Configuración del inicio de sesión del administrador basado en RADIUS en el switch Arista

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Diagrama de la red
- Configurar
  - Configuración de Cisco ISE
    - Paso 1. Obtención del perfil de dispositivo de red de Arista para Cisco ISE
    - Paso 2. Agregar Arista Switch como un Dispositivo de Red
    - Paso 3. Validar que el nuevo dispositivo se muestre en Dispositivos de red
    - Paso 4. Creación de los Grupos de Identidad de Usuario Requeridos
    - Paso 5. Establezca un nombre para el grupo de identidades AdminUser
    - Paso 6. Crear los usuarios locales y agregarlos a su grupo correspondiente
    - Paso 7. Crear el perfil de autorización para el usuario administrador
    - Paso 8. Crear un conjunto de políticas que coincida con la dirección IP del switch Arista
    - Paso 9. Ver el Nuevo Conjunto de Políticas
  - Configuración del switch Arista
    - Paso 1. Habilite la autenticación RADIUS
    - Paso 2. Guardar configuración
- Verificación
  - Revisión de ISE
- Resolución de problemas
  - Situación 1. "Solicitud 5405 RADIUS rechazada"
    - Problema
    - Posibles Causas
    - Solución
  - Situación 2: el switch Arista no puede conmutar por error para realizar una copia de seguridad de ISE PSN
    - Problema
    - Posibles Causas
    - Solución

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) para autenticar los inicios de sesión del administrador en los switches Arista mediante RADIUS.

Prerequisites

Requirements

Antes de continuar, asegúrese de que:

- Cisco ISE (versión 3.x recomendada) está instalado y en funcionamiento.
- Switch Arista que ejecuta EOS con soporte RADIUS.
- Active Directory (AD) o base de datos de usuarios interna configurada en ISE.

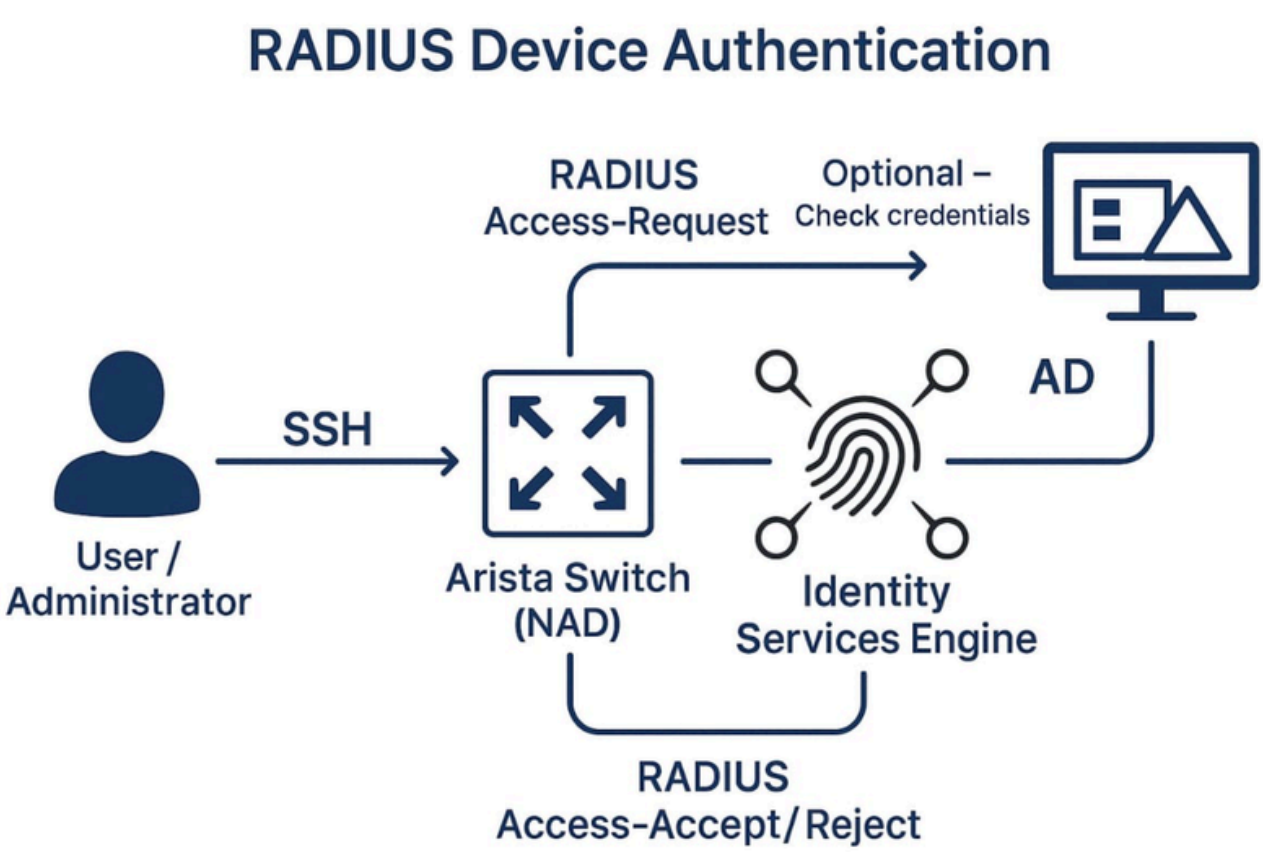
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de imagen de software del switch Arista: 4.33.2F
- Parche 4 de Cisco Identity Services Engine (ISE) versión 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red



Este es un diagrama de red que ilustra la autenticación de dispositivos basada en RADIUS para un switch Arista que utiliza Cisco ISE, con Active Directory (AD) como fuente de autenticación opcional.

El diagrama incluye:

- Arista Switch (actúa como dispositivo de acceso a la red, NAD)
- Cisco ISE (que actúa como servidor RADIUS)
- Active Directory (AD) [Opcional] (se utiliza para la verificación de identidad)
- Usuario/Administrador (que inicia sesión mediante SSH)

Configurar

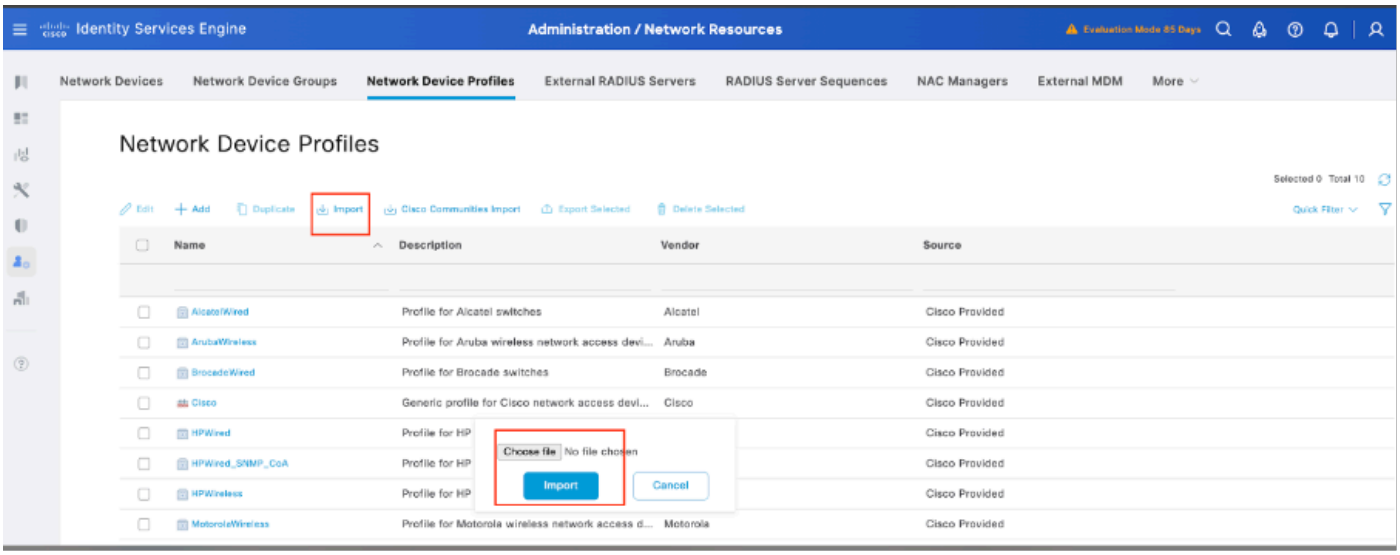
Configuración de Cisco ISE

Paso 1. Obtención del perfil de dispositivo de red de Arista para Cisco ISE

La comunidad de Cisco ha compartido un perfil NAD dedicado para los dispositivos Arista. Este perfil, junto con los archivos de diccionario necesarios, se puede encontrar en el artículo Arista CloudVision WiFi Dictionary y NAD Profile for ISE Integration. La descarga e importación de este perfil en la configuración de ISE facilita una integración más fluida

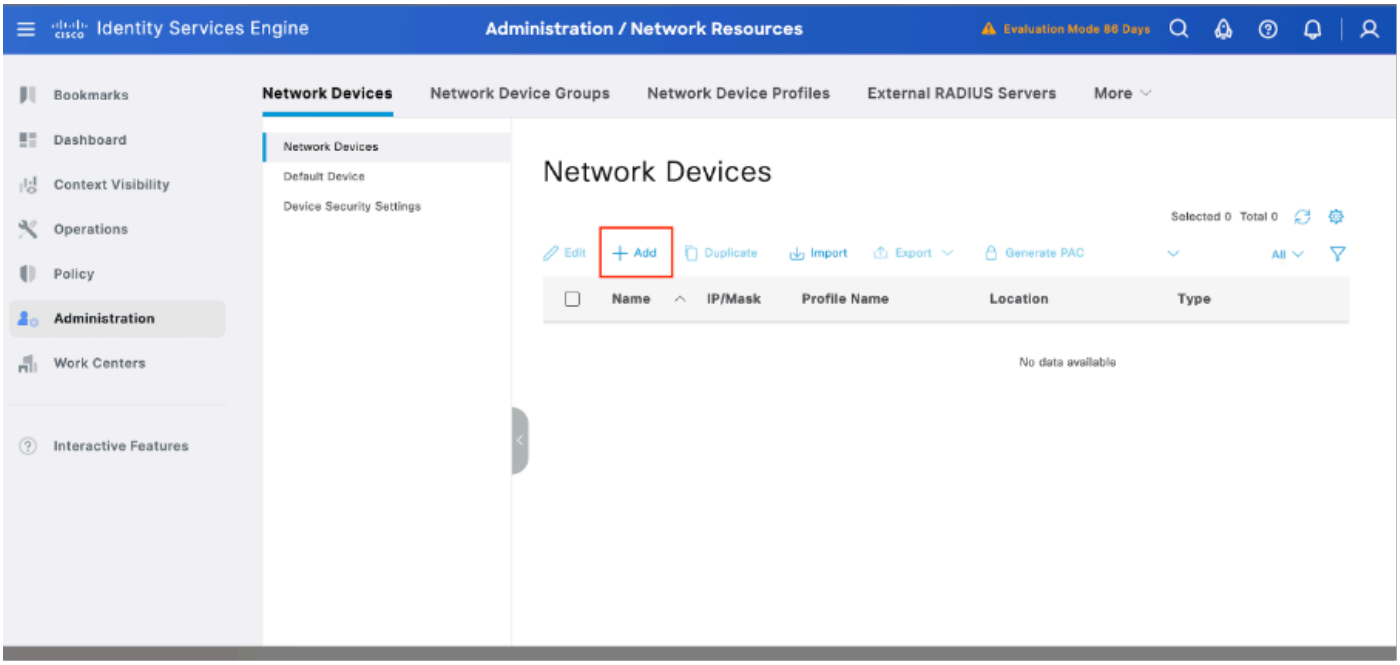
Estos son los pasos para importar el perfil de Arista NAD en Cisco ISE:

1. Descargue el perfil:
    - Obtenga el perfil de Arista NAD del enlace de la comunidad de Cisco proporcionado anteriormente. Comunidad de Cisco.
2. Acceda a Cisco ISE:
    - Inicie sesión en la consola administrativa de Cisco ISE
3. Importar el perfil NAD:
    - Vaya a Administration > Network Resources > Network Device Profiles.
    - Haga clic en el botón Import.
    - Cargue el archivo de perfil de Arista NAD descargado.



Paso 2. Agregar un switch Arista como dispositivo de red

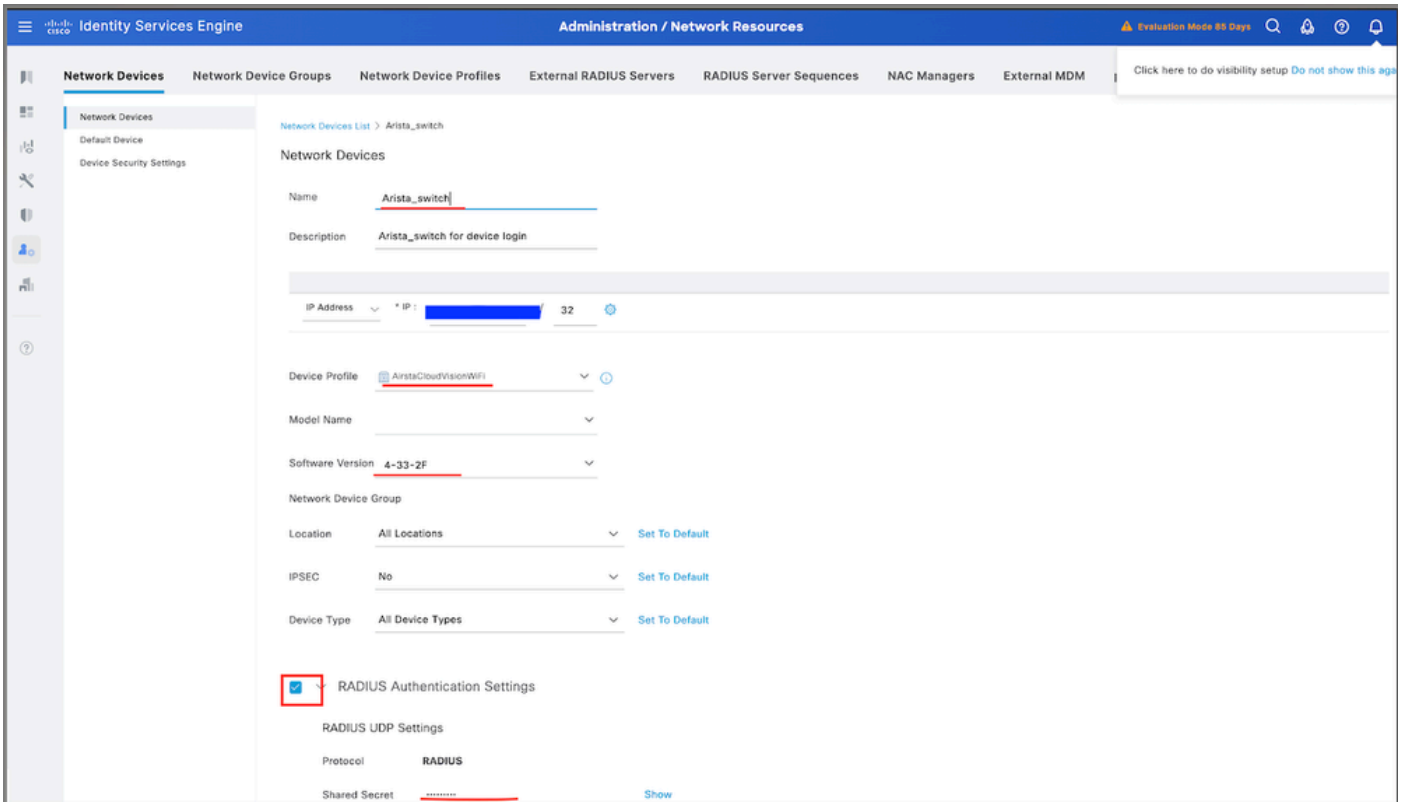
1. Vaya a Administration > Network Resources > Network Devices > +Add.



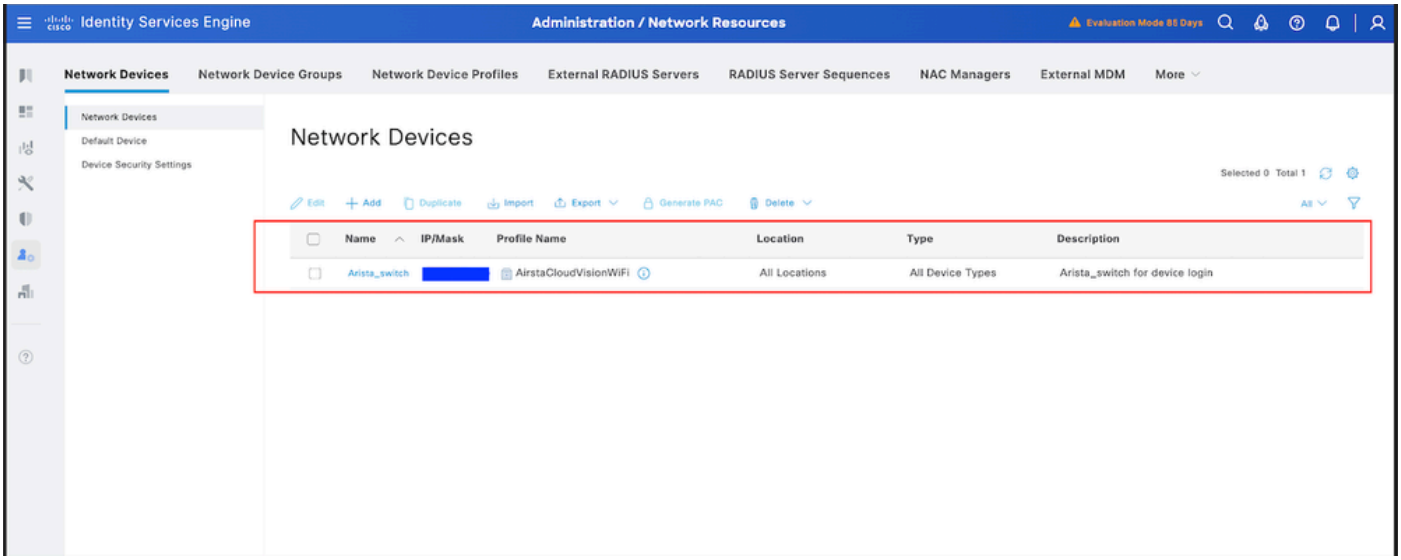
2. Haga clic en Agregar e ingrese estos detalles:

1. Nombre: Arista-Switch
2. IP Address: <Switch-IP>
3. tipo de dispositivo: Seleccione Otro Cableado
4. Perfil de dispositivo de red: seleccione AirstaCloudVisionWiFi.
5. Configuración de autenticación RADIUS:
    1. Habilitar autenticación RADIUS
    2. Ingrese el secreto compartido (debe coincidir con la configuración del switch).

3. Haga clic en Guardar.

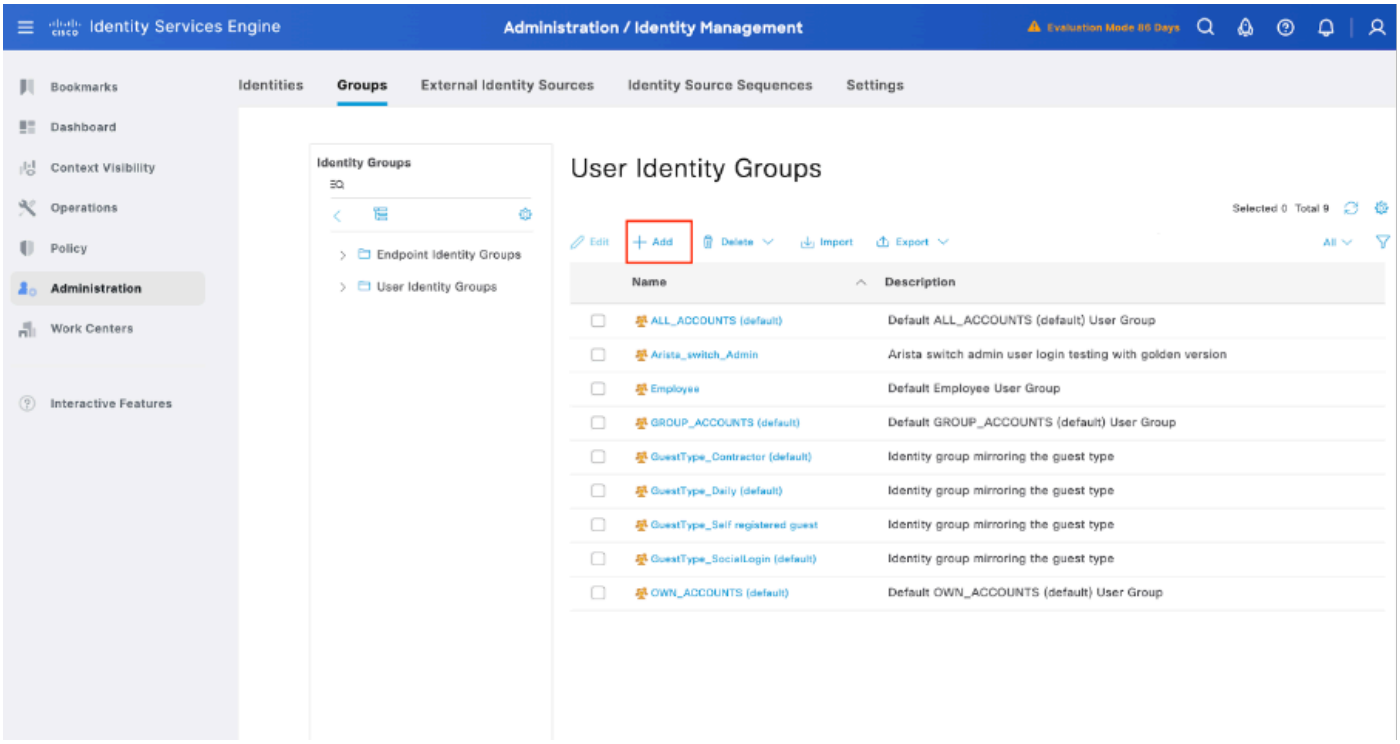


Paso 3. Validate the New Device is Shown under Network Devices



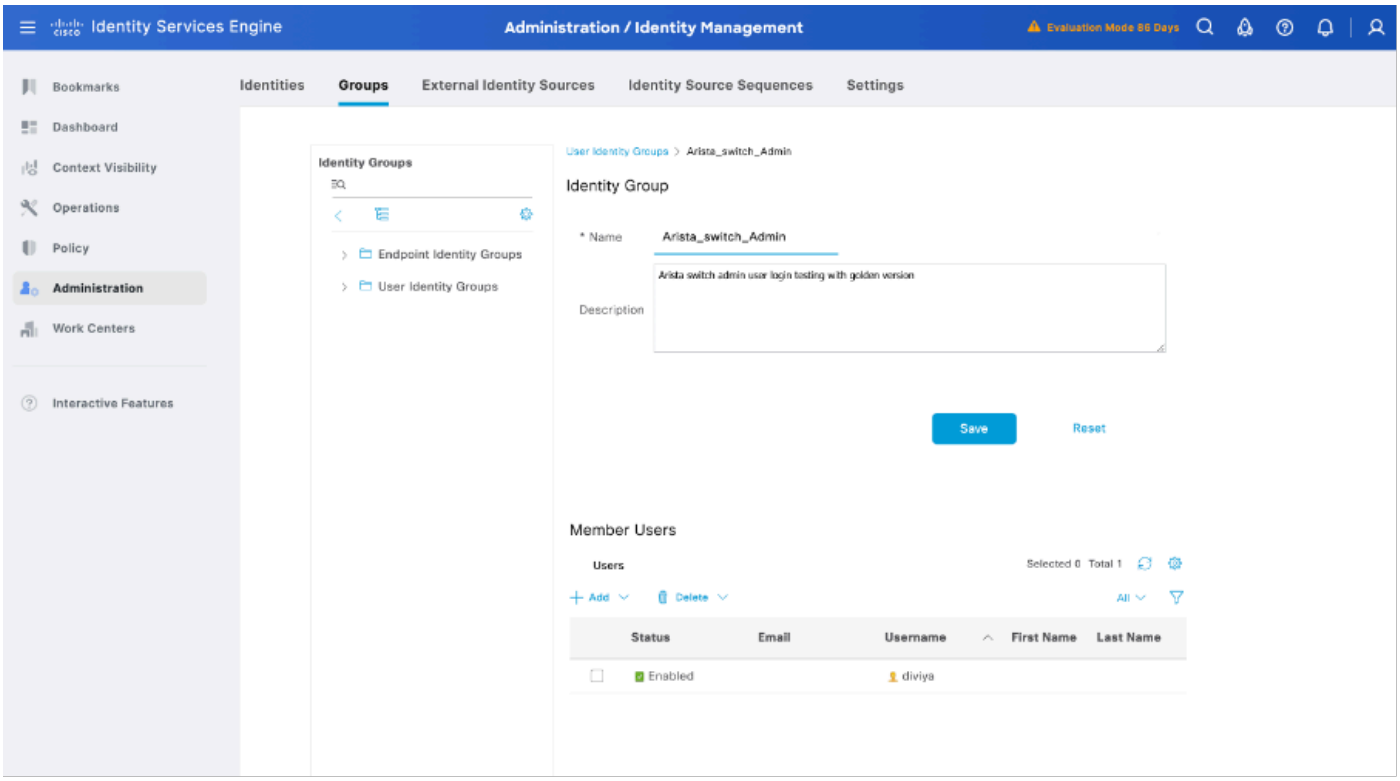
Paso 4. Crear los grupos de identidad de usuario necesarios

Vaya a Administration > Identity Management > Groups > User Identity Groups > + Add:



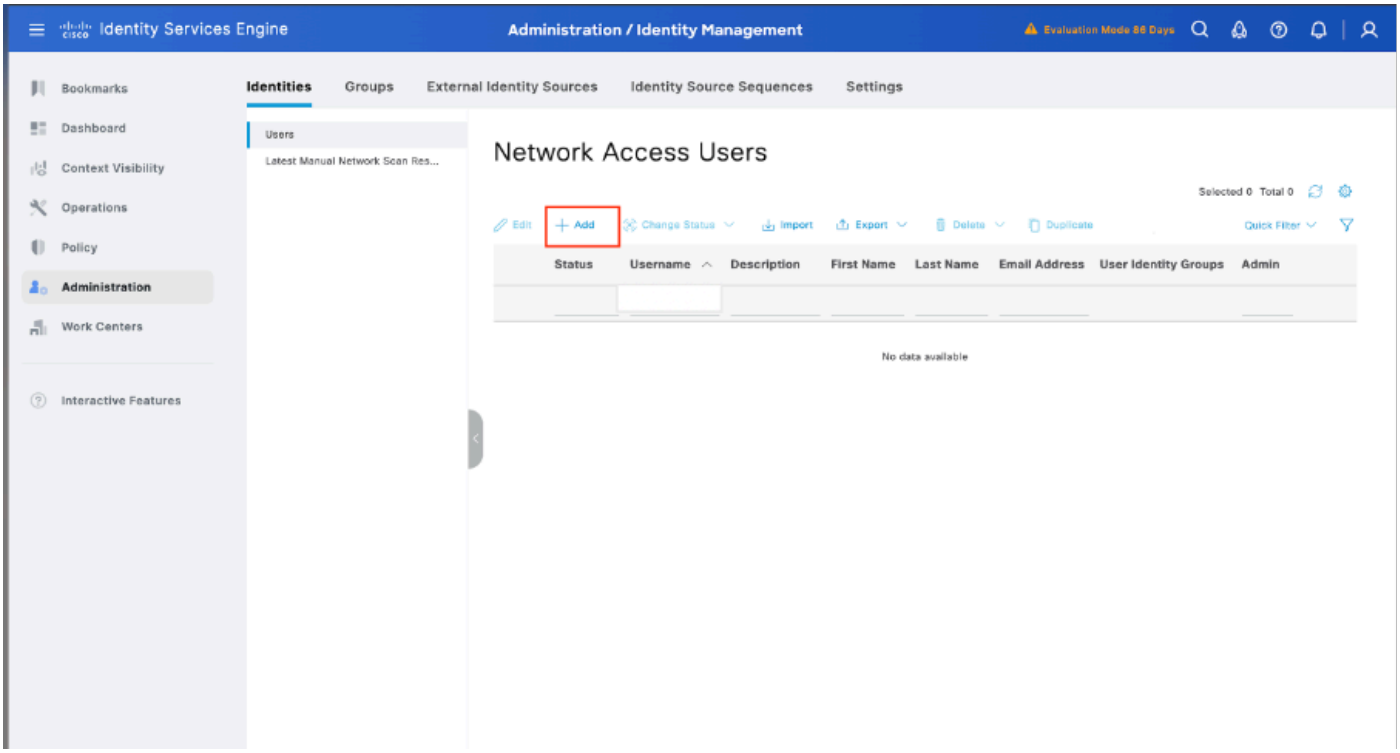
Paso 5. Establezca un nombre para el grupo de identidad de usuario de administrador

Haga clic en Submit para guardar la configuración:

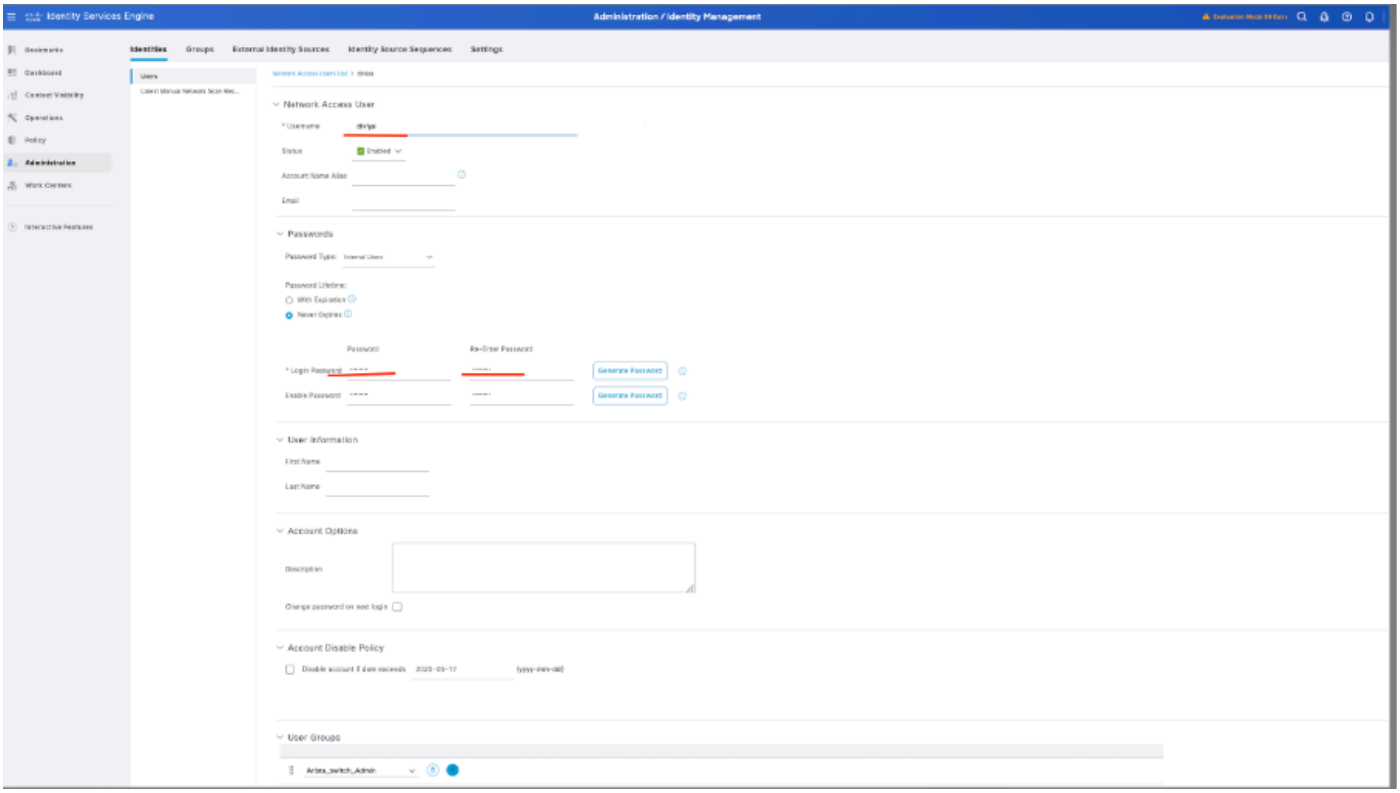


Paso 6. Crear los usuarios locales y agregarlos a su grupo correspondiente

Vaya a Administration > Identity Management > Identities > + Add:



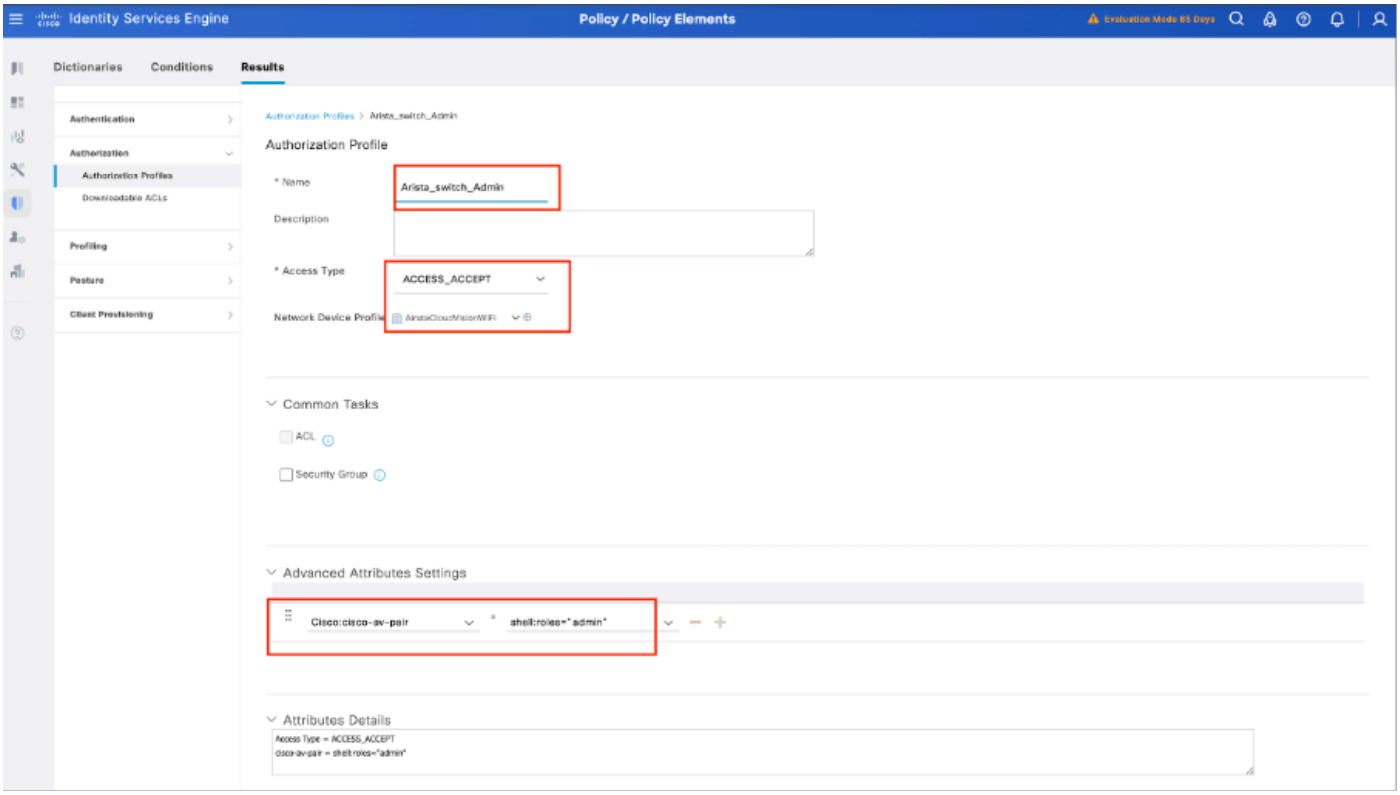
6.1. Añada el usuario con derechos de administrador. Establezca un nombre y una contraseña y asígneselos a Arista_switch_Admin, desplácese hacia abajo y haga clic en Enviar para guardar los cambios.



Paso 7. Crear el perfil de autorización para el usuario administrador

Vaya a Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización > +Agregar.

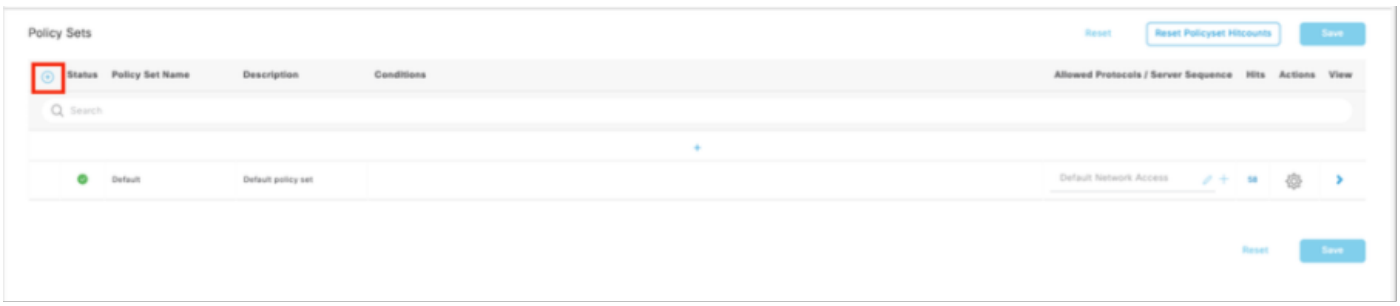
Defina un nombre para el perfil de autorización, deje el tipo de acceso como ACCESS_ACCEPT y en Advanced Attributes Settings agregue cisco-av-pair=shell:roles="admin" con y haga clic en Submit.



Paso 8. Crear un conjunto de políticas que coincida con la dirección IP del switch Arista

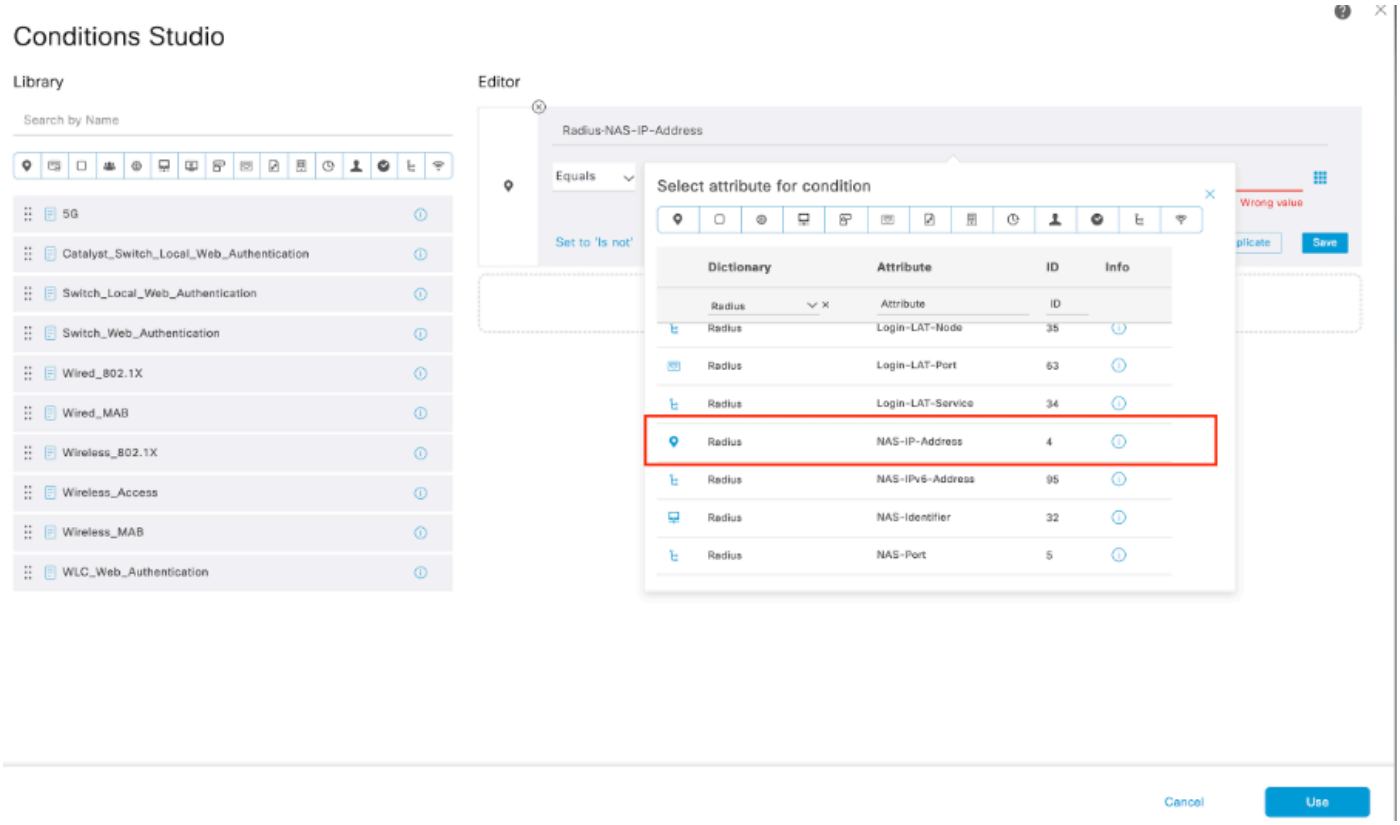
Esto es para evitar que otros dispositivos concedan acceso a los usuarios.

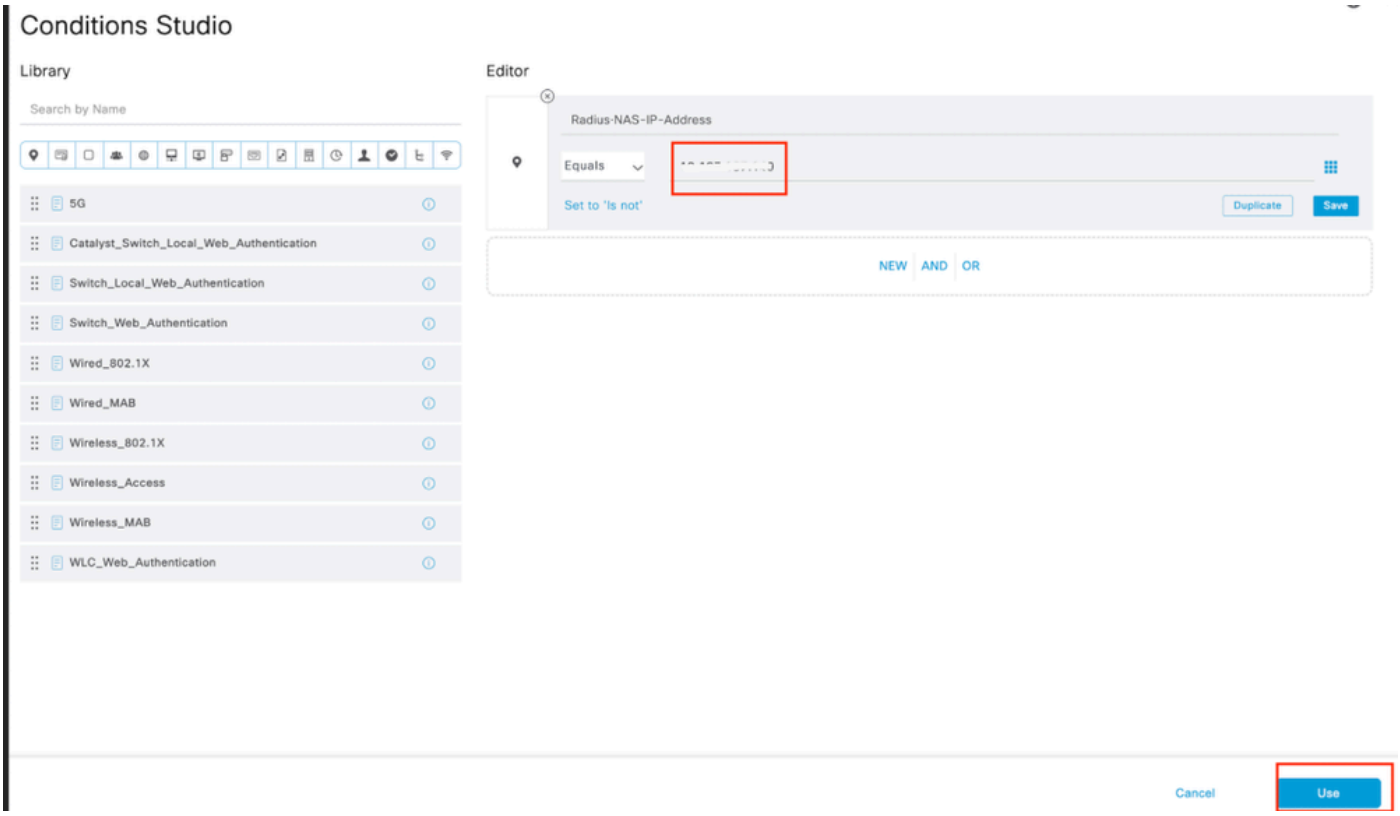
Vaya a Policy > Policy Sets >Add icon sign en la esquina superior izquierda.



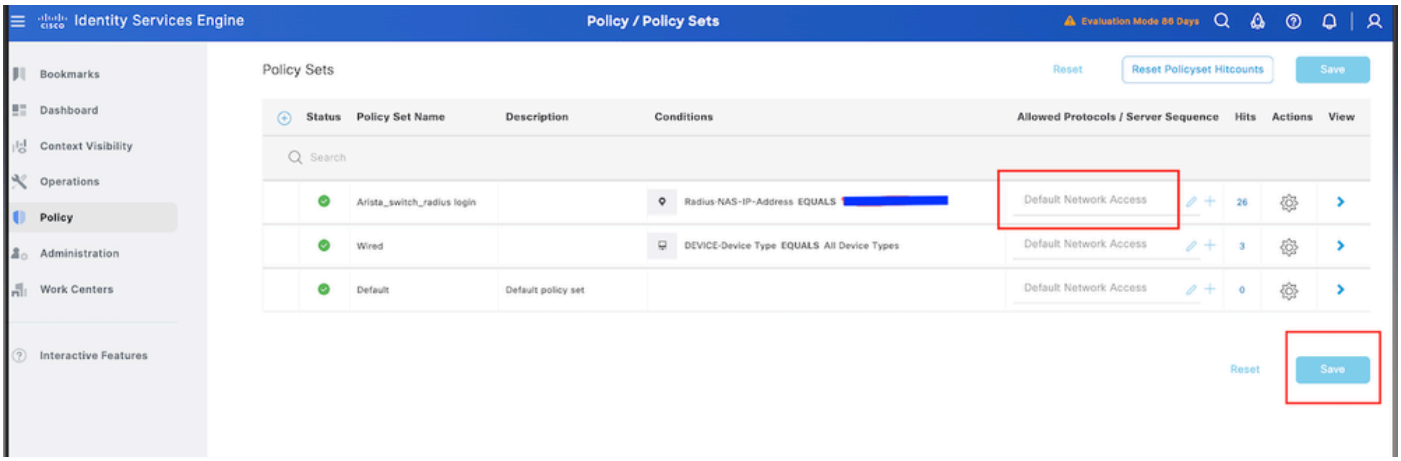
8.1 Se coloca una nueva línea en la parte superior de los conjuntos de políticas. Haga clic en el icono Add para configurar una nueva condición.

8.2 Agregue una condición superior para el atributo RADIUS NAS-IP-Address que coincida con la dirección IP del switch de Arista, luego haga clic en Use.





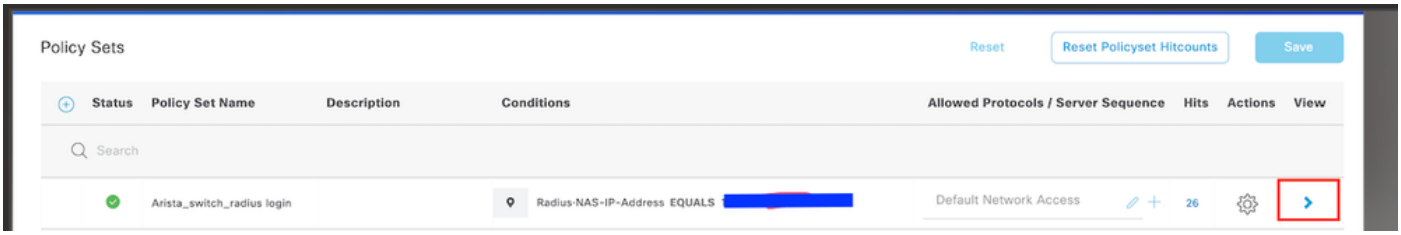
8.3 Una vez completado, haga clic en Guardar:



Consejo: Para este ejercicio hemos permitido la lista Default Network Access Protocols . Puede crear una lista nueva y reducirla según sea necesario.

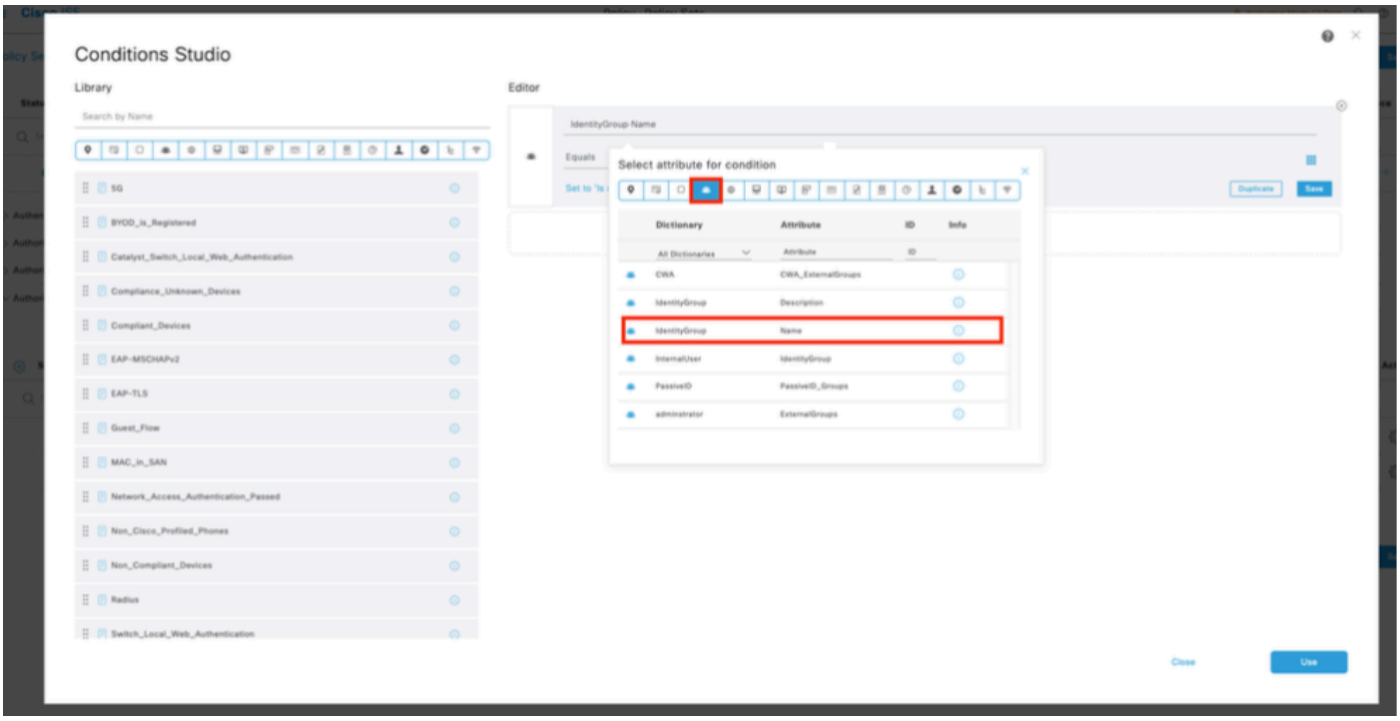
Paso 9. Ver el nuevo conjunto de políticas

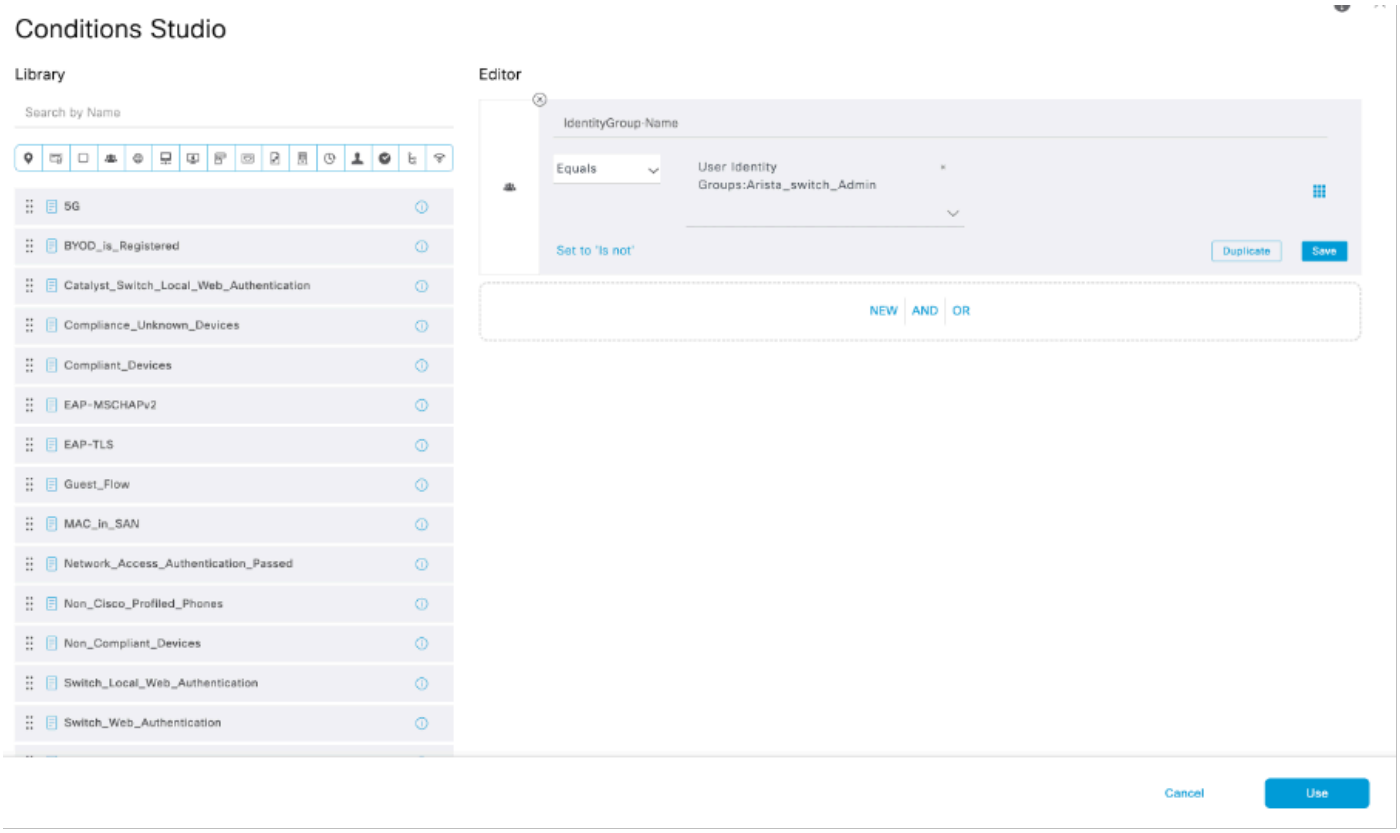
Haga clic en el icono > situado al final de la fila:



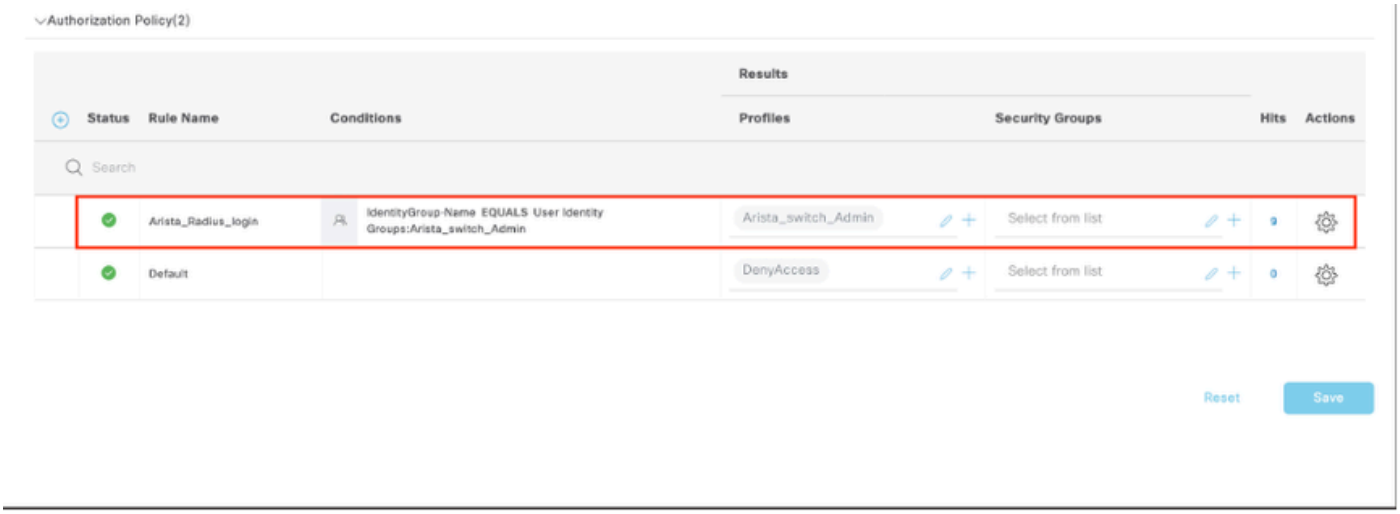
9.1 Expanda el menú Authorization Policy y haga clic en (+) para agregar una nueva condición.

9.2 Establezca las condiciones para que coincidan con el Grupo de Identidad de Diccionario con Nombre de Atributo Igual a Grupos de Identidad de Usuario: Arista_switch_Admin (el nombre de grupo creado en el paso 7) y haga clic en Usar.





9.3 Valide que la nueva condición esté configurada en la política de autorización, luego agregue un perfil de usuario en Perfiles:



Configuración del switch Arista

Paso 1. Habilite la autenticación RADIUS

Inicie sesión en el switch Arista e ingrese al modo de configuración:

configurar

!

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

```
radius-server timeout 5
radius-server retransmit 3
radius-server deadtime 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 default start-stop group ISE
aaa accounting commands 15 default start-stop group ISE
aaa accounting system default start-stop group ISE
!
```

Finalizar

Paso 2. Guardar configuración

Para conservar la configuración tras los reinicios:

```
memoria de escritura
```

or

```
copy running-config startup-config
```

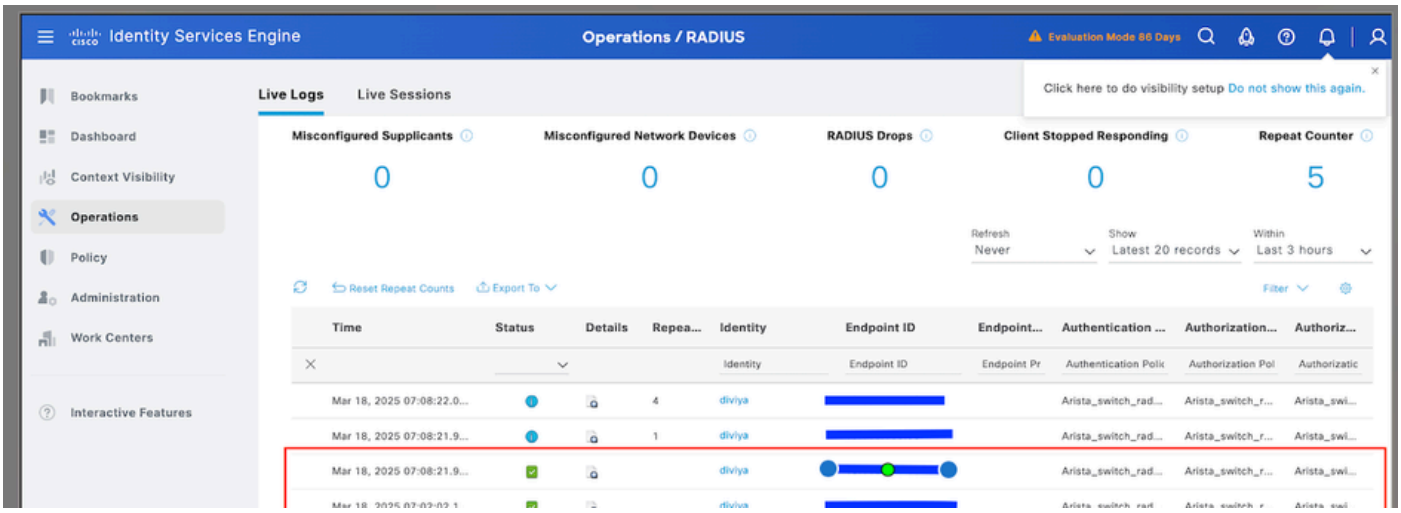
Verificación

Revisión de ISE

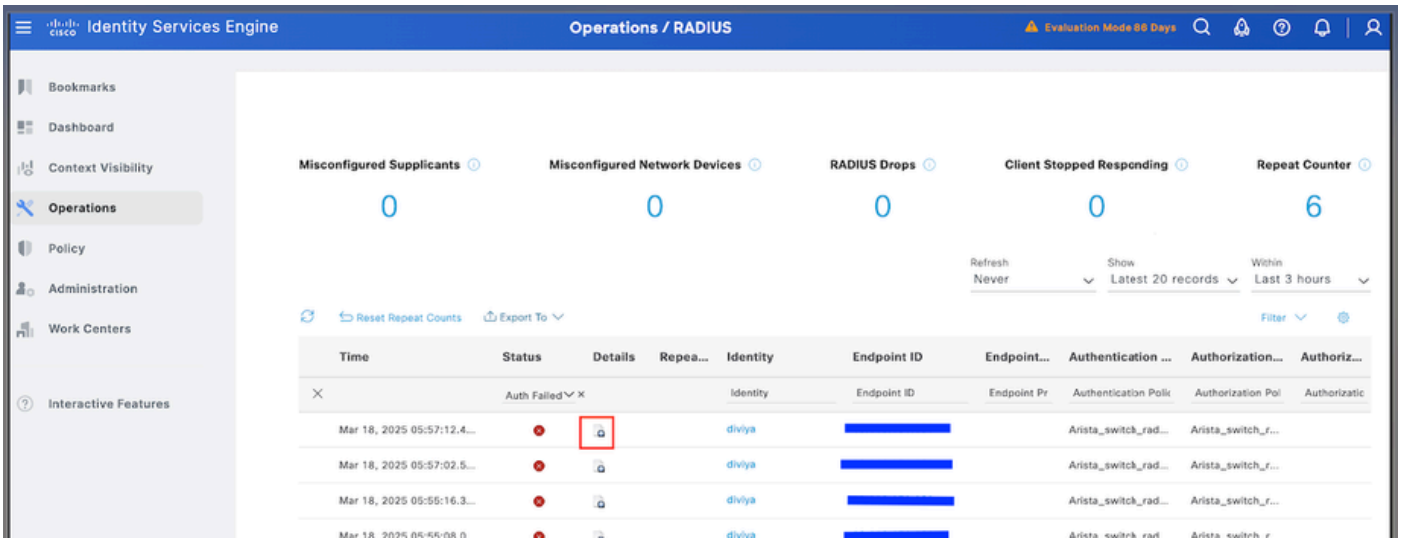
1. Intente iniciar sesión en el switch de Arista con las nuevas credenciales de Radius:

    1.1 Navegue hasta Operaciones > Radio > Registros en vivo.

    1.2 La información mostrada muestra si un usuario ha iniciado sesión correctamente.



2. Para obtener información sobre el estado de fallo, revise los detalles de la sesión:

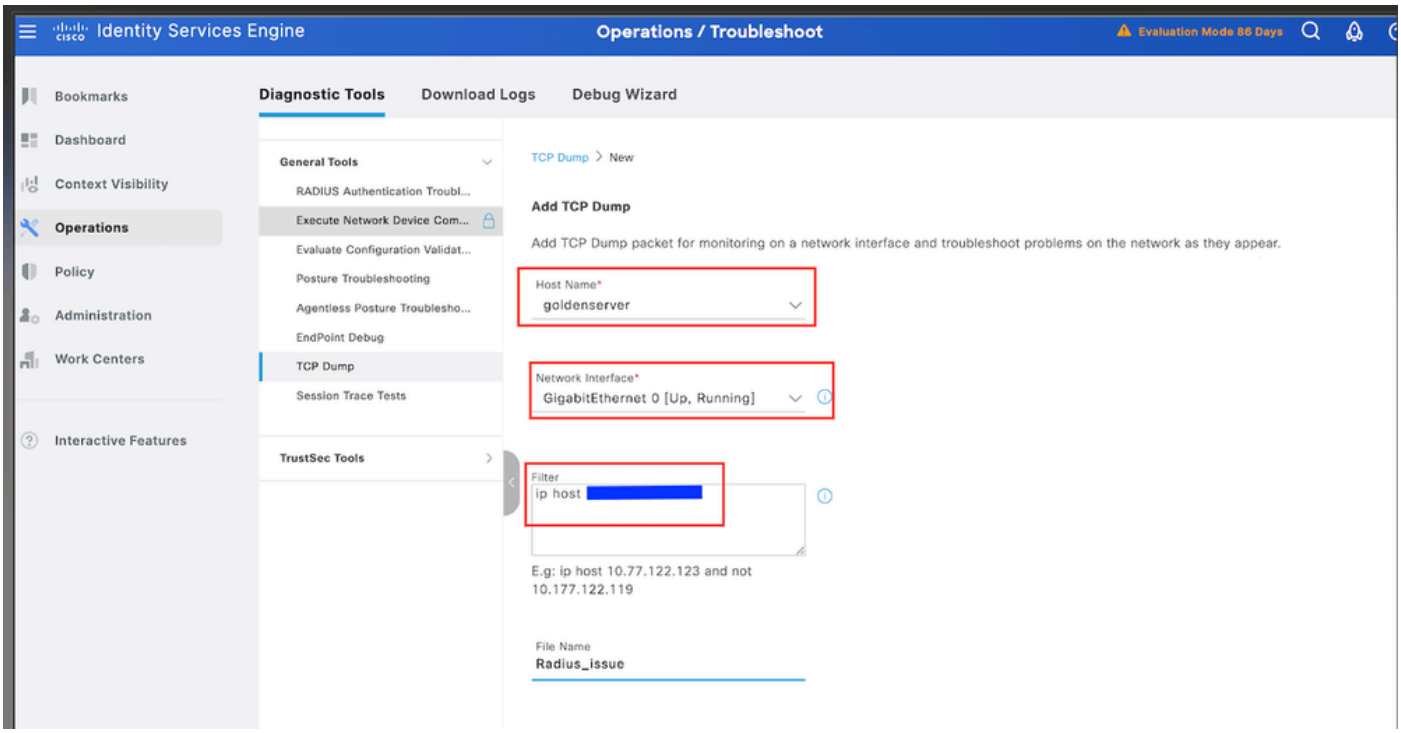


3. Para las solicitudes que no se muestran en los registros de Radius Live , revise si la solicitud UDP está llegando al nodo ISE a través de una captura de paquetes.

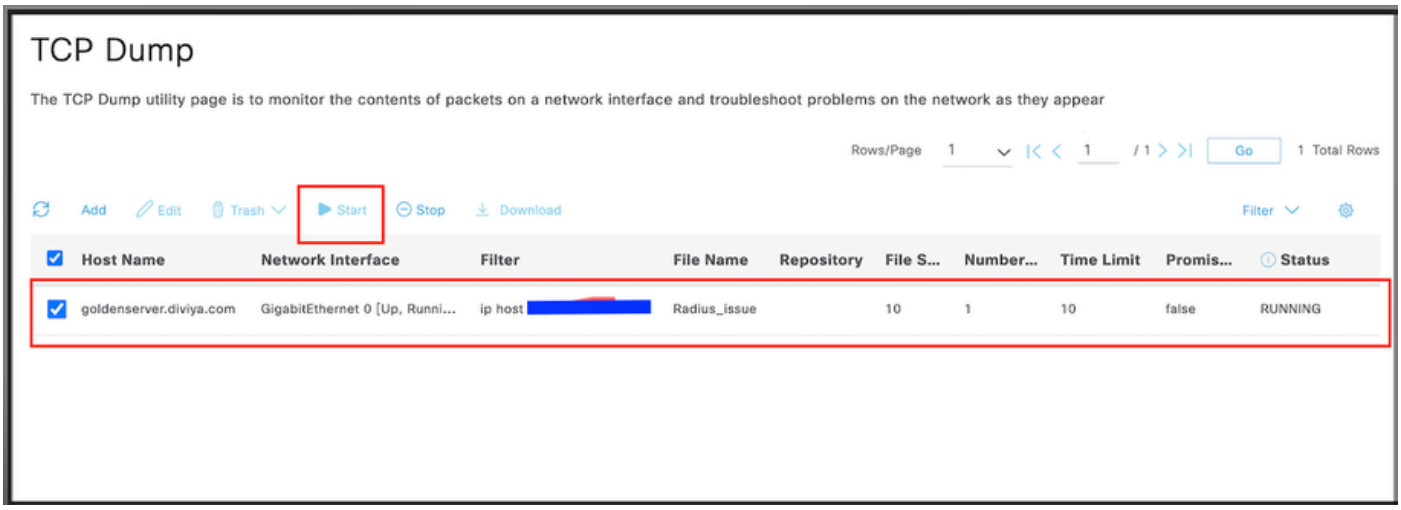
3.1. Vaya a Operaciones > Solución de problemas > Herramientas de diagnóstico > Volcado de TCP.

3.2. Agregue una nueva captura y descargue el archivo en su máquina local para revisar si los paquetes UDP llegan al nodo ISE.

3.3. Rellene la información solicitada, desplácese hacia abajo y haga clic en Guardar.



3.4. Seleccione e inicie la captura.



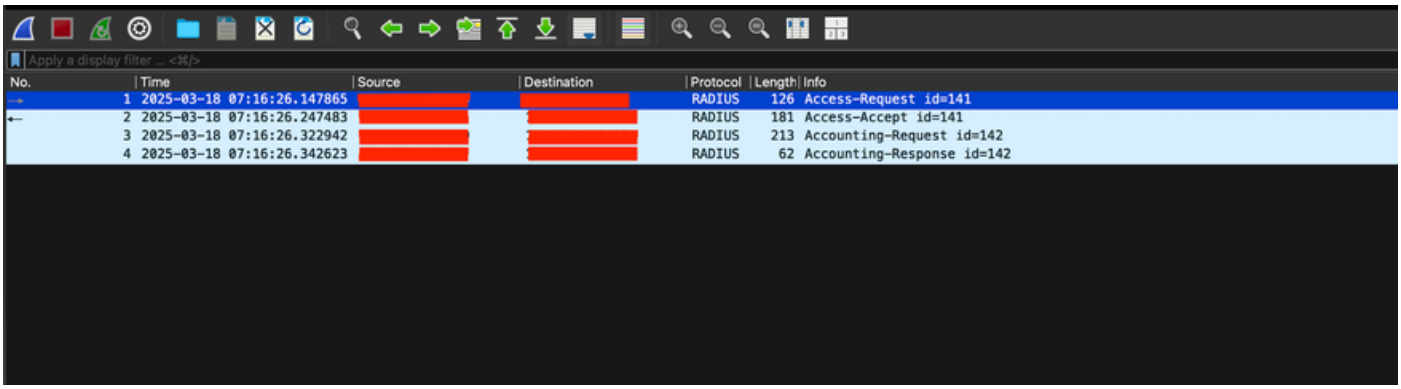
3.5. Intente iniciar sesión en el switch Arista mientras se ejecuta la captura de ISE.

3.6. Detenga el volcado de TCP en ISE y descargue el archivo en un equipo local.

3.7. Revisar la salida del tráfico.

Resultado esperado:

Paquete n.º 1. Solicitud del switch Arista al servidor ISE a través del puerto 1812 (RADIUS).
Paquete n.º 2. Respuesta del servidor ISE aceptando la solicitud inicial.



Resolución de problemas

Situación 1. "Solicitud 5405 RADIUS rechazada"

Problema

Este escenario implica la solución de problemas de un error "5405 RADIUS Request dropped" (Solicitud de RADIUS rechazada 5405) con el motivo "11007 Failed locate Network Device or AAA Client" (no se pudo encontrar el dispositivo de red o el cliente AAA) en Cisco ISE cuando un dispositivo de red (como un switch Arista) intenta autenticarse.

Posibles Causas

- Cisco Identity Services Engine (ISE) no puede identificar el switch Arista porque su dirección IP no figura entre los dispositivos de red conocidos.
- La solicitud RADIUS proviene de una dirección IP que ISE no reconoce como un dispositivo de red o cliente AAA válido.
- Puede haber una discordancia en la configuración entre el switch y el ISE (como una IP incorrecta o un secreto compartido).

Solución

- Agregue el switch a la lista de dispositivos de red de Cisco ISE con la dirección IP correcta.
- Verifique que la dirección IP y el secreto compartido configurados en ISE coincidan exactamente con lo establecido en el switch.
- Una vez corregida, la solicitud RADIUS debe reconocerse y procesarse correctamente.

Situación 2: el switch Arista no puede conmutar por error para realizar una copia de seguridad de ISE PSN

Problema

Un switch Arista está configurado para utilizar Cisco ISE para la autenticación RADIUS. Cuando el nodo de servicios de políticas (PSN) principal de ISE deja de estar disponible, el switch no conmuta por error automáticamente a un PSN de copia de seguridad. Como resultado, los registros de autenticación solo aparecen desde el PSN de ISE principal y no hay registros desde el PSN secundario/de respaldo cuando el primario está inactivo.

Posibles Causas

- La configuración del servidor RADIUS del switch Arista solo apunta al nodo ISE principal, por lo que no se utilizan servidores de copia de seguridad.
- La prioridad del servidor RADIUS no está establecida correctamente o falta la IP de ISE de copia de seguridad en la configuración.
- Los valores de tiempo de espera y retransmisión en el switch se establecen en un nivel demasiado bajo, lo que impide que se realice correctamente el repliegue a PSN de respaldo.
- El switch utiliza un FQDN para el PSN, pero la resolución de DNS no devuelve todos los registros A, lo que hace que solo se establezca contacto con el servidor principal.

Solución

- Asegúrese de introducir varias IP PSN de ISE en la configuración del grupo de servidores RADIUS del switch. Esto permite que el switch utilice el ISE PSN de respaldo si el primario es inalcanzable.

  Ejemplo de configuración:

  radius-server host <ISE1-IP> key <secret>

  radius-server host <ISE2-IP> key <secret>

- Verifique que la prioridad del servidor RADIUS, el tiempo de espera y los valores de retransmisión estén correctamente configurados para una conmutación por fallas confiable.
- Si utiliza FQDN, compruebe la configuración y la resolución de DNS para asegurarse de que el switch devuelve y utiliza todas las direcciones IP de PSN.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).