在帶有ISE伺服器的UCS Manager上配置TACACS+身份驗證域

目錄

簡介

本檔案介紹在Unified Compute System Manager(UCSM)上設定終端存取控制器存取控制系統Plus(TACACS+)驗證。TACACS+是用於驗證、授權和責任服務(AAA)的網路協定，它提供了一種管理網路訪問裝置(NAD)的集中方法，您可以在其中通過伺服器管理和建立規則，在本使用案例中，我們使用的是身份服務引擎(ISE)。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco UCS管理器(UCSM)
- 終端存取控制器存取控制系統Plus(TACACS+)
- 身分識別服務引擎 (ISE)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCSM 4.2(3d)
- 思科身分識別服務引擎(ISE)版本3.2

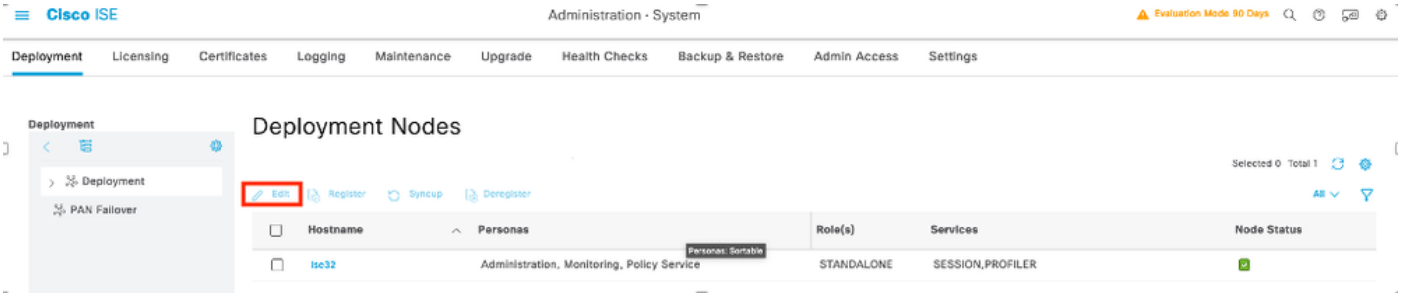
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

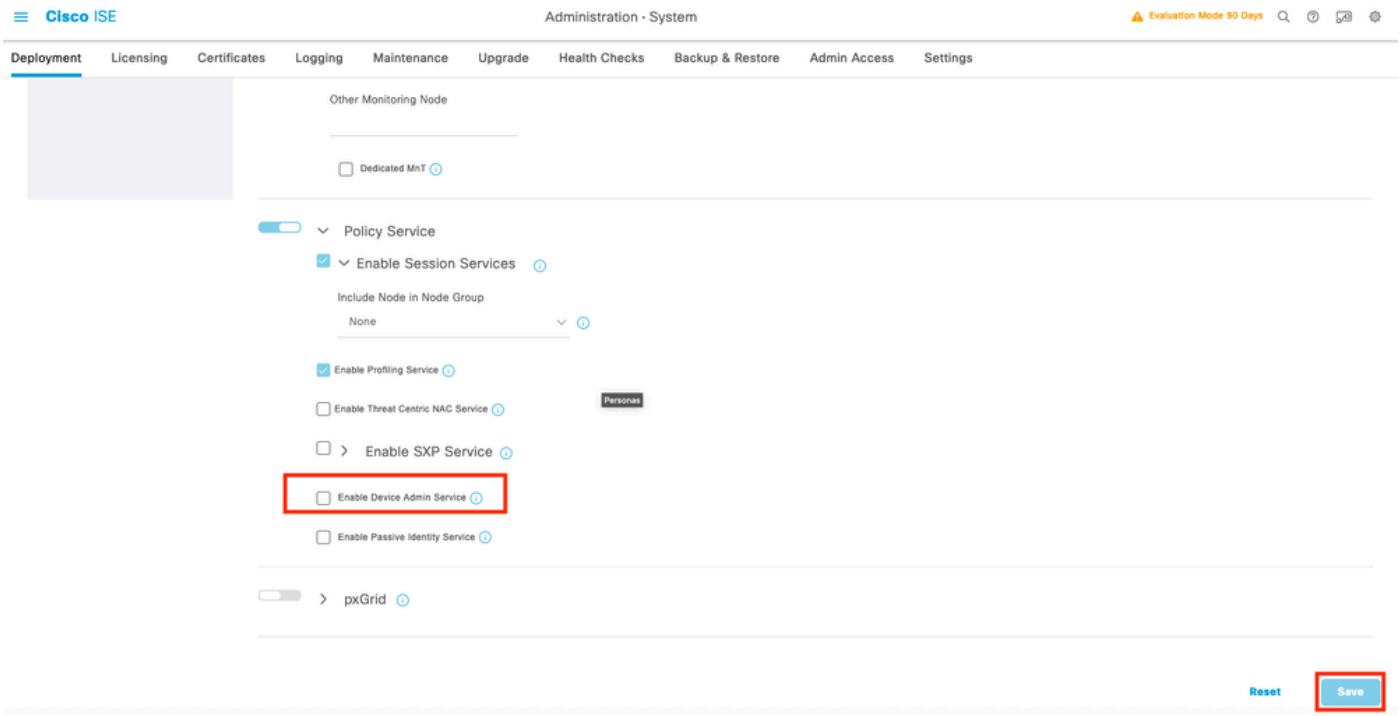
ISE上的TACACS+配置

在ISE上設定TACACS+

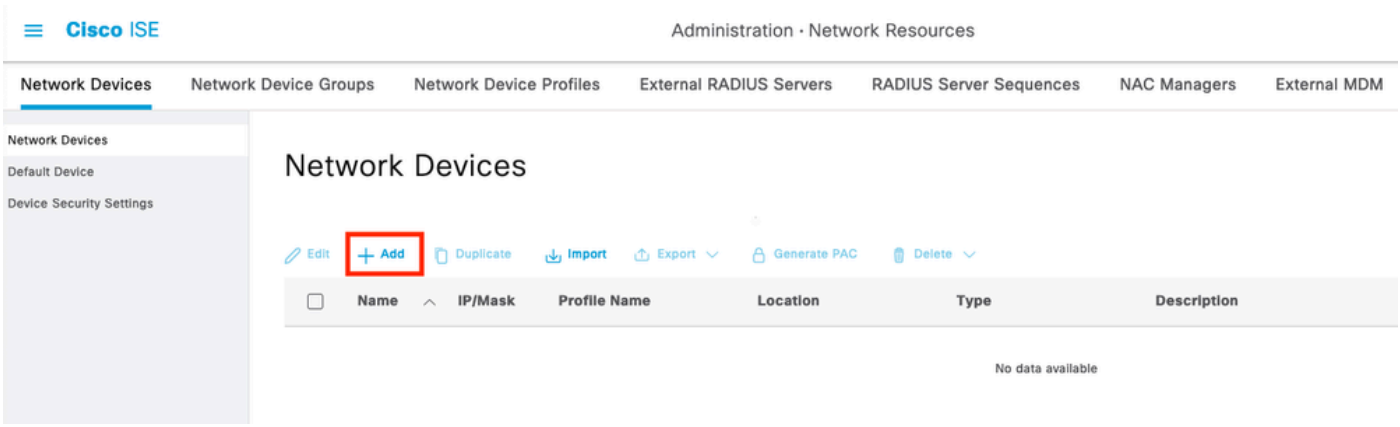
步驟1。第一個任務是檢查ISE是否具有處理TACACS+身份驗證的正確功能，以便您需要在策略服務節點(PSN)中檢查是否具有裝置管理服務(Device Admin Service)的功能，瀏覽選單Administration > System > Deployment，選擇ISE執行TACACS+的節點，然後選擇按鈕編輯。



步驟2.向下滾動，直到您看到名為Device Administration Service的相應功能（注意，要啟用此功能，您首先需要在節點上啟用策略伺服器角色，並且部署中還要有TACACS+許可證），選中該覈取方塊，然後儲存配置：

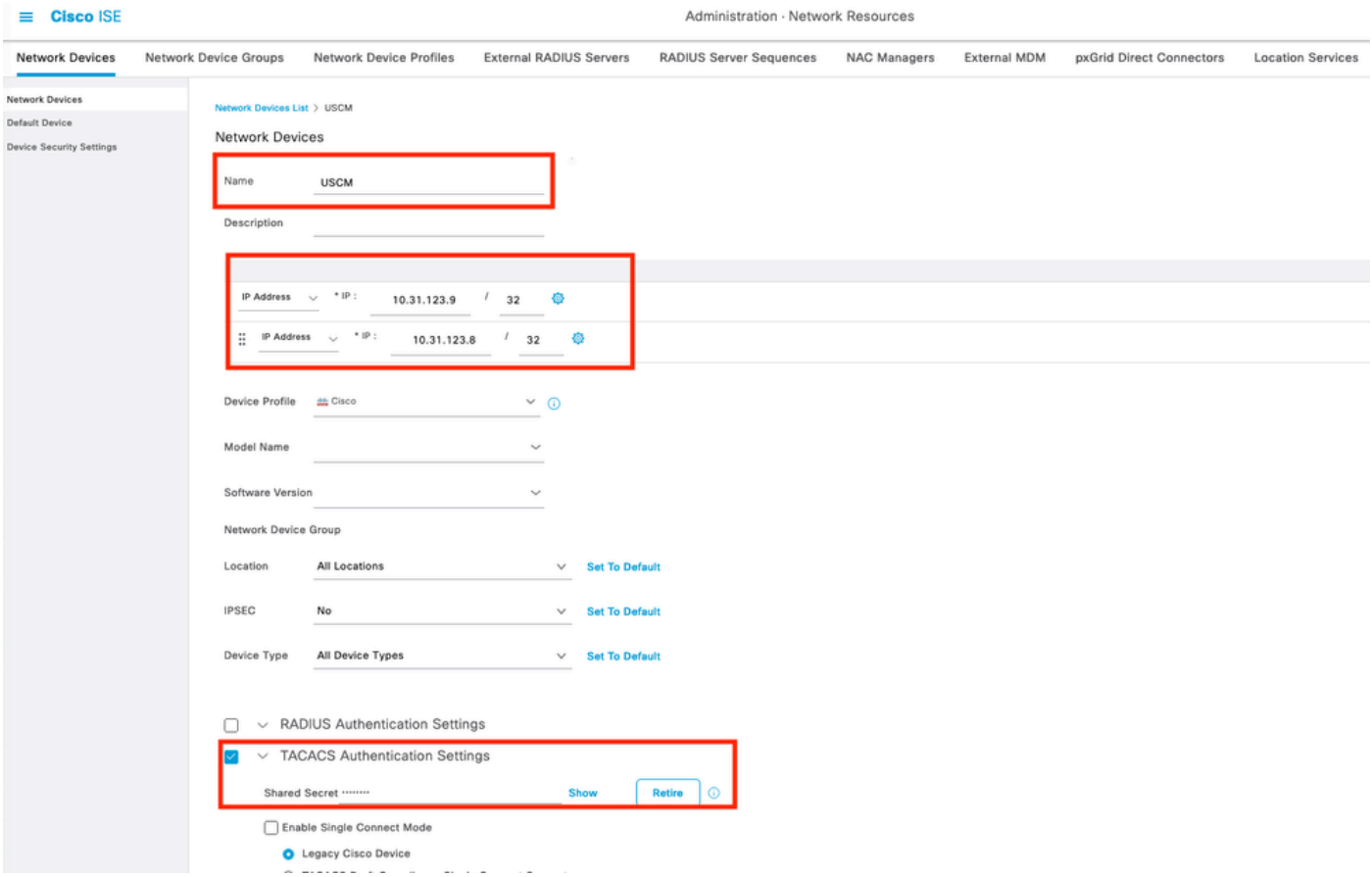


步驟3。設定使用ISE作為TACACS+伺服器的網路存取裝置(NAD)，導覽至Administration > Network Resources > Network Devices功能表，然後選取按鈕+Add。



步驟4。在本節中設定：

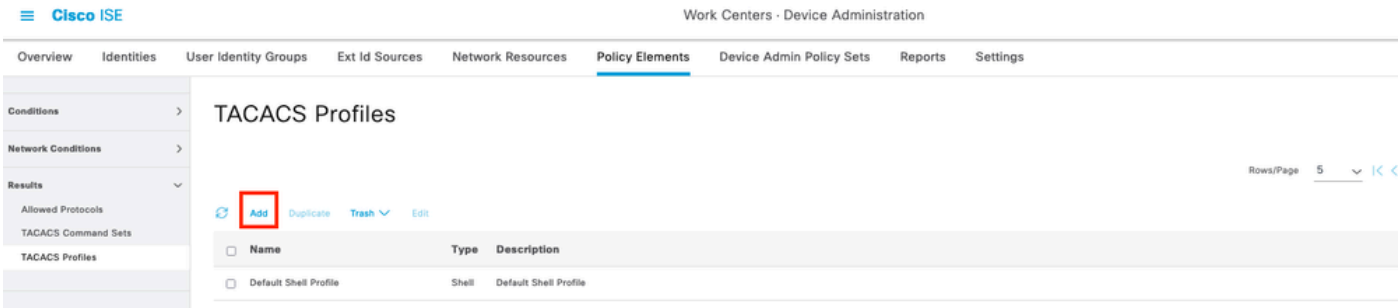
- 作為TACACS+客戶端的UCSM的名稱。
- UCSM用來向ISE傳送請求的IP地址。
- TACACS+共用密碼，這是用於加密UCSM和ISE之間的資料包的密碼



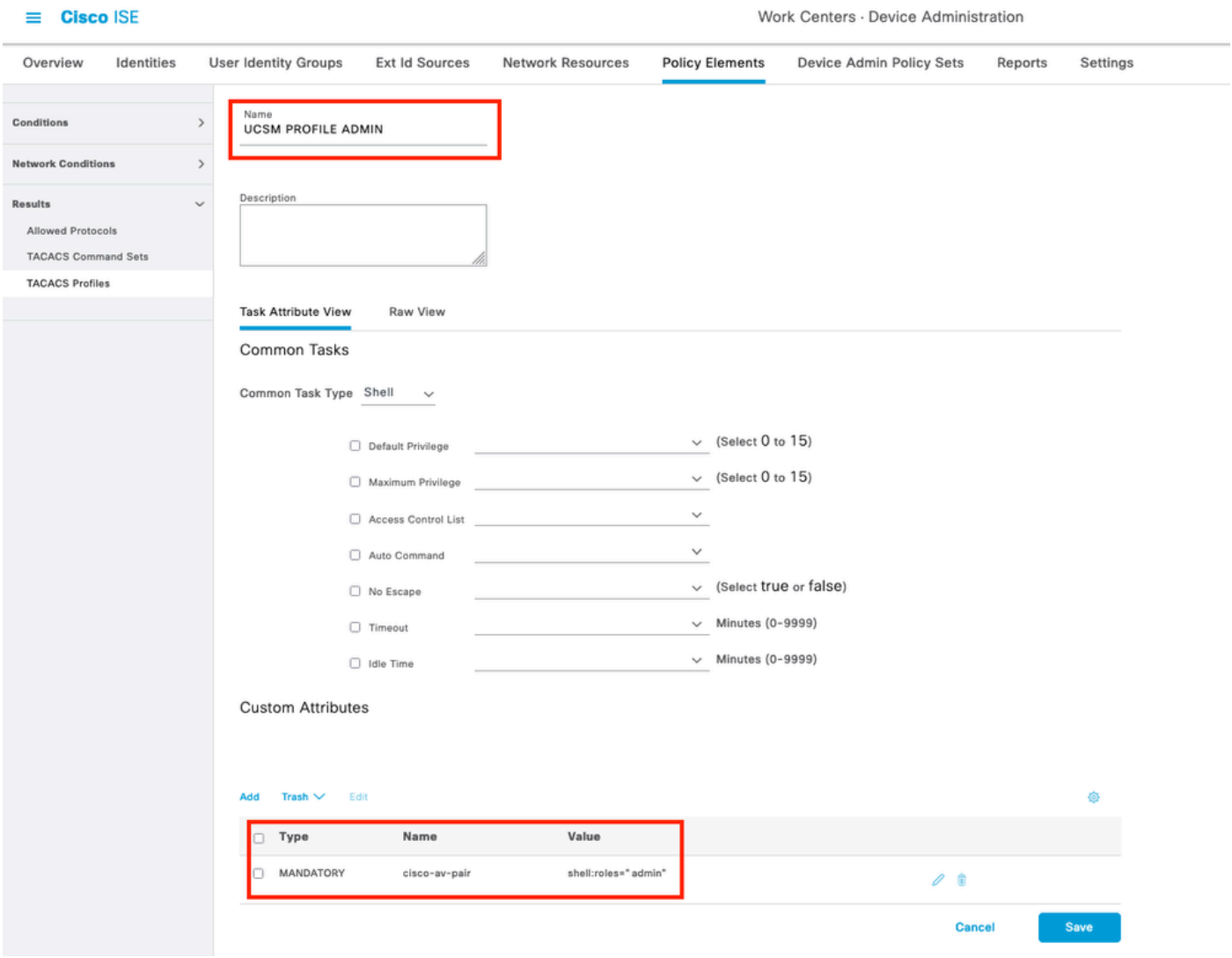
附註：對於群集配置，為兩個交換矩陣互聯新增管理埠IP地址。此配置可確保在第一交換矩陣互聯發生故障且系統故障切換到第二交換矩陣互聯時，遠端使用者可以繼續登入。所有登入請求均源自這些IP地址，而不是Cisco UCS Manager使用的虛擬IP地址。

在ISE上配置屬性和規則

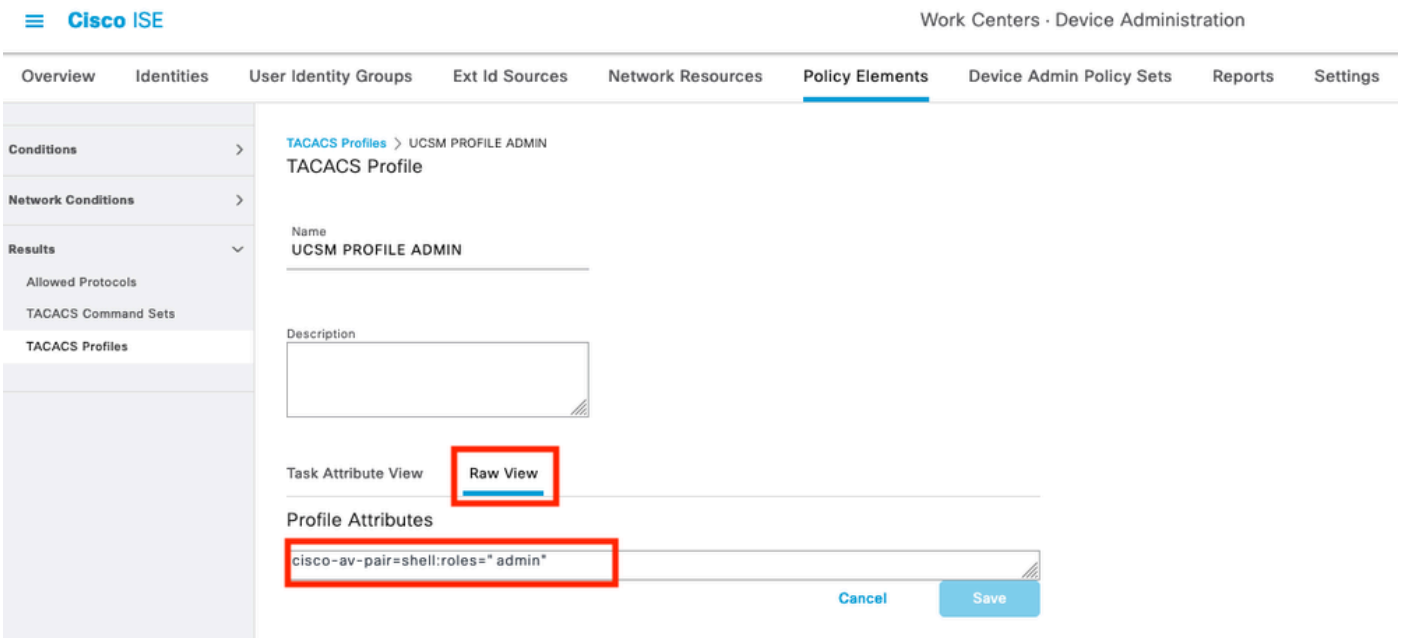
步驟1。建立TACACS+設定檔，導覽至Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles功能表，然後選擇Add



步驟2 。在此部分中使用名稱配置配置檔案，並在Custom Attributes部分中，選擇Add，然後建立一個特性MANDATORY的屬性，將其命名為cisco-av-pair，在值中選擇一個可用於UCSM的角色並輸入該角色作為shell角色，在本示例中，它使用角色admin，並且所選輸入需要為shell:roles="admin"，如下所示，



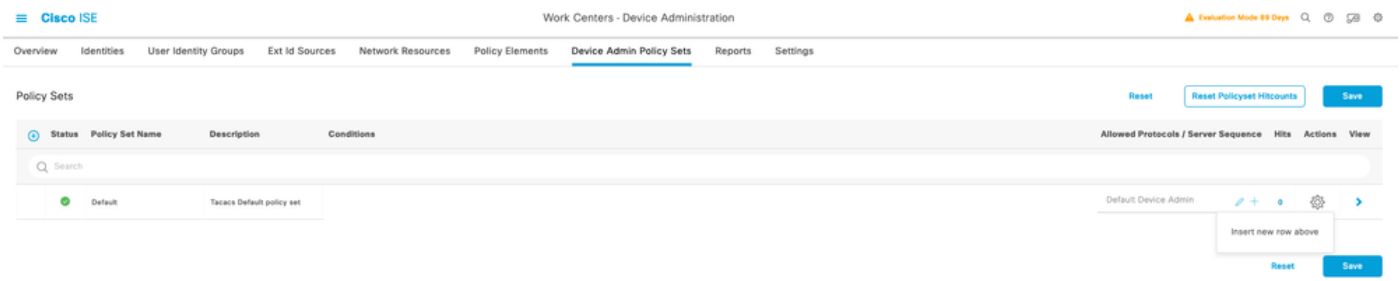
在同一選單中，如果您為TACACS配置檔案選擇Raw View，則可以驗證通過ISE傳送的屬性的相應配置。



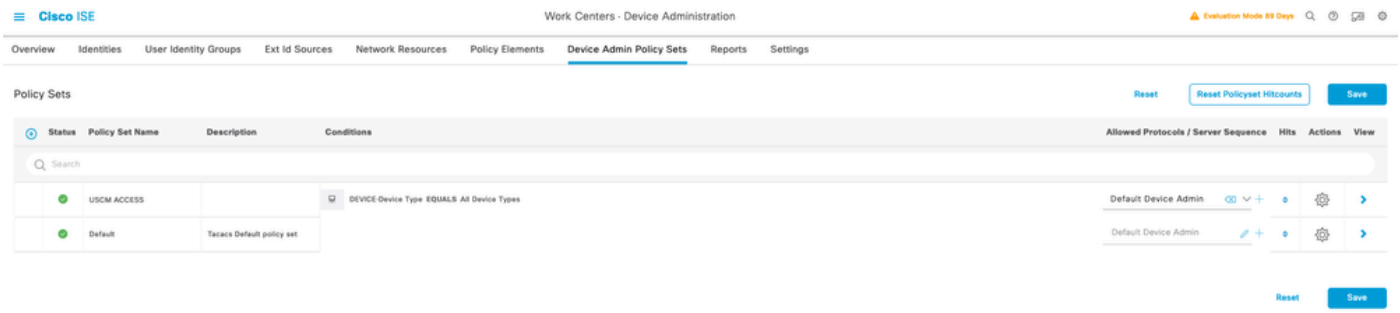
附註：cisco-av-pair name是為TACACS+提供程式提供屬性ID的字串。

步驟3。勾選並儲存組態。

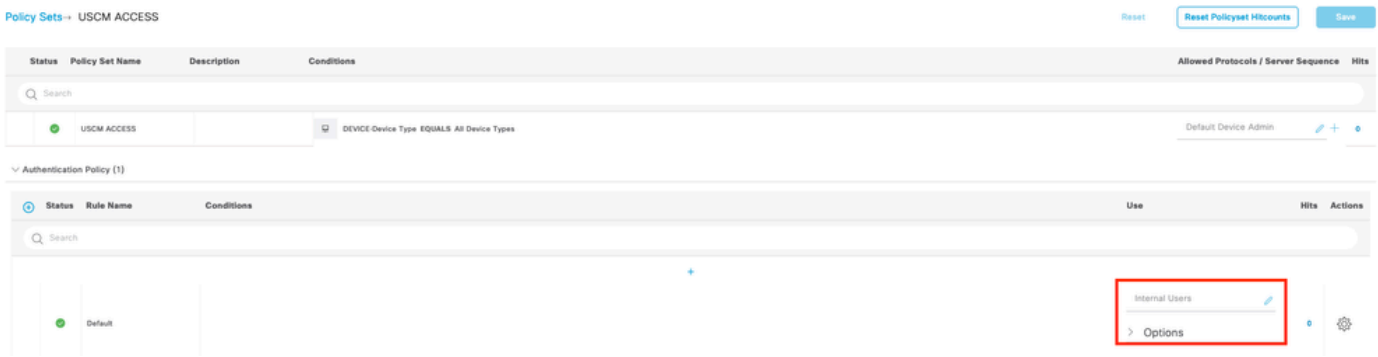
步驟4.建立用於UCSM的Device Admin Policy Set，導航選單Work Centers > Device Administration > Device Admin Policy Sets，然後從現有策略集中選擇齒輪圖示，然後選擇Insert new row



步驟5.命名此新策略集，根據UCSM伺服器正在進行中的TACACS+身份驗證的特徵新增條件，然後選擇Allowed Protocols > Default Device Admin，儲存配置。

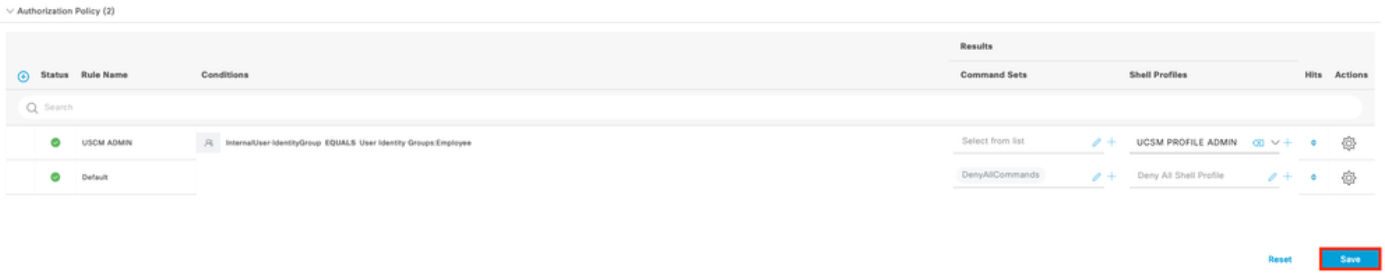


步驟6.在「>檢視」選項中選擇，然後在「身份驗證策略」部分中選擇外部身份源，ISE從其中查詢在UCSM中輸入的使用者名稱和憑據，在此示例中，憑據對應於ISE中儲存的內部使用者。



步驟7.下滾至名為Authorization Policy的部分直到Default policy，選擇齒輪圖示，然後插入一個規則。

步驟8.命名新的授權規則，新增與已經作為組成員身份進行身份驗證的使用者有關的條件，並在Shell Profiles部分新增您先前配置的TACACS配置文件，儲存配置。



UCSM上的TACACS+配置

使用Cisco UCS Manager具有管理員許可權的使用者登入GUI。

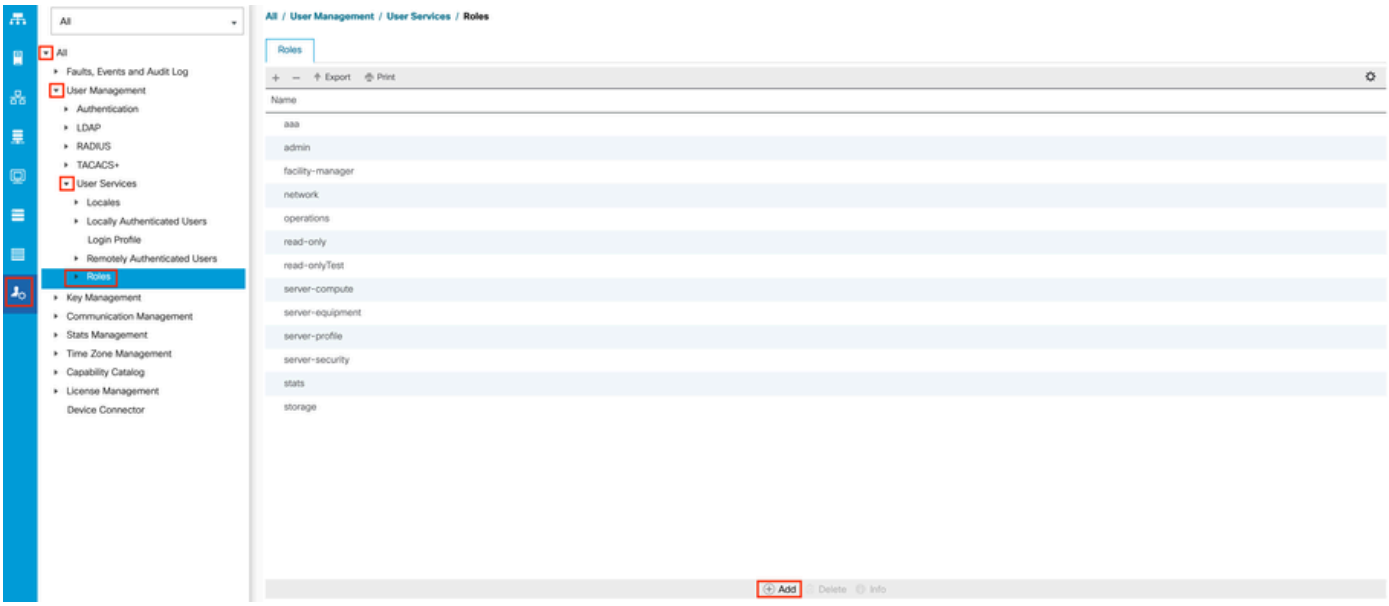
為使用者建立角色

步驟1.在導航窗格中，選擇Admin選項卡。
步驟2.在Admin選項卡上，展開All > User Management >User Services > Roles。

步驟3.在窗格Work中，選擇選General項卡。

步驟4.選擇Add作為自定義角色。此示例使用預設角色。

步驟5.驗證名稱角色是否與先前在TACACS設定檔上設定的名稱相符。

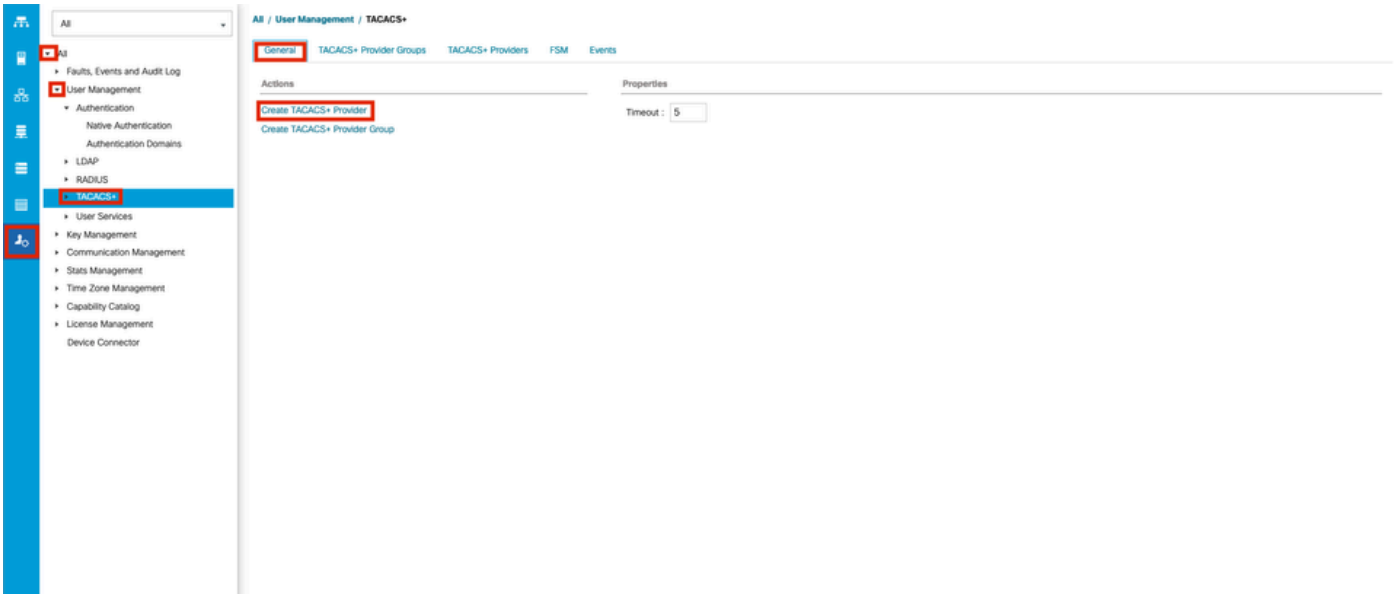


建立TACACS+提供程式

步驟1.在導航窗格中，選擇Admin選項卡。
步驟2.在Admin選項卡上，展開All > User Management > TACACS+。

步驟3.在窗Work格中，選擇頁籤General。

步驟4.在區域Actions中，選擇Create TACACS+ Provider.



步驟5.在嚮導**Create TACACS+ Provider**中，輸入適當的資訊。

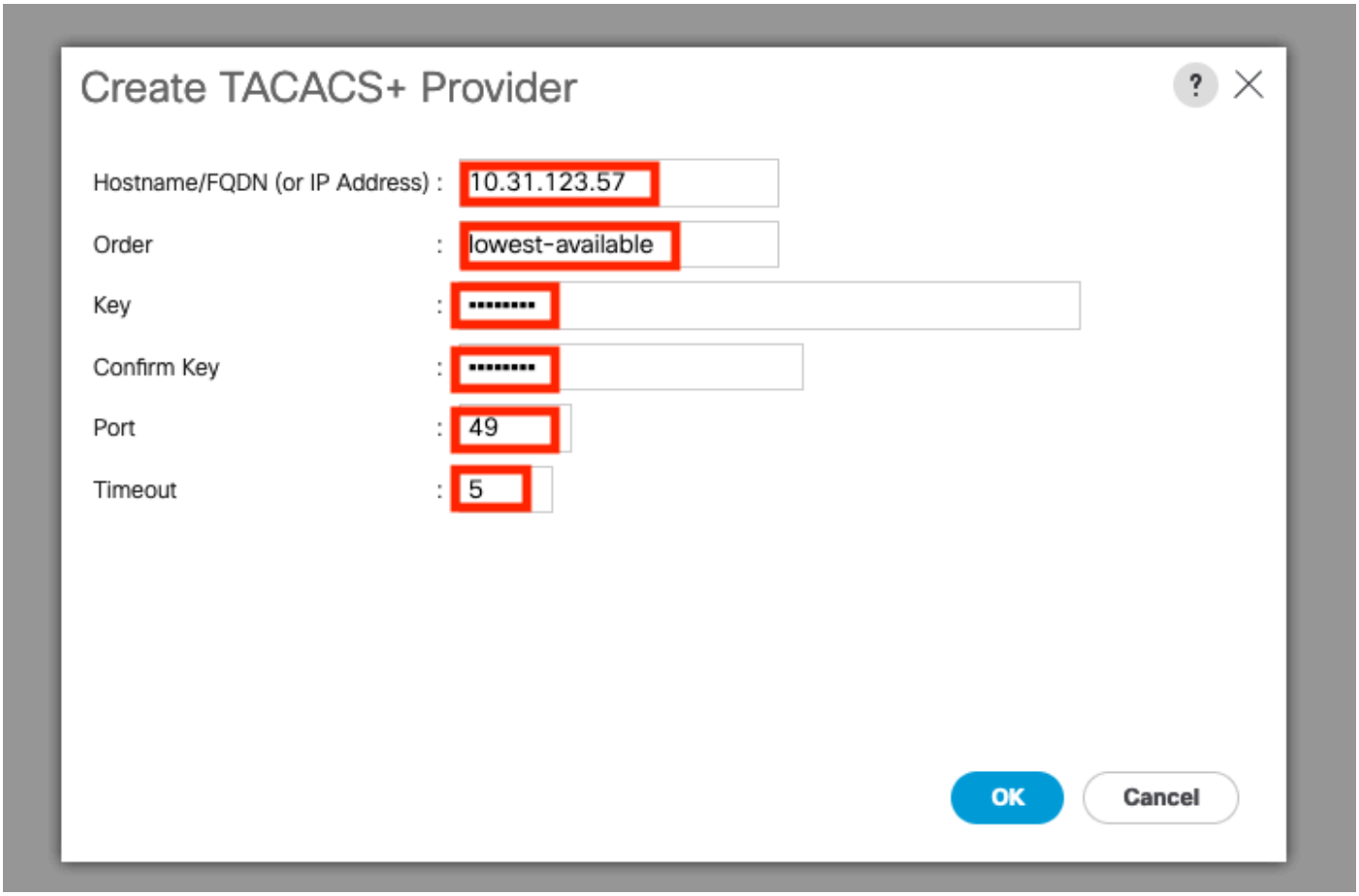
- 在「Hostname」欄位中，鍵入TACACS+伺服器的IP地址或主機名。
- 在Order欄位中，Cisco UCS使用此提供程式驗證使用者的順序。

  如果希望Cisco UCS根據此Cisco UCS例項中定義的其他提供商分配下一個可用訂單，請輸入一個介於1和16之間的整數，或輸入最小可用訂單或0（零）。

- 在Key欄位中，輸入資料庫的SSL加密金鑰。

- 在Confirm Key欄位中，為確認目的重複的SSL加密金鑰。
- 在Port欄位中，輸入Cisco UCS與TACACS+資料庫（埠49預設埠）進行通訊的埠。

- 在Timeout欄位中，系統嘗試在超時前連線TACACS+資料庫所花費的時間長度（以秒為單位）。



步驟6.選擇Ok。

附註：如果使用主機名而不是IP地址，則必須在Cisco UCS Manager中配置DNS伺服器。

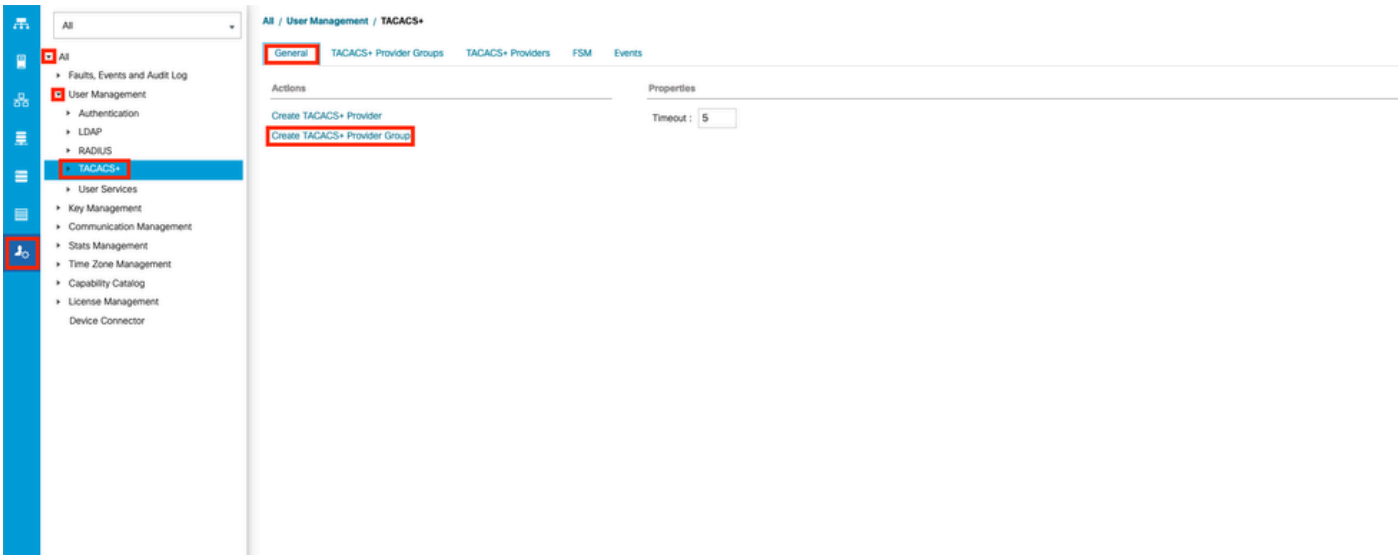
建立TACAC+提供程式組

步驟1.在窗**Navigation**格中，選擇選項**Admin**卡。

步驟2.在選項**Admin**卡上，展開**All > User Management > TACACS+**。

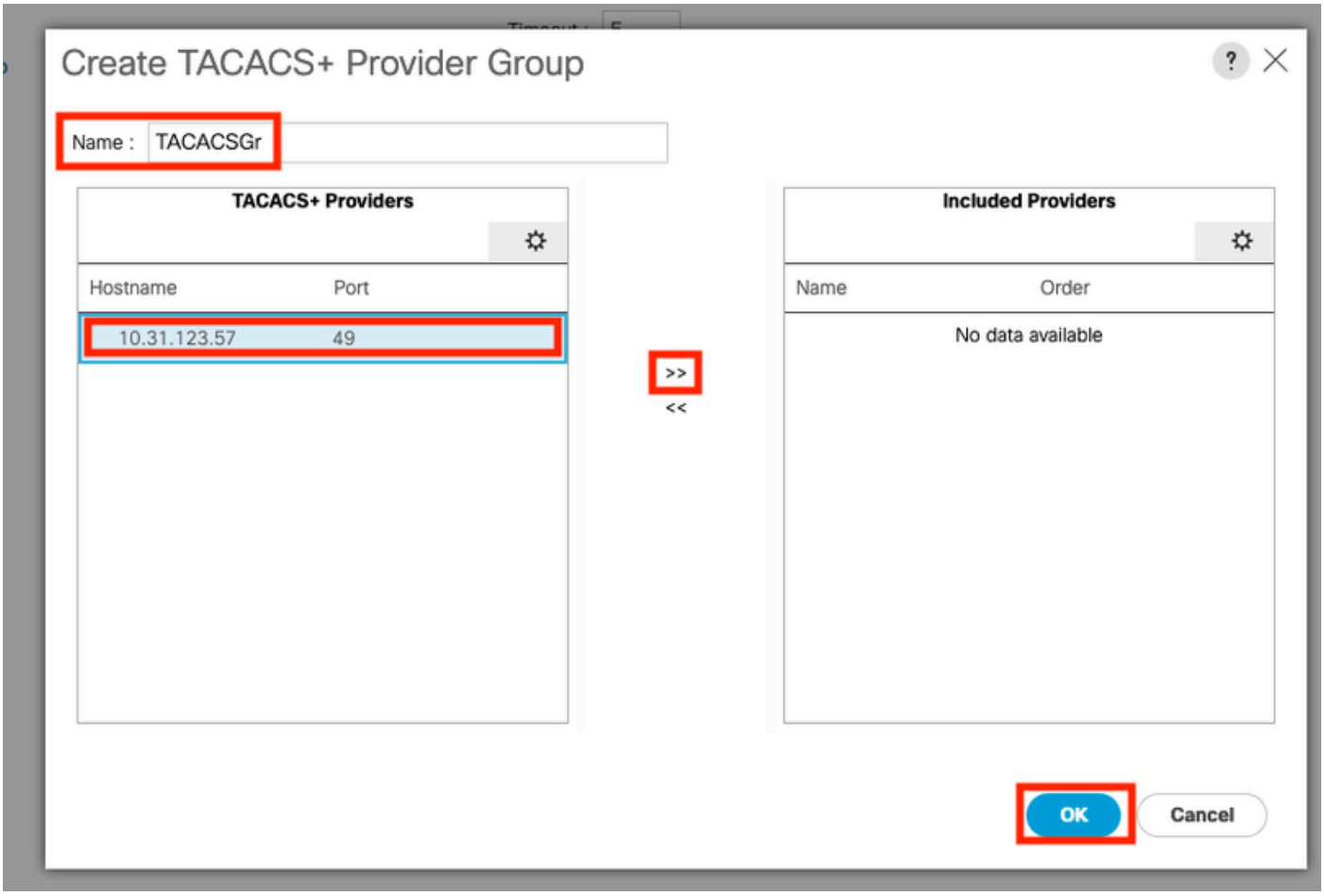
步驟3.在窗**Work**格中，選擇選項**General**卡。

步驟4.在區**Actions**域中，選Create TACACS+ Provider擇Group。



步驟5.在「建立TACACS+提供程式組」對話方塊中，輸入請求的資訊。

- 在「名稱」欄位中，輸入組的唯一名稱。
- 在「TACACS+提供程式」表中，選擇要包含在組中的提供程式。
- 選擇>>按鈕將提供程式新增到Included Providers表。



步驟6.選擇Ok。

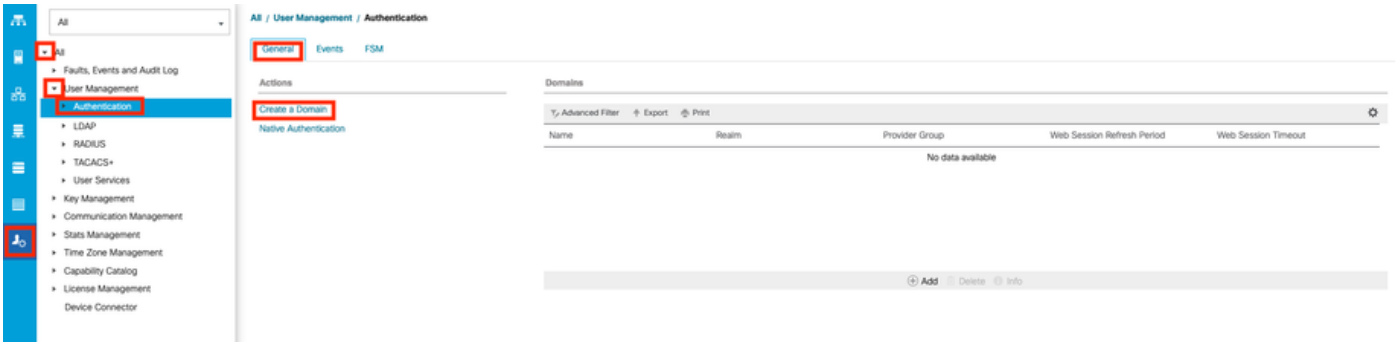
建立身份驗證域

步驟1。在窗格Navigation中，選擇選項Admin卡。

步驟2.在頁籤Admin上，展開 All > User Management > Authentication

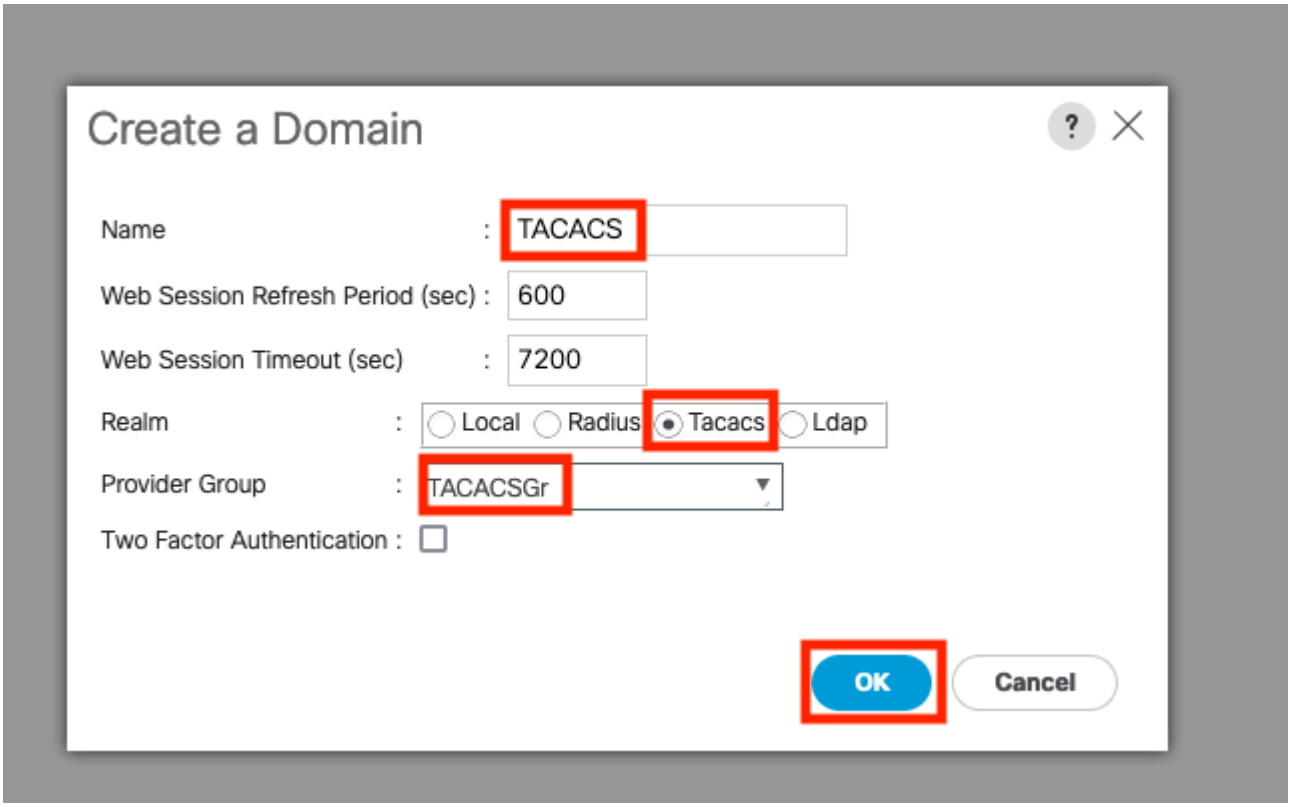
步驟3.在窗Work格中，選擇選項General卡。

步驟4.在Actions區域中，選擇Create a Domain.



步驟5.在「建立域」對話框中，輸入請求的資訊。

- 在「名稱」欄位中，輸入域的唯一名稱。
- 在Realm中，選擇Tacacs選項。
- 在「Provider Group」下拉選單中，選擇以前建立的TACACS+提供程式組，然後選擇「OK」



疑難排解

UCSM上的常見TACACS+問題

- 金鑰錯誤或字元無效。
- 連接埠錯誤.
- 由於防火牆或代理規則，無法與提供商通訊。
- FSM不是100%。

驗證UCSM TACACS+配置：

必須確保UCSM已實施配置檢查，有限狀態機(FSM)的狀態顯示為100%完成。

從UCSM命令列驗證配置

<#root>

UCS-A#

scope security

UCS-A /security #

scope tacacs

UCS-A /security/tacacs #

show configuration

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
  scope tacacs
      enter auth-server-group TACACSGr
          enter server-ref 10.31.123.57
              set order 1
          exit
      exit
      enter server 10.31.123.57
          set order 1
          set port 49
          set timeout 5
  !       set key
      exit
      set timeout 5
  exit
```

<#root>

UCS-A /security/tacacs #

show fsm status

```
UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status

    FSM 1:
        Status: Nop
        Previous Status: Update Ep Success
        Timestamp: 2023-06-24T20:54:05.021
        Try: 0
        Progress (%): 100
        Current Task:
```

從NXOS驗證Tacacs配置：

<#root>

UCS-A#

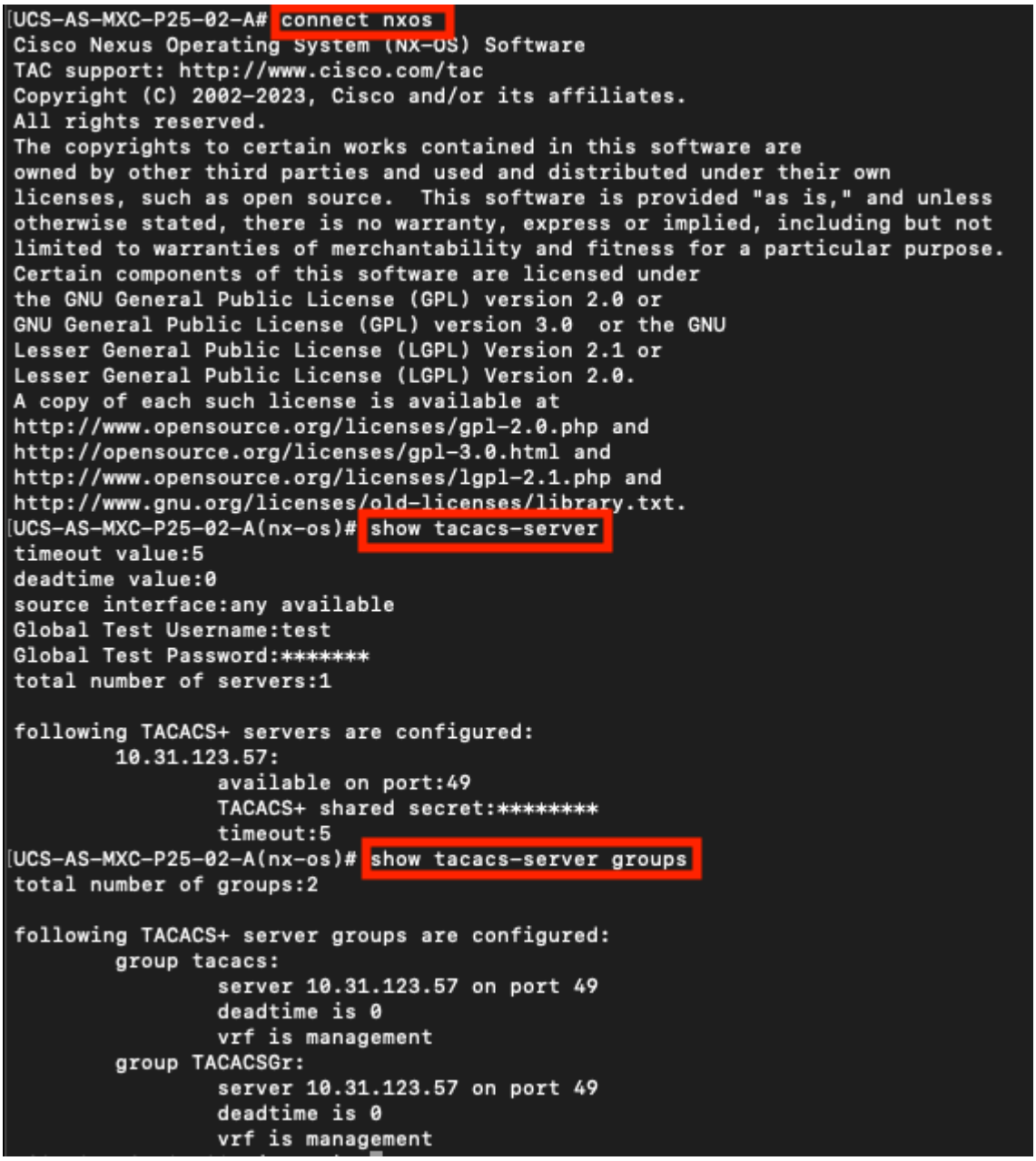
connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups



要測試來自NX-OS的身份驗證，請使用**test aaa**命令（僅適用於NXOS）。

驗證伺服器的配置：

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

<TACACS+-server-IP-address or FQDN> <username> <password>

```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

UCSM回顧

可達性驗證

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

ping

 <TACACS+-server-IP-address or FQDN>

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

連線埠驗證

<#root>

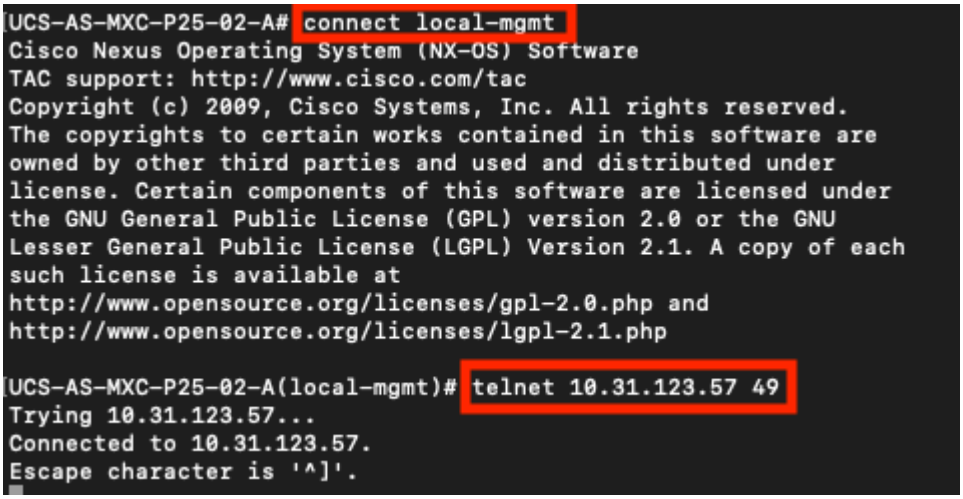
UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

<TACACS+-server-IP-address or FQDN> <Port>



檢視錯誤的最有效方法是啟用NXOS調試，通過此輸出，您可以檢視導致通訊錯誤的組、連線和錯誤消息。

- 開啟與UCSM的SSH會話，使用具有管理員許可權的任何特權使用者（最好是本地使用者）登入，轉到NX-OS CLI上下文並啟動終端監控。

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

- 啟用調試標誌並驗證SSH會話輸出到日誌檔案。

<#root>

UCS-A(nx-os)#

debug aaa all

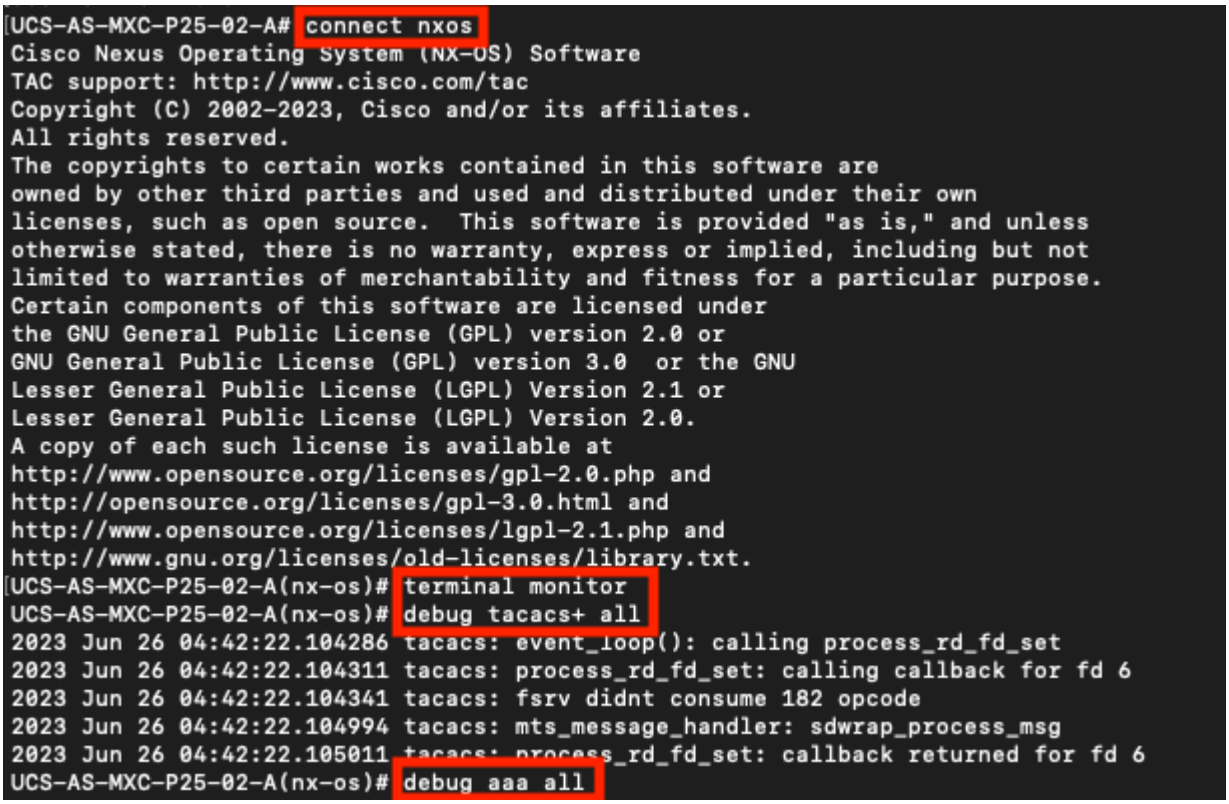
UCS-A(nx-os)#

```
debug aaa aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request-lowlevel

UCS-A(nx-os)#
debug tacacs+ all
```



- 現在開啟一個新的GUI或CLI會話，並嘗試以遠端使用者(TACACS+)身份登入。
- 收到登入失敗消息後，關閉關閉會話或使用此命令的調試。

```
UCS-A(nx-os)# undebug all
```

ISE上的常見TACAC問題

- 在ISE中，在嘗試在UCSM分配管理員或任何其他角色所需的屬性中配置tacacs配置檔案時，會顯示此行為，在「儲存」按鈕上選擇此行為：

此錯誤是由以下錯誤https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917導致的，請確保您找到解決此缺陷的位置。

ISE稽核

步驟1.檢查TACACS+可維護性是否正在運行，可以簽入：

- GUI:如果節點在管理>系統>部署中列出了DEVICE ADMIN服務，請檢視該節點。
- CLI:執行命令show ports | include 49以確認TCP連線埠中有屬於TACACS+的連線

<#root>

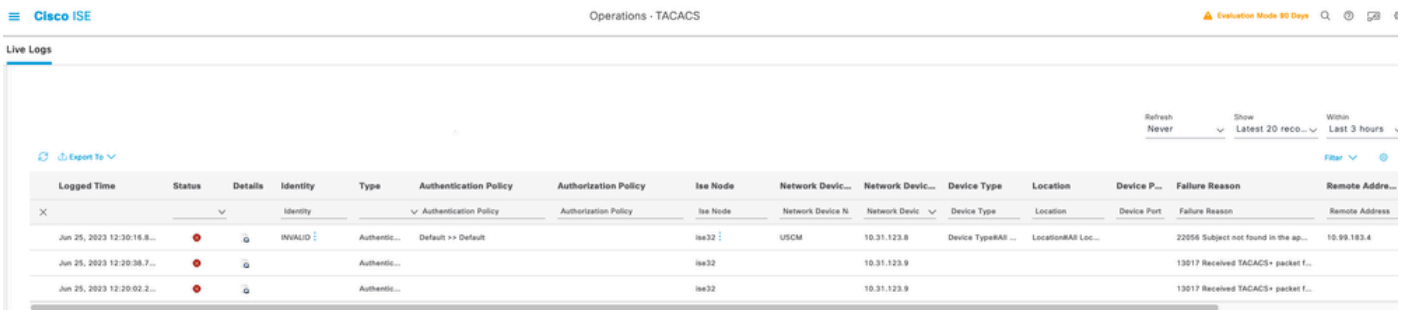
```
ise32/admin#
```

```
show ports | include 49
```

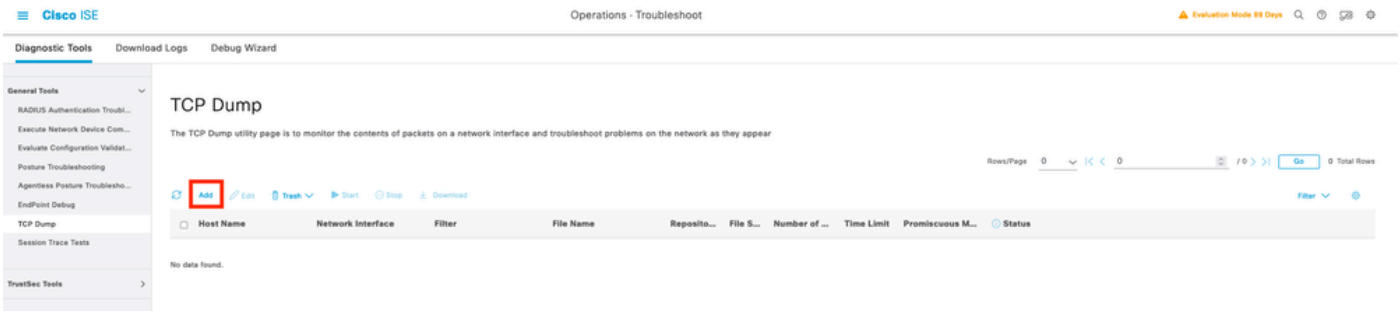
```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

步驟2.確認是否存在有關TACACS+驗證嘗試的即時日誌：可在Operations > TACACS > Live logs選單中進行檢查。

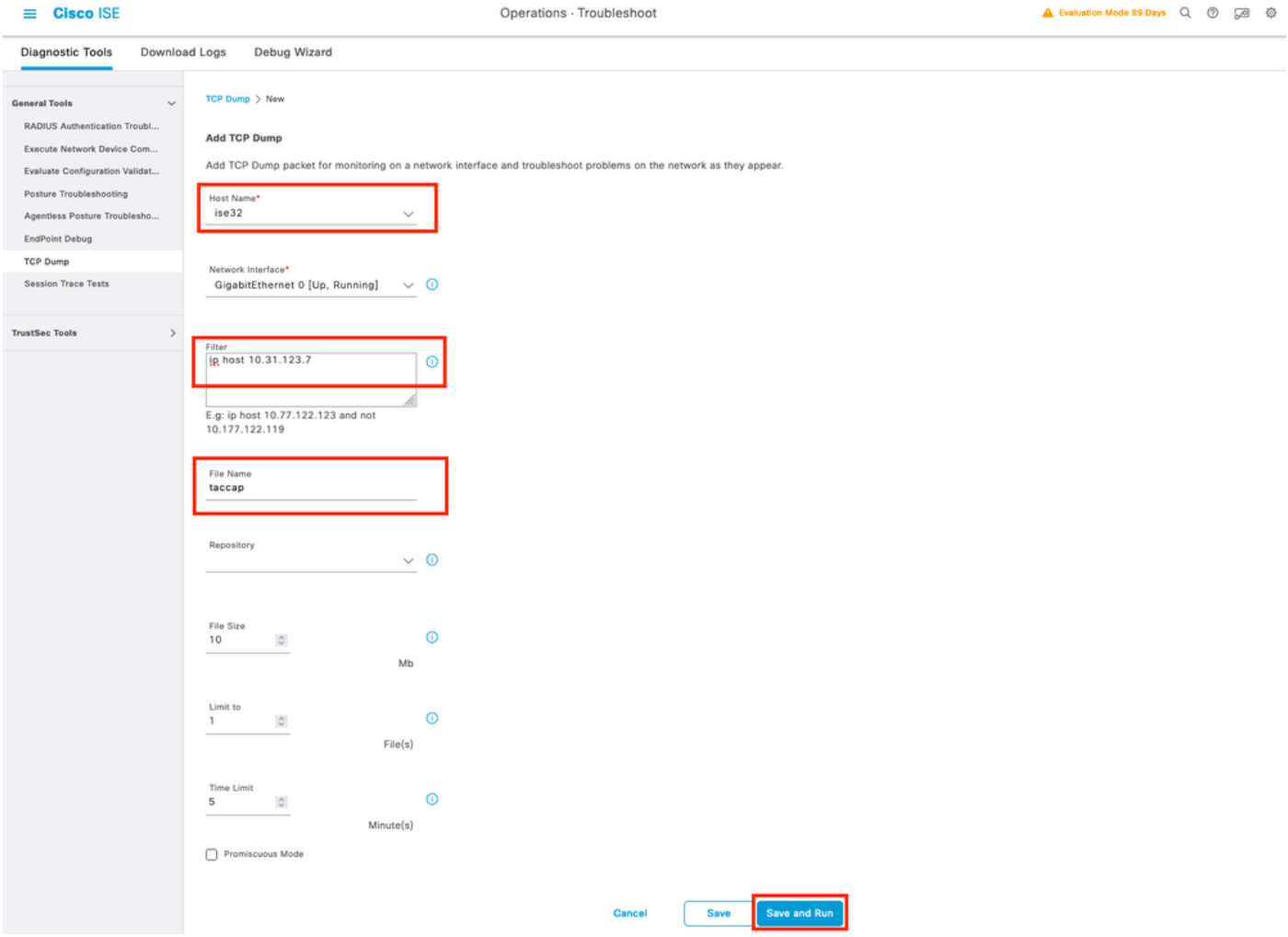
根據故障原因，您可以調整配置或解決故障原因。



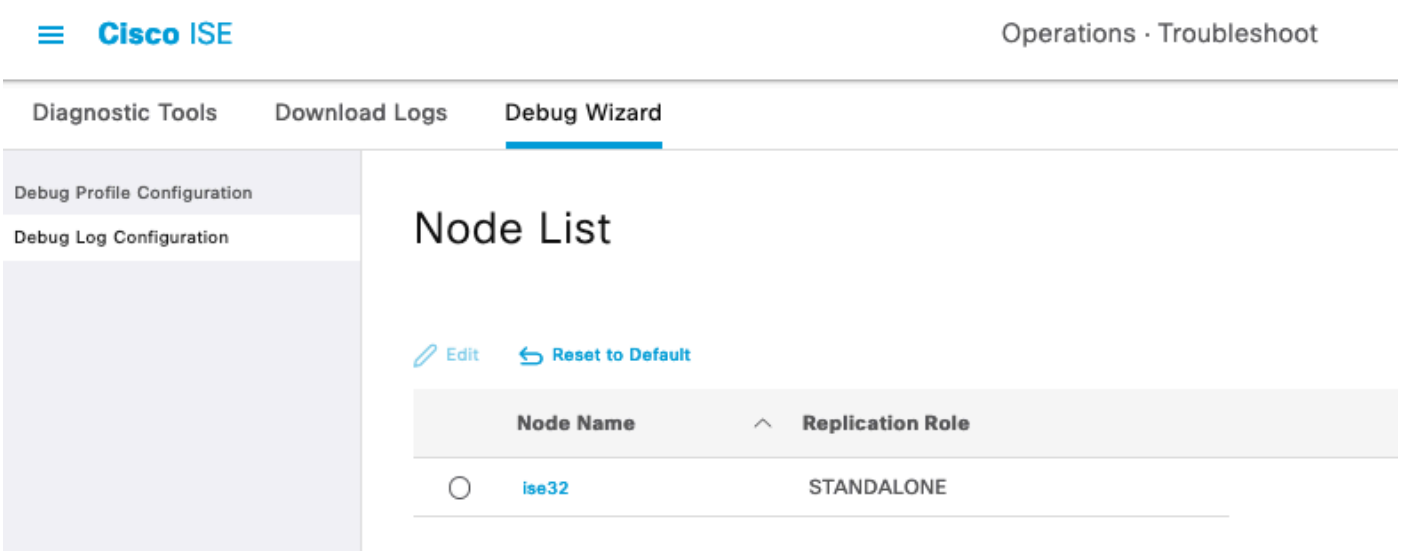
步驟3 如果沒有看到任何即時日誌，請繼續抓取資料包捕獲，導航到選單Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump（新增時選擇）



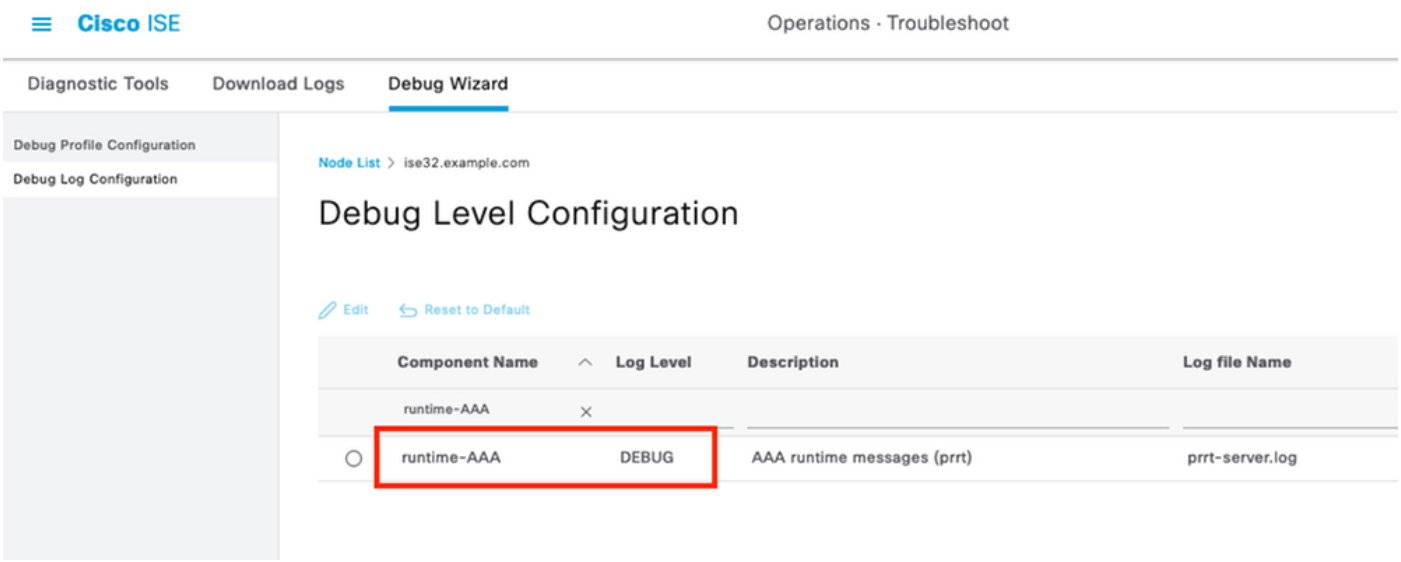
選擇UCSM從中傳送身份驗證的策略服務節點，然後在過濾器中繼續輸入與從中傳送身份驗證的UCSM的IP對應的ip主機X.X.X.X，命名捕獲並向下滾動以儲存，運行捕獲並從UCSM登入。



步驟4.在Operations > Troubleshoot > Debug Wizard > Debug log configuration中執行身份驗證的PSN內調試中啟用元件runtime-AAA，選擇PSN節點，然後在編輯按鈕中選擇下一步。



查詢元件runtime-AAA並將其級別更改為調試，然後重新重現問題，然後繼續分析日誌。



附註：有關詳細資訊，請參閱Cisco Youtube的頻道How to Enable Debugs on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8中的影片。

相關資訊

Cisco UCS Manager管理管理指南

Cisco UCS CIMC配置指南TACACS+

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）。