ACS 5.x:基於AD組成員身份的TACACS+身份驗 證和命令授權配置示例

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>組態</u> 配置ACS 5.x以進行身份驗證和授權</u> <u>配置Cisco IOS裝置以進行身份驗證和授權</u> <u>驗證</u> <u>相關資訊</u>

<u>簡介</u>

本文提供使用Cisco Secure Access Control System(ACS)5.x及更高版本根據使用者的AD群組成員 身分設定TACACS+驗證和命令授權的範例。ACS使用Microsoft Active Directory(AD)作為外部身份 庫來儲存資源,例如使用者、電腦、組和屬性。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

 ACS 5.x已完全整合到所需的AD域。如果ACS未與所需的AD域整合,請參閱ACS 5.x及更高版 <u>本:與Microsoft Active Directory整合配置示例</u>以瞭解詳細資訊,以便執行整合任務。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco安全ACS 5.3
- Cisco IOS[®]軟體版本12.2(44)SE6。注意:可以在所有Cisco IOS裝置上完成此配置。
- Microsoft Windows Server 2003域

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u> 組態</u>

配置ACS 5.x以進行身份驗證和授權

在開始配置ACS 5.x進行身份驗證和授權之前,應該已經將ACS成功與Microsoft AD整合。如果 ACS未與所需的AD域整合,請參閱<u>ACS 5.x及更高版本:與Microsoft Active Directory整合配置示例</u> 以瞭解詳細資訊,以便執行整合任務。

在本節中,您將兩個AD組對映到兩個不同的命令集和兩個Shell配置檔案,一個在Cisco IOS裝置上 具有完全訪問許可權,另一個具有有限訪問許可權。

- 1. 使用管理員憑據登入ACS GUI。
- 選擇Users and Identity Stores > External Identity Stores > Active Directory, 並驗證ACS是否 已加入所需的域,以及連線狀態是否顯示為已連線。按一下Directory Groups選項卡。

Users and Identity Stores > External Identity Stores	s > Active Directory
General Directory Groups Directory	Attributes
Connection Details	
Active Directory Domain Name:	MCS55.com
Please specify the credentials used to join	this machine to the Active Directory Domain:
Username:	training
Password:	•••••
You may use the Test Connection Button to	o ensure credentials are correct and Active Directory Domain is reachable.
	Test Connection
Click on 'Save Changes' to connect to the A	Active Directory Domain and save this configuration. Once you have success
can select the Directory Groups and Direct	ory Autobutes to be available for use in policy fules.
End Uses Authentication Cattions	
Enable password change	
Enable machine authentication	
Enable Machine Access Restriction	S
Connectivity Status	
Joined to Domain:mcs55.com Connec	ctivity Status:CONNECTED
• = Remired fields	
- Save Changes Discard Changes	Clear Configuration

3. 按一下「Select」。

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 policy rules. Click 'Select' to launch a dialog to select groups from	options in group mapping conditions in 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	
E存需安到映到距值後期的SNEII距值储条和叩力集的组。	。按一下·UK」(唯正)。
Search Base DN DC=MCS55,DC=com	
Search Filter Go]
Group Name	Group Type
MCS55.com/Users/Domain Guests	GLOBAL
MCS55.com/Users/Network Admins	GLOBAL
MCS55.com/Users/Network Maintenance Team	GLOBAL
MCS55.com/Users/Schema Admins	UNIVERSAL
OKCancel	
Database: Active Directory Use * for wildcard search (i.e. admin*) Search filter applies to group name and not the fully qualified pa	th.

5. 按一下「Save Changes」。

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
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
Save Changes Discard Changes Clear Configuration

6. 選擇Access Policies > Access Services > Service Selection Rules,並確定處理TACACS+身 份驗證的接入服務。在本示例中,它是Default Device Admin。

Access P	ccess Policies > Access Services > Service Selection Rules							
• Sir	Single result selection Rule based result selection							
Servi	ce Sel	ection Po	olicy					
Filter	State	JS 🔻	Match if:	Equals -	Enabled	Clear Filter	Go 🔻	
		Status	Name	Protocol	Conditions		Results Service	Hit Count
1		0	Rule-1	match Tacacs	•		Default Device Admin	1
2		Θ	Rule-2	match Radius	*		Default Network Access	0

7. 選擇Access Policies > Access Services > Default Device Admin > Identity,然後按一下 Identity Source旁邊的Select。

	Acces	s Policies >	Access Services > Default Device Admin > Identity			
	۲	Single rest	ult selection 💿 Rule based result selection			
	lden	tity Source	Internal Users Select			
			Advanced Options			
	Sa	ve Changes	Discard Changes			
3. j	選擇AD)1,然後按─ tv:5tore	-下OK。	50 ·	per page	Go
	Filtor	-	Match if Gol 💌		hei heile (
	T inter.	Nama .	Devriction			
	0	AD1				
	0	CN Usemame	Predefined Certificate Authentication Profile			
	0	DenyAccess				
	0	Internal Hosts				
	0	Internal Users				
	0	LUAP	Domain Controller LDAP			
	0	NAC Profiler	Default Entry for NAC Profiler			
	0	safeword	THIS IS NOT USED nic 2011.11.22			
	0	saleword-ias				
			R Page	-	l of 1 🕞	
	OK	Cancel				

9. 按一下「Save Changes」。

Access Policies > Access Services > Default Device Admin > Identity			
Single resu	lection		
Identity Source:	AD1	Select	
	 Advanced Options 	Section 1	
Save Changes	Discard Changes		

10. 選擇Access Policies > Access Services > Default Device Admin > Authorization,然後按一 下Customize。

ccess P Standa	olicies rd Po	i > Access	s Senices	 Default Device Admin > Authorization Default Device Admin > Authorization 			
Device Administration Authorization Policy Filter: Status Match if: Equals Version Policy Clear Filter Go							
		Status	Name	Conditions Compound Condition	R Shell Profile	esults Command Sets	Hit Count
		No data	to displa	У			
		Default		If no rules defined or no enabled rule matches.	Permit Access	DenyAlCommands	1
** Default If no rules defined or no enabled rule matches. Permit Access DenyAlCommands 1 Create • Duplicate • Edit Delete ^ Move to •							

11. 將AD1:ExternalGroups從「可用」(Available)複製到「自定義條件」(Customize Conditions)的「選定」(Selected)部分,然後將「殼輪廓」(Shell Profile)和「命令集」 (Command Sets)從「可用」(Available)移動到「自定義結果」(Customize Results)的「選定 」部分。現在按一下**OK**。

Customize Conditions	
Available: Selected:	
ACS Host Name AD1:ExternalGroups	* <u> </u>
Authentication Method	
Authentication Status	
Compound Condition	
Device Filter	
Device IP Address	
Ean Authentication Method	
Eap Tunnel Building Method	
End Station Filter	- L
Customize Results	
Available: Selected:	
Shell Profile	
Command Sets	
Cancel ここでにででした。 ここでにので、こので、こので、こので、こので、こので、こので、こので、こので、こので、こ	
Cancel こので、Cancel こので、Cancel こので、Cancel こので、Cancel こので、Cancel こので、Cancel	
OK Cancel このたい Cancel この下 Create以建立新規則。 こccss Policies > Access Services > Default Device Admin > Authorization Standard Policy! Exception Policy	
Cancel Cancel この下 Create以建立新規則。 Cocess Policies > Access: Services > Default Device Admin > Authorization Standard Policyl Exception Policy Device Administration Authorization Policy	
Cancel Cancel C - 下Create以建立新規則。 Cess Policies > Access Services > Default Device Admin > Authorization Standard Policy! Exception Policy Device Administration Authorization Policy Filter: Status ・ Match if Equals ・ Enabled ・ Clear Filter Ga ▼	
Cancel C Cancel C Cancel C Cancel C Cancel C Conces > Access Services > Default Device Admin > Authorization C Coss Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization Policy Filter: Status Match if: Equals Enabled Clear Filter G Conditions Results	Hit Count
OK Cancel スー下Create以建立新規則。 スー下Create以建立新規則。 ccess Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization Policy Filter: Status Match if Equals Enabled Clear Filter Command Sets Name AD1.ExternalGroups Shell Profile Command Sets No date to diverse Device Adminent Sets Shell Profile Command Sets	Hit Count
Cancel Cancel Cancel Corr Create以建立新規則。 Coss Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization Policy Filter: Status ・ Match if Equals ・ Enabled ・ Clear Filter Go ▼ Status Name AD1.ExternalGroups Shell Profile Command Sets No data to display ************************************	Hit Count
Cancel Cancel Cancel Cancel Constant and and policy in the policy of the the policy	Hit Count
Cancel こので、Cancel こので、Cancel <	Hit Count 0 Customize Hit Count
Cancel Concel Concel Concel Concel Concel Concested 以建立新規則。 Cosss Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization Policy Filter Status Match if Equals Enabled Cear Filter Go Command Sets No data to display Conditions Results Status Name AD1 ExternalGroups Shell Profile Command Sets No data to display Cease Conditions Results Shell Profile Command Sets No data to display Cease Conditions Command Sets No data to display Cease Conditions Command Sets No data to display Cease Conditions Command Sets No data to display Cease C	Hit Count 0 Customize Hit Count

13. 在AD1:ExternalGroups條件中按一下Select。

General Name: Rule-1	Status: Lnabled •	. 6	
The Custom	ize button in the lower right area on nd results are available here for u	of the policy rules screen controls which policy use in policy rules.	
0			
Conditions			
contains any			
,			
		~	
		~	
Select Deselec	l Clear		
Results			
Shell Profile. Permit.	Access Sela	set	
Command Sets:			
	L <u>∞</u> .		
K Cancel	+		He

14. 選擇要在Cisco IOS裝置上提供完全訪問許可權的組。按一下「OK」(確定)。

String	g Enum Definition	Showing 1-2 of 2 50	 per page Go
Filter	- Match if: - Go - Go		
	Enum Name		•
	MCS55.com/Users/Network Admins		
	MCS55.com/Users/Network Maintenance Team		
		M Page	1 of 1 🕨 🕅
ОК	Cancel		

15. 在「外殼配置檔案」(Shell Profile)欄位中按一下**選擇**。

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 Image: Contains any	
MCS55.com/Users/Network Admins	
Select Deselect Clear Results Shell Profile: Permit Access Command Sets: Select	E
Select Deselect	

16. <u>按一下Create</u>可為完全訪問使用者建立新的Shell Profile。

Shell	Profiles	Showing 1-2 of 2	50 🝷	per page	Go
Filter:	✓ Match if: ✓ Go ▼				
	Name - Description				
O	DenyAccess				
O	Permit Access				
Grea	te Duplicate Edit Delete	🔳 🔳 Page		1 of 1 🕩	
OK	Cancel				Help

17. 在General索引標籤中提供Name和Description(可選),然後按一下Common Tasks索引標

General Cor	mmon Tasks Custom Attributes	
🌣 Name:	Full-Privilege	
Description:	To push default privilege 15 for IOS	
Required fiel	ds	

General Common 1	asks 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. 現在,選擇新建立的完全訪問**外殼配置檔案**(在本示例中為「完全許可權」),然後按一下 OK。

Shell I	Profiles	
Filter:		Match if: 🗾 🗸 Go 💌
	Name 🔺	Description
\bigcirc	DenyAccess	
۲	Full-Privilege	To push default privilege 15 for IOS
\odot	Permit Access	
Creat	te Duplicate	Edit Delete
ок	Cancel	

20. 在「命令集」欄位中按一下選擇。

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	
C AD1:ExternalCmups:	
contains any	
MCS55.com/Users/Network Admins	
Select Deselect Clear	
Results	
Shell Profile: Full-Privilege Select	-
Command Sets:	
Select	
OK Cancel	llelp

21. 按一下Create以為Full-Access使用者建立新的命令集。

Comm	and Sets	Showing 1-1 of 1 5	0 🔻 per page Go
Filter:	✓ Match if: Go ▼		
	Command Set Name 🔺 Description		
	DenyAllCommands		
Creat	Duplicate Edit Delete File Operations Export	M Page	1 of 1 🕨 🕅
OK	Cancel		Help

22. 提供**名稱**,並確保選中Permit any command that is not in the table旁邊的覈取方塊。按一下 「Submit」。註:有關命令集的詳細<u>資訊,請參閱建立、複製和編輯</u>裝置管理的命令集。

	General Name: Descripti Permit a	Full-Access on:		*
	Grant Add /\ Grant	Command Edit V Replace A Delete Command	Arguments *	
[23. 技	Permit Select Com Submit C 安一下「O	▼ mand/Arguments from Command Set: ancel K」(確定)。	DenyAllCommands Select	
	Comma	nd Sets		
	Filter:	✓ Match	if: Go 🔻	
	C	ommand Set Name	Description	
		ull-Access		
	Create	Duplicate Edit D	elete File Operations Export	
	QK	Cancel		

24. 按一下「**OK**」(確定)。這樣就完成了**Rule-1**的配置。

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 IVI AD1:LxternalGroups: contains any	
MCS55.com/Users/Network Admins	
Select Deselect Clear Results Shell Profile. Full-Privilage Command Sets: Select	
	Help
5. 按一下 Create 可為受限訪問使用者創 建新 規則。	- napr

Device	a Adm	inistratio	n Authori	ization Policy			
Filter.	Statu	IS	-	Match if. Equals	Filter Go 🔻	,	
		Status	Name	Conditions AD1:ExternalGroups	R/ Shell Profile	csults Command Sets	Hit Count
1		Θ	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	D
Create		Duplical	te •	Edit Delete \land Move to V			Customize Hit Cou

26. 選擇AD1:ExternalGroups,然後按一下Select。

			4
General			
Name: Rule 2	Status: Enabled	- 0	
The Customize but conditions and resu	ton in the lower right are its are available here fo	rea of the policy rules screen controls which policy or use in policy rules.	
Conditions Image: AD1.ExternalGroups. contains any			
		A. 197	1
Select Deselect (Clear		
Shell Profile. Permit Access	5	Select	
Command Sets:			
OK Cancel			Help

27. 選擇要提供有限訪問許可權的組(或)組,然後按一下**確定**。

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

28. 在「外殼配置檔案」(Shell Profile)欄位中按一下選擇。

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: Permit Access Select	
Command Sets:	
Select Deselect	
OK Cancel	Help

29. 按一下Create以建立新的Shell Profile以進行受限訪問。

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

30. 在General 索引標籤中提供Name和Description(可選),然後點選Common Tasks索引標籤



31. 將Default Privilege和**Maximum Privilege**更改為**Static**,分別使用值1和**15**。按一下「 **Submit**」。

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 👻		
= Required fields			

32. 按一下「**OK**」(確定)。

Shell	Profiles	
Filter:	- M	atch if: 🔹 🖌 🕞 🗢
	Name 🔺	Description
\odot	DenyAccess	
\odot	Full-Privilege	To push default privilege 15 for IOS
۲	Limited-Privilege	To push default privilege 1 for IOS
0	Permit Access	
Crea	te Duplicate	Edit Delete
OK	Cancel	

33. 在「命令集」欄位中按一下選擇。

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	Help

34. 按一下Create為受限訪問組建立新的命令集。

Comn	nand Sets
Filter:	· Match if: ▼ Go ▼
	Command Set Name Description
	DenyAllCommands
	Full-Access
Crea	Duplicate Edit Delete File Operations Export
OK	Cancel

35. 提供**名稱**,並確保未選中**Permit any command that is not in the table**旁邊的覈取方塊。在**命** 令部分提供的空白處鍵入**show**後,單擊Add,然後在**Grant**部分中選擇**Permit**,以便僅允許有 限訪問組中的使用者使用show命令。

General		
Name:	Show-Access	
Description		
Permit any	command that is not in the table below	
Grant	Command	Arguments
Add A	Edit V Replace A Delete	
Grant	Command	Arguments
Permit	▼ show	
Select Comm	and/Arguments from Command Set:	DenyAllCommands - Select
ubmit Can	icel	

36. 類似地,使用Add為有限訪問組中的使用者新增任何其他允許使用的命令。按一下「 Submit」。註:有關命令集的詳細<u>資訊,請參閱建立、複製和編輯</u>裝置管理的命令集。

🌻 Name:	Show-Access	
Descriptio	an:	
Description	511.	
Permit ar	v command that is not in the table	e below
	.,	
Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	
Add /\	Edit V Replace A De	elete
Creat	Comment	A
Grant	Command	Arguments
Permit	•	
Select Com	mand/Arguments from Command S	Set: DenvAllCommands
	5	
		Select

Filter	:	•	Match	if:	•	G	o 🔻	
	Command Se	et Name		Descriptio	n			
	DenyAllComma	ands						
	Full-Access							
V	Show-Access							
Crea	ate	te		Pelete	File Opera	ations	Export	

38. 按一下「**OK**」(確定)。



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.

Conditions

AD1:ExternalGroups:
contains any
MCS55.com/Users/Network Maintenance Team
Select Deselect Clear
Results
Shell Profile: Limited-Privilege Select
Command Sets:
Show-Access
Select Deselect
. 按一下「Save Changes」。

)evice	Adm	inistratio	n Authori	zation Policy			
Filter:	Stati	IS	•	Match if: Equals • Enabled • Clear Filter Gr	• •		
		Status	Name	Conditions AD1:ExternalGroups	Re Shell Profile	sults Command Sets	Hit Count
1		0	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.	Permit Access	DenyAllCommands	0
Create		Duplica	te] •	Edit Delete A Move to V		Ci	Istomize Hit Cou

40. 按一下「Create」以將Cisco IOS裝置新增為ACS上的AAA Client。

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. 提供TACACS+的名稱、IP地址、共用密碼,然後按一下Submit。

Name: lab-route	ſ		
Description:			
Network Device Group	5		
Location	All Locations	Select	
Device Type	All Device Types	Select	
IP Address	n () ID Danna(s) Bu Mark ()	Authentication Options	
 Billio 400 400 00 7 	a () in Range(a) by maak ()	Shared Secret: ••••••• Show	
V IF. 152.100.20.7		Single Connect Device	
		Egacy TACACS+ Single Connect Support	
		TACACS+ Draft Compliant Single Connect Suppo	rt
		▼ RADIUS 📄	
		Shared Secret: Show	
		CoA port: 1700	
B = Required fields			

配置Cisco IOS裝置以進行身份驗證和授權

完成這些步驟,以設定Cisco IOS裝置和ACS以進行驗證和授權。

- 1. 使用username命令建立對回退具有完全許可權的本地使用者,如下所示: username admin privilege 15 password 0 cisco123!
- 2. 提供ACS的IP地址以啟用AAA並新增ACS 5.x作為TACACS伺服器。 aaa new-model

tacacs-server host 192.168.26.51 key cisco123

注意:金鑰應與ACS上為此Cisco IOS裝置提供的共用金鑰匹配。

3. 使用<u>test aaa</u>命令測試TACACS伺服器的可達性,如下所示。

test aaa group tacacs+ user1 xxxxx legacy Attempting authentication test to server-group tacacs+ using tacacs+ User was successfully authenticated.

上一個命令的輸出顯示TACACS伺服器可訪問且使用者已成功通過身份驗證。**注意**:使用者 1和密碼xxx屬於AD。如果測試失敗,請確保上一步中提供的共用金鑰正確。

4. 配置登入並啟用身份驗證,然後使用Exec和命令授權,如下所示:

```
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
```

注意:如果TACACS伺服器無法訪問,則Local和Enable關鍵字分別用於回退到Cisco IOS本地 使用者和enable secret。

<u>驗證</u>

驗證透過Telnet登入Cisco IOS裝置的驗證和授權。

 以user1的身份通過Telnet連線到Cisco IOS裝置,該使用者屬於AD中的完全訪問組。Network Admins組是AD中對映到ACS上設定的完全特權外殼配置檔案和完全訪問命令的組。嘗試運行 任何命令以確保您具有完全訪問許可權。

```
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. 以user2身份通過Telnet連線到Cisco IOS裝置,該使用者在AD中屬於受限訪問組。(Network Maintenance Team組是AD中對映到在ACS上設定Limited-Privilege Shell Profile和Show-Access Command的組)。如果您嘗試運行除Show-Access命令集中提到的命令以外的任何命 令,您應該會收到Command Authorization Failed錯誤,其中顯示user2具有有限的訪問許可權。

username: user2 password: router1>enable password: router1# router1# routerlfshow version Cisco IOS Software, C3550 Software (C3550-IPBASEK9-M), Version 12.2(44)SE6, 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" ľ 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@ciace.com. routerl#conf t Command authorization failed. router1#wr mem Command authorization failed. router1#

 3. 登入到ACS GUI並啟動監控和報告檢視器。選擇AAA Protocol > TACACS+Authorization以驗 證user1和user2執行的活動。

3 🖌 🖻						Launch Interac	tive Viewer	
Showing Pa	ge 1 of 1				Gote	Page: Go		
AAA Protocol > T/	ACACS+ Authoriz	ation						
Authorization Status Date :	: Pass or Fail June 08, 2012							
Generated on June	8, 2012 11:57:34 AM	IIST						
Preload								
≺-Pass ×-Fail	Click for detail	ila						
ACS View Timestamp	ACS Timestamp	Status	Details	Fallure Reason	User Name	Command Set	Shell Profile	Network Device
Jun 8,12 6 21 19 410 AM	Jun 8,12 6:21:19.393 AM		94		user2	[CasiAVestit]		lab-retaine
Jan 8.12 4:20 59:800 AM	3xt 8.12 6:20:59 799 AM		- 4 <u>i</u>	13005 Command felled to match a Pennit rule	user2	[Ond-W-write memory]		<u>lab-roczer</u>
Int. 5,12 6:20 56:566 AM	Jun 8,12 8:20:58 850 AM	*	<u>0</u>	13025 Command failed to match a Permit rule	1002	[CmdAVwconfigure terminal]		lab-costar
Jan 8,12 6:20:50.056 AM	Jun 8,12 6:20:50.036 AM	1	- <u>1</u>	9	1002	[CndAV-show version]		Minostar 1
Ten 8,12 d 20 78,505 AM	han 8,12 6:20:38.490 AM	1	9	Commands run by	sam2	[Cmd-8V-earble]		lab-roozer
Jun 8.12 0.20.34.420 AM	Jan 8,12 6:20:34.406 AM	1	2	user 2	1182	[CmdAV=]	Limited-Privilege	lab-roster
Jun 8,12 6:20.02.616 AM	han 8,12 6:20:02.596 AM	~	<u>Q</u>		userl	[CmdAVestit]		lab-rotater
Nov. 8,12 4:20:00.263 AM	Jun 8,12 6:20:00.246 AM	*	- AL	Commands run by	and a	[CndAV=venion 2]		Mercetar
Jan 5,12 6:19:57:203 AM	Jun 8.12 6:19:57.260 AM	1	2	user1	wet	[CaddWreournip]		lab-router
Jun 8,12 6:19:55:103 AM	Jun 8,12 6.19:55.076 AM	1	2		see1	[CndAV-configure terminal.]		Morrouter
No. 8,12 6 19:52,763 AM	3x18.12 6:19:52 740 AM		्		sser1	[Ond-8V=]	Pall-Peivilege	(ab-rouser

相關資訊

- <u>思科安全存取控制系統</u>
- 技術支援與文件 Cisco Systems