Configurer l'autorisation de commande d'authentification TACACS+ ISE 2.0

Table des matières

Introduction Informations générales Conditions préalables Exigences Composants utilisés Configurer Diagramme du réseau Configurations Configurer ISE pour l'authentification et l'autorisation Joindre ISE 2.0 à Active Directory Ajouter un périphérique réseau Activer le service Device Admin Configurer les jeux de commandes TACACS **Configurer le profil TACACS** Configurer la stratégie d'autorisation TACACS Configuration du routeur Cisco IOS pour l'authentification et l'autorisation Vérifier Vérification du routeur Cisco IOS Vérification ISE 2.0 Dépannage Informations connexes

Introduction

Ce document décrit comment configurer l'authentification TACACS+ et l'autorisation de commande en fonction de l'appartenance au groupe Microsoft Active Directory (AD).

Informations générales

Pour configurer l'authentification TACACS+ et l'autorisation de commande en fonction de l'appartenance à un groupe Microsoft Active Directory (AD) d'un utilisateur avec Identity Service Engine (ISE) 2.0 et versions ultérieures, ISE utilise AD comme magasin d'identités externe pour stocker des ressources telles que des utilisateurs, des machines, des groupes et des attributs.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Le routeur Cisco IOS est entièrement opérationnel
- Connectivité entre le routeur et ISE.
- Le serveur ISE est amorcé et a une connectivité avec Microsoft AD

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configurer

L'objectif de la configuration est de :

- Authentifier un utilisateur Telnet via AD
- Autoriser l'utilisateur Telnet à passer en mode d'exécution privilégié après la connexion
- Vérifier et envoyer chaque commande exécutée à ISE pour vérification

Diagramme du réseau



Configurations

Configurer ISE pour l'authentification et l'autorisation

Joindre ISE 2.0 à Active Directory

1. Accédez à Administration > Identity Management > External Identity Stores > Active Directory > Add. Fournissez le nom du point de connexion, le domaine Active Directory et cliquez sur Envoyer.



2. Lorsque vous êtes invité à joindre tous les noeuds ISE à ce domaine Active Directory, cliquez sur **Oui.**



3. Fournissez un nom d'utilisateur et un mot de passe AD, puis cliquez sur OK.

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

Le compte AD requis pour l'accès au domaine dans ISE peut avoir l'un des éléments suivants :

- Ajouter des stations de travail au droit utilisateur de domaine dans le domaine respectif
- Autorisation Créer des objets ordinateur ou Supprimer des objets ordinateur sur le conteneur d'ordinateurs respectif où le compte de l'ordinateur ISE est créé avant qu'il ne joigne l'ordinateur ISE au domaine

Note: Cisco recommande de désactiver la stratégie de verrouillage pour le compte ISE et de configurer l'infrastructure AD pour envoyer des alertes à l'administrateur si un mot de passe incorrect est utilisé pour ce compte. Lorsque le mauvais mot de passe est entré, ISE ne crée pas ou ne modifie pas son compte d'ordinateur lorsque cela est nécessaire et peut donc refuser toutes les authentifications.

4. Vérifiez l'état des opérations. L'état du noeud doit apparaître comme Terminé. Cliquez sur **Fermer**.

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

5. L'état d'AD est opérationnel.

Operations	perations Policy Guest Access		s v Admin	istration	► Work Centers				
urces 🕨 [es								
entity Sourc	e Sequences	 Settings 							
Connection Authentication Domains Groups Attributes * Join Point Name AD * Active Directory Domain example.com									
Join o	Leave 👤 Tes	t User 🛛 💼 Diagno:	stic Tool 🛛 🏀 Re	efresh Table		-			
ISE N	ode	-	ISE Node Ro	ole Sta	itus				
Joey.e	example.com		STANDALON	NE 🔽	Operational				
						-			

6. Accédez à **Groups > Add > Select Groups From Directory > Retrieve Groups.** Cochez les cases **Administrateurs réseau** Groupe AD et **Équipe de maintenance réseau** Groupe AD, comme illustré dans cette image.

Note: L'utilisateur admin est membre du groupe AD Administrateurs réseau. Cet utilisateur dispose de privilèges d'accès complets. Cet utilisateur est membre du groupe AD de l'équipe

de maintenance du réseau. Cet utilisateur ne peut exécuter que des commandes show.

Select Directory Group This dialog is used to select	ps It groups from the Directory.			1						
Domain example.com										
Name Filter *	SID Filte	· ·	Type Filter ALL	*						
Retrieve	Groups 62 Groups Retrieved.									
Name example.com/Builtin/I	Distributed COM Users	 Group SID example.com/S-1-5-32-562 	Group Type BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Event Log Readers	example.com/S-1-5-32-573	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Guests	example.com/S-1-5-32-546	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Hyper-V Administrators	example.com/S-1-5-32-578	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	IIS_IUSRS	example.com/S-1-5-32-568	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	incoming Forest Trust Builders	example.com/S-1-5-32-557	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/f	Network Configuration Operators	example.com/S-1-5-32-556	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Performance Log Users	example.com/S-1-5-32-559	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Performance Monitor Users	example.com/S-1-5-32-558	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Pre-Windows 2000 Compatible Ac	example.com/S-1-5-32-554	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Print Operators	example.com/S-1-5-32-550	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	RDS Endpoint Servers	example.com/S-1-5-32-576	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	RDS Management Servers	example.com/S-1-5-32-577	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	RDS Remote Access Servers	example.com/S-1-5-32-575	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	Remote Desktop Users	example.com/S-1-5-32-555	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	Remote Management Users	example.com/S-1-5-32-580	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/I	Replicator	example.com/S-1-5-32-552	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Server Operators	example.com/S-1-5-32-549	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Terminal Server License Servers	example.com/S-1-5-32-561	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Users	example.com/S-1-5-32-545	BUILTIN, DOM	AIN LOCAL						
example.com/Builtin/	Windows Authorization Access Gr	example.com/S-1-5-32-560	BUILTIN, DOM	AIN LOCAL						
example.com/Networ	k Admins	S-1-5-21-70538695-790656579-429	3929702-1239 GLOBAL							
example.com/Networ	k Maintenance Team	S-1-5-21-70538695-790656579-429	3929702-1240 GLOBAL							
	teal aist inte bi		ti si paralanta di usi Alta da s	OK Cancel						

7. Cliquez sur **Enregistrer** pour enregistrer les groupes AD récupérés.



Ajouter un périphérique réseau

Accédez à Work Centers > Device Administration > Network Resources > Network Devices. Cliquez sur Add. Indiquez le nom et l'adresse IP, cochez la case TACACS+ Authentication Settings et indiquez la clé secrète partagée.

-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 🗌				

Activer le service Device Admin

Accédez à Administration > System > Deployment. Choisissez required Node. Cochez la case Enable Device Admin Service et cliquez sur Save.

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				

Note: Pour TACACS, vous devez disposer de licences distinctes.

Configurer les jeux de commandes TACACS

Deux jeux de commandes sont configurés. First **PermitAllCommands** pour l'utilisateur admin qui autorise toutes les commandes sur le périphérique. Deuxième **PermitShowCommands** pour l'utilisateur qui autorise uniquement les commandes show.

1. Accédez à Work Centers > Device Administration > Policy Results > TACACS Command Sets. Cliquez sur Add. Fournissez le nom PermitAllCommands, choisissez la case à cocher Permit any command qui n'est pas répertoriée et cliquez sur Submit.

Home	 Operations 	Policy	Guest Access	Administration	✓ Work Centers	
Groups	 Network Resource 	ces Netv	work Device Groups	 Policy Conditions 		Policy Sets
TAC/	ACS Command Sets	> New				
		1	Name * Permit	AllCommands		
		D	escription			
2 Per	rmit any command th	nat is not lis	ted below 🗹			
	+ Add 🌐 Trash	- Ge	dit 🕇 Move Up	↓ Move Down		
C	Grant		Command	Argu	ments	

2. Accédez à Work Centers > Device Administration > Policy Results > TACACS Command Sets. Cliquez sur Add. Fournissez le nom PermitShowCommands, cliquez sur Add et autorisez les commandes show et exit. Par défaut, si Arguments est laissé vide, tous les arguments sont inclus. Cliquez sur Submit.

Home	 Operations 	Policy	olicy		✓ 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			

Configurer le profil TACACS

Un seul profil TACACS est configuré. Le profil TACACS est le même concept que le profil Shell sur ACS. L'application effective des commandes se fait via des jeux de commandes. Accédez à **Work Centers > Device Administration > Policy Results > TACACS Profiles.** Cliquez sur **Add.** Fournissez Name ShellProfile, cochez la case **Default Privilege** et entrez la valeur 15. Cliquez sur **Submit.**

dentity Services Engine	Home	+ Operations	Policy	Guest Access	Administration	· Work Centers	-		
TrustSec Device Administration			Sa ili						e seri le c
Overview + Identities User Ident	ity Groups	Network Resource	es Netv	vork Device Groups	Policy Conditions	· Policy Results	Policy Sets	Reports	Settings
TACACS Command Sets	TACA	CS Profiles > New							
TACACS Profiles	TAC	ACS Profile							
			1 Na	me* ShellProfile					
			_						
			Descri	ption					
		Took Attributo \	filmer.	Daw More					
		Task Autouro	V IU W	Naw YIOW					
	Com	mon Tasks							
	2	Default Privile	90 IS	Б	tila tra	(Select 0 to 15))		
		Maximum Priv	riege		1	(Select 0 to 15))		
		Access Contro	ol List			0			
		Auto Comman	nd			3			
		No Escape	-			Select true or	false)		
		Timeout	-						
		-				•			
		die Time	L			2			

Configurer la stratégie d'autorisation TACACS

Par défaut, la stratégie d'authentification pointe vers All_User_ID_Stores, qui inclut Active Directory. Elle reste donc inchangée.

Accédez à Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule Above.

Operations	Policy	Guest Access	Administration	✓ Work Centers				0	License Wa
letwork Resour	rces Netwo	ork Device Groups	Policy Conditions	Policy Results	Policy Sets	Reports	Settings		
Define the Po For Policy Ex	licy Sets by o port go to Ad	configuring rules bas Iministration > System	ed on conditions. Drag m > Backup & Restore	and drop sets on the I > Policy Export Page	eft hand side	to change t	he order.		
Status	Nam	10	Description	on					
~	Defa	ult	Tacacs_D	Vefault					
Regular 🔾 Pr	roxy Sequent	ce ()							
▶ Authen	tication Po	olicy							
▼ Authori	ization Pol	icy							
Except	tions (0)								
Standar	rd								
Sta	tus Rule	Name	Conditions (ident	tity groups and other o	onditions)	Comma	nd Sets	Shell Profiles	
	Tacacs_D	Vefault		DenyAllCommands					Edit

Deux règles d'autorisation sont configurées ; La première règle attribue le profil TACACS ShellProfile et la commande Set PermitAllCommands en fonction de l'appartenance au groupe AD des administrateurs réseau. La deuxième règle attribue le profil TACACS ShellProfile et la commande Set PermitShowCommands en fonction de l'appartenance au groupe AD de l'équipe de maintenance du réseau.

Operations	Policy	Guest Access	•	Administration	- Work Centers				0	License Warning
stwork Resour	ces Netwo	ork Device Groups	۰P	olicy Conditions	 Policy Results 	Policy Set	s R	eports Settings		
For Policy Exp	port go to Adr	ministration > System	m > B	ackup & Restore	Policy Export Page					
Status	Nam	0		Descriptio	n					
1	Defa	ult		Tacacs_D	efault					
Regular 🖸 Pr	roxy Sequenc	ю ()								
Authen	tication Po	licy								
▼ Authori	zation Poli	cy								-
► Except	tions (0)									
Standar	ď									
Sta	tus Rule N	Name		Conditions (ident	ity groups and other	conditions)		Command Sets	Shell Profiles	
	PermitAllO	Commands	if	AD:ExternalGrou example.com/Net	ps EQUALS twork Admins		then	PermitAllComman	nds AND ShellProfile	Edit 🕶
	PermitSho	wCommands	if	AD:ExternalGroup example.com/Net	ps EQUALS twork Maintenance Te	sam	then	PermitShowComr	mands AND ShellProf	le Edit •
	Tacacs_D	efault	if n	o matches, then	DenyAllCommand	s				Edit 💌

Configuration du routeur Cisco IOS pour l'authentification et l'autorisation

Complétez ces étapes afin de configurer le routeur Cisco IOS pour l'authentification et l'autorisation.

1. Créez un utilisateur local avec des privilèges complets pour le secours avec la commande **username** comme indiqué ici.

username cisco privilege 15 password cisco

2. Activez un nouveau modèle. Définissez le serveur TACACS ISE et placez-le dans le groupe ISE_GROUP.

```
aaa new-model
tacacs server ISE
address ipv4 10.48.17.88
key cisco
aaa group server tacacs+ ISE_GROUP
server name ISE
```

Note: La clé du serveur correspond à celle définie sur le serveur ISE précédemment.

3. Testez l'accessibilité du serveur TACACS à l'aide de la commande test aaa comme indiqué.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Le résultat de la commande précédente indique que le serveur TACACS est accessible et que

l'utilisateur a été authentifié avec succès.

4. Configurez la connexion et activez les authentifications, puis utilisez les autorisations exec et command comme indiqué.

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

Note: La liste de méthodes créée est nommée AAA, qui est utilisée ultérieurement, lorsqu'elle est attribuée à la ligne vty.

5. Affectez des listes de méthodes à la ligne 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

Vérifier

Vérification du routeur Cisco IOS

1. Établissez une connexion Telnet avec le routeur Cisco IOS en tant qu'administrateur appartenant au groupe d'accès complet dans Active Directory. Le groupe Admins réseau est le groupe dans Active Directory qui est mappé aux commandes ShellProfile et PermitAllCommands définies sur l'ISE. Essayez d'exécuter n'importe quelle commande pour garantir un accès complet.

```
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. Établissez une connexion Telnet avec le routeur Cisco IOS en tant qu'utilisateur appartenant au groupe d'accès limité dans Active Directory. Le groupe Équipe de maintenance réseau est le groupe dans AD qui est mappé à **ShellProfile** et **PermitShowCommands** Command définis sur l'ISE. Essayez d'exécuter n'importe quelle commande pour vous assurer que seules les commandes show peuvent être exécutées.

Username:**user** Password:

Router#show ip interface 3	brief exclude u	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 fai	led.								
Router# show running-confi hostname Router Router#	g include hostn	ame							

Vérification ISE 2.0

1. Accédez à **Operations > TACACS Livellog.** Vérifiez que les tentatives effectuées sont visibles.

cisco Iden	tity Services Er	ngine	Home	- Operations	Policy	Guest Access	► Administration	Work Centers	
RADIUS Live	elog TACACS	Livelog	Reports	Troubleshoot	Adaptive Netw	ork Control			
🙀 Add or Remove Columns 👻 🚱 Refresh Refresh									
Generated Tir	ne	Status All 🔻	Details	Username ①	Type All *	Authentication F	Policy ①	Authorization Policy	
2015-08-18	14:28:12.011	1	ò	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:28:05.11	~	ò	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:27:55.408	8	à	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:27:53.013	•	ò	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:27:47.387	×	0	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:27:41.034	~	ò	user	Authorization			Tacacs_Default >> PermitShowCo	
2015-08-18	14:27:40.415	~	à	user	Authentication	Tacacs_Default :	>> Default >> Default	t	
2015-08-18	14:24:43.715		ò	admin	Authorization			Tacacs_Default >> PermitAllComm	
2015-08-18	14:24:40.834	~	ò	admin	Authorization			Tacacs_Default >> PermitAllComm	
2015-08-18	14:24:40.213	~	ò	admin	Authentication	Tacacs_Default :	>> Default >> Default	t	
2015-08-18	14:20:42.923	~	à	admin	Authorization			Tacacs_Default >> PermitAllComm	
2015-08-18	14:20:42.762	_	Q	admin	Authentication	Tacacs_Default :	>> Default >> Default	t	

2. Cliquez sur les détails de l'un des rapports rouges. La commande ayant échoué exécutée précédemment est visible.

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						

Dépannage

Erreur : La commande 13025 ne correspond pas à une règle d'autorisation

Vérifiez les attributs SelectedCommandSet pour vous assurer que les jeux de commandes attendus ont été sélectionnés par la stratégie d'autorisation.

Informations connexes

Technical Support & Documentation - Cisco Systems

Notes de version ISE 2.0

Guide d'installation matérielle ISE 2.0

Guide de mise à niveau ISE 2.0

Guide de l'outil de migration ACS vers ISE

Guide d'intégration d'ISE 2.0 Active Directory

Guide d'administration du moteur ISE 2.0

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.