Konfigurieren der Autorisierung für den Authentifizierungsbefehl ISE 2.0 TACACS+

Inhalt

Einleitung Hintergrundinformationen Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurationen Konfigurieren der ISE für Authentifizierung und Autorisierung Beitreten zu ISE 2.0 zu Active Directory Netzwerkgerät hinzufügen Geräteverwaltungsdienst aktivieren Konfigurieren von TACACS-Befehlssätzen Konfigurieren des TACACS-Profils Konfigurieren der TACACS-Autorisierungsrichtlinie Konfigurieren des Cisco IOS-Routers für Authentifizierung und Autorisierung Überprüfung **Cisco IOS Router-Verifizierung ISE 2.0-Verifizierung** Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie die TACACS+-Authentifizierung und die Befehlsautorisierung basierend auf der Gruppenmitgliedschaft von Microsoft Active Directory (AD) konfiguriert werden.

Hintergrundinformationen

Um die TACACS+-Authentifizierung und -Befehlsautorisierung auf der Grundlage der Gruppenmitgliedschaft von Microsoft Active Directory (AD) eines Benutzers mit Identity Service Engine (ISE) 2.0 und höher zu konfigurieren, verwendet ISE AD als externen Identitätsspeicher, um Ressourcen wie Benutzer, Computer, Gruppen und Attribute zu speichern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS Router ist voll betriebsbereit
- Verbindung zwischen Router und ISE
- ISE-Server ist bootstrapping und hat Verbindung zu Microsoft AD

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Service Engine 2.0
- Cisco IOS[®] Softwareversion 15.4(3)M3
- Microsoft Windows Server 2012 R2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

Konfigurieren

Ziel der Konfiguration ist es,

- Telnet-Benutzer über AD authentifizieren
- Autorisieren Sie den Telnet-Benutzer, sodass er nach der Anmeldung in den privilegierten EXEC-Modus versetzt wird.
- Überprüfen und jeden ausgeführten Befehl zur Überprüfung an die ISE senden

Netzwerkdiagramm



Konfigurationen

Konfigurieren der ISE für Authentifizierung und Autorisierung

Beitreten zu ISE 2.0 zu Active Directory

1. Navigieren Sie zu Administration > Identity Management > External Identity Stores > Active Directory > Add. Geben Sie den Namen des Join Points und die Active Directory-Domäne an, und klicken Sie auf Submit (Senden).



2. Wenn Sie aufgefordert werden, allen ISE-Knoten dieser Active Directory-Domäne beizutreten, klicken Sie auf **Ja**.



3. Geben Sie den AD-Benutzernamen und das Kennwort ein, und klicken Sie auf OK.

Join Domain Please specify the credentials required	d to Join ISE node(s) to the Active Directory Domain.
* AD User Name () * Password	Administrator
Specify Organizational Unit ()	
	OK Cancel

Das für den Domänenzugriff in der ISE erforderliche AD-Konto kann einen der folgenden Werte aufweisen:

- Hinzufügen von Workstations zur Domänenbenutzerrechte in der entsprechenden Domäne
- Berechtigung "Computerobjekte erstellen" oder "Computerobjekte löschen" für den entsprechenden Computer-Container, in dem das Konto des ISE-Computers erstellt wird, bevor er dem ISE-Computer zur Domäne beitritt

Anmerkung: Cisco empfiehlt, die Sperrrichtlinie für das ISE-Konto zu deaktivieren und die AD-Infrastruktur so zu konfigurieren, dass Warnmeldungen an den Administrator gesendet werden, wenn ein falsches Kennwort für das Konto verwendet wird. Bei Eingabe eines falschen Passworts erstellt oder ändert die ISE ihr Computerkonto nicht, wenn dies erforderlich ist, und verweigert daher möglicherweise alle Authentifizierungen.

4. Überprüfen Sie den Betriebsstatus. Der Knotenstatus muss als "Abgeschlossen" angezeigt werden. Klicken Sie auf **Close** (Schließen).

Join Operation Status Status Summary: Successful		×
ISE Node	Node Status	
Joey.example.com	Completed.	
	Clo	se

5. Der Status der AD ist operationell.

Operations	▶ Policy	Guest Access	- Admini	stration	▶ Work Center	ərs	
urces D	evice Portal M	anagement pxG	rid Services	Feed S	ervice	rid Iden	
entity Source	Sequences	 Settings 					
Conne * . * Active D	ection Join Point Nan Directory Doma	Authentication D ne AD iin example.com	omains	Groups	Attrib	outes	
on on	Leave 👤 Tes	st User 🛛 💼 Diagnos	tic Tool 🛛 🛞 Re	fresh Table		_	
ISE No	de	•	ISE Node Ro	le Sta	itus		
Joey.ex	kample.com		STANDALON	IE 🔽	Operational		
				L			

6. Navigieren Sie zu Gruppen > Hinzufügen > Gruppen auswählen aus Verzeichnis > Gruppen abrufen. Aktivieren Sie die Kontrollkästchen Netzwerkadministratoren AD-Gruppe und Netzwerkwartungsteam AD-Gruppe, wie in dieser Abbildung dargestellt. Benutzer ist Mitglied der AD-Gruppe des Netzwerkwartungsteams. Dieser Benutzer kann nur show-Befehle ausführen.

Domain example.com	•	
Name Filter * SID Filter	* Type Filter ALL	*
Retrieve Groups 62 Groups Retrieved.		
Name aramole com/Ruitin/Distributed COM Users	Group SID example com/S-1.5-32-582	Group Type BUILTIN, DOMAIN LOCAL
example.comBuiltin/Event Los Readers	example.com/S-1-5-32-502	BUILTIN DOMAIN LOCAL
example.com/Builtin/Cueste	example.com/8.1.5.32.546	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Junas// Administratore	example.com/S-1-5-32-540	BUILTIN, DOMAIN LOCAL
example.com/Builtin/IIC III/CDC	example.com/2.1.6.22.689	BUILTIN, DOMAIN LOCAL
example comBuiltin/Incoming Example Comst Taust Building	example com/9.1.5.32.557	BUILTIN DOMAIN LOCAL
example comBuiltin Naturati Configuration Operators	example com/9.1.5.32.558	BUILTIN, DOMAIN LOCAL
example comBuiltin/Deformance Los Lisers	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Derformance Log Osers	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Pen/Windows 2000 Compatible Ac	example.com/2.1.5.32.554	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Briet Onerators	example com/2 1 5 22 550	BUILTIN, DOMAIN LOCAL
example.com/builtin/DDC Endpoint Convers	example.com/6.1.6.32.636	BUILTIN, DOMAIN LOCAL
example.com/Builtin/PDC Management Cenuerr	example.com/6-1-6-32-576	BUILTIN, DOMAIN LOCAL
example.com/Builtin/PD/C Remote Access Convers	example.com/9 1 6 22 676	BUILTIN, DOMAIN LOCAL
example.com/Builtin/NoS Nemote Access Servers	example.com/8-1-5-32-575	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Remote Desktop Users	example.com/S-1-0-32-000	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Renliceter	example.com/8-1-6-32-660	BUILTIN, DOMAIN LOCAL
example.com/Sultriv/Vepicator	example.com/Q-1-0-32-002	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Terminal Peners Linesse Peners	example.com/0.1.6.32.584	BUILTIN, DOMAIN LOCAL
example.com/Builtin/ terminal Server License Servers	example.com/0-1-0-32-001	BUILTIN, DOMAIN LOCAL
example.com/Sultin/Users	example.com/0-1-0-32-040	BUILTIN, DOMAIN LOCAL
example combiners Admine	0.4 6.04 70538605 700555570 400000700 4000	CLOBAL
example.com/Network Mointenance Team	0 1 5 01 70538805 700555570 400000770 1040	CLOBAL
example.com/wetwork maintenance ream	3-1-0-21-70038695-790656579-4293929702-1240	GLUBAL

7. Klicken Sie auf **Speichern**, um abgerufene AD-Gruppen zu speichern.



Netzwerkgerät hinzufügen

Navigieren Sie zu **Work Centers > Device Administration > Network Resources > Network Devices**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen und die IP-Adresse ein, aktivieren Sie das Kontrollkästchen **TACACS+-Authentifizierungseinstellungen**, und geben Sie den Schlüssel für den gemeinsamen geheimen Schlüssel an.

-thele- cisco Identity Services Engine	Home + Operations	Policy Guest Access	+ Administration	✓ Work Centers			
TrustSec Tevice Administration							
Overview + Identities User Identity C	Proups • Network Reso	urces Network Device Groups	 Policy Conditions 	 Policy Results 	Policy Sets	Reports Setti	ings
0	Network Devices List > N	lew Network Device					
Network Devices	Network Devices						
Default Devices	1	Name Router					
TACACS External Servers	Desc	ription					
TACACS Server Sequence			_				
	2 P Address: 1	0.48.66.32 / 32]				
	Device	Profile					
		Cisco • 🗹					
	Model	Name					
	Software V	ersion					
	 Network Device G 	roup					
	Location All Lo	cations 📀 Set To De	fault				
	Device Type All De	evice Types 📀 Set To De	fault				
	RADIUS Authe	ntication Settings					
	- TICLCC. 1.0	and and a feature					
2	· IAGAUS+ AUD	encation settings					
		Shared Sec	aret	Show			
		Enable Single Connect Mo	ode 🗌				

Geräteverwaltungsdienst aktivieren

Navigieren Sie zu **Administration > System > Deployment.** Wählen Sie den gewünschten Knoten. Aktivieren Sie das Kontrollkästchen **"Geräte-Admin-Service aktivieren**", und klicken Sie auf **Speichern.**

cisco Ide	entity Services	Engine	Home +	Operations	▶ Policy	Guest Acces	s • Admin	istration	Vork Centers
• System	 Identity Mar 	nagement +	Network Reso	urces > De	vice Portal Ma	nagement pxC	Grid Services	Feed Service	pxGrid Identity Mapping
Deployme	nt Licensing	Certificates	+ Logging	 Maintena 	ance Upgrad	ie Backup & F	Restore + A	dmin Access	Settings
					FQI	ON Joey.examp	ele.com		
					IP Addre Node Ty	pe Identity Ser	s rvices Engine	(ISE)	
				Personas					
				Administ	tration		Role STAN	DALONE	take Primary
				Monitori	ing		Role	MARY *	Other Monitoring Node
				Policy Se	ervice				
				V	Enable Session	n Services			
					Inclu	ide Node in Node	Group None	2	· · · · · · · · · · · · · · · · · · ·
				\checkmark	Enable Profilin	g Service			
					Enable SXP Se	ervice			
						Use Ir	Interface Giga	bitEthernet 0	* 1
				1 🗹	Enable Device	Admin Service	Ð		
					Enable Identit	y Mapping	۲		
				D pxGrid	۲				
			2	Save Re	set				

Anmerkung: Für TACACS müssen separate Lizenzen installiert sein.

Konfigurieren von TACACS-Befehlssätzen

Es werden zwei Befehlssätze konfiguriert. Erster **PermitAllCommands** für den Benutzer admin, der alle Befehle auf dem Gerät zulässt. Zweiter **PermitShowCommands** für Benutzer, der nur show-Befehle zulässt.

1. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Klicken Sie auf **Hinzufügen.** Geben Sie den Namen **PermitAllCommands ein**, aktivieren Sie das Kontrollkästchen **Alle Befehle zulassen**, die nicht aufgeführt sind, und klicken Sie auf **Senden**.

Home	Operations Policy		 Guest Access 	Administration	✓ Work Centers		
Groups	 Network Resourt 	ces Netw	ork Device Groups	 Policy Conditions 	✓ Policy Results	Policy Sets	
TACA	ACS Command Sets	> New					
		1	Name * Permit	AllCommands			
		De	escription				
2 Per	mit any command t	hat is not list	ed below				
2							
	+ Add	n ▼ 🕑 Ed	it 1 Move Up	↓ Move Down			
C	Grant		Command	Argu	ments		
	No data found.	0					
-							

2. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Klicken Sie auf **Hinzufügen.** Geben Sie den Namen **PermitShowCommands ein**, klicken Sie auf **Add**, und lassen Sie die Befehle **show** und **exit zu**. Wenn Arguments leer gelassen wird, werden standardmäßig alle Argumente eingeschlossen. Klicken Sie auf **Senden**.

Home	 Operations 	Policy	Guest Access	Administration	✓ Work Centers	
Groups	 Network Resource 	irces Netv	vork Device Groups	 Policy Conditions 		Policy Sets
TAC	CACS Command Set	ts > New				
Co	mmand Set					
		1	Name • Permit	ShowCommands		
	ormit any command	D	escription			
2	0 Selected + Add Tras	sh ▼ ØE	dit † Move Up	↓ Move Down		
	Grant		Command	Arg	uments	
<u>а</u> Г	PERMIT		show			
٦L	PERMIT		exit			

Konfigurieren des TACACS-Profils

Es wird ein einzelnes TACACS-Profil konfiguriert. Das TACACS-Profil entspricht dem Shell-Profil auf dem ACS. Die eigentliche Befehlserzwingung erfolgt über Befehlssätze. Navigieren Sie zu Work Centers > Device Administration > Policy Results > TACACS Profiles. Klicken Sie auf Hinzufügen. Geben Sie den Namen ShellProfile ein, aktivieren Sie das Kontrollkästchen Default Privilege (Standardberechtigung), und geben Sie den Wert 15 ein. Klicken Sie auf Submit (Senden).

cisco Ider	ntity Services	Engine	Home	Operations	Policy	Guest Access	Administration	- Work Centers	-		
 TrustSec 	C Device Ar	sministration	1.6.55	lin di Silsili	ana ile						
Overview	+ Identities	User Identity	Groups	Network Resource	ces Netv	vork Device Groups	Policy Conditions	· Policy Results	Policy Sets	Reports	Settings
TACACS Co	ommand Sets	9	TACA	CS Profiles > New							
TACACS Pr	ofiles		TAC	ACS Profile							
					1 Na	me * ShellProfile					
					Descri	etien					
					Descri	paon					
					_						
				Task Attribute	View	Raw View					
			Com	mon Tasks							
			2	Default Privil	ege 15	F.S		(Select 0 to 15)			
				Maximum Pr	ivilege			(Select 0 to 15			
				Access Cont	rol List		LL LISUR (L)	0			
				Auto Comma	and			0			
				No Escape	Ē			(Select true or	false)		
				Timeout	Г			0			
				🗆 Idle Time	Ē			0			

Konfigurieren der TACACS-Autorisierungsrichtlinie

Die Authentifizierungsrichtlinie verweist standardmäßig auf All_User_ID_Stores, das AD enthält, sodass sie unverändert bleibt.

Navigieren Sie zu Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule oben.

Operations	Policy	Guest Access	Administration	✓ Work Centers				0	License Wa
letwork Resou	rces Netw	ork Device Groups	Policy Conditions	 Policy Results 	Policy Sets	Reports	Settings		
Define the Po For Policy E	olicy Sets by ort go to Ac	configuring rules bas fministration > System	ed on conditions. Drag m > Backup & Restore	and drop sets on the > Policy Export Page	left hand side	to change th	ne order.		
Status	s Nan	ne	Description	on					
~	Defa	ault	Tacacs_D	efault					
Regular 🖸 P	roxy Sequer	ce 🔿							
▶ Auther	ntication P	olicy							
- Author	ization Pol	licy							
Except	otions (0)								
Standa	rd								
Sta	atus Rule	Name	Conditions (ident	ity groups and other	conditions)	Comma	nd Sets	Shell Profiles	
	Tacacs_0	Default		DenyAllCommand	5				Edit

Es werden zwei Autorisierungsregeln konfiguriert: Die erste Regel weist dem TACACS-Profil ShellProfile und dem Befehl Set PermitAllCommands basierend auf der AD-Gruppenmitgliedschaft von Netzwerkadministratoren zu. Die zweite Regel weist dem TACACS-Profil ShellProfile und dem Befehl Set PermitShowCommands basierend auf der AD-Gruppenmitgliedschaft des Netzwerkwartungsteams zu.

operations	▶ Policy	Guest Access	•	Administration	✓ Work Centers				0	License Warning
stwork Resour	rces Netw	ork Device Groups	۰P	olicy Conditions	 Policy Results 	Policy Sets	R	eports Settings		
For Policy Ex	port go to Ad	ministration > Syste	m > B	ackup & Restore	Policy Export Page					
Status	Nam	0		Descriptio	n					
X	Defa	ult		Tacacs_D	efault					
Regular 💿 P	roxy Sequent	æ ()								
Authen	tication Po	licy								
* Author	ization Poli	cy								-
► Excep	tions (0)									
Standar	rd									
Sta	atus Rule	Name		Conditions (ident	ity groups and other	conditions)		Command Sets	Shell Profiles	
	PermitAll	Commands	if	AD:ExternalGroup example.com/Net	ps EQUALS work Admins		then	PermitAllCommands	AND ShellProfile	Edit 💌
	PermitSh	owCommands	if	AD:ExternalGroup example.com/Net	ps EQUALS work Maintenance Te	eam	then	PermitShowComman	nds AND ShellProfi	le Edit 🕶
	Tacacs_D	efault	if n	o matches, then	DenyAllCommand	is				Edit 💌

Konfigurieren des Cisco IOS-Routers für Authentifizierung und Autorisierung

Führen Sie diese Schritte aus, um den Cisco IOS-Router für die Authentifizierung und Autorisierung zu konfigurieren.

1. Erstellen Sie mit dem Befehl **username** einen lokalen Benutzer mit voller Berechtigung für den Fallback, wie hier gezeigt.

username cisco privilege 15 password cisco

2. Aktivieren Sie ein neues Modell. Definieren Sie den TACACS-Server ISE, und platzieren Sie ihn in der Gruppe ISE_GROUP.

tacacs server ISE address ipv4 10.48.17.88 key cisco aaa group server tacacs+ ISE_GROUP server name ISE

aaa new-model

Anmerkung: Der Serverschlüssel entspricht dem auf dem ISE-Server zuvor definierten Schlüssel.

3. Testen Sie die Erreichbarkeit des TACACS-Servers mit dem Befehl test aaa wie dargestellt.

Die Ausgabe des vorherigen Befehls zeigt an, dass der TACACS-Server erreichbar ist und der Benutzer erfolgreich authentifiziert wurde.

4. Konfigurieren Sie die Anmeldung, aktivieren Sie die Authentifizierungen, und verwenden Sie dann die exec- und Command-Autorisierungen wie dargestellt.

aaa authentication login AAA group ISE_GROUP local aaa authentication enable default group ISE_GROUP enable aaa authorization exec AAA group ISE_GROUP local aaa authorization commands 0 AAA group ISE_GROUP local aaa authorization commands 1 AAA group ISE_GROUP local aaa authorization commands 15 AAA group ISE_GROUP local aaa authorization config-commands

Anmerkung: Die erstellte Methodenliste erhält den Namen AAA und wird später verwendet, wenn sie Zeile vty zugewiesen wird.

5. Zuordnen von Methodenlisten zu Zeile vty 0 4.

```
line vty 0 4
authorization commands 0 AAA
authorization commands 1 AAA
authorization commands 15 AAA
authorization exec AAA
login authentication AAA
```

Überprüfung

Cisco IOS Router-Verifizierung

1. Telnet zum Cisco IOS-Router als Administrator, der zur Gruppe mit vollem Zugriff in AD gehört. Die Gruppe Netzwerkadministratoren ist die Gruppe in AD, die dem Befehlssatz ShellProfile und PermitAllCommands auf der ISE zugeordnet ist. Versuchen Sie, einen beliebigen Befehl auszuführen, um vollständigen Zugriff zu gewährleisten.

```
Username:admin
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router(config)#exit
Router#
```

2. Telnet zum Cisco IOS-Router als Benutzer, der zur Gruppe mit beschränktem Zugriff in AD gehört. Die Gruppe "Netzwerkwartungsteam" ist die Gruppe in AD, die dem Befehlssatz **ShellProfile** und **PermitShowCommands** auf der ISE zugeordnet ist. Versuchen Sie, einen beliebigen Befehl auszuführen, um sicherzustellen, dass nur show-Befehle ausgegeben werden können.

Password:

Router#show ip interface b:	rief exclude un	nassigned	
Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0/0	10.48.66.32	YES NVRAM up	up

Router#**ping 8.8.8.8** Command authorization failed.

Router#**configure terminal** Command authorization failed.

Router#**show running-config** | **include hostname** hostname Router Router#

ISE 2.0-Verifizierung

1. Navigieren Sie zu **Operationen > TACACS-Livelog.** Stellen Sie sicher, dass die durchgeführten Versuche erkannt werden.

cisco Identity Services E	ngine H	ome 👻	Operations	▶ Policy →	Guest Access	Administration	Work Centers
RADIUS Livelog TACACS	Livelog Rep	orts + Tr	oubleshoot	Adaptive Netwo	ork Control		
🚔 Add or Remove Columns 🕶	😵 Refresh						Refresh Eve
Generated Time	Status All 🔻 Deta	ills Usern	ame 🕐	Type All 🔫	Authentication Po	licy ⁽⁾	Authorization Policy (
2015-08-18 14:28:12.011	2	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:28:05.11	2	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:55.408	8	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:53.013	8	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:47.387	2	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:41.034	2	user		Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:40.415	2	user	1	Authentication	Tacacs_Default >	> Default >> Default	
2015-08-18 14:24:43.715	2	admin	1	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:24:40.834	2	admin	1	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:24:40.213	2	admin		Authentication	Tacacs_Default >	> Default >> Default	
2015-08-18 14:20:42.923	2	admin	1	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:20:42.762	2	admin	1	Authentication	Tacacs_Default >	> Default >> Default	

2. Klicken Sie auf die Details eines der roten Berichte. Fehlgeschlagener Befehl, der früher ausgeführt wurde, wird angezeigt.

verview							
Request Type	Authorization						
Status							
Session Key	Joey/229259639/49						
Message Text	Failed-Attempt: Command Authorization failed						
Username	user						
Authorization Policy	Tacacs_Default >> PermitShowCommands						
Shell Profile							
Matched Command Set							
Command From Device	configure terminal						

Authorization Details	
Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Fehlerbehebung

Fehler: 13025 Befehl konnte nicht mit einer Zulässigkeitsregel übereinstimmen

Überprüfen Sie die SelectedCommandSet-Attribute, um zu überprüfen, ob die erwarteten Befehlssätze von der Autorisierungsrichtlinie ausgewählt wurden.

Zugehörige Informationen

Technischer Support und Dokumentation für Cisco Systeme

ISE 2.0 - Versionshinweise

ISE 2.0 Hardware-Installationshandbuch

ISE 2.0 Upgrade-Leitfaden

ACS auf ISE Migration - Tool-Leitfaden

ISE 2.0 Active Directory Integration Guide

ISE 2.0 Engine - Administratorhandbuch

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.