在Arista交換機上配置基於RADIUS的管理員登入

目錄

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)以使用RADIUS驗證Arista交換機上的管理員登入。

必要條件

需求

繼續之前，請確保：

- 思科ISE（推薦版本3.x）已安裝且運行正常。
- 運行EOS且支援RADIUS的Arista交換機。
- ISE中配置的Active Directory(AD)或內部使用者資料庫。

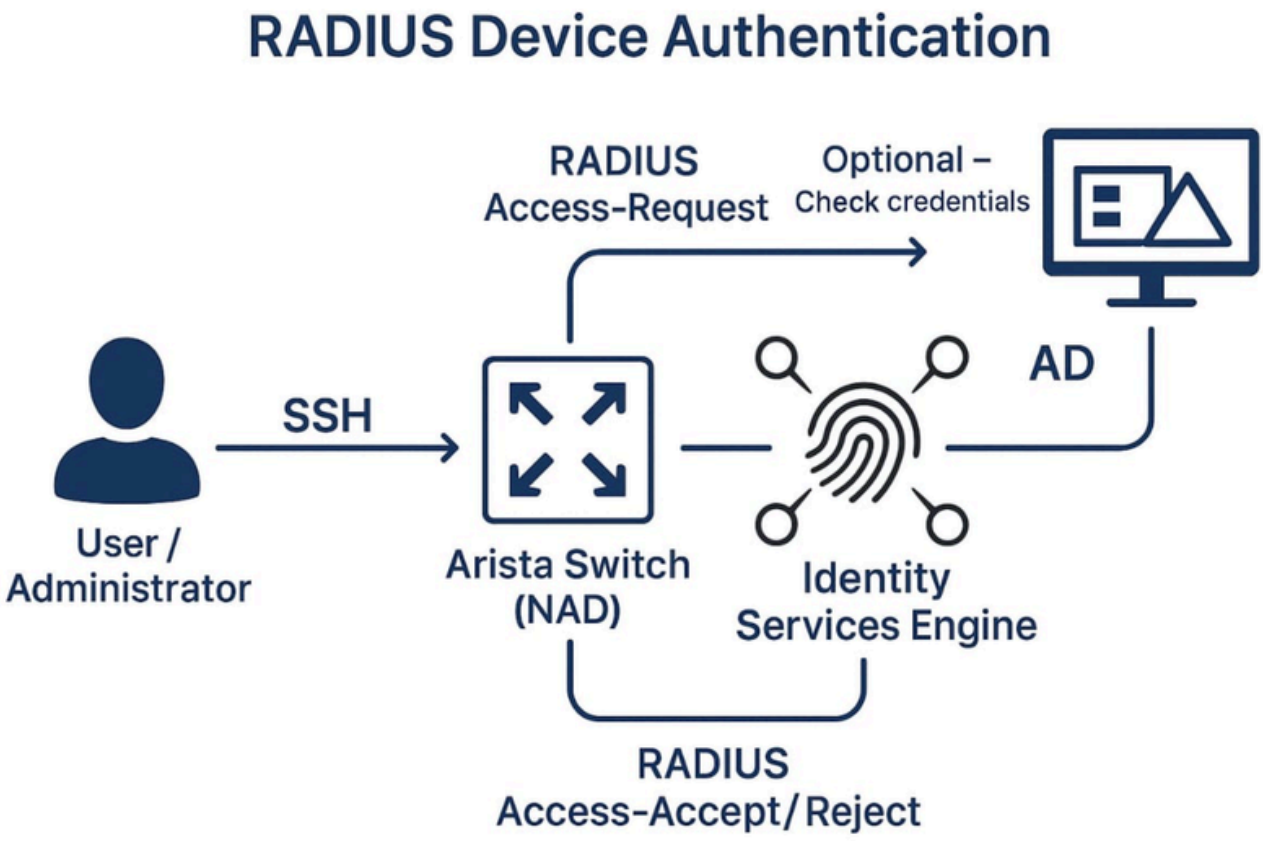
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Arista switch軟體映像版本：4.33.2F
- 思科身分識別服務引擎(ISE)版本3.3補丁4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表



以下網路圖說明使用Cisco ISE對Arista交換機進行基於RADIUS的裝置身份驗證，並將Active Directory(AD)作為可選身份驗證源。

該圖包括：

- Arista交換器（充當網路接入裝置，需要支援）
- Cisco ISE（充當RADIUS伺服器）

- Active Directory(AD)[可選](用於身份驗證)
- 使用者/管理員（通過SSH登入）

設定

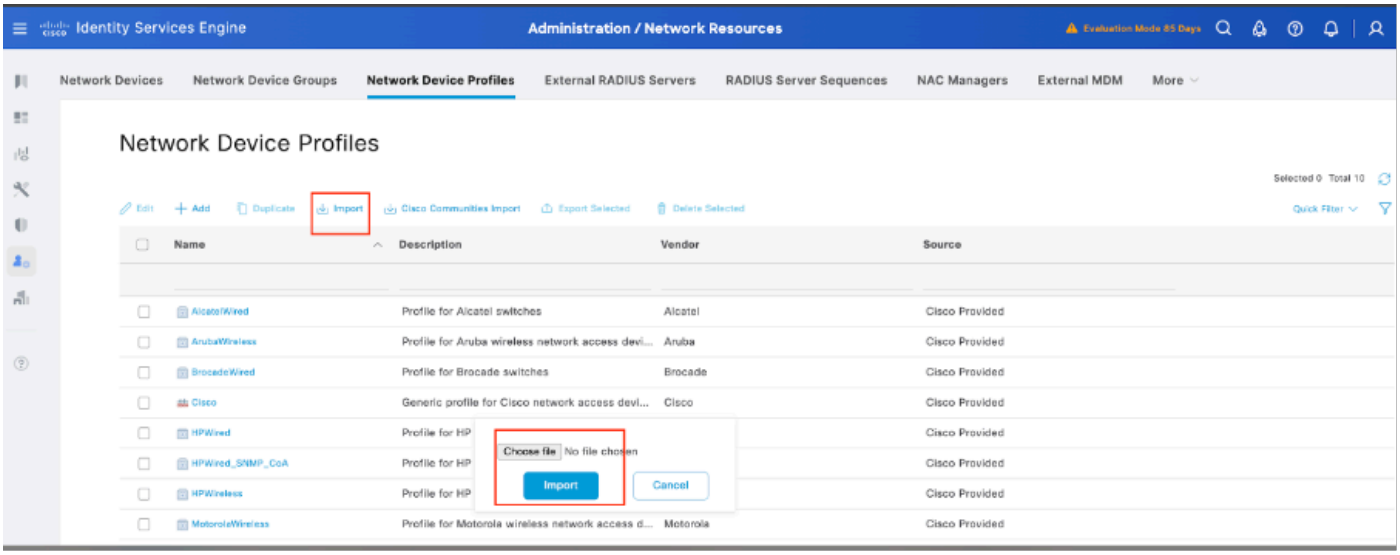
配置Cisco ISE

步驟 1. 獲取思科ISE的Arista網路裝置配置檔案

思科社群已共用Arista裝置的專用NAD配置檔案。此配置檔案以及必要的字典檔案，可在Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration一文中找到。將此配置檔案下載並匯入到ISE設定有助於更順利的整合。

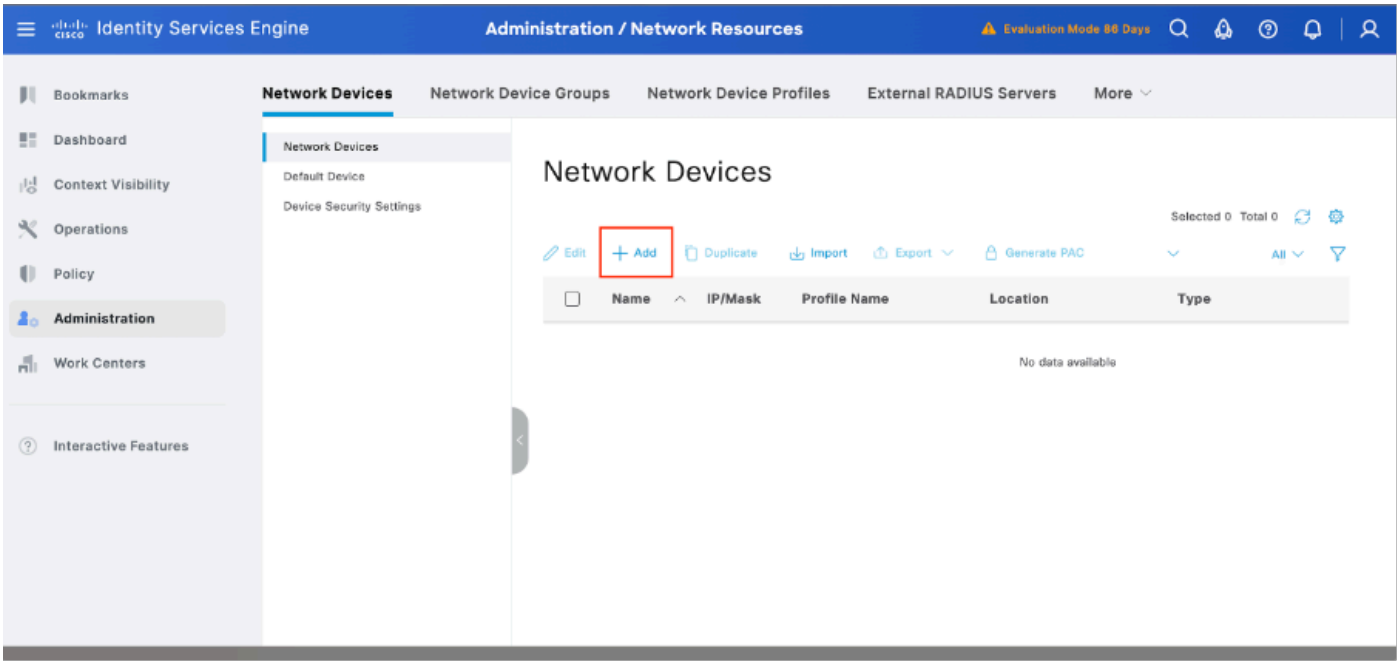
以下是將Arista NAD配置檔案匯入思科ISE的步驟：

1. 下載設定檔：
   - 從上面提供的思科社群連結獲取Arista NAD配置文件。思科社群
2. 訪問思科ISE:
   - 登入到您的Cisco ISE管理控制檯。
3. 匯入NAD配置檔案：
   - 導覽至Administration > Network Resources > Network Device Profiles。
   - 按一下Import按鈕。
   - 上傳下載的Arista NAD配置檔案。



步驟 2. 新增Arista交換機作為網路裝置

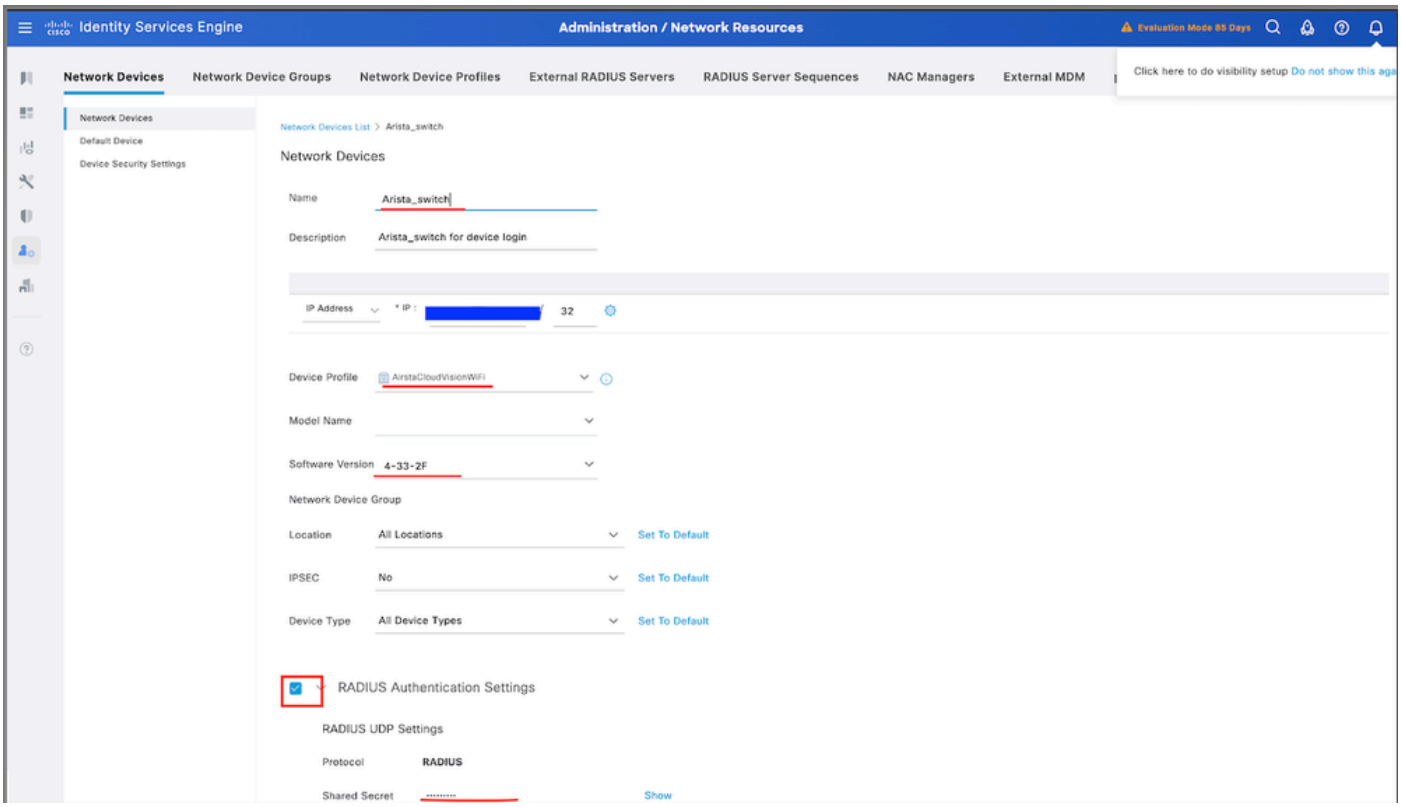
1. 導覽至Administration > Network Resources > Network Devices> +Add。



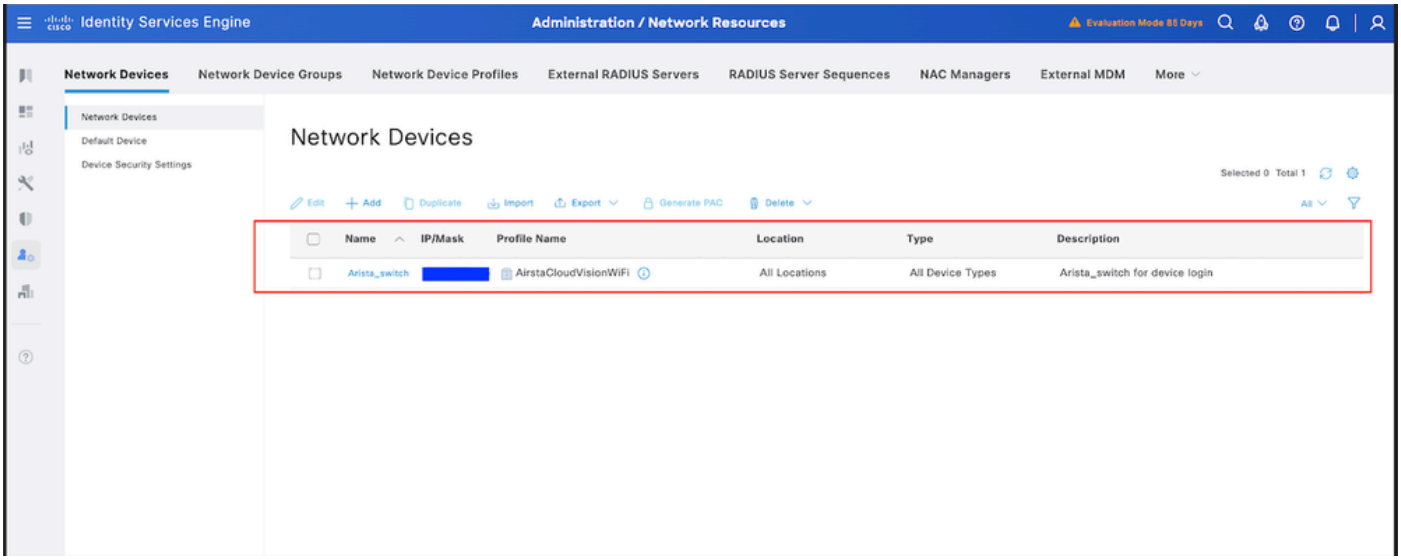
2.按一下Add並輸入以下詳細資訊：

1. 名稱:Arista-Switch
2. IP 位址:<Switch-IP>
3. 裝置型別:選擇其他有線
4. 網路裝置配置檔案:選擇AirstaCloudVisionWiFi。
5. RADIUS驗證設定:
    1. 啟用RADIUS驗證
    2. 輸入Shared Secret（必須與交換機配置匹配）。

3.按一下Save。

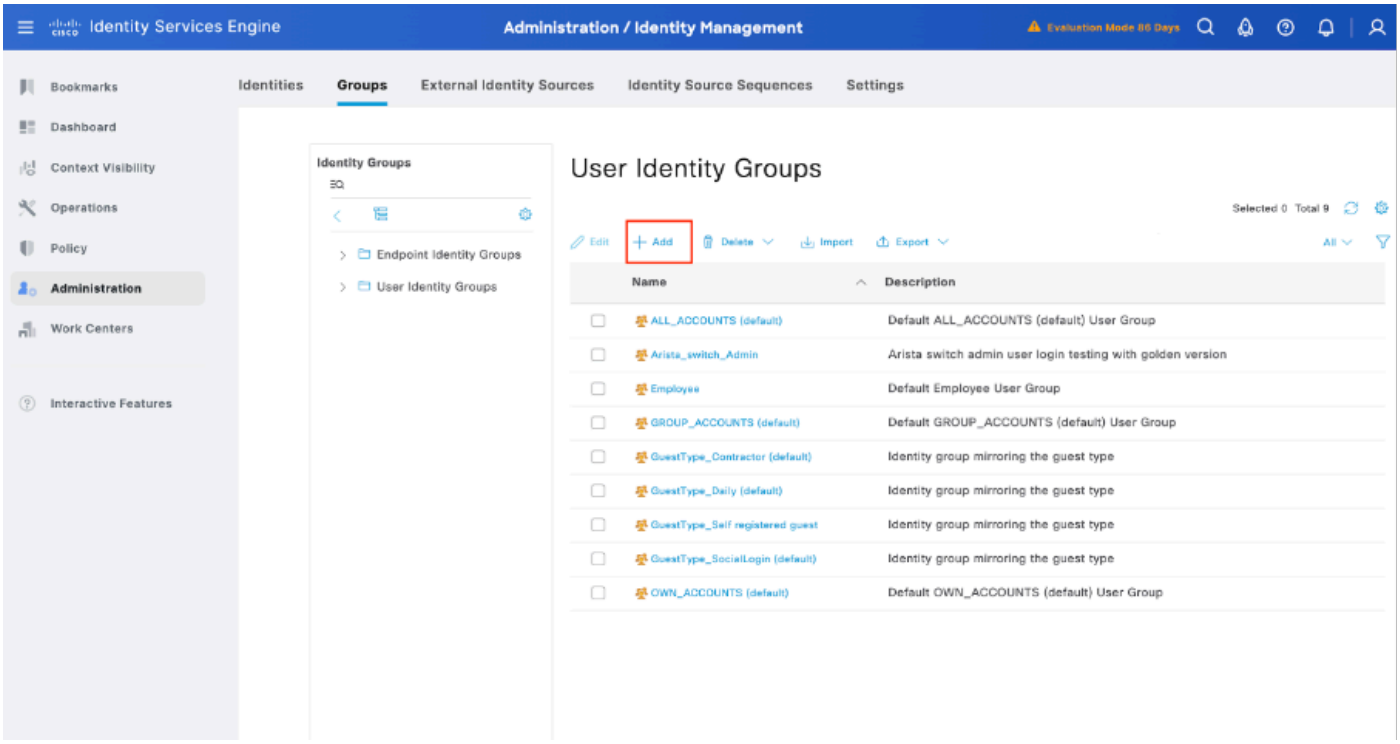


步驟 3. 驗證新裝置是否顯示在「Network Devices（網路裝置）」下



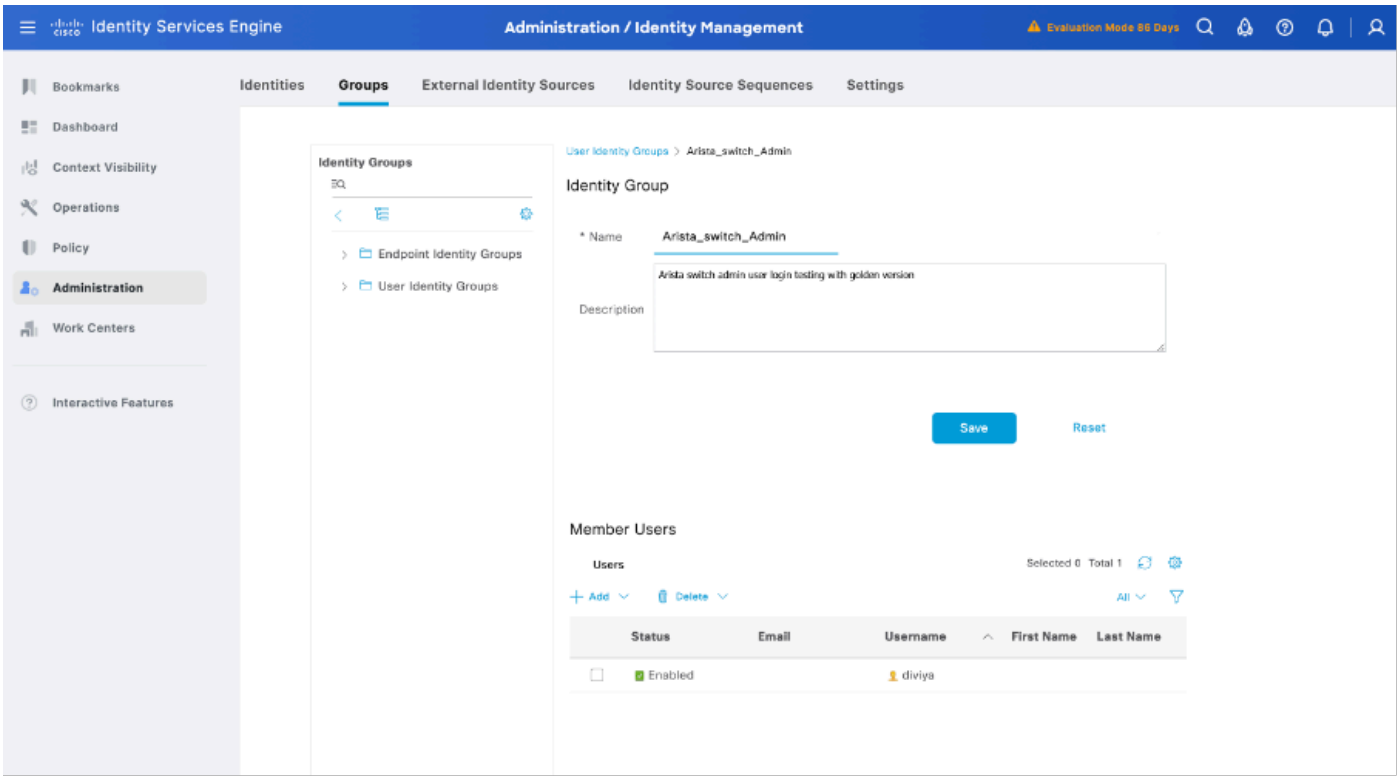
步驟 4. 建立所需的使用者身份組

導航到管理>身份管理>組>使用者身份組> + Add:



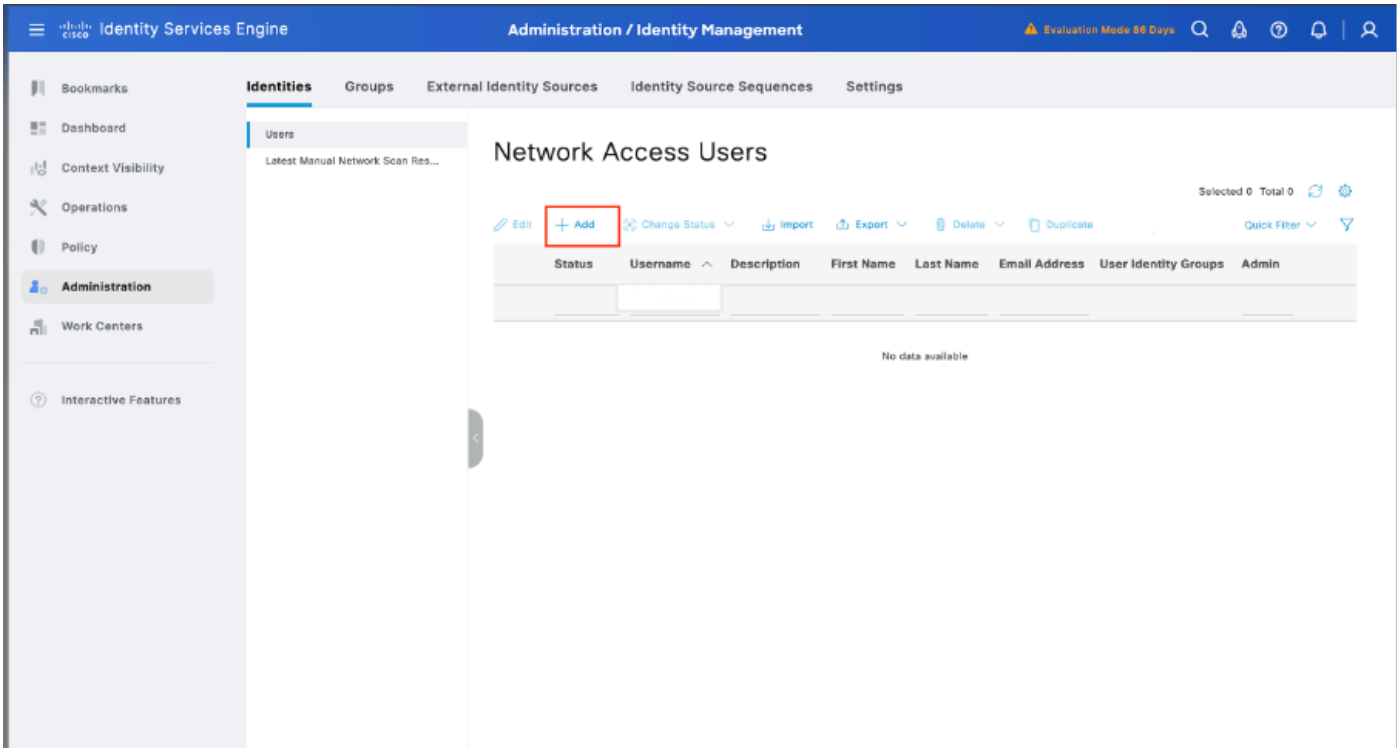
步驟 5. 設定管理員使用者身份組的名稱

按一下Submit以儲存組態：

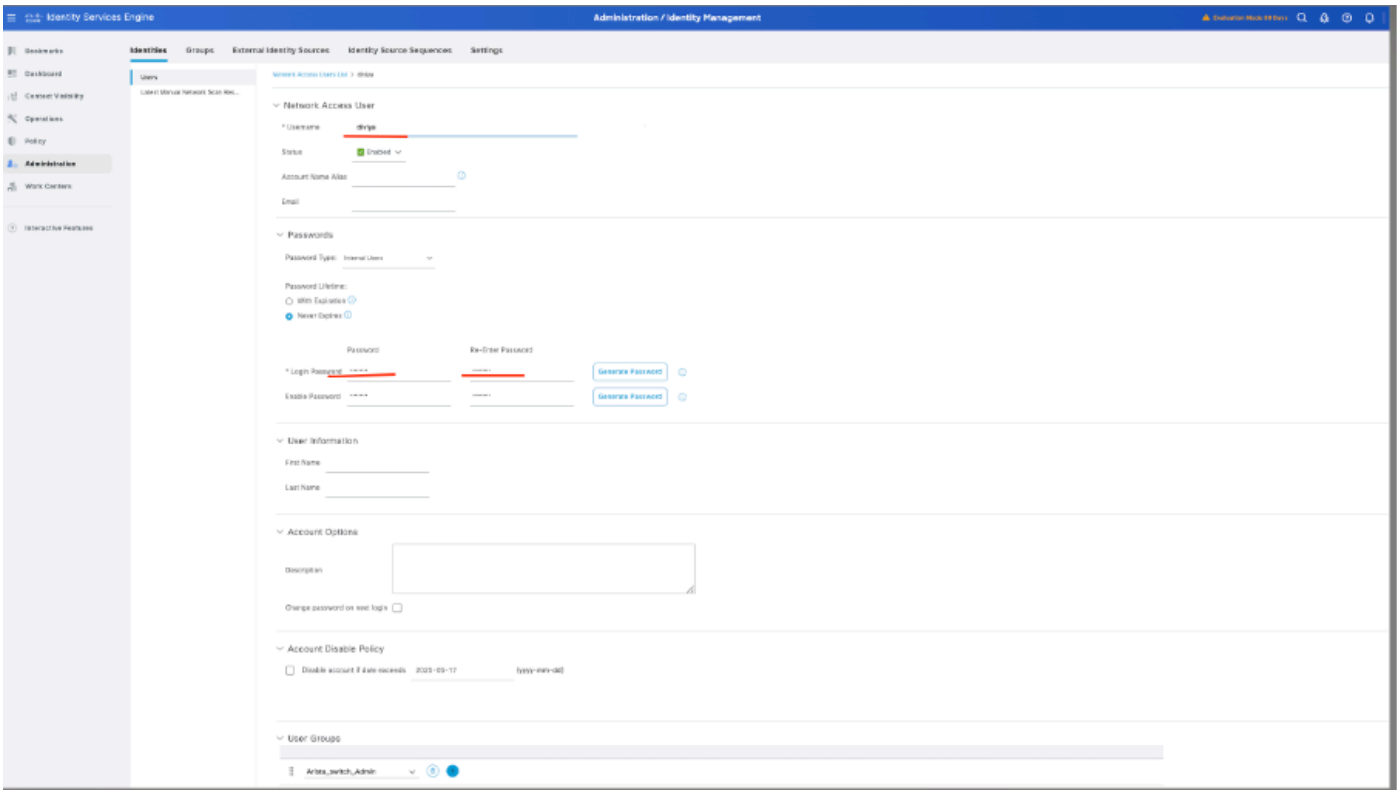


步驟 6. 建立本地使用者並將其新增到其往來行組

導航到管理>身份管理>身份> +新增:



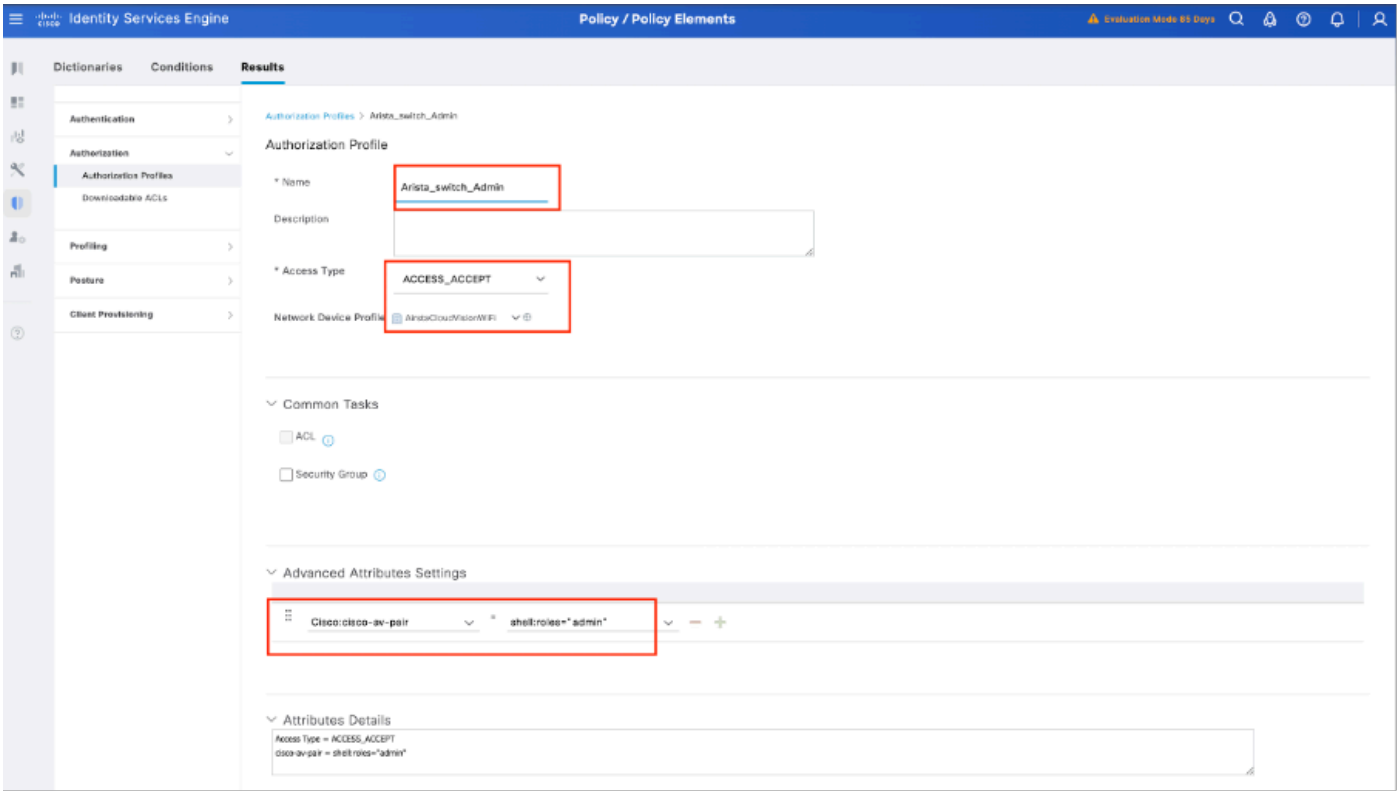
6.1.新增具有管理員許可權的使用者。設定名稱、密碼並將其分配給Arista_switch_Admin，向下滾動並點選Submit以儲存更改。



步驟 7. 為管理員使用者建立授權配置檔案

導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

定義授權配置檔案的名稱，將訪問型別保留為ACCESS_ACCEPT，然後在Advanced Attributes Settings下新增cisco-av-pair=shell:roles="admin"，然後按一下Submit。



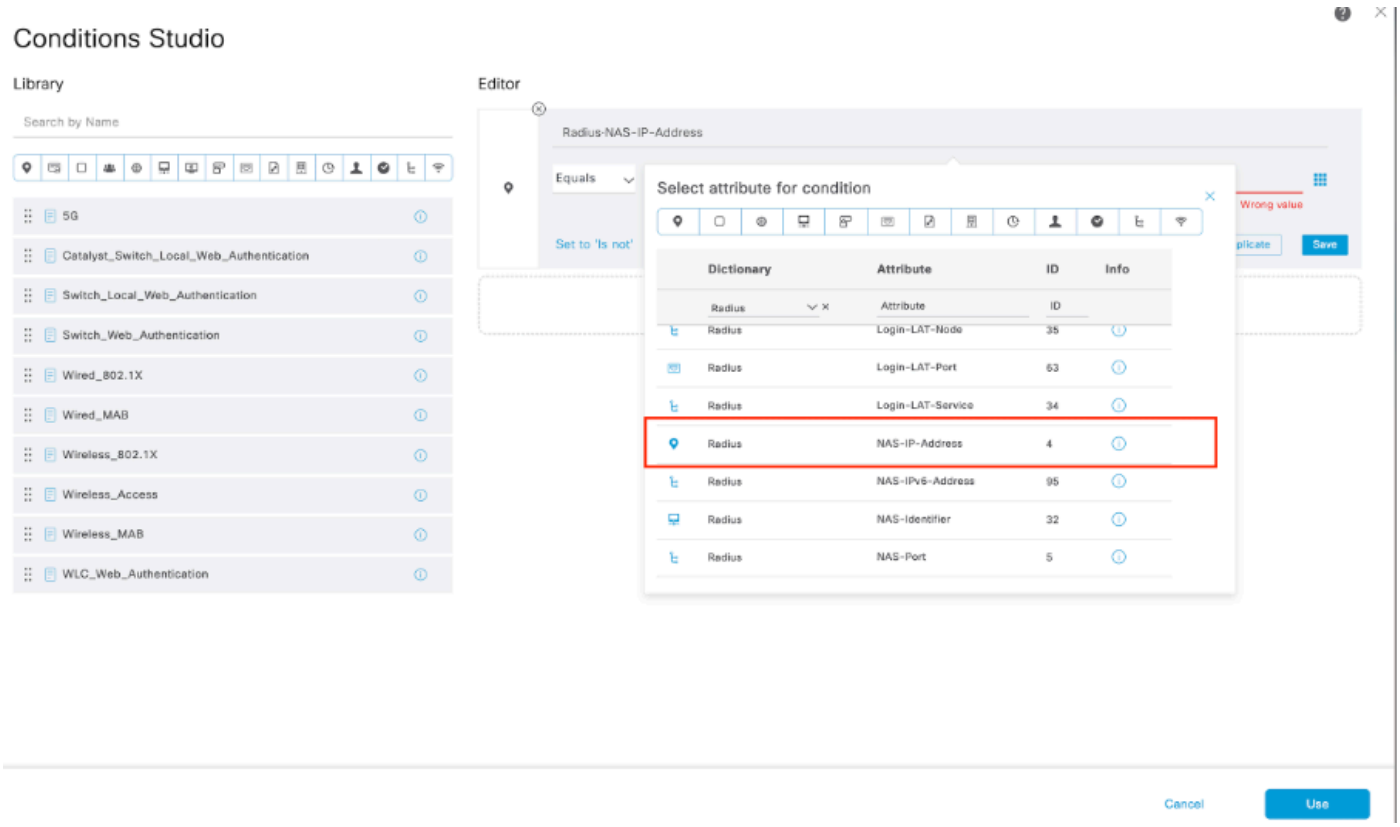
步驟 8. 建立與Arista交換機IP地址匹配的策略集

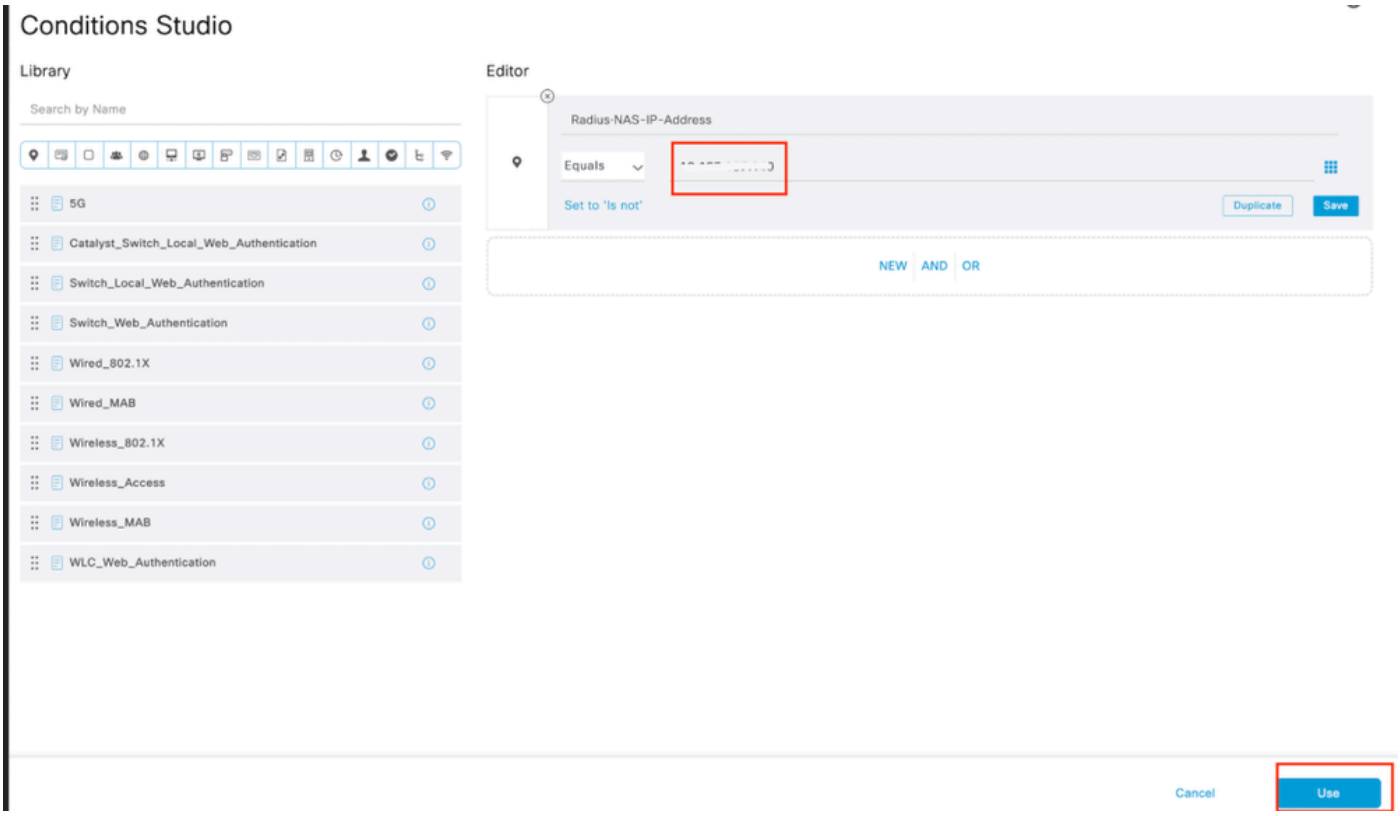
這是為了防止其他裝置向使用者授予訪問許可權。

導航至Policy > Policy Sets > Add icon sign（策略>策略集>新增圖示符號），圖示符號位於左上角。

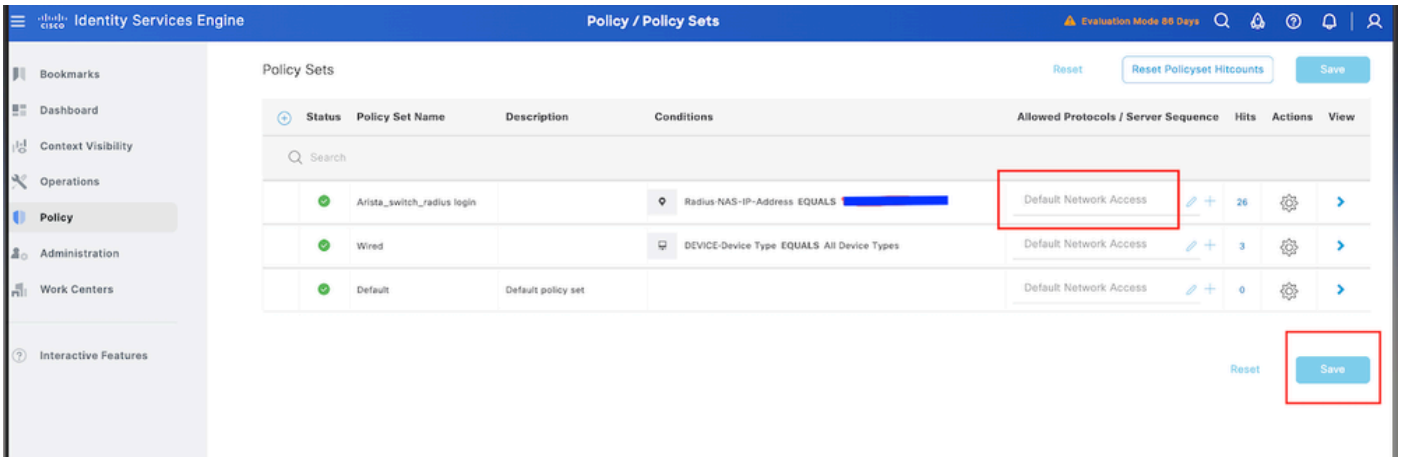
8.1新行位於策略集的頂部。按一下Add圖示配置新條件。

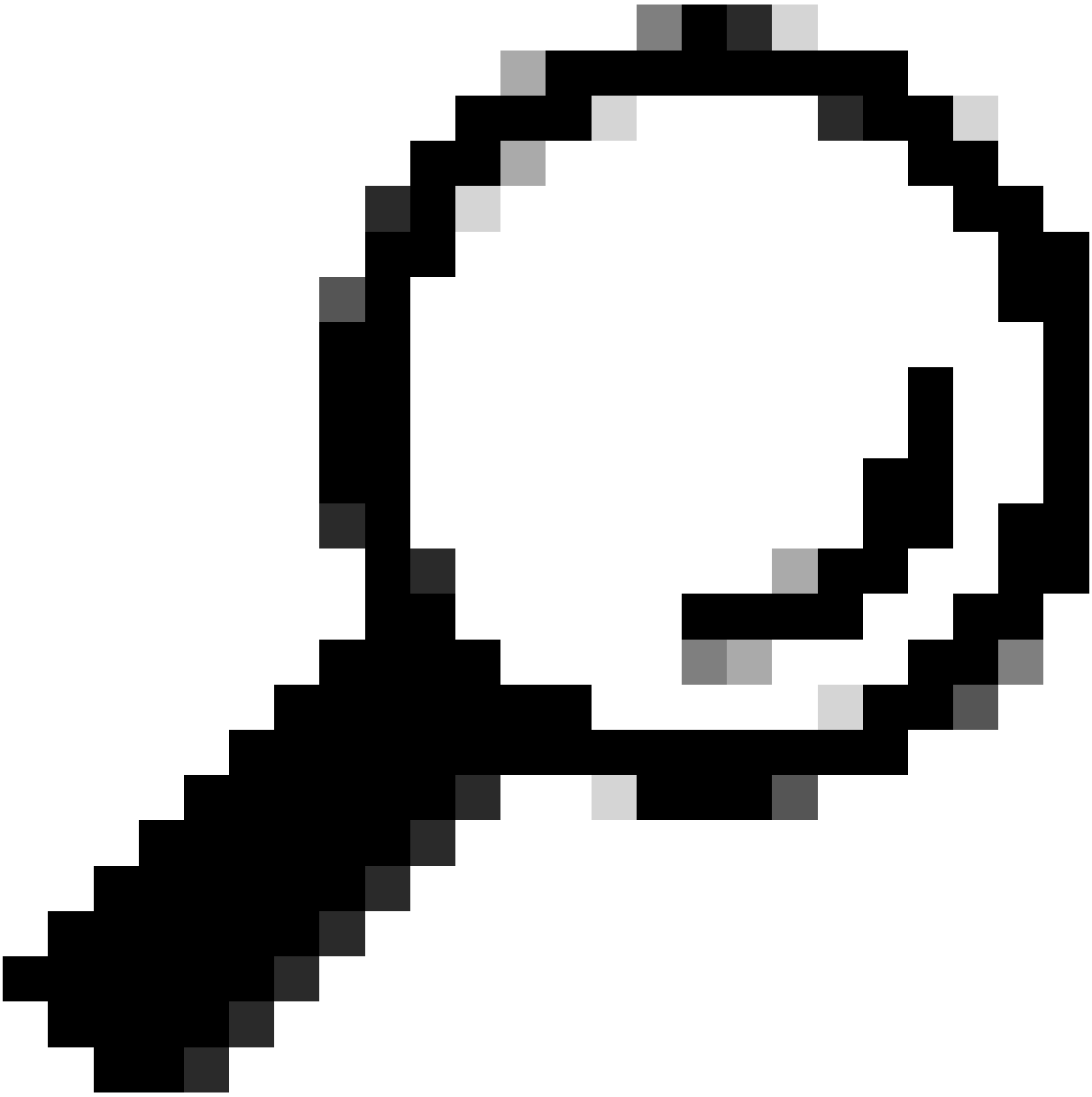
8.2為RADIUS NAS-IP-Address 屬性新增與Arista交換機IP地址匹配的頂部條件，然後按一下Use。





8.3完成後，按一下Save:

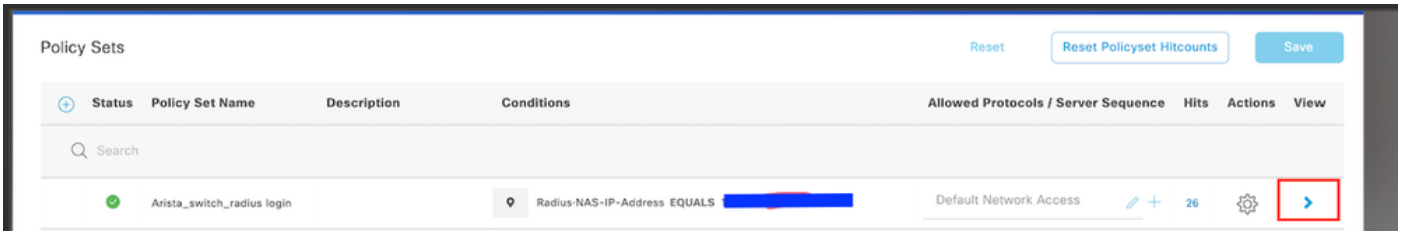




提示：在本練習中，我們允許使用Default Network Access Protocols清單。您可以建立一個新清單並根據需要縮小該清單的範圍。

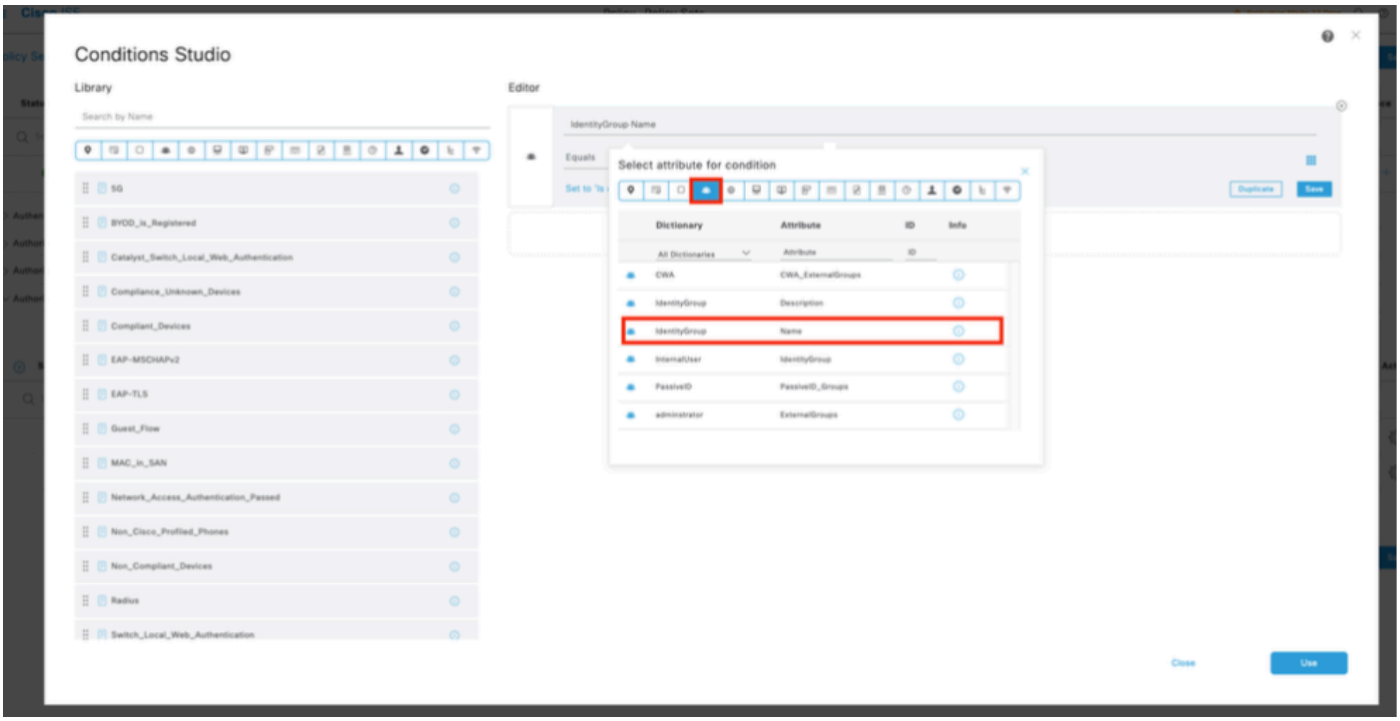
步驟 9. 檢視新策略集

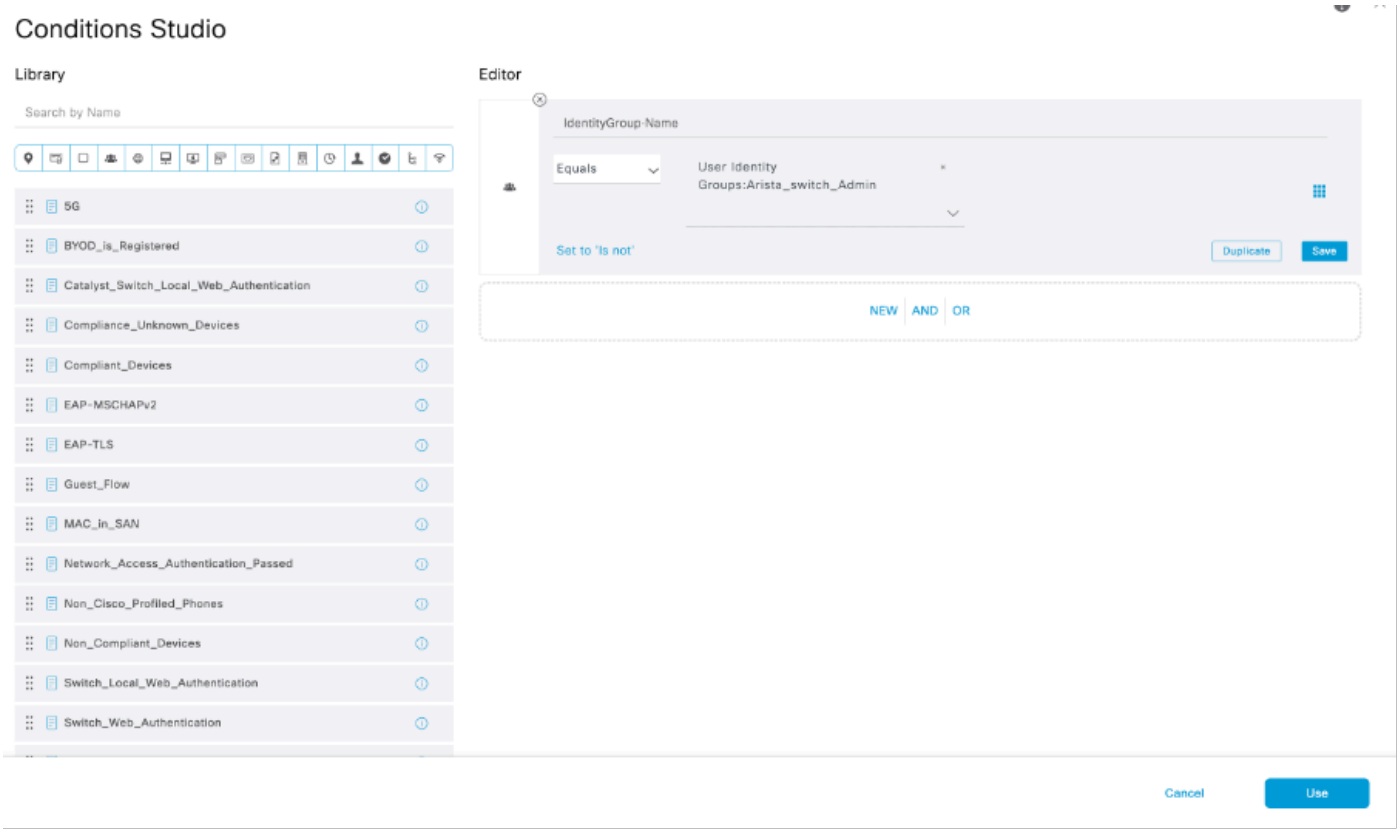
按一下位於行末的>圖示：



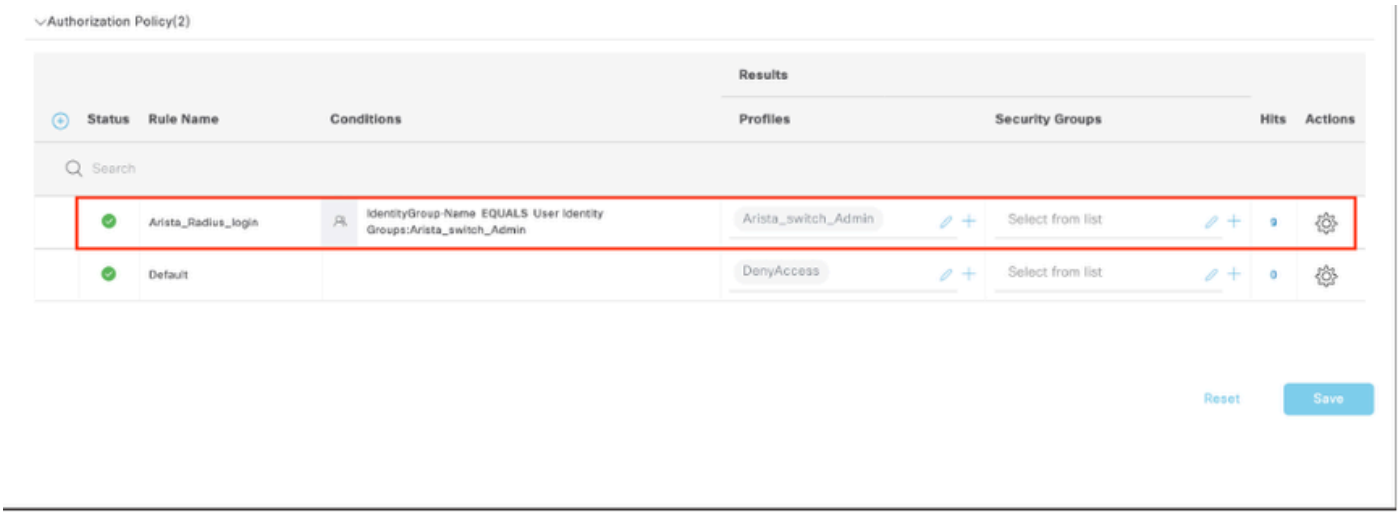
9.1展開Authorization Policy選單，然後按一下(+)新增新條件。

9.2設定條件以匹配Dictionary Identity Group with Attribute Name Equals User Identity Groups:Arista_switch_Admin(在步驟7中建立的組名)，然後點選Use(使用)。





9.3驗證在Authorization policy中配置的新條件，然後在Profiles下新增使用者配置檔案



配置Arista交換機

步驟1.啟用RADIUS身份驗證

登入到Arista switch並進入配置模式：

設定

!

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

radius伺服器逾時5

radius-server retransmit 3

radius-server deadtime 30

!

aaa群組伺服器radius ISE

伺服器<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

!

end

步驟2.儲存配置

要在重新啟動後保留設定，請執行以下操作：

寫記憶體

或

copy running-config startup-config

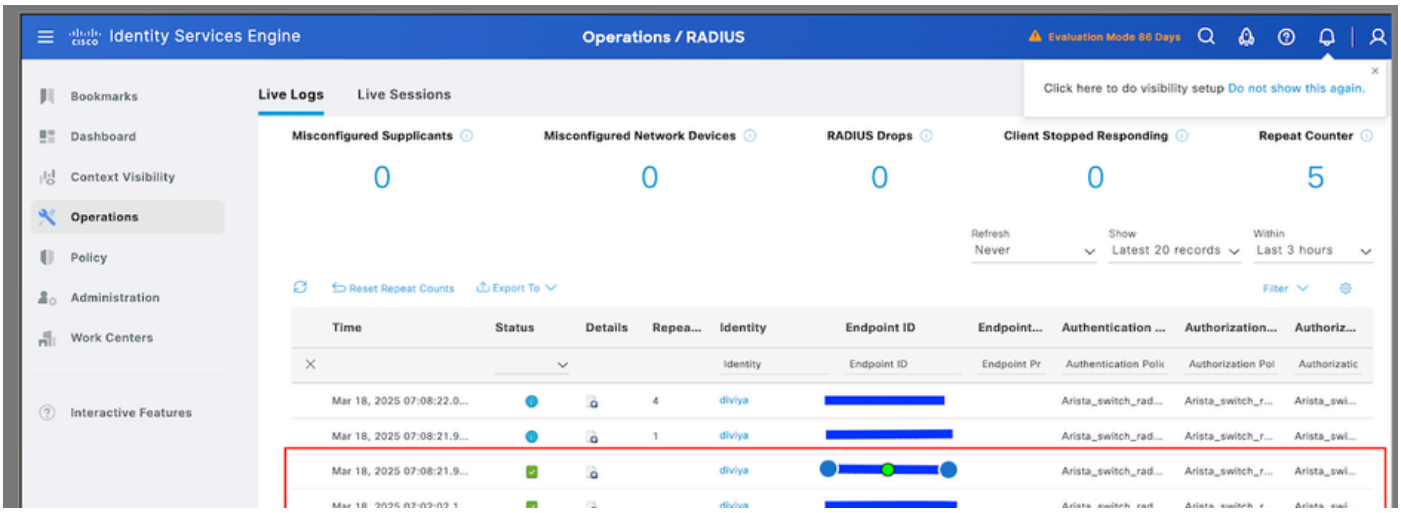
驗證

ISE稽核

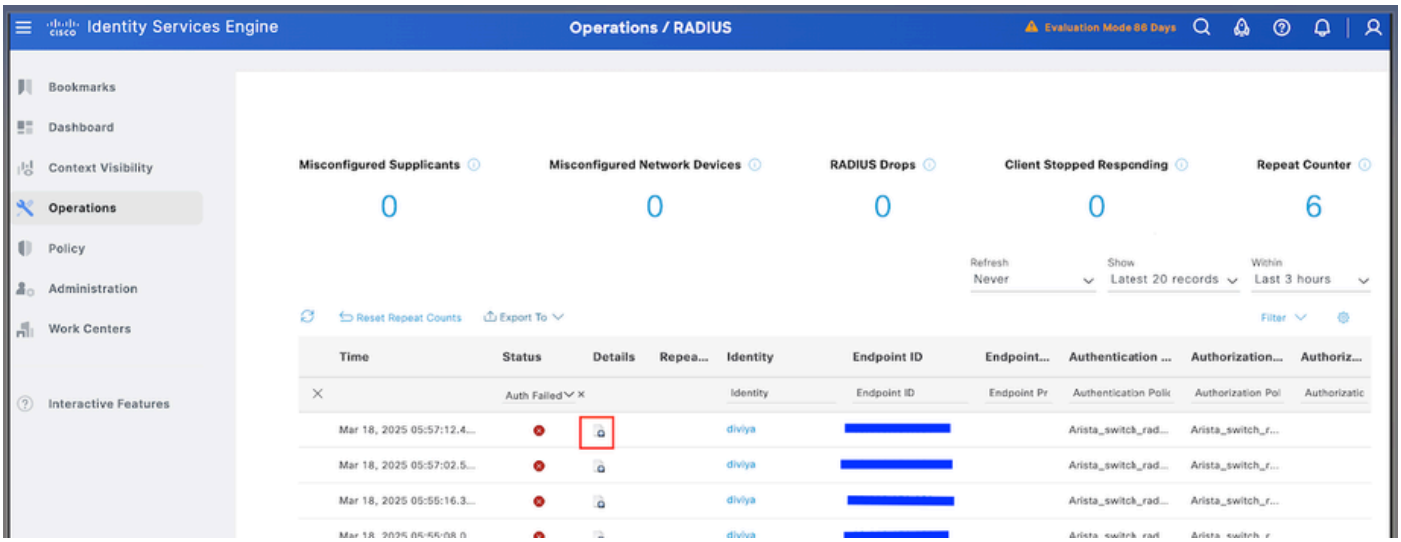
1.嘗試使用新的Radius憑證登入到Arista交換機：

1.1導航到操作> Radius >即時日誌。

1.2顯示的資訊顯示了使用者是否成功登入。



2.對於失敗狀態，請檢視會話的詳細資訊：

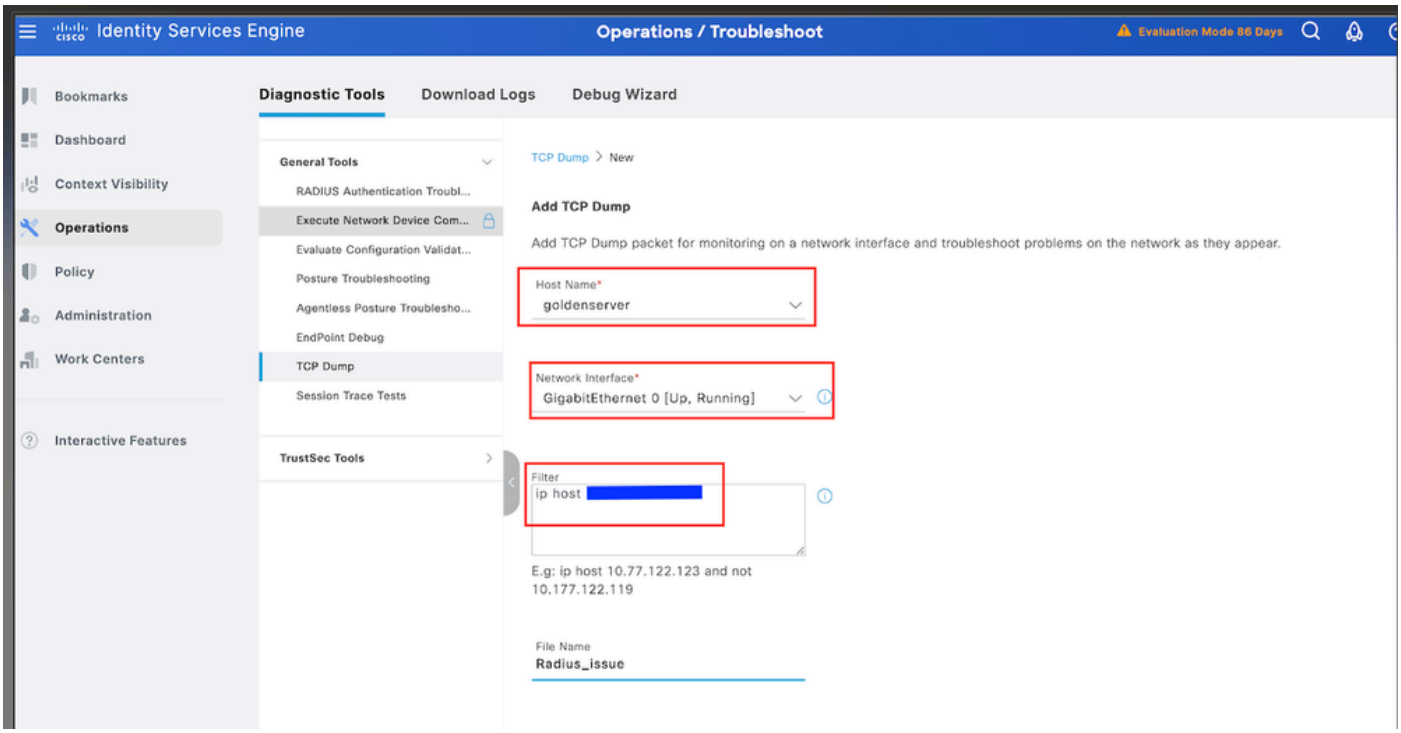


3.對於未顯示在Radius Live日誌中的請求，請檢視UDP請求是否通過資料包捕獲到達ISE節點。

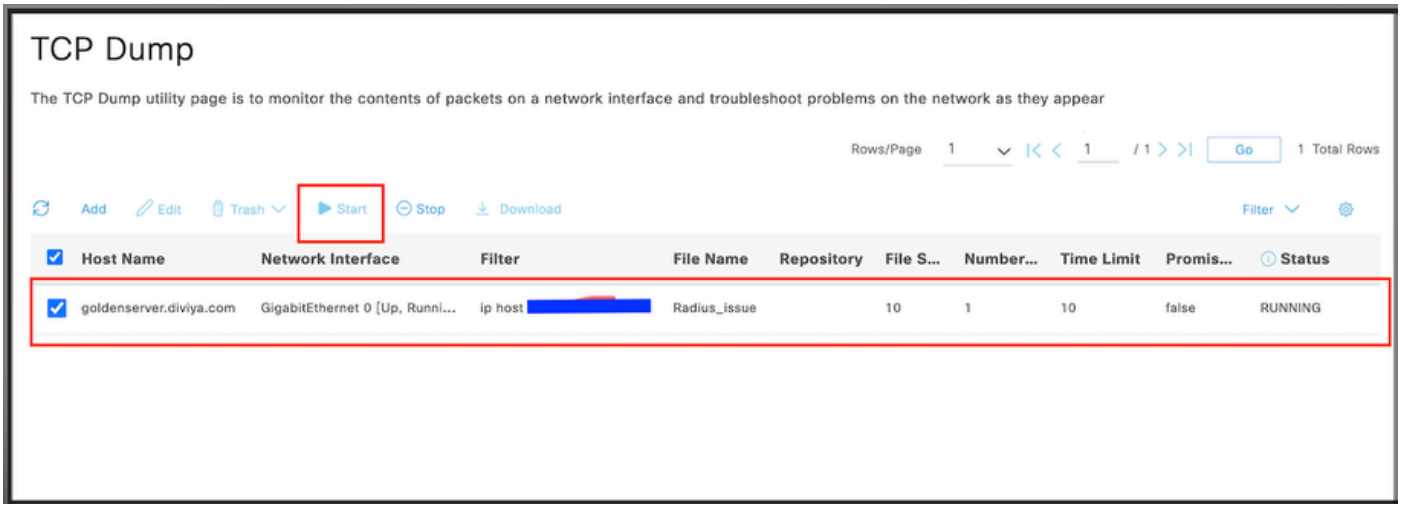
3.1.導航到操作>故障排除>診斷工具> TCP轉儲。

3.2.新增新的捕獲並將檔案下載到本地電腦，以檢視UDP資料包是否到達ISE節點。

3.3.填寫請求的資訊，向下滾動並按一下儲存。



3.4.選擇並啟動捕獲。



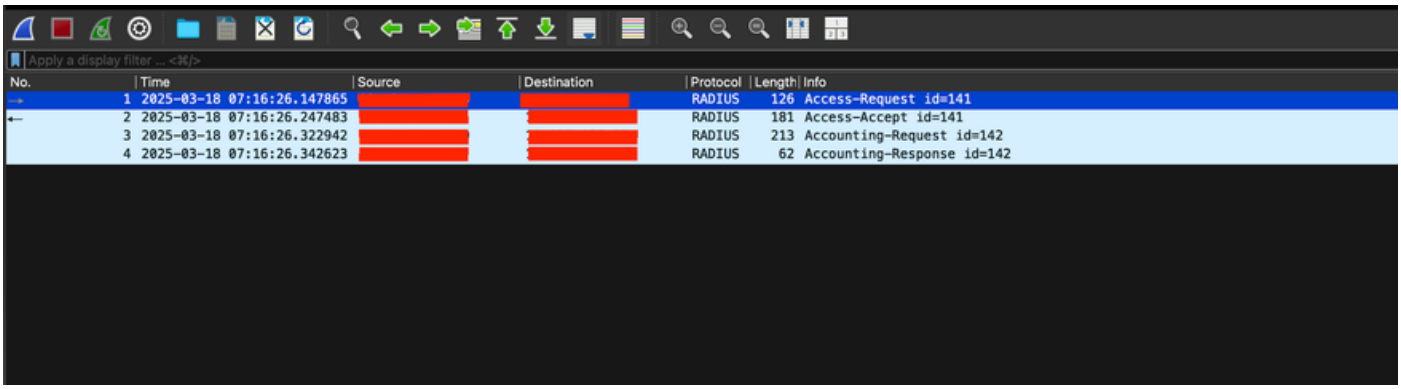
3.5.嘗試在ISE捕獲運行時登入到Arista交換機。

3.6.停止ISE中的TCP轉儲並將檔案下載到本地電腦。

3.7.審查流量輸出。

預期輸出：

資料包No1。從Arista交換機通過埠1812(RADIUS)向ISE伺服器發出請求。
資料包No2。ISE伺服器回覆接受初始請求。



疑難排解

案例1. "5405 RADIUS Request dropped"

問題

此案例涉及當網路裝置（例如Arista交換機）嘗試進行身份驗證時，在Cisco ISE中診斷「5405 RADIUS Request dropped」錯誤，原因為「11007 Could not locate Network Device or AAA Client」。

可能原因

- 思科身份服務引擎(ISE)無法識別Arista交換機，因為其IP地址未列在已知網路裝置中。
- RADIUS請求來自ISE無法識別為有效網路裝置或AAA客戶端的IP地址。
- 交換機和ISE之間的配置可能不匹配（例如IP或共用金鑰不正確）。

解決方案

- 將交換機新增到具有正確IP地址的網路裝置的Cisco ISE清單。
- 驗證ISE中配置的IP地址和共用金鑰是否與交換機上的設定完全匹配。
- 更正後，必須正確識別並處理RADIUS請求。

場景2:Arista交換機無法故障切換到備份ISE PSN

問題

Arista交換機配置為使用Cisco ISE進行RADIUS身份驗證。當主ISE策略服務節點(PSN)不可用時，交換機不會自動故障切換到備用PSN。因此，身份驗證日誌僅從主ISE PSN顯示，在主主裝置關閉時，從輔助/備份PSN沒有日誌。

可能原因

- Arista交換機的RADIUS伺服器配置僅指向主ISE節點，因此不使用備份伺服器。
- 未正確設定RADIUS伺服器優先順序，或者配置中缺少備份ISE IP。
- 交換機上的超時和重傳設定設定太低，導致無法成功回退到備份PSN。
- 交換機將FQDN用於PSN，但DNS解析不會返回所有A記錄，只會與主伺服器聯絡。

解決方案

- 確保在交換機的RADIUS伺服器組配置中輸入多個ISE PSN IP。這樣，如果主裝置無法訪問，交換機可以使用備份ISE PSN。

  配置示例：

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

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

- 驗證RADIUS伺服器優先順序、超時和重新傳輸值是否正確配置為可靠故障轉移。
- 如果使用FQDN，請檢查DNS設定和解析，以確保交換機返回和使用所有PSN IP地址。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。