Configurazione dell'autenticazione TACACS+ sullo switch Arista con ISE

Sommario

Introduzione

In questo documento viene descritto come integrare Cisco ISE TACACS+ con uno switch Arista per un accesso AAA centralizzato di amministratore.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo Cisco ISE e TACACS+.
- Switch Arista

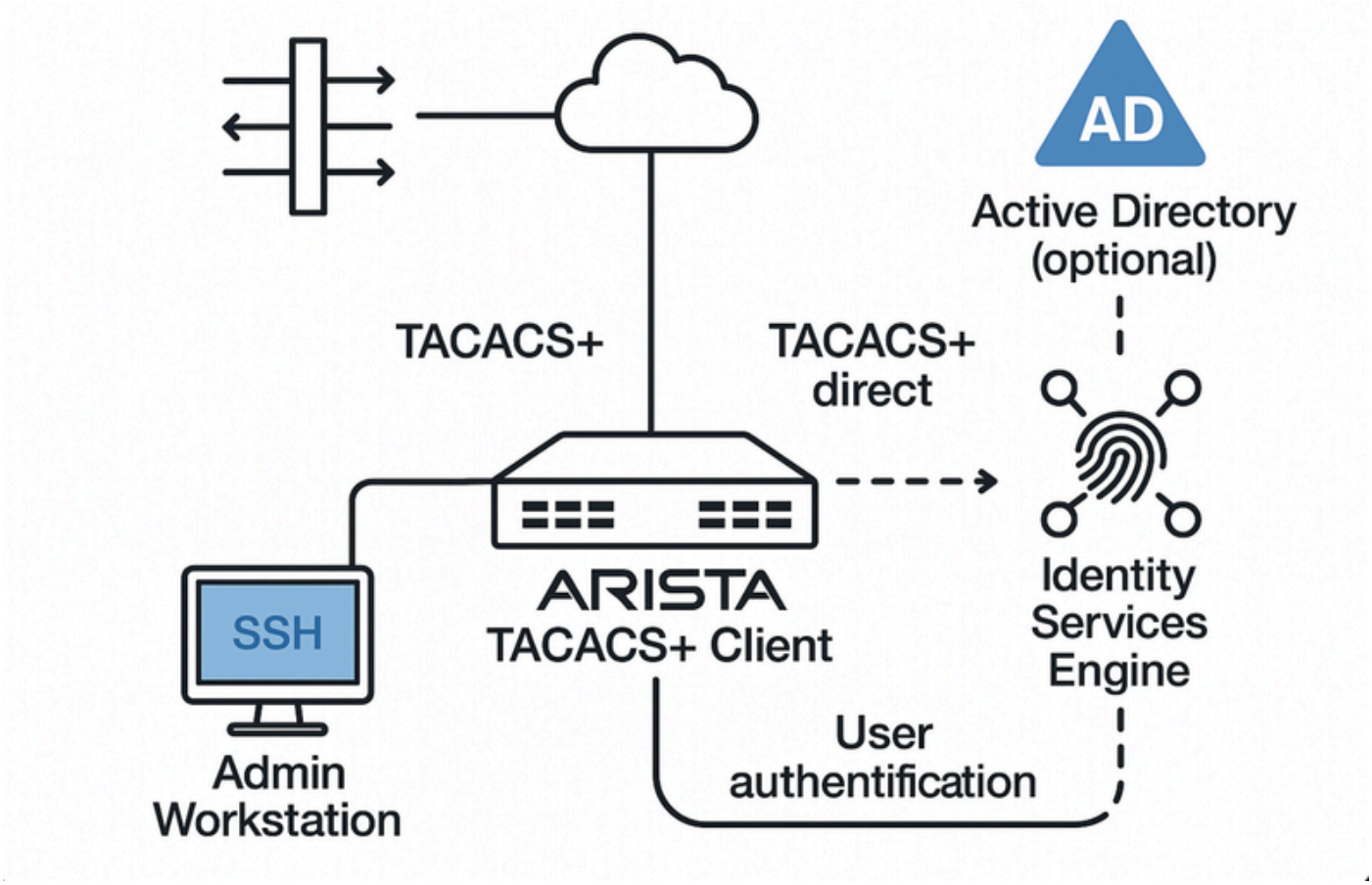
Componenti usati

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

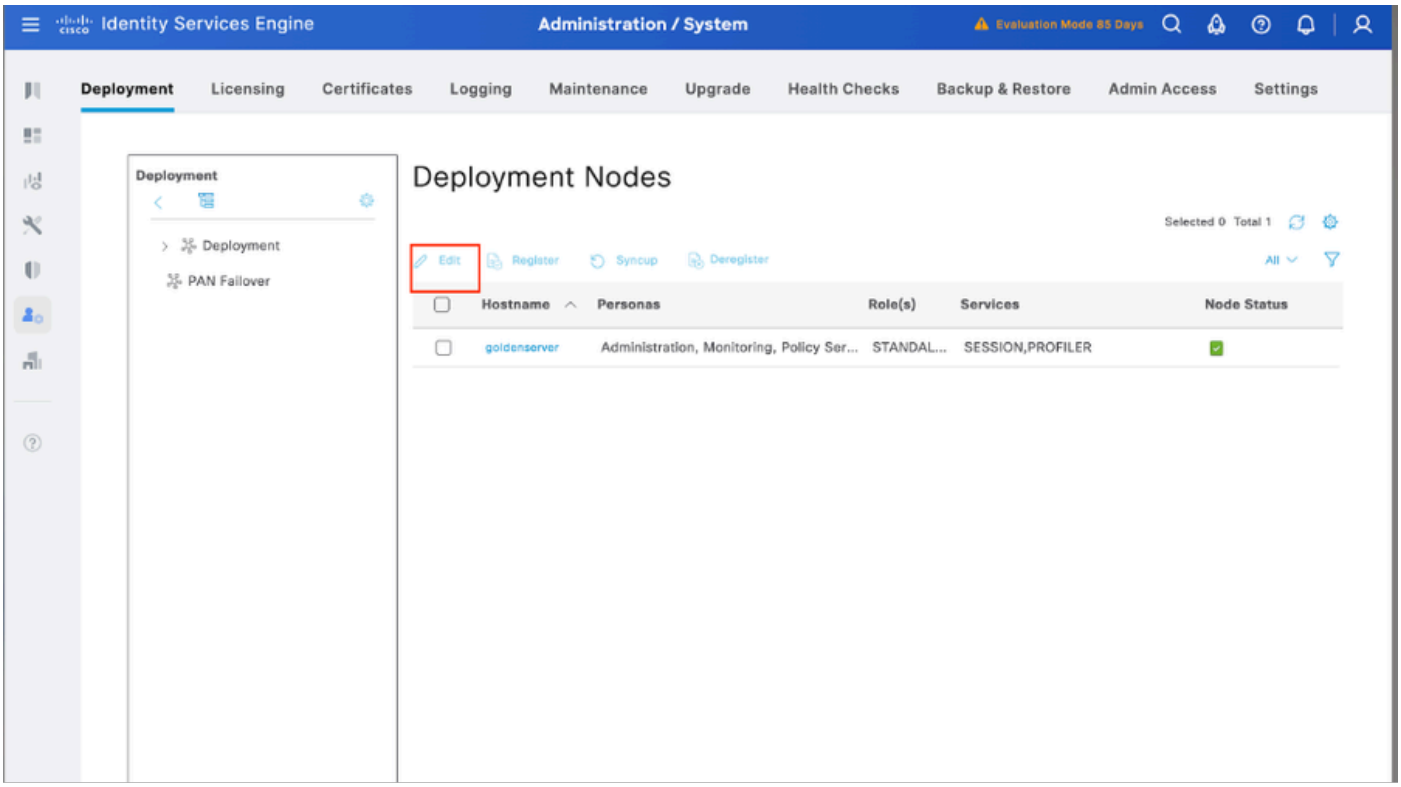


Configurazioni

Configurazione TACACS+ su ISE

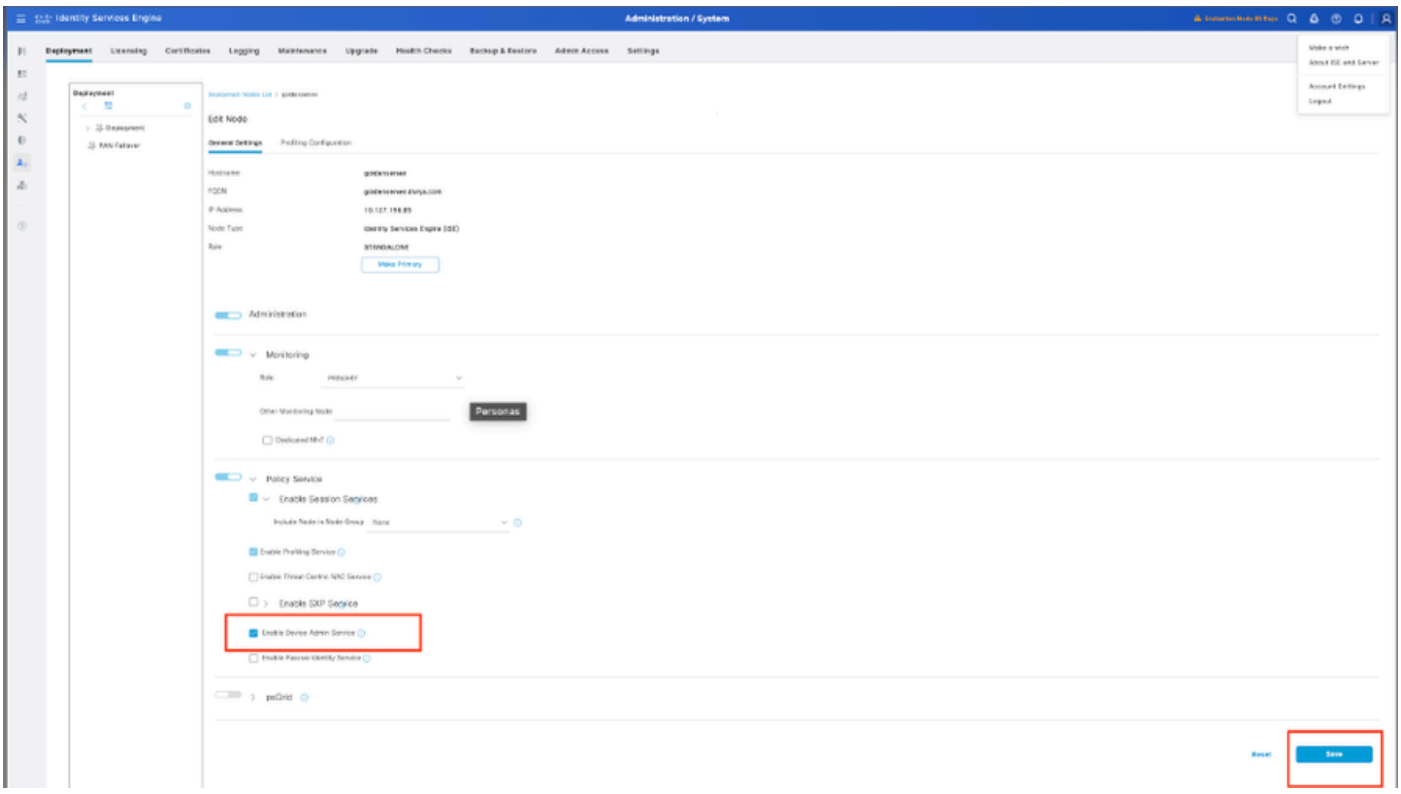
Passaggio 1. Il passaggio iniziale consiste nel verificare se Cisco ISE dispone delle funzionalità necessarie per gestire l'autenticazione TACACS+. A tale scopo, verificare che nel nodo PSN (Policy Service Node) desiderato sia attivata la funzionalità Servizio amministrazione dispositivi.

Passare a Amministrazione > Sistema > Distribuzione, selezionare il nodo appropriato in cui ISE elabora l'autenticazione TACACS+ e fare clic su Modifica per rivedere la configurazione.



Passaggio 2. Scorrere verso il basso per individuare la funzionalità Servizio di amministrazione del dispositivo. Notare che l'abilitazione di questa funzionalità richiede che la persona del servizio criteri sia attiva sul nodo, insieme alle licenze TACACS+ disponibili nella distribuzione.

Selezionare la casella di controllo per abilitare la funzionalità, quindi salvare la configurazione.

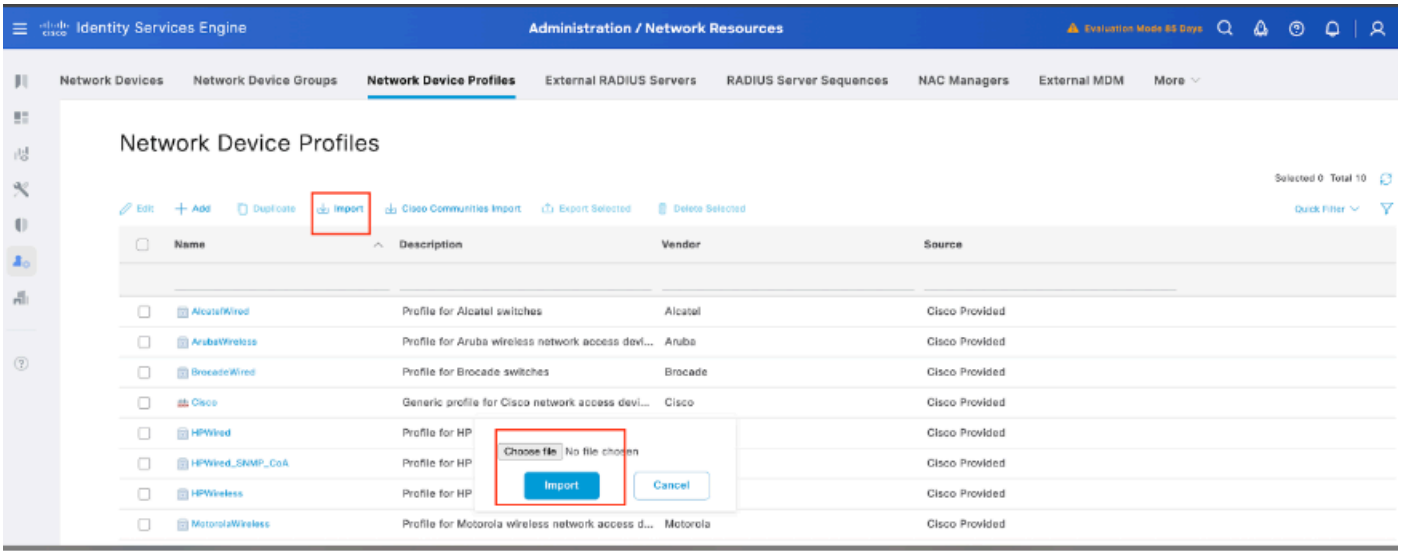


Passaggio 3. Come ottenere il profilo del dispositivo di rete Arista per Cisco ISE.

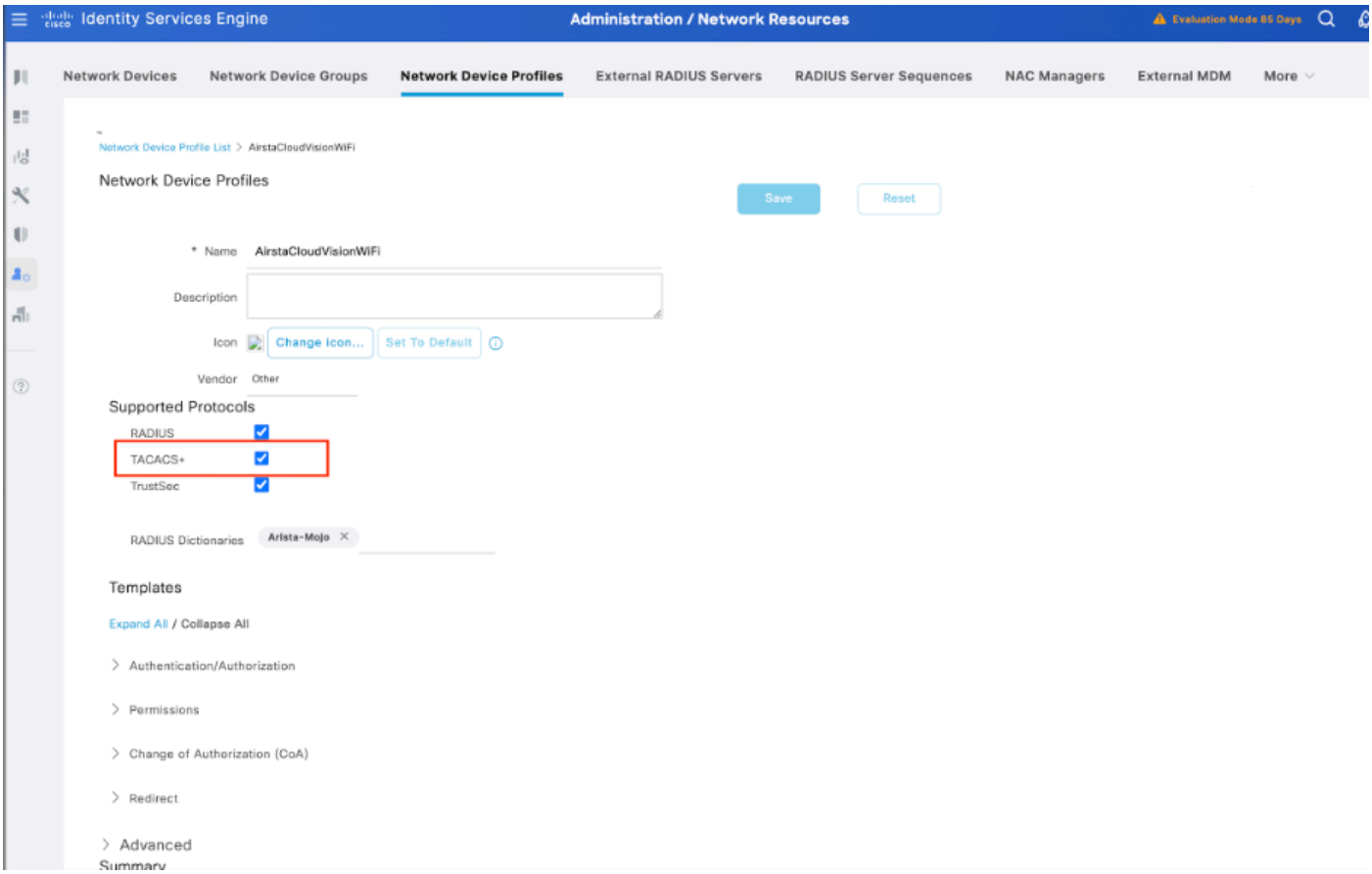
La Cisco Community ha condiviso un profilo NAD dedicato per i dispositivi Arista. Questo profilo, insieme ai file del dizionario necessari, è disponibile nell'articolo Arista CloudVision WiFi Dictionary e NAD Profile for ISE Integration. Il download e l'importazione di questo profilo nella configurazione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

Procedura per importare il profilo Arista e AD in Cisco ISE:

1. Scarica il profilo:
    - Ottenere il profilo Arista NAD 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.

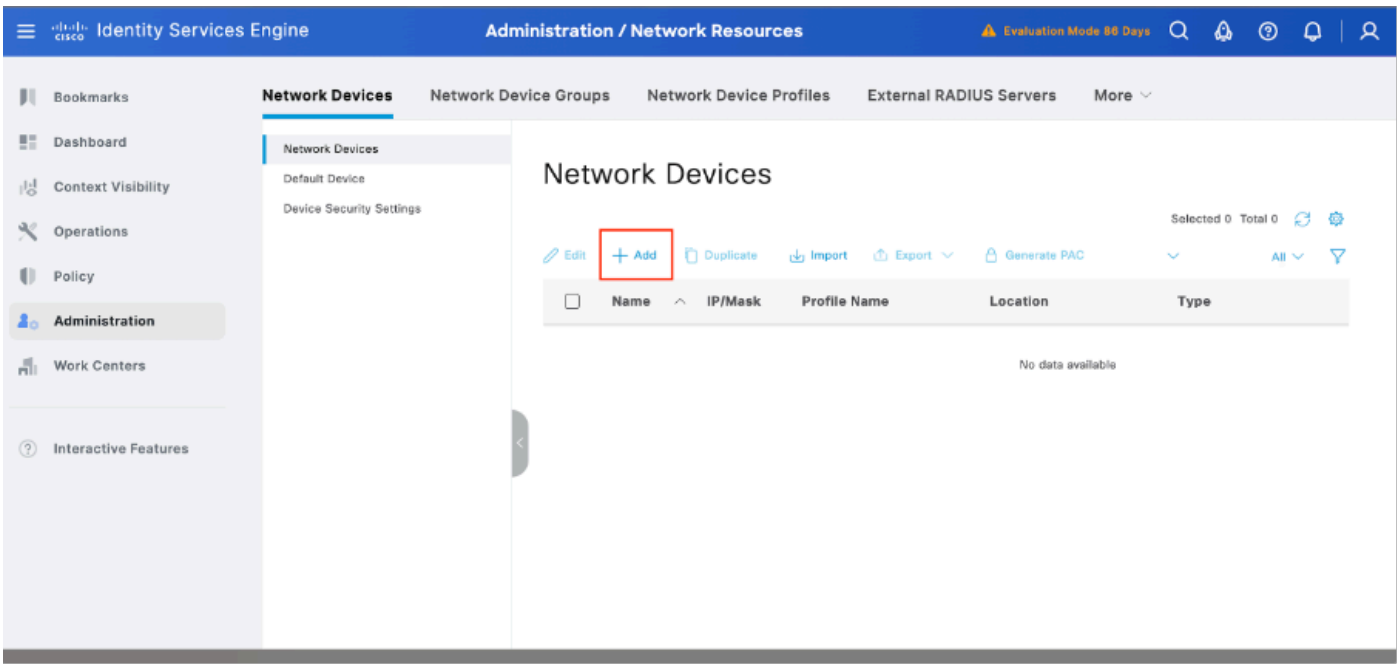


Al termine del caricamento, accedere all'opzione Edit e abilitare TACACS+ come protocollo supportato.



Passaggio 2: Aggiungere lo switch Arista come dispositivo di rete.

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

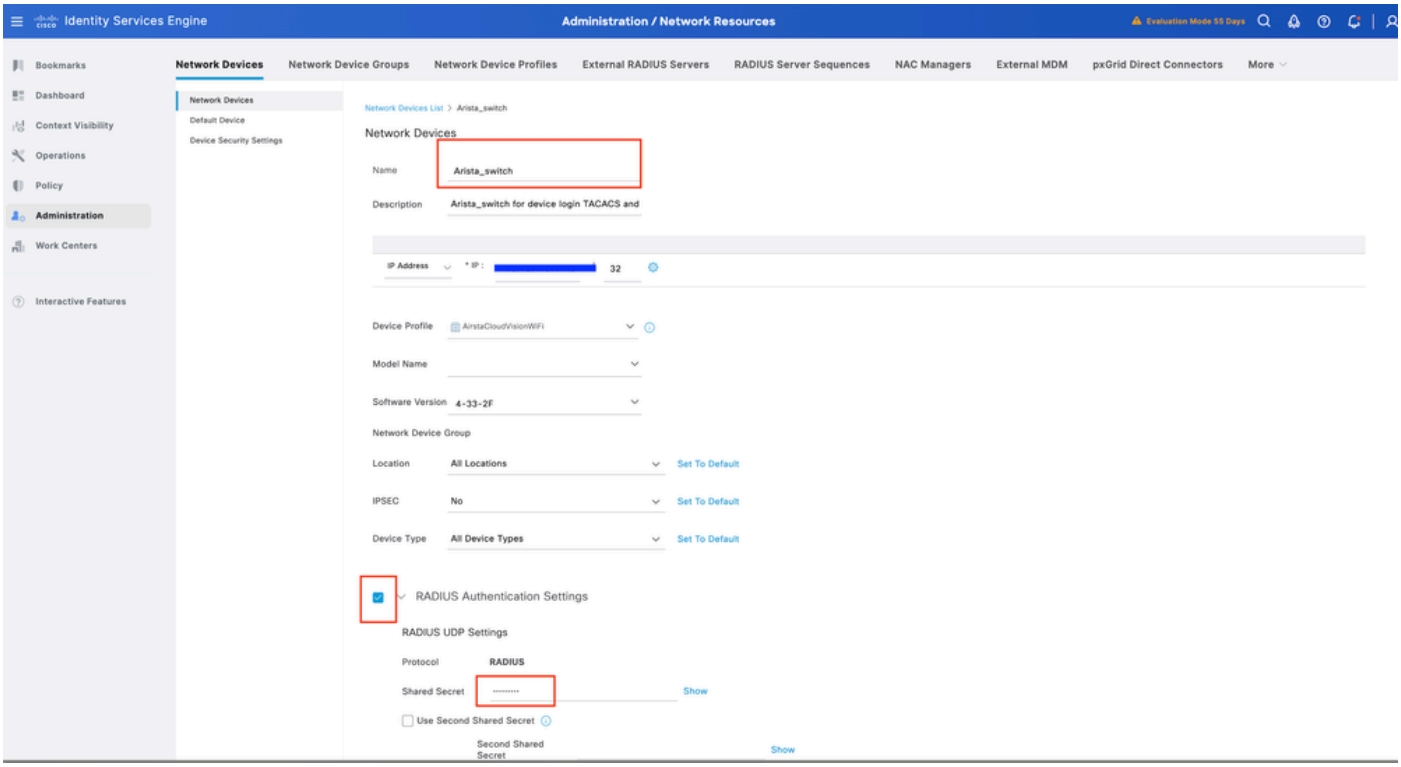


2. Fare clic su Add (Aggiungi) e inserire i seguenti dati:

- Indirizzo IP: <IP switch>
- Tipo di dispositivo: Scegli altro cablato
- Profilo dispositivo di rete: selezionare AirstaCloudVisionWiFi.

- Impostazioni autenticazione RADIUS:
  - Abilita autenticazione RADIUS.
  - Immettere il segreto condiviso (deve corrispondere alla configurazione dello switch).

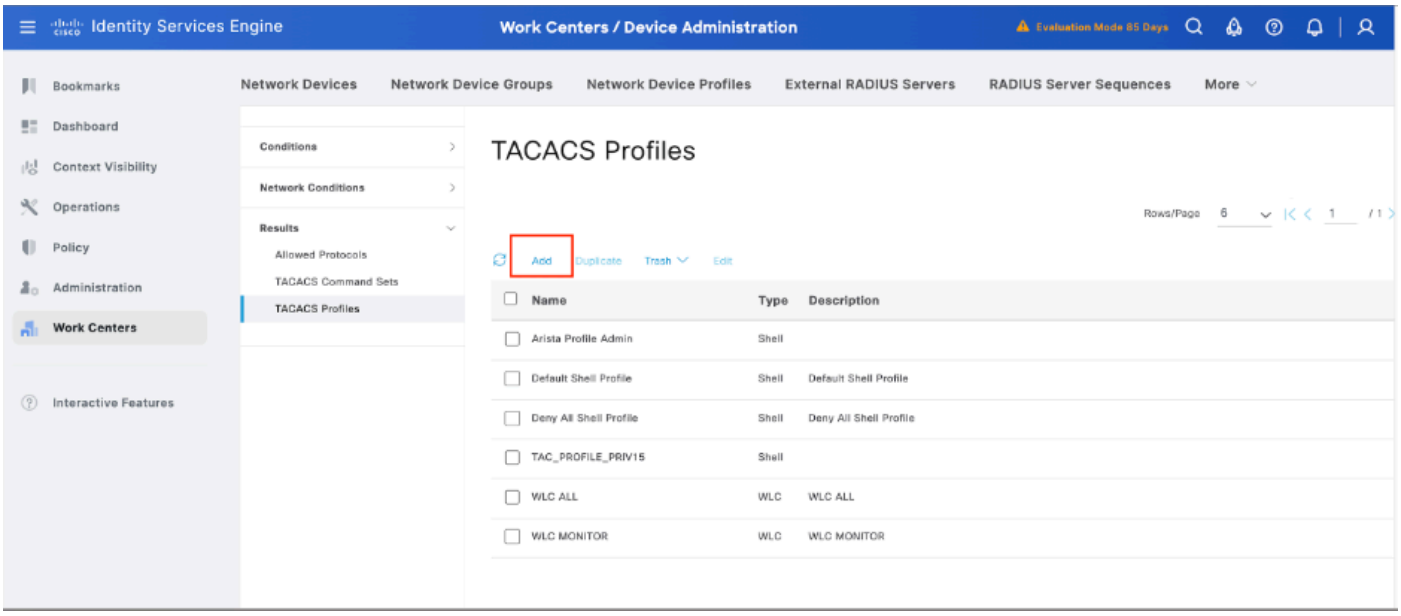
3. Fare clic su Salva:



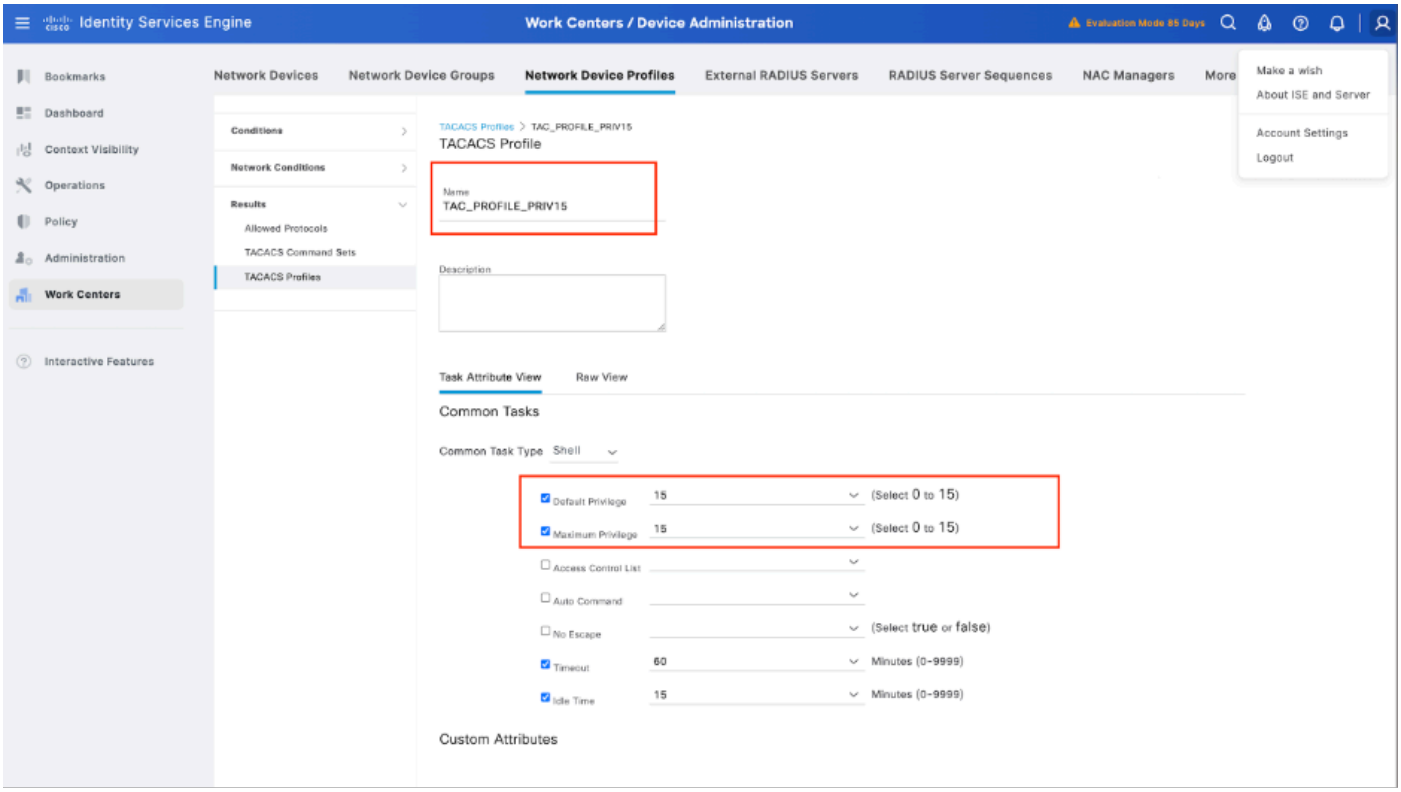
Passaggio 3. Verificare che il nuovo dispositivo sia visualizzato in Dispositivi di rete:

Passaggio 4. Configurare il profilo TACACS.

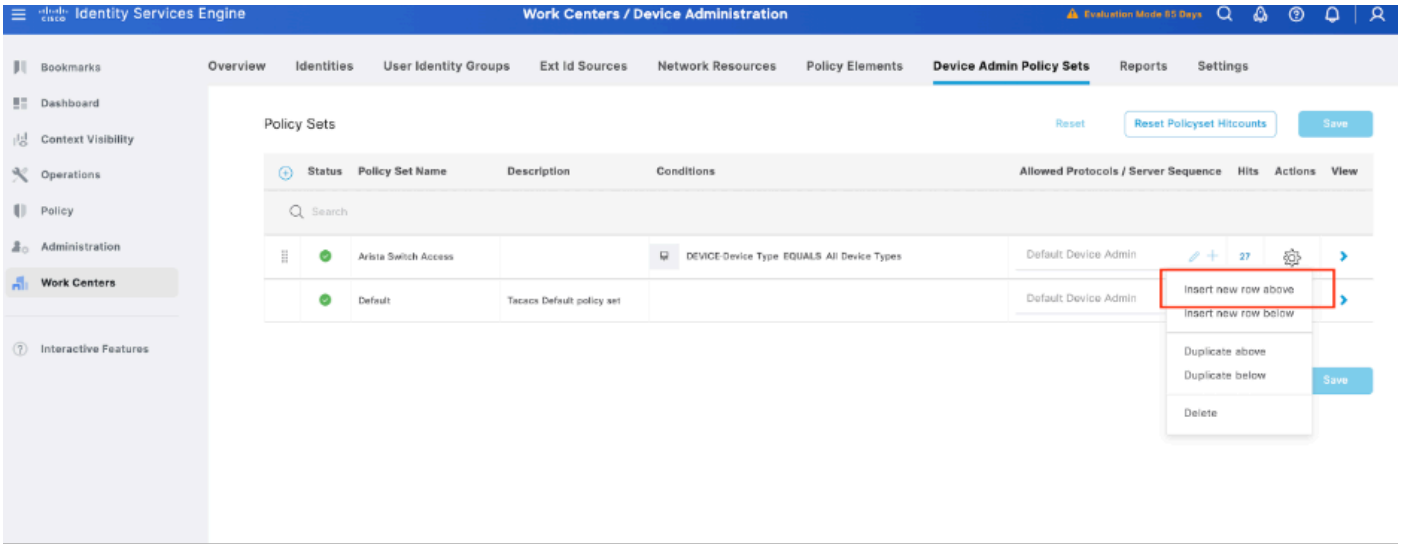
Creare un profilo TACACS, selezionare il menu Work Center > Device Administration > Policy Elements > Results > TACACS Profiles, quindi selezionare Add:



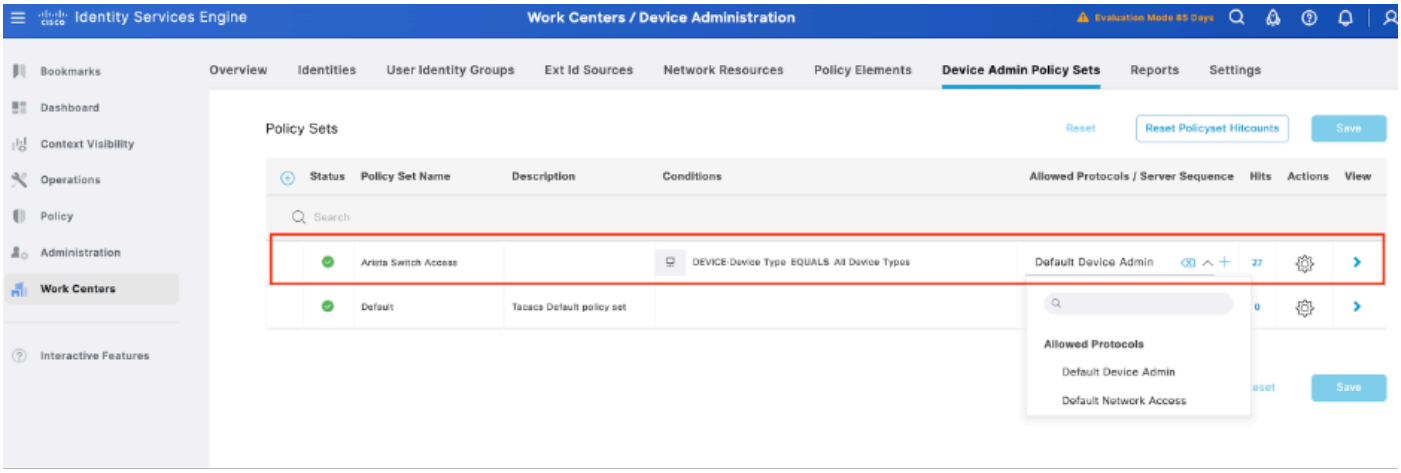
Immettere un nome, selezionare la casella di controllo Privilegio predefinito e impostare il valore su 15. Selezionare inoltre Privilegio massimo, impostarne il valore su 15 e fare clic su Sottometti:



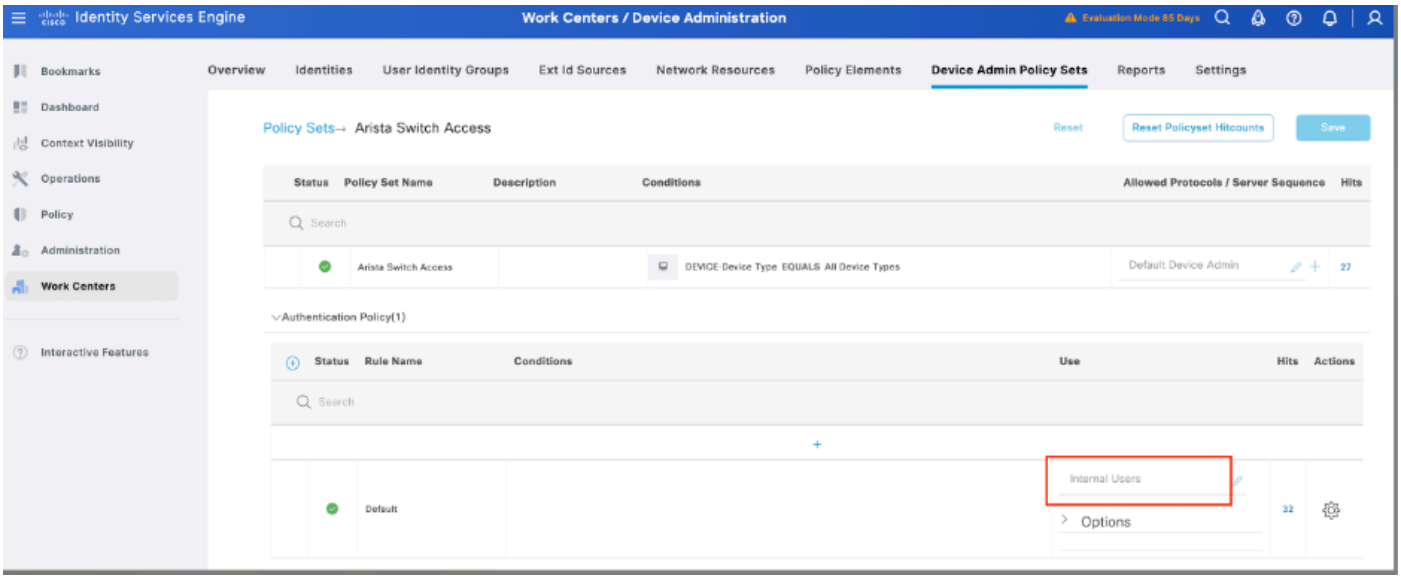
Passaggio 5. Creare un set di criteri di amministrazione del dispositivo da utilizzare per lo switch Arista, selezionare il menu Work Center > Device Administration > Device Admin Policy Sets, quindi selezionare l'icona del dispositivo da inserire nella riga precedente da un set di criteri esistente.



Passaggio 6. Assegnare un nome al nuovo set di criteri, aggiungere le condizioni in base alle caratteristiche delle autenticazioni TACACS+ in corso sullo switch Arista e selezionare Protocolli consentiti > Amministrazione predefinita dispositivi, quindi salvare la configurazione.

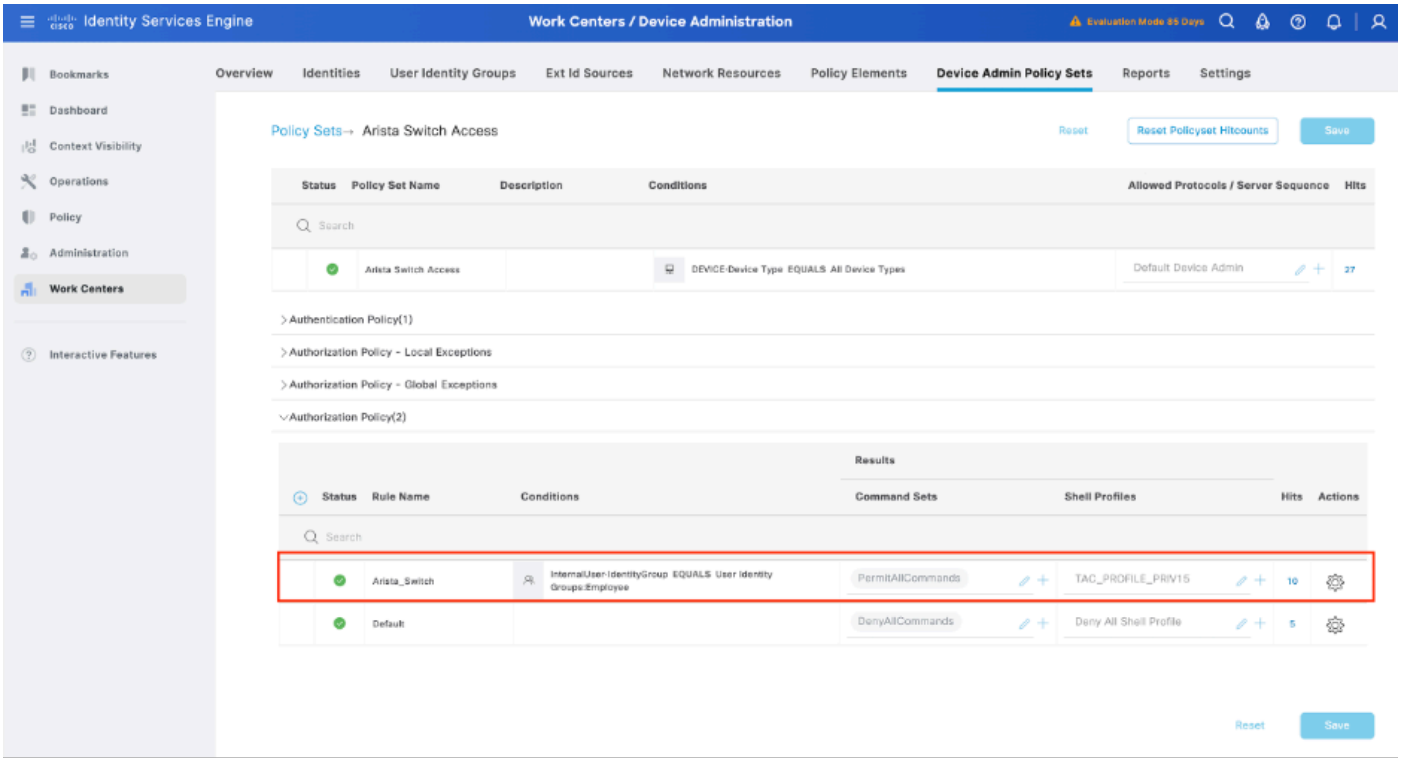


Passaggio 7. Selezionare nell'opzione > view, quindi nella sezione Authentication Policy (Criteri di autenticazione) selezionare l'origine identità esterna utilizzata da Cisco ISE per eseguire la query del nome utente e delle credenziali per l'autenticazione sullo switch Arista. Nell'esempio, le credenziali corrispondono a Internal Users memorizzato in ISE.



Passaggio 8. Scorrere verso il basso fino a visualizzare la sezione Criteri di autorizzazione relativa ai criteri predefiniti, selezionare l'icona dell'ingranaggio, quindi inserire una regola.

Passaggio 9. Assegnare un nome alla nuova regola di autorizzazione, aggiungere le condizioni relative all'utente già autenticato come appartenenza al gruppo e, nella sezione Profili shell, aggiungere il profilo TACACS configurato in precedenza e salvare la configurazione.



Configurazione switch Arista

Passaggio 1. Abilitare l'autenticazione TACACS+

Accedere allo switch Arista e accedere alla modalità di configurazione:

configurazione

!

tacacs-server host <ISE-IP> chiave <TACACS-SECRET>

!

acs server di gruppo aaa+ ISE_TACACS

  server <ISE-IP>

!

aaa authentication login default group ISE_TACACS local

aaa authorization exec default group ISE_TACACS local

comandi di accounting aaa 15 gruppo start-stop predefinito ISE_TACACS

!

End

Passaggio 2. Salvataggio della configurazione

Per salvare in modo permanente la configurazione dopo il riavvio:

scrittura di memoria

O

copy running-config startup-config

Verifica

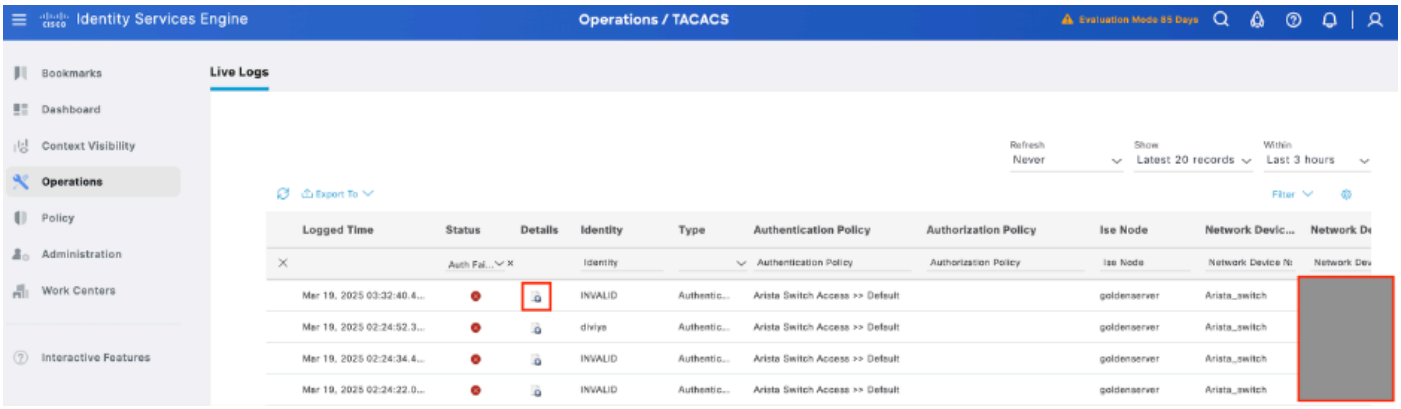
Recensione ISE

Passaggio 1. Verificare che il servizio TACACS+ sia in esecuzione e che sia possibile archiviarlo:

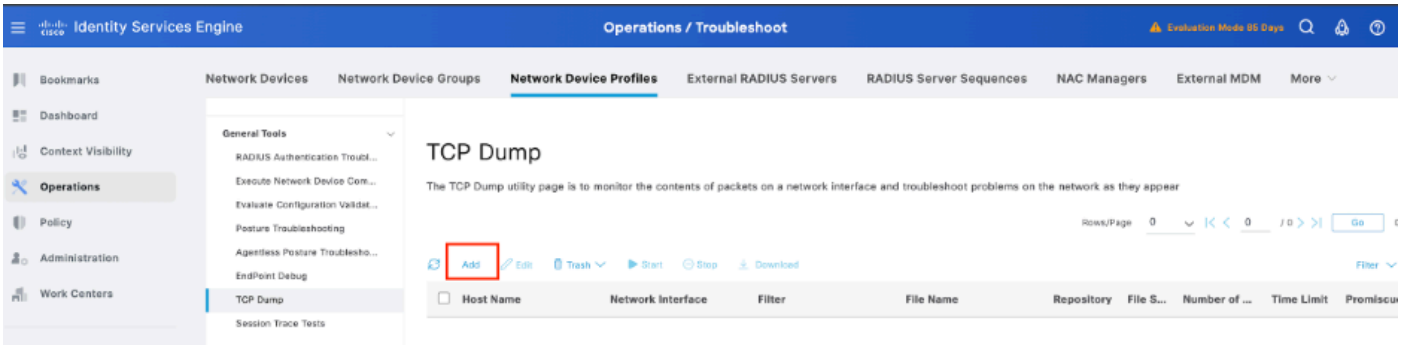
- GUI: Verificare se il nodo è elencato con il servizio DEVICE ADMIN in > Sistema > Distribuzione.
- CLI: Eseguire il comando show ports | includere 49 per confermare che la porta TCP contiene connessioni che appartengono a TACACS+

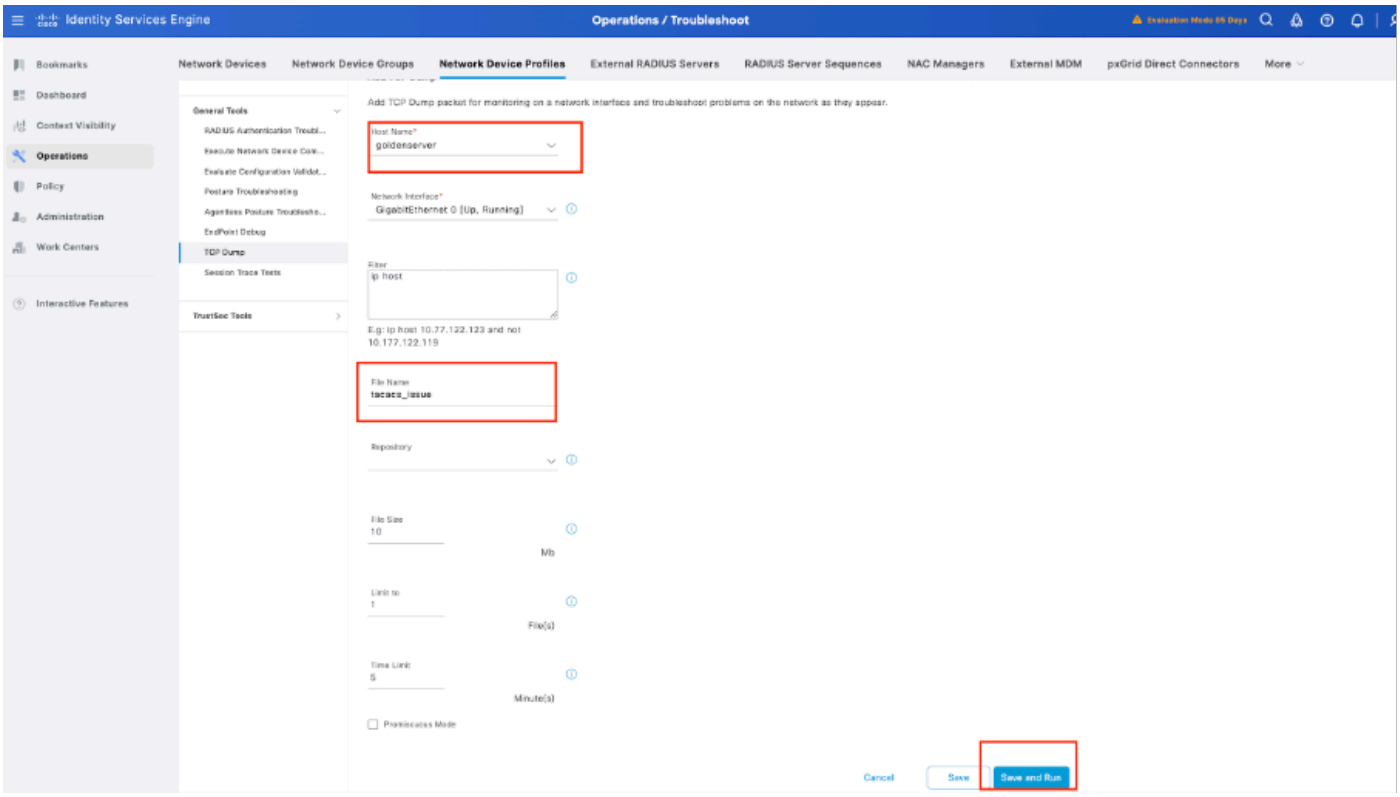
Passaggio 2. Conferma se sono presenti livellog relativi ai tentativi di autenticazione TACACS+: è possibile selezionare questa opzione nel menu Operazioni > TACACS > Live logs,

A seconda del motivo dell'errore, è possibile modificare la configurazione o risolvere la causa dell'errore.



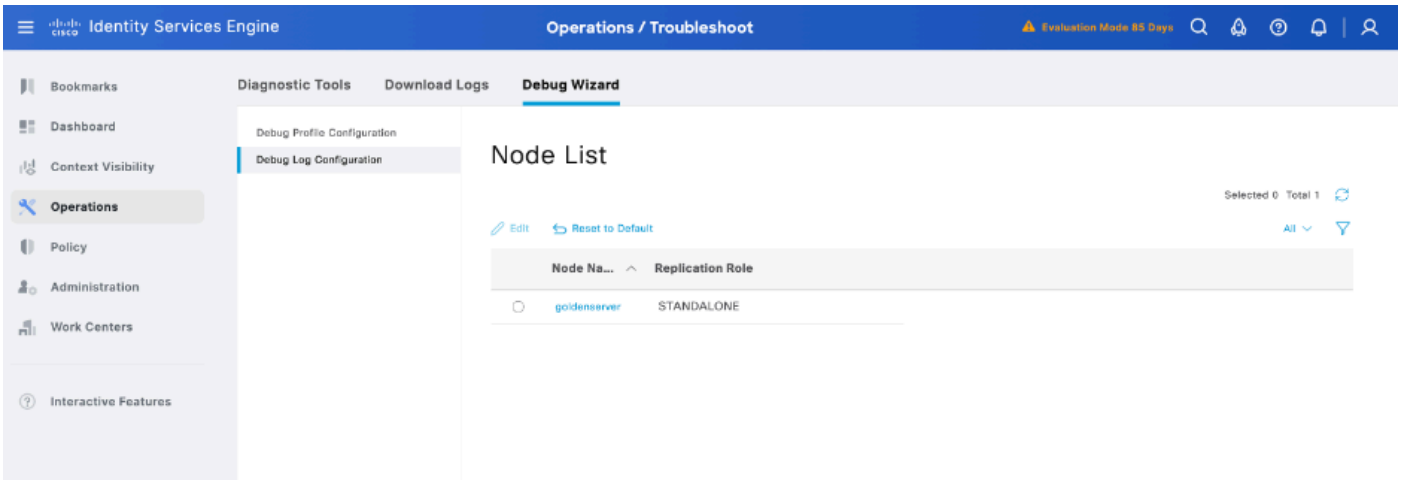
Passaggio 3. Se non viene visualizzato alcun catalogo, procedere all'acquisizione di un pacchetto. Passare al menu Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > TCP Dump , selezionare Aggiungi:

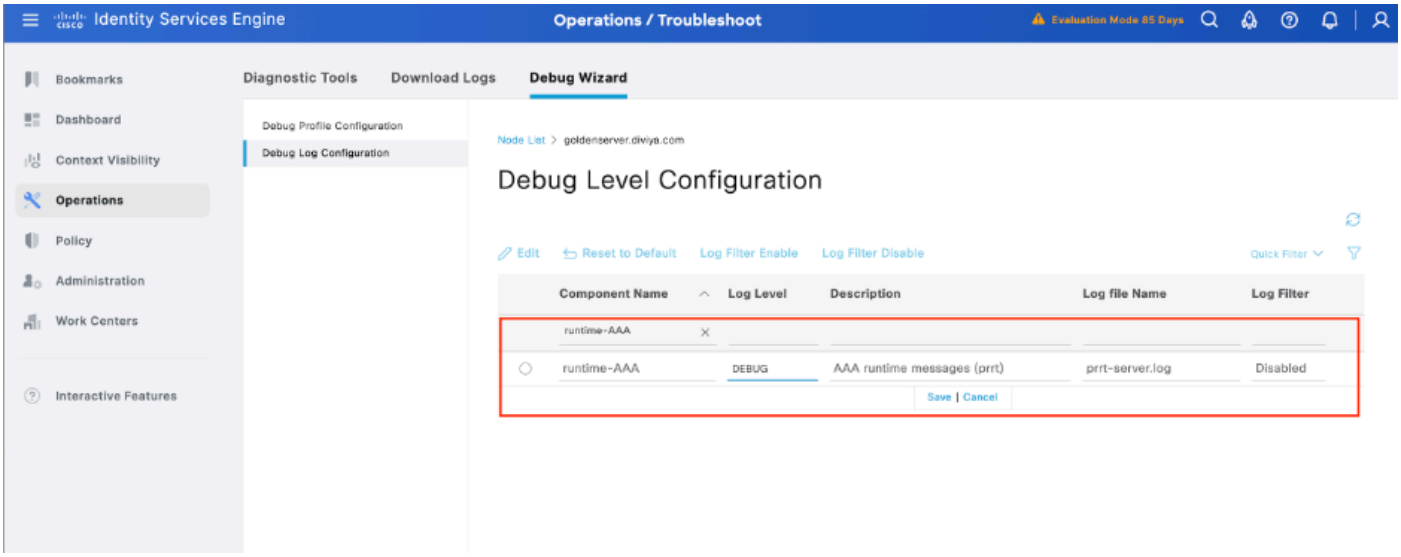




Passaggio 4. Abilitare il componente runtime-AAA nel debug nel PSN da cui viene eseguita

l'autenticazione in Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug, selezionare il nodo PSN, quindi selezionare il pulsante Modifica:





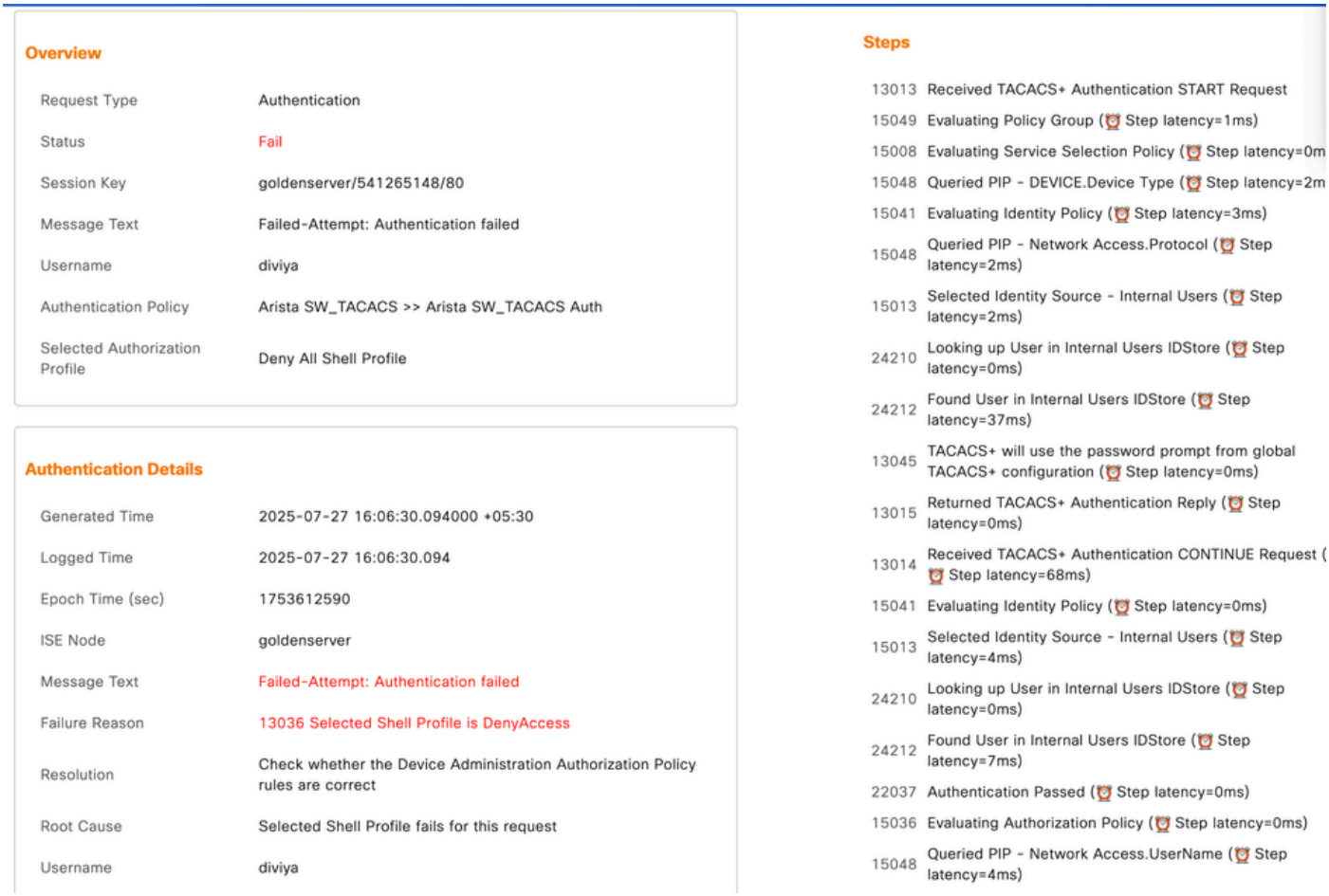
Identificare il componente runtime-AAA, impostarne il livello di log per eseguire il debug, riprodurre il problema e analizzare i log per ulteriori informazioni.

Risoluzione dei problemi

Problema 1

L'autenticazione TACACS+ tra Cisco ISE e lo switch Arista (o un dispositivo di rete) non riesce con il messaggio di errore:

"13036 Selected Shell Profile is DenyAccess"



L'errore "13036 Selected Shell Profile is DenyAccess" in Cisco ISE in genere indica che, durante un tentativo di amministrazione di un dispositivo TACACS+, i criteri di autorizzazione corrispondono a un profilo della shell impostato su DenyAccess. Ciò non è in genere il risultato di un profilo della shell non configurato correttamente, ma indica piuttosto che nessuna delle regole di autorizzazione configurate corrisponde agli attributi utente in ingresso (ad esempio, appartenenza a gruppi, tipo di dispositivo o posizione). Di conseguenza, ISE torna a una regola predefinita o a una regola di negazione esplicita, che determina il rifiuto dell'accesso.

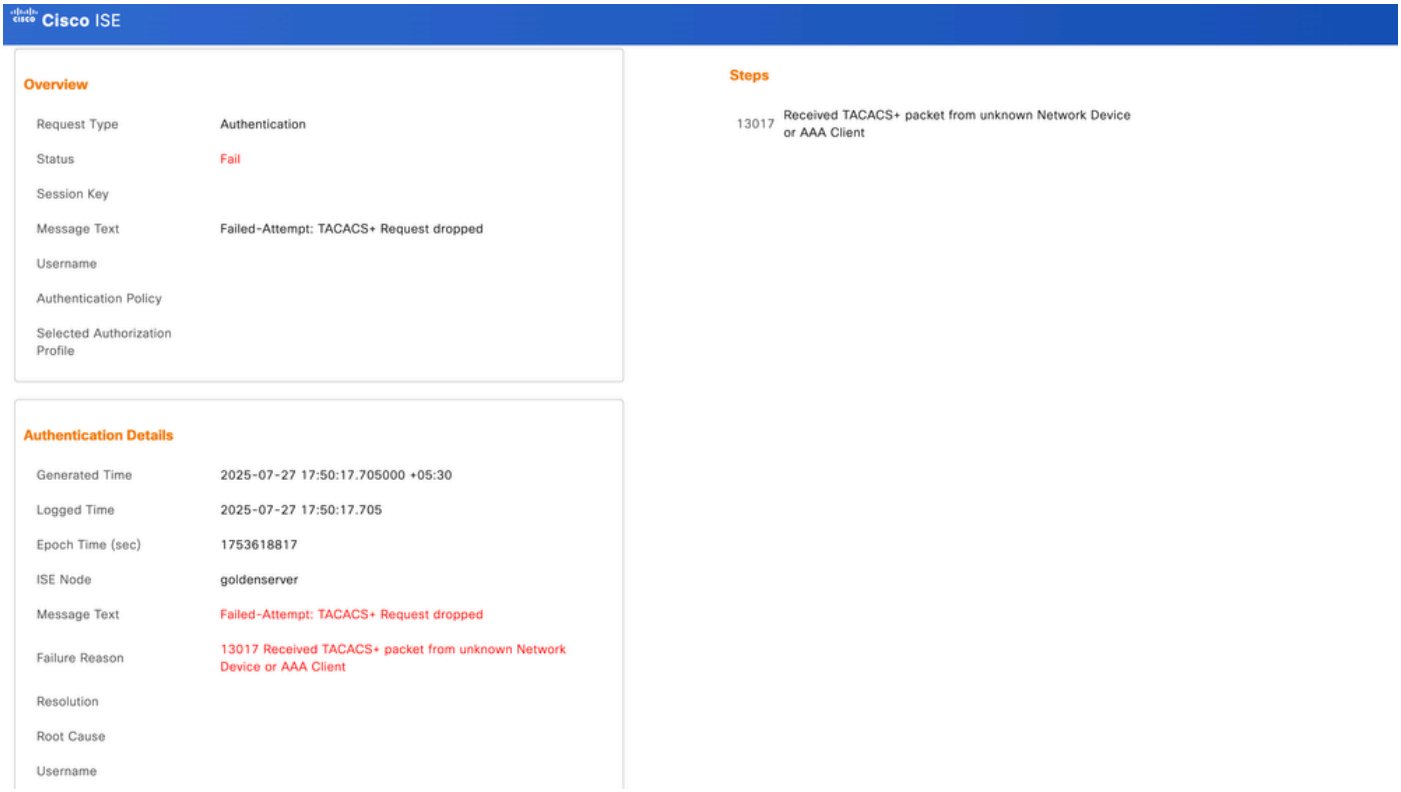
Possibili cause

- Rivedere le regole dei criteri di autorizzazione in ISE. Verificare che l'utente o il dispositivo corrisponda alla regola corretta che assegna il profilo di shell desiderato, ad esempio quella che consente l'accesso appropriato.
- Verificare che il mapping AD o del gruppo di utenti interno sia corretto e che le condizioni dei criteri, ad esempio l'appartenenza al gruppo di utenti, il tipo di dispositivo e il protocollo, siano specificate correttamente.
- Usare i log live ISE e i dettagli del tentativo non riuscito di vedere esattamente quale regola corrisponde e perché.

Problema 2

L'autenticazione TACACS+ tra Cisco ISE e lo switch Arista (o un dispositivo di rete) non riesce con il messaggio di errore:

"13017: ricevuto pacchetto TACACS+ da dispositivo di rete o client AAA sconosciuto"



Possibili cause

- Il motivo più comune è che l'indirizzo IP dello switch non viene aggiunto come dispositivo di rete in ISE (in Amministrazione > Risorse di rete > Dispositivi di rete).
- Verificare che l'indirizzo IP o l'intervallo corrisponda esattamente all'indirizzo IP di origine usato dallo switch Arista per inviare i pacchetti TACACS+.
- Se lo switch usa un'interfaccia di gestione, verificare che l'IP esatto (non solo una subnet/intervallo) sia stato aggiunto in ISE.

Soluzione

- Selezionare Amministrazione > Risorse di rete > Dispositivi di rete nella GUI di ISE.
- Verificare che l'indirizzo IP di origine esatto sullo switch Arista sia in uso per la comunicazione TACACS+ (molto spesso l'IP dell'interfaccia di gestione).
- Specificare il segreto condiviso (deve corrispondere a quello impostato sullo switch Arista).

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).