配置ISE 2.0 TACACS+身份驗證命令授權

目錄

簡介 背景資訊 必要條件 需求 採用元件 設定 網路圖表 組態 配置ISE進行身份驗證和授權 <u>將ISE 2.0加入Active Directory</u> 新增網路裝置 啟用裝置管理服務 配置TACACS命令集 配置TACACS配置檔案 配置TACACS授權策略 配置Cisco IOS路由器以進行身份驗證和授權 驗證 <u>Cisco IOS路由器驗證</u> ISE 2.0驗證 疑難排解 相關資訊

簡介

本檔案介紹如何根據Microsoft Active Directory(AD)群組成員身分設定TACACS+驗證和命令授權。

背景資訊

要根據身份服務引擎(ISE)2.0及更高版本的使用者的Microsoft Active Directory(AD)組成員身份配置 TACACS+身份驗證和命令授權,ISE使用AD作為外部身份儲存來儲存資源,如使用者、電腦、組 和屬性。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco IOS路由器完全可操作
- 路由器和ISE之間的連線。

• ISE伺服器已引導並且與Microsoft AD連線

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 思科身分識別服務引擎2.0
- Cisco IOS[®]軟體版本15.4(3)M3
- Microsoft Windows Server 2012 R2

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

設定

組態的目的是:

- 通過AD驗證telnet使用者
- 授權telnet使用者,使其在登入後進入特權執行模式
- 檢查並將每個執行的命令傳送到ISE進行驗證

網路圖表



組態

配置ISE進行身份驗證和授權

將ISE 2.0加入Active Directory

1.導航到**管理>身份管理>外部身份庫> Active Directory >新增**。提供加入點名稱、Active Directory域並點選**提交。**



2.當系統提示將所有ISE節點加入此Active Directory域時,按一下是。



3.提供AD使用者名稱和密碼,然後按一下OK。

Join Domain Please specify the credentials require	d to Join ISE node(s) to the Active Directory Domain.
* AD User Name ①	Administrator
* Password	••••••
Specify Organizational Unit ()	OK Cancel

在ISE中訪問域所需的AD帳戶可以具有以下任一項:

- 將工作站新增到相應域中的域使用者許可權
- ・在建立ISE電腦帳戶的ISE電腦加入ISE電腦到域之前,在相應的電腦容器上建立電腦對象或刪
 除電腦對象許可權

附註:思科建議禁用ISE帳戶的鎖定策略,並配置AD基礎設施,以便在為該帳戶使用錯誤密碼 時向管理員傳送警報。輸入錯誤密碼時,ISE不會在必要時建立或修改其電腦帳戶,因此可能 會拒絕所有身份驗證。

4.複查工序狀態。節點狀態必須顯示為已完成。按一下「Close」。

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

5. AD的狀態為運行。



Connection	Authentication De	omains (Groups Attributes
* Join Point* Active Directory D	Name AD Iomain example.com		
👷 Join 👷 Leave 🔰	🔰 Test User 🛛 音 Diagnos	tic Tool 🛛 🛞 Refrest	Table
ISE Node	•	ISE Node Role	Status
Joey.example.co	m	STANDALONE	Operational

6.定位至**「組」>「新增」>「從目錄選擇組」>「檢索組」。**選中**Network Admins** AD Group和 **Network Maintenance Team** AD Group覈取方塊,如下圖所示。

附註:使用者admin是網路管理員AD組的成員。此使用者具有完全訪問許可權。此使用者是 網路維護團隊AD組的成員。此使用者只能執行show命令。

Select Directo This dialog is us	ory Groups and to select groups from the Directo	iry.		
Domain	example.com			7
Name Filter		SID Filter		Type Filter AL
	Retrieve Groups 62 Groups Re	trieved.		
Name			Group SID	
example.co	m/Builtin/Distributed COM Users		example.com/S-1-5-32-562	
example.co	m/Builtin/Event Log Readers		example.com/S-1-5-32-573	

Narr	10 .	Group SID	Group Type
exar	mple.com/Builtin/Distributed COM Users	example.com/S-1-5-32-562	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Event Log Readers	example.com/S-1-5-32-573	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Guests	example.com/S-1-5-32-546	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Hyper-V Administrators	example.com/S-1-5-32-578	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/IIS_IUSRS	example.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Incoming Forest Trust Builders	example.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Network Configuration Operators	example.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Performance Log Users	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Performance Monitor Users	example.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Pre-Windows 2000 Compatible Ac	example.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Print Operators	example.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/RDS Endpoint Servers	example.com/S-1-5-32-576	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/RDS Management Servers	example.com/S-1-5-32-577	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/RDS Remote Access Servers	example.com/S-1-5-32-575	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Remote Desktop Users	example.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
exar	nple.com/Builtin/Remote Management Users	example.com/S-1-5-32-580	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Replicator	example.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Server Operators	example.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Terminal Server License Servers	example.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Users	example.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
exar	mple.com/Builtin/Windows Authorization Access Gr	example.com/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
🗸 exar	nple.com/Network Admins	S-1-5-21-70538695-790656579-4293929702-1239	GLOBAL
🖌 exar	mple.com/Network Maintenance Team	S-1-5-21-70538695-790656579-4293929702-1240	GLOBAL

×

۳

7.按一下**儲存**以儲存檢索到的AD組。



新增網路裝置

導航至**工作中心>裝置管理>網路資源>網路裝置**。按一下「Add」。提供名稱、IP地址,選中 TACACS+身份驗證設定覈取方塊並提供共用金鑰。

dentity Services Engine	Home > C	perations + Policy	Guest Access	+ Administration	✓ Work Centers			
TrustSec Topyice Administration								
Overview Identities User Identity	Groups - Ne	twork Resources Net	work Device Groups	Policy Conditions	 Policy Results 	Policy Sets	Reports	Settings
9	Network Dev	ices List > New Network	k Device					
Network Devices	Network I	Devices						
Default Devices		1 Name Rou	uter					
TACACS External Servers		Description						
TACACS Server Sequence				_				
	2 P A	ddress: 10.48.66.32	/ 32					
		Device Profile						
			Cisco v 🖤					
		Model Name						
		Software Version						
	* Notwo	ork Device Group						
	Los	ation All Locations	Set To Del	fault				
	Device	Type All Device Types	Set To De	fault				
		per service rypes						
	- FRA	DIUS Authentication Set	ungs					
	• TA/	CACS+ Authentication S	ettings					
	3		Shared Sec	ent [
			anared aec		Show			
		Enal	ble Single Connect Mo	de 🗌				

啟用裝置管理服務

導航到**管理>系統>部署。選擇**所需的節點。選中Enable Device Admin Service覈取方塊,然後按一 下Save。

cisco lo	lentity Services	Engine	Home 🕨	Operations	Policy	Guest Acces	ss • Admir	histration	Work Centers
• System	Identity Man	nagement +	Network Reso	urces > De	vice Portal Ma	nagement px	Grid Services	Feed Service	a
Deploym	ent Licensing	 Certificates 	+ Logging	 Maintena 	ance Upgrad	de Backup &	Restore A	dmin Access	 Settings
					FQI	DN Joey.exam	ple.com		
					IP Addre Node Ty	pe Identity Se	8 rvices Engine	(ISE)	
				Personas					
				Adminis	tration		Role STAN	DALONE	Make Primary
				Monitor	ing		Role	MARY *	Other Monitoring Node
				Policy S	ervice				
				1	Enable Sessio	n Services			
					Inclu	ude Node in Nod	le Group Non	e · ·	· · · · · · · ·
				\checkmark	Enable Profilin	g Service			
					Enable SXP Se	ervice			
						Use I	Interface Giga	bitEthernet 0	* 1
				1 🗹	Enable Device	Admin Service	Ð		
					Enable Identit	y Mapping	Ð		
				D pxGrid	Ð				
			2	Save Re	set				

附註:對於TACACS,您需要安裝單獨的許可證。

配置TACACS命令集

配置了兩個命令集。第一個用於使用者admin的**PermitAllCommands**,它允許裝置上的所有命令。 第二個使用者的**PermitShowCommands**,僅允許show命令。

1.導航至**工作中心>裝置管理>策略結果> TACACS命令集。按一下「Add」。**提供名稱 PermitAllCommands,選中Permit any command覈取方塊(未列出),然後按一下Submit。

Home	► Operations ► Policy ► Guest Acc		Guest Access	Administration	✓ Work Centers	
Groups	Network Resource	rces Netw	ork Device Groups	 Policy Conditions 	✓ Policy Results	Policy Sets
TAC	ACS Command Set	s > New				
Con	nmand Set					
		T				
		' L	Name Permit	AllCommands		
		De	escription	8	8 8	181
2 Pe	rmit any command t	that is not list	ed below 🗹			
	+ Add	h• C∕Ec	lit 🕇 Move Up	↓ Move Down		
	Grant		Command	Argu	monte	
	Grant		Command	Argu	ments	
	No data found.					

2.導航到**工作中心>裝置管理>策略結果> TACACS命令集。按一下「Add」。**提供名稱 **PermitShowCommands**,按一下**Add**並允許**show**和**退出**命令。預設情況下,如果Arguments留空 ,則包含所有引數。按一下**Submit(提交)。**

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			

配置TACACS配置檔案

已配置單個TACACS配置檔案。TACACS配置檔案與ACS上的外殼配置檔案概念相同。實際的命令 執行是通過命令集完成的。導航到工作中心(Work Centers)>裝置管理(Device Administration)>策略 結果(Policy Results)> TACACS配置檔案(TACACS Profiles)。按一下「Add」。提供名稱 ShellProfile,選中Default Privilege覈取方塊,然後輸入值15。按一下提交。

dentity Services Engine	Home	Operations	Policy	Guest Access	Administration	· Work Centers			
TrustSec Pevice Administration	1.6.55	in di sila lis	66316						i istri isti
Overview + Identities User Identity	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	TACA	CS Profile	_		_				
			1 Na	me* ShellProfile	61] [.6164.100]				
			Descri	ption					
		Task Attribute \	line.	Raw View					
	Com	non Tasks		Nun Yiun					
	2	Default Privile	90 15			(Select 0 to 15)		
		Maximum Priv	viege			(Select 0 to 15)		
		C Access Contro	ol List			0			
		 Auto Comman 	d [0			
		No Escape				(Select true or	false)		
		Timeout				0			
		Idle Time				0			

配置TACACS授權策略

預設情況下,「身份驗證策略」指向All_User_ID_Stores(包括AD),因此它保持不變。

導航到Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule above。

Operations	Policy Guest Access		Access Administration Work Centers					0	License Wa
letwork Resour	ces Netw	ork Device Groups	 Policy Conditions 	 Policy Results 	Policy Sets	Reports Se	sttings		
Define the Po For Policy Ex	licy Sets by o	configuring rules bas ministration > Syster	ed on conditions. Drag n > Backup & Restore	and drop sets on the > Policy Export Page	left hand side	to change the c	rder.		
Status	Nam	10	Description	on					
~	Defa	ult	Tacacs_D	efault					
Regular 🔾 Pr	roxy Sequen	ce 🔾							
▶ Authen	tication Po	olicy							
▼ Authori	zation Pol	icy							_
Except Standar	tions (0) d								
Sta	tus Rule	Name	Conditions (ident	ity groups and other	conditions)	Command	Sets	Shell Profiles	
2	Tacacs_D	Vefault		DenyAllCommand	s				Edit

配置了兩個授權規則;第一個規則根據網路管理員AD組成員身份分配TACACS配置檔案 ShellProfile和命令Set PermitAllCommands。第二個規則基於網路維護團隊AD組成員身份分配 TACACS配置檔案ShellProfile和命令Set PermitShowCommands。

Operations	Policy	Guest Access	 Administrat 	Work Centers			0	License Warning
twork Resour	ces Netw	vik Device Gravins	Policy Condit	ions Policy Results	Policy Sets	Renarts Sattinas		
Ear Dalicy Ex		ministration > System	n > Backup & Re	store > Dolicy Export Dep	1 0103 0005 1	abara aarriga		
Status	Nam	0	Des	cription	0			
	Defa	ult	Taca	acs_Default				
Regular 💿 Pr	roxy Sequence	æ0						
Authen	tication Po	licy						
+ Authori	zation Poli	cy						
Excep Standar	tions (0)							
Sta	tus Rule	Name	Conditions	(identity groups and other	r conditions)	Command Sets	Shell Profiles	
	PermitAll	Commands	if AD:Externa example.co	IGroups EQUALS m/Network Admins	then	PermitAllComman	ds AND ShellProfile	Edit 🕶
	PermitSh	owCommands	if AD:Externa example.co	IGroups EQUALS m/Network Maintenance	then	PermitShowComm	ands AND ShellProfi	le Edit 🕶
	Tacacs_D	efault	if no matches, t	hen DenyAllComman	ds			Edit 🕶

配置Cisco IOS路由器以進行身份驗證和授權

完成這些步驟,設定用於驗證和授權的Cisco IOS路由器。

1.使用username命令建立具有完全回退許可權的本地使用者,如下所示。

username cisco privilege 15 password cisco 2.啟用aaa new-model。定義TACACS伺服器ISE,並將其放入組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

附註:伺服器金鑰與之前在ISE伺服器上定義的金鑰匹配。

3.使用test aaa命令測試TACACS伺服器的可達性,如下所示。

Router#test aaa group tacacs+ admin Krakow123 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。

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 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

附註:建立的方法清單名為AAA,稍後在將其分配給行vty時使用。

5.將方法清單分配給行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



Cisco IOS路由器驗證

1.以admin身份telnet至Cisco IOS路由器,該管理員屬於AD中的完全訪問組。Network Admins組是 AD中對映到ISE上設定的ShellProfile和PermitAllCommands命令的組。嘗試運行任何命令以確保完 全訪問。

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. Telnet至Cisco IOS路由器,使其成為屬於AD中有限訪問組的使用者。網路維護組是AD中對映到 ISE上設定的**ShellProfile**和**PermitShowCommands**命令的組。嘗試運行任何命令以確保只能發出 show命令。

Username:**user** Password:

Router#show ip interface brief | exclude unassignedInterfaceIP-AddressOK? Method StatusProtocolGigabitEthernet0/010.48.66.32YES NVRAM upup

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

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

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



1.導覽至Operations > TACACS Livelog。確保看到已完成的嘗試。

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 🕶	😵 Refres	sh					Refresh Eve
Generated Time	Status All 🔻	Details	Username 🕐	Type All T	Authentication P	olicy (Authorization Policy
2015-08-18 14:28:12.011	_	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	8	ò	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:47.387	~	ò	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	~	ò	user	Authentication	Tacacs_Default >	> Default >> Default	
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	
2015-08-18 14:20:42.923	~	ò	admin	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:20:42.762	~	à	admin	Authentication	Tacacs_Default >	> Default >> Default	

2.按一下其中一個紅色報表的詳細資訊。以前執行的失敗命令可見。

verview	
Request Type	Authorization
Status	Fail
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		

疑難排解

錯誤:13025命令無法匹配Permit規則

檢查SelectedCommandSet屬性以驗證預期的Command Sets是否由授權策略選擇。

相關資訊

技術支援與文件 - Cisco Systems

<u>ISE 2.0版本說明</u>

ISE 2.0硬體安裝指南

<u>ISE 2.0升級指南</u>

ACS到ISE遷移工具指南

ISE 2.0 Active Directory整合指南

ISE 2.0引擎管理員指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。