

Configurazione dell'accesso con amministratore basato su RADIUS sullo switch Arista

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione di Cisco ISE](#)

[Passaggio 1. Come ottenere il profilo del dispositivo di rete Arista per Cisco ISE](#)

[Passaggio 2. Aggiungere lo switch Arista come dispositivo di rete](#)

[Passaggio 3. Verificare che il nuovo dispositivo sia visualizzato in Dispositivi di rete](#)

[Passaggio 4. Creazione dei gruppi di identità utente richiesti](#)

[Passaggio 5. Impostazione di un nome per il gruppo di identità AdminUser](#)

[Passaggio 6. Creare gli utenti locali e aggiungerli al gruppo corrispondente](#)

[Passaggio 7. Creare il profilo di autorizzazione per l'utente amministratore](#)

[Passaggio 8. Creare un set di criteri corrispondente all'indirizzo IP dello switch Arista](#)

[Passaggio 9. Visualizzare il nuovo set di criteri](#)

[Configurazione dello switch Arista](#)

[Passaggio 1. Abilitazione dell'autenticazione RADIUS](#)

[Passaggio 2. Salvataggio della configurazione](#)

[Verifica](#)

[Recensione ISE](#)

[Risoluzione dei problemi](#)

[Scenario 1. "Richiesta RADIUS 5405 ignorata"](#)

[Problema](#)

[Possibili cause](#)

[Soluzione](#)

[Scenario 2: errore switch Arista nel failover sul backup del PSN ISE](#)

[Problema](#)

[Possibili cause](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) per autenticare gli accessi amministratore sugli switch Arista tramite RADIUS.

Prerequisiti

Requisiti

Prima di procedere, assicurarsi che:

- Cisco ISE (versione 3.x consigliata) è installato e operativo.
- Switch Arista con EOS e supporto RADIUS.
- Active Directory (AD) o il database utente interno configurato in ISE.

Componenti usati

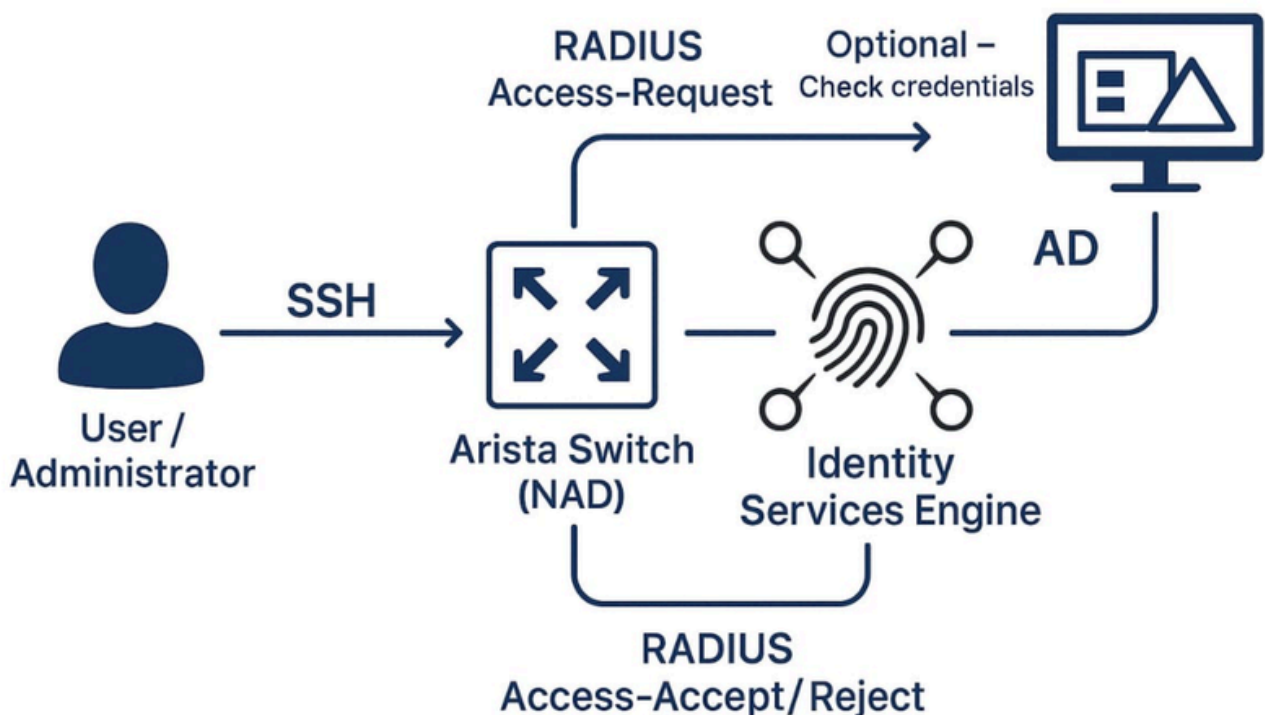
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Versione immagine software switch Arista: 4.33.2F
- Patch 4 per Cisco Identity Services Engine (ISE) versione 3.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

RADIUS Device Authentication



Di seguito è riportato un diagramma di rete che illustra l'autenticazione basata su RADIUS per uno

switch Arista che utilizza Cisco ISE, con Active Directory (AD) come origine di autenticazione facoltativa.

Il diagramma include:

- Switch Arista (dispositivo di accesso alla rete, AD)
- Cisco ISE (funge da server RADIUS)
- Active Directory (AD) [Facoltativo] (utilizzato per la verifica dell'identità)
- Utente/Amministratore (che accede tramite SSH)

Configurazione

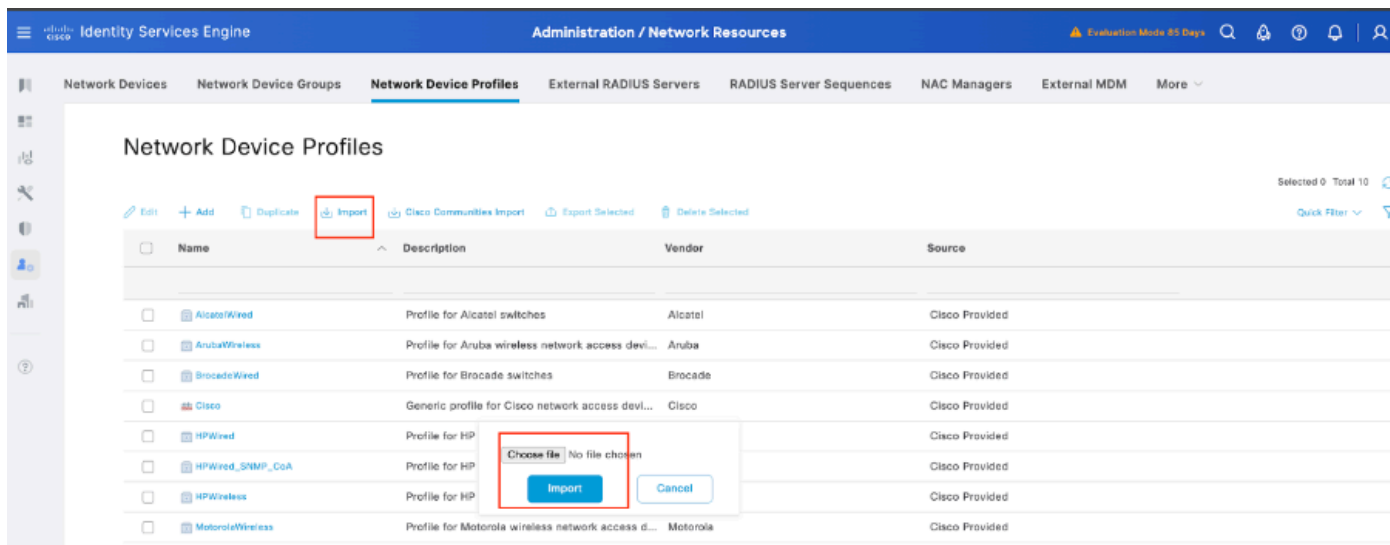
Configurazione di Cisco ISE

Passaggio 1. Come ottenere il profilo di dispositivo di rete Arista per Cisco ISE

La Cisco Community ha condiviso un profilo NAD dedicato per i dispositivi Arista. Questo profilo, insieme ai file del dizionario necessari, è disponibile nell'articolo [Arista CloudVision WiFi Dictionary e NAD Profile for ISE Integration](#). Il download e l'importazione di questo profilo nella configurazione ISE semplifica l'integrazione

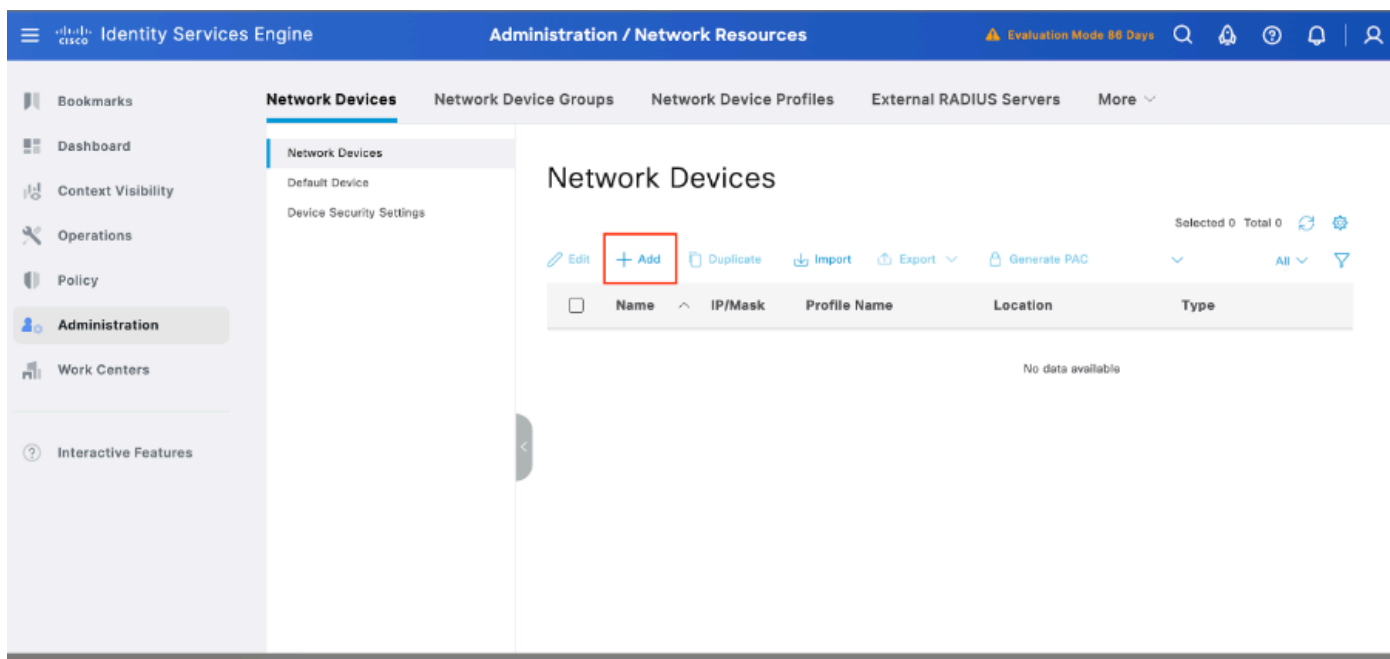
Di seguito viene riportata la procedura per importare il profilo Arista e AD in Cisco ISE:

1. Scarica il profilo:
 - Ottenere il profilo Arista E AD dal collegamento alla Cisco Community indicato sopra. [Cisco Community](#).
2. Access Cisco ISE:
 - Accedere alla console di amministrazione di Cisco ISE.
3. Importare il profilo NAD:
 - Selezionare Amministrazione > Risorse di rete > Profili dispositivi di rete.
 - Fare clic sul pulsante Importa.
 - Caricare il file di profilo Arista e AD scaricato.



Passaggio 2. Aggiunta dello switch Arista come dispositivo di rete

1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



2. Fare clic su Add (Aggiungi) e inserire i seguenti dettagli:

1. Nome: Arista-Switch
2. Indirizzo IP: <IP switch>
3. Tipo di dispositivo: Scegli altro cablato
4. Profilo dispositivo di rete: selezionare AirstaCloudVisionWiFi.
5. Impostazioni autenticazione RADIUS:
 1. Abilita autenticazione RADIUS
 2. Immettere il segreto condiviso (deve corrispondere alla configurazione dello switch).

3. Fare clic su Salva.

Identity Services Engine Administration / Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM

Network Devices List > Arista_switch

Network Devices

Name: Arista_switch

Description: Arista_switch for device login

IP Address: [Redacted] / 32

Device Profile: AristaCloudVisionWiFi

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](#)

Passaggio 3. Verificare che il nuovo dispositivo sia visualizzato in Dispositivi di rete

Identity Services Engine Administration / Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | More

Network Devices

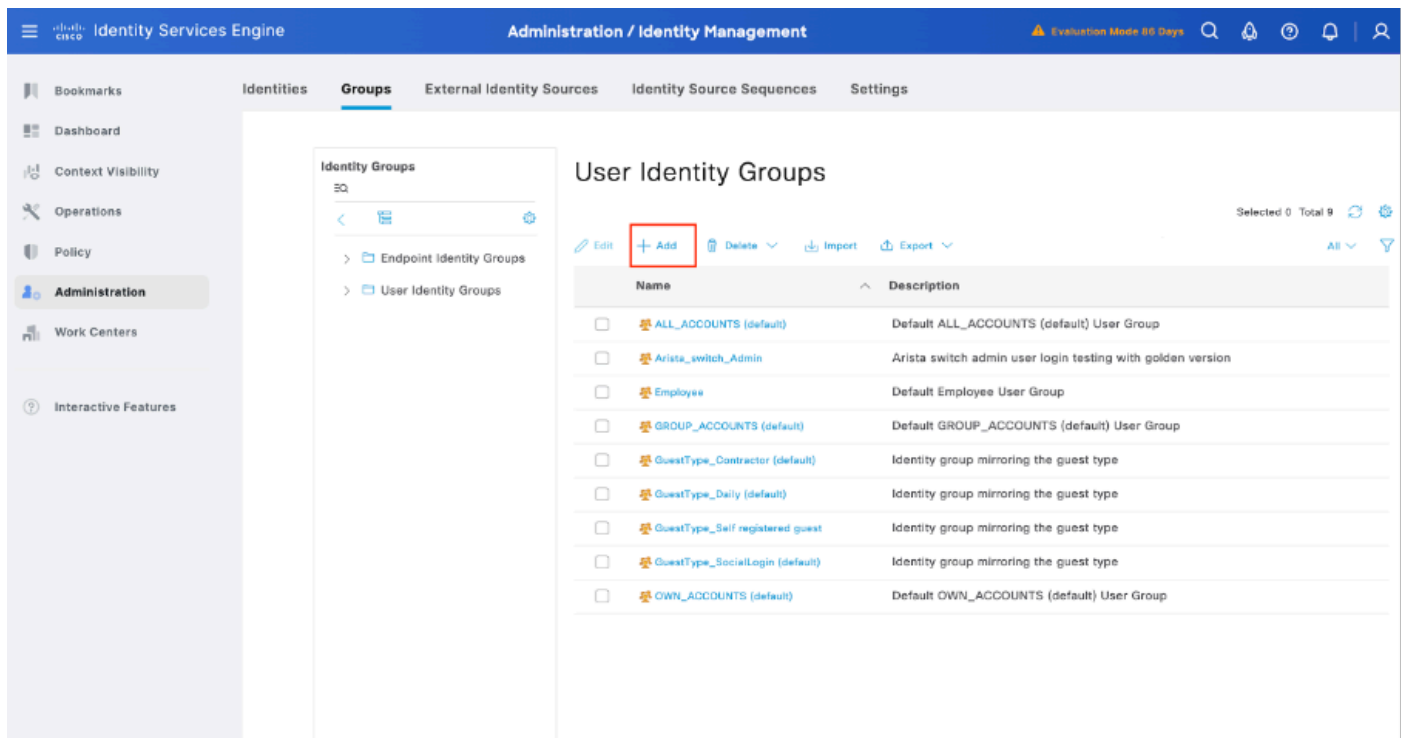
Selected 0 Total 1

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

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

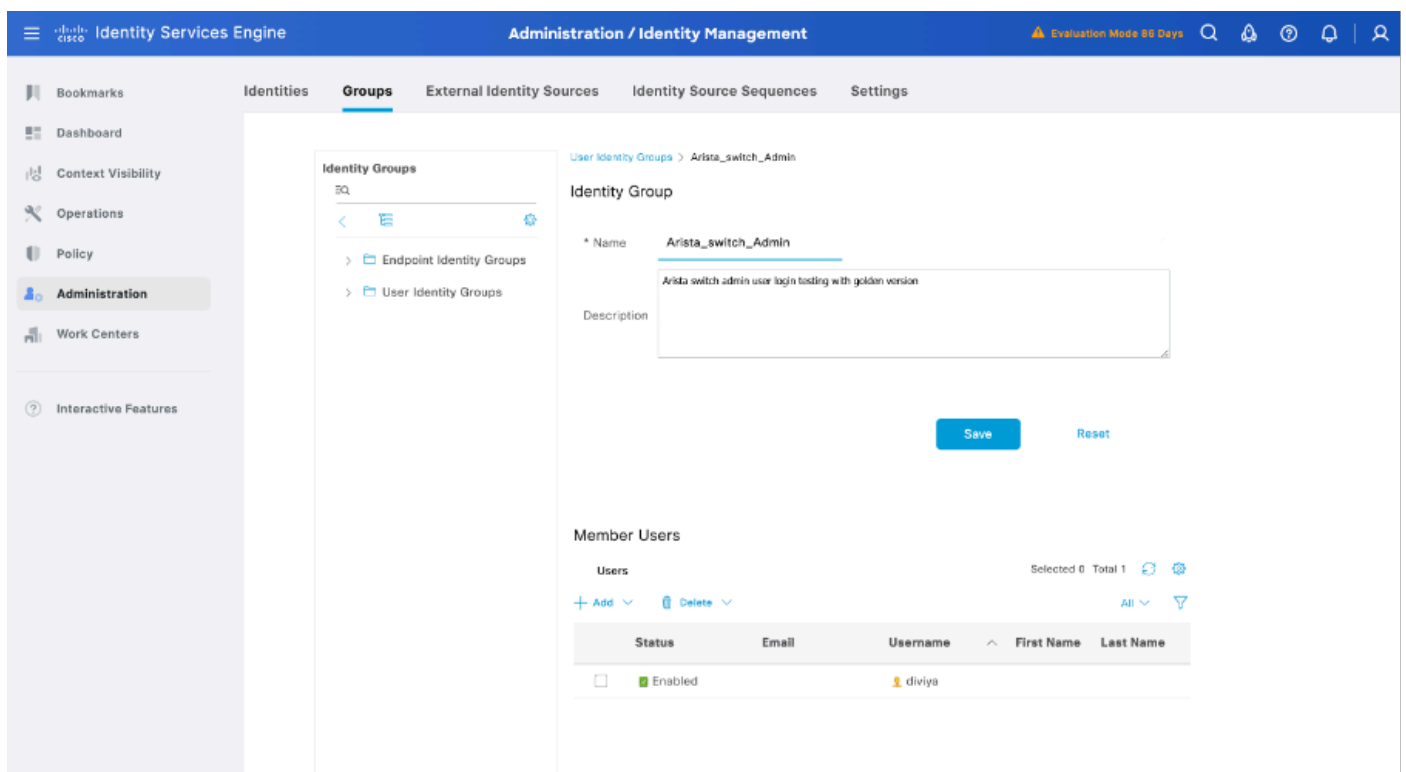
Passaggio 4. Creare i gruppi di identità utente richiesti

Passare a Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente > +
Aggiungi:



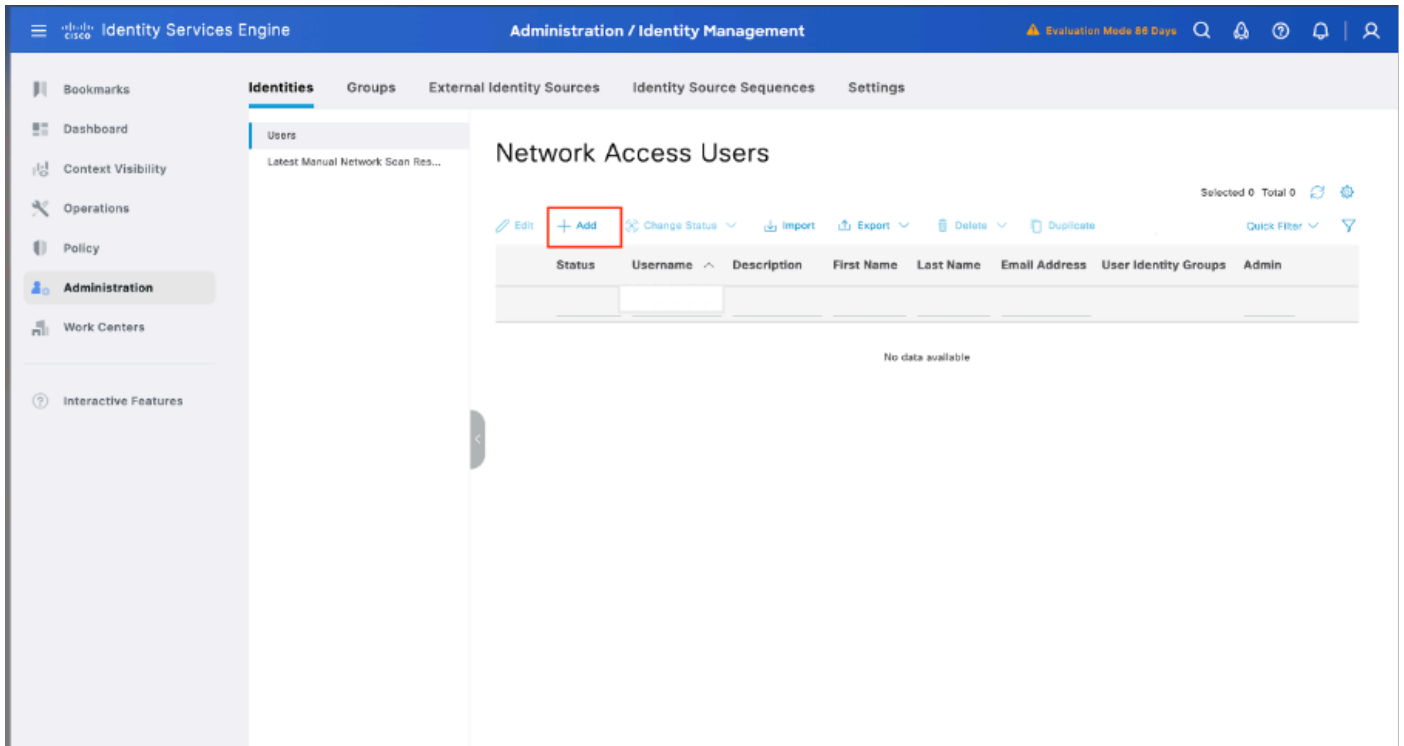
Passaggio 5. Imposta un nome per il gruppo di identità dell'utente amministratore

Per salvare la configurazione, fare clic su Submit (Invia):

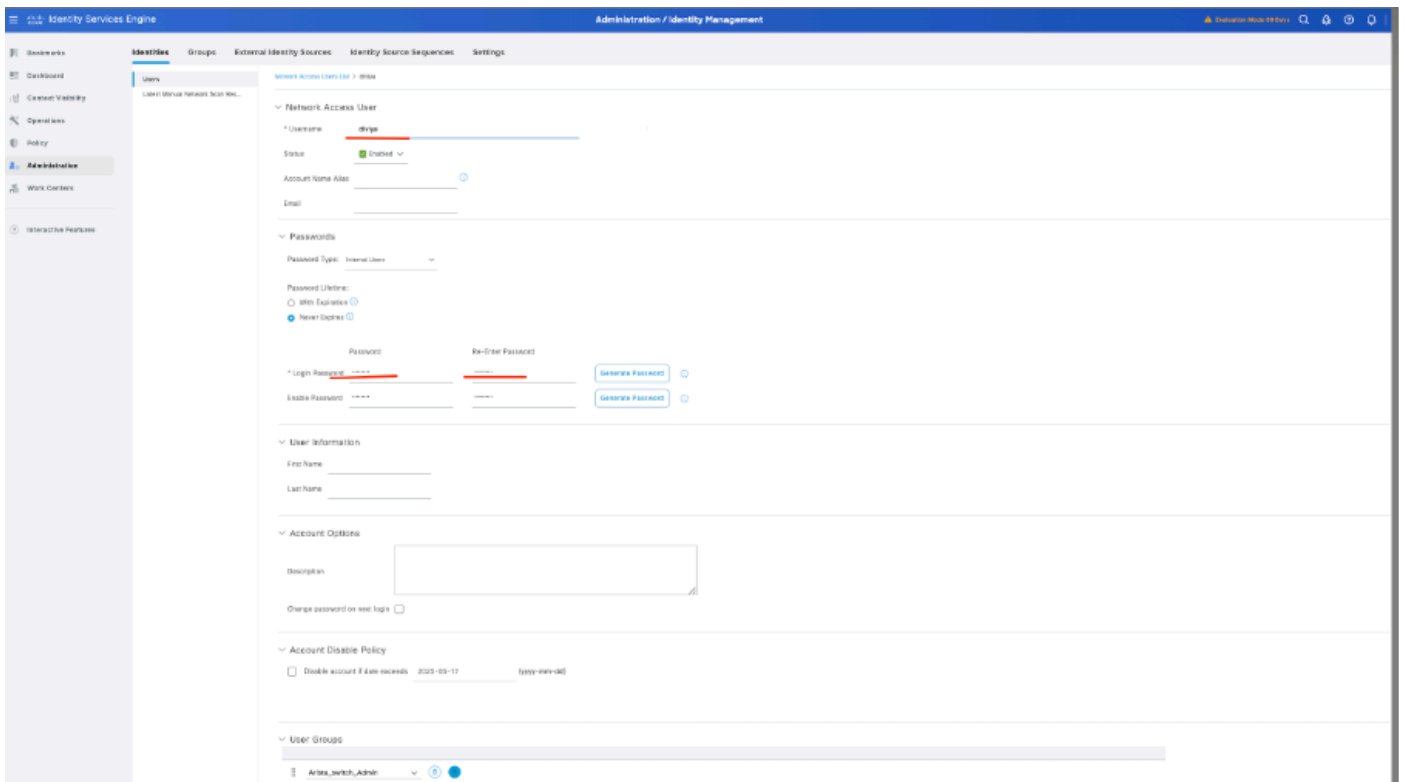


Passaggio 6. Creare gli utenti locali e aggiungerli al gruppo corrispondente

Passare a Amministrazione > Gestione delle identità > Identità > + Aggiungi:



6.1. Aggiungere l'utente con diritti di amministratore. Impostare un nome e una password e assegnarli ad Arista_switch_Admin, scorrere verso il basso e fare clic su Invia per salvare le modifiche.



Passaggio 7. Creare il profilo di autorizzazione per l'utente amministratore

Passare a Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione > +Aggiungi.

Definire un nome per il profilo di autorizzazione, lasciare il tipo di accesso impostato su ACCESS_ACCEPT e in Impostazioni avanzate attributi aggiungere cisco-av-pair=shell:roles="admin" con e fare clic su Submit.

Passaggio 8. Creare un set di criteri corrispondente all'indirizzo IP dello switch Arista

In questo modo si impedisce ad altre periferiche di concedere l'accesso agli utenti.

Selezionare Policy > Policy Sets > Add icon sign (Criterio > Set di criteri > Aggiungi icona) nell'angolo superiore sinistro.

8.1 Una nuova riga viene posizionata in cima ai set di criteri. Fare clic sull'icona Aggiungi per configurare una nuova condizione.

8.2 Aggiungere una condizione superiore per l'attributo RADIUS NAS-IP-Address corrispondente all'indirizzo IP dello switch Arista, quindi fare clic su Usa.

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	

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'

NEW AND OR

Cancel Use

8.3 Al termine, fare clic su Save (Salva):

Identity Services Engine

Policy / Policy Sets

Evaluation Mode 88 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Policy Sets

Reset

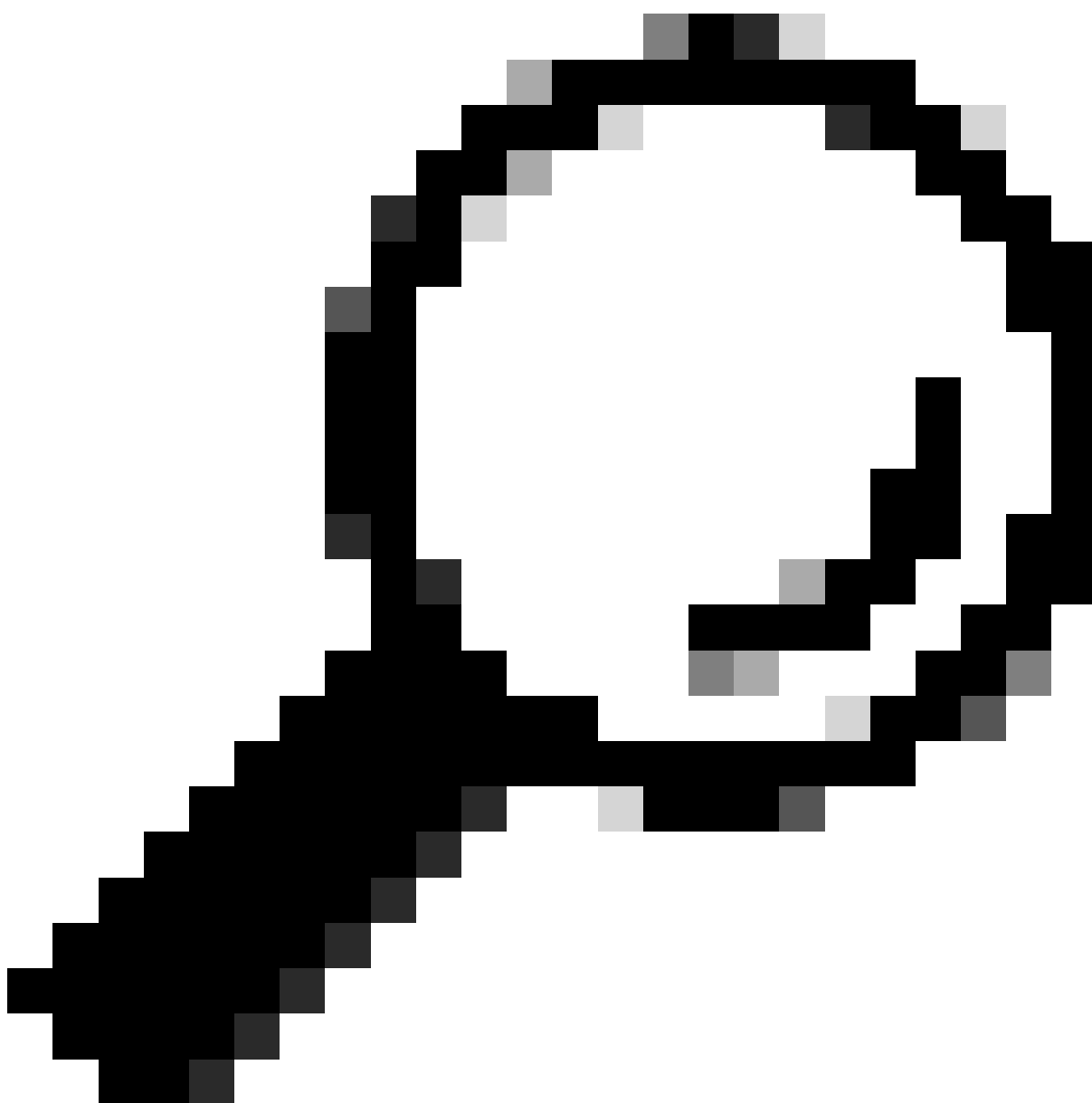
Reset Policyset Hitcounts

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



Suggerimento: Per questo esercizio è stata selezionata l'opzione Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

Passaggio 9. Visualizza il nuovo set di criteri

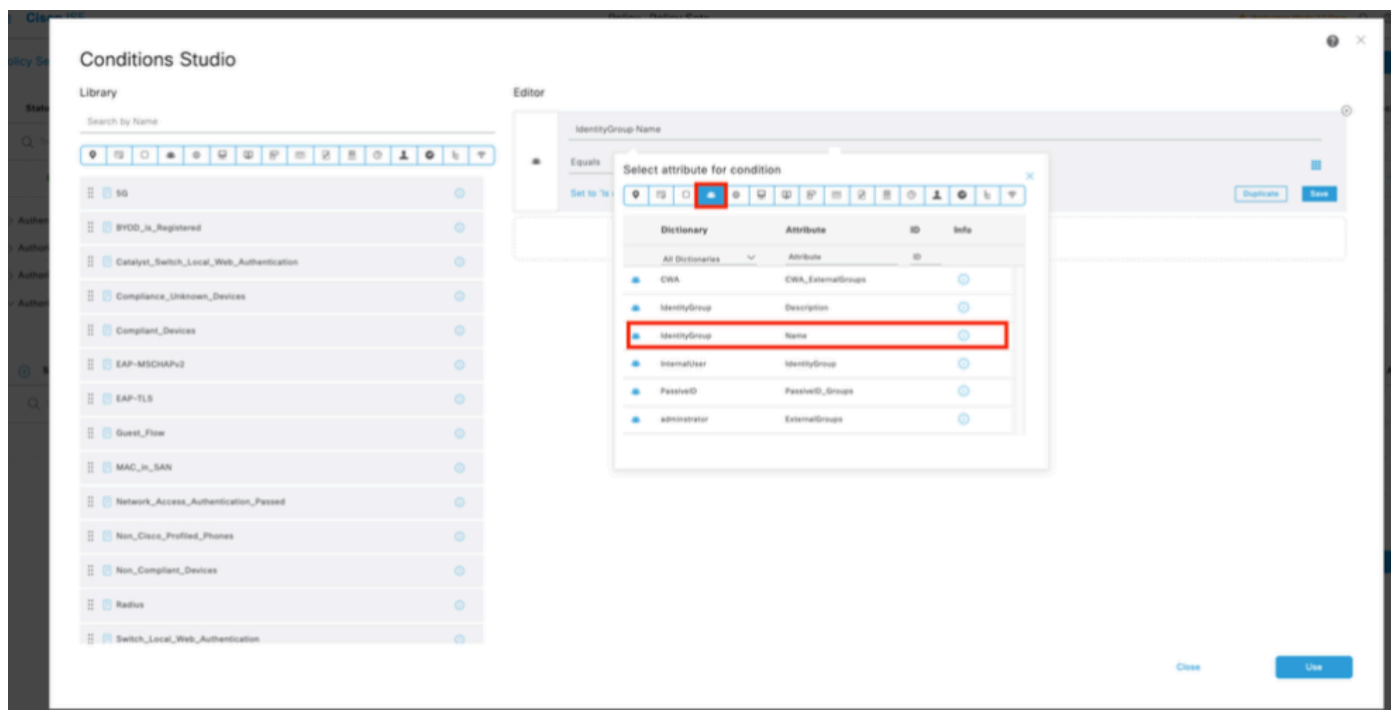
Fate clic sull'icona > posizionata alla fine della riga:



9.1 Espandere il menu Criteri di autorizzazione e fare clic su in (+) per aggiungere una nuova condizione.



9.2 Impostare le condizioni in modo che corrispondano al gruppo di identità del dizionario con nome attributo uguale a gruppi di identità utente: Arista_switch_Admin (nome del gruppo creato al passaggio 7) e fare clic su Usa.



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 Verificare che la nuova condizione sia configurata nel criterio di autorizzazione, quindi aggiungere un profilo utente in Profili:

Authorization Policy(2)

Status	Rule Name	Conditions	Results			
			Profiles	Security Groups	Hits	Actions
✓	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

Configurazione dello switch Arista

Passaggio 1. Abilitazione dell'autenticazione RADIUS

Accedere allo switch Arista e accedere alla modalità di configurazione:

configurazione

!

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

timeout radius-server 5

ritrasmissione radius-server 3

deadtime server radius 30

!

aaa group server radius ISE

server <ISE-IP>

!

aaa authentication login default group ISE local

aaa authorization exec default group ISE local

aaa accounting exec start-stop gruppo predefinito ISE

comandi di accounting aaa 15 gruppo start-stop predefinito ISE

aaa account system default start-stop group ISE

!

end

Passaggio 2. Salvataggio della configurazione

Per salvare in modo permanente le impostazioni dopo il riavvio:

memoria di scrittura

o

copy running-config startup-config

Verifica

Recensione ISE

1. Tentare di accedere allo switch Arista utilizzando le nuove credenziali Radius:

1.1 Passare a Operazioni > Raggio > Log attivi.

1.2 Le informazioni visualizzate indicano se l'accesso è riuscito.

Operations / RADIUS

Live Logs | Live Sessions

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	Details icon	4	diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 07:08:21.9...	Success	Details icon	1	diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 07:08:21.9...	Success	Details icon	1	diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 07:08:21.9...	Success	Details icon	1	diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic

2. Per lo stato di errore, esaminare i dettagli della sessione:

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

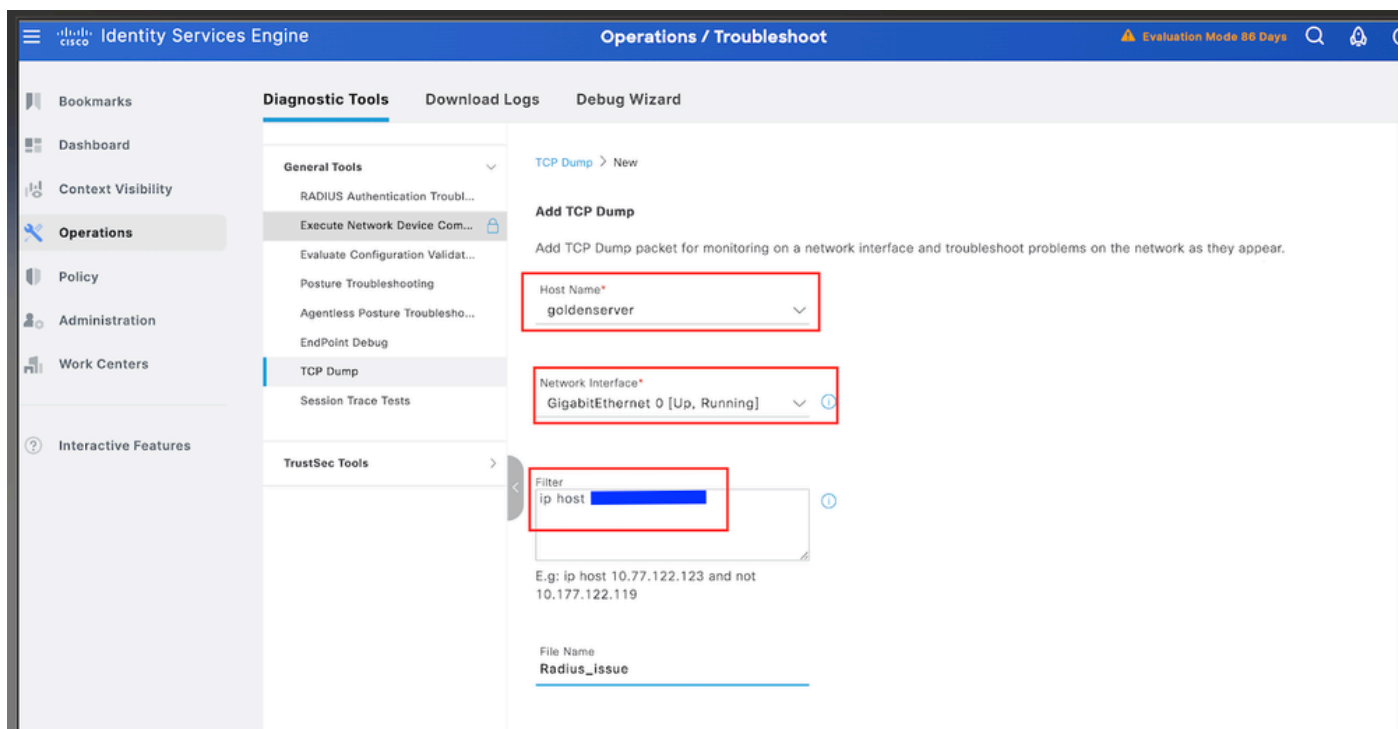
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 05:57:12.4...	Auth Failed	Details icon		diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 05:57:02.5...	Auth Failed	Details icon		diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 05:56:16.3...	Auth Failed	Details icon		diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic
Mar 18, 2025 05:56:08.0...	Auth Failed	Details icon		diviya	[Redacted]	Endpoint Pr	Authentication Polik	Authorization Pol	Authorizatic

3. Per le richieste non visualizzate nei log Radius Live , verificare se la richiesta UDP sta raggiungendo il nodo ISE tramite un'acquisizione di pacchetti.

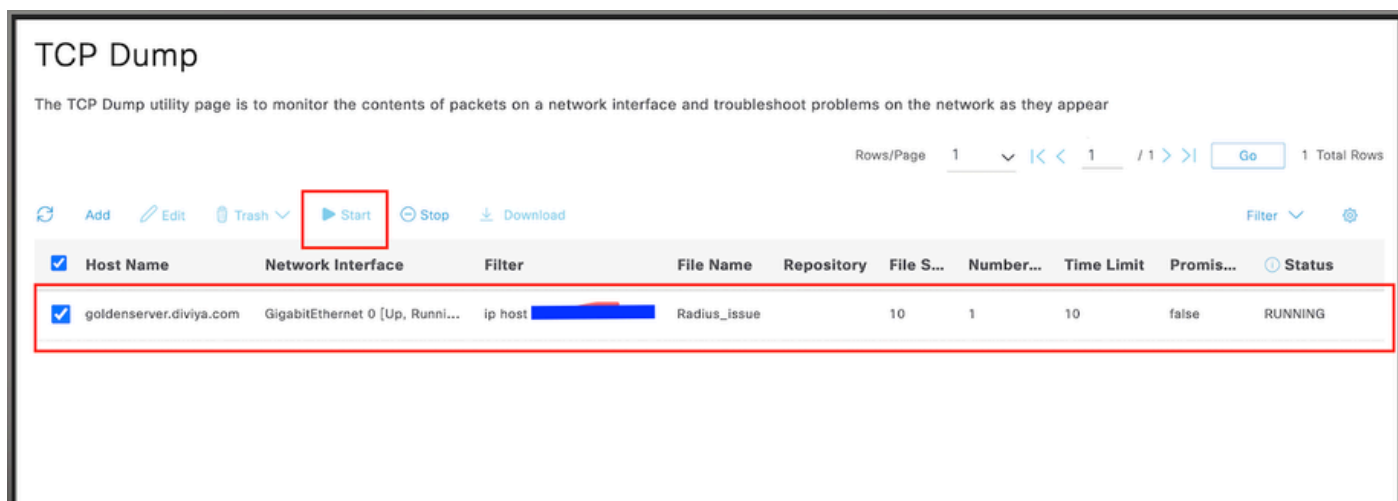
3.1. Passare a Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Dump TCP.

3.2. Aggiungere una nuova acquisizione e scaricare il file sul computer locale per verificare se i pacchetti UDP stanno arrivando al nodo ISE.

3.3. Inserire le informazioni richieste, scorrere verso il basso e fare clic su Salva.



3.4. Selezionare e avviare l'acquisizione.



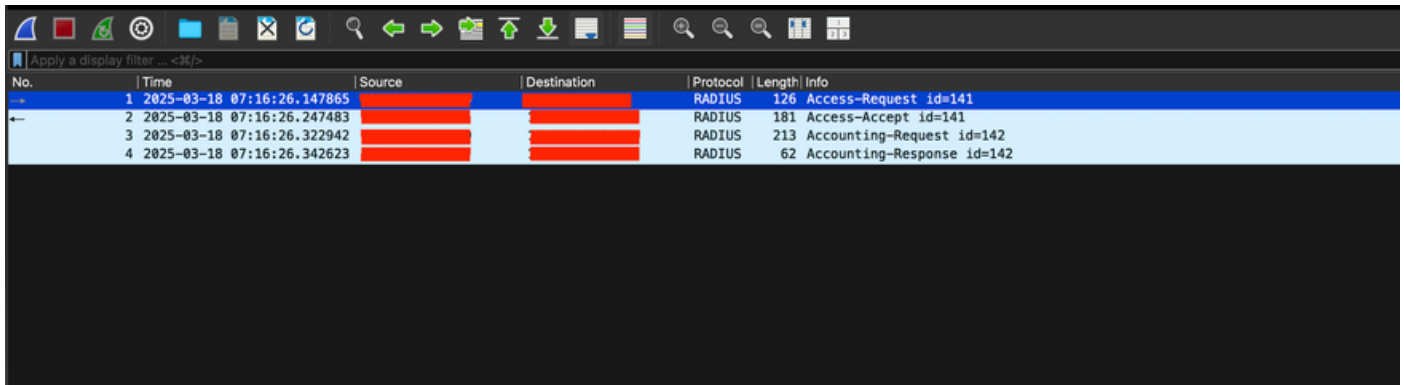
3.5. Tentativo di accedere allo switch Arista mentre l'acquisizione ISE è in esecuzione.

3.6. Arrestare il dump TCP in ISE e scaricare il file su un computer locale.

3.7. Esaminare l'output del traffico.

Output previsto:

Pacchetto n. 1. Richiesta dallo switch Arista al server ISE tramite la porta 1812 (RADIUS).
Pacchetto n. 2. Il server ISE risponde accettando la richiesta iniziale.



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

Risoluzione dei problemi

Scenario 1. "Richiesta RADIUS 5405 ignorata"

Problema

In questo scenario viene descritto come risolvere l'errore "Richiesta RADIUS 5405 ignorata" e il motivo per cui "Impossibile individuare il dispositivo di rete o il client AAA" in Cisco ISE (ad esempio, uno switch Arista) durante il tentativo di autenticazione da parte di un dispositivo di rete.

Possibili cause

- Cisco Identity Services Engine (ISE) non è in grado di identificare lo switch Arista perché il relativo indirizzo IP non è elencato tra i dispositivi di rete noti.
- La richiesta RADIUS proviene da un indirizzo IP che ISE non riconosce come dispositivo di rete o client AAA valido.
- Potrebbe essersi verificata una mancata corrispondenza nella configurazione tra lo switch e l'ISE (ad esempio, un IP errato o un segreto condiviso).

Soluzione

- Aggiungere lo switch all'elenco di dispositivi di rete Cisco ISE con l'indirizzo IP corretto.
- Verificare che l'indirizzo IP e il segreto condiviso configurati in ISE corrispondano esattamente a quello impostato sullo switch.
- Una volta corretta, la richiesta RADIUS deve essere riconosciuta ed elaborata correttamente.

Scenario 2: errore dello switch Arista nel failover sul backup del PSN di ISE

Problema

Uno switch Arista è configurato per l'utilizzo di Cisco ISE per l'autenticazione RADIUS. Quando il

PSN (Policy Service Node) principale di ISE non è più disponibile, lo switch non esegue automaticamente il failover su un PSN di backup. Di conseguenza, i log di autenticazione vengono visualizzati solo dal PSN ISE primario e non esistono log dal PSN secondario/di backup quando il PSN primario non è attivo.

Possibili cause

- La configurazione del server RADIUS dello switch Arista punta solo al nodo ISE primario, pertanto non vengono utilizzati server di backup.
- Priorità del server RADIUS non impostata correttamente o IP di backup ISE mancante dalla configurazione.
- Le impostazioni di timeout e ritrasmissione sullo switch sono impostate su un valore troppo basso. Ciò impedisce il corretto fallback al PSN di backup.
- Lo switch utilizza un FQDN per il PSN, ma la risoluzione DNS non restituisce tutti i record A, causando il contatto solo con il server primario.

Soluzione

- Verificare che nella configurazione del gruppo di server RADIUS dello switch siano stati immessi più IP ISE PSN. In questo modo, lo switch può utilizzare il numero di serie del servizio (PSN) ISE di backup se il server primario non è raggiungibile.

Esempio di configurazione:

```
chiave <ISE1-IP> host radius-server <secret>
```

```
chiave <ISE2-IP> host radius-server <secret>
```

- Verificare che i valori di priorità, timeout e ritrasmissione del server RADIUS siano configurati correttamente per un failover affidabile.
- Se si utilizzano FQDN, controllare le impostazioni DNS e la risoluzione per verificare che tutti gli indirizzi IP dei nomi di dominio primario (PSN) vengano restituiti e utilizzati dallo switch.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).