將ISE配置為DNAC GUI的外部身份驗證

目錄
<u>簡介</u> 11. 11. 11. 11. 11. 11. 11. 11. 11. 11.
<u>必要條件</u>
<u>採用元件</u>
開始之前
<u>設定</u>
<u>(選項1)使用RADIUS配置DNAC外部身份驗證</u>
<u>(選項1)為RADIUS配置ISE</u>
<u>(選項2)使用TACACS+配置DNAC外部身份驗證</u>
<u>(選項2)為TACACS+配置ISE</u>
<u>驗證</u>
驗證RADIUS設定
<u>驗證TACACS+配置</u>
疑難 <u>排解</u>
<u>參考資料</u>

簡介

本文檔介紹如何將思科身份服務引擎(ISE)配置為用於Cisco DNA Center GUI管理的外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題:

- TACACS+和RADIUS通訊協定。
- 思科ISE與思科DNA中心整合。
- Cisco ISE策略評估。

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(ISE)版本3.4補丁1。
- Cisco DNA中心版本2.3.5.5。

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。 開始之前

- 請確保在System > Settings > External Services > Authentication and Policy Servers上至少配置了一個RADIUS身份驗證伺服器。
- 只有對DNAC具有超級管理員角色許可權的使用者可以執行此過程。
- 啟用外部身份驗證回退。
- ▲ 注意:在低於2.1.x的版本中,當啟用外部身份驗證時,如果AAA伺服器無法訪問或AAA伺服器拒絕未知使用者名稱,Cisco DNA Center將回退到本地使用者。在當前版本中,如果 AAA伺服器無法訪問或AAA伺服器拒絕未知使用者名稱,Cisco DNA Center不會回退到本地 使用者。啟用外部身份驗證回退後,外部使用者和本地管理員可以登入到Cisco DNA Center。

要啟用外部身份驗證回退,請通過SSH連線到Cisco DNA Center例項並輸入此CLI命令(magctl rbac external_auth_fallback enable)。

設定

(選項1)使用RADIUS配置DNAC外部身份驗證

步驟1.(可選)定義自定義角色。

配置滿足要求的自定義角色,而您可以使用預設的使用者角色。可從System > Users & Roles > Role Based Access Control頁籤執行此操作。

程式

a.建立新角色。

	Create a User Role	୦ ୦ ୦
Create a New Role Define the name of the role, and then pr Role Name* DevOps-Role Describe the role (optional)	ovide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.	

b.定義訪問。

■ Cisco DNA Center	Create a User Role	Q @ 4								
Define the Access										
These permissions enable different capa permissions allow. Click here to Learn M	These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to Learn More.									
Define the DevOps-Role role. Custom role a role is configured with Deny permission, 1	permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If Il related content for that capability is removed from the GUI.									
Access • Permission	Description									
> Assurance 💿 Deny 🔿 Read 🤇	Write Assure consistent service levels with complete visibility across all aspects of your network.									
> Network O Deny O Read O	Write Access to Network Analytics related components.									
> Network O Deny O Read O	Write Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.									
> Network Provision O Deny O Read O	Write Configure, upgrade, provision and manage your network devices.									
> Network Services O Deny () Read ()	Write Configure additional capabilities on the network beyond basic network connectivity and access.									
> Platform O Deny O Read O	Write Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.									
> Security O Deny O Read O	Write Manage and control secure access to the network.									
		2								
-(] Exit	Review Back	Next								

DevOps角色訪問

c.建立新角色。

■ Cisco DNA Center		Create a User Role	Q @ 4 4
Summary Review the DevOps-Role role. Make :	ure all the details are as you expect them to be.	If you need to change something, clicking edit will take you back to that section	
 Role Name & Description Edit 			
Role Name DevOps-Role			
Role Description			
 Role Capability Edit 			
ASSURANCE			
Monitoring and Troubleshooting	Deny		
Monitoring Settings	Deny		
Troubleshooting Tools	Deny		
NETWORK ANALYTICS			
Data Access	Read		
NETWORK DESIGN			
Advanced Network Settings	Deny		
Image Repository	Deny		
Network Hierarchy	Deny		
Network Profiles	Deny		
Network Settings	Deny		
Virtual Network	Denv		
-{] Exit			Back Create Role

DevOps角色摘要

≡ Cisco	DNA Center		Create a User Role	Q @ 4
	Network Device	Deny		
	Port Management	Deny		
	Topology	Deny		
	License	Deny		
	Network Telemetry	Deny		
	PnP	Deny		
	Provision	Deny		
	NETWORK SERVICES			
	App Hosting	Deny		
	Bonjour	Deny		
	Stealthwatch	Deny		
	Umbrella	Deny		
	PLATFORM			
	APIs	Write		
	Bundles	Write		
	Events	Write		
	Reports	Write		
	SECURITY			
	Group-Based Policy	Deny		
	IP Based Access Control	Deny		
	Security Advisories	Deny		
	SYSTEM			
	Machine Reasoning	Deny		1
	Cuntom Management	Domi		
Exit				Back Create Role

稽核和建立DevOps角色

步驟2.使用RADIUS配置外部身份驗證。

可從System > Users & Roles > External Authentication頁籤執行此操作。

程式

a.要在Cisco DNA Center中啟用外部身份驗證,請選中啟用外部使用者覈取方塊。

b.設定AAA屬性。

在AAA attributes欄位中輸入Cisco-AVPair。

c.(可選)配置主要和輔助AAA伺服器。

確保至少在主AAA伺服器上,或者在主伺服器和輔助伺服器上都啟用了RADIUS協定。

■ Cisco DNA Center

System / Users & Roles

User Management		External Authentication
Role Based Access Control		Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here 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 chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.
External Authentication		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 cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair=Role=SUPER-ADMIN-ROLE".
		An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".
	а	E Enable External User 🛛
	b	✓ AAA Attribute AAA Attribute Cisco-AVPair
		Reset to Default Update
	С	 AAAA Server(s) Primary AAA Server

(RADIUS)外部身份驗證配置步驟

(選項1)為RADIUS配置ISE

步驟1.將DNAC伺服器新增為ISE上的網路裝置。

可從管理>網路資源>網路裝置索引標籤完成此操作。

程式

a.定義(DNAC)網路裝置名稱和IP。 b.(可選)為策略集條件對裝置型別進行分類。 c.啟用RADIUS身份驗證設定。 d.設定RADIUS共用金鑰。

≡	deale Identity Services I	Engine				Administra	ation / Network Resources	E.		۹	۵ (୭୦	1 1
н	Bookmarks	Network Devices	Network Dev	rice Groups N	etwork Device Profiles	External RADIUS Servers	RADIUS Server Sequences	External MDM	pxGrid Direct Connectors				
11日 1月 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日	Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Network Device Onfrant Device Device Security Settings	a	Network Device On Network Device Name Description IP Address Device Profile Model Name Software Version	DNAC POAC Serve	or IP	/_32						
			b	Software Versio Network Device Location IPSEC Device Type Covice Type RADIUS Protocol	n Group All Locations No DNAC-Servers US Authentication Settin UDP Settings RADRUS C	 Set To Def Set To Def Set To Def 	the the						
				Use S	econd Shared Secret () Second Shared Secret		Show						

適用於RADIUS的ISE網路裝置(DNAC)

步驟2.建立RADIUS授權設定檔。

這可通過頁籤完成 Policy > Policy Elements > Results > Authorization > 授權配置檔案。

附註:建立3個RADIUS授權配置檔案,每個使用者角色一個。

程式

a.單擊Add並定義RADIUS授權配置檔名稱。

b.在「高級屬性設定」中輸入Cisco:cisco-av-pair,並填充正確的「使用者」角色。

- 對於(DecOps-Role)使用者角色,請輸入ROLE=DevOps-Role。
- 對於(NETWORK-ADMIN-ROLE)使用者角色, 輸入ROLE=NETWORK-ADMIN-ROLE。
- 對於(SUPER-ADMIN-ROLE)使用者角色,輸入ROLE=SUPER-ADMIN-ROLE。

c.複查屬性詳細資訊。

d.按一下「Save」。

≡ deade Identity Service	es Engine	Policy / Policy Elements	
JII Bookmarks	Dictionaries Conditions	issults	
E Dashboard	Authentication	Authorization Profiles 3: New Authorization Profile	
Context Visibility	Allowed Protocols	Authorization Profile a	
N Operations	Asthorization 🗸	* Name DevOres. Brofile	
Policy	Authorization Profiles	Developer Private	
Administration	Profiling	uescription	
Nork Centers	Posture	* Access Type ACCESS_ACCEPT ~	
	Client Provisioning	Network Device Profile 🗮 Cisco 🗸 🖗	
③ Interactive Help		Service Template	
		Track Movement	
		Agentiess Posture	
		Passive Identity Tracking	
		> Common Tasks	
		× Arlunnard Attributes Sattions	
		- Autorized Attributes Jetungs	
		Elisco:cisco-av-pair v ROLE+DevOps-Role v - +	
		C	
		~ Attributes Details	
		Access Type = ACCESS, ACCEPT claco-ar-pair = ACCE-De-Op-Role	
			d
			Submit Cancel

建立授權設定檔

步驟3.建立使用者組。

可從管理>身份管理>組>使用者身份組頁籤完成此操作。

程式

a.按一下Add並定義身份組名稱

b.(可選)定義說明。

c.按一下提交。



建立使用者身份組

步驟4.建立本地使用者。

可從Administration > Identity Management > Identities > Users頁籤執行此操作。

程式

a.按一下Add並定義使用者名稱。

b.設定登入密碼。

c.將使用者新增到相關使用者組。

d.按一下「Submit」。

≡	dentity Services E	Engine			Administration / Identity Management	٩	۵	0	0 A
н н	Bookmarks	Identities G	roups Exte	rnal Ide	ntity Sources Identity Source Sequences Settings				
명	Context Visibility	Latest Manual Net Results	twork Scan		Next Access User List > New Network Access User				
0	Policy			a (* Username DevOps_User				
2 0	Administration Work Centers				Account Name Alias				
•	Interactive Help				Email Password Type: Internal Ukers Password Lifetime: With Expiration ③ Password targine 60 days Never Expires ④				
				b	Password Re-Enter Password * Login Password				

建立本地使用者1-2

=	deader Identity Services i	Engine			Admini	istration / Identity Manageme	ent		۹	۵	0	¢	A
н	Bookmarks	Identities	Groups	External Identity Sources	Identity Source Sequences	Settings							
	Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Users Latest Man Results	ual Network Scan	Login Password Enable Password Cuser Inform First Name Last Name Cocount Op Description	a		Generate Password	0					
				Account Dis Disable acc User Groups I DevOps	able Policy 2025-03-20 C 3 V (1) (2) (2)	(yyyy-mm-dd)			d		Car	ncel	

建立本地使用者2-2

步驟5.(可選)新增RADIUS策略集。

可從Policy > Policy Sets頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義策略集名稱。

c.將Policy Set Condition設定為Select Device Type,您之前是在上建立的(步驟1 > b)。

d.設定Allowed協定。

e.按一下「Save」。

f.按一下(>)策略集檢視配置身份驗證和授權規則。

E cisco internity Services Engin	le	Policy / Policy Set	ts and the second s	Q & @) Q Q
II Bookmarks	Status Policy Set Name	Description Conditions	Allowed Prot	ocols / Server Sequence Hits Actio	ns View
E Dashboard	Q Search	C		d	f
i Context Visibility	DNAG - Bulley	P DEVICE-Device Type EDUALS AS Device Types	BDNAC-Separat		Ġ
X Operations	C Divis - Policy	a nearce raise the educe we nearce thes	Delaut Hel		Ċ
Policy	Default	Default policy set	Default Netv	ork Access 🥜 🕂 🔹 🛱	*
2 Administration					е
📲 Work Centers				Reset	Save
Interactive Help					

新增RADIUS策略集

步驟6.配置RADIUS身份驗證策略。

可從Policy > Policy Sets >按一下(>)頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義身份驗證策略名稱。

c.設定身份驗證策略條件並選擇先前在上建立的裝置型別(步驟1>b)。

d. 設定Authentication Policy Use for Identity源。

e.按一下「Save」。

≡ dentity Services En	gine Policy / Policy Sets		Q & @	0 Q A
JI Bookmarks	Policy Sets-+ DNAC - Policy	Reset Reset Policy Se	t Hit Counts	Save
Dashboard	Status Policy Set Name Description Conditions	Allowed Proto	cols / Server Sequ	ence Hits
No Constantions	Q Search			
Policy	DNAC - Pelicy DIAAC - Pelicy DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers	Default Netwo	ork Access	9 + o
Administration	V Authentication Policy(2)			
Work Centers				
	Status Rule name Conditions	d	Prics	Actions
Interactive Help	Burkon C BUNAC - Authentication DEVICE Device Type EQUALS All Device TypestiDNAC-Servers Default Default	Internal Users Options All_User_IO_Stores Options	· ·	\$ \$
	> Authorization Policy - Local Exceptions			
	> Authorization Policy - Global Exceptions			
	> Authorization Policy(1)			
			Reset	e Save

新增RADIUS身份驗證策略

步驟7.配置RADIUS授權策略。

可從Policy > Policy Sets>按一下(>)頁籤完成此操作。

此步驟用於為每個用戶角色建立授權策略:

- 超級管理員角色
- NETWORK-ADMIN-ROLE
- DevOps 角色

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義授權策略名稱。

c.設定授權策略條件並選擇在中建立的使用者組(步驟3)。

d.設定授權策略結果/配置檔案並選擇您在(Step2)中建立的授權配置檔案。

e.按一下「Save」。

\equiv $\frac{1}{1000}$ Identity Services Eng	jine	Policy / Policy Sets		Q & Ø Q
Bookmarks	Policy Sets -> DNAC - Policy		Reset	Reset Policy Set Hit Counts Save
id Context Visibility	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
Operations Policy	ONAC - Policy	DEVICE Device Type EQUALS AI Device TypesIIDNAC-Servers		Default Network Access 🥒 🔶
Administration	>Authentication Policy(2)			
HIII Work Centers	> Authorization Policy - Local Exceptions			
Interactive Help	>Authorization Policy - Global Exception	5		
			Results	
	+ Status Rule Name	Conditions	Profiles Security	y Groups Hits Actions
	Q Search b	С	d	a
	Super Admin	R IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr × V + Select	t from list 🖉 + 🔹 🚳
	Network Admin	R IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role × v + Select	t from list 🥒 + 🔹 🚳
	DevOps	β IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile 0 + Select	t from list 🥒 🕂 🔹 🚳
	Oefault		DenyAccess 0 + Select	t from list 🥒 + 🔹 🏠
				е
				Reset

新增授權策略

(選項2)使用TACACS+配置DNAC外部身份驗證

步驟1.(可選)定義自定義角色。

配置滿足要求的自定義角色,而您可以使用預設的使用者角色。可從System > Users & Roles > Role Based Access Control頁籤執行此操作。

程式

a.建立新角色。

≡ Cisco	DNA Center	Create a User Role	୧୭୯୫
	Create a New Polo		
	Create a New Role		
	Define the name of the role, and then provide an optional description. To make it ex	asier to assign roles down the road, describe the role as clearly as possible.	
(Role Name* SecOps-Role		
	Describe the role (optional)		
			2
- Exit			Next

b.定義訪問。

■ Cisco DNA Center	Create a User Role	୧୭୯୫
Define the Access		
These permissions enable different capabilities in C permissions allow. Click here to Learn More.	isco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these 🛛 🗙	
Define the SecOps-Role role. Custom roles permit o a role is configured with Deny permission, all related 1	r restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If content for that capability is removed from the GUI.	
> Network Analytics O Deny O Read O Write	Access to Network Analytics related components.	
> Network Design O Deny O Read O Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.	
> Network Provision	Configure, upgrade, provision and manage your network devices.	
> Network Services O Deny O Read O Write	Configure additional capabilities on the network beyond basic network connectivity and access.	
> Platform	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
> Security O Deny O Read O Write	Manage and control secure access to the network.	
> System O Deny O Read O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.	
> Utilities O Deny	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.	
		2
€ Exit	Review Back	Next

SecOps角色訪問

c.建立新角色。

■ Cisco DNA Center		Create a User Role	Q @ 4 4
Summary Review the SecOps-Role rol	e Make sure all the details are as you expect them	to be. If you need to change something, clicking edit will take you back to that section	
✓ Role Name & Descripti Role Name SecOp Role Description	ION Edit		
 Role Capability Edit ASSURANCE 			
Monitoring and Troubleshooting	Deny		
Monitoring Settings	Deny		
Troubleshooting Tools	Deny		
NETWORK ANALYTICS			
Data Access	Write		
NETWORK DESIGN			
Advanced Network Setting	as Deny		
Image Repository	Deny		
Network Hierarchy	Deny		
Network Profiles	Deny		
Network Settings	Deny		
Virtual Network	Denv		
€ Exit			Back Create Role
L			

SecOps角色摘要

■ Cisco DNA Center		Create a User Role	Q @ & A
PnP	Deny		
Provision	Deny		
NETWORK SERVICES			
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Deny		
Events	Deny		
Reports	Deny		
SECURITY			
Group-Based Policy	Write		
IP Based Access Control	Write		
Security Advisories	Write		
SYSTEM			
Machine Reasoning	Deny		
System Management	Deny		
UTILITIES			
Audit Log	Deny		
Event Viewer	Read		
Network Reasoner	Read		1
-⊖ Exit		Back	Create Role

檢視和建立SecOps角色

步驟2.使用TACACS+配置外部身份驗證。

可從System > Users & Roles > External Authentication頁籤執行此操作。

a.要在Cisco DNA Center中啟用外部身份驗證,請選中啟用外部使用者覈取方塊。

b.設定AAA屬性。

在AAA attributes欄位中輸入Cisco-AVPair。

c.(可選)配置主要和輔助AAA伺服器。

確保至少在主AAA伺服器上,或者在主伺服器和輔助伺服器上都啟用了TACACS+協定。

■ Cisco DNA Center	System / Users & Roles	Q @ & 4
User Management Role Based Access Control External Authentication	External Authentication Gisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configuration inside Authorization profile would look like "cisco-av-pair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE". AAA Attribute Cisco-AVPair Reset to Default Update Update	le here on Cisco DNA Center is the ured here on Cisco DNA Center.
С	AAA Server(s) Primary AAA Server Secondary AAA Server IP Address ISE Server 2 IP Shared Secret Shared Secret Infe Infe Hide Advanced Settings Hide Advanced Settings O RADIUS TACACS Port 9	

(TACACS+)外部身份驗證配置步驟

(選項2)為TACACS+配置ISE

步驟1.啟用Device Admin Service。

可從Administration > System > Deployment > Edit(ISE PSN Node)> Check Enable Device Admin Service頁籤完成此操作。

=	dealer Identity Services	Engine	•						Administration	/ System				۹	۵	0	Q 2
н	Bookmarks	Deploy	yment	Licensing	Certificate	es Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings					
22	Dashboard																
15	Context Visibility					Adm	inistration										
*	Operations																
0	Policy						Monitoring										
20	Administration					R	le P	RIMARY	×								
nii.	Work Centers					0	her Monitoring Node										
٢	Interactive Help						Dedicated MnT)									
							Policy Service - Enable Session Se Include Node in N hable Profiling Servic - Enable SXP Servic - Enable SXP Servic - Enable Device Admin nable Passive Identit	Invices () None () NAC Service () () Service () ()		~ 0							
						— ~	pxGrid () nable pxGrid Cloud (٥						0		2	
														Reset		Save	

啟用裝置管理服務

步驟2.將DNAC伺服器新增為ISE上的網路裝置。

可從管理>網路資源>網路裝置索引標籤完成此操作。

程式

a.定義(DNAC)網路裝置名稱和IP。 b.(可選)為策略集條件對裝置型別進行分類。 c.啟用TACACS+身份驗證設定。 d.設定TACACS+共用金鑰。

≡ dealer Identity Services	Engine	Administration / Network Resources	Q & @ Q	۹
JI Bookmarks	Network Devices Network	Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors		
Image: Provide and the system Image: Provide and the system	Network Devices Default Device Default Device Device Security Settings	Device Orolips Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxOrld Direct Connectors		
L	b	Network Device Group: Location At Locations V Set To Default IPSEC No Set To Default Drvice Type DMAC-Servers Set To Default Image: State Single Connect Single Connect Support Image: Legacy Disc Drvice Image: Legacy Disc Drvice		

適用於TACACS+的ISE網路裝置(DNAC)

步驟3.為每個DNAC角色建立TACACS+配置檔案。

可從工作中心>裝置管理>原則元素>結果> TACACS設定檔索引標籤完成此操作。

附註:建立3個TACACS+配置檔案,每個使用者角色一個。

程式

a.按一下「Add」,定義TACACS設定檔名稱。

b.按一下Raw View選項卡。

c.輸入Cisco-AVPair=ROLE=並填寫正確的使用者角色。

- 對於(SecOps-Role)使用者角色,請輸入Cisco-AVPair=ROLE=SecOps-Role。
- 對於(NETWORK-ADMIN-ROLE)使用者角色,輸入Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE。
- 對於(SUPER-ADMIN-ROLE)使用者角色,輸入Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE。

◇ 附註:請記住,AVPair值(Cisco-AVPair=ROLE=)區分大小寫,並確保其與DNAC使用者角色 匹配。

d.按一下「Save」。

≡ dentity Services	s Engine		Worl	k Centers / Device Ac			۹	۵	© Ç	N N	
JI Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
	Conditions	> TACACS Profiles	New								
14 Context Visibility	Network Conditions	TACACS Pro	file a								
Operations	Results	Vame SecOps_Role									
Administration	TACACS Command Sets										
Work Centers	TACACS Profiles	Description									
Interactive Help		C Profile Attribute C Cisco-AVPaire	b Raw View utes ROLE=SecOps-Role	Cancel	d Save						

建立TACACS配置檔案(SecOps_Role)

步驟4.建立使用者組。

可從工作中心>裝置管理>使用者身份組頁籤完成此操作。

程式

a.按一下Add並定義身份組名稱。

b.(可選)定義說明。

c.按一下提交。

≡	dentity Services	Engine		Work	Centers / Device Ad	ministration			Q	۵	0	θI	8
Щ	Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
53	Dashboard		User identit	y Groups > New User Iden	tity Group								
15	Context Visibility	Identity Groups	Identity	Group									
~%	Operations	< 18	a Name	SecOps									
-0	Policy	> 🛅 Endpoint lo	dentity Groups	SecOps-Role	< <u> </u>								
8.	Administration	> 🛅 User Ident	ity Groups Descrip	tion									
đ	Work Centers)								
3	Interactive Help								C		Car	ncel	

建立使用者身份組

步驟5.建立本地使用者。

可從工作中心(Work Centers)>裝置管理(Device Administration)>身份(Identities)>使用者(Users)頁 籤執行此操作。

程式

a.按一下Add並定義使用者名稱。

b.設定登入密碼。

c.將使用者新增到相關使用者組。

d.按一下「Submit」。

≡	diale Identity Services	Engine				Work	Centers / Device	Administration			٩	۵ 🕼	0 Q Q
Л	Bookmarks	Overview	Identities	User Ider	ntity Groups	Ext Id Sources	Network Resource	es Policy Elements	Device Admin Policy Se	ets Reports	Settings		
53	Dashboard	Users			Vetwork Access Use	rs List > New Network Ar	ccess User						
1d	Context Visibility												
×	Operations				V Network Address Addre Address Address Add	cess User	~						
0	Policy			а	* Username	SecOps_User			_				
8.	Administration				Status	Enabled 🗸							
đ	Work Centers				Account Name	Alias	0						
					Email								
(?)	Interactive Help												
					V Password:	3							
					Password Typ	e: Internal Users	~						
					Password Life	time:							
					 With Expir 	ation ①							
					Password v	rill expire in 60 days							
					O Never Exp	ires 🕓							
						Password	R	-Enter Password					
				b	* Login Passw	ord			Generate Password	0			
					Enable Passw	ord			Generate Password	0			
										~			
					✓ User Infor	mation							

```
建立本地使用者1-2
```

≡ dentity Services	Engine			Worl	k Centers / Device Ad	ministration			٩	۵ ۵) 0 0 0
JU Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings		
Dashboard	Users		✓ User Infor	mation							
14 Context Visibility			First Name								
ℜ Operations			Last Name								
Dolicy											
Administration			✓ Account C	ptions							
H Work Centers			Description	Γ							
③ Interactive Help			Change passv	vord on next login)						
			V Account D	isable Policy	is 2025-03-20	(yyyy-mm-dd)					
				С							
			 ✓ User Grou ∷ SecOpt 	ps i	<u> </u>				d		Cancel

建立本地使用者2-2

步驟6.(可選)新增TACACS+策略集。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義策略集名稱。

c.將Policy Set Condition設定為Select Device Type,您之前是在上建立的(步驟2 > b)。

d.設定Allowed協定。

e.按一下「Save」。

f.按一下(>)策略集檢視配置身份驗證和授權規則。

≡	dentity Services En	ngine			Policy / Policy Sets	Q & @ Q A
н	Bookmarks	Policy Sets				Reset Reset Policy Set Hit Counts Save
	Dashboard	🕘 Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
PS 15	Context Visibility	Q Search	b		C C	d f
*	Operations	6	DNAC - BANKY			
0	Policy	Ċ	Diake - Policy		псилсовите туре сдокса на ренсе турезнокис-зетиез	
8.	Administration	0	Default	Default policy set		Default Network Access 🖉 + o 🔯 🕨
-file	Work Centers					e
(?)	Interactive Help					Reset Seve

新增TACACS+策略集

步驟7.配置TACACS+身份驗證策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義身份驗證策略名稱。

c.設定身份驗證策略條件並選擇先前在上建立的裝置型別(步驟2 > b)。

d. 設定Authentication Policy Use for Identity源。

e.按一下「Save」。

≡	dentity Services I	Engine Work Centers / Device Administration	Q & @ Q A
Л	Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements	Device Admin Policy Sets Reports Settings
53	Dashboard	Policy Sets DNAC - Policy	Peset Deliny Set Mit Counts
1d	Context Visibility		Reset Policy Set hit coulds
×	Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits
0	Policy	Q Search	
20	Administration	DNAC - Policy DEVICE Oevice Type EQUALS All Device Types#ONAC	Default Device Admin 🖉 🕂 o
កា	Work Centers		
		✓Authentication Policy(2)	
(?)	Interactive Help	Status Rule Name Conditions	Use Hits Actions
		Q Search	d
		b c	Internal Users
		DNAC - Authentication DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	> Options 0 🔅
			All_User_ID_Stores.
		Default	> Options • 🚱
		>Authorization Policy - Local Exceptions	
		>Authorization Policy - Global Exceptions	
		> Authorization Policy(4)	

新增TACACS+身份驗證策略

步驟8.配置TACACS+授權策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

此步驟用於為每個用戶角色建立授權策略:

- 超級管理員角色
- NETWORK-ADMIN-ROLE
- SecOps角色

程式

a.按一下Actions並選擇(在上面插入新行)。

b.定義授權策略名稱。

c.設定授權策略條件並選擇在中建立的使用者組(步驟4)。

d.設定授權策略Shell Profiles並選擇您在中建立的TACACS配置檔案(步驟3)。

e.按一下「Save」。

≡	dialic Identity Services E	Engin	e				Wa	ork Centers / Device Ad	ministratio	n			٩	۵ ۵) G	א א
н	Bookmarks	Over	view	Ident	ties User Ide	ntity Groups	Ext Id Sources	s Network Resources	Policy Ele	ements Device Adr	min Policy Set	s Reports	Settings			
51	Dashboard		Q	Search												
명	Context Visibility			0	DNAC - Policy			DEVICE-Device Type EQUAL	S All Device Typ	pes#DNAC		Defa	ult Device Admi	n ,	0+	0
×	Operations															
-0	Policy		> Authe	ntication	Policy(2)											
20	Administration		> Autho	rization	Policy - Local Except	lions										
đ	Work Centers		> Autho	rization	Policy - Global Excep	tions										
			~Autho	rization	Policy(1)											
?	Interactive Help									Results						
			۲	Status	Rule Name	Condi	tions			Command Sets	1	Shell Profiles		Hits	Act	lons
			Q	Search				1								
	SUPER-ADMIN	-ROI	E	•	Super Admin	8	identityGroup-Name EQ	QUALS User Identity Groups:SUPER-	ADMIN	Select from list	0+	SUPER_ADMIN_	ROLE 🐼 🤉	<u>_</u> +	< <u>\$</u>	>
	NETWORK-ADMI	N-RO	DLE	0	Network Admin	R	identityGroup-Name EQ	QUALS User Identity Groups:NETWO	RK-ADMIN	Select from list	0 +	NETWORK_ADM	N_ROLE 🚾	-	<i>{</i> 2	3
	SecOps-Role	е		0	SecOps	8	identityGroup-Name EQ	QUALS User Identity Groups:SecOps		Select from list	0 +	SecOps_Role	(3)	-	<i>{</i> 2	2
				٥	Default					DenyAllCommands	0 +	Deny All Shell Pro	file d	+ 0	< <u>\$</u>	>
															:	2
													R	pset	Sa	

新增授權策略

驗證

驗證RADIUS設定

1- DNAC — 顯示外部使用者系統>使用者和角色>外部身份驗證>外部使用者。 您可以檢視首次透過RADIUS登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色。

■ Cisco DNA Center	System) / Users & Roles	0	1004
User Management Role Based Access Control	External Authentication Cisco DNA Center supports external servers for authentication and authorization of	f External Users.Use the fields in this window to create, update and delete.	AAA Servers.The AAA Attribute here on Cisco D?	NA Center is the
External Authentication	name of the AAA attribute chosen on the AAA server. The default attribute expect The value of the AAA attribute to be configured for authorization on AAA server w configuration inside Authorization profile would look like "cisco-av-pairs RolesSU	ed is Cisco-AVPair, but if the user chooses to change it to any other AAA al build be in the format of "Role=role1". On ISE server, choose the cisco-av-p PER-ADMIN-ROLE".	Iribute, it needs to be configured here on Cisco i uir attribute from cisco specific AAA attributes lis	DNA Center.
	An example configuration in the case of manually defining the AAA attribute would	be *Cisco-AVPair=Role=SUPER-ADMIN-ROLE"		
	 AAA Attribute AAA Attribute Cisco-AVPair 			
	Reset to Default Update			
	> AAA Server(s)			
	✓ External Users		EQ, Find	
	Username • devops_user	Role DevOps-Role	Action	
		Showing 1 of 1		

外部使用者

2. DNAC — 確認使用者訪問許可權。



```
有限的使用者訪問
```

3.a ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs。

=	dentity Services I	Engine	Operat	ions / RADIUS	Α Φ Φ Α
н	Bookmarks	Live Logs Live Sessions			
16	Context Visibility	Misconfigured Supplicants 💿	Misconfigured Network Devices 🕕	RADIUS Drops 🕕	Client Stopped Responding 💿 Repeat Counter 💿
*	Operations	0	0	5761	0 0
0	Policy				Refresh Show Within
8.	Administration	Ø 10 Reset Recest Courts - ŵ Export To ∨			Never Latest 20 records Last 60 Seconds Filer
-fil	Work Centers	Time Status I	Details Repea Identity Endpoint I	D Endpoint Profile Authentication Policy	Authorization Policy Authorization Profiles IP Addre
(?)	Interactive Help	× _ <u>Auth</u> ×	Identity Endpoint ID	Endpoint Profile Authentication Policy	Authorization Policy Authorization Profiles IP Addres
		Jan 19, 2025 11:19:18.1 🦉	a DevOps_User	DNAC - Policy >> DNAC - Auto	entication DNAC - Policy >> DevOps DevOps-Profile
		Last Updated: Sun Jan 19 2025 23:19:57 GA	IT+0100 (Central European Standard Time)		Records Shown: 1

RADIUS即時日誌

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click(Details)for Authorization \log_{\circ}

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	DevOps_User
Endpoint Id	
Endpoint Profile	
Authentication Policy	DNAC - Policy >> DNAC - Authentication
Authorization Policy	DNAC - Policy >> DevOps
Authorization Result	DevOps-Profile
Authentication Details	2025-01-10 22:10:18 155
Source Timestamp	2025-01-19 23:19:18.156
Received Timestamp	2025-01-19 23:19:18.156
Policy Server	ise34
Event	5200 Authentication succeeded
Username	DevOps_User
User Type	User
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:DevOps
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	DNAC
Device Type	All Device Types#DNAC-Servers
Location	All Locations

Steps		
Step ID	Description	Latency
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP- Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

RADIUS詳細即時日誌1-2

Cisco ISE	
IdentityPolicyMatchedRule	DNAC - Authentication
AuthorizationPolicyMatchedF ule	DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedRul	e DNAC - Authentication
TotalAuthenLatency	35
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device TypeIIAII Device TypesIIDNAC-Servers
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:DevOps
EnableFlag	Enabled
RADIUS Username	DevOps_User
Device IP Address	
CPMSessionID	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
CiscoAVPair	AuthenticationidentityStore=Internal Users, FQSubjectName=9271630-8c01-11e6-996c- 52540046821064v008_user. UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5de df467
Result	
Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R
	tG/WY:8e34/526427220/15433
cisco-av-pair	ROLE=DevOps-Role

RADIUS詳細即時日誌2-2

驗證TACACS+配置

1- DNAC — 顯示外部使用者系統>使用者和角色>外部身份驗證>外部使用者。 您可以檢視首次通過TACACS+登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色

o

■ Cisco DNA Center	System / Users & Roles	Q @ @ 4
User Management Role Based Access Control External Authentication	 AAA Attribute AAA Attribute Cisco-AVPair Reset to Default Update 	
	AAA Server(s) Primary AAA Server Secondary AAA Server P Address IP Address Shared Secret IP Address trive Info View Advanced Settings View Advanced Settings Update Update	
	✓ External Users ✓ Filter Role Action username * Role SecOps-Role Delete	EQ, Find
	Showing 1 of 1	

外部使用者

2. DNAC — 確認使用者訪問許可權。

Cisco DNA Center			Q @
⁸ ∰ ⁸ Policy	Group-Based Access Control		Explore
0 Workflows	IP & URL Based Access Control	enter with the adoption journey map.	×
🕺 Tools		time to value, as you guide your organization on its	
C Platform			
🕢 Activities			
Explore			
		0~0	
		,e,	
		Network Bug Identifier	
		Identify bugs in the network	
요 secops_user			

有限的使用者訪問

3.a ISE - TACACS+即時日誌工作中心>裝置管理>概述> TACACS即時日誌。

≡	dentity Services	Engine					Operat	ions / TACACS			q	۵ ۵	Ð	A
Л	Bookmarks	Live Log	js											
	Dashboard		-											
₁ 13	Context Visibility								Defee		Character .	Within		
*	Operations								Neve	er v	Latest 20 records	Last 60	Second	ds∨
0	Policy	6	う 企 Export To 〜									Filter	< e	Þ
80	Administration		Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
đ	Work Centers	>	<			Identity	×	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
			Jan 19, 2025 05:12:4	2	0	SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All De	vice Types#D	NAC	Loc
	Internetive Mele		Jan 19, 2025 05:12:4	2	0	SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All De	vice Types#D	NAC	Loc
0	Interactive Help	La	ist Updated: Sun Jan 19 2	025 17:16:38	GMT+0100	(Central Europea	an Standard Time)					Record	s Shown	n: 2

TACACS即時日誌

3.b ISE — 詳細的TACACS+即時日誌工作中心(Work Centers)>裝置管理(Device Administration)>概述(Overview)> TACACS即時日誌(TACACS Livelog)>按一下(詳細資訊)獲取 授權日誌。

erview		Steps		
equest Type	Authorization	Step ID	Description	Latency (ms)
tatus	Pass	13005	Received TACACS+ Authorization Request	
essies Key		15049	Evaluating Policy Group	1
ession key	13034/020427220/13306	15008	Evaluating Service Selection Policy	1
essage Text	Device-Administration: Session Authorization succeeded	15048	Queried PIP - DEVICE.Device Type	4
sername	SecOps_User	15041	Evaluating Identity Policy	7
uthorization Policy	DNAC - Policy >> SecOps	15013	Selected Identity Source - Internal Users	5
hall Deallin	Carolan Dala	24210	Looking up User in Internal Users IDStore	1
hell Profile	SecUps_kole	24212	Authentication Passed	
atched Command Set		15036	Evaluating Authorization Policy	
ommand From Device		15048	Oueried PIP - Network Access UserName	10
		15048	Queried PIP - IdentityGroup.Name	2
		15017	Selected Shell Profile	2
horization Details		22081	Max sessions policy passed	1
enerated Time	2025-01-10-17-12-42-269-11-00	22080	New accounting session created in Session cache	0
enerated time	2025-01-19 17:12:43:308 +1:00	13034	Returned TACACS+ Authorization Reply	0
ogged Time	2025-01-19 17:12:43.368			_
poch Time (sec)	1737303163			
E Node	ise34			
essage Text	Device-Administration: Session Authorization succeeded			
ailure Reason				
esolution				
oot Cause				
sername	SecOps_User			
etwork Device Name	DNAC			

TACACS+詳細即時日誌1-2

Cisco ISE	
1700	riomeneout
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentit yStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;1 3=1;14=0;15=0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco- AVPair=ROLE=SecOps-Role; }

TACACS+詳細即時日誌2-2

疑難排解

目前尚無適用於此組態的具體診斷資訊。

參考資料

- <u>Cisco Identity Services Engine管理員指南,版本3.4 >裝置管理</u>
- Cisco DNA Center管理員指南2.3.5版
- Cisco DNA Center:具有外部驗證的基於角色的存取控制

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)。