配置ISE 2.0 TACACS+身份验证命令授权

目录

简介 背景信息 先决条件 要求 使用的组件 配置 网络图 配置 <u>配置ISE进行身份验证和授权</u> 加入ISE 2.0到Active Directory 添加网络设备 启用设备管理服务 配置TACACS命令集 配置TACACS配置文件 配置TACACS授权策略 配置Cisco IOS路由器以进行身份验证和授权 验证 <u>Cisco IOS路由器验证</u> ISE 2.0验证 故障排除 相关信息

简介

本文档介绍如何基于Microsoft Active Directory(AD)组成员身份配置TACACS+身份验证和命令授权。

背景信息

要根据具有身份服务引擎(ISE)2.0及更高版本的用户的Microsoft Active Directory(AD)组成员身份配置TACACS+身份验证和命令授权,ISE使用AD作为外部身份库来存储资源,例如用户、计算机、组和属性。

先决条件

要求

Cisco 建议您了解以下主题:

• Cisco IOS路由器完全正常运行

- •路由器和ISE之间的连接。
- ISE服务器已引导并且与Microsoft AD连接

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科身份服务引擎2.0
- •思科IOS[®]软件版本15.4(3)M3
- Microsoft Windows Server 2012 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

配置

配置的目的是:

- 通过AD验证Telnet用户
- 授权telnet用户,使其在登录后进入特权执行模式
- 检查并将每个执行的命令发送到ISE进行验证

网络图



配置

配置ISE进行身份验证和授权

加入ISE 2.0到Active Directory

1.导航到**管理>身份管理>外部身份库> Active Directory >添加**。提供加入点名称、Active Directory域并点击**提交。**

Operations	Policy	Guest Access	✓ Administra	ition 🕨 Wo	rk Centers	
sources + De	vice Portal Ma	nagement pxGrid	d Services >	Feed Service	pxGrid Identity M	apping
Identity Source \$	Sequences	 Settings 				
Connec	ction					1.0
Active Di	rectory Domair	AD example.com				ω Φ
Submit	Cancel					

2.当提示将所有ISE节点加入此Active Directory域时,点击是。

1	Would you like to Join all ISE Nodes to this Active Directory Domain?
	Yes No

3.提供AD用户名和密码,然后单击确定。

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 ()		
l	OK Cancel	

在ISE中访问域所需的AD帐户可以具有下列任一项:

- 将工作站添加到相应域中的域用户权限
- 在创建ISE计算机的帐户后将ISE计算机加入域之前,在相应计算机容器上创建计算机对象或删除计算机对象权限

注意:思科建议禁用ISE帐户的锁定策略,并配置AD基础设施,以便在为该帐户使用错误密码 时向管理员发送警报。输入错误密码时,ISE不会在必要时创建或修改其计算机帐户,因此可 能会拒绝所有身份验证。

4.复查工序状态。节点状态必须显示为已完成。单击 Close。

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

5. AD状态为运行。

Operation	ns	Guest A	ccess	✓ Admir	nistration	► Wa	ork Centers
urces	Device Portal M	anagement	pxGrid	Services	Feed S	ervice	pxGrid Iden
entity Sou	Irce Sequences	 Settings 					

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

6.定位至**"组">"添加">"从目录选择组">"检索组"。**选中**Network Admins** AD Group和**Network** Maintenance Team AD Group复选框,如下图所示。

注意:用户admin是网络管理员AD组的成员。此用户具有完全访问权限。此用户是网络维护团队AD组的成员。此用户只能执行show命令。

Domain example com		
me Filter *	C Filter *	iter Al I
Retrieve Groups 62 Groups Retrieve	d.	
ame	Group SID example com/S 1 5 32 562	Group Type
rample.com/Builtin/Event Log Readers	example.com/S-1-5-32-562	BUILTIN, DOMAIN LOCAL
rample.com/Builtin/Guests	example.com/S.1.5.32.546	BUILTIN, DOMAIN LOCAL
rample.com/Builtin/Hyper-V Administrators	example.com/S-1-5-32-578	BUILTIN DOMAIN LOCAL
kample.com/Builtin/IIS_IUSRS	example.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Incoming Forest Trust Builders	example.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Network Configuration Operato	example.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Performance Log Users	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Performance Monitor Users	example.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Pre-Windows 2000 Compatible	Ac example.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Print Operators	example.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/RDS Endpoint Servers	example.com/S-1-5-32-576	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/RDS Management Servers	example.com/S-1-5-32-577	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/RDS Remote Access Servers	example.com/S-1-5-32-575	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Remote Desktop Users	example.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Remote Management Users	example.com/S-1-5-32-580	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Replicator	example.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Server Operators	example.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Terminal Server License Serve	rs example.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Users	example.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Windows Authorization Access	Gr example.com/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
kample.com/Builtin/Windows Authonzation Access kample.com/Network Admins	str example.com/s-1-5-32-560 S-1-5-21-70538695-790656579-4293929703	2-1239 GLOBAL

OK Cancel

7.单击**保存**以保存检索到的AD组。



添加网络设备

导航至**工作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)>网络设备(Network Devices)**。单击 Add。提供名称、IP地址,选中TACACS+**身份验证** 设置复选框并提供共享密钥。

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 🗌				

启用设备管理服务

导航到**管理>系统>部署。选**择所需的节点。选中Enable Device Admin Service复选框,然后单击 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				

注意:对于TACACS,您需要安装单独的许可证。

配置TACACS命令集

配置了两个命令集。用户admin的第一个**PermitAllCommands**,它允许设备上的所有命令。第二个 **PermitShowCommands**用于仅允许show命令的用户用户。

1.导航到**工作中心>设备管理>策略结果> TACACS命令集。**单击 Add。提供名称 PermitAllCommands,选中Permit any command复选框(未列出),然后单击Submit。

Home	 Operations 	ons ► Policy ► Gue		Administration	✓ Work Centers		
Groups	Network Resource	ces Netwo	ork Device Groups	 Policy Conditions 		Policy Sets	
TAC/	ACS Command Sets	s > New					
		1	Name * Permit	AllCommands			
		De	scription				
2 Pe	rmit any command t	nat is not list	ed below 🔽				
	+ Add	h - C iEd	it 🕈 Move Up	↓ Move Down			
(Grant		Command	Argu	ments		
	No data found.	6					

2.导航到**工作中心>设备管理>策略结果> TACACS命令集。**单击 **Add。**提供名称 **PermitShowCommands**,单击**Add**并允许**show**和**exit**命令。默认情况下,如果Arguments留空,则 包括所有参数。单击"Submit"。

Home	 Operations 	ons ► Policy ► Guest		Administration	✓ Work Centers	
Groups	 Network Resource 	rces Netw	vork Device Groups	 Policy Conditions 		Policy Sets
TA	CACS Command Set	s > New				
Co	mmand Set					
		1	Name • Permit	ShowCommands		
		D	escription			
P	ermit any command to 0 Selected	that is not lis	ted below			
2	+ Add 🛍 Tras	h• ŒE	dit 🕇 Move Up	↓ Move Down		
- 1	Grant		Command	Argu	uments	
<u>а</u> Г	PERMIT		show			
۲Ľ	PERMIT		exit			

配置TACACS配置文件

配置单个TACACS配置文件。TACACS配置文件与ACS上的外壳配置文件概念相同。实际的命令实施通过命令集完成。导航到工作中心(Work Centers)>设备管理(Device Administration)>策略结果 (Policy Results)> TACACS配置文件(TACACS Profiles)。单击 Add。提供名称ShellProfile,选中 Default Privilege复选框,然后输入值15。单击Submit。

cisco	Identi	y Services	Engine	Home	+ Operations	+ Policy	Guest Access	Administration	- Work Centers			
 Trus 	stSec	· Device A	dministration	1.5.61	15.3 515.1							e seri le c
Overv	iew	Identities	User Identity	Groups	Network Resource	rces Netv	vork Device Groups	Policy Conditions	· Policy Results	Policy Sets	Reports	Settings
TACACS	S Comr	nand Sets	G	TACA	CS Profiles > New							
TACACS	S Profile	05		TAC	ACS Profile							
						1 Na	me* ShellProfile	611 (Constant)				
						Descri	ption					
					Task Attribute	View	Raw View					
				Com	mon Tasks							
				2	🕑 Default Privi	lege 15		HULE HELD	(Select 0 to 15))		
					Maximum P	rivilege		н. с.р.: н	(Select 0 to 15)		
					Access Con	trol List			0			
					Auto Comm	and			0			
					No Escape	Ē			(Select true or	false)		
					Timeout	Ē			0			
					🗆 Idle Time	Ē			0			

配置TACACS授权策略

默认情况下,"身份验证策略"(Authentication Policy)指向All_User_ID_Stores(包括AD),因此它保持不变。

导航至工作中心(Work Centers)>设备管理(Device Administration)>策略集(Policy Sets)>默认 (Default)>授权策略(Authorization Policy)>编辑(Edit)>在上述位置插入新规则(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 Setti	ngs	
Define the Po For Policy Ex	licy Sets by o port go to Ad	configuring rules bas ministration > Syster	ed on conditions. Drag m > Backup & Restore	and drop sets on the > Policy Export Page	e left hand side	to change the ord	br.	
Status	Nam	0	Description	on				
~	Defa	ult	Tacacs_D	efault				
Regular 🔾 P	roxy Sequence	e 🔿						
Authen	tication Po	licy						
+ Author	ization Poli	cy						
Except	tions (0)							
Standar	d							
Sta	tus Rule I	Name	Conditions (ident	ity groups and other	conditions)	Command Se	s Shell Profile	15
	Tacacs_D	efault		DenyAllCommand	is			Edit

配置两个授权规则;第一条 规则根据Network Admins AD Group membership分配TACACS配置文

件ShellProfile和命令Set PermitAllCommands。第二条 规则根据网络维护团队AD组成员资格分配 TACACS配置文件ShellProfile和命令Set PermitShowCommands。

Operations	▶ Policy	Guest Access	•	Administration	- Work Centers					0	License Warning
stwork Resour	rces Netw	ork Device Groups	۰P	olicy Conditions	 Policy Results 	Policy Set	s R	teports S	ettings		
For Policy Ex	port go to Ad	ministration > Syste	m > B	ackup & Restore	Policy Export Page						
Status	Nam	0		Descriptio	n						
×	Defa	ult		Tacacs_D	efault						
Regular 💿 P	roxy Sequent	20 C									
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	
	PermitAlk	Commands	if	AD:ExternalGroup example.com/Net	ps EQUALS work Admins		then	PermitAl	Commands	AND ShellProfile	Edit 👻
	PermitSh	owCommands	if	AD:ExternalGroup example.com/Net	ps EQUALS work Maintenance T	eam	then	PermitSh	owComma	nds AND ShellProfi	le Edit 🕶
2	Tacacs_D	efault	if n	o matches, then	DenyAllCommand	is					Edit 💌

配置Cisco IOS路由器以进行身份验证和授权

完成以下步骤以配置Cisco IOS路由器以进行身份验证和授权。

1.使用username命令创建具有完全回退权限的本地用户,如下所示。

username cisco privilege 15 password cisco 2.启用aaa new-model。定义TACACS服务器ISE,并将其放置在ISE_GROUP组中。

aaa new-model

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

注意: 服务器密钥与之前在ISE服务器上定义的密钥匹配。

3.如图所示,使用test aaa命令测试TACACS服务器的可达性。

Router#test aaa group tacacs+ admin Krakow123 legacy Attempting authentication test to server-group tacacs+ using tacacs+ User was successfully authenticated. 上一个命令的输出显示TACACS服务器可访问,且用户已成功通过身份验证。

4.配置登录并启用身份验证,然后使用exec和命令授权,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

注意:创建的方法列表名为AAA,稍后在将其分配至线路vty时使用。

5. 将方法列表分配给行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

验证

Cisco IOS路由器验证

1. Telnet至Cisco IOS路由器,作为属于AD中完全访问组的管理员。Network Admins group是AD中 映射到ISE上的ShellProfile和PermitAllCommands命令集的组。尝试运行任何命令以确保完全访问 。

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.以属于AD中有限访问组的用户Telnet至Cisco IOS路由器。网络维护团队组是AD中映射到ISE上设置的ShellProfile和PermitShowCommands命令的组。尝试运行任何命令以确保只能发出show命令

0

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.

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

1.导航到**操作> TACACS实时日志。**确保看到所做的尝试。

cisco Identity Sen	vices Engine	Home	- Operations	Polloy P	Guest Access	Administration	Work Centers
RADIUS Livelog T	ACACS Livelog	Reports	 Troubleshoot 	 Adaptive Network 	ork Control		
Add or Remove Co	lumns 👻 🍪 Refr	esh					Refresh Eve
Generated Time	Status All 🔻	Details	Username 🕐	Type All T	Authentication P	Policy ()	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 😵	à	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:53.	013 😵	à	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:47.	387 🗹	O.	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:41.	034 🗹	à	user	Authorization			Tacacs_Default >> PermitShowCo
2015-08-18 14:27:40.	415 🗹	à	user	Authentication	Tacacs_Default >	>> Default >> Default	
2015-08-18 14:24:43.	715 🗹	Q	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 🗹	à	admin	Authentication	Tacacs_Default >	>> Default >> Default	
2015-08-18 14:20:42.	923 🗹	Q	admin	Authorization			Tacacs_Default >> PermitAllComm
2015-08-18 14:20:42.	762 🗹	ò	admin	Authentication	Tacacs_Default >	>> Default >> Default	

2.单击其中一个红色报表的详细信息。以前执行的失败命令可见。

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

故障排除

Error:13025命令无法匹配Permit规则

检查SelectedCommandSet属性以验证预期命令集是否已由授权策略选择。

相关信息

<u>技术支持和文档 - Cisco Systems</u>

ISE 2.0版本说明

ISE 2.0硬件安装指南

<u>ISE 2.0升级指南</u>

ACS至ISE迁移工具指南

ISE 2.0 Active Directory集成指南

ISE 2.0引擎管理员指南

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。