# 配置基於Radius和TACACS的使用者身份驗證

### 目錄

<u>簡介</u>

<u>必要條件</u>

<u>需求</u>

<u>採用元件</u>

#### <u>設定</u>

<u>適用於vEdge和控制器的基於RADIUS的使用者身份驗證和授權</u> <u>vEdge和控制器的TACACS型使用者驗證和授權</u>

#### <u>相關資訊</u>

## 簡介

本文檔介紹如何為使用ISE的vEdge和控制器配置基於RADIUS和TACACS的使用者身份驗證和授權。

必要條件

需求

本文件沒有特定需求。

採用元件

本演示使用ISE 2.6版。vEdge雲和控制器運行19.2.1

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。

## 設定

Viptela軟體提供三個固定使用者群組名稱:basic、netadmin和operator。 您必須將使用者指派給至 少一個群組。預設TACACS/Radius使用者自動置於基本組中。

#### 適用於vEdge和控制器的基於RADIUS的使用者身份驗證和授權

步驟 1.為ISE建立影片半徑詞典。若要這麼做,請建立包含下列內容的文字檔案:

```
# -*- text -*-
```

- #
- # dictionary.viptela

# # # Version: #	\$Id\$		
VENDOR	Viptela	4191	6
BEGIN-VENDOR	Viptela		
ATTRIBUTE	Viptela-Group-Name	1	string

步驟 2.將詞典上傳到ISE。為此,請導航到策略>策略元素>詞典。從詞典清單中,導航到Radius > Radius Vendors,然後按一下Import(如圖所示)。

Sets Profiling Posture Client Provisio	ning * Policy Elements			
aries + Conditions + Results				
Contarles	RADIUS Vendors			
	/an +as Xonn @input	(Detaport		
. E	C Name	<ul> <li>Vendor ID</li> </ul>	Description	
Cont	Armony	14079	Octonary for Wendor Arengade	
Country Country Country	Attached Locent	800	Dictionary for Wendor Acatel-Lucent	
in the set of the set	C Andre	1403	Determine for Meeter Acuta	
Li Internation	D becade	1588	Dictionary for Wandor Bracade	
C International Conference	C Care		Deficerary for Vendor Case	
(iii) Internal (her	C Constant	00	Electronary by Manday Caro, MISM	
C IONASSET		2016	Decisional y no remain cano marri	
E #		35306	Defenses by Meeter MW	
LLIDP		11	Participants for International	
MAC .		34.36	Definition for bander Latiner	
MOM_LOG		11.1	Performent for Manager Minister	
i wa		144	Continents for Interfer Material Context	
Lin Multo		200	successive to version metalogical symptot	
C Multimedia		1963	country to rendo notice	
I NETFLOW		14042	sectorary to venue accert	
Destaurity Process				
C RAAR				
Didde/TE destance				
C Normaliand Radius				
Tester0				
E Postas				
C PROFILIR				
Radue .				
<ul> <li></li></ul>				
<ul> <li>IADUS Medors</li> </ul>				
(iii) Senator				
E Sheet				
E SP				
TAGACS				
E YOMAO				

上傳您在步驟1中建立的檔案。

Identity Services Engine	Home + Co	ntext Valbility 🔹 🕨	Operations	* Policy	+ Administration	Work Centers
Policy Sets Profiling Posture	<b>Client Provisioning</b>	Policy Elements				
Dictionaries + Conditions + R	esuits					

Dictionaries		the state of the second se		
	2	Use this for to import a HADIUS	s vendor, beect the tile using the browser and	cick import.
(a + 15. +	161	* Vendor file:		
+ IT Guilt		Crowne in Constant Advent		
Cuestilizzens				
<ul> <li>I Meetike Materine</li> </ul>		Import Cancel		
<ul> <li>Image of the second seco</li></ul>				
• Ti Internal"A				
III InternetEnderint				
III Internal law				
<ul> <li>III IOTASSET</li> </ul>				
• 🗇 P				
• 11 LLDP				
+ III MAG				
<ul> <li>III MDM LOG</li> </ul>				
<ul> <li>III MHE</li> </ul>				
<ul> <li>III MUD</li> </ul>				
<ul> <li>Multimedia</li> </ul>				
<ul> <li>III NETFLOW</li> </ul>				
<ul> <li>III Network Access</li> </ul>				
Metwork Condition				
<ul> <li>III NAMP</li> </ul>				
<ul> <li>III NMAPExtension</li> </ul>				
<ul> <li>III Normalised Radius</li> </ul>				
<ul> <li>PassiveiD</li> </ul>				
<ul> <li>Posture</li> </ul>				
<ul> <li>PROFILER</li> </ul>				
* 🧱 Radius				
<ul> <li>III IETE</li> </ul>				
<ul> <li>RADIUS Vendors</li> </ul>				
<ul> <li>Ession</li> </ul>				
<ul> <li>III SNMP</li> </ul>				
<ul> <li>11 \$50P</li> </ul>				
<ul> <li>TACACS</li> </ul>				
<ul> <li>10-MAC</li> </ul>				
<ul> <li>III Threat</li> </ul>				

步驟 3.建立授權配置檔案。在此步驟中,Radius授權配置檔案將(例如)netadmin許可權級別分配 給經過身份驗證的使用者。為此,請導航到策略>策略元素>授權配置檔案,並指定兩個高級屬性 ,如下圖所示。

thereity Services Engine	Home + Context Visibility + Operations Policy + Administration + Work Centers
Policy Sets Profiling Posture C	Sant Provisioning Policy Demons
Dictionaries + Conditions + Rasul	
0	
+ Authentication	Authorization Profiles > vEdge-netadmin
	Nectorization Provide
Authorization	• Name utop-retadron
Authorization Profiles	Description
Downloadable ACLs	*Access Type Access Accept *
+ Profiling	Network Device Profile (BCOsto) + (9)
1 Barbar	
	Service Template
+ Client Provisioning	Track Movement () (2)
	Passive Identity Tracking
	Common Tasks
	* Advanced Attributes Settings
	Radue:Service-Type 🙃 * NAS Prompt O
	Viptela Viptela Group Name 💿 = (vetadmin 🌀 — 🕂
	* Attributes Details
	Access Type = ACCESS ACCEPT
	Service-Type = 7 Vertela Column Name = netation

步驟 4.根據您的實際設定,策略集的外觀可能有所不同。出於本文演示的目的,我們建立了稱為終 端訪問的策略條目,如下圖所示。

222	benity Se	rvices Engine	Pare	+ Context Vielbilly	+ Operations	- Policy	* Administration	+ Web Centers				
Policy 1	inte Pro	fling Posture	Clert Provisio	ning - A Policy Dans	eria							
Policy	Sets								Reset Policyset Hitsour			lava
۲	Status	Policy Set Na	ne .	Description		Condition			Allowed Protocols / Server Sequence	Hits	Actions	View
Bearth												
	0	Terrinal Access				10 14	due NAS Port Type B	DOALS Vitual	Oxfaul Network Access + + •	1	o	>

點選>,下一個螢幕會出現,如下圖所示。

the lower for the	ces Engine equina .	Contest Halding + Operations	+Policy = + /	desiniation	+ Mort Centers			S. 0	0 0
Policy Sets Profile	ng Posture Client Provision	ng 🔸 Policy Elements							
Policy Sets + T	erminal Access						eet Policyaet Hitoourta	Head	(Int
Status P	folicy Set Name	Description	Conditions				Allowed Protocols / Se	ner Seguend	e Hits
Search									
0	Service Access		III Radua N	A5-Port-Type D1	DOALS Vitual		Default Network Access		
> Automication I	Palicy (1)								
> Authorization Pr	olicy - Local Exceptions								
3 Autorization Pr	olicy - Global Exceptions								
V Autorization Pr	olicy (2)								
				Results					
the Status	Rule Name	Conditione		Profiles		Security	Groups	Hits	Actions
Search.									
1 0	vEstpe-netactroin	<ul> <li>MentlyGroup Name 800 Groupstall, admin</li> </ul>	ALS User Identity	(rubiper	wadnin]	• Select	un lat 🔹 🔻	+ 1	0
۲	Colout			(+ Ourpho	orea	· Detect	un îst 🔹	• •	٥

Reset Seve

此策略根據使用者組lab\_admin進行匹配並分配在第3步中建立的授權配置檔案。

步驟 5.定義NAS (vEdge路由器或控制器),如下圖所示。

Ilentity Services Engine Home Context Visibility Operations Policy Administration Work Centers	Q,
System      Identity Management     Vetwork Resources     Device Portal Management     pxGrid Services     Feed Service     Threat Centric NAC	
Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM      Location Server	ces
0	
Network Devices List > vedge-01	
Default Device * Name vEdge-01	
Device Security Settings Description	
IP Address * IP : 10.48.87.232 / 32	- 
* Device Profile dia Cisco 💌 🕀	
Model Name	
Software Vareion	
* Network Device Group	
IPSEC No. Cot To Default	
All Device Types Set To Default	
← RADIUS Authentication Settings	
RADIUS UDP Settings	
Protocol RADIUS	
* Shared Secret Show	
Use Second Shared Secret 🔲 🛞	
Show	
CoA Port 1700 Set To Default	
RADIUS DTLS Settings (1)	
DTLS Required	
Shared Secret radius/dtls	
CoA Port 2083 Set To Default	
Issuer CA of ISE Certificates for CoA Select if required (optional)	
DNS Name	
General Settings	
Enable KeyWrap 🗌 🕡	
* Key Encryption Key Show	
* Message Authenticator Code Key Show	

## 步驟 6.配置vEdge/控制器。

```
system
aaa
auth-order radius local
radius
server 10.48.87.210
vpn 512
key cisco
exit
!
```

步驟 7.驗證。登入到vEdge並確保將netadmin組分配給遠端使用者。

vEdgeCloud1# show users

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

## vEdge和控制器的TACACS型使用者驗證和授權

步驟 1.建立TACACS配置檔案。在此步驟中,會將建立的TACACS設定檔指派給已驗證的使用者 ,例如netadmin許可權層級。

• 從Custom attribute部分選擇Mandatory以增加屬性:

類型	名稱	價值
必填	Viptela-Group-Name	netadmin

thentity Services Engine	Home + Context Validity + Ope	ndors + Policy + Administration 🖪	Work Centers	
Network Access     Ouest Access	Thatlac + 8100 + Pollar + 7	Posture - Ceutos Administration - Pasatust	2	
+ Overview + Identifies User Identifi	Croups Ext.Id Sources + Network I	Resources Policy Elements Device Admin	Pulcy Sets Reports Settings	
0	The second s			
+ Conditiona	TACACE Points > risign			
Network Conditions	No.	ne «Eitpe_netadmin		
• Results				
Alound Protocols	Descripti	line .		
TAGACE Command Sets	Task Atribute View	Raw View		
	Common Tasks			
	Common Task Type [the] 1			
	Orlant Protege	0	(Select 8 to 18)	
	🗇 Maximum Privilege	0	(Select 9 to 18)	
	<ul> <li>Access Control Unit</li> </ul>	0	1	
	<ul> <li>Arts Command</li> </ul>	0	1	
	<ul> <li>No Except</li> </ul>	0	(Select true or false)	
	<ul> <li>Timest</li> </ul>	0	Minutes (2-0000)	
	🗇 ide Tire	0	Minutes (2-9999)	
	Custom Attributes			
	+ AN BINNE COM			۰-
	C Type N	iame Value		
	[Handstoy 4]	Istela-Group-Name netadmin	0	~*
				Cancel Save

### 步驟 2.為SD-WAN建立裝置組。

20 Martily Services Engine wants + Cantad Validity + Operator	a + Maky Administration + Mark Carriers	
Hyden - Henty Messpenett - Select Resurses - Deite Post Heng	ement paddet Bankow + Feed Bankov + Thread Cantrix NAC	
Nation Devices Nation Device Stronger     Nation Device Profiles     External No	OUS Servers AUOUS Server Sequences NAC Managers Extend MOM	* Location Services
Nationsh Device Groups		
Al Groups Choose prop -		
Chates And Dates Clin Stee Charges	nten kimpet dibert: Effethen / Spencht /	Cologon All De -
C Name	Description	No. of Network Devices
<ul> <li>A device type</li> </ul>	All Device Types	-
O 80-884		1
<ul> <li>Allowers</li> </ul>	AT Locations	
<ul> <li>In PRECidence</li> </ul>	In this a RADUS over POSC Device	-

## Add Group

Name *	SD-WAN		
Description			
Parent Group *	All Device Types	×т	



## 步驟 3.配置裝置並將其分配給SD-WAN裝置組:

Network Devices Ltd > vfdge-01	
Network Devices	
* Name v6spe-01	
Description	
P Address • * * P: 10.46.67.232 / 12	· .
Device Profile Caco + 19	
Model Name *	
Software Version	
* Network Device Oncur	
Location At Locations O Set To Default	
PSEC No Contraction	
Device Type SD-WAN O Set To Default	
BADUS Autorication Sellings	
E + SACACS Authentication Settings	
Legacy Gen Device	
TACACE Draft Compliance Single Connect Support	
Advanced Trustlec Settings	
Save Reset	

Save

Cancel

根據您的實際設定,策略集的外觀可能有所不同。出於本文檔中演示的目的,將建立策略。

the best Services Engr	w Hore + Context Heldelly	• Operations • Paloy	· Advertise ·	Work Centers				- N 1	• •	
+ InmontAccess + Ouest-N	com + Tratfec + 8100 + P	ofter + Postare + Device Adv	rotation A Passivell	0						
* Overview * Identifies UK	er reently Groups . Get to Sources	Heleon Resources - + Pring D	enerts Deuts-Alexe	Putty Sets Reports	Settings					
Policy Sets						Constant Proto	and Witchison			-
							and the second se	-	-	
Status Policy Set	Name Description	Conditions				Altrend Protocols / Serv	r Sequence	105 7	-ctions	Ver
bard-										
/ © 1000		Q 004	OE Device Type ISSIAL	A Al Onica Typest00-1	104N	Default Device Admin			0	>
O teas	Secon Delect	policy set				Delaut Device Admin	++ +	•	0	•
									<b>H</b> )(	ten )

### 按一下>,下一個螢幕將會顯示,如下圖所示。此策略根據名為SD-WAN的裝置型別進行匹配,並 分配在步驟1中建立的Shell配置檔案。

the second second	nicos Engine interes i	Context Visibility In Operations	• Nacy • Americana • Rich Carlos	5 6 6	e •
A Referent Access	+ Guest Access + TrustBec	+ 8100 + Poller + Poller	Opera Adversionation     F PassiveD		
+ Overview - + 10	berthes User-Dently-Drouge	Cold Bourges + Network Resource	+ Putry Danards Deuter Amer Putry Sets Reports Bellings		
Policy Sets +	vEdges		Reset Policytet Mitorynta	(test)	Seve
Status.	Policy Set Name	Description	Conditions Allowed Protocols / S	ever beganne.	140
See 1					
۲	rläps		Q DEVELORIS Spectral Anterior Spectral International Detail Device Admin.	•• •	
3 Autoritatio	n Policy (1)				
> Autorization	Policy - Local Exceptions				
> Autorization	Policy - Global Exceptions				
* Autorization	Pulky (2)				
			Reads		
- Data	Rule Name	Conditions	Command Bats Bhall Profiles	100	Actions
Search				_	
٥	vExpension	a. 10x10,01x2 None 800	All Carrierity Grapical, John	+	0
0	Owned		(alternational art)	+ +	0

Reset Seve

#### 步驟 5.配置vEdge:

```
system
aaa
auth-order tacacs local
!
tacacs
server 10.48.87.210
vpn 512
key cisco
exit
!
```

步驟 6.驗證。登入到vEdge並確保將netadmin組分配給遠端使用者:

vEdgeCloud1# show users

SESSION	USER	CONTEXT	FROM	PROTO	AUTH GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

## 相關資訊

- 思科ISE裝置管理規範部署指南: <u>https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973</u>
- 配置使用者訪問和身份驗證:<u>https://sdwan-</u> <u>docs.cisco.com/Product\_Documentation/Software\_Features/Release\_18.4/02System\_and\_Interface</u>

#### 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)。