

AristaスイッチでのRADIUSベースの管理者ログインの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[設定](#)

[Cisco ISEの設定](#)

[ステップ 1 : Cisco ISE用Aristaネットワークデバイスプロファイルの取得](#)

[ステップ 2 : ネットワークデバイスとしてのAristaスイッチの追加](#)

[ステップ 3 : Network Devicesの下に新しいデバイスが表示されていることを確認します](#)

[ステップ 4 : 必要なユーザIDグループの作成](#)

[ステップ 5 : AdminUser IDグループの名前を設定します](#)

[手順 6 : ローカルユーザを作成して対応グループに追加する](#)

[手順 7 : 管理者ユーザの許可プロファイルの作成](#)

[ステップ 8 : AristaスイッチのIPアドレスに一致するポリシーセットの作成](#)

[ステップ 9 : 新しいポリシーセットの表示](#)

[Aristaスイッチの設定](#)

[ステップ 1 : RADIUS認証の有効化](#)

[ステップ 2 : save configuration](#)

[確認](#)

[ISEのレビュー](#)

[トラブルシューティング](#)

[シナリオ1: 「5405 RADIUS Request dropped」](#)

[問題](#)

[考えられる原因](#)

[解決方法](#)

[シナリオ2:AristaスイッチがバックアップISE PSNにフェールオーバーできない](#)

[問題](#)

[考えられる原因](#)

[解決方法](#)

はじめに

このドキュメントでは、RADIUSを使用してAristaスイッチで管理者ログインを認証するように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

続行する前に、次のことを確認してください。

- Cisco ISE (バージョン3.xを推奨) がインストールされ、動作している。
- RADIUSをサポートするEOSを実行しているAristaスイッチ
- ISEで設定されたActive Directory(AD)または内部ユーザデータベース。

使用するコンポーネント

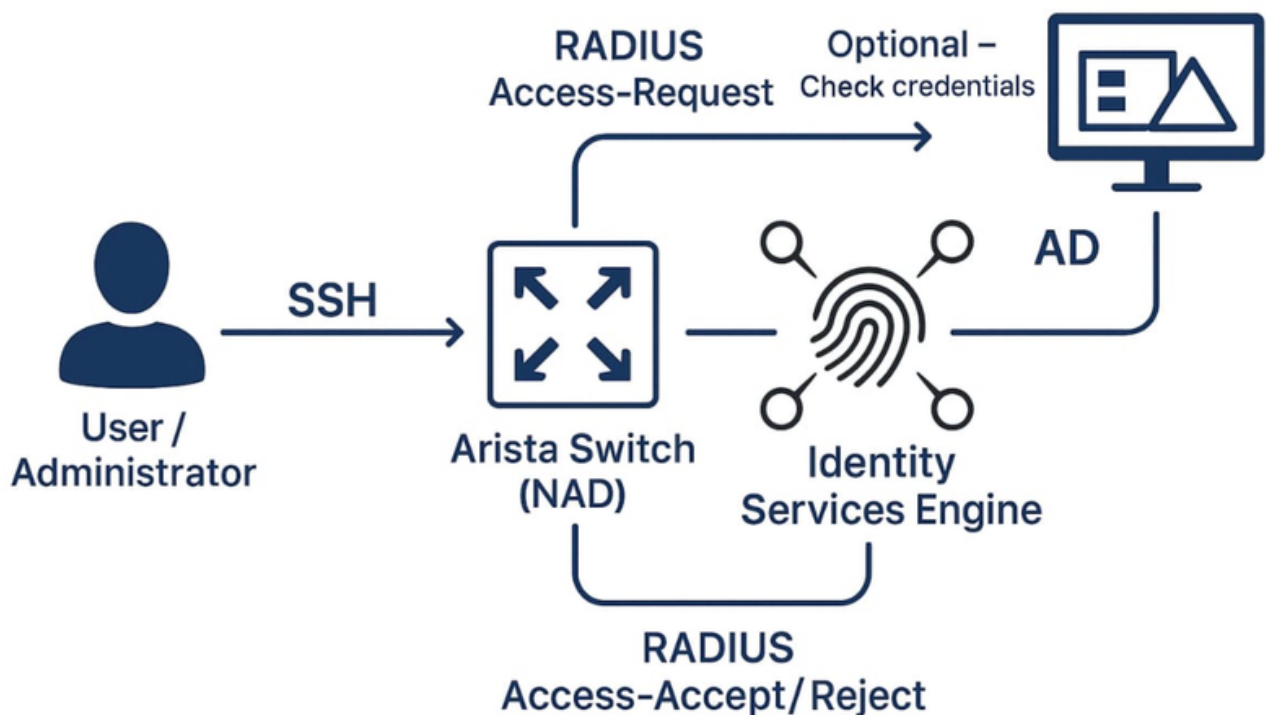
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Aristaスイッチソフトウェアイメージバージョン : 4.33.2F
- Cisco Identity Services Engine(ISE)バージョン3.3パッチ4

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。

ネットワーク図

RADIUS Device Authentication



Cisco ISEを使用し、オプションの認証ソースとしてActive Directory(AD)を使用するAristaスイッチのRADIUSベースのデバイス認証を示すネットワーク図を次に示します。

図には次のものが含まれます。

- Aristaスイッチ (ネットワークアクセスデバイス、NADとして機能)
- Cisco ISE (RADIUSサーバとして機能)
- Active Directory(AD) [オプション] (ID検証に使用)
- ユーザ/管理者 (SSH経由でログインするユーザ)

設定

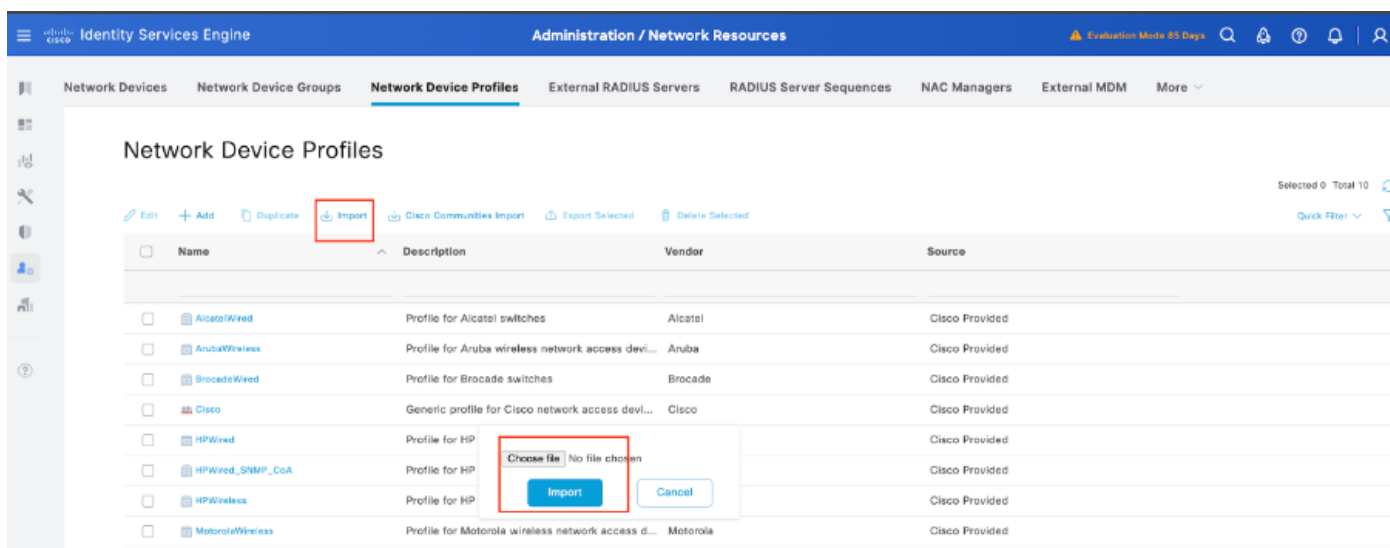
Cisco ISEの設定

ステップ1:Cisco ISE用のAristaネットワークデバイスプロファイルの取得

シスココミュニティは、Aristaデバイス専用のNADプロファイルを共有しています。このプロファイルと必要な辞書ファイルについては、『[Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration](#)』を参照してください。このプロファイルをダウンロードしてISE設定にインポートすると、統合が円滑になります

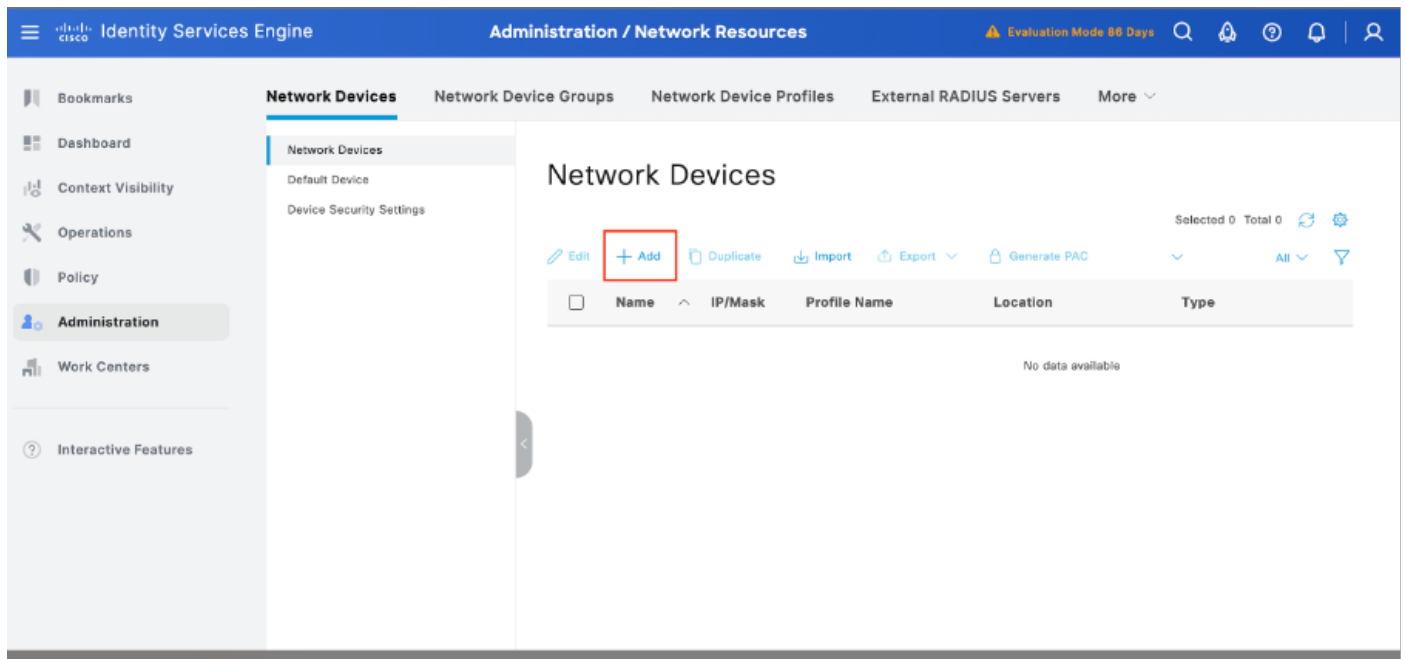
Arista NADプロファイルをCisco ISEにインポートする手順は次のとおりです。

1. プロファイルをダウンロードします。
 - Arista NADプロファイルは、上記のシスココミュニティのリンクから入手できます。
[シスココミュニティ](#)。
2. Cisco ISEへのアクセス：
 - Cisco ISE管理コンソールにログインします
3. NADプロファイルをインポートします。
 - Administration > Network Resources > Network Device Profilesの順に選択します
 - Importボタンをクリックする
 - ダウンロードしたArista NADプロファイルファイルをアップロードします。



ステップ2：ネットワークデバイスとしてのAristaスイッチの追加

1. Administration > Network Resources > Network Devices> +Addの順に選択します。



2. Addをクリックして、次の詳細情報を入力します。

1. 名前: Arista-Switch
2. IPアドレス: <Switch-IP>
3. デバイスタイプ：他の有線を選択
4. Network Device Profile:AirstaCloudVisionWiFiを選択します。
5. RADIUS認証設定:
 1. RADIUS認証の有効化
 2. 共有秘密を入力します（スイッチ設定と一致している必要があります）。

3. Saveをクリックします。

The screenshot shows the 'Network Devices' configuration page in the Cisco ISE Administration console. The breadcrumb trail is 'Administration / Network Resources'. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices' and shows the configuration for a device named 'Arista_switch'.

Configuration details:

- Name: Arista_switch
- Description: Arista_switch for device login
- IP Address: [Redacted] / 32
- Device Profile: AirstaCloudVisionWiFi
- Model Name: [Redacted]
- Software Version: 4-33-2F
- Network Device Group: [Redacted]
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)
- ☒ RADIUS Authentication Settings
 - RADIUS UDP Settings
 - Protocol: RADIUS
 - Shared Secret: [Redacted] (Show)

ステップ3：ネットワークデバイスの下に新しいデバイスが表示されていることを確認する

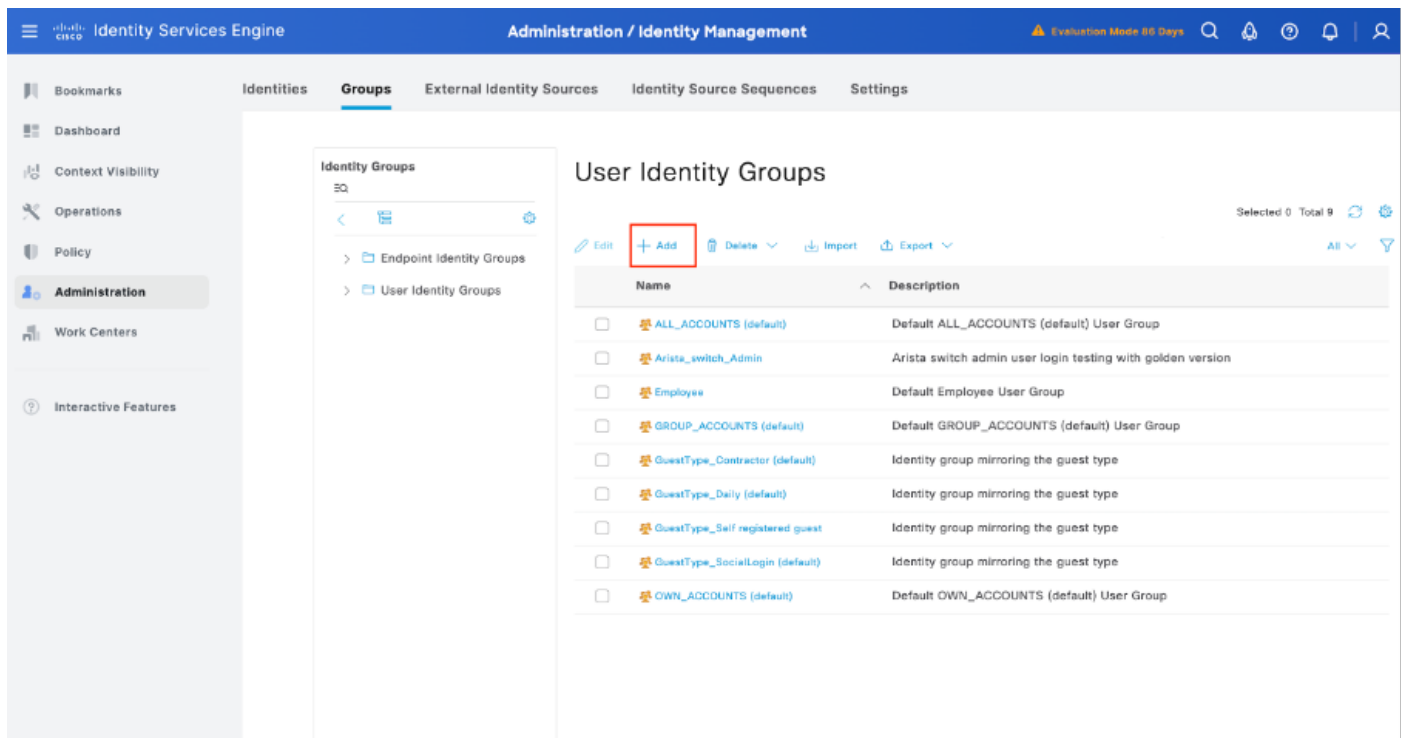
The screenshot shows the 'Network Devices' list in the Cisco ISE Administration console. The breadcrumb trail is 'Administration / Network Resources'. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices' and shows a table of network devices.

Table with 7 columns: Name, IP/Mask, Profile Name, Location, Type, Description. The table contains one row for 'Arista_switch'.

Name	IP/Mask	Profile Name	Location	Type	Description
Arista_switch	[Redacted]	AirstaCloudVisionWiFi	All Locations	All Device Types	Arista_switch for device login

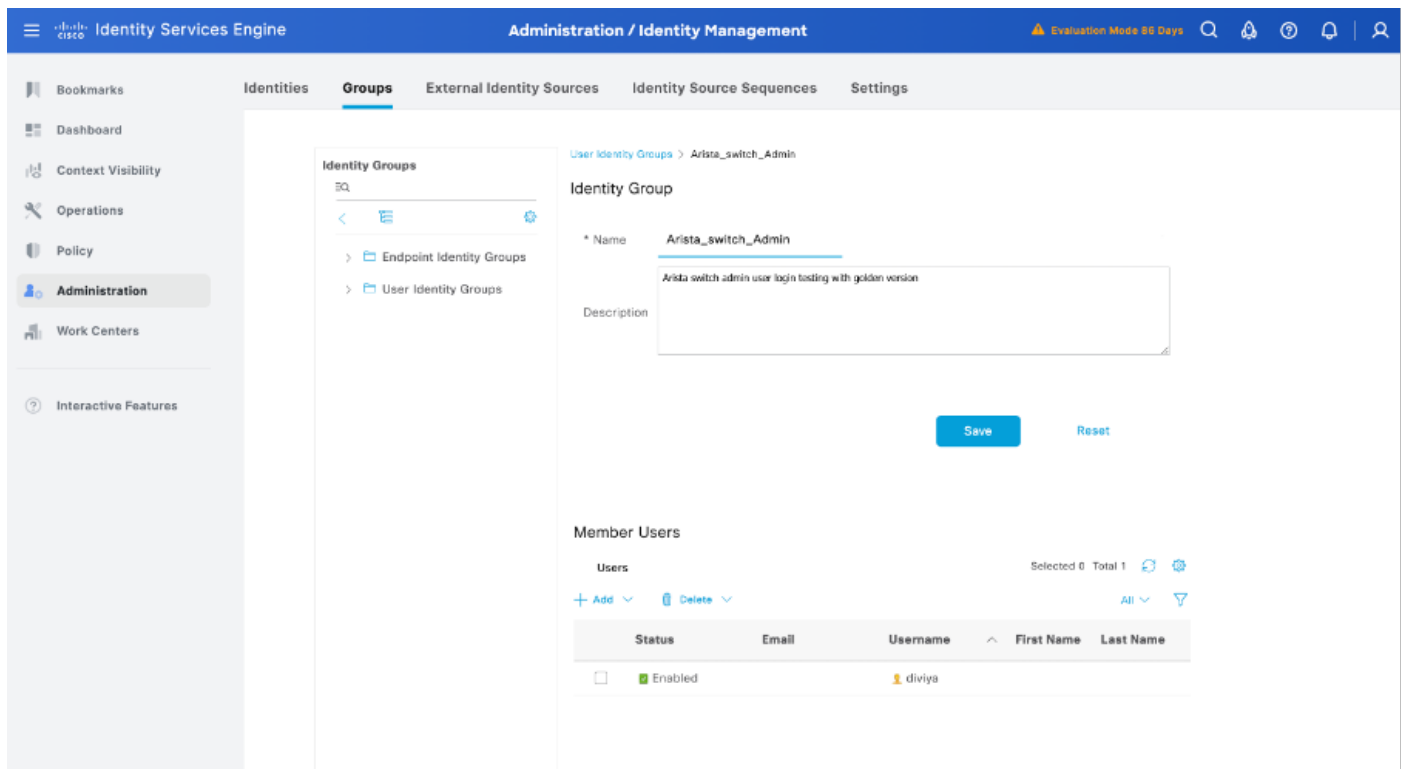
ステップ4：必要なユーザIDグループの作成

Administration > Identity Management > Groups > User Identity Groups > + Addの順に移動します。



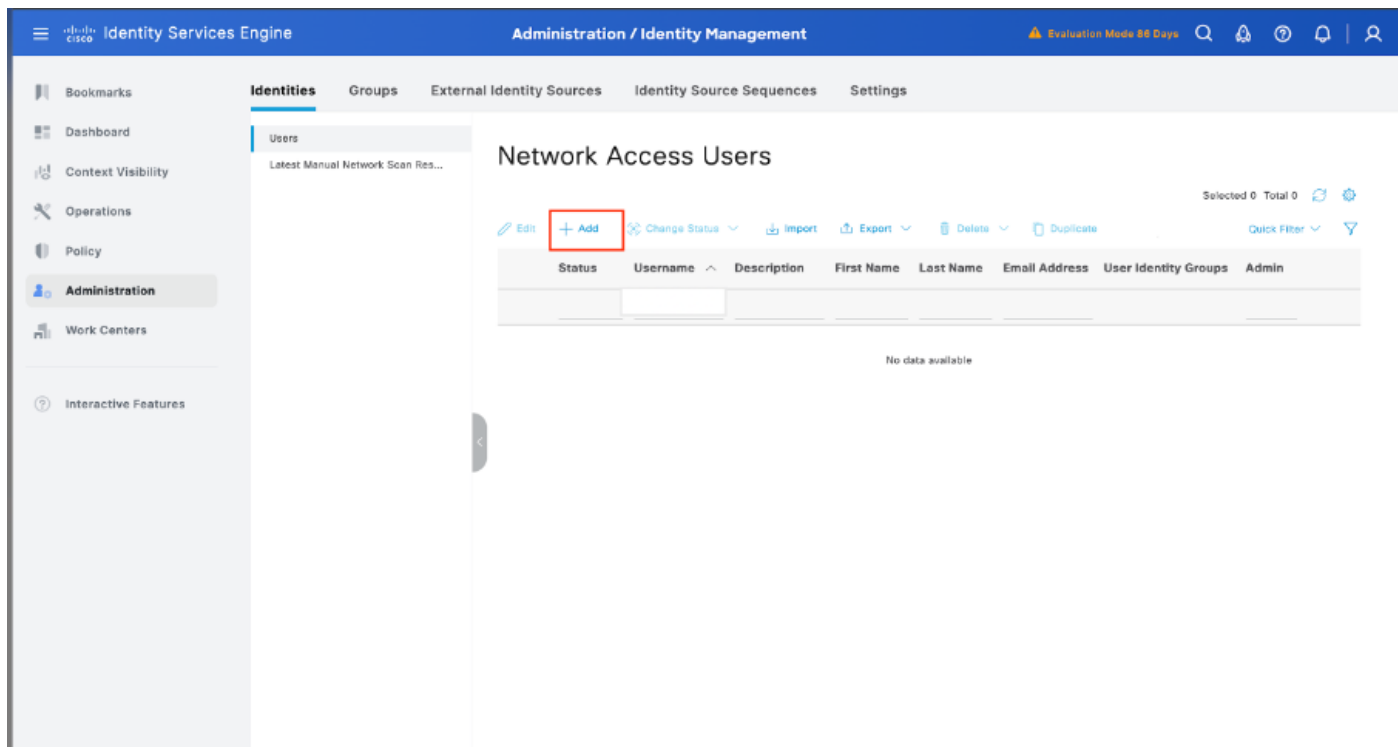
ステップ5：管理者ユーザIDグループの名前を設定する

Submitをクリックして、設定を保存します。

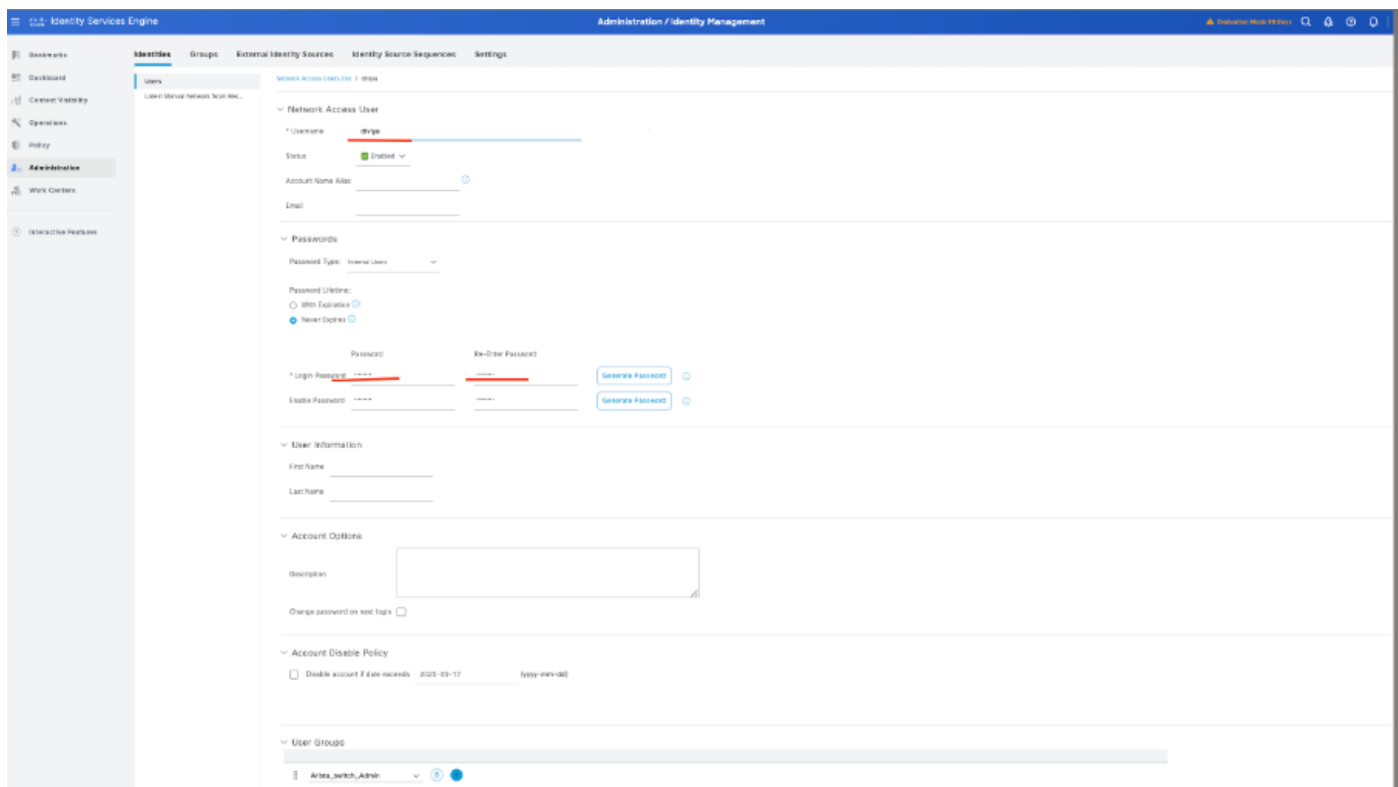


ステップ6：ローカルユーザを作成し、対応するグループに追加する

Administration > Identity Management > Identities > + Addの順に移動します。



6.1.管理者権限を持つユーザを追加する。名前とパスワードを設定してArista_switch_Adminに割り当て、下にスクロールしてSubmitをクリックし、変更を保存します。



ステップ7：管理者ユーザの許可プロファイルの作成

Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

許可プロファイルの名前を定義し、アクセスタイプをACCESS_ACCEPTのままにして、

Advanced Attributes Settingsでcisco-av-pair=shell:roles="admin"を追加し、Submitをクリックします。

Identity Services Engine Policy / Policy Elements

Authorization Profiles > Arista_switch_Admin

Authorization Profile

* Name: Arista_switch_Admin

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: AristaCloudManagedWIFI

Common Tasks

☐ ACL

☐ Security Group

Advanced Attributes Settings

Cisco:cisco-av-pair * shell:roles="admin"

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:roles="admin"

ステップ8:AristaスイッチのIPアドレスに一致するポリシーセットの作成

これは、他のデバイスがユーザにアクセス権を付与するのを防ぐためです。

左上隅のPolicy > Policy Sets >Add icon signに移動します。

Policy Sets

Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits Actions View

Search

Default Default policy set

Default Network Access

Reset Save

8.1新しい品目がポリシーセットの一番上に配置されます。Addアイコンをクリックして、新しい条件を設定します。

Status Policy Set Name Description Conditions Allowed Protocols / Server Sequence Hits Actions View

Search

New Policy Set 1

Default Default policy set

Default Network Access

Reset Save

8.2 AristaスイッチのIPアドレスに一致するRADIUS NAS-IP-Address属性にトップ条件を追加し、

Useをクリックします。

Conditions Studio

Library

Search by Name

5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	
Wireless_Access	
Wireless_MAB	
WLC_Web_Authentication	

Editor

Radius-NAS-IP-Address

Equals

Set to 'Is not'

Select attribute for condition

Dictionary	Attribute	ID	Info
Radius	Attribute	ID	
Radius	Login-LAT-Node	35	
Radius	Login-LAT-Port	63	
Radius	Login-LAT-Service	34	
Radius	NAS-IP-Address	4	
Radius	NAS-IPv6-Address	95	
Radius	NAS-Identifier	32	
Radius	NAS-Port	5	

Wrong value

Duplicate

Save

Cancel

Use

Conditions Studio

Library

Search by Name

5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	
Wireless_Access	
Wireless_MAB	
WLC_Web_Authentication	

Editor

Radius-NAS-IP-Address

Equals

Set to 'Is not'

Duplicate

Save

NEW AND OR

Cancel

Use

8.3完了したら、Saveをクリックします。

Identity Services Engine

Policy / Policy Sets

Evaluation Mode 88 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Policy Sets

Reset

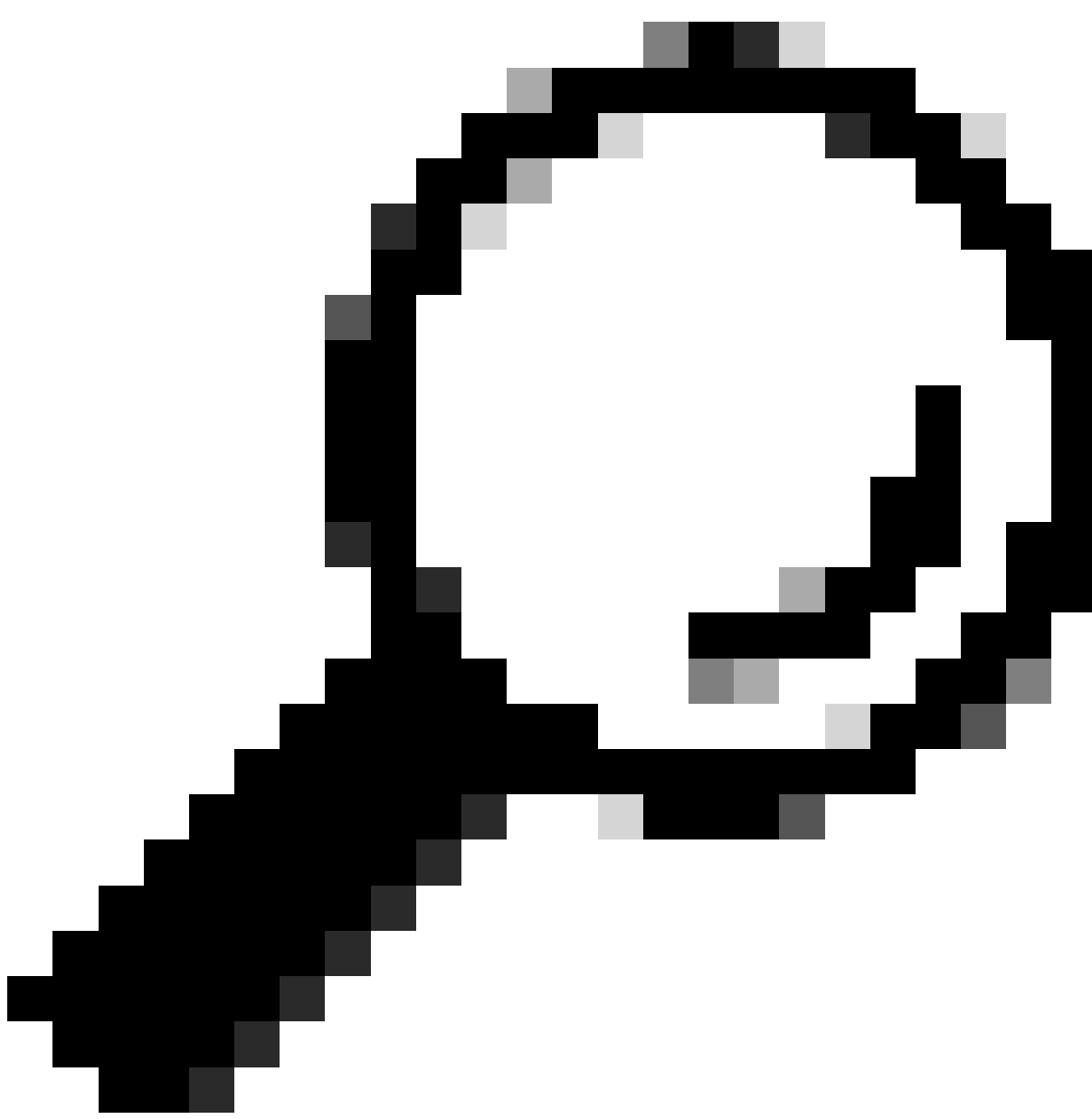
Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista_switch_radius login		Radius NAS-IP-Address EQUALS	Default Network Access	26		
✓	Wired		DEVICE-Device Type EQUALS All Device Types	Default Network Access	3		
✓	Default	Default policy set		Default Network Access	0		

Reset

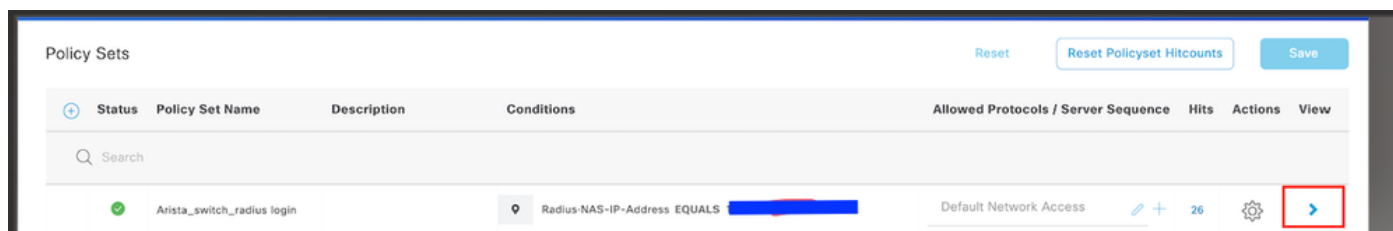
Save



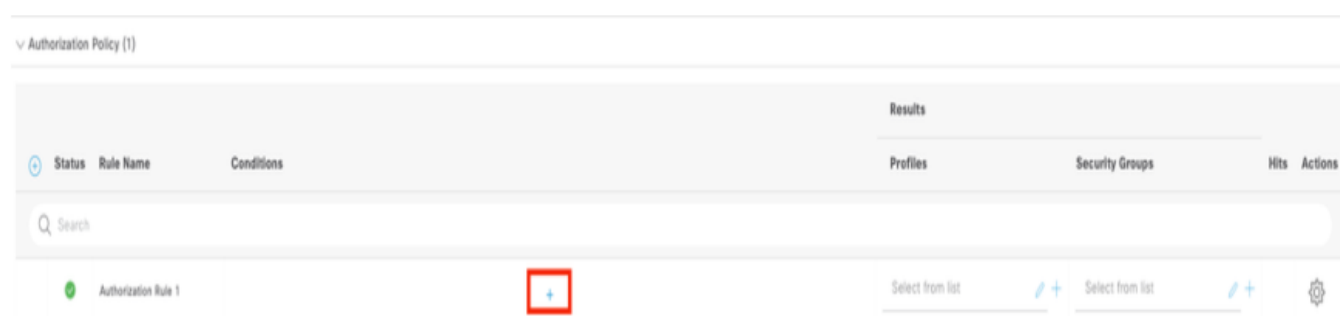
ヒント：この演習では、デフォルトのNetwork Access Protocolsリストを許可しています。新しいリストを作成し、必要に応じて絞り込むことができます。

手順9：新しいポリシーセットの表示

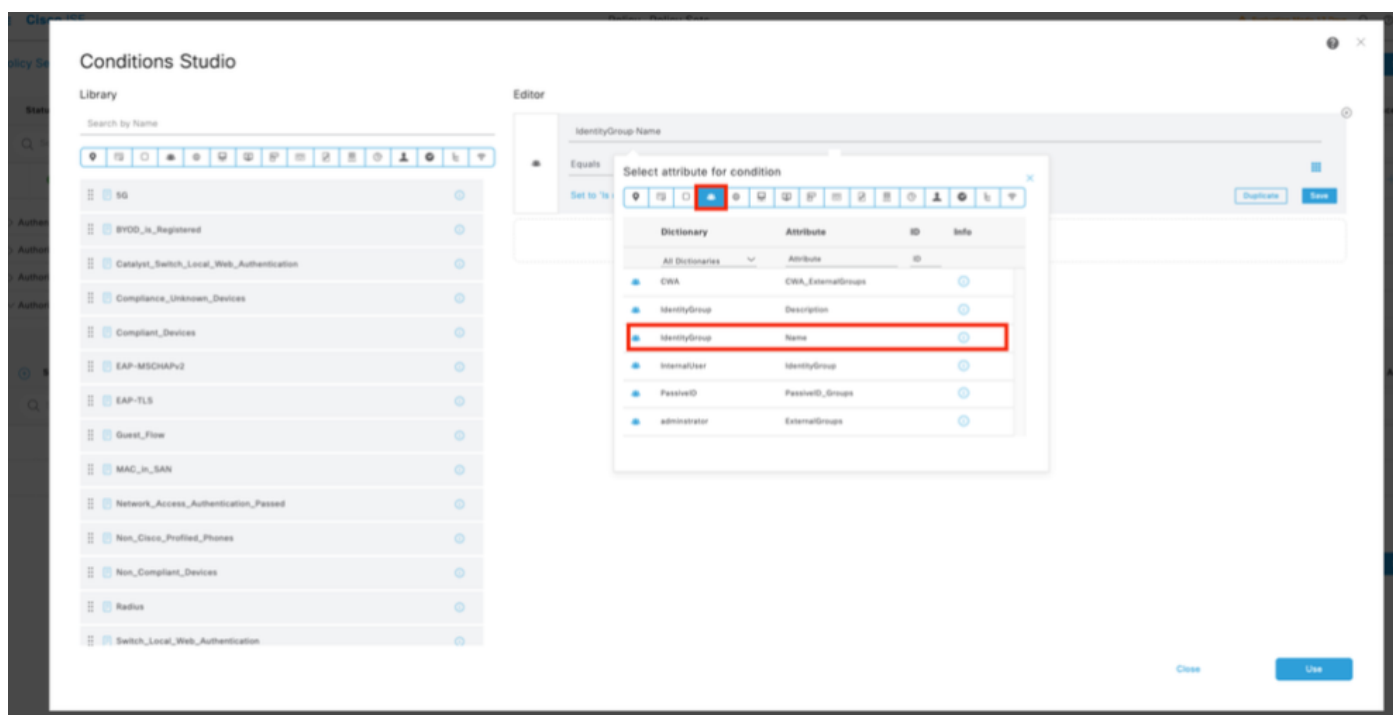
行の最後にある >アイコンをクリックします。



9.1 Authorization Policyメニューを展開し、(+)をクリックして新しい条件を追加します。



9.2条件を設定して、Dictionary Identity Group をName Equals User Identity Groups: Arista_switch_Admin (ステップ7で作成したグループ名) という属性と一致させ、Useをクリックします。



Conditions Studio

Library

Search by Name

5G	
BYOD_is_Registered	
Catalyst_Switch_Local_Web_Authentication	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
Guest_Flow	
MAC_in_SAN	
Network_Access_Authentication_Passed	
Non_Cisco_Profiling_Phones	
Non_Compliant_Devices	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	

Editor

IdentityGroup-Name

Equals User Identity Groups:Arista_switch_Admin

Set to 'Is not'

Duplicate Save

NEW AND OR

Cancel

Use

9.3新しい条件が認可ポリシーで設定されていることを検証し、次にProfilesの下にユーザプロファイルを追加します。

Authorization Policy(2)

Status	Rule Name	Conditions	Results			
			Profiles	Security Groups	Hits	Actions
Search						
✓	Arista_Radius_login	IdentityGroup-Name EQUALS User Identity Groups:Arista_switch_Admin	Arista_switch_Admin	Select from list	9	⚙️
✓	Default		DenyAccess	Select from list	0	⚙️

Reset Save

Aristaスイッチの設定

ステップ 1 : RADIUS認証の有効化

Aristaスイッチにログインし、設定モードに入ります。

設定

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

RADIUSサーバタイムアウト(5)

RADIUSサーバ再送信3

RADIUSサーバのデッドタイム(30)

!

aaaグループサーバradius ISE

サーバ<ISE-IP>

!

aaa authentication login default group ISEローカル

aaa authorization exec default group ISEローカル

aaa accounting exec default start-stopグループISE

aaa accountingコマンド15 default start-stop group ISE

aaa accounting system default start-stopグループISE

!

最後

ステップ 2 : save configuration

リブート後も設定を保持するには、次の手順を実行します。

write memory

または

copy running-config startup-config (実行コンフィギュレーションのスタートアップコンフィギュレーションのコピー)

確認

ISEのレビュー

1. 新しいRADIUSクレデンシャルを使用して、Aristaスイッチへのログインを試行します。

1.1 Operations > Radius > Live logsの順に移動します。

1.2表示される情報は、ユーザが正常にログインしたかどうかを示します。

Operations / RADIUS

Misconfigured Supplicants: 0, Misconfigured Network Devices: 0, RADIUS Drops: 0, Client Stopped Responding: 0, Repeat Counter: 5

Refresh: Never, Show: Latest 20 records, Within: Last 3 hours

Reset Repeat Counts, Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 07:08:22.0...	Success		4	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...	Success		1	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...	Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...	Success			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

2. 「失敗」ステータスについては、セッションの詳細を確認します。

Operations / RADIUS

Misconfigured Supplicants: 0, Misconfigured Network Devices: 0, RADIUS Drops: 0, Client Stopped Responding: 0, Repeat Counter: 6

Refresh: Never, Show: Latest 20 records, Within: Last 3 hours

Reset Repeat Counts, Export To

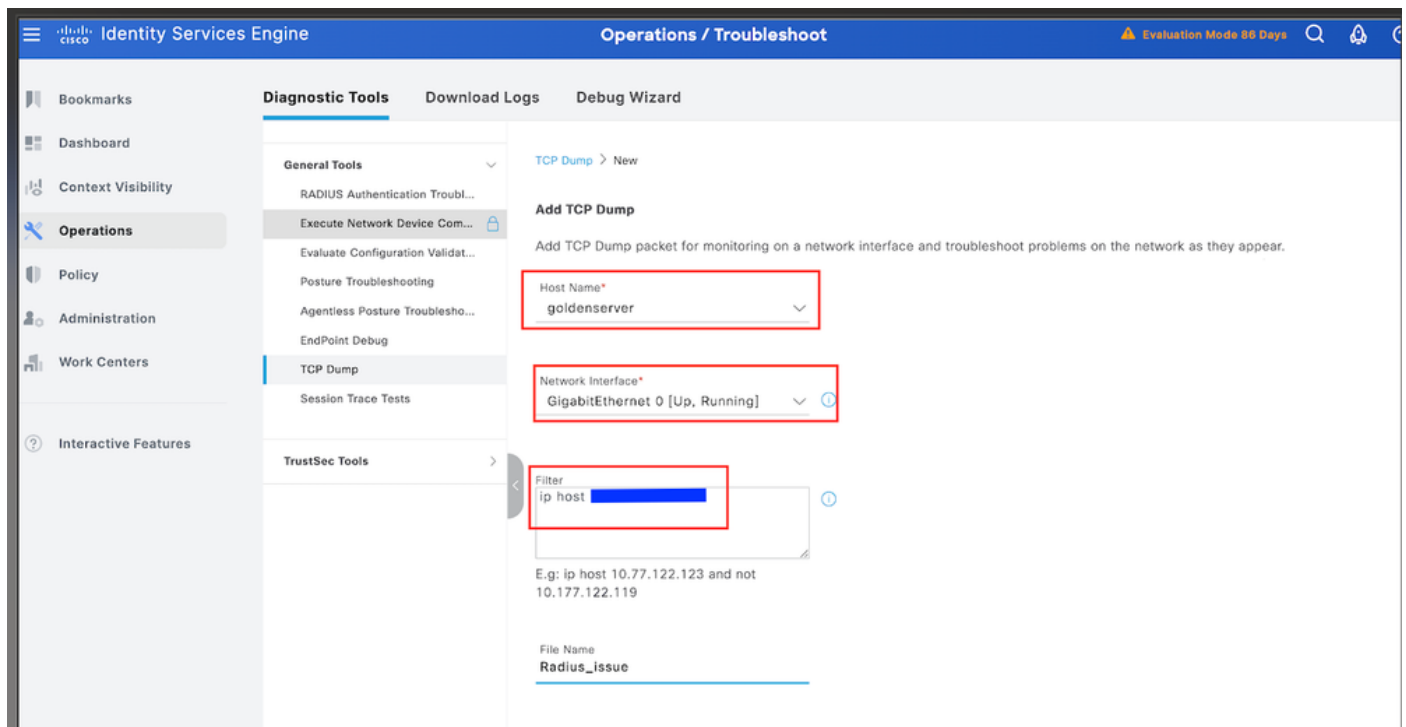
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 05:57:12.4...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:57:02.5...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:16.3...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:08.0...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

3. 要求がRadiusライブログに表示されない場合（これは、UDP要求がパケットキャプチャを介してISEノードに到達しているかどうかを確認するために使用されます）。

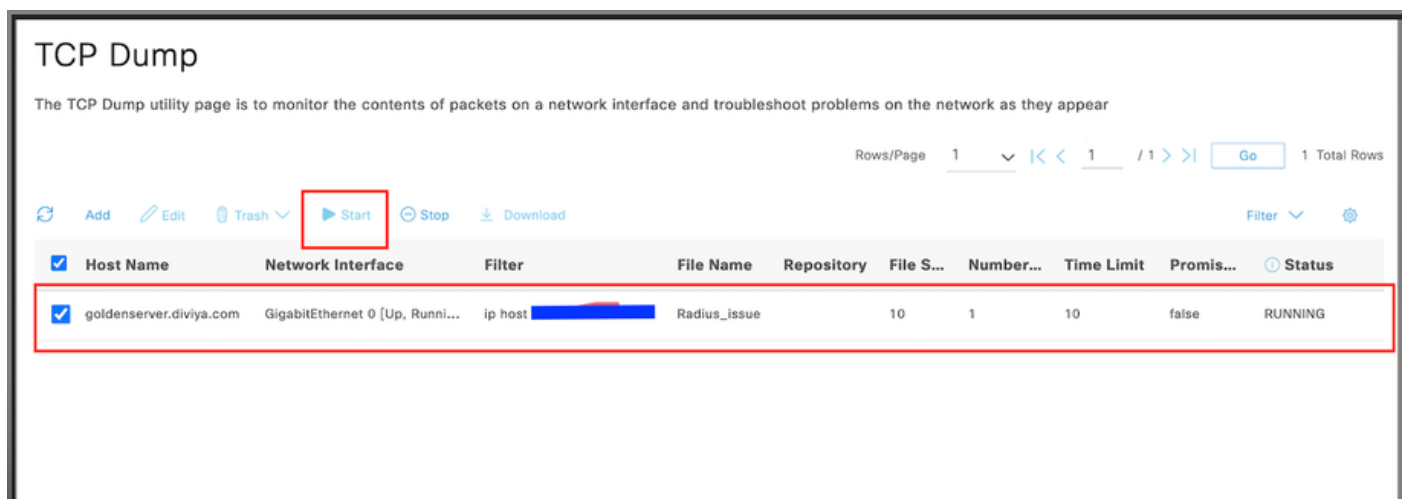
3.1. Operations > Troubleshoot > Diagnostic Tools > TCP dumpの順に移動します。

3.2. 新しいキャプチャを追加し、UDPパケットがISEノードに到着しているかどうかを確認するためにファイルをローカルマシンにダウンロードします。

3.3. 必要な情報を入力し、スクロールダウンしてSaveをクリックします。



3.4. キャプチャを選択して開始します。



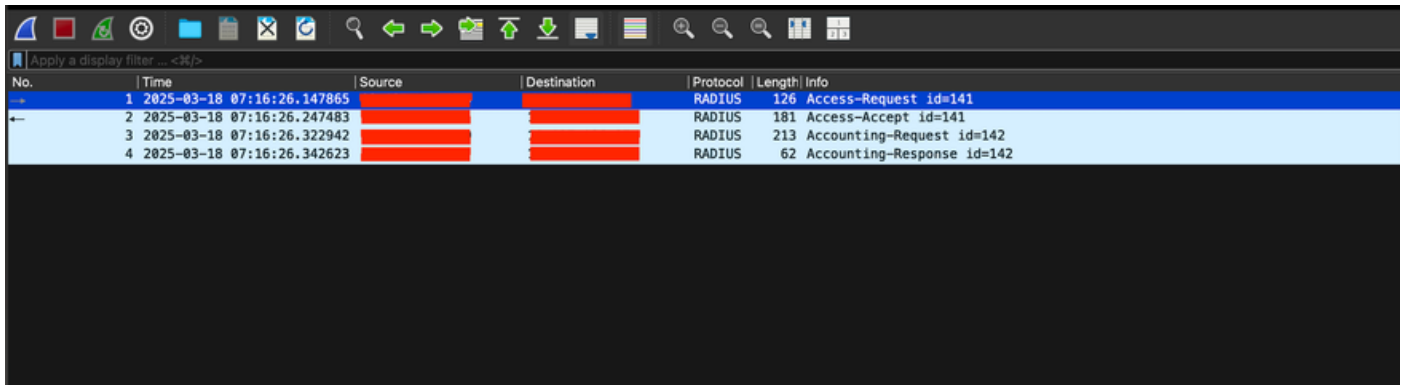
3.5. ISEキャプチャの実行中にAristaスイッチへのログインを試みます。

3.6. ISEでTCPダンプを停止し、ファイルをローカルマシンにダウンロードする。

3.7. トラフィック出力を確認する。

予想される出力：

パケット番号1。AristaスイッチからISEサーバにポート1812(RADIUS)経由で要求します。
 パケット番号2。ISEサーバが初期要求を受け入れて応答します。



No.	Time	Source	Destination	Protocol	Length	Info
1	2025-03-18 07:16:26.147865	10.10.10.10	10.10.10.10	RADIUS	126	Access-Request id=141
2	2025-03-18 07:16:26.247483	10.10.10.10	10.10.10.10	RADIUS	181	Access-Accept id=141
3	2025-03-18 07:16:26.322942	10.10.10.10	10.10.10.10	RADIUS	213	Accounting-Request id=142
4	2025-03-18 07:16:26.342623	10.10.10.10	10.10.10.10	RADIUS	62	Accounting-Response id=142

トラブルシューティング

シナリオ1: 「5405 RADIUS Request dropped」

問題

このシナリオでは、ネットワークデバイス (Aristaスイッチなど) が認証を試行する際に、Cisco ISEで「11007 Could not locate Network Device or AAA Client」という理由で「5405 RADIUS Request dropped」エラーをトラブルシューティングします。

考えられる原因

- AristaスイッチのIPアドレスが既知のネットワークデバイスの中にリストされていないため、Cisco Identity Services Engine(ISE)はそのスイッチを識別できません。
- RADIUS要求は、ISEが有効なネットワークデバイスまたはAAAクライアントとして認識しないIPアドレスから送信されます。
- スイッチとISEの設定が一致していない (IPや共有秘密が正しくない) 可能性があります。

解決方法

- 正しいIPアドレスを持つネットワークデバイスのCisco ISEリストにスイッチを追加します。
- ISEに設定されているIPアドレスと共有秘密が、スイッチに設定されている内容と正確に一致することを確認します。
- 修正した後は、RADIUS要求が正しく認識され、処理される必要があります。

シナリオ2:AristaスイッチがバックアップISE PSNにフェールオーバーできない

問題

Aristaスイッチは、RADIUS認証にCisco ISEを使用するように設定されています。プライマリISEポリシーサービスノード(PSN)が使用不能になっても、スイッチは自動的にバックアップ

PSNにフェールオーバーしません。その結果、認証ログはプライマリISE PSNからのみ表示され、プライマリがダウンした場合のセカンダリ/バックアップPSNからのログはありません。

考えられる原因

- AristaスイッチのRADIUSサーバ設定はプライマリISEノードだけをポイントするため、バックアップサーバは使用されません。
- RADIUSサーバの優先度が正しく設定されていないか、バックアップISE IPが設定に含まれていません。
- スwitchのタイムアウトおよび再送信の設定が小さすぎるため、バックアップPSNへのフォールバックが正常に行われません。
- スwitchはPSNにFQDNを使用しますが、DNS解決はすべてのAレコードを返すわけではなく、プライマリサーバだけにアクセスが発生します。

解決方法

- 複数のISE PSN IPがスイッチのRADIUSサーバグループ設定に入力されていることを確認します。これにより、プライマリに到達できない場合に、スイッチがバックアップISE PSNを使用できるようになります。

設定例：

```
radius-server host <ISE1-IP> key <シークレット>
```

```
radius-server host <ISE2-IP> key <シークレット>
```

- RADIUSサーバのプライオリティ、タイムアウト、および再送信の値が、信頼性の高いフェールオーバー用に正しく設定されていることを確認します。
- FQDNを使用する場合は、DNS設定と解決を確認して、すべてのPSN IPアドレスがスイッチによって返され、使用されていることを確認します。

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。