DNAC GUIの外部認証としてのISEの設定

内容
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>はじめる前に</u>
<u>設定</u>
<u>(オプション1)RADIUSを使用したDNAC外部認証の設定</u>
<u>(オプション1)RADIUS用のISEの設定</u>
<u>(オプション2)TACACS+を使用したDNAC外部認証の設定</u>
<u>(オプション2)TACACS+用のISEの設定</u>
<u>確認</u>
RADIUS設定の確認
<u>TACACS+設定の確認</u>
トラブルシュート
<u>参考資料</u>

はじめに

このドキュメントでは、Cisco DNA Center GUI管理の外部認証としてCisco Identity Services Engine(ISE)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- TACACS+およびRADIUSプロトコル。
- ・ Cisco ISEとCisco DNA Centerの統合
- Cisco ISEポリシー評価

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)バージョン3.4パッチ1。
- Cisco DNA Centerバージョン2.3.5.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

はじめる前に

- System > Settings > External Services > Authentication and Policy Serversで、少なくとも 1つのRADIUS認証サーバが設定されていることを確認します。
- DNACでSUPER-ADMIN-ROLE権限を持つユーザのみがこの手順を実行できます。
- 外部認証フォールバックを有効にします。

▲ 注意:2.1.xより前のリリースでは、外部認証が有効な場合、AAAサーバに到達できないか、 AAAサーバが未知のユーザ名を拒否すると、Cisco DNA Centerはローカルユーザにフォー ルバックします。現在のリリースでは、AAAサーバに到達できない場合、またはAAAサーバ が未知のユーザ名を拒否した場合、Cisco DNA Centerはローカルユーザにフォールバック しません。外部認証フォールバックを有効にすると、外部ユーザとローカル管理者はCisco DNA Centerにログインできます。

外部認証フォールバックを有効にするには、Cisco DNA CenterインスタンスにSSHで接続し、次のCLIコマンドを入力します(magctl rbac external_auth_fallback enable)。

設定

(オプション1) RADIUSを使用したDNAC外部認証の設定

ステップ1:(オプション)カスタムロールを定義します。

要件を満たすカスタムロールを設定する代わりに、デフォルトのユーザロールを使用できます。 これは、System > Users & Roles > Role Based Access Controlの順に選択することで実行できま す。

手順

a.新しいロールを作成します。

Create a User Role

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name* DevOps-Role)
Describe the role (optional)	

2 Next

DevOpsロール名

Exit

b.アクセスを定義します。

≡ Cisco DNA Center	Create a User Role	Q @ & A								
Define the Access										
Access - Permission Access - Permission Assurance Deny Read Write Network Analytics Deny ORead Write	Description Assure consistent service levels with complete visibility across all aspects of your network. Access to Network Analytics related components.									
Network Network Network Network Network Network Network Network Network Services Openy Read Write	Set up network merarchy, update your soltware image repository, and compute network promes and settings for managing your sites and network devices. Configure, upgrade, provision and manage your network devices. Configure additional capabilities on the network beyond basic network connectivity and access.									
Platform OPeny Pread Write Security OPeny Read Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations. Manage and control secure access to the network.	2								
- Exit	Review Back	Next								

DevOpsロールアクセス

c.新しいロールを作成します。

■ Cisco DNA Center	Create a User Role		Q @ 4
Summary Review the DevOps-Role role. Make s	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		
v 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ロールの概要

≡ 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
	Custom Management	Danu		
Exit				Back Create Role

DevOpsロールのレビューと作成

ステップ2:RADIUSを使用して外部認証を設定する。

これは、System > Users & Roles > External Authenticationの順にタブから実行できます。

手順

a. Cisco DNA Centerで外部認証を有効にするには、Enable External Userチェックボックスにチェックマークを入れます。

b. AAA属性を設定します。

AAA attributesフィールドに、Cisco-AVPairと入力します。

c. (オプション)プライマリおよびセカンダリAAAサーバを設定します。

RADIUSプロトコルがプライマリAAAサーバで、少なくとも、またはプライマリとセカンダリの 両方のサーバで有効になっていることを確認します。

E Cisco DNA Center	System / Users & Roles	Q @ C 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 here on Cisco-avPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco-avPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco-avPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco-avPair, but if the user chooses to change it to any other AAA attribute from cisco specific AAA attribute configuration inside Authorization profile would look like "cisco-av-pairs 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 (* AAA Attribute Cisco-AVPair (* AAA Attribute Cisco-AVPair (* Configured for authorization (* AAA Attribute Cisco-AVPair (* Update	to DNA Center is the isco DNA Center. es list. A sample
c	V AAA Server(s) Primary AAA Server Secondary AAA Server IP Address IP Address ISE Server 1 IP V Shared Secret Shared Secret ****** Infe Hide Advanced Settings Hide Advanced Settings Hide Advanced Settings O TACACS O RADIUS O TACACS Authentication Port 1812	

(RADIUS)外部認証の設定手順

(オプション1) RADIUS用のISEの設定

ステップ1:DNACサーバをISE上のネットワークデバイスとして追加します。

これは、タブAdministration > Network Resources > Network Devicesから実行できます。

手順

a. (DNAC)ネットワークデバイス名とIPを定義します。

- b. (オプション)ポリシーセット条件のデバイスタイプを分類します。
- c. RADIUS認証設定を有効にします。
- d. RADIUS共有秘密を設定します。



RADIUS用ISEネットワークデバイス(DNAC)

ステップ2: RADIUS認可プロファイルを作成します。

これは、タブから実行できます Policy > Policy Elements > Results > Authorization > 認可プロフ ァイル.

💊 注:各ユーザロールに1つずつ、3つのRADIUS認可プロファイルを作成します。

手順

a. Addをクリックして、RADIUS許可プロファイル名を定義します。

- b. Advanced Attributes SettingsでCisco:cisco-av-pairを入力し、正しいユーザロールを入力します
- 0
- ・ (DecOps-Role)ユーザロールに、ROLE=DevOps-Roleと入力します。
- (NETWORK-ADMIN-ROLE)ユーザロールに、ROLE=NETWORK-ADMIN-ROLEと入力します。
- ・ (SUPER-ADMIN-ROLE)ユーザロールに、ROLE=SUPER-ADMIN-ROLEと入力します。
- c. 属性の詳細を確認します。
- d. Saveをクリックします。

≡ deals Identity Services	s Engine	Policy / Policy Elements	Q & @ Q ;
JII Bookmarks 또한 Dashboard (영 Context Visibility	Dictionaries Conditions Authentication v	Authorization Profile a	
Operations Policy Administration Work Centers	Authorization Profiles Downloadable ACLs Profiling > Postare >	Name DevOps-Predie Description Access Type AccESS_ACCEPT	
() Interactive Help	Citent Previalening.	Network Device Profile accurate Constraints Service Frenglate Track Movement G Agentiess Posture G Passive Identity Tracking G O	
		Control Attributes Settings b Advanced Attributes Settings b 	
		V Attributes Details Room Tope - ACISS, ACIST doce wyper - ROLT-OwdgeSide	d Submit Cancel

認証プロファイルの作成

ステップ3:ユーザグループを作成します。

これは、タブAdministration > Identity Management > Groups > User Identity Groupsから実行できます。

手順

a. Addをクリックして、IDグループ名を定義します

b. (オプション)摘要を定義します。

c. Submitをクリックします。



ユーザIDグループの作成

ステップ4:ローカルユーザを作成します。

これは、タブAdministration > Identity Management > Identities > Usersから実行できます。

手順

a. Addをクリックして、ユーザ名を定義します。

b.ログインパスワードを設定します。

c.関連するユーザグループにユーザを追加します。

d. Submitをクリックします。

=	dentity Services E	Engine			Administration / Identity Management	Q	۵ (D (9 S
н	Bookmarks	Identities	Groups	External	al Identity Sources Identity Source Sequences Settings				
15	Dashboard Context Visibility	Users Latest Manual Results	I Network Scan		Network Access Users List > New Network Access User				
×	Operations				V Network Access User				
0	Policy			a	a Username DerOps_User				
20	Administration				Status Enabled V				
-fil	Work Centers				Account Name Alias				
(?)	Interactive Help				tmai				
					Passwords Descent Tune Understitling				
					Descent Linitary				
					Vith Expiration ①				
					Password will expire in 60 days Never Expires ①				
					Plassword Re-Enter Plassword				
					* Login Password Generate Password				
					Enable Password O				
					~ User Information				
					First Name				
					Last Name				

ローカルユーザの作成1-2

=	dentity Services I	Engine					Admin	istration / Identity M	anageme	ent			Q	۵	0	Q	A
н	Bookmarks	Identities	Groups	Extern	al Identity Sources	Identity Source	e Sequences	Settings									
	Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Users Latest Many Results	aal Network Scan		* Login Password Enable Password V User Informal First Name Last Name V Account Opti	ion				Generate Password	0						
					Description Change password ~ Account Disa Disable acco ~ User Groups H DevOps	on next login ble Policy unt if date exceed C	s 2025-03-20	(yyyy-mm	- dd)								
													d Jbmit)	Can	cel	

ローカルユーザの作成2-2

ステップ5:(オプション)RADIUSポリシーセットを追加します。

これは、Policy > Policy Setsタブで実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.ポリシーセット名を定義します。

c.ポリシーセットConditionを、先ほど作成したSelect Device Type(ステップ1>b)に設定します。

d. Allowedプロトコルを設定します。

e. Saveをクリックします。

f. (>) Policy Set Viewをクリックして、認証および認可ルールを設定します。

≡ dentity Services Engi	ne		Policy / Policy Sets		Q	<u>ରୁ ଡ ଢ଼∣ ଛ</u>
JI Bookmarks	 Status Policy Set Name 	Description	Conditions	Allow	ed Protocols / Server Sequence Hit	ts Actions View
E Dashboard	Q Search b		с	(d	f
N Operations	O DNAG - Policy	Default policy set	DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers	Defa	It Network Access	
Administration						e
Fill Work Centers					Res	et Save
Interactive Help						

RADIUSポリシーセットの追加

手順6:RADIUS認証ポリシーを設定します。

これは、タブPolicy > Policy Sets > (>)をクリックすることで実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.認証ポリシー名を定義します。

c.認証ポリシーの条件を設定し、前に作成したデバイスタイプを選択します(ステップ1 >b)。 d.アイデンティティソースの認証ポリシーUseを設定します。

e. Saveをクリックします。

≡ deale Identi	Services Engine Policy / Policy Sets		۵ ۵	• C	0 A
Bookmarks	Policy Sets-+ DNAC - Policy	Reset	set Policy Set Hit Counts	S	lave
Dashboard	Status Policy Set Name Description Conditions	Alf	owed Protocols / Server Sr	quence	Hits
Tel Context Visib	Q. Search				
Operations	DNAC - Policy DEVICE Device Type EQUALS All Device TypesIDNAC-Servers	1	Default Network Access	0+	0
& Administration					
S Work Centers	VAuthentication Policy(2)				
- All	Status Rule Name Conditions	Use	H	lits Ac	tions
Interactive He	Q. Search		d		
	DIALG - Authentication DIALG - Authentication DIVICE Device Type EQUALS All Device TypesIONAC-Servers	> Options		0 දි	¢
	Default	All_User_ID_ > Options	Stores 🥜	2 ố	ŵ
	> Authorization Policy - Local Exceptions				
	> Authorization Policy - Global Exceptions				
	> Authorization Policy(1)				
			Reset	(s	e ivre

RADIUS認証ポリシーの追加

手順7:RADIUS許可ポリシーを設定します。

これは、タブPolicy > Policy Sets> Click (>)から実行できます。

各ユーザの役割の許可ポリシーを作成するには、次の手順を実行します。

- スーパー管理者ロール
- ネットワーク管理者ロール
- DevOpsロール

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.許可ポリシー名を定義します。

c.許可ポリシー条件を設定し、(ステップ3)で作成したユーザグループを選択します。

d.許可ポリシーの結果/プロファイルを設定し、(ステップ2)で作成した許可プロファイルを選 択します。

e. Saveをクリックします。

≡ dentity Services En	ngine	Policy / Policy Sets		
Bookmarks	Policy Sets→ DNAC - Policy		Reset	Reset Policy Set Hit Counts Save
명 Context Visibility 文 Operations	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
Policy	ONAC - Policy	DEVICE-Device Type EQUALS All Device TypesIIDNAC-Serve	n	Default Network Access 🥒 + o
2 Administration	>Authentication Policy(2)			
H Work Centers	> Authorization Policy - Local Exception	5		
Interactive Help	>Authorization Policy - Global Exceptio	15		
			Results	
	🕂 Status Rule Name	Conditions	Profiles Security	Groups Hits Actions
	Q Search b	с	d	a
	Super Admin	A IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr × + Select	from list 🕜 🕂 🔹 🕼
	Network Admin	R identityGroup-Name EQUALS User identity Groups:NETWORK-ADMIN	Network-Admin_Role \times + Select	from list 🥒 + 🔹 🏠
	DevOps	R IdentityGroup Name EQUALS User Identity Groups:DevOps	DevOps-Profile 🖉 + Select	from list 🖉 + 🔹 🚳
	Opfault		DenyAccess 🥒 + Select	from list 🥒 + 🔹 🏠
				Reset Save

許可ポリシーの追加

(オプション2)TACACS+を使用したDNAC外部認証の設定

ステップ1:(オプション)カスタムロールを定義します。

要件を満たすカスタムロールを設定する代わりに、デフォルトのユーザロールを使用できます。 これは、System > Users & Roles > Role Based Access Controlの順に選択することで実行できま す。

手順

a.新しいロールを作成します。

Elisco DNA Center		Cisco	DNA	Center
-------------------	--	-------	-----	--------

Create a User Role

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name*	
SecOps-Role]
Describe the role (optional)	

	2
- Exit	Next

SecOpsロール名

b.アクセスを定義します。

⊟ Cisc	o DNA Center				Create a User Role	Q @ C 4				
	Define th	e Acce	SS							
	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 SecO a role is configur	ps-Role role ed with Den 1	e. Custom y permissio	roles permit o on, all related	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	⊖ Read	() 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	Write	Configure, upgrade, provision and manage your network devices.					
	> Network Services	O Deny	⊖ Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.					
	> Platform	O Deny	O Read	 Write 	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.					
	> Security	O Deny	○ Read	O Write	Manage and control secure access to the network.					
	> System	O Deny	○ Read	O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.					
	> Utilities	O Deny	Read	Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.					
						2				
🕣 Exit					Review Back	Next				

SecOpsロールアクセス

c.新しいロールを作成します。

	A Center	Create a User Role	
Sur	mmary w the SecOps-Role role Make sur	re 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	
V Ro Ro	ole Name & Description Edit Ne Name SecOps-Role		
~ Ro	ole Capability Edit		
AS	SSURANCE		
	Monitoring and Troubleshooting	Deny	
	Monitoring Settings	Deny	
	Troubleshooting Tools	Deny	
NE	TWORK ANALYTICS		
	Data Access	Write	
NE	TWORK DESIGN		
	Advanced Network Settings	Deny	
	Image Repository	Deny	
	Network Hierarchy	Deny	
	Network Profiles	Deny	
	Network Settings	Deny	
	Virtual Network	Denv	
Exit			Back Create Role

SecOpsロールの概要

■ Cisco DNA Center		Create a User Role	ର ⊚ ୯ ୫
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		C	Back Create Role

SecOpsロールのレビューと作成

ステップ 2:TACACS+を使用して外部認証を設定する。 これは、System > Users & Roles > External Authenticationの順にタブから実行できます。

a. Cisco DNA Centerで外部認証を有効にするには、Enable External Userチェックボックスにチェックマークを入れます。

b. AAA属性を設定します。

AAA attributesフィールドに、Cisco-AVPairと入力します。

c. (オプション)プライマリおよびセカンダリAAAサーバを設定します。

TACACS+プロトコルがプライマリAAAサーバで、少なくとも、またはプライマリとセカンダリ の両方のサーバで有効になっていることを確認します。

	E Cisco DNA Center	System / Users & Roles	Q @ @ \$
	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 C 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	Isco DNA Center is the I Cisco DNA Center.
h	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 attrib configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".	utes list. A sample
	а	An example configuration in the case of manually defining the AAA attribute would be *Cisco-AVPair=Role=SUPER-ADMIN-ROLE*	
	b	~ AAA Attribute AAA Attribute Cisco-AVPair	
		Reset to Default Update	
	c	∼ AAA Server(s) Primary AAA Server P Address P Address ISE Server 1 IP Shared Secret Infe Infe Infe RADIUS O RADIUS Port 49	

(TACACS+)外部認証の設定手順

(オプション2)TACACS+用のISEの設定

ステップ1: Enable Device Admin Service.

これは、タブAdministration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Serviceから実行できます。

≡	dealer Identity Services	Engine				Administration / System								۵ ۵	0	0 A	
JI.	Bookmarks	Deploy	yment l	Licensing	Certificate	s Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings					
53	Dashboard																
15	Context Visibility					Adn	ninistration										
*	Operations																
-0	Policy						Monitoring										
20	Administration					R	ple P	RIMARY	×								
ri)	Work Centers					0	ther Monitoring Node										
						ĩ	Dedicated MnT (
Ŷ	Interactive Help																
						— ~	Policy Service										
							 Enable Session Se 	rvices 🕕									
							Include Node in No	ode Group None		~ 0							
						E	nable Profiling Service	0									
							nable Threat Centric I	WAC Service 🕢									
						_											
							 Enable and dervice 	•0									
						1 💷	nable Device Admin !	Service ()									
							inable Passive Identit	y Service 🕕									
							avGrid O										
						 	pxumo () nable pxGrid Cloud ()										
																0	
																2	_
														Reset		Save	
•																	

ステップ2:DNACサーバをISE上のネットワークデバイスとして追加します。

これは、タブAdministration > Network Resources > Network Devicesから実行できます。

手順

a. (DNAC)ネットワークデバイス名とIPを定義します。

b. (オプション)ポリシーセット条件のデバイスタイプを分類します。

c. TACACS+認証設定を有効にします。

d. TACACS+共有秘密を設定します。

$\equiv \frac{\mathrm{ded}_{\mathrm{fisc}}}{\mathrm{csce}}$ Identity Services	Engine	Administration / Network Resources	۵ ۵	0	0 A
JII Bookmarks	Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors			
 Enableard Context Visibility Operations Policy Administration Work Centers Interactive Help 	Vetenk Device Defaul Device Device Security Settings	a			
		Location All Lecations V Set To Default IPSEC No V Set To Default Device Type DNAC-Servers V Set To Default C VRADIUS Authentication Settings V TACACS Authentication Settings V TACACS Authentication Settings V TACACS Authentication Settings V TACACS Durbenter Show Retrie V Set To Default Netrie			

TACACS+用ISEネットワークデバイス(DNAC)

ステップ3:各DNACロールのTACACS+プロファイルを作成します。

これは、タブWork Centers > Device Administration > Policy Elements > Results > TACACS Profilesから実行できます。

💊 注:ユーザロールごとに1つずつ、3つのTACACS+プロファイルを作成します。

手順

a. Addをクリックして、TACACS Profileの名前を定義します。

b. Raw Viewタブをクリックします。

c. Cisco-AVPair=ROLE=と入力し、正しいユーザロールを入力します。

・ (SecOps-Role)ユーザロールに、Cisco-AVPair=ROLE=SecOps-Roleと入力します。

- (NETWORK-ADMIN-ROLE)ユーザロールに、Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLEと入力します。
- (SUPER-ADMIN-ROLE)ユーザロールに、Cisco-AVPair=ROLE=SUPER-ADMIN-ROLEと入 力します。
- ✤ 注:AVPair値(Cisco-AVPair=ROLE=)は大文字と小文字が区別されることを覚えておき、 DNACユーザロールに一致していることを確認してください。

d. Saveをクリックします。

≡	dentity Services	Engine			Work Centers / Device Administration						م ر	۵	0	Q	8
Л	Bookmarks	Overview	Identities	User	Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
53	Dashboard	Conditions		>	TACACS Profiles >	New									
15	Context Visibility	Network Co	nditions	>	TACACS Profi	a									
*	Operations	Results		~	Name SecOps_Role										
0	Policy	Allowed I TACACS	Protocols Command Sets												
80	Administration	TACACS	Profiles		Description		-								
កា	Work Centers														
3	Interactive Help			С	Task Attribute Vie Profile Attribu Cisco-AVPair=R	b Raw View Les OLE=SecOps-Role	Cancel	d Save							

TACACSプロファイルの作成(SecOps_Role)

ステップ4:ユーザグループを作成します。

これは、タブWork Centers > Device Administration > User Identity Groupsから実行できます。

手順

a. Addをクリックして、IDグループ名を定義します。

b. (オプション)摘要を定義します。

c. Submitをクリックします。

= 1	dealer Identity Services I	Engine		Work	Centers / Device Ad	ministration			a 4	0	0 A
щ	Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings		
- 22 - 7	Dashboard		User Identit	y Groups > New User Iden	tity Group						
ь В	Context Visibility	Identity Groups	Identity	Group							
*	Operations	< 18	a Name	SecOps)						
0.	Policy	> 🛅 Endpoint Id	entity Groups	SecOos-Role	<──						
80	Administration	> 🛅 User Identi	ty Groups Descrip	tion							
តា	Work Centers)						
									С		
?	Interactive Help								Submit	Cane	cel

ユーザIDグループの作成

ステップ5:ローカルユーザを作成します。

これは、タブWork Centers > Device Administration > Identities > Usersから実行できます。

手順

a. Addをクリックして、ユーザ名を定義します。

b.ログインパスワードを設定します。

c.関連するユーザグループにユーザを追加します。

d. Submitをクリックします。

≡	dentity Services	Engine		Work Centers / Device Administration								۵ ۵) Q	A
Л	Bookmarks	Overview	Identities	User Ident	ity Groups	Ext Id Sources	Network Resour	ces Policy Elements	Device Admin Policy	Sets Reports	Settings			
53	Dashboard	Users		Net	work Access Users	List > New Network Ac	cess User							
망	Context Visibility													
*	Operations			č	Network Acc	ess User								
-0	Policy			a	* Username	SecOps_User	J							
8.	Administration				Status	Enabled 🗸								
đ	Work Centers				Account Name Al	ias	0							
					Email									
?	Interactive Help				0									
				~	Passwords									
					Password Type:	Internal Users	~							
					Password Lifetin	ne:								
					 With Expirat Parameter will 	on 🕕								
					 Never Expire 	is 🕕								
									_					
				. (Password	R	e-Enter Password	ר					
				D	* Login Passwor	d			Generate Password	0				
					Enable Passwor	d			Generate Password	0				
				~	User Inform	ation								

```
ローカルユーザの作成1-2
```

≡	abala Identity Services	Engine			Work	Centers / Device Ad	ministration			٩	\$ @) Q X	٩
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
	Dashboard	Users		✓ User Inform	mation								
명	Context Visibility			First Name									
~×	Operations			Last Name									
-0	Policy			- Cast Hollie									
8.	Administration			V Account O	otions								
đ	Work Centers			Description	,								
?	Interactive Help			Change passw	rord on next login			Å					
				✓ Account D Disable a	isable Policy	s 2025=03=20	(yyyy-mm-dd)						
					С								
				 ✓ User Grou ∷ SecOps 	ps s	× (1)				d		Dancel	

ローカルユーザの作成2-2

ステップ6:(オプション)TACACS+ポリシーセットを追加します。

これは、タブWork Centers > Device Administration > Device Admin Policy Setsから実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.ポリシーセット名を定義します。

c.ポリシーセットConditionを、先ほど作成したSelect Device Type(ステップ2>b)に設定します。

d. Allowedプロトコルを設定します。

e. Saveをクリックします。

f. (>) Policy Set Viewをクリックして、認証および認可ルールを設定します。

≡	abale Identity Services E	ngine			Policy / Policy Sets		۵ ۵	0	Р У
н	Bookmarks	Policy Sets				Reset Reset Policy Se	t Hit Counts		Save
	Dashboard	Status Policy Status	Set Name Des	scription	Conditions	Allowed Protocols / Server Seque	nce Hits	Actions	View
명	Context Visibility	Q Search			0	d			
- %	Operations	0		(2	100	
0	Policy	DNAC -	Policy		DEVICE-Device Type EQUALS All Device Types#UNAC-Servers	Default Network Access 🔕 🗸	<u>י</u>	(Ç)	Ċ
8.	Administration	O Default	Defa	ault policy set		Default Network Access	+ •	ŝ	>
di.	Work Centers							_	e
							Reset		Save
?	Interactive Help							_	

TACACS+ポリシーセットの追加

手順7:TACACS+認証ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>)をク リックします。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.認証ポリシー名を定義します。

c.認証ポリシーの条件を設定し、前に作成したデバイスタイプを選択します(ステップ2>b)。

d.アイデンティティソースの認証ポリシーUseを設定します。

e. Saveをクリックします。

$\equiv \frac{\mathrm{diab}}{\mathrm{cisco}}$ Identity Servic	es Engine Work Centers / Device Administration		9 A
II Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements	Device Admin Policy Sets Reports Settings	
E Dashboard	Policy Sets→ DNAC - Policy	Reset Reset Policy Set Hit Counts	e
1-1 Context Visibility			
ℜ Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence	Hits
Dolicy	Q. Search		
Administration	DNAC - Pelicy DEVICE Device Type EQUALS All Device Typest0NAC	Default Device Admin	0
Work Centers			
	VAuthentication Policy(2)		
Interactive Help	Status Rule Name Conditions	Use Hits Ac	tions
	Q, Search	d	
	b	Internal Users	
	DNAC - Authentication E DEVICE-Device Type EQUALS All Device TypesIIDNAC-Servers	> Options • §	<u>څ</u>
		All_User_ID_Stores	
	O Default:	> Options 0 A	\$ ³
	> Authorization Policy - Local Exceptions		
	>Authorization Policy - Global Exceptions		
	>Authorization Policy(4)		

ステップ8: TACACS+認可ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>)の順 にクリックします。

各ユーザの役割の許可ポリシーを作成するには、次の手順を実行します。

- スーパー管理者ロール
- ネットワーク管理者ロール
- SecOpsロール

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b.許可ポリシー名を定義します。

c.許可ポリシー条件を設定し、(ステップ4)で作成したユーザグループを選択します。

d. (ステップ3)で作成した認可ポリシーシェルプロファイルと選択 TACACSプロファイルを設 定します。

e. Saveをクリックします。

TACACS+認証ポリシーの追加

≡	deale Identity Services I	Engine		v	Vork Centers / Device Ad	ministratio	n			٩	a 0	Q 2	<u>م</u>
Щ	Bookmarks	Overview Ide	ntities User Identity	Groups Ext Id Sourc	es Network Resources	Policy Ele	ments Device Adm	nin Policy Sets	Reports S	ettings			
51	Dashboard	Q Searc	h										
1d	Context Visibility	0	DNAC - Policy		DEVICE-Device Type EQUAL	.S All Device Typ	es#DNAC		Default [levice Admin		· + •	
х	Operations												
0	Policy	> Authenticat	ion Policy(2)										
å 0	Administration	> Authorizatio	on Policy - Local Exceptions										
al.	Work Centers	> Authorizatio	on Policy - Global Exceptions										
		~Authorizatio	on Policy(1)										
?	Interactive Help						Results						
		🕒 Statu	is Rule Name	Conditions			Command Sets	s	ihell Profiles		Hits	Actions	
		Q Sea	rch		1								
	SUPER-ADMIN	I-ROLE	Super Admin	A IdentityGroup-Name	EQUALS User identity Groups:SUPER-	ADMIN	Select from list	/ +	SUPER_ADMIN_ROL	E 🛛 🗸	•	(2)	
	NETWORK-ADM	IN-ROLE	Network Admin	R IdentityGroup-Name	EQUALS User Identity Groups:NETWO	RK-ADMIN	Select from list	0 +	NETWORK_ADMIN_I	ROLE 🐼 🗠	•	403	
	SecOps-Rol	e 🧿	SecOps	R IdentityGroup-Name	EQUALS User identity Groups:SecOps		Select from list	0 +	SecOps_Role	@ ~	•	(3)	
		٥	Default				DenyAllCommands	0 +	Deny All Shell Profile	0	+ 0	{ĝ}	
												2	
										Ret	. (Save	h

許可ポリシーの追加

確認

RADIUS設定の確認

1- DNAC – 外部ユーザの表示システム>ユーザとロール>外部認証>外部ユーザ RADIUSから初めてログインした外部ユーザのリストを表示できます。表示される情報には、ユ ーザ名とロールが含まれます。

	■ Cisco DNA Center	System /	Users & Roles		2
I	User Management Role Based Access Control External Authentication	External Authentication Cisco DNA Center supports external servers for authentication and authorization of E name of the AAA attribute chosen on the AAA server. The default attribute expected The value of the AAA attribute to be configured for authorization on AAA server woul configuration inside Authorization profile would look like "cisco-av-pairs Role=SUPER An example configuration in the case of manually defining the AAA attribute would be C Enable External User AAA Attribute AAA Attribute AAA Attribute Cisco-AVPair	tternal Users.Use the fields in this window to create, update and delete AAA Servers.The s Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be in the format of "Role-role1". On ISE server, choose the cisco-av-pair attribute from o -ADMIN-ROLE" *Cisco-AVPair=Role=SUPER-ADMIN-ROLE"	AAA Attribute here on Cisco DNA Center is th to be configured here on Cisco DNA Center. cisco specific AAA attributes list. A sample	2
		Reset to Default Update			
		 ✓ External Users \[\Vee Filter \] 		EQ, Find	
		Username +	Role	Action	
		devops_user	DevOps-Role	Delete	
			Showing 1 of 1		

2. DNAC – ユーザアクセスを確認します。

Cisco DNA Center			Q @ 4
Cisco DNA Center Image: Workflows Image: Tools Image: Tools Image: Platform Image: Tools	Overview Manage Developer Toolkit Runtime Dashboard	enter with the adoption journey map. time to value, as you guide your organization on its	Q ③ A

制限付きユーザアクセス

3.a ISE:RADIUSライブログ操作> RADIUS >ライブログ。

≡	death Identity Services	Engine	Ор	erations / RADIUS		
ji,	Bookmarks	Live Logs Live Sessions				
::	Dashboard					
명	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				Never V Latest 20	records v Last 60 Secondsv
di.	Work Centers	€ 10 Reset Repeat Counts @ Export To	Patalla Bassa Mastila Pat	ului IB Fodoslai Bastila Autostication Ba	New Anthony and a New Ave	Filter V 🔘
		Time Status	x identity Ends	ID Endpoint Profile Authentication Policy	Authorization Policy Au	thorization Profiles IP Addres
(?)	Interactive Help	Jan 19, 2025 11:19:18.1	0 DevOps_User	DNAC - Policy >> DN	AC - Authentication DNAC - Policy >> DevOps Dev	Ops-Profile
		Last Updated: Sun Jan 19 2025 23:19:57	GMT-0100 (Central European Standard Time)			Records Shown: 1

RADIUSライブログ

3.b ISE:RADIUSライブログ操作> RADIUS >ライブログ>認証ログの(詳細)をクリックします。

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	
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	DNAG
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詳細ライブログ1-2

Class ISE	
IdentityPolicyMatcheoRole	UNAC - Authentication
AuthorizationPolicyMatche ule	dR DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedR	ule DNAC - Authentication
TotalAuthenLatency	35
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#DNAC-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, PQ3wijectName=9237830-8c01-11e6-996c- 525400-4521 fadevop_use UniqueSubjectID=964d28083db66a1f8bcc98565c8f5eaa5de df467
Dente	
Result	
Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R tG/WY:ise34/526427220/15433
cisco-av-pair	ROLE=DevOps-Role
~	

RADIUS詳細ライブログ2-2

TACACS+設定の確認

1- DNAC – 外部ユーザの表示システム>ユーザとロール>外部認証>外部ユーザ TACACS+から初めてログインした外部ユーザのリストを表示できます。表示される情報には、 ユーザ名とロールが含まれます。

	■ Cisco DNA Center	System / Users & Roles	Q @ C 4
I	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 Image: Secret IP Address Image: Secret Image: Secret Image:	
		✓ External Users \[\Vee Filter \]	EQ, Find
		Username ~ Role Action secops_user SecOps-Role Deleter	
		Showing 1 of 1	

外部ユーザ

2. DNAC – ユーザアクセスを確認します。

Cisco DNA Center			Q ()
⁰ ∏ ⁰ Policy	Group-Based Access Control		C Explore
- Workflows	IP & URL Based Access Control	enter with the adoption journey map.	×
% Tools		time to value, as you guide your organization on its	
Platform			
Activities			
Explore			
		Retwork Bug Identifier Identify bugs in the network	
요 secops_user			

制限付きユーザアクセス

3.a ISE:TACACS+ライブログワークセンター>デバイス管理>概要> TACACS Livelog。

≡	abalic Identity Services	Engine					Operat	ions / TACACS			Q	۵ ۵	D Q	2
н	Bookmarks	Live Log	s											
	Dashboard													
pla S	Context Visibility								Defra		Show	Within		
*	Operations								Neve	r v	Latest 20 records	2 Last	60 Secor	nds∨
	Policy	6	🖞 🏦 Export To 🗸									Filte	~	۲
80	Administration		Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
đ	Work Centers	>		Y		Identity	`	Authentication Policy	Authorization Policy	Shell Profile	Device Type			Lo
			Jan 19, 2025 05:12:4		ò	SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All De	vice Types	IIDNAC	Loc
?	Interactive Help	La	Jan 19, 2025 05:12:4 st Updated: Sun Jan 19 2	025 17:16:38	GMT+0100	Central Europe	Authentication an Standard Time)	DNAG - Policy >> DNAG - Authentication			Device Type#All De	Reco	IDNAC	Loc vn: 2

TACACSライブログ

3.b ISE:詳細なTACACS+ライブログワークセンター>デバイス管理>概要> TACACS Livelog > (詳細)をクリックして認証ログを表示します。

1	cince Cisco ISE				
	Overview		Steps		
	Request Type Status	Authorization Pass	Step ID 13005 15049	Description Received TACACS+ Authorization Request Evaluating Policy Group	Latency (ms)
	Session Key Message Text	ise34/526427220/13958 Device-Administration: Session Authorization succeeded	15008 15048	Evaluating Service Selection Policy Queried PIP - DEVICE.Device Type	1
	Username Authorization Policy	SecOps_User DNAC - Policy >> SecOps	15041 15013 24210	Evaluating Identity Policy Selected Identity Source - Internal Users Looking up User in Internal Users IDStore	7 5 1
	Shell Profile Matched Command Set Command From Device	SecOps_Role	24212 22037 15036	Found User in Internal Users IDStore Authentication Passed Evaluating Authorization Policy	
	Authorization Details		15048 15017 22081	Queried PIP - IdentityGroup.Name Selected Shell Profile Max sessions policy passed	2 2
	Generated Time	2025-01-19 17:12:43.368 +1:00 2025-01-19 17:12:43.368	22080 13034	New accounting session created in Session cache Returned TACACS+ Authorization Reply	°
	Epoch Time (sec) ISE Node Message Text	1737303163 ise34 Device-Administration: Session Authorization succeeded			
	Failure Reason Resolution				
	Root Cause Username	SecOps_User			
	Network Device Name	DNAC			

TACACS+の詳細なライブログ1-2

Cisco ISE	
13150	nononcoon
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= 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+の詳細なライブログ2-2

トラブルシュート

現在のところ、この設定に関する特定の診断情報はありません。

参考資料

- <u>Cisco Identity Services Engine管理者ガイドリリース3.4 >デバイス管理</u>
- <u>Cisco DNA Center管理者ガイド、リリース2.3.5</u>
- <u>Cisco DNA Center:外部認証によるロールベースアクセスコントロール</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。