum Name					
MCS55.com/Users/Network Admins					
MCS55.com/Users/Network Maintenance Team					
OK Cancel					

28. Clique em Select no campo Shell Profile.

Conditions		
AD1:Extems	Groups:	
contains any	▼	
MCS55.com/Us	ers/Network Maintenance Te	am A
Select	Deselect Clear	
Results		
Shell Profile:	Permit Access	Select
Command Sets:		<u>N</u>
		* ·

29. Clique em Create para criar um novo Shell Profile para acesso limitado.

Shell Profiles				
Filter	-	Match if: Go 💌		
	Name 🔺	Description		
\odot	DenyAccess			
0	Full-Privilege	To push default privilege 15 for IOS		
\bigcirc	Permit Access			
	t. Dualizat			
Create Duplicate Edit Delete				
OK	Cancel			

30. Forneça um Nome e Descrição (opcional) na guia Geral e clique na guia Tarefas comuns.

31. Altere o Privilégio padrão e o Privilégio máximo para Estático com valores 1 e 15 respectivamente. Clique em Submit.

Default Privilege:	Static	-	Value	1 👻]	
Maximum Privilege:	Static	-	Value	15 👻		
Shell Attributes						
Access Control List:	Not in l	Jse 🔻				
Auto Command:	Not in l	Jse 🔻				
No Callback Verify:	Not in l	Jse 🔻				
No Escape:	Not in U	Jse 👻				
No Hang Up:	Not in l	Jse 👻				
Timeout:	Not in l	Jse 🔻				
Idle Time:	Not in l	Jse 👻				
Callback Line:	Not in l	Jse 👻				
Callback Rotary:	Not in (Jse 🔻				
= Required fields						

32. Click OK.

Shell Profiles					
Filter:	•	Aatch if:			
	Name 🔺	Description			
۲	DenyAccess				
\odot	Full-Privilege	To push default privilege 15 for IOS			
۲	Limited-Privilege	To push default privilege 1 for IOS			
0	Permit Access				
Create Duplicate Edit Delete					
OK	OKCancel				

33. Clique em Selecionar no campo Conjuntos de Comandos.

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	
Conditions	
AD1:ExternalGroups:	
contains any	
MCS55.com/Users/Network Maintenance Team	
Select Deselect Clear	
Results	
Shell Profile: Limited-Privilege Select	
Command Sets:	
Select Deselect	
OK Cancel	Hel

34. Clique em Criar para criar um novo Conjunto de Comandos para o grupo de acesso limitado.

Command Sets				
Filter	• Match if: • Go •			
	Command Set Name Description			
	DenyAllCommands			
	Full-Access			
Crea	ate Duplicate Edit Delete [File Operations Export			
OK	Cancel			

35. Forneça um Nome e verifique se a caixa de seleção ao lado de Permitir qualquer comando que não esteja na tabela abaixo não está marcada. Clique em Adicionar depois de digitar show no espaço fornecido na seção command e escolha Permit na seção Grant para que somente os comandos show sejam permitidos para os usuários no grupo de acesso limitado.

General		
🌣 Name:	Show-Access	
Description	n:	
Permit any	/ command that is not in the table below	Argumente
Grant	Command	Arguments
Add A	Edit V Replace A Delete	
Grant	Command	Arguments
Permit	✓ show	
Select Comm	and/Arguments from Command Set:	DenvAllCommands -
		Select
1		

36. Da mesma forma, adicione outros comandos a serem permitidos para os usuários em um grupo de acesso limitado com o uso de Add. Clique em Submit.

Observação: consulte <u>Criação, Duplicação e Edição de Conjuntos de Comandos para</u> <u>Administração de Dispositivos</u> para obter mais informações sobre Conjuntos de Comandos.

General		
Name:	Show-Access	
Description:		
Permit any	command that is not in the table below	
Grant	Command	Arguments
Permit Permit	show	
Permit	enable	
Add /\	Edit V Replace A Delete	
Grant	Command	Arguments
Permit	▼	
Select Comma	nd/Arguments from Command Set:	DenyAllCommands
bmit Cano	el	

37. Click OK.

Command Sets
Filter: Match if: Go
Command Set Name Description
DenyAllCommands
Full-Access
Show-Access
Create Duplicate Edit Delete File Operations Export
OKCancel

38. Click OK.



The Customize button in the lower right area of the policy rules screen con conditions and results are available here for use in policy rules.

Con	diti	ons
~~		~

AD1:ExternalGroups:
contains any
MCS55.com/Users/Network Maintenance Team
Select Clear
Results
Shell Profile: Limited-Privilege Select
Command Sets: Show-Access
Select Deselect
OK Cancel

39. Clique em Save Changes.

Ľ	Access Policies > Access Services > Default Device Admin > Authorization								
	Device Administration Authorization Policy								
	Filter	Filter: Status - Match if: Equals - Enabled - Clear Filter Go -							
			Status	Name	Conditions AD1:ExternalGroups	Re Shell Profile	command Sets	Hit Count	
	1			Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0	
	2		Θ	Rule-2	contains any (MCS55.com/Users/Network Maintenance Team)	Limited-Privilege	Show-Access	0	
		** Default If no rules defined or no enabled rule matches.					DenyAllCommands	0	
Create • Duplicate • Edit Delete 🛆 Move to V						ustomize Hit Count			
Save Changes Discard Changes									

40. Clique em Create para adicionar o dispositivo Cisco IOS como um AAA Client no ACS.

Network Resources > Network Devices and AAA Clients						
Network Devices						
Filter: IP Address • Match if: Equals • 192.168.26.7 Clear Filter Go	-					
Name IP Address Description NDG:Location NDG:Device Type						
No data to display						
Create Duplicate Edit Delete File Operations Export						

41. Forneça um nome, endereço IP, segredo compartilhado para TACACS+ e clique em Enviar.

Network Resources > Network De	vices and AVAClients > Create			
Name: lab-router Description:				
Network Device Groups				
Location	All Locations	Select		
Device Type	All Device Types	Select		
IP Address Single IP Address	 IP Range(s) By Mask 	Authentication	Options	
IP: 192.168.26.7		Shared Sec	cret: •••••	Show
		☐ Single © Legac ○ TACA ▼ RADIUS Shared Se CoA port:	Connect Device y TACACS+ Single Connect Sup CS+ Draft Compliant Single Connect ecret:	oport nect Support
e Required fields				
Submit Cancel				

Configurar o dispositivo IOS Cisco para autenticação e autorização

Conclua estas etapas para configurar o dispositivo Cisco IOS e o ACS para Autenticação e Autorização.

1. Crie um usuário local com privilégio total para fallback com o comando username, como mostrado aqui:

username admin privilege 15 password 0 cisco123!

2. Forneça o endereço IP do ACS para habilitar o AAA e adicionar o ACS 5.x como servidor TACACS.

aaa new-model
tacacs-server host 192.168.26.51 key cisco123

Observação: a chave deve corresponder ao segredo compartilhado fornecido no ACS para este dispositivo IOS Cisco.

3. Teste a alcançabilidade do servidor TACACS com o comando test aaa como mostrado.

test aaa group tacacs+ user1 xxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+

User was successfully authenticated.

A saída do comando anterior mostra que o servidor TACACS está acessível e que o usuário foi autenticado com êxito.

Observação: User1 e a senha xxx pertencem ao AD. Se o teste falhar, verifique se o segredo compartilhado fornecido na etapa anterior está correto.

4. Configure o login e habilite as autenticações e use as autorizações de execução e de comando como mostrado aqui:

aaa authentication login default group tacacs+ local aaa authentication enable default group tacacs+ enable aaa authorization exec default group tacacs+ local aaa authorization commands 0 default group tacacs+ local aaa authorization commands 1 default group tacacs+ local aaa authorization commands 15 default group tacacs+ local aaa authorization config-commands

Observação: as palavras-chave Local e Enable são usadas para fallback para o usuário local do Cisco IOS e enable secret, respectivamente, se o servidor TACACS estiver inacessível.

Verificar

Para verificar a autenticação e o login de autorização no dispositivo IOS Cisco através de Telnet.

 Faça Telnet para o dispositivo Cisco IOS como user1 que pertence ao grupo de acesso completo no AD. O grupo Administradores de Rede é o grupo no AD que é mapeado para Perfil do Shell de Privilégio Completo e Comando de Acesso Completo no ACS. Tente executar qualquer comando para garantir que você tenha acesso total.

```
username: user1
password:
router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#router rip
router1(config-router)#version 2
router1(config-router)#exit
router1(config)#exit
router1(config)#exit
```

2. Execute Telnet para o dispositivo Cisco IOS como o usuário2 que pertence ao grupo de acesso limitado no AD. (O grupo Network Maintenance Team é o grupo no AD que é mapeado para Limited-Privilege Shell Profile e Show-Access Command set no ACS). Se você tentar executar qualquer comando diferente dos mencionados no conjunto de comandos Show-Access, receberá um erro Command Authorization Failed, que mostra que o usuário2 tem acesso limitado.

```
username: user2
password:
router1>enable
password:
router1#
router1#
routerlfshow version
Cisco IOS Software, C3550 Software (C3550-IPBASEK9-M), Version 12.2(44)5E6, RELEASE S
OFTWARE (fcl)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text base: 0x00003000, data base: 0x00EA3DE8
ROM: Bootstrap program is C3550 boot loader
routerl uptime is 16 hours, 46 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-44.SE6.bin"
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stgrg.html
If you require further assistance please contact us by sending email to
export@ciscs.com.
routerl‡cont t
Command authorization failed.
router1#wr mem
Command authorization failed.
router1#
```

3. Faça login na GUI do ACS e inicie o Monitoring and Reports viewer. Escolha AAA Protocol > TACACS+Authorization para verificar as atividades executadas por user1 e user2.

ſ	🛃 🖳 🕺								
	Showing Pag	ge 1 of 1				Gote	Page: Go		
ŀ	AAA Protocol > TACACS+ Authorization								
ŀ	Authorization Status : Date :	Pass or Fail June 08, 2012							
	Generated on June 8	2012 11:57:34 AM	IST						
é	Reload								
	 ✓=Pass X=Fail 	4-Click for deta	ila						
	ACS View Timestamp	ACS Timestamp	Status	Details	Fallure Reason	User Name	Command Set	Shell Profile	Network _e Device
	Jan 8,12 6 21 19,410 AM	han 0,12 6:21:19.393 AM		Q,		user2	[CadAVecit]		lab-router 1
l	Net 8,12 4:20:59,800 AM	bin 8,12 6:20:59,799 AM		4	13005 Command Billed to match a Permit rale	10er2	[Ond/Wheele memory]		bb-room 1
I	Inn 1,12 6:20 56:566 AM	han 9,12 6:20:56 950 AM	*	9	13025 Command the last to match a Permit rule	2002	[CndAV+configure terminal]		lab-costar 1
I	Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50:036 AM	1	- 14	9	2002	[Cmd/W-show version]		Mercuter 1
I	No. 8,12 8:20 78:508 AM	han 8,12 6:20:38,490 AM	1	9	Commands run by	wer2	[Cad&V=eable]		lab-roozer 1
I	Not. 8.12 (0:20:34.426 AM	Jun 8,12 6:20:34.406 AM	1	<u>_</u>	user 2	1002	[CmdAV=]	Limited-Privilege	lab-costar 1
ľ	Jun 8,12 6:20:02.616 AM	han 9,12 6:20:02.596 AM	~	Q,		usel	[CndAVweit]		lab-router 1
	No. 8.12 6:20:00.263 AM	Jun 8,12 6:20:00.246 AM	*	- 4L	Commands run by	and a	[CndAV-venion 2]		lab-roster 2
	han 9,12 6:19:57.203 AM	Jan 8.12 6:19:57.260 AM	1	94	user1	<u>seel</u>	[Cmd/Wrrouterrip]		lab-rourer 1
	Jun 8,12 6:19:55:103 AM	Jun 8,12 6.19:55:076 AM	1	- 44		peerl	[CndAV-configure terminal]		Mercuter 1
	No. 8,12 4:19:52:763 AM	3xt 8.12 6:19:52 740 AM		9		wet	[Cmd-8V=]	Pall-Privilege	ab-rouge

Informações Relacionadas

- <u>Cisco Secure Access Control System</u>
- Suporte Técnico e Documentação Cisco Systems

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.

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.