ISE 2.0 TACACS+ 인증 명령 권한 부여 구성

목차

소개 배경 정보 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 네트워크 다이어그램 설정 인증 및 권한 부여를 위한 ISE 구성 Active Directory에 ISE 2.0 조인 네트워크 디바이스 추가 장치 관리 서비스 사용 TACACS 명령 집합 구성 TACACS 프로파일 구성 TACACS 권한 부여 정책 구성 인증 및 권한 부여를 위해 Cisco IOS 라우터 구성 다음을 확인합니다. Cisco IOS 라우터 확인 ISE 2.0 확인 문제 해결 관련 정보

소개

이 문서에서는 Microsoft AD(Active Directory) 그룹 멤버십을 기반으로 TACACS+ 인증 및 명령 권 한 부여를 구성하는 방법에 대해 설명합니다.

배경 정보

ISE(Identity Service Engine) 2.0 이상을 사용하는 사용자의 Microsoft AD(Active Directory) 그룹 멤 버십을 기반으로 TACACS+ 인증 및 명령 권한 부여를 구성하려면 ISE는 AD를 외부 ID 저장소로 사 용하여 사용자, 머신, 그룹 및 특성과 같은 리소스를 저장합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

• Cisco IOS Router는 완벽하게 작동함

- 라우터와 ISE 간의 연결
- ISE 서버가 부트스트랩되고 Microsoft AD에 연결됨

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙을 참고하십시오.</u>

구성

이 구성의 목표는 다음과 같습니다.

- AD를 통해 텔넷 사용자 인증
- 로그인 후 특별 권한 EXEC 모드로 들어가도록 텔넷 사용자에게 권한 부여
- 확인을 위해 실행된 모든 명령을 확인하고 ISE에 보냅니다.

네트워크 다이어그램



설정

인증 및 권한 부여를 위한 ISE 구성

Active Directory에 ISE 2.0 조인

1. Administration(관리) > Identity Management(ID 관리) > External Identity Stores(외부 ID 저장소) > Active Directory > Add(추가)로 이동합니다. 가입 포인트 이름, Active Directory 도메인을 제공하 고 제출을 클릭합니다.

Operations	Policy	Guest Access	→ Administra	tion 🕨 Wo	rk Centers	
sources + Dev	rice Portal Ma	nagement pxGrid	I Services + F	Feed Service	pxGrid Iden	tity Mapping
Identity Source S	equences	 Settings 				
Connect	ion	. 40				
Active Dire	ectory Domai	n example.com				- C
Submit C	ancel					

2. 모든 ISE 노드를 이 Active Directory 도메인에 가입시키라는 메시지가 표시되면 **Yes(예)**를 클릭 합니다.



3. AD 사용자 이름 및 암호를 입력하고 확인을 **클릭합니다**.

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

ISE에서 도메인 액세스에 필요한 AD 계정은 다음 중 하나를 가질 수 있습니다.

- 각 도메인의 도메인 사용자 권한에 워크스테이션 추가
- ISE 시스템의 계정이 ISE 시스템을 도메인에 조인하기 전에 생성된 각 컴퓨터 컨테이너에서 컴 퓨터 개체 만들기 또는 컴퓨터 개체 삭제 권한

참고: Cisco에서는 ISE 계정에 대한 잠금 정책을 비활성화하고 해당 계정에 잘못된 비밀번호 가 사용되는 경우 관리자에게 알림을 전송하도록 AD 인프라를 구성하는 것을 권장합니다. 잘 못된 비밀번호를 입력하면 ISE는 필요한 경우 머신 계정을 생성하거나 수정하지 않으므로 모 든 인증을 거부할 수 있습니다.

4. 운영 상태 검토 노드 상태는 완료로 표시되어야 합니다. 닫기를 클릭합니다.

Join Operation Status Status Summary: Successful		
ISE Node	Node Status	
Joey.example.com	Completed.	
	Clos	e

5. AD 작동 상태



6. **그룹 > 추가 > 디렉토리에서 그룹 선택 > 그룹 검색으로 이동합니다.** 이 이미지에 표시된 대로 **Network Admins** AD Group(네트워크 관리자 AD 그룹) 및 **Network Maintenance Team** AD Group(네트워크 유지 관리 팀 AD 그룹) 확인란을 선택합니다.

참고: 사용자 관리자가 Network Admins AD 그룹의 구성원입니다. 이 사용자는 전체 액세스 권한을 가집니다. 이 사용자는 네트워크 유지 관리 팀 AD 그룹의 구성원입니다. 이 사용자는 show 명령만 실행할 수 있습니다.

Select Directory Groups This dialog is used to select groups from the Directory.		
Domain example.com	· · · · · · · · · · · · · · · · · · ·	
Name Filter * SID	Filter * Type	e Filter ALL *
Retrieve Groups 62 Groups Retrieved	and a state as a second state of the	and the second state of the second state of the second
Name example.com/Builtin/Distributed COM Users	 Group SID example.com/S-1-5-32-562 	Group Type BUILTIN, DOMAIN LOCAL
example.com/Builtin/Event Log Readers	example.com/S-1-5-32-573	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Guests	example.com/S-1-5-32-546	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Hyper-V Administrators	example.com/S-1-5-32-578	BUILTIN, DOMAIN LOCAL
example.com/Builtin/IIS_IUSRS	example.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Incoming Forest Trust Builders	example.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Network Configuration Operator	s example.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Performance Log Users	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Performance Monitor Users	example.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Pre-Windows 2000 Compatible	Ac example.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Print Operators	example.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
example.com/Builtin/RDS Endpoint Servers	example.com/S-1-5-32-576	BUILTIN, DOMAIN LOCAL
example.com/Builtin/RDS Management Servers	example.com/S-1-5-32-577	BUILTIN, DOMAIN LOCAL
example.com/Builtin/RDS Remote Access Servers	example.com/S-1-5-32-575	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Remote Desktop Users	example.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Remote Management Users	example.com/S-1-5-32-580	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Replicator	example.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Server Operators	example.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Terminal Server License Server	example.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Users	example.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
example.com/Builtin/Windows Authorization Access (3r example.com/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
example.com/Network Admins	S-1-5-21-70538695-790656579-4293929	9702-1239 GLOBAL
example.com/Network Maintenance Team	S-1-5-21-70538695-790656579-4293929	9702-1240 GLOBAL
<u>a kinin di da di kinin</u> di k in	lite in the second second	OK Cancel

7. **저장**을 눌러 검색된 AD 그룹을 저장합니다.



네트워크 디바이스 추가

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. Add(추가)를 클릭합니다. Name(이 름), IP Address(IP 주소)를 입력하고 TACACS+ Authentication Settings(TACACS+ 인증 설정) 확인 란을 선택한 다음 Shared Secret key(공유 비밀 키)를 입력합니다.**

-thele Identity Services Engine	Home	Operations	+ Policy	+ Guest Access	Administration	✓ Work Centers			
TrustSec Topyice Administration	n					an san di sa			
Overview + Identities User Ide	ntity Groups	* Network Resour	ces Netwo	ork Device Groups	Policy Conditions	Policy Results	Policy Sets	Reports	Settings
	Network	k Devices List > Ne	w Network D	Nevice					
Network Devices	Netwo	ork Devices							
Default Devices		1 · N	ame Route	r .					
TACACS External Servers		Descri	ption						
TACACS Server Sequence					_				
	2	* IP Address: 10	.48.66.32	/ 32					
					_				
		Device P	rofile						
			tt Ci	sco • 0					
		Model N	lame						
		Software Ve	rsion						
		Network Device Gr	oup						
		Location All Loc	ations	Set To Def	fault				
	D	evice Type All Dev	vice Types	Set To Def	fault				
	0	N DADIE IS Authors	feation Cattle						
		 Nunus Aument 	Justion Settin	φ.					
		 TACACS+ Auther 	ntication Set	ings					
	3			Shared Sec	net Casara	Show			
			Fachte	Cierto Connect Ho	~ [Snow			
			Chable	single Connect Mo	00 []				

장치 관리 서비스 사용

Administration(관리) > System(시스템) > Deployment(구축)로 이동합니다. 필요한 노드를 선택합 니다. Enable Device Admin Service(디바이스 관리 서비스 활성화) 확인란을 선택하고 Save(저장)를 클릭합니다.

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				

참고: TACACS의 경우 별도의 라이센스를 설치해야 합니다.

TACACS 명령 집합 구성

두 개의 명령 집합이 구성됩니다. 첫 번째 **PermitAllCommands** - 사용자 admin을 위한 것으로 디바 이스의 모든 명령을 허용합니다. show **명령만** 허용하는 사용자 사용자를 위한 두 번째 PermitShowCommands.

1. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭합니다. 이름 PermitAllCommands를 제공하고, 나열되지 않은 모든 명령 허용 확인란을 선택하고 Submit(제출)을 클릭합니다.

Home	Home		For a state of the state of	Administration	✓ Work Centers		
Groups	Network Resource	es Netw	vork Device Groups	Policy Conditions	✓ Policy Results	Policy Sets	
TAC/	ACS Command Sets	> New					
		1	Name * Permit	AllCommands			
		D	escription		8		
2 Per	mit any command th	at is not lis	ted below 🗹				
	+ Add 🗎 Trash	- Ge	dit 🕈 Move Up	↓ Move Down			
C	Grant		Command	Argu	ments		
	No data found.						

2. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭합니다. Name PermitShowCommands를 입력하고 Add(추가)를 클릭한 후 permit show and exit commands(표시 및 종료 명령 허용)를 클릭합니다. 기본적으로 인수를 비워 둘 경우 모든 인수가 포함됩니다. Submit(제출)을 클릭합니다.

Home	 Operations 	Policy	Guest Access	 Administration 	✓ Work Centers	
Groups	 Network Resource 	rces Netw	ork Device Groups	 Policy Conditions 		Policy Sets
TAC	CACS Command Sets	s > New				
Co	mmand Set					
		1	Name * Permit	ShowCommands		
Ρ	ermit any command t	De hat is not list	escription			
	0 Selected					
2	+ Add 💼 Tras	h • C íEo	dit 1 Move Up	↓ Move Down		
	Grant		Command	Argu	iments	
<u>а</u> Г	PERMIT		show			
۶L	PERMIT		exit			

TACACS 프로파일 구성

단일 TACACS 프로파일이 구성됩니다. TACACS 프로파일은 ACS의 셸 프로파일과 동일한 개념입 니다. 실제 명령 적용은 명령 집합을 통해 수행됩니다. Work Centers(**작업 센터) > Device** Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Profiles(TACACS 프로필)로 이동합니다. Add(추가)를 클릭합니다. Name ShellProfile을 제공하고 Default Privilege 확인란을 선 택하고 값 15를 입력합니다. Submit을 클릭합니다.

dentity Services Engine	Home	Operations	Policy	Guest Access	Administration	· Work Centers			
TrustSec Pevice Administration	1.6.66								Els Filles
Overview + Identities User Identity	Groups	Network Resource	es Netw	vork Device Groups	Policy Conditions	· Policy Results	Policy Sets	Reports	Settings
TACACS Command Sets	TACAG	CS Profiles > New							
TACACS Profiles	TACA	CS Profile							
			1 Na	me* ShellProfile					
			Descri	ption					
	1	Task Attribute	View	Raw View					
	Com	non Tasks							
	2	🛛 Default Privile	ge 15	F.S) (Select 0 to 15))		
		Maximum Priv	/lege			(Select 0 to 15)		
		Access Contre	ol List			0			
		 Auto Comman 	nd			0			
		No Escape	Ē			(Select true or	false)		
		Timeout	Г			0			
		idle Time				0			

TACACS 권한 부여 정책 구성

인증 정책은 기본적으로 AD를 포함하는 All_User_ID_Stores를 가리키므로 변경되지 않습니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Sets(정책 집합) > Default(기본값) > Authorization Policy(권한 부여 정책) > Edit(편집) > Insert New Rule Above(위에 새 규칙 삽입)로 이동합니다.

Operations	Policy	Guest Access	Administration	✓ Work Centers				0	License Wa
letwork Resou	urces Netw	ork Device Groups	Policy Conditions	 Policy Results 	Policy Sets	Reports	Settings		
Define the P For Policy E	olicy Sets by xport go to Ad	configuring rules bas Iministration > System	ed on conditions. Drag m > Backup & Restore	and drop sets on the > Policy Export Page	e left hand side	to change th	he order.		
Status	s Nam	10	Description	on					
×	Defa	ult	Tacacs_D	Vefault					
Regular 🖸 F	Proxy Sequen	ce 🔿							
Auther	ntication Po	blicy							
▼ Author	rization Pol	icy							
Except	ptions (0)								
Standa	ard								
St	tatus Rule	Name	Conditions (ident	tity groups and other	conditions)	Comma	nd Sets	Shell Profiles	
	Tacacs_C	Default		DenyAllCommand	is				Edit

두 가지 권한 부여 규칙이 구성됩니다. 첫 번째 규칙은 Network Admins AD 그룹 구성원 자격을 기 반으로 TACACS 프로필 ShellProfile 및 Set PermitAllCommands 명령을 할당합니다. 두 번째 규칙 은 네트워크 유지 관리 팀 AD 그룹 멤버십을 기반으로 TACACS 프로필 ShellProfile 및 명령 집합 PermitShowCommands를 할당합니다.

operations	Policy	Guest Access	•	Administration	✓ Work Centers				0	License Warning
etwork Resour	ces Netwo	rk Device Groups	 Pc 	olicy Conditions	 Policy Results 	Policy Sets	Re	ports Settings		
For Policy Exp	port go to Adn	ninistration > System	m > Ba	ckup & Restore	Policy Export Page					
Status	Name	•		Descriptio	n					
Sec.	Defau	it.		Tacacs_D	efault					
Regular 💿 Pr	roxy Sequence	•0								
Authen	tication Pol	icy								
▼ Authori	zation Polic	γ								-
Except	tions (0)									
Standar	ď									
Sta	tus Rule N	lame		Conditions (ident	ity groups and other	conditions)		Command Sets	Shell Profiles	
	PermitAllC	ommands	if i	AD:ExternalGroup example.com/Net	ps EQUALS work Admins		then	PermitAllCommand	s AND ShellProfile	Edit 🕶
	PermitSho	wCommands	if a	AD:ExternalGroup example.com/Net	ps EQUALS work Maintenance Te	eam	then	PermitShowComma	nds AND ShellProf	ile Edit •
	Tacacs_De	fault	if no	matches, then	DenyAllCommand	is				Edit 🕶

인증 및 권한 부여를 위해 Cisco IOS 라우터 구성

인증 및 권한 부여를 위해 Cisco IOS 라우터를 구성하려면 다음 단계를 완료하십시오.

1. 여기 표시된 대로 username 명령으로 폴백할 수 있는 전체 권한을 가진 로컬 사용자를 생성합니 다.

username cisco privilege 15 password cisco 2. aaa 새 모델을 활성화합니다. TACACS 서버 ISE를 정의하고 그룹 ISE_GROUP에 배치합니다.

aaa new-model

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

참고: 서버 키는 이전에 ISE 서버에 정의된 것과 일치합니다.

3. 표시된 대로 test aaa 명령을 사용하여 TACACS 서버 연결성을 테스트합니다.

Router#test aaa group tacacs+ admin Krakow123 legacy

Attempting authentication test to server-group tacacs+ using tacacs+ User was successfully authenticated.

이전 명령의 출력에서는 TACACS 서버에 연결할 수 있으며 사용자가 성공적으로 인증되었음을 보여줍니다.

4. 로그인을 구성하고 인증을 활성화한 다음 표시된 대로 exec 및 명령 권한 부여를 사용합니다.

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

참고: 생성된 메서드 목록의 이름은 AAA이며, 나중에 이 목록이 행 vty에 할당될 때 사용됩니 다.

5. 방법 목록을 라인 vty 0 4에 지정합니다.

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

다음을 확인합니다.

Cisco IOS 라우터 확인

1. AD의 전체 액세스 그룹에 속하는 관리자로 Cisco IOS 라우터에 텔넷 연결합니다. Network Admins 그룹은 ISE에 설정된 ShellProfile 및 PermitAllCommands 명령에 매핑된 AD의 그룹입니다. 모든 명령을 실행하여 전체 액세스를 확인합니다.

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#

2. AD의 제한된 액세스 그룹에 속하는 사용자로 Cisco IOS 라우터에 텔넷 연결합니다. Network Maintenance Team 그룹은 ISE에서 설정된 ShellProfile 및 **PermitShowCommands** 명령**에 매핑되** 는 AD의 그룹입니다. show 명령만 실행할 수 있도록 명령을 실행해 보십시오.

Username:**user** Password:

Router#show ip interface brief | exclude unassignedInterfaceIP-AddressOK? Method StatusGigabitEthernet0/010.48.66.32YES NVRAM up

Protocol up

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

Router#configure terminal Command authorization failed.

ISE 2.0 확인

1. Operations(운영) **> TACACS Livelog(TACACS 라이브 로그)로 이동합니다.** 시도한 내용이 표시 되는지 확인합니다.

cisco Identity Services E	ngine Home	✓ Operations	Policy P	Guest Access	Administration	Work Centers
RADIUS Livelog TACACS	Livelog Reports	Troubleshoot	Adaptive Network	ork Control		
🙀 Add or Remove Columns 🕶	😵 Refresh					Refresh Eve
Generated Time	Status All 🔻 Details	Username ①	Type All *	Authentication Po	olicy T	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	S 🔓	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:53.013	S 🚡	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 6	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:40.415	2	user	Authentication	Tacacs_Default >	> Default >> Default	
2015-08-18 14:24:43.715	2	admin	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:24:40.834	2	admin	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:24:40.213	Sec. 1	admin	Authentication	Tacacs_Default >	> Default >> Default	
2015-08-18 14:20:42.923	A 10	admin	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:20:42.762	Solution	admin	Authentication	Tacacs_Default >	> Default >> Default	

2. 빨간색 보고서 중 하나의 상세내역을 클릭합니다. 이전에 실행된 실패한 명령을 볼 수 있습니다.

erview	
Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Jsername	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Natched 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

문제 해결

오류: 13025 명령이 허용 규칙을 매칭하지 못했습니다.

SelectedCommandSet 특성을 검사하여 필요한 명령 집합이 권한 부여 정책에 의해 선택되었는지 확인합니다.

관련 정보

<u>기술 지원 및 문서 - Cisco Systems</u>

<u>ISE 2.0 릴리스 정보</u>

<u>ISE 2.0 하드웨어 설치 가이드</u>

<u>ISE 2.0 업그레이드 가이드</u>

ACS에서 ISE로의 마이그레이션 툴 가이드

<u>ISE 2.0 Active Directory 통합 가이드</u>

<u>ISE 2.0 엔진 관리자 설명서</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.