Konfigurieren der TACACS+-Authentifizierung auf einem Arista-Switch mit der ISE

Inhalt

- Einleitung
- Voraussetzungen
- Verwendete Komponenten
- Netzwerkdiagramm
- Konfigurationen
  - TACACS+-Konfiguration auf der ISE
  - Arista-Switch konfigurieren
    - Schritt 1: Aktivieren der TACACS+-Authentifizierung
    - Schritt 2: Speichern der Konfiguration
- Überprüfung
  - ISE-Prüfung
- Fehlerbehebung
  - Problem 1
    - Mögliche Ursachen
  - Problem 2
    - Mögliche Ursachen
    - Lösung

Einleitung

In diesem Dokument wird die Integration von Cisco ISE TACACS+ mit einem Arista-Switch für zentrales AAA-Management des Administratorzugriffs beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ISE und TACACS+-Protokoll.
- Arista Switches

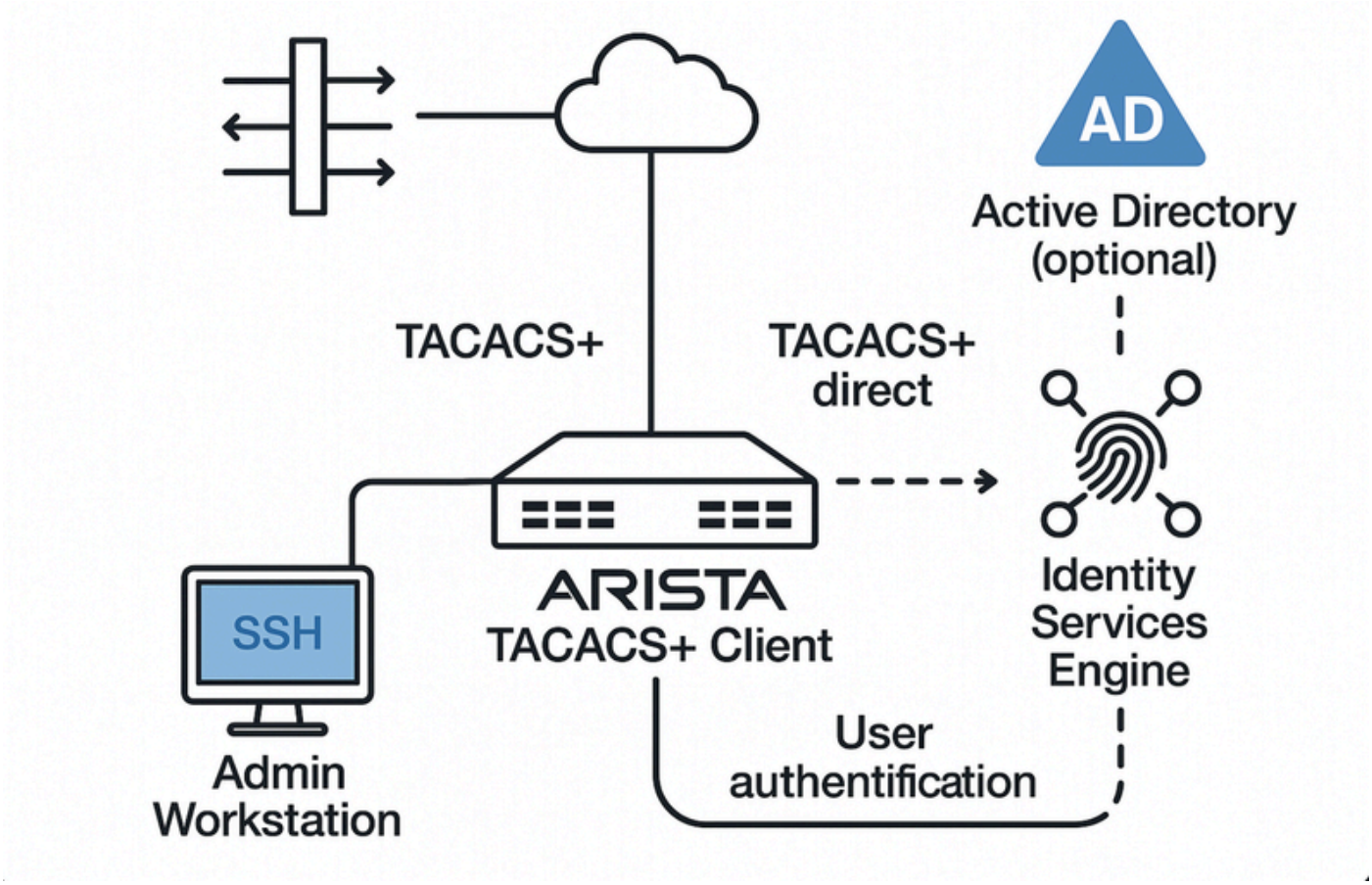
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Arista Switch Software-Image-Version: 4,33,2 F
- Cisco Identity Services Engine (ISE) Version 3.3 Patch 4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen

Netzwerkdiagramm

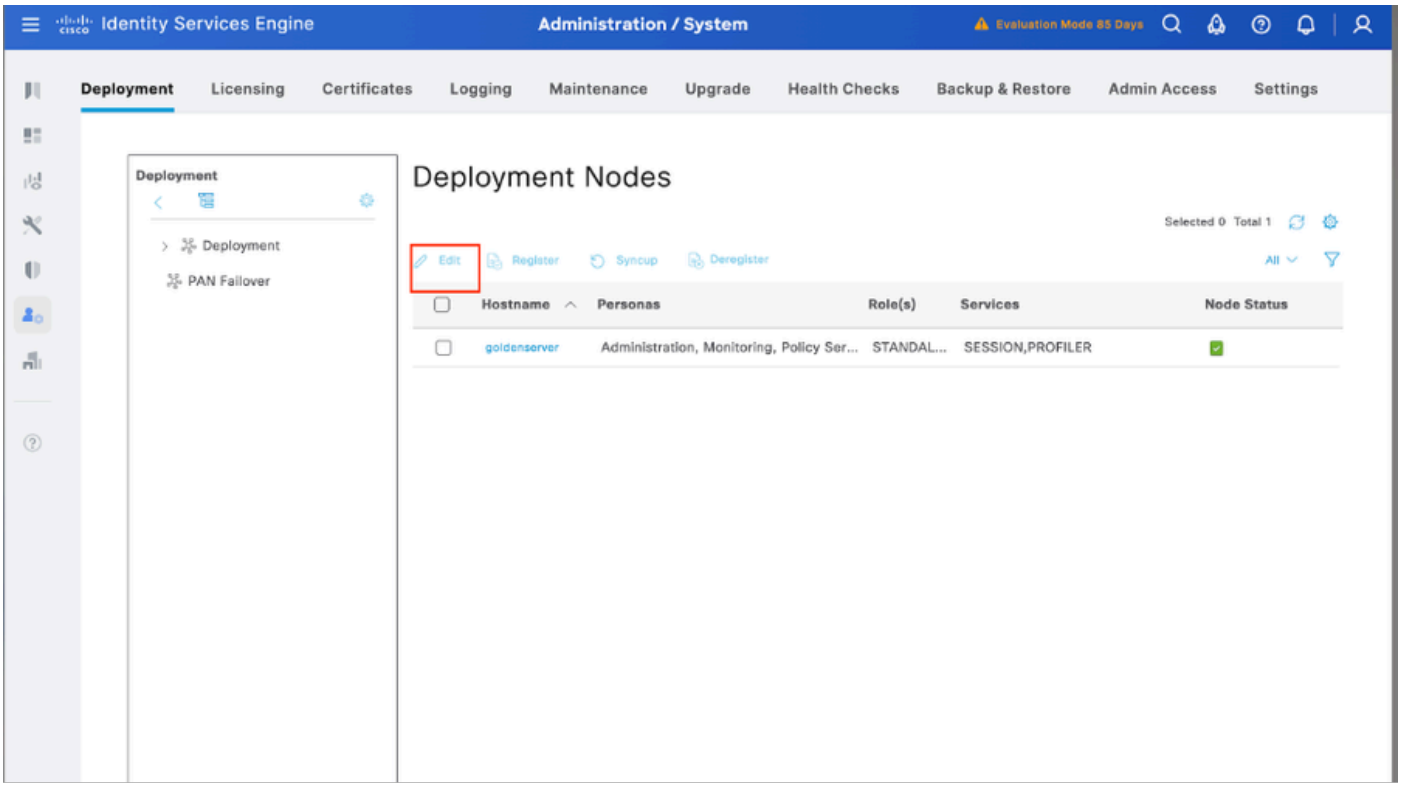


Konfigurationen

TACACS+-Konfiguration auf der ISE

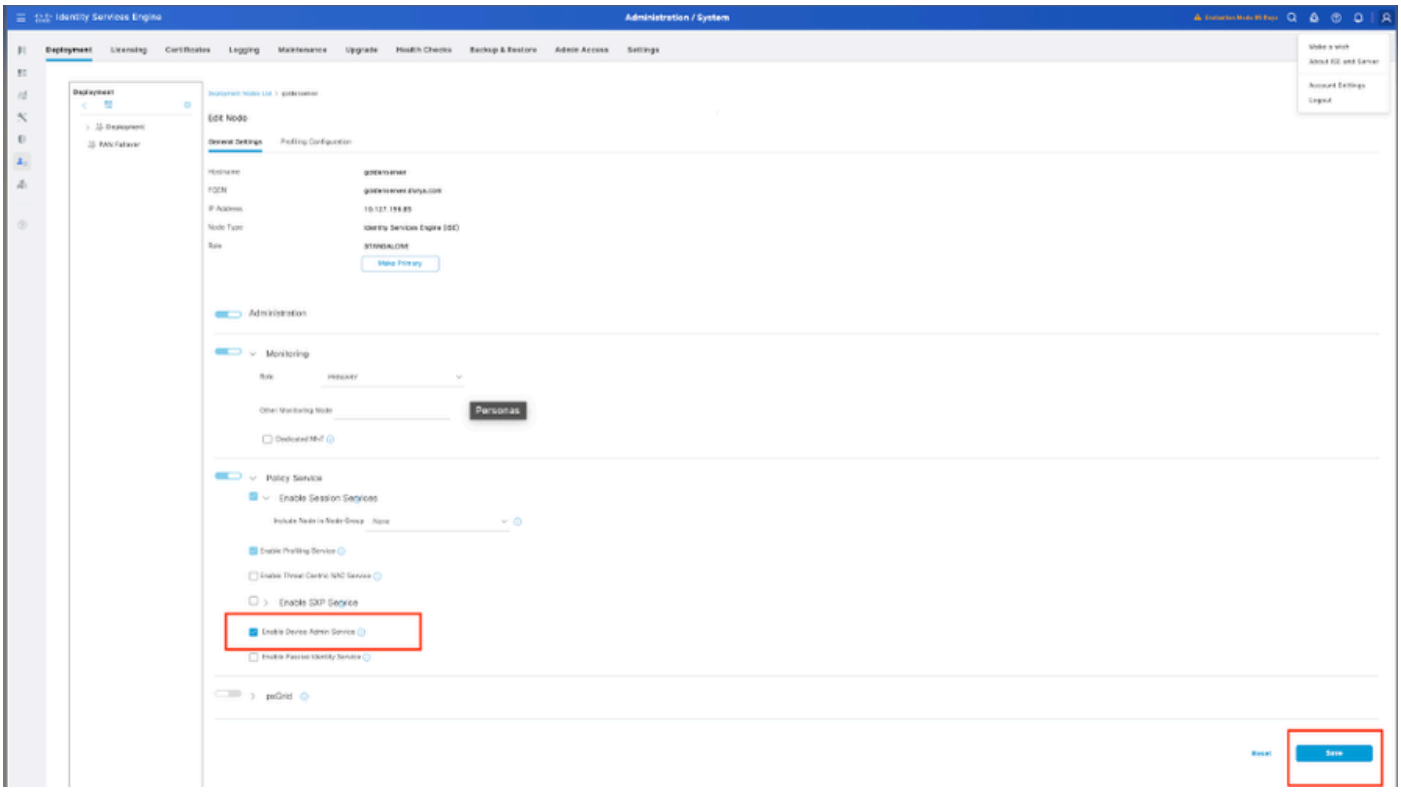
Schritt 1: Im ersten Schritt wird überprüft, ob die Cisco ISE über die erforderlichen Funktionen für die TACACS+-Authentifizierung verfügt. Vergewissern Sie sich dazu, dass die Funktion für den Geräteadministratordienst auf dem gewünschten Policy Service Node (PSN) aktiviert ist.

Navigieren Sie zu Administration > System > Deployment, wählen Sie den entsprechenden Knoten aus, auf dem ISE die TACACS+-Authentifizierung verarbeitet, und klicken Sie auf Edit, um die Konfiguration zu überprüfen.



Schritt 2: Scrollen Sie nach unten, um nach der Device Administration Service-Funktion zu suchen. Beachten Sie, dass zur Aktivierung dieser Funktion die Rolle des Richtliniendiensts auf dem Knoten aktiv sein muss, zusammen mit den verfügbaren TACACS+-Lizenzen in der Bereitstellung.

Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, und speichern Sie dann die Konfiguration.

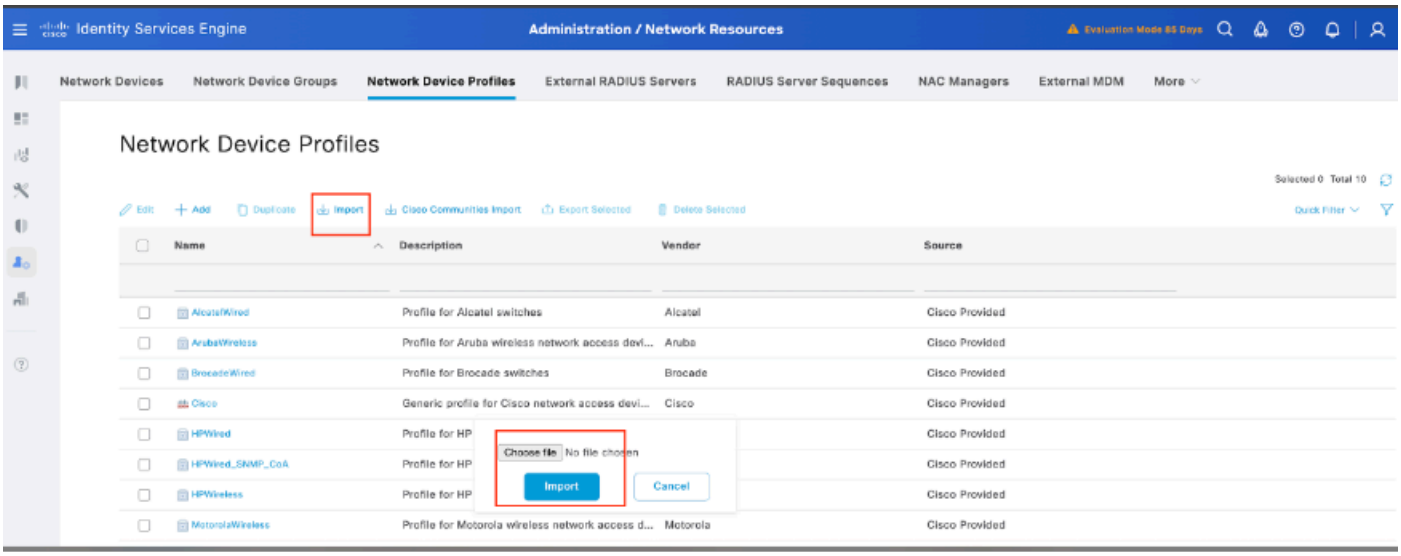


Schritt 3: Anfordern des Arista-Netzwerkgeräteprofils für die Cisco ISE

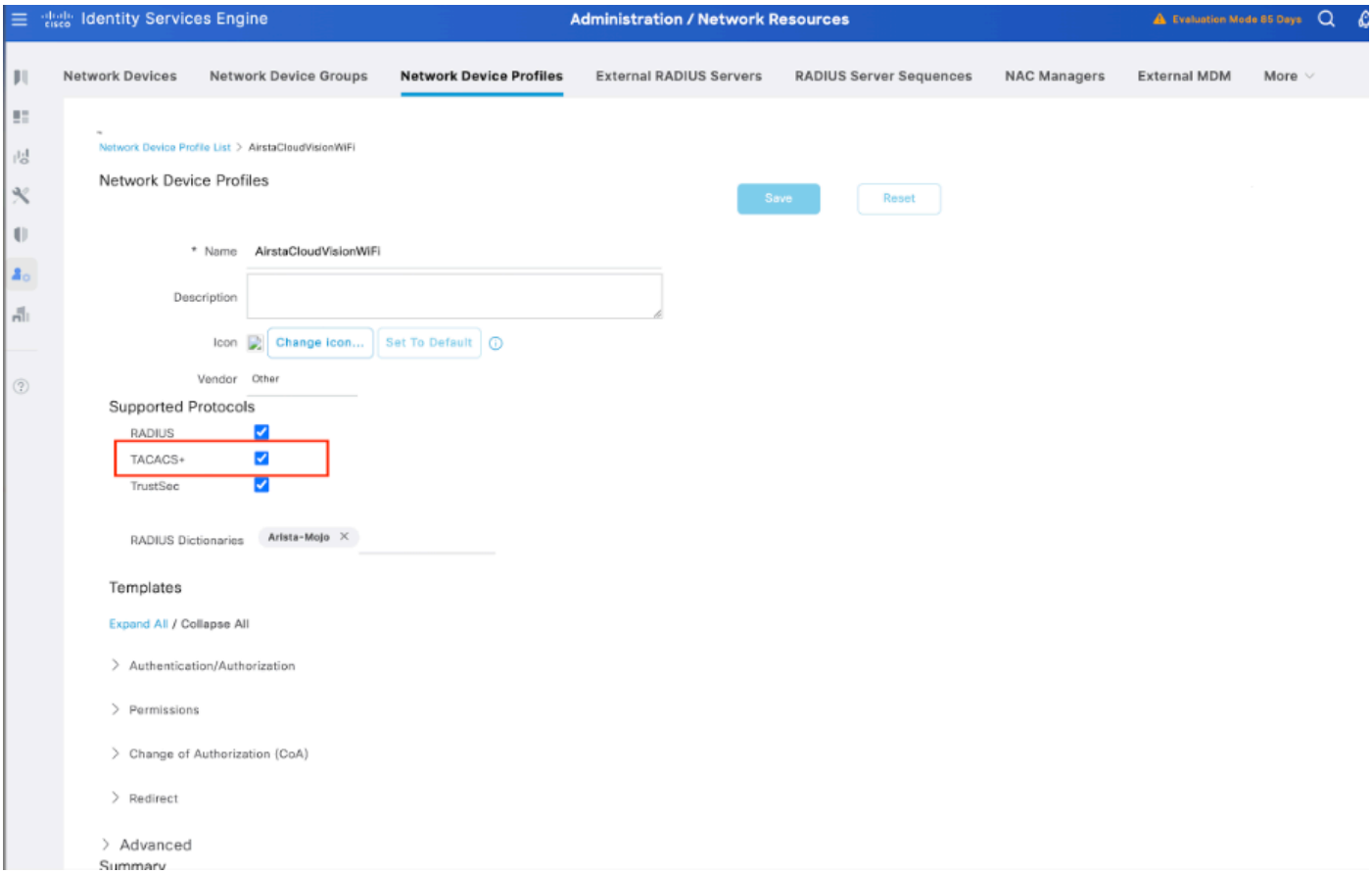
Die Cisco Community hat ein dediziertes NAD-Profil für Arista-Geräte freigegeben. Dieses Profil, zusammen mit den erforderlichen Wörterbuchdateien, finden Sie im Artikel Arista CloudVision WiFi Dictionary und NAD Profile for ISE Integration. Das Herunterladen und Importieren dieses Profils in Ihre ISE-Konfiguration vereinfacht die Integration

Schritte zum Importieren des Arista NAD-Profils in die Cisco ISE:

1. Profil herunterladen:
    - Rufen Sie das Arista NAD-Profil über den oben angegebenen Link zur Cisco Community Cisco Community
2. Zugriff auf die Cisco ISE:
    - Melden Sie sich bei Ihrer Cisco ISE-Verwaltungskonsole an
3. NAD-Profil importieren:
    - Navigieren Sie zu Administration > Network Resources > Network Device Profiles..
    - Klicken Sie auf die Schaltfläche Importieren
    - Laden Sie die heruntergeladene Arista NAD-Profildatei hoch.

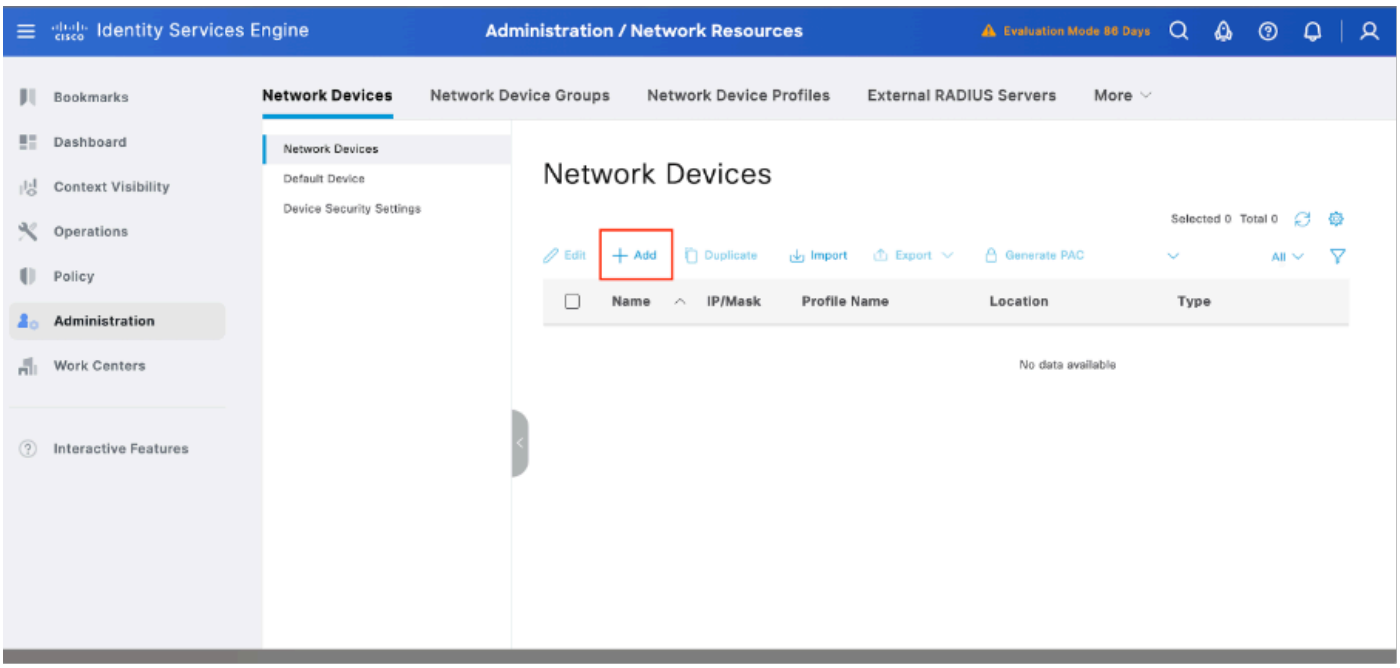


Navigieren Sie nach Abschluss des Uploads zur Option Edit (Bearbeiten), und aktivieren Sie TACACS+ als unterstütztes Protokoll.



Phase 2: Hinzufügen eines Arista-Switches als Netzwerkgerät

1. Navigieren Sie zu Administration > Network Resources > Network Devices > +Add:

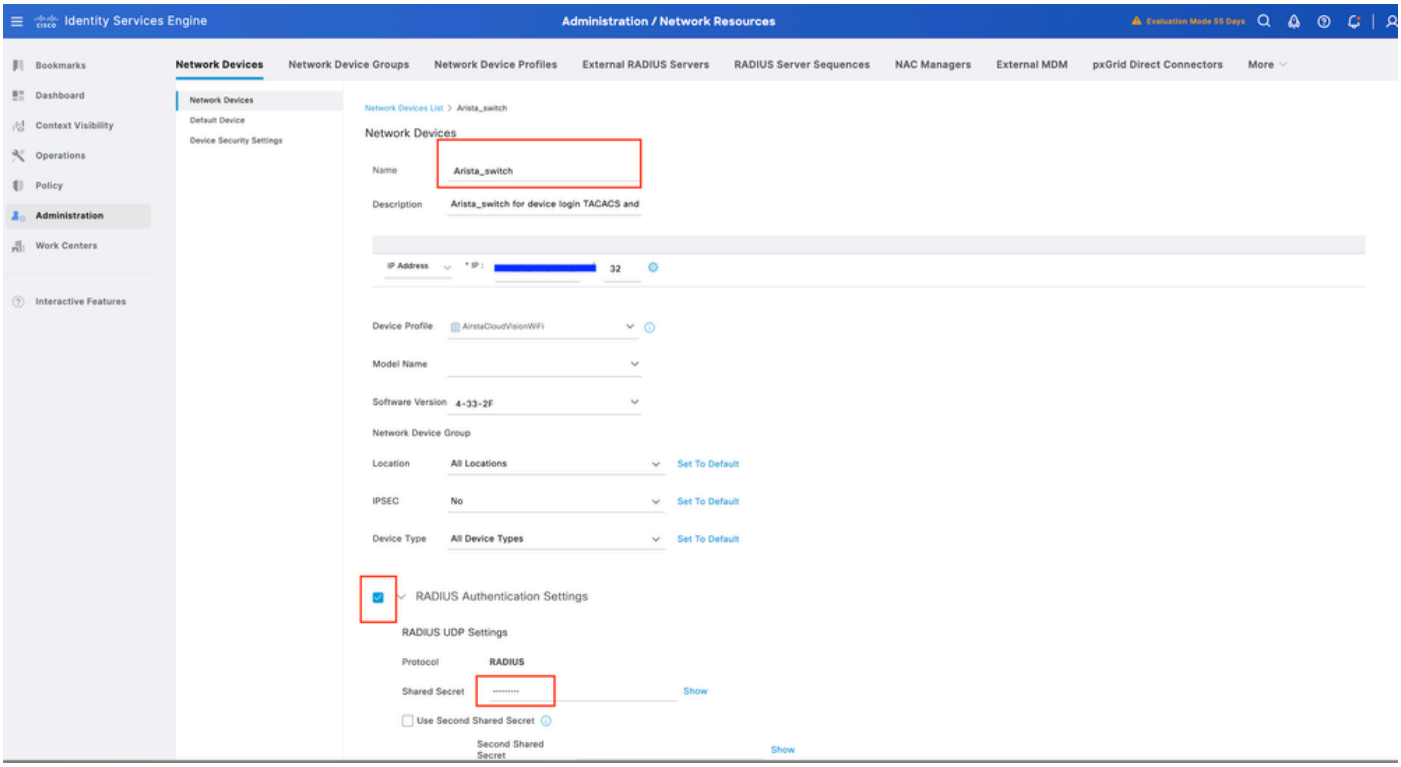


2. Klicken Sie auf Hinzufügen, und geben Sie die folgenden Details ein:

- IP-Adresse: <Switch-IP>
- Gerätetyp: Andere verkabelte auswählen
- Netzwerkgeräteprofil: Wählen Sie AirstaCloudVisionWiFi aus.

- RADIUS-Authentifizierungseinstellungen:
  - Aktivieren Sie die RADIUS-Authentifizierung.
  - Geben Sie den gemeinsamen geheimen Schlüssel ein (muss mit der Switch-Konfiguration übereinstimmen).

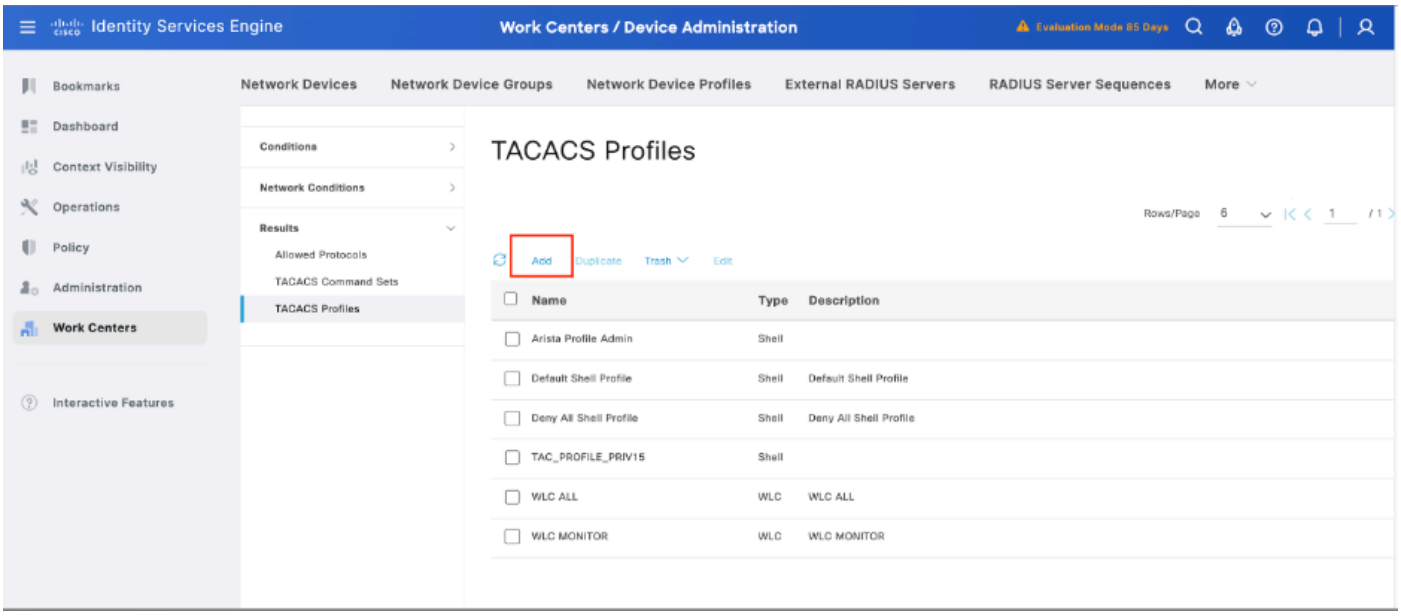
3. Klicken Sie auf Speichern:



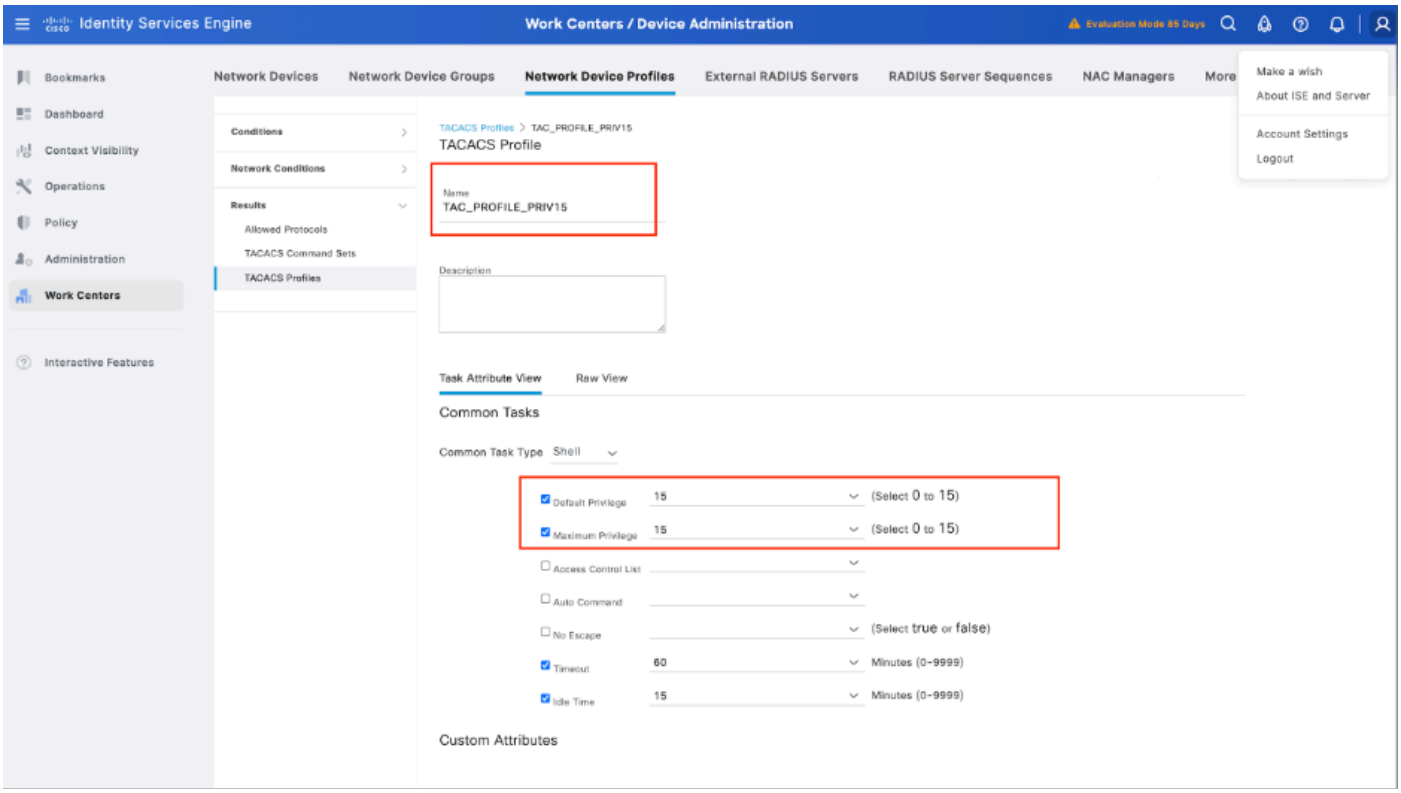
Schritt 3: Überprüfen Sie, ob das neue Gerät unter Netzwerkgeräte angezeigt wird:

Schritt 4: Konfigurieren des TACACS-Profils

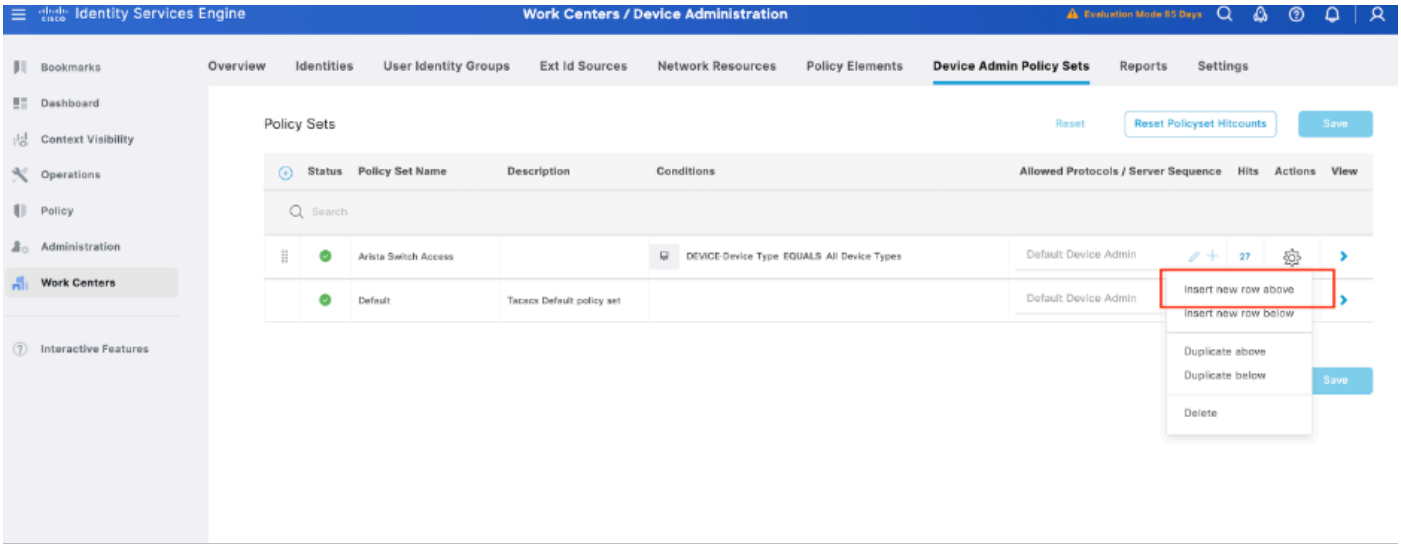
Erstellen Sie ein TACACS-Profil, navigieren Sie zum Menü Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles, und wählen Sie dann Add:



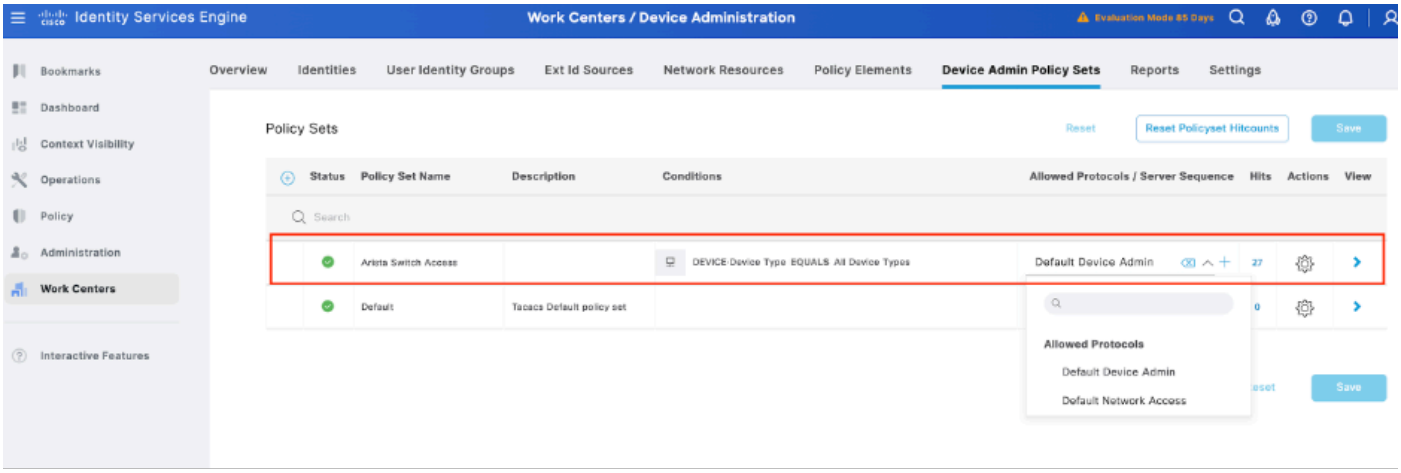
Geben Sie einen Namen ein, aktivieren Sie das Kontrollkästchen Standardberechtigung, und legen Sie den Wert auf 15 fest. Wählen Sie außerdem Maximale Berechtigung, legen Sie den Wert auf 15 fest, und klicken Sie auf Senden:



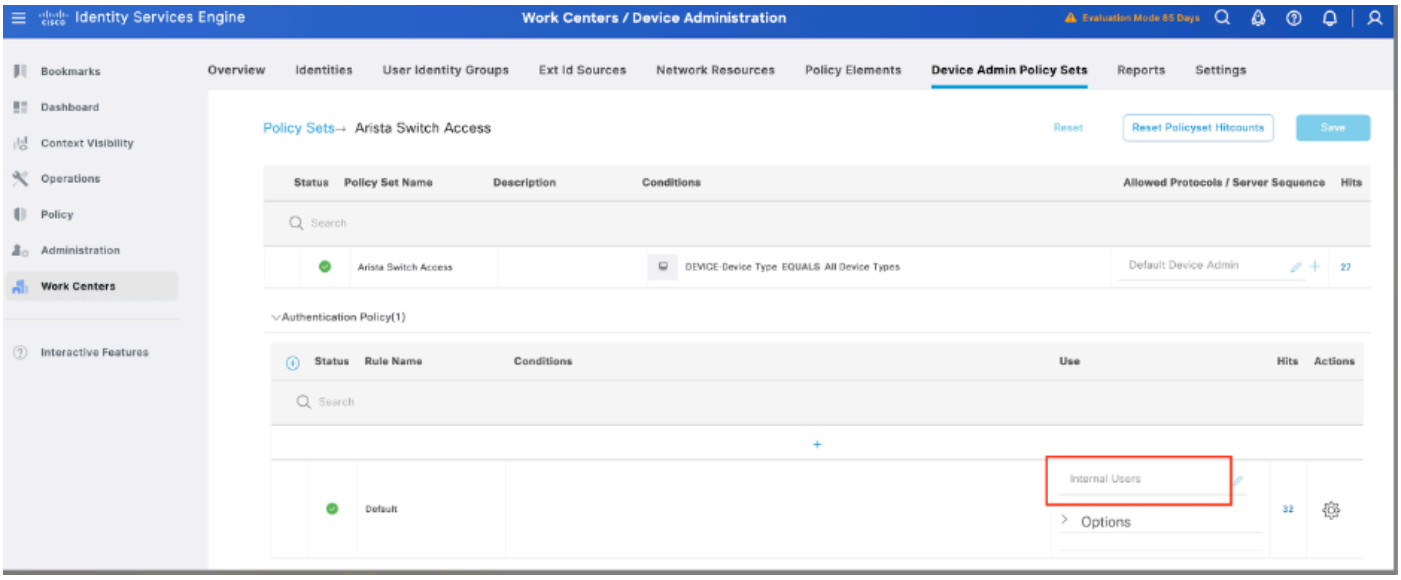
Schritt 5: Erstellen Sie einen Device Admin Policy Set für Ihren Arista Switch, navigieren Sie zum Menü Work Centers > Device Administration > Device Admin Policy Sets, und wählen Sie dann aus einem vorhandenen Policy Set das Zahnradsymbol aus, um dann oben eine neue Zeile einfügen auszuwählen.



Schritt 6: Benennen Sie diesen neuen Richtliniensatz, fügen Sie Bedingungen hinzu, die von den Merkmalen der TACACS+-Authentifizierungen abhängen, die vom Arista-Switch ausgeführt werden, und wählen Sie Zulässige Protokolle > Standardgeräteadministrator, und speichern Sie die Konfiguration.

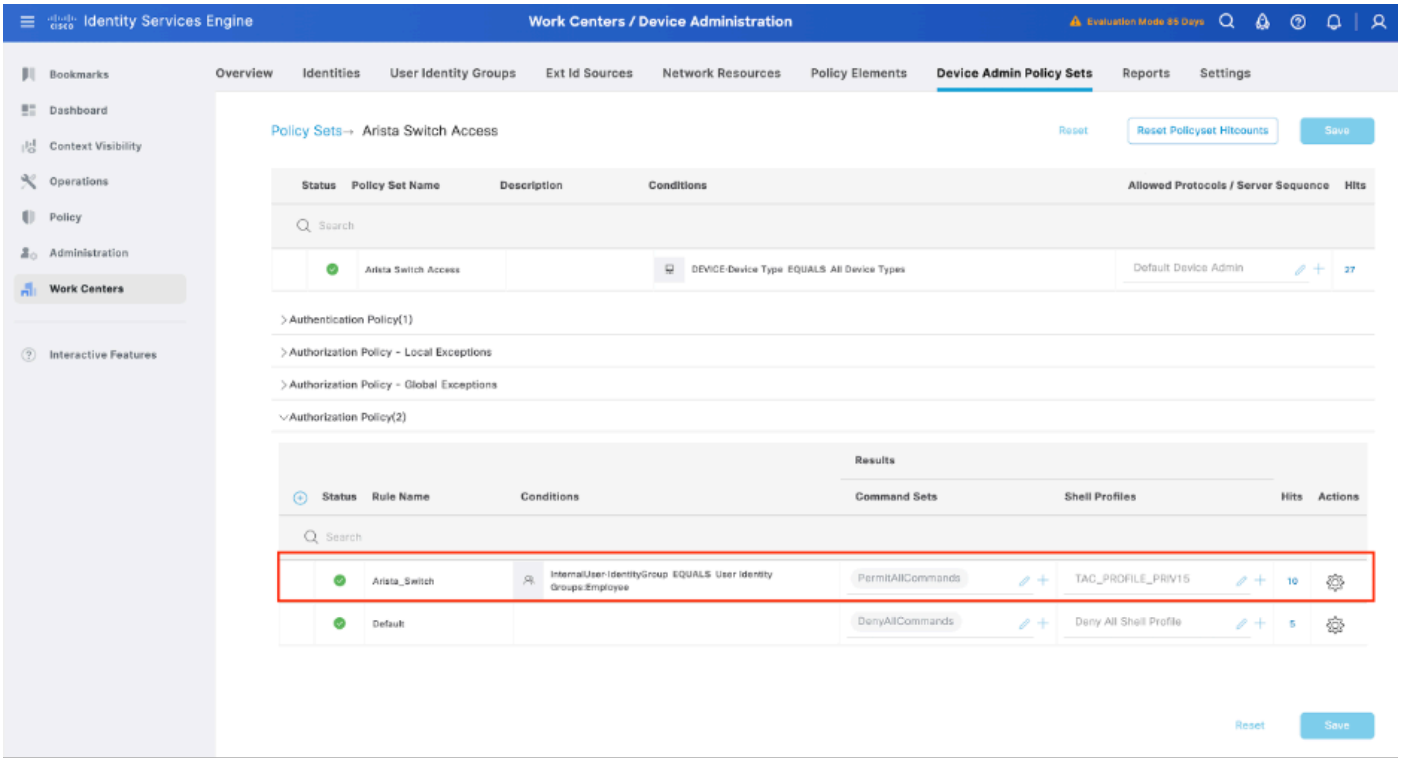


Schritt 7: Wählen Sie in der Option > view (Ansicht) und dann im Abschnitt Authentication Policy (Authentifizierungsrichtlinie) die externe Identitätsquelle aus, die Cisco ISE verwendet, um den Benutzernamen und die Anmeldeinformationen für die Authentifizierung am Arista-Switch abzufragen. In diesem Beispiel entsprechen die Anmeldeinformationen internen Benutzern, die in der ISE gespeichert sind.



Schritt 8: Blättern Sie nach unten bis zum Abschnitt Autorisierungsrichtlinie zu Standardrichtlinie, wählen Sie das Zahnradsymbol aus, und fügen Sie eine Regel oben ein.

Schritt 9: Benennen Sie die neue Autorisierungsregel, fügen Sie Bedingungen für den Benutzer hinzu, der bereits als Gruppenmitgliedschaft authentifiziert wurde, und speichern Sie im Abschnitt Shell Profiles (Shell-Profile) das zuvor konfigurierte TACACS-Profil.



Arista-Switch konfigurieren

Schritt 1: Aktivieren der TACACS+-Authentifizierung

Melden Sie sich beim Arista-Switch an, und wechseln Sie in den Konfigurationsmodus:

konfigurieren

!

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

!

aaa Group Server TACACS+ ISE_TACACS

  server <ISE-IP>

!

aaa, Authentifizierung, Anmeldung, Standardgruppe ISE_TACACS, lokal

aaa, Autorisierung, exec-Standardgruppe ISE_TACACS, lokal

aaa accounting-Befehle 15 standardmäßige Start-Stopp-Gruppe ISE_TACACS

!

End

Schritt 2: Speichern der Konfiguration

So halten Sie die Konfiguration auch nach einem Neustart aufrecht:

Schreibspeicher

ODER

copy running-config startup-config

Überprüfung

ISE-Prüfung

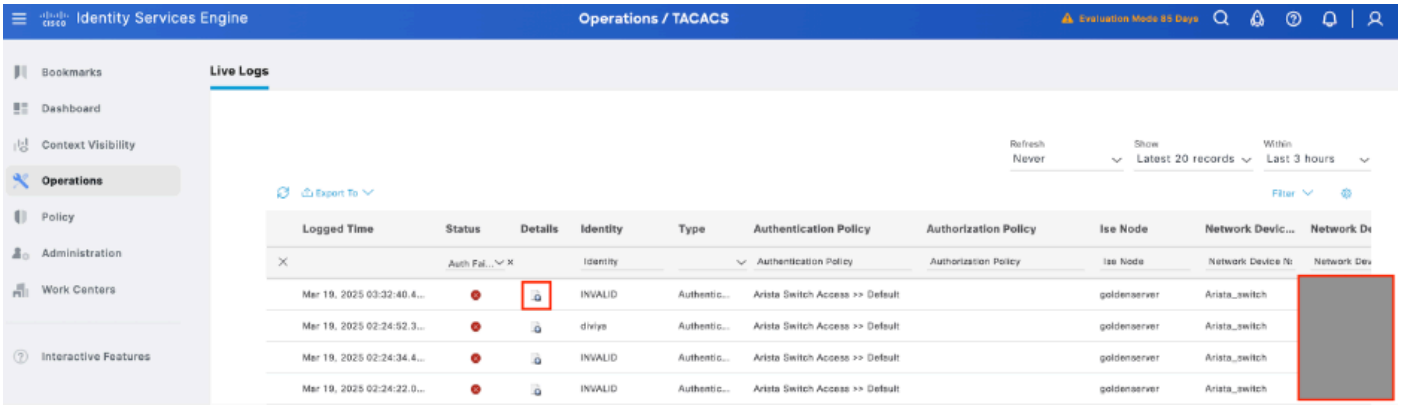
Schritt 1: Überprüfen Sie, ob die TACACS+-Wartungsfreundlichkeit ausgeführt wird. Dies kann wie folgt eingecheckt werden:

- GUI: Überprüfen Sie, ob der Knoten mit dem Service DEVICE ADMIN unter > System > Deployment aufgeführt ist.
- CLI: Führen Sie den Befehl show ports aus. | einschließlich 49, um zu bestätigen, dass es Verbindungen im TCP-Port gibt, die zu TACACS+ gehören.

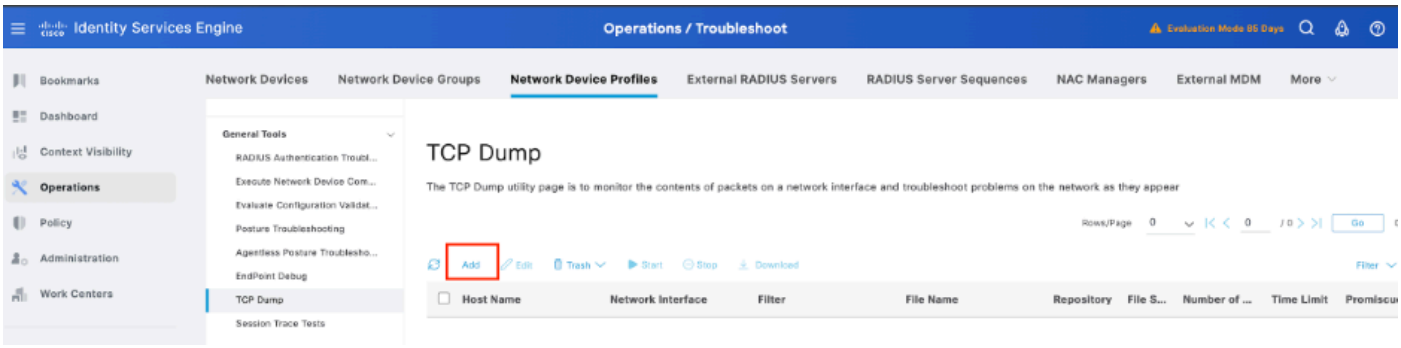
Schritt 2: Bestätigen Sie, ob Livelogs zu TACACS+-Authentifizierungsversuchen vorhanden sind:

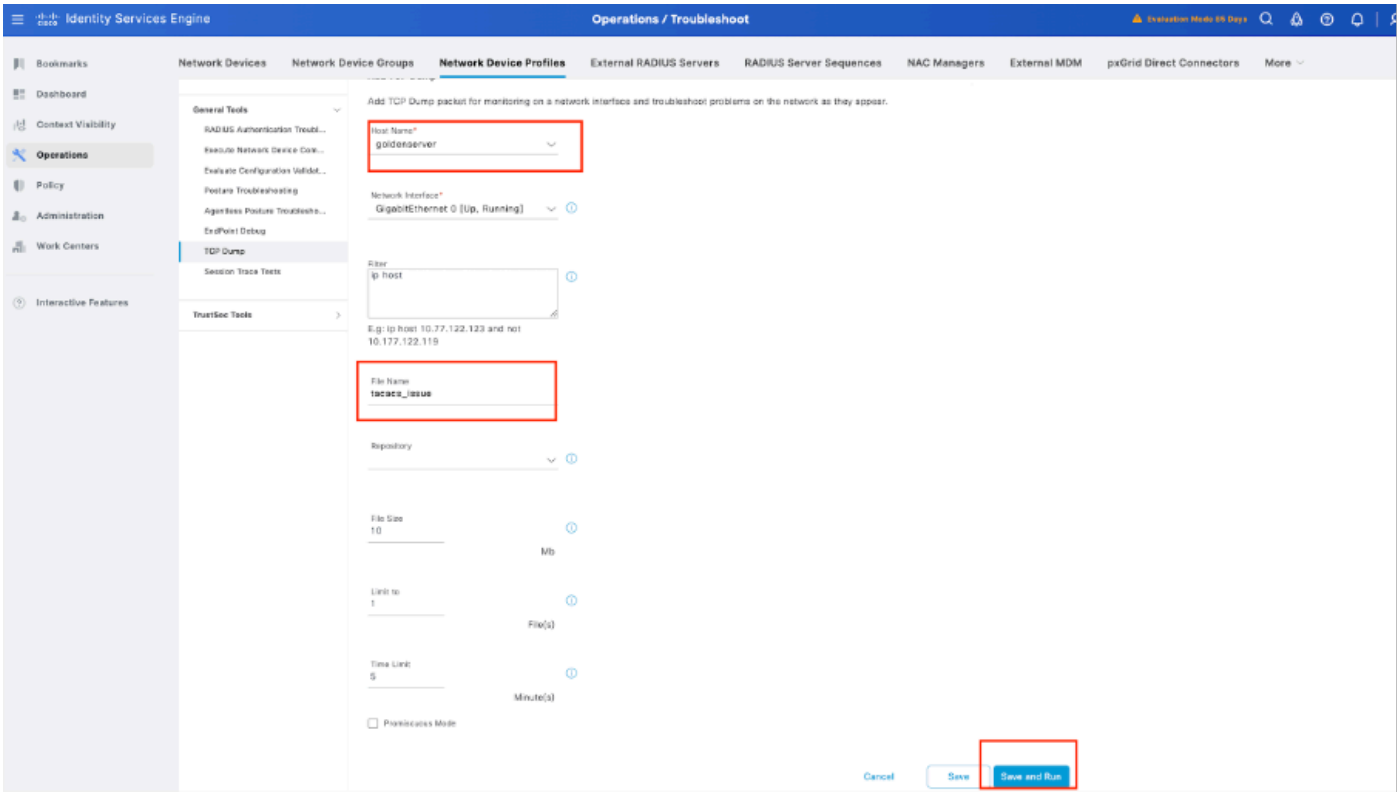
Dies kann im Menü Vorgänge > TACACS > Live-Protokolle überprüft werden.

Abhängig vom Fehlergrund können Sie die Konfiguration anpassen oder die Fehlerursache beheben.

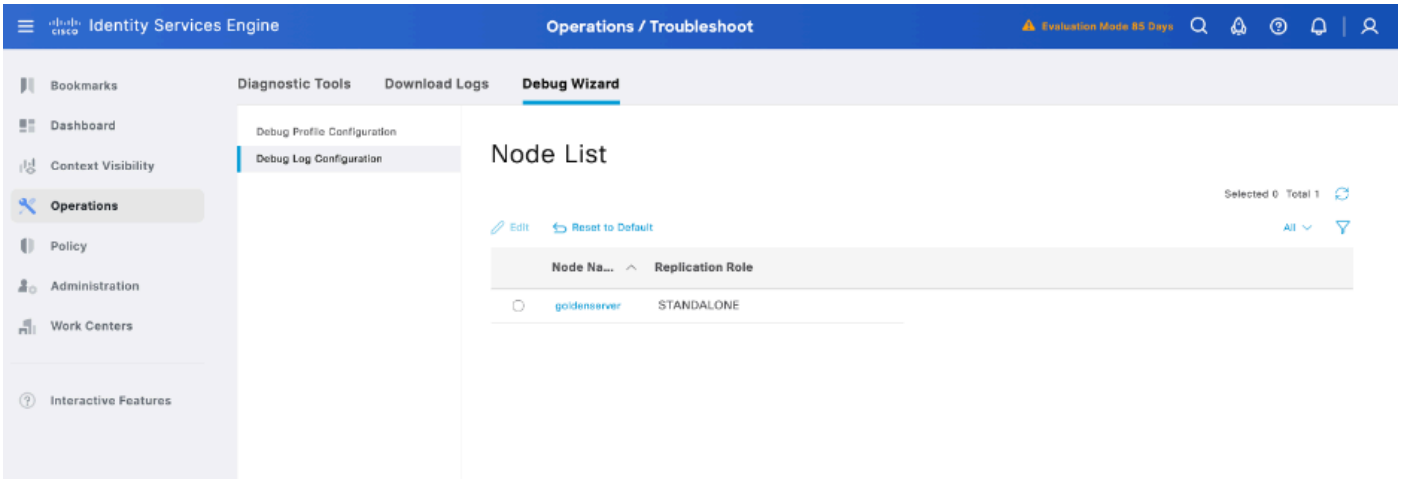


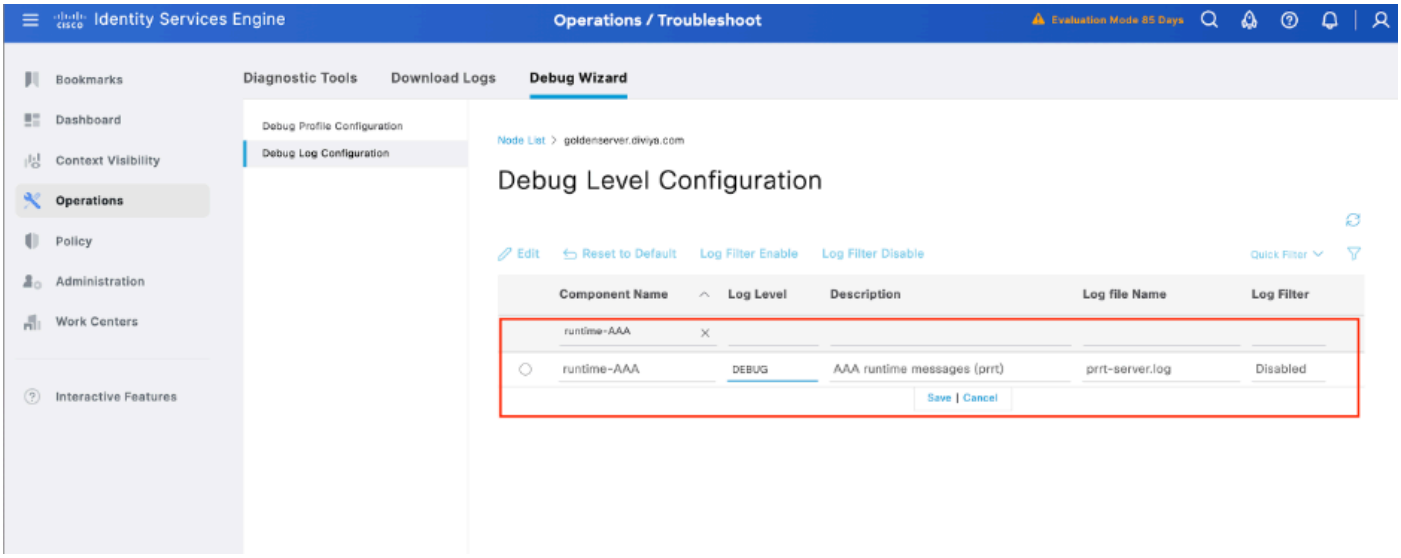
Schritt 3: Falls kein Livelog angezeigt wird, fahren Sie mit der Paketerfassung fort. Navigieren Sie zum Menü Vorgänge > Fehlerbehebung > Diagnosetools > Allgemeine Tools > TCP-Dump, und wählen Sie Hinzufügen:





Schritt 4: Aktivieren Sie die Komponente Laufzeit-AAA beim Debuggen innerhalb des PSN, von dem aus die Authentifizierung durchgeführt wird. Wählen Sie dazu Operations > Troubleshoot > Debug Wizard > Debug log configuration, wählen Sie PSN node aus, und wählen Sie dann die Schaltfläche Edit:





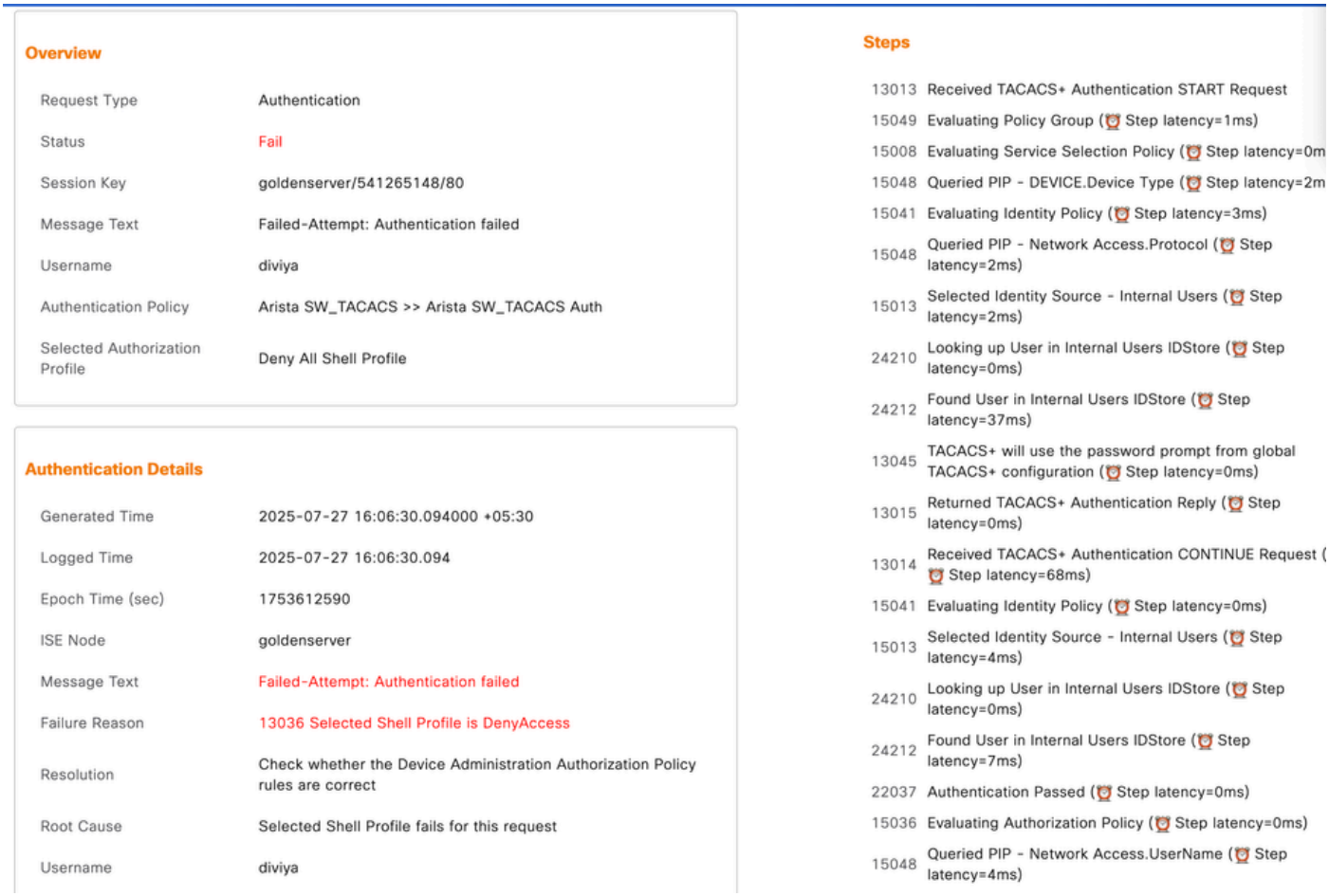
Identifizieren Sie die Laufzeit-AAA-Komponente, legen Sie deren Protokollierungsebene auf debug fest, reproduzieren Sie das Problem, und analysieren Sie die Protokolle für weitere Untersuchungen.

Fehlerbehebung

Problem 1

Die TACACS+-Authentifizierung zwischen der Cisco ISE und dem Arista-Switch (oder einem anderen Netzwerkgerät) schlägt mit der folgenden Fehlermeldung fehl:

"13036 Selected Shell Profile is DenyAccess"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/541265148/80
Message Text	Failed-Attempt: Authentication failed
Username	diviya
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group (Step latency=1ms)
15008	Evaluating Service Selection Policy (Step latency=0m
15048	Queried PIP - DEVICE.Device Type (Step latency=2m
15041	Evaluating Identity Policy (Step latency=3ms)
15048	Queried PIP - Network Access.Protocol (Step latency=2ms)
15013	Selected Identity Source - Internal Users (Step latency=2ms)
24210	Looking up User in Internal Users IDStore (Step latency=0ms)
24212	Found User in Internal Users IDStore (Step latency=37ms)
13045	TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms)
13015	Returned TACACS+ Authentication Reply (Step latency=0ms)
13014	Received TACACS+ Authentication CONTINUE Request (Step latency=68ms)
15041	Evaluating Identity Policy (Step latency=0ms)
15013	Selected Identity Source - Internal Users (Step latency=4ms)
24210	Looking up User in Internal Users IDStore (Step latency=0ms)
24212	Found User in Internal Users IDStore (Step latency=7ms)
22037	Authentication Passed (Step latency=0ms)
15036	Evaluating Authorization Policy (Step latency=0ms)
15048	Queried PIP - Network Access.UserName (Step latency=4ms)

Der Fehler "13036 Selected Shell Profile is DenyAccess" (ausgewähltes Shell-Profil ist DenyAccess) in der Cisco ISE bedeutet normalerweise, dass die Autorisierungsrichtlinie während eines TACACS+-Geräteverwaltungsversuchs einem Shell-Profil mit DenyAccess entsprach. Dies ist normalerweise nicht das Ergebnis eines falsch konfigurierten Shell-Profils selbst, sondern zeigt vielmehr an, dass keine der konfigurierten Autorisierungsregeln mit den eingehenden Benutzerattributen (z. B. Gruppenmitgliedschaft, Gerätetyp oder Standort) übereinstimmt. Daher wird die ISE auf eine Standardregel oder eine explizite Ablehnungsregel zurückgesetzt, was dazu führt, dass der Zugriff verweigert wird.

Mögliche Ursachen

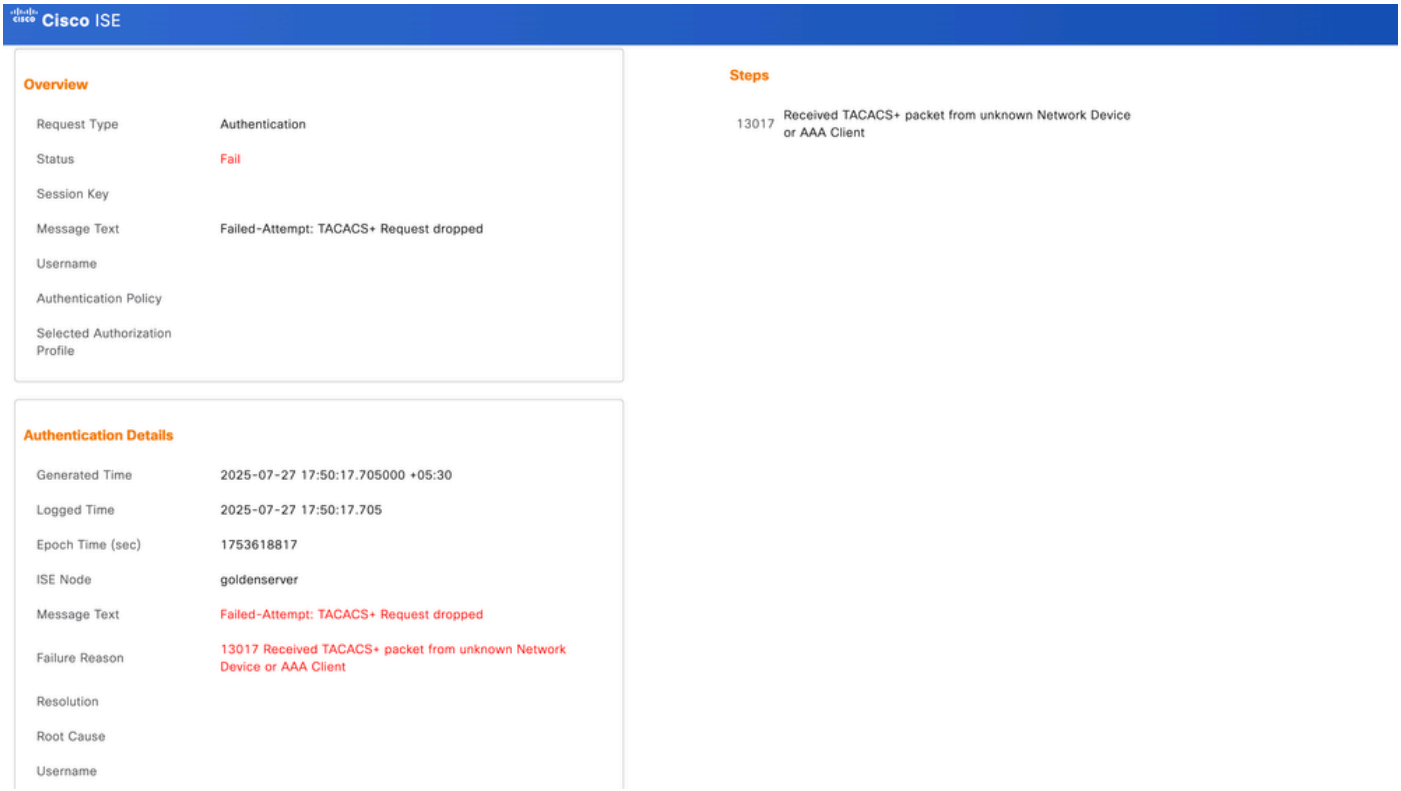
- Überprüfen der Autorisierungsrichtlinienregeln in der ISE Überprüfen Sie, ob der Benutzer oder das Gerät mit der richtigen Regel übereinstimmt, die das gewünschte Shell-Profil zuweist, z. B. eine Regel, die den entsprechenden Zugriff ermöglicht.
- Stellen Sie sicher, dass die AD- oder interne Benutzergruppenzuordnung korrekt ist und dass die Richtlinienbedingungen, z. B. die Benutzergruppenmitgliedschaft, der Gerätetyp und das Protokoll, korrekt angegeben sind.
- Verwenden Sie ISE-Live-Protokolle und Details zum fehlgeschlagenen Versuch, um genau zu sehen, welche Regel zugeordnet wurde und warum.

Problem 2

Die TACACS+-Authentifizierung zwischen der Cisco ISE und dem Arista Switch (oder einem

anderen Netzwerkgerät) schlägt fehl und gibt die folgende Fehlermeldung aus:

"13017 empfangenes TACACS+-Paket von unbekanntem Netzwerkgerät oder AAA-Client"



Mögliche Ursachen

- Der häufigste Grund ist, dass die IP-Adresse des Switches nicht als Netzwerkgerät in der ISE hinzugefügt wird (unter Administration > Network Resources > Network Devices).
- Stellen Sie sicher, dass die IP-Adresse oder der IP-Bereich genau mit der Quell-IP übereinstimmt, die vom Arista-Switch zum Senden von TACACS+-Paketen verwendet wird.
- Wenn Ihr Switch eine Management-Schnittstelle verwendet, stellen Sie sicher, dass die genaue IP (nicht nur ein Subnetz/Bereich) in der ISE hinzugefügt wird.

Lösung

- Gehen Sie zu Administration > Network Resources > Network Devices in der ISE GUI.
- Überprüfen Sie, ob die genaue Quell-IP-Adresse auf dem Arista-Switch für die TACACS+-Kommunikation verwendet wird (meistens die IP-Adresse der Verwaltungsschnittstelle).
- Geben Sie den gemeinsamen geheimen Schlüssel an (er muss mit dem übereinstimmen, was auf dem Arista-Switch festgelegt ist).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.