# ACS 5.x:ADグループメンバーシップに基づく TACACS+認証およびコマンド認可の設定例

### 内容

<u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>コンフィギュレーション</u> <u>認証および認可のためのACS 5.xの設定</u> <u>認証および認可のためのCisco IOSデバイスの設定</u> <u>確認</u> <u>関連情報</u>

## はじめに

このドキュメントでは、Cisco Secure Access Control System(ACS)5.x以降を使用するユーザの ADグループメンバーシップに基づくTACACS+認証およびコマンド認可の設定例を紹介します。 ACS は外部 ID ストアとしてユーザ、マシン、グループ、および属性を保存するために Microsoft Active Directory (AD)を使用します。

# 前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

 ACS 5.xは、目的のADドメインに完全に統合されています。ACSが必要なADドメインと統合されていない場合、統合タスクを実行するための詳細については、『<u>ACS 5.x以降</u> <u>: Microsoft Active Directoryとの統合の設定例</u>』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure ACS 5.3
- Cisco IOS<sup>®</sup>ソフトウェアリリース12.2(44)SE6。

注:この設定は、すべてのCisco IOSデバイスで実行できます。

・ Microsoft Windows Server 2003 ドメイン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在 的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

コンフィギュレーション

認証および認可のためのACS 5.xの設定

認証と認可のためのACS 5.xの設定を開始する前に、ACSはMicrosoft ADと正常に統合されている 必要があります。ACSが必要なADドメインと統合されていない場合、統合タスクを実行するため の詳細については、『<u>ACS 5.x以降:Microsoft Active Directoryとの統合の設定例</u>』を参照してく ださい。

このセクションでは、2つのADグループを、2つの異なるコマンドセットと2つのシェルプロファ イルにマッピングします。一方はフルアクセスを使用し、もう一方はCisco IOSデバイス上で制限 付きアクセスを使用します。

- 1. 管理者クレデンシャルを使用してACS GUIにログインします。
- 2. Users and Identity Stores > External Identity Stores > Active Directoryの順に選択し、ACSが 目的のドメインに参加していること、および接続ステータスがconnectedと表示されている ことを確認します。

Directory Groupsタブをクリックします。

Use	Users and Identity Stores > External Identity Stores > Active Directory								
	General Directory Groups Directory Attributes								
	Connection Details								
	<ul> <li>Active Directory Domain Name: MCS55.com</li> </ul>								
	Please specify the credentials used to join this machine Username:	to the Active Directory Domain:							
	C Deseuverd								
	Password:								
	You may use the Test Connection Button to ensure credentials are correct and Active Directory Domain is reachable. Test Connection Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have success can select the Directory Groups and Directory Attributes to be available for use in policy rules.								
	End User Authentication Settings								
	Enable password change								
	Enable machine authentication	Enable machine authentication							
	Enable Machine Access Restrictions								
	Connectivity Status Joined to Domain:mcs55.com Connectivity Status:CONNECTED								
	o = Remired fields								
- S	Save Changes Discard Changes Clear Configuration								

3. [Select] をクリックします。

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 more formed a
cisco.com/Users/Domain Users
Required fields
Save Changes Discard Changes Clear Configuration

4. 設定の後半で、シェルプロファイルとコマンドセットにマッピングする必要があるグループ を選択します。[OK] をクリックします。

Ex	ternal Use	r Groups				
Sea	irch Base D	N DC=MCS55,DC=com				
Sea	rch Filter	Go				
Ľ	Group	Name		Group Type		
E	MCS5	5.com/Users/Domain Guests		GLOBAL	*	
	MCS5	5.com/Users/Network Admins		GLOBAL		=
	MCS5	5.com/Users/Network Maintenance Team		GLOBAL		
E	MCS5	5.com/Users/Schema Admins		UNIVERSAL	÷	
	K Canc	abase: Active Directory				
	Usi Sea	* for wildcard search (i.e. admin*) arch filter applies to group name and not the fully qualified particle in the fully qua	ath.			÷

5. [Save Changes] をクリックします。

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
C = Required fields
Save Changes Discard Changes Clear Configuration

6. Access Policies > Access Services > Service Selection Rulesの順に選択し、TACACS+認証 を処理するアクセスサービスを識別します。この例では、Default Device Adminです。

Access P Sir	ccess Policies > Access Services > Service Selection Rules Single result selection  Rule based result selection							
Servio	Service Selection Policy							
Filter:	Filter: Status Vert 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	4		Default Network Access	0

7. Access Policies > Access Services > Default Device Admin > Identityの順に選択し、Identity Sourceの横にあるSelectをクリックします。



8. [AD1] を選択し、[OK] をクリックします。

Ident	tity Store		Showing 1-9 of 9 50 • per page Go
Filte	r: [	Match if. 🚽 🛛 🐨	
	Name 🔺	Description	
٥	AD1		
0	CN Usemame	Predefined Certificate Authentication Profile	
0	DenyAccess		
0	Internal Hosts		
0	Internal Users		
0	LDAP	Domain Controller LUAP	
0	NAC Profiler	Default Entry for NAC Profiler	
0	safeword	THIS IS NOT USED inic 2011.11.22	
0	safeword-ias		
			M Page 1 of 1 P
OK	Cancel		

9. [Save Changes] をクリックします。

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

10. Access Policies > Access Services > Default Device Admin > Authorizationの順に選択し、 Customizeをクリックします。

E	Access Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy							
	Device Administration Authorization Policy         Filter: Status       Match if: Equals         Enabled       Clear Filter         Go       The state of t							
			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
	Create I Duplicate I Edit Delete A Move to Y Custemize Hit Count Save Changes Discard Changes							

11. AD1:ExternalGroupsをAvailableから Customize ConditionsのSelectedセクションにコピー し、次にシェルプロファイルとコマンドセットをCustomize ResultsのAvailableから Selectedセクションに移動します。ここで、[OK] をクリックします。

Customize Conditions			
Available:		Selected:	
ACS Host Name	*	AD1:ExternalGroups	*
Authentication Method			
Authentication Status			
Compound Condition	= [ < ]		
Device Filter			
Device IP Address			
Device Port Filter	$\gg$		
Eap Authentication Method			
Eap Tunnel Building Method	~		
End Station Filter	<b>T</b>		T
Customize Results			
Available:		Selected:	
	*	Shell Profile	*
		Command Sets	
	$\gg$		V
		L	- * .
OK Cancel			
Cancer			

12. 新しいルールを作成するには、[Create] をクリックします。

^	ccess F Standa	Policies ard Po	i > Access	s Services	> Default Device Admin > Authorization			
	Devic	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	/			
	**		<u>Default</u>		If no rules defined or no enabled rule matches	s. Permit Access	DenyAllCommands	0
	Creat	e   •	Duplic	ate   🔻	Edit Delete Move to			Customize Hit Count
	Create Save Changes Discard Changes							

13. AD1:ExternalGroups条件でSelectをクリックします。

Connect						
Name: Rule-1	Status:	Lnabled • (				
The Custom conditions ar	ze button in the lo id results are ava	ower right area of i ilable here for use	the policy rule in policy rule	s screen confra s.	ols which policy	
Conditions           AD1:ExternalGroups           contains any						
					A	
Select Deselect	Clear					
Shell Profile. Permit /	Ассеза	Select	]			
Command Sets:						
		× ×				
UK Cancel		-				He

14. Cisco IOSデバイスでフルアクセスを提供するグループを選択します。[OK] をクリックします。

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

15. Shell ProfileフィールドでSelectをクリックします。

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       Results       Shell Profile:       Permit Access       Command Sets:	E
Select Deselect OK Cancel	

16. Createをクリックして、フルアクセスユーザ用の新しいシェルプロファイルを作成します。

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 ▶ ▶
OK	Cancel	Help

17. GeneralタブでNameとDescription(オプション)を指定し、Common Tasksタブをクリックします。

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

18. デフォルト権限と最大権限を値15の静的に変更します。[Submit] をクリックします。

ſ

ſ

General Common	Custom Attrib	outes
Privilege Level		
Default Privilege:	Static - Val	ue 15 🔻
Maximum Privilege:	Static - Val	ue 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. 新しく作成したフルアクセスシェルプロファイル(この例ではFull-Privilege)を選択し、 OKをクリックします。

Shell	Profiles
Filter:	✓ Match if: ✓ Go ▼
	Name  Description
$\odot$	DenyAccess
٥	Full-Privilege To push default privilege 15 for IOS
0	Permit Access
Crea	ate Duplicate Edit Delete
ОК	Cancel

20. Command SetsフィールドでSelectをクリックします。

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: Conditions       Image: Contains any Image: Conta	
MCS55.com/Users/Network Admins	
Select     Deselect       Results       Shell Profile:       Full-Privilege	E
Command Sets:	
Select Deselect OK Cancel	- I leip

21. Createをクリックして、フルアクセスユーザ用の新しいコマンドセットを作成します。

Command Sets	Showing 1-1 of 1 50 v per page G							
Filter: 🔹 Match if: 🔹 Go 💌								
Command Set Name   Description								
DenyAllCommands								
Create Duplicate Edit Delete   File Operations Export M Page 1 of 1 P M								
OK Cancel	Hel							

22. 名前を入力し、Permit any command that is not in the table belowの横にあるチェックボッ クスにチェックマークが付いていることを確認します。[Submit] をクリックします。

注:コマンドセットの詳細については、『<u>デバイス管理用コマンドセットの作成、複製、お</u> <u>よび編集</u>』を参照してください。

Name:	Full-Access		
Description:			
Permit any c	command that is not in the table below		
Grant	Command	Arguments	
		*	
		-	
Add A	Edit V Replace A Delete	· · · · · · · · · · · · · · · · · · ·	
Grant	Command	Arguments	
Permit	•		
Select Comman	d/Arguments from Command Set:	DenyAllCommands -	
Select Comman			

23. [OK] をクリックします。

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

#### 24. [OK] をクリックします。これで、Rule-1の設定は完了です。

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: Conditions       Image: Contains any	
MCS55.com/Users/Network Admins	
Select     Deselect     Clear       Results     Shell Profile.     Full-Privilage       Command Sets:     Select	
Ful-Access	
Select Deselect	Help

25. Createをクリックして、制限付きアクセスユーザ用の新しいルールを作成します。

E	Access Policies > Access Services > Default Device Admin > Authorization Standard Policy Exception Policy Device Administration Authorization Policy									
	Filter	Statu	IS		Match if. Equals    Enabled	Filter Go	7			
	Status Name			Name	Conditions AD1:ExternalGroups	Results Shell Profile Command Sets		Hit Count		
l	1 C Rule-1 contains any (MCS55.com/Users/Network Admins)				contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0		
	** Default If no rules defined or no enabled rule matches. Permit Access DenyAlCommands 0							0		
	Create   Duplicate   Edit Delete A Move to V Customize Hit Count									
1	Create Save Changes Discard Changes									

26. AD1:ExternalGroupsを選択して、Selectをクリックします。

							4
General							
Name: Rule 2		Status:	Enabled	- (	0		
The C condit	ustomize button ions and results	in the lov are avail	wer right are able here fo	a of t r use	the policy rules screen contro ain policy rules.	is which policy	
Conditions							
AD1.External	Groups.						
contains any	-						
						4	
							=
						-	
Select	eselect Clea	ar					
Beaulta							
Shell Profile	Parmit Access			olori			
Command Sets:			0	01001			
			×				
		,	-				-
OK Cancel							Help

27. 制限付きアクセスを提供するグループを選択し、OKをクリックします。

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

28. Shell ProfileフィールドでSelectをクリックします。

The Customize button in the l conditions and results are ava	ower right area of the policy rules screen controls which policy ailable here for use in policy rules.	
Conditions		
AD1:ExternalGroups:		
contains any		
MCS55.com/Users/Network Maintenance	Feam +	
Select Deselect Clear		
Results		
Shell Profile: Permit Access	Select	
Command Sets:		
Select Deselect		
K Cancel		н

29. Createをクリックして、制限付きアクセス用の新しいシェルプロファイルを作成します。

Shell	Shell Profiles					
Filter		✓ Match if: ✓ Go ▼				
	Name 4	Description				
0	DenyAccess					
0	Full-Privilege	To push default privilege 15 for IOS				
$\odot$	Permit Access	3				
Create Duplicate Edit Delete						
OK	Cancel					

30. GeneralタブでNameとDescription(オプション)を指定し、Common Tasksタブをクリックします。

General Cor	nmon Tasks Custom Attributes
🌻 Name:	Limited-Privilege
Description:	To push default privilege 1 for IOS
🔅 = Required fiel	ds

31. デフォルト権限と最大権限をそれぞれ値1と15で静的に変更します。[Submit] をクリックし ます。

Static		
	•	Value 1 👻
Static	<b>.</b>	Value 15 👻
Not in	Use 👻	]
Not in	Use 👻	]
Not in	Use 👻	]
Not in	Use 👻	]
Not in	Use 👻	]
Not in	Use 🔻	]
Not in	Use 👻	
Not in	Use 👻	]
Not in	Use 👻	]
	Static Not in Not in Not in Not in Not in Not in Not in	Static   Not in Use  Not in Use

32. [OK] をクリックします。

Shell Profiles					
Filter:		Aatch 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				
Create Duplicate Edit Delete					
OK	OK Cancel				

33. Command SetsフィールドでSelectをクリックします。

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

34. Createをクリックして、制限付きアクセスグループ用の新しいコマンドセットを作成します。

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

35. 名前を入力し、次の表に記載されていないコマンドを許可の横にあるチェックボックスが選 択されていないことを確認します。Addをクリックし、commandセクションにあるスペー スでshowと入力して、GrantセクションでPermitを選択し、制限付きアクセスグループのユ ーザにshowコマンドだけが許可されるようにします。

General		
Name:	Show-Access	
Description	:	
Permit any	command that is not in the table below	A conversion to
Grant	Command	Arguments
Add /	Edit V Replace A Delete	
Grant	Command	Arguments
Permit	✓ show	
Select Comma	and/Arguments from Command Set:	DenvAllCommands -
Select Comma	and/Arguments from Command Set:	DenyAllCommands -

36. 同様に、Addを使用して、制限付きアクセスグループのユーザに許可するその他のコマンド を追加します。[Submit] をクリックします。

注:コマンドセットの詳細については、『<u>デバイス管理用コマンドセットの作成、複製、お</u> <u>よび編集</u>』を参照してください。

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

37. [OK] をクリックします。

Command Sets					
Filter	· Match if: ▼ Go ▼				
	Command Set Name   Description				
	DenyAllCommands				
	Full-Access				
V	Show-Access				
Crea	ate Duplicate Edit Delete File Operations Export				
ОК	Cancel				

38. [OK] をクリックします。



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	d	iti	0	ne
COII	u		v	15

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. [Save Changes] をクリックします。

A	Access Policies > Access Services > Default Device Admin > Authorization									
	Standard Policy Exception Policy									
Device Administration Authorization Policy										
Filter: Status • Match if: Equals • Enabled • Clear Filter Go v										
			Status	Name	Conditions AD1:ExternalGroups	Re Shell Profile	Command Sets	Hit Count		
	1	1 🖸 😑 Rule-1 contains any (MCS55.com/Users/Network Admins)					Full-Access	0		
	2	2 F1 O 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 A Move to V Customize Hit Count									
Γ	Save Changes Discard Changes									

40. Createをクリックして、Cisco IOSデバイスをAAAクライアントとしてACSに追加します。

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. TACACS+に対してName, IP Address, Shared Secretを指定し、Submitをクリックします。

Ne	etwork Resources > Network D	evices and AAA Clients > Create	a and a second		
	o 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	
	6 IP: 192 168 26 7		Shared Sec	cret: •••••	Show
	- H . 192.100.20.1		Single (	Connect Device	
			Eegac	y TACACS+ Single Connect Sup	port
			C TACA	CS+ Draft Compliant Single Conn	ect Support
			Shared Se	ecret:	Show
			CoA port:	1700	
	e = Required fields				
	Submit Cancel				

認証および認可のためのCisco IOSデバイスの設定

認証と認可のためにCisco IOSデバイスとACSを設定するには、次の手順を実行します。

1. 次に示すように、フォールバックの完全な権限を持つローカルユーザをusernameコマンド で作成します。

username admin privilege 15 password 0 cisco123!

2. AAAを有効にして、TACACSサーバとしてACS 5.xを追加するために、ACSのIPアドレスを 指定します。

aaa new-model
tacacs-server host 192.168.26.51 key cisco123

注:キーは、このCisco IOSデバイス用にACSで提供される共有秘密と一致する必要があり ます。

3. 次に示すように、aaa コマンド により、TACACS サーバの到達可能性をテストします。

test aaa group tacacs+ user1 xxxxx legacy Attempting authentication test to server-group tacacs+ using tacacs+ User was successfully authenticated. 前のコマンドの出力では、TACACS サーバが到達可能であり、ユーザが正常に認証された ことを示しています。

注:User1とパスワードxxxはADに属しています。テストに失敗した場合は、前の手順で指定した共有秘密が正しいことを確認してください。

4. ログインを設定して認証を有効にし、次に示すようにExecおよびコマンド認可を使用しま す。

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: TACACSサーバに到達できない場合、LocalおよびEnableキーワードは、Cisco IOSロー カルユーザおよびenable secretへのフォールバックにそれぞれ使用されます。

#### 確認

認証と認可を確認するには、Telnetを使用してCisco IOSデバイスにログインします。

1. ADのフルアクセスグループに属するuser1としてCisco IOSデバイスにTelnet接続します。 Network Adminsグループは、ACSで設定されるFull-Privilege Shell ProfileとFull-Access CommandにマッピングされるADのグループです。フルアクセス権があることを確認するた めに、任意のコマンドを実行してみてください。

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

2. ADの制限付きアクセスグループに属するuser2としてCisco IOSデバイスにTelnet接続します(Network Maintenance Teamグループは、ACSでLimited-Privilegeシェルプロファイルと

Show-AccessコマンドセットにマッピングされるADのグループです)。Show-Accessコマン ドセットに記載されているコマンド以外のコマンドを実行しようとすると、「Command Authorization Failed」エラーが発生し、user2によるアクセスが制限されていることが示さ れます。

username: user2
password:
router1>enable
password:
routerla
routerla
router1#snow version
Cisco IOS Soltware, ESSSU Soltware (CSSSU-IPBASEK9-M), Version 12.2(44)5E6, RELEASE S
OFTWARK (TCI) Conversional (v) 1985 2000 her Cinner Revolution Turk
Copyright (c) 1986-2009 by CISCO Systems, Inc.
Complete Mon D9-Mar-D9 20:26 Dy gereddy
image text base: 0x00003000, data base: 0x00EA3DE8
ROM: Bootstrap program is C3550 boot loader
routerl untime is 16 hours. 45 minutes
System returned to BOM by namer-na
System recurred to non by power on System image file is "flash:c3550-iphasek9-mz.122-44.SE6.bip"
by den indye file ib fiden doodd fybloerb merife fileferbin
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:
nutb://www.cisco.com/wwi/export/crypto/tool/stdrg.html
If you require further assistance please contact us by sending email to
cxport#cigco.com.
routerl#conf t
Command authorization failed.
router1#wr mem
Command authorization failed,
router1t

3. ACS GUIにログインし、モニタリングとレポートビューアを起動します。AAA Protocol > TACACS+Authorizationの順に選択して、user1とuser2が実行したアクティビティを確認します。

🛃 ቅ 🖻 Lauch Interactive Viewer								
Showing Pa	ge 1 of 1				Gotz	Page: Go		
AAA Protocol > TACACS+ Authorization								
Authorization Status Date :	: Pass or Fail June 08, 2012							
Generated on June 8	8, 2012 11:57:34 AM	IST						
Reload								
<ul> <li>✓=Pass</li> <li>×=Fail</li> </ul>	&-Click for deta	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	han 8,12 6:21:19.393 AM		94		user2	[CadAVecit]		lab-router 1
Jan 8.12 d 20 59.800 AM	3xi 8,12 6:29:59,799 AM		4	13025 Compand felled to match a Pennit rate	user2	[Ond-Wheelte memory ]		Intercorer 1
Jan 1,12 8:20 18:088 AM	Jun 6,12 6:20:56.850 AX	*	9	13025 Command Solied to match a Permit rule	21072	[CndAV+configure terminal_]		Interester 1
Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50:036 AM	1	- N.	9	<u>10087</u>	[CndJUV=show version ]		Mercutar 1
hen 8,12 d 20 78,506 AM	7an 8,12 6:20:38.490 AM	*	9	Commands run by	tuter2	[Cad&Vmenable ]		lab-roczer 1
Jun 8.12 6:20:34.426 AM	Jun 8,12 6:20:34:406 AM	1	- 4 <u>1</u>	user 2	11072	[CmdAV=]	Limited-Privilage	lab-costar 1
Jun 8,12 6:20.02.616 AM	has 8,12 6:20:02.596 AM	~	Q,		userl	[Cod&Vecit]		lab-router
Jun 8.12 4:20:00.263 AM	Jun 8,12 6:20:00:246 AM	*	- 4L	Commands run by	used.	[CndAV-venion 2]		lab-roster 2
Jan 5,12 6:19 57 203 AM	Jun 8.12 6:19:57.260 AM		94	user1	<u>wet</u>	[Ond/Wrotenrip]		lab-rouxer 1
Jun 8,12 6:19:55:103 AM	Jun 8,12 6.19:55.076 AM	1	- 12		seel	[OndAV-configure terminal]		Mercuter 1
No. 8,12 4:19:52,763 AM	3xt 8.12 6:19:52 740 AM		9		wet	[Cmd8V=]	Pull-Privilege	(ab-router )

# 関連情報

- <u>Cisco Secure Access Control System</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。