# 在DNA Center和ISE 3.1上配置RADIUS外部身份 驗證

F	目錄	
<u>簡</u>		
必	<u>必要條件</u>	
	<u>需求</u>	
	採用元件	
設	<u>設定</u>	
驗	<u>驗證</u>	
更	<u>更多角色</u>	

## 簡介

本文檔介紹如何使用運行3.1版的Cisco ISE伺服器在Cisco DNA Center上配置RADIUS外部身份驗 證。

### 必要條件

#### 需求

思科建議您瞭解以下主題:

• Cisco DNA Center和Cisco ISE已經整合,並且整合處於活動狀態。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco DNA Center 2.3.5.x版本。
- Cisco ISE 3.1版本。

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

步驟 1. 登入Cisco DNA Center GUI 並導航至System > Settings > Authentication and Policy Servers。

驗證是否已配置RADIUS協定以及ISE狀態是否為Active(對於ISE型別伺服器)。

Settings / External Services

#### Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

-		100 TEL 100
( Add	V	1 Export

⊕ Add ∨ ① Export				As of: Jul 19, 2023 4:38 PM 🛛 📿
IP Address	Protocol	Туре	Status	Actions
1000	RADIUS_TACACS	AAA	ACTIVE	
0.000	RADIUS	ISE	ACTIVE	
1 million 1 - 2	RADIUS	ААА	ACTIVE	
10.11 million	RADIUS	ААА	ACTIVE	
	RADIUS_TACACS	AAA	ACTIVE	



#### 注意:RADIUS\_TACACS協定型別適用於此文檔。



警告:如果ISE伺服器未處於活動狀態,則必須首先修復該整合。

步驟 2.在ISE伺服器導航到管理>網路資源>網路裝置,點選過濾器圖示,寫入Cisco DNA中心IP地 址,確認條目是否存在。如果是,請繼續執行步驟3。

如果缺少條目,您必須看到無可用資料消息。

**Network Devices** 

										Selected 0 Total 0	C	٢
🖉 Edit	$+ \operatorname{Add}$	C	) Duplicate	Import ريل	$\triangle$ Export $\vee$	Generate PAC	📋 Deleti	$\sim$		Quick Filte	er $\sim$	$\bigtriangledown$
	Name	^	IP/Mask	Profile N	lame	Location		Туре	Description			
			x.x.x.x	_								
No data	available											

在這種情況下,您必須為Cisco DNA Center建立一個網路裝置,然後按一下Add按鈕。

#### Network Devices

							Selected 0 Total 0 🖯	Ø
0 Ed	iit 🕂 Add 🗓	Duplicate 🕁 Import	🟦 Export 🖂 🔒 Generate P/	AC 📑 Delete 🗸			Quick Filter $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	$\nabla$
	Name $\land$	IP/Mask	Profile Name	Location	Туре	Description		
		x.x.x.x						
No	fata available							

在Cisco DNA Center中配置名稱、描述和IP地址(或地址),所有其他設定均設定為預設值,本文 檔中不需要這些設定。 Network Devices List > New Network Device

### Network Devices

<ul> <li>Name</li> </ul>	mxc-dnac	5			
Description	Cisco DNA	Center			
IP Ad	dress 🗸 * lP :	-	. <b>n</b> . *	/32	- 
* Device Profile	att Cisco	¥0			
Model Name		~			
Software Versio	n	~			
* Network Der	vice Group				
Location	All Locations	~ [	Set To D	efault	
IPSEC	Is IPSEC Device	~	Set To D	efault	
Device Type	All Device Types	~ (	Set To D	efault	

向下滾動並透過按一下RADIUS Authentication Settings覈取方塊並配置Shared Secret來啟用它。



RADIUS UDP Settings





提示:此共用金鑰將在以後需要,因此請將其儲存到其他位置。

然後,按一下Submit。

步驟 3.在ISE伺服器上,導航到策略>策略元素>結果,建立授權配置檔案。

確保您處於Authorization > Authorization Profiles下,然後選擇Add選項。

E Cisco ISE				Policy - Policy Eler	ments	<b>(</b> ) Q	0 7	9 Ø			
Dictionaries Condit	Dictionaries Conditions Results										
Authentication Allowed Protocols	Authentication Allowed Protocols Standard Authorization Profiles For Policy Export go to Administration > System > Backup & Restore > Policy Export Page										
Authorization	~	/ Edit	+ Add Duplicate	Delete		Selected 0		, s 2			
Authorization Profiles Downloadable ACLs	8		Name	Profile	^	Description		-			
			APs_19.5.0	🗮 Cisco 👔		172_19_5_0-INFRA_VN					
Profiling	>		AuthTemplate	🗮 Cisco 🕧							
Posture	>		Blackhole_Wireless_Access	🗮 Cisco 👔		Default profile used to blacklist wireless devices. Ensure that you configure a BLACK	40LE ACL on	the			
Client Provisioning	>		CY_CAMPUS_MAC	🗯 Cisco 🕧		CY_CAMPUS_MAC					
	1		CV Quest profile	th Cieco 🔿		PV Guest erafile					

#### 配置Name,增加Description以保留新配置檔案的記錄,並確保Access Type設定為 ACCESSES\_ACCEPT。

Results	
Authorization Profiles > Ne Authorization Profil	ew Authorization Profile
* Name	DNAC_AUTH_PROFILE
Description	External Authentication for Cisco DNA Center
* Access Type	ACCESS_ACCEPT ~
Network Device Profile	diste Cisco ∨⊕
Service Template	
Track Movement	
Agentless Posture	
Passive Identity Tracking	

在左側列中搜尋cisco-av-pair選項並將其選中。

在右列手動鍵入Role=SUPER-ADMIN-ROLE。

一旦它看起來像以下映像,請按一下Submit。



Access Type = ACCESS\_ACCEPT

cisco-av-pair = Role=SUPER-ADMIN-ROLE

步驟 4.在ISE伺服器上,導航到工作中心>分析器>策略集,配置身份驗證和授權策略。

#### 確定預設策略並按一下藍色箭頭進行配置。

≡ Cisco	ISE		Work Cer	iters • Profile	r			1	Q (2)	P	
Overview	Ext Id Sources	Network Devices	Endpoint Classif	ication No	ode Config	Feeds	Manual Scans	More	• ~		
Policy Sets					F	leset	Reset Policyset	Hitcounts		Save	
🕂 Status	s Policy Set Name	Description	Con	ditions	Allow	ed Protoco	ls / Server Sequenc	ce Hits	Actions	Viev	w
Q Searc	ch										
$\otimes$	Wire-dot1x			Wired_802.1X	internal	_user	$\boxtimes   \lor  +$	0	ŝ	>	
$\otimes$	MAB		-	Wired_MAB	Default	Network Acc	cess $\propto -$	0	\$ <u>`</u>	>	
۲	Default	Default policy s	set		Default	Network Ac	cess $\propto +$	180517	\$ <u>}</u>	>	]

在Default Policy Set內部,展開Authentication Policy,並在Default部分下展開Options,並確保它 們與下面的配置匹配。

n	view Ex	t Id Sources	Network Devic	ces Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More ~	-
i	y Sets→	Default						Reset	Reset Policyset Hitcour	nts	Save
	Status P	olicy Set Name	Descript	tion Conditions					Allowed Protocols / Ser	ver Seque	nce Hits
	Q Search										
	•	Default	Default	t policy set				D	efault Network Access	∞ ~+	180617
										_	
4	uthenticatio	n Policy (3)									
(	Status	Rule Name	Cone	ditions				Use		Hits	Actions
(	Q Search										
				8				Internal End	ipoints 🛛 🛛 🗸		
	۲	MAB	OR	Wireless_MAB				> Options		4556	<u>لې</u>
				Wired 802.1X				All_User_ID	_Stores 🛛 🗸 🗸		
	0	Dot1X	OR	Wireless_802.1X				> Options		0	
								All_User_ID	_Stores 🛛 🗸		
								✓ Options			
								If Auth fail			
	0	Default						If User no	t found	62816	ŝ
								If Drosses	fail		
								II PIOCOSS	raii		



在預設策略集中,展開Authorization Policy,並選擇Add圖示以建立新的Authorization Condition。

≡ Cisco	ISE			Work Centers - P	rofiler			0	Q 0	) ja (¢
Overview	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More ~	
Policy Sets	→ Default						Reset	Reset Policyset Hitcou	nts	Save
Status	Policy Set Name	Description	Conditions					Allowed Protocols / Se	rver Seque	nce Hits
Q Sear	rch									
٥	Default	Default policy	set				1	Default Network Access	<u>a</u> ~+	180617
> Authentic	ation Policy (3)									
> Authoriza	tion Policy - Local Ex	ceptions								
> Authoriza	tion Policy - Global E	xceptions								
$\vee$ Authoriza	tion Policy (25)									
					Result	s				
🕒 Stat	tus Rule Name	Conditions	1		Profile	5	Security	Groups	Hits	Actions
Q Sei	arch									

#### 配置Rule Name,然後按一下Add圖示配置Condition。

≡	Cisco	ISE			Work Centers - F	Profiler				<b>)</b> (	) ,e ¢
Over	/iew	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	s Profiling Policies	More	-
Poli	cy Sets	→ Default						Reset	Reset Policyset Hitco	unts	Save
	Status	Policy Set Name	Description	Conditions					Allowed Protocols / S	erver Sequ	ence Hits
(	Q Sea	rch									
	0	Default	Default policy	set				_	Default Network Access	<u>∞</u> ~+	180617
>/	uthentic	ation Policy (3)	antions								
>/	uthoriza	tion Policy - Global Ex	ceptions								
$\sim$	uthoriza	tion Policy (26)									
						Results					
(	+ Sta	tus Rule Name	Conditions			Profiles		Security	Groups	Hits	Actions
(	Q Se	arch									
		DNAC-SUPER-AD	MIN-ROLE	+		Select from	list	- + Select fre	om list —		ŝ

作為情況的一部分,請將其與步驟2中配置的網路裝置IP地址關聯。

#### Conditions Studio

Library	Editor				_
Search by Name		Network Access-De	avice IP Address		×
		Equals 🗸	10.88.244.151		
:: E BYOD_is_Registered		Set to 'Is not'		Duplicate	Save
:: E Catalyst_Switch_Local_Web_Aut hentication			NEW AND OR		
:: E Compliance_Unknown_Devices					
:: E Compliant_Devices					
: E CY_Campus					
E CY_CAMPUS_MAC					
: E CY_Campus_voice					
: E CY_Guest					
E EAP-MSCHAPv2					
" <b>C</b> = = = = = = = = = = = = = = = = = = =					
				Close	Use

#### 點選儲存。

將它另存為新的庫條件,並根據需要為其命名,在這種情況下,命名為DNAC。

# Save condition

O Save as existing Library Condition (replaces current version and impact all policies that use this condition

 $\times$ 

Select from list		$\sim$
Save as a new Libra	ry Condition	
DNAC	Description (optional) Condition Description	7
	Close	Save

#### 最後,配置在步驟3中建立的配置檔案。

=	Cisco	ISE			Work Centers - I	Profiler			G	9 9 6	0 20 4
Over	view	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More	·
Poli	cy Sets	→ Default						Reset	Reset Policyset Hitcou	nts	Save
	Status	Policy Set Name	Description	Conditions					Allowed Protocols / Se	rver Seque	ince Hits
(	Q Sear	ch									
	0	Default	Default policy	set				1	Default Network Access	<u>∞</u> ~+	180617
> /	uthentic	ation Policy (3)									
> /	uthoriza	tion Policy - Local Ex	ceptions								
> /	uthoriza	tion Policy - Global E	xceptions								
$\sim l$	Authoriza	tion Policy (25)									
						Results					
0	• Stat	tus Rule Name	Conditions			Profile	5	Security	Groups	Hits	Actions
(	Q Sea	arch									
	•	DNAC-SUPER-AD	MIN-ROLE E DNAC			DNAC_AU	JTH_PROFILE ×	v+ Select from	m list $\sim$ +		ŝ

按一下Save。

# 步驟 5. 登入到Cisco DNA Center GUI,然後導航到System > Users & Roles > External Authentication。

#### 按一下Enable External User選項,並將AAA Attribute設定為Cisco-AVPair。

■ Cisco DNA Center	System / Users & Roles
User Management Role Based Access Control	External Authentication
External Authentication	<ul> <li>Cisco DNA Center supports external servers for authentication and authorization of external Osers. Use the helds in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choose it needs to be configured here on Cisco DNA Center.</li> <li>The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".</li> <li>An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".</li> <li>Cisco-AVPair</li> <li>Cisco-AVPair</li> <li>Cisco-AVPair</li> <li>Update</li> </ul>



注意:ISE伺服器在後端使用Cisco-AVPair屬性,因此第3步中的配置有效。

向下滾動檢視AAA伺服器配置部分。在步驟1中配置ISE伺服器的IP地址,並在步驟3中配置共用金 鑰。

然後按一下檢視高級設定。

~ AAA Server(s)

Primary AAA Server			Secondary AAA Server		
IP Address			IP Address		
In the second		$\sim$	MUMUE IN		$\sim$
Shared Secret			Shared Secret		
	SHOW			SHOW	
	Info			Info	
View Advanced Settings			View Advanced Settings		
Undate			Undate		
Update			Update		

確認已選取RADIUS選項,然後按一下兩個伺服器上的「更新」按鈕。

~ AAA Server(s)

Primary AAA Server		Secondary AAA Server			
IP Address		IP Address			
10 (11 100 A));					
Shared Secret		Shared Secret			
	SHOW		SHOW		
	Into		Info		
Hide Advanced Settings		Hide Advanced	Settings		
• RADIUS O TACACS		• RADIUS	⊖ TACACS		
Authentication Port		Authentication Po	rt		
1812		1812			
Accounting Port		Accounting Port			
1813		1813			
Retries		Retries			
3		3			
Timeout (seconds)		Timeout (seconds	)		
		4			

您必須看到每條成功消息。



現在您可以使用在ISE選單>管理>身份管理>身份>使用者下建立的任何ISE身份登入。

如果沒有任何建立,請登入ISE,導航到上面的路徑,然後增加新的網路訪問使用者。

■ Cisco ISE	Administration - Identity Management	0.0000
Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🖒 Export 🗸 🔮 Delete 🗸 🌔 Duplicate	Selected 0 Total 24 🖉 🔕

驗證

載入Cisco DNA Center GUI 和從ISE身份以使用者登入。

Cisco DNA Center The bridge to possible Success! Username test		cisco
<ul> <li>Success!</li> <li>Username test</li> <li>Password</li> </ul>	Ciso Th	<b>co</b> DNA Cente ne bridge to possible
Username test Password	✓ Succ	ess!
Password	Username test	
	Password	

DNA Center登入



注意:ISE標識上的任何使用者現在都可以登入。您可以為ISE伺服器上的身份驗證規則增加更精細的粒度。

登入成功後,使用者名稱顯示在Cisco DNA Center GUI上



# Welcome, test

歡迎畫面

# 更多角色

預設情況下,您可以對Cisco DNA Center上的每個角色重複這些步驟:SUPER-ADMIN-ROLE、 NETWORK-ADMIN-ROLE和OBSERVER-ROLE。

■ Cisco DNA Center	System / Users & Roles Q. (							
User Management	User Roles							
Role Based Access Control	Create customized roles for your organization, grant high level	access or granular functionality controls. When denying access, th	hose aspects of Cisco DNA Center are removed from the users inte	erface.				
External Authentication								
	1							
	Create a New Role	SUPER-ADMIN-ROLE	NETWORK-ADMIN-ROLE	OBSERVER-ROLE				
		Complete control of the Cisco DNA Center deployment, all access enabled.	General Purpose role without ability to change system configurations.	Read only access, unable to view some sensitive data in the system settings.				

在本文檔中,我們使用SUPER-ADMIN-ROLE角色示例,但是,您可以在ISE上為思科DNA中心上 的每個角色配置一個授權配置檔案,唯一的考慮是在步驟3上配置的角色需要與思科DNA中心上的 角色名稱完全匹配(區分大小寫)。

#### 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)。