Konfigurieren der TACACS+-Authentifizierungsdomäne auf dem UCS Manager mit ISE Server

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der TACACS+-Authentifizierung (Terminal Access Controller Access-Control System Plus) im Unified Compute System Manager (UCSM) beschrieben. TACACS+ ist ein Netzwerkprotokoll, das für AAA-Dienste (Authentication, Authorization und Accountability Services) verwendet wird. Es bietet eine zentralisierte Methode zur Verwaltung von Netzwerkzugriffsgeräten (Network Access Devices, NAD), mit der Sie Regeln über einen Server verwalten und erstellen können. In diesem Anwendungsfall verwenden wir die Identity Services Engine (ISE).

Voraussetzungen

Anforderungen

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

- Cisco UCS Manager (UCSM)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Identity Services Engine (ISE)

Verwendete Komponenten

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine (ISE) Version 3.2

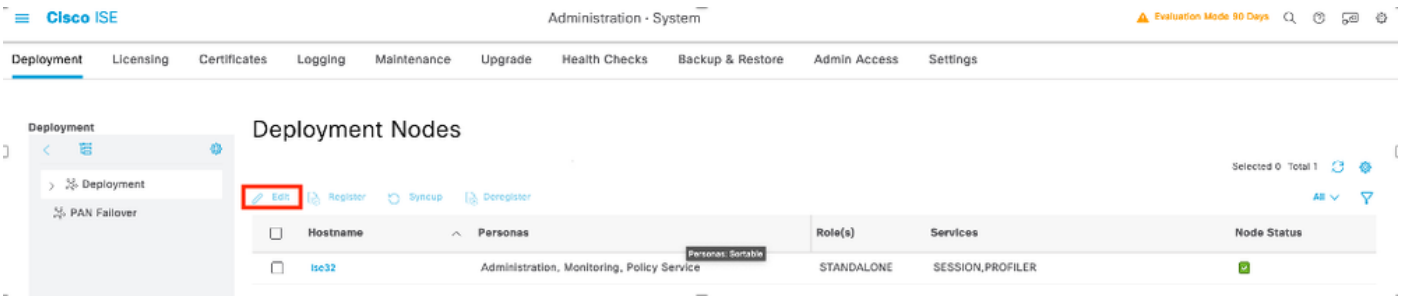
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfiguration

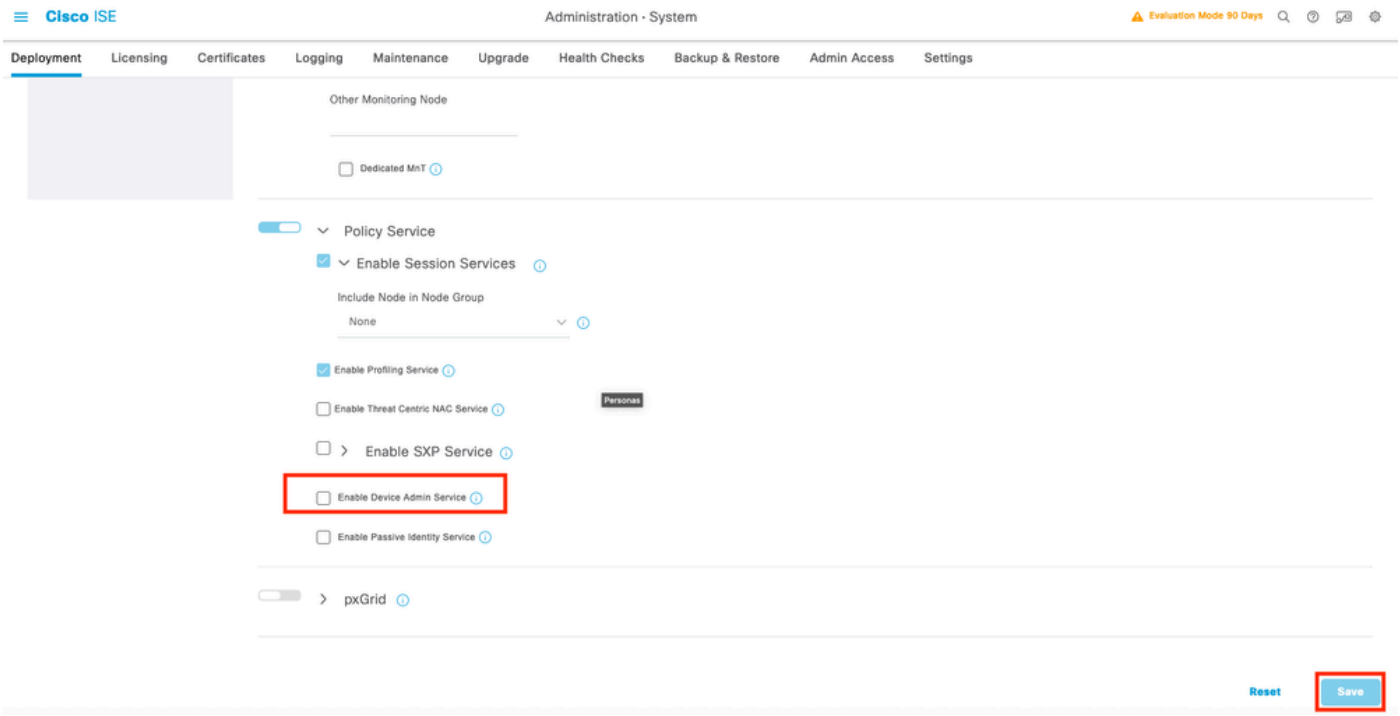
TACACS+-Konfiguration auf der ISE

Einrichtung von TACACS+ auf der ISE

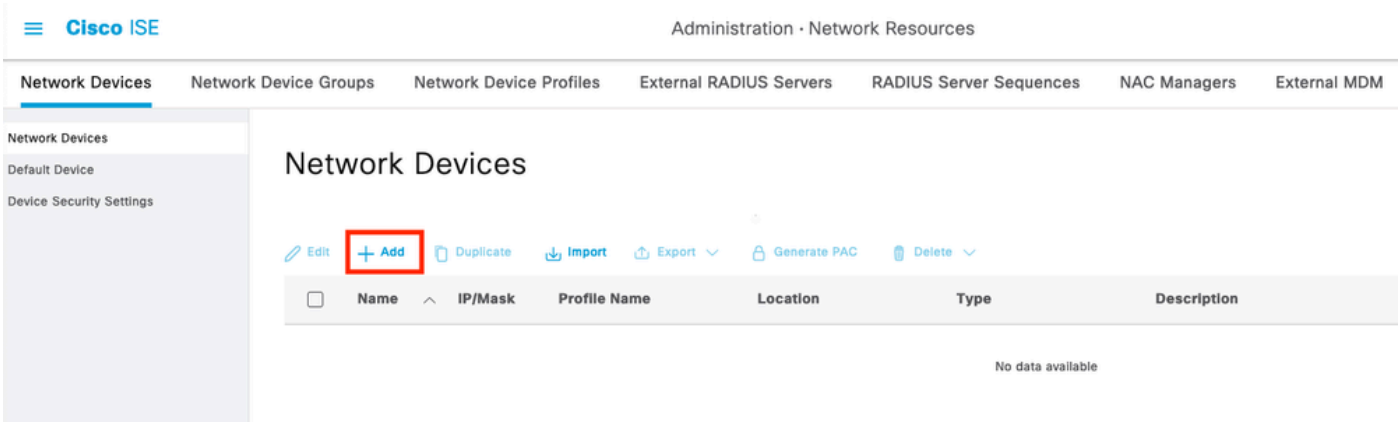
Schritt 1. Die erste Aufgabe besteht darin, zu überprüfen, ob die ISE über die richtigen Funktionen für die Behandlung von TACACS+-Authentifizierungen verfügt. Sie müssen prüfen, ob Sie innerhalb des gewünschten Policy Service Node (PSN) die Funktion für den Device Admin Service haben. Navigieren Sie durch das Menü Administration > System > Deployment, wählen Sie den Knoten aus, an dem die ISE TACACS+ ausführt, und wählen Sie dann die Schaltfläche Edit.



Schritt 2. Blättern Sie nach unten, bis Sie die entsprechende Funktion namens Device Administration Service sehen (beachten Sie, dass für die Aktivierung dieser Funktion zunächst Policy Server-Personal auf dem Knoten aktiviert sein muss und außerdem Lizenzen für TACACS+ in Ihrer Bereitstellung verfügbar sind), aktivieren Sie dieses Kontrollkästchen, und speichern Sie dann die Konfiguration:

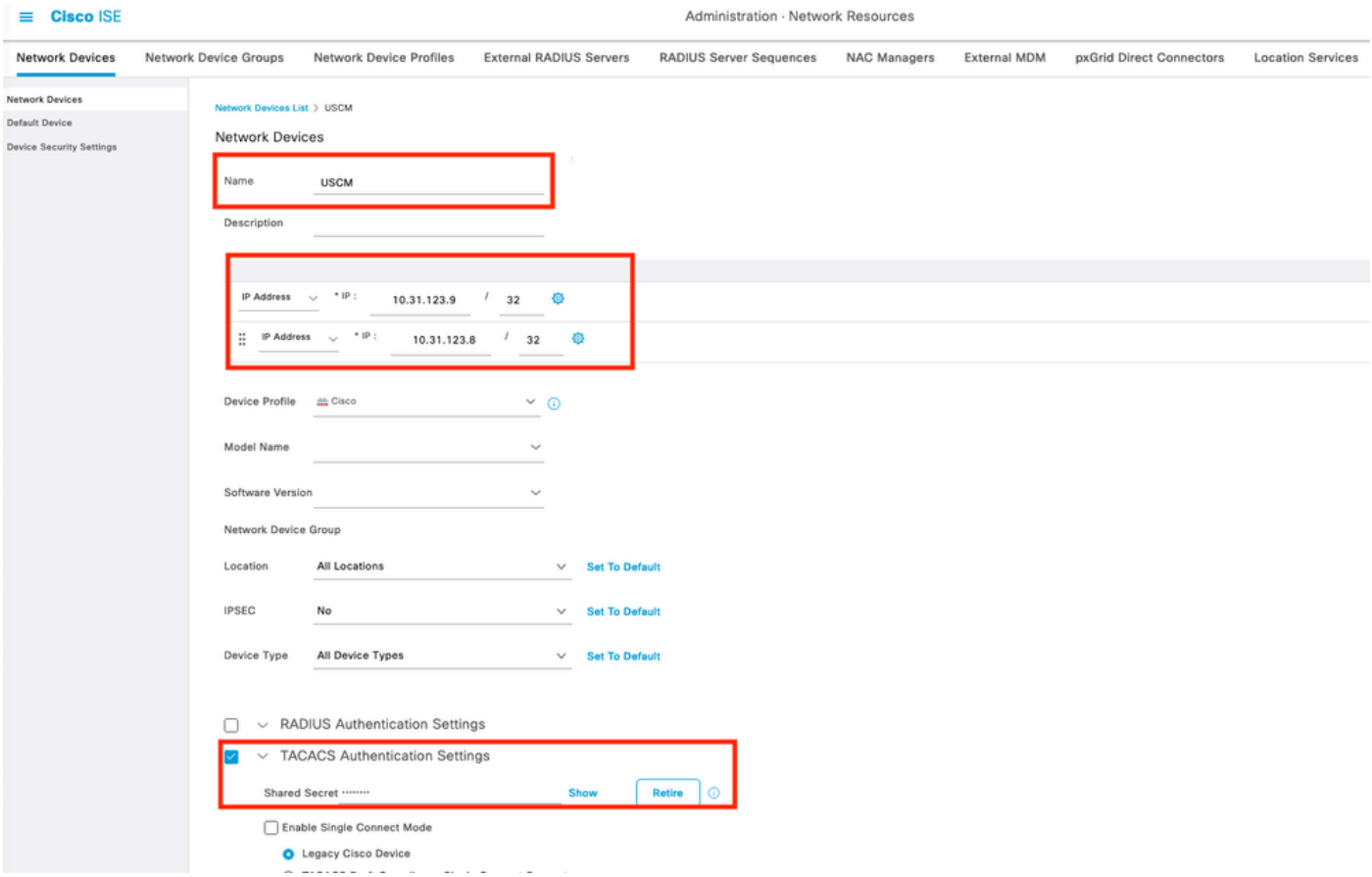


Schritt 3: Konfigurieren Sie das Netzwerkzugriffsgerät (Network Access Device, NAD), das die ISE als TACACS+-Server verwendet, navigieren Sie zum Menü Administration > Network Resources > Network Devices, und wählen Sie dann die Schaltfläche +Add.



Schritt 4. Konfigurieren Sie in diesem Abschnitt Folgendes:

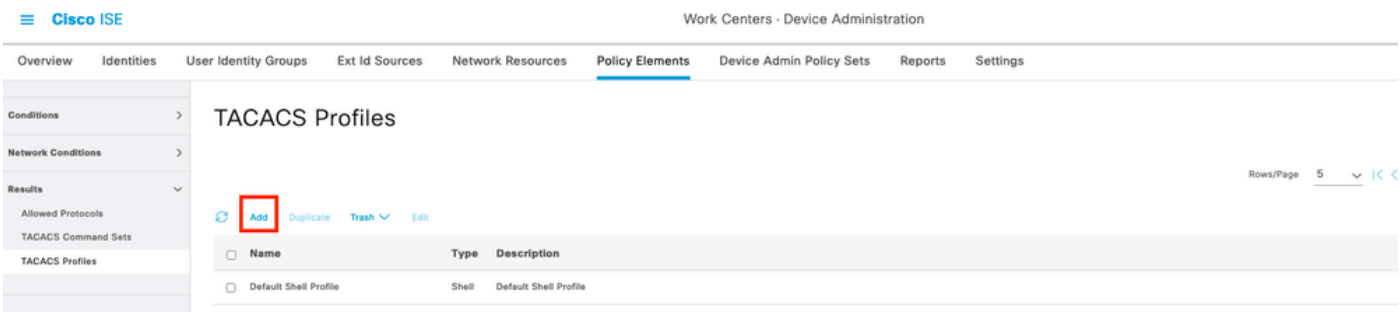
- Ein Name für das UCSM als TACACS+-Client.
- Die IP-Adressen, die das UCSM verwendet, um eine Anforderung an die ISE zu senden.
- Gemeinsamer TACACS+-Schlüssel: Dieses Kennwort wird zur Verschlüsselung der Pakete zwischen UCSM und ISE verwendet.



Anmerkung: Fügen Sie in Clusterkonfigurationen die IP-Adressen des Management-Ports für beide Fabric Interconnects hinzu. Mit dieser Konfiguration wird sichergestellt, dass sich Remote-Benutzer weiterhin anmelden können, wenn das erste Fabric Interconnect ausfällt und das System ein Failover zum zweiten Fabric Interconnect durchführt. Alle Anmeldeanfragen stammen von diesen IP-Adressen, nicht von der virtuellen IP-Adresse, die von Cisco UCS Manager verwendet wird.

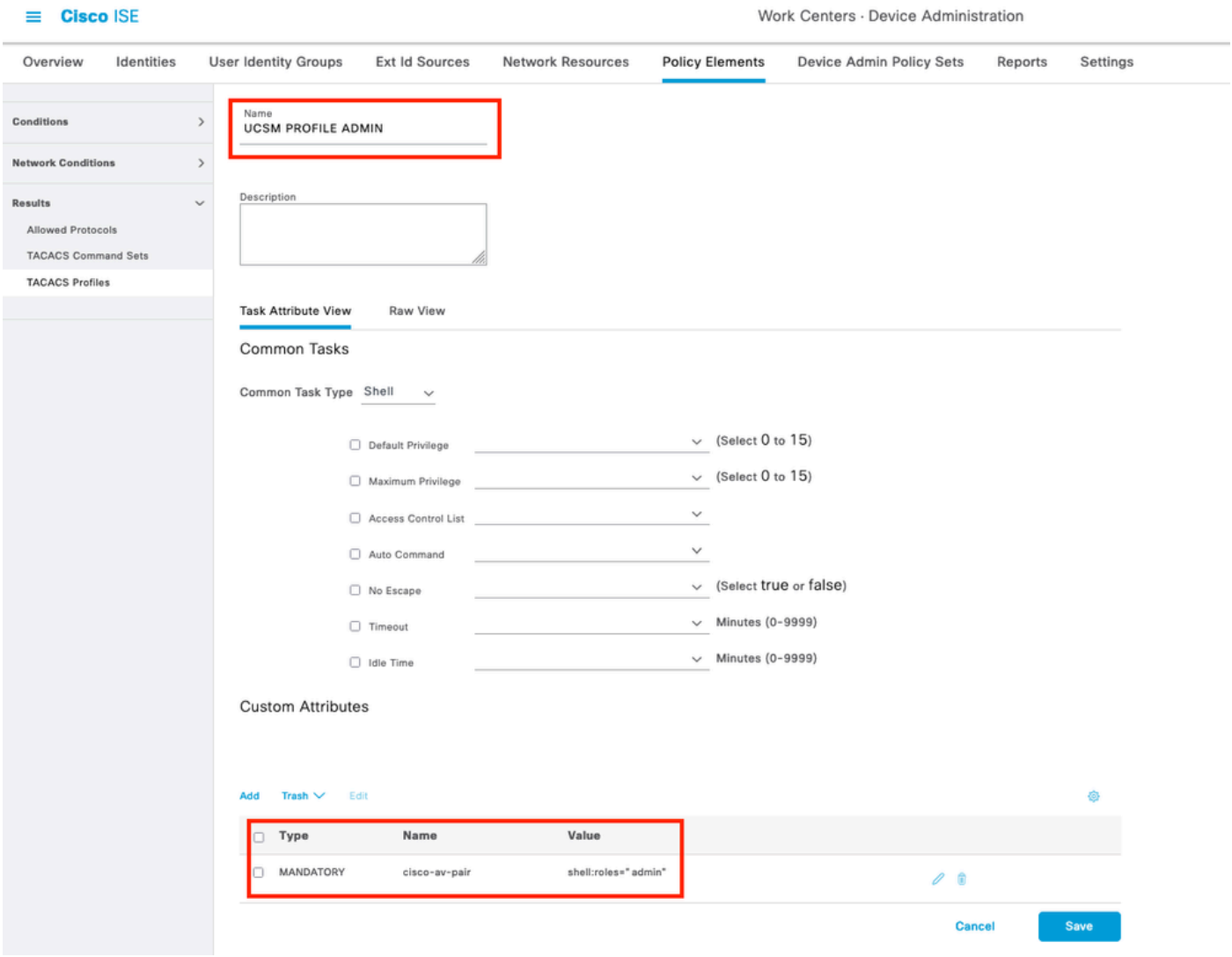
Konfigurieren der Attribute und Regeln für die ISE

Schritt 1. Erstellen Sie ein TACACS+-Profil, navigieren Sie zum Menü Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles , und wählen Sie Add

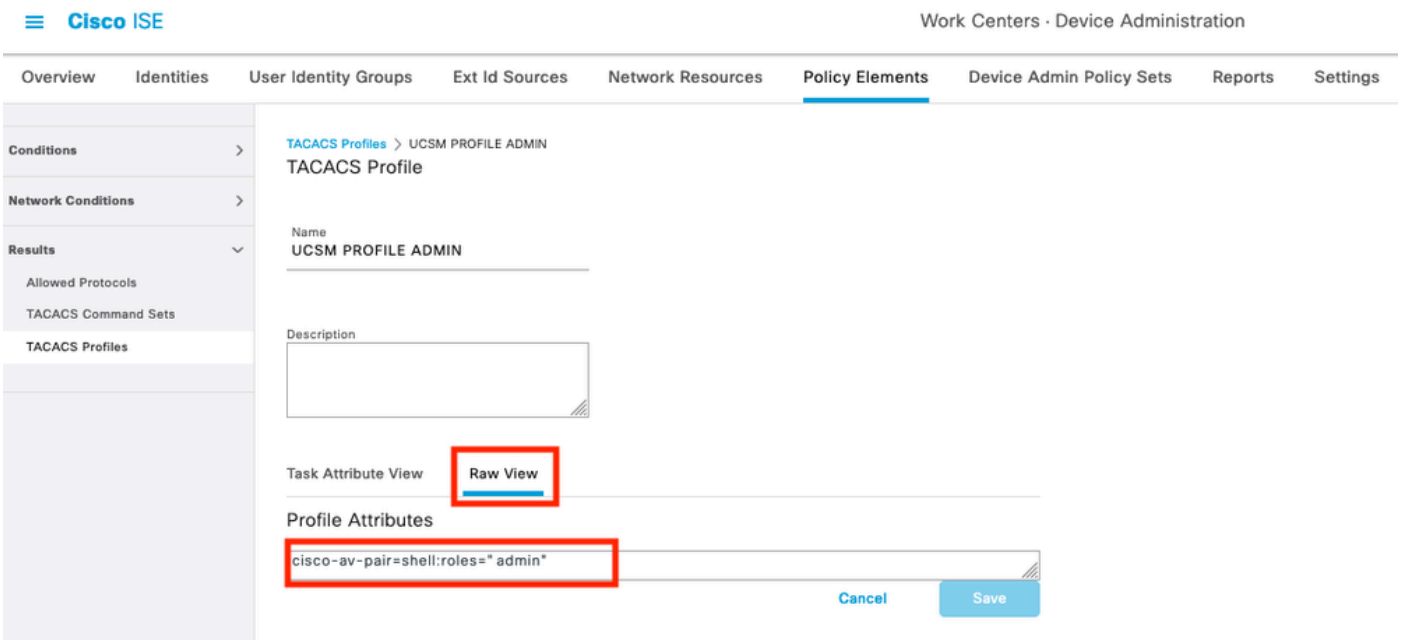


Schritt 2. In diesem Abschnitt konfigurieren Sie das Profil mit einem Namen und im Abschnitt Benutzerdefinierte Attribute wählen Sie Hinzufügen , als Nächstes erstellen Sie ein Attribut der

Eigenschaft MANDATORY , nennen Sie es als cisco-av-pair und im Wert wählen Sie eine der Rollen innerhalb des UCSM und geben Sie ein, dass als Shell-Rolle, in diesem Beispiel verwendet es die Rolle admin und die ausgewählte Eingabe muss shell:roles="admin" wie hier gezeigt,



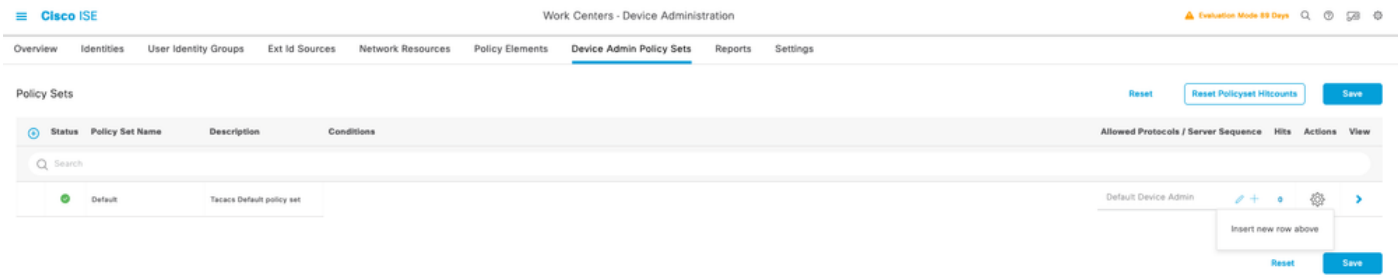
Wenn Sie im selben Menü die Rohansicht für das TACACS-Profil auswählen, können Sie die entsprechende Konfiguration des Attributs überprüfen, das über die ISE gesendet werden soll.



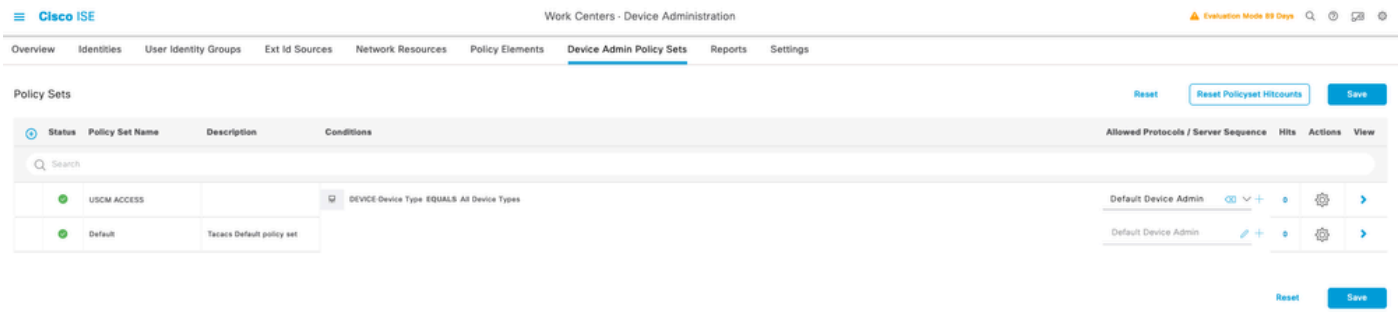
Anmerkung: Der cisco-av-pair-Name ist die Zeichenfolge, die die Attribut-ID für den TACACS+-Anbieter bereitstellt.

Schritt 3. Markieren Sie das Häkchen und speichern Sie Ihre Konfiguration.

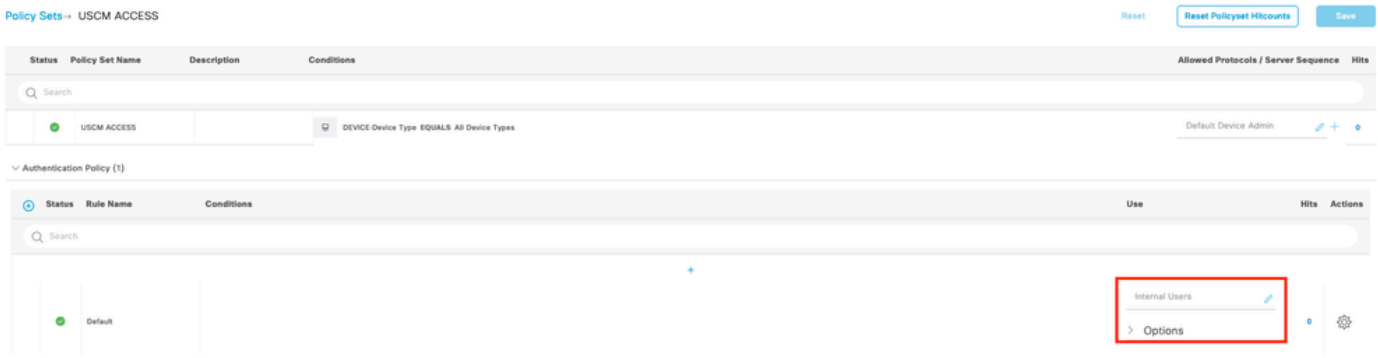
Schritt 4: Erstellen eines Geräte-Admin-Richtliniensatzes für Ihr UCSM, navigieren Sie im Menü Work Centers > Device Administration > Device Admin Policy Sets, und wählen Sie dann aus einem vorhandenen Richtliniensatz das Zahnrad-Symbol aus, um dann neue Zeile einfügen auszuwählen.



Schritt 5. Benennen Sie diesen neuen Richtliniensatz, fügen Sie Bedingungen hinzu, die von den Merkmalen der TACACS+-Authentifizierungen abhängen, die vom UCSM-Server ausgeführt werden, und wählen Sie Zulässige Protokolle > Standardgeräteadministrator, speichern Sie Ihre Konfiguration.

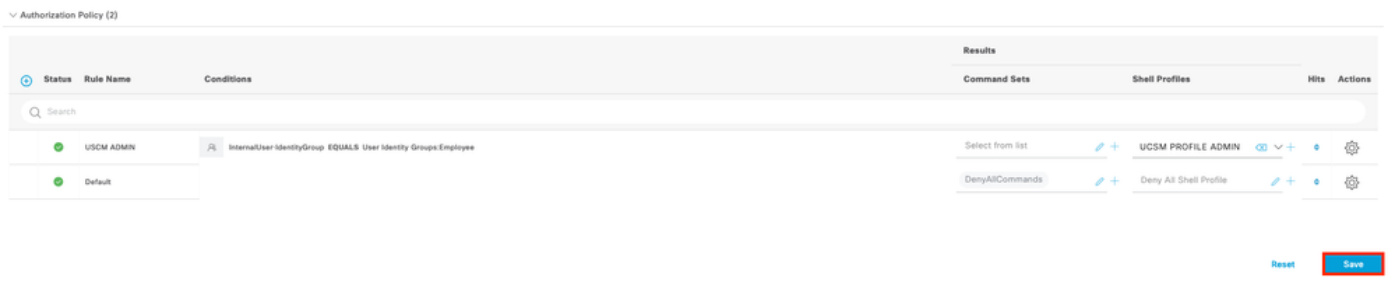


Schritt 6. Wählen Sie in der Ansichtsoption > aus, und wählen Sie im Abschnitt Authentifizierungsrichtlinie die externe Identitätsquelle aus, von der die ISE den Benutzernamen und die im UCSM eingegebenen Anmeldeinformationen abfragt. In diesem Beispiel entsprechen die Anmeldeinformationen internen Benutzern, die in der ISE gespeichert sind.



Schritt 7: Blättern Sie nach unten bis zum Abschnitt Autorisierungsrichtlinie bis zur Standardrichtlinie, wählen Sie das Zahnradsymbol aus, und fügen Sie dann eine Regel ein.

Schritt 8: Benennen Sie die neue Autorisierungsregel, fügen Sie Bedingungen für den Benutzer hinzu, die bereits als Gruppenmitgliedschaft authentifiziert wurden, und speichern Sie die Konfiguration im Abschnitt Shell Profiles (Shell-Profile), und fügen Sie das zuvor konfigurierte TACACS-Profil hinzu.



TACACS+-Konfiguration auf UCSM

Melden Sie sich mit einem Benutzer mit Administratorrechten bei**Cisco UCS Manager**der GUI an.

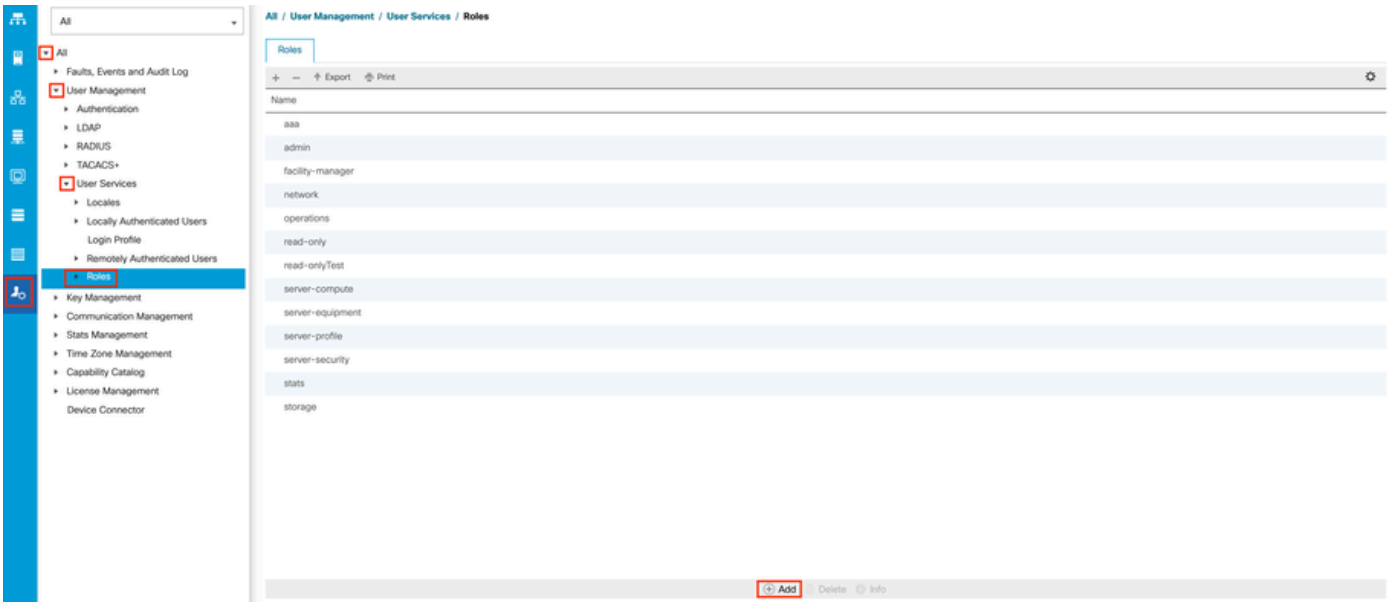
Rollen für Benutzer erstellen

Schritt 1: Wählen Sie im Navigationsbereich die Registerkarte Admin (Admin) aus.
Schritt 2: Erweitern Sie auf der Registerkarte Admin die Option All (Alle) > User Management (Benutzerverwaltung) > User Services (Benutzerdienste) > Roles (Rollen).

Schritt 3. Wählen Sie**Work**im Bereich die Registerkarte**General**aus.

Schritt 4: Wählen Sie Hinzufügen für benutzerdefinierte Rollen aus. In diesem Beispiel werden Standardrollen verwendet.

Schritt 5: Überprüfen der Übereinstimmung der Namensrolle mit dem zuvor im TACACS-Profil konfigurierten Namen

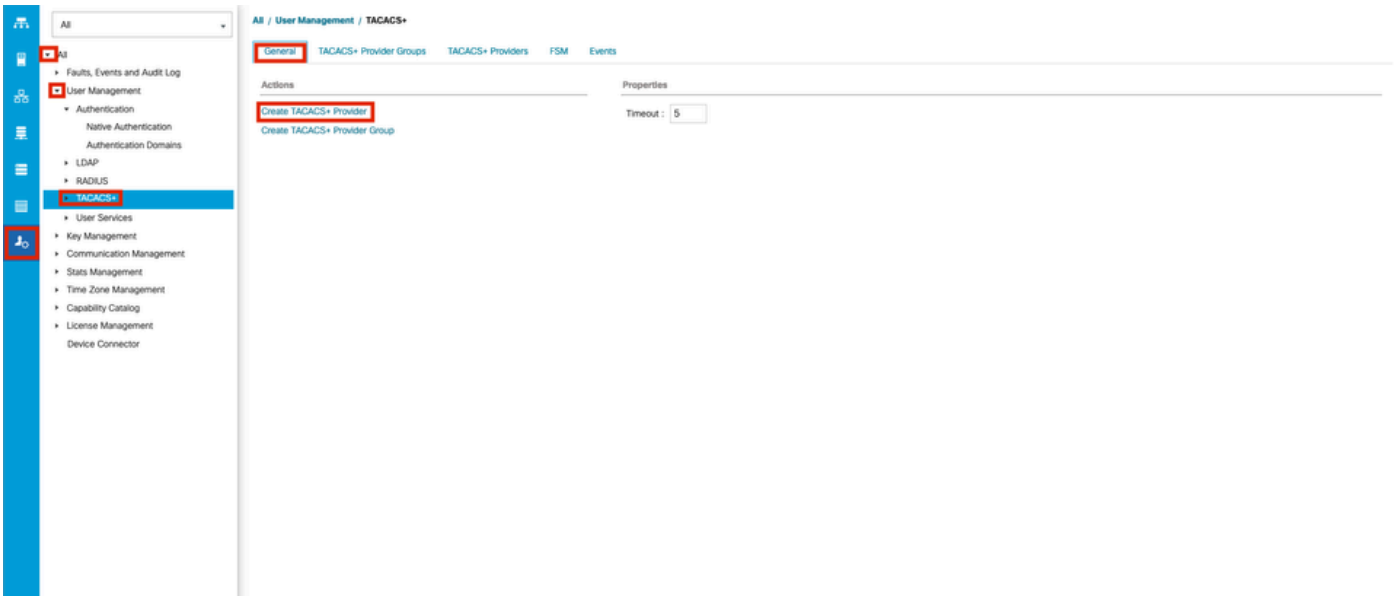


Erstellen eines TACACS+-Anbieters

Schritt 1: Wählen Sie im Navigationsbereich die Registerkarte Admin (Admin) aus.
Schritt 2: Erweitern Sie auf der Registerkarte Admin die Option All (Alle) > User Management (Benutzerverwaltung) > TACACS+.

Schritt 3. Wählen Sie**Work**im Bereich die**General** Registerkarte aus.

Schritt 4. Wählen Sie**Actions**im Bereich**Create TACACS+ Provider.**



Schritt 5. Geben Sie**Create TACACS+ Provider**im Assistenten die entsprechenden Informationen ein.

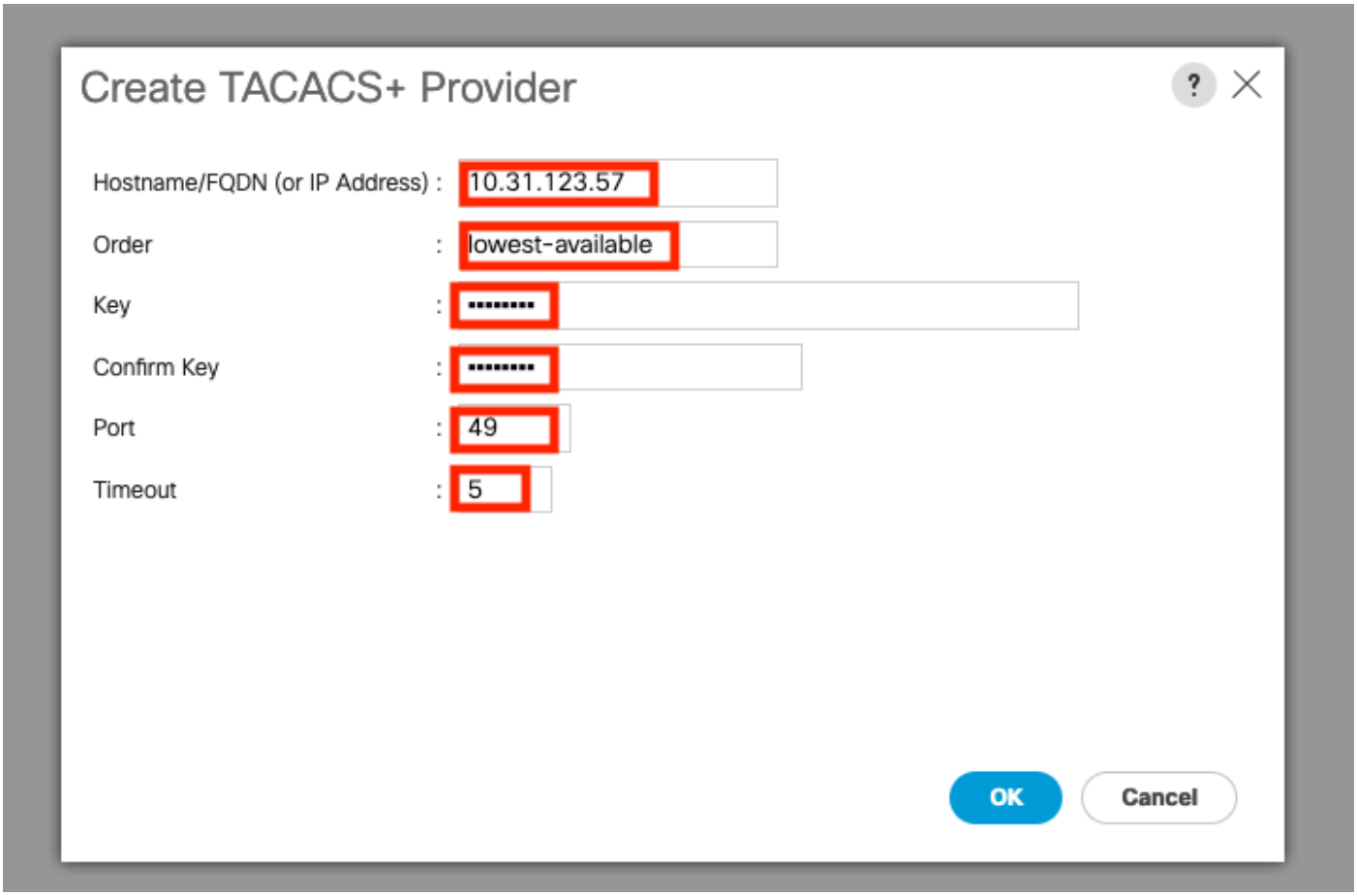
- Geben Sie im Feld Hostname die IP-Adresse oder den Hostnamen des TACACS+-Servers ein.
- Im Feld "Order" (Bestellung) die Reihenfolge, in der Cisco UCS diesen Anbieter zur Benutzerauthentifizierung verwendet.

  Geben Sie eine Ganzzahl zwischen 1 und 16 ein, oder geben Sie den kleinsten verfügbaren Wert oder 0 (Null) ein, wenn Cisco UCS die nächste verfügbare Reihenfolge basierend auf den anderen Anbietern zuweisen soll, die in dieser Cisco UCS-Instanz definiert sind.

- Geben Sie im Feld Key (Schlüssel) den SSL-Verschlüsselungsschlüssel für die Datenbank ein.

- Im Feld Confirm Key (Schlüssel bestätigen) wird der SSL-Verschlüsselungsschlüssel zur Bestätigung wiederholt.
- Im Feld Port den Port, über den Cisco UCS mit der TACACS+-Datenbank kommuniziert (Standardport für Port 49).

- Geben Sie im Feld Timeout (Zeitüberschreitung) die Zeitdauer in Sekunden an, die das System vor dem Timeout mit der TACACS+-Datenbank verbringt.



Schritt 6. Wählen Sie OK.

Anmerkung: Wenn Sie einen Hostnamen anstelle einer IP-Adresse verwenden, müssen Sie einen DNS-Server in Cisco UCS Manager konfigurieren.

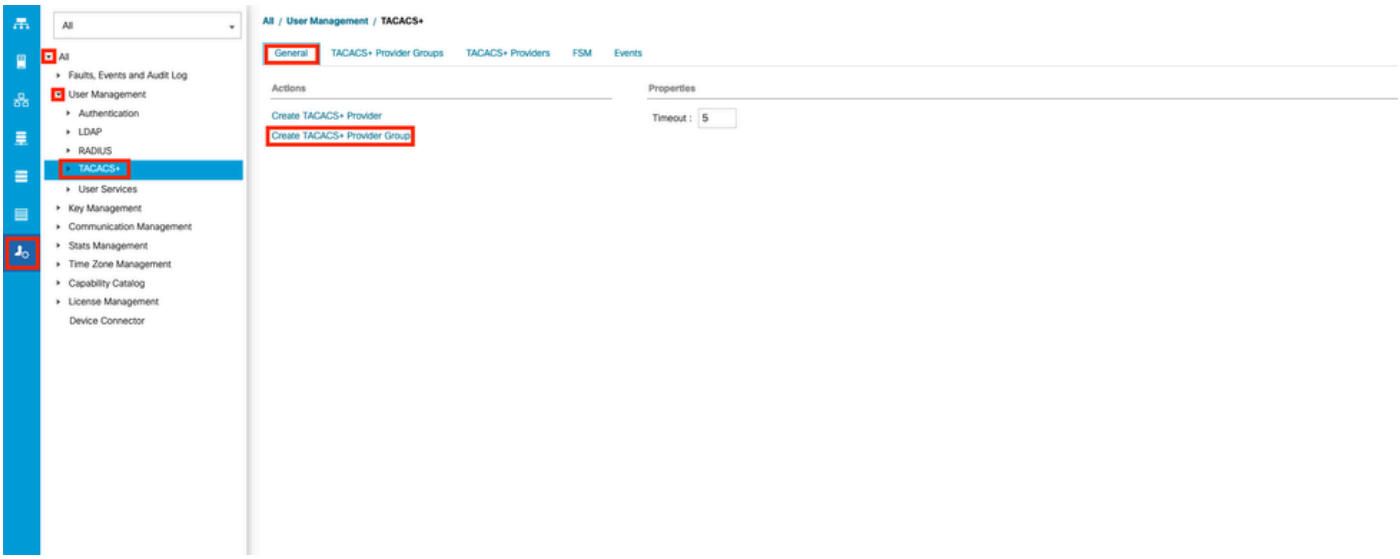
Erstellen einer TACAC+-Anbietergruppe

Schritt 1.Wählen Sie**Navigation**im Bereich die **Admin** Registerkarte aus.

Schritt 2. Erweitern Sie auf**Admin**der Registerkarte **All** > **User Management** > **TACACS+**.

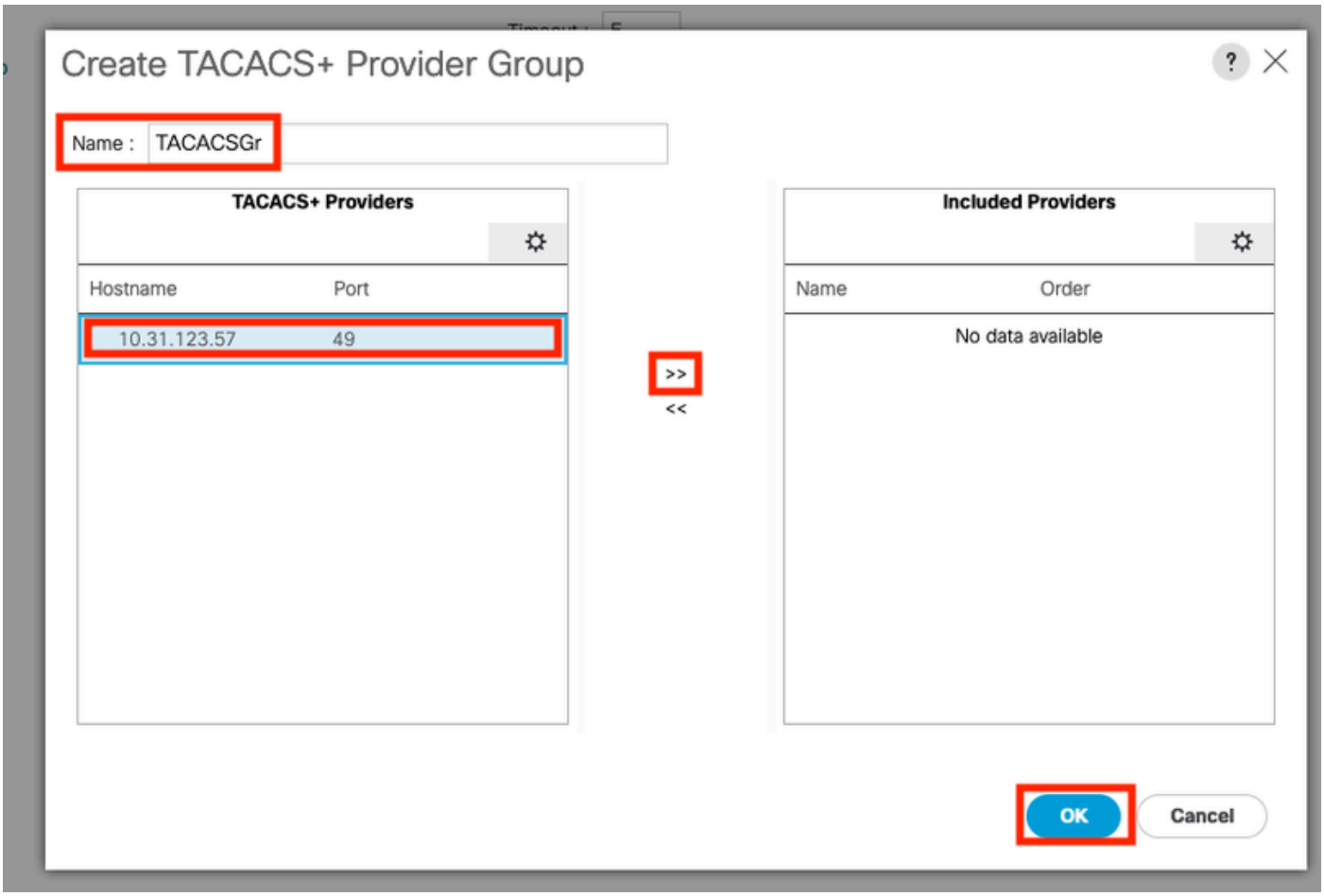
Schritt 3. Wählen Sie**Work**im Bereich die **General** Registerkarte aus.

Schritt 4. Wählen Sie**Actions**im Bereich Gruppe Create TACACS+ Provideraus.



Schritt 5: Geben Sie im Dialogfeld Create TACACS+ Provider Group (TACACS+-Anbietergruppe erstellen) die angeforderten Informationen ein.

- Geben Sie im Feld Name einen eindeutigen Namen für die Gruppe ein.
- Wählen Sie in der Tabelle TACACS+-Anbieter die Anbieter aus, die in die Gruppe aufgenommen werden sollen.
- Wählen Sie die Schaltfläche >>, um die Anbieter der Tabelle Eingeschlossene Anbieter hinzuzufügen.



Schritt 6. Wählen Sie OK.

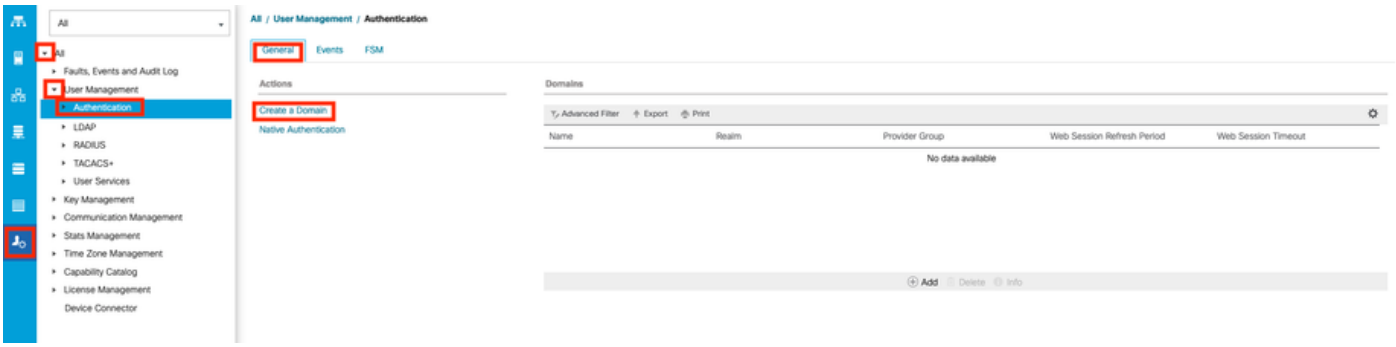
Erstellen einer Authentifizierungsdomäne

Schritt 1. Wählen Sie im **Navigation** Bereich die **Admin** Registerkarte aus.

Schritt 2: Erweitern Sie auf der **Admin** Registerkarte **All** > **User Management** > **Authentication**

Schritt 3. Wählen Sie**Work**im Bereich die **General** Registerkarte aus.

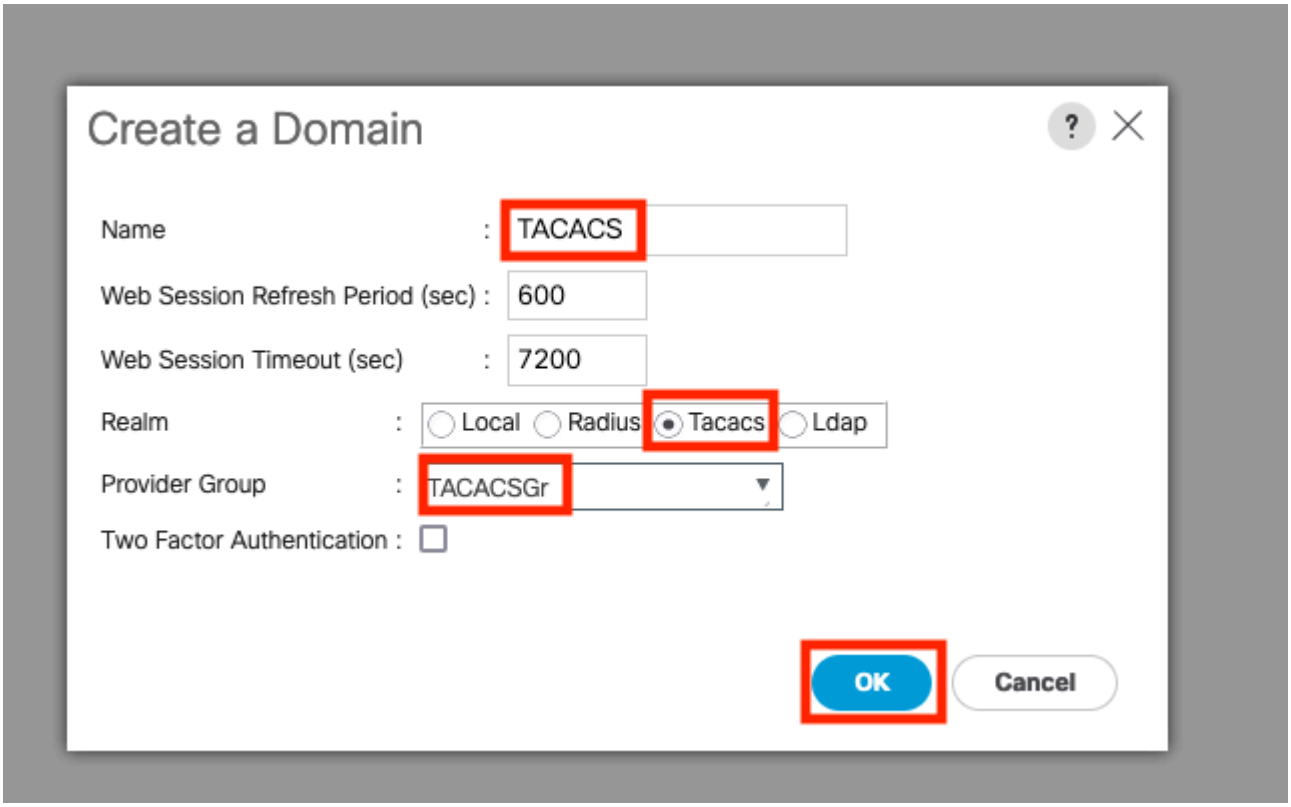
Schritt 4. Wählen Sie**Actions**im Bereich**Create a Domain.**



Schritt 5. Geben Sie im Dialogfeld Create Domain (Domäne erstellen) die angeforderten Informationen ein.

- Geben Sie im Feld Name einen eindeutigen Namen für die Domäne ein.

- Wählen Sie im Bereich die Option TACACS aus.
- Wählen Sie in der Dropdown-Liste Provider Group (Anbietergruppe) die zuvor erstellte TACACS+-Anbietergruppe aus, und wählen Sie OK.



Fehlerbehebung

Häufige TACACS+-Probleme mit UCSM

- Falscher Schlüssel oder ungültige Zeichen.
- Falscher Port.
- Keine Kommunikation mit unserem Anbieter aufgrund einer Firewall- oder Proxy-Regel.
- FSM liegt nicht bei 100 %.

Überprüfen der UCSM TACACS+-Konfiguration:

Sie müssen sicherstellen, dass UCSM die Konfiguration implementiert hat, mit der der Status des Finite-State-Rechners (FSM) überprüft wird, um den Status als 100 % abgeschlossen anzuzeigen.

Überprüfen der Konfiguration über die UCSM-Befehlszeile

<#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:
```

Überprüfen Sie die TACACS-Konfiguration vom NX-OS:

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups

```
[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)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*******
total number of servers:1

following TACACS+ servers are configured:
        10.31.123.57:
                available on port:49
                TACACS+ shared secret:********
                timeout:5
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group tacacs:
                server 10.31.123.57 on port 49
                deadtime is 0
                vrf is management
        group TACACSGr:
                server 10.31.123.57 on port 49
                deadtime is 0
                vrf is management
```

Um die Authentifizierung über NX-OS zu testen, verwenden Sie**test aaa**den Befehl (nur über NX-OS verfügbar).

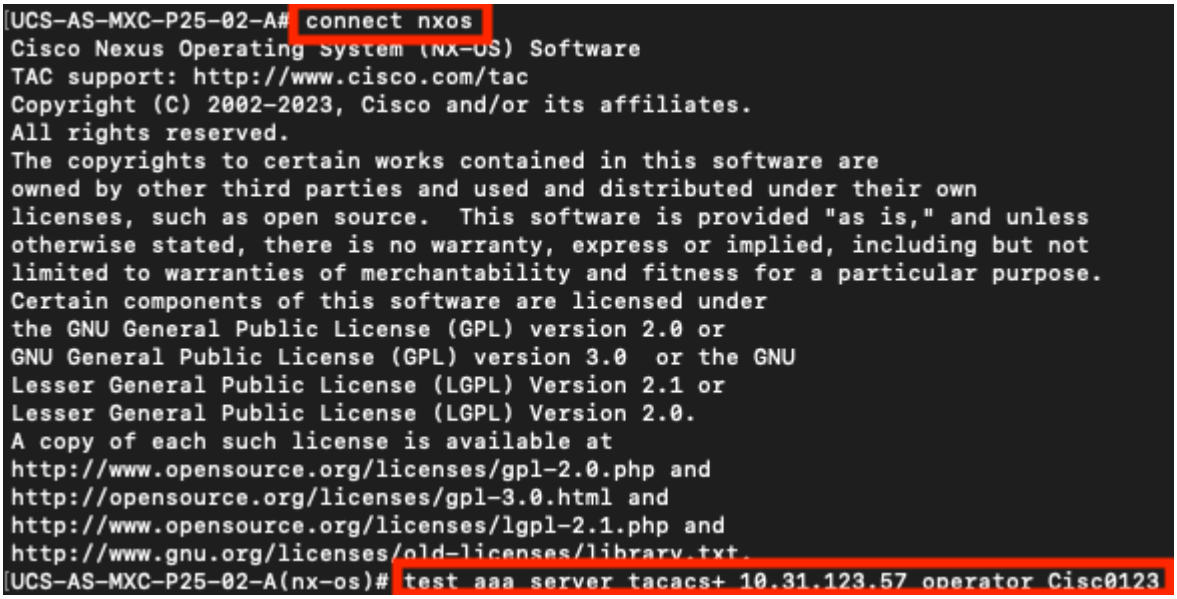
Validieren Sie die Konfiguration unseres Servers:

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

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



UCSM-Prüfung

Überprüfung der Erreichbarkeit

<#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
```

Portüberprüfung

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

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

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco 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)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.
```

Die effektivste Methode, um Fehler zu erkennen, ist das Aktivieren des NXOS-Debugging. Mit dieser Ausgabe können Sie die Gruppen, die Verbindung und die Fehlermeldung anzeigen, die zu Fehlkommunikation führt.

- Öffnen Sie eine SSH-Sitzung mit UCSM, und melden Sie sich mit einem beliebigen privilegierten Benutzer mit Administratorberechtigungen (vorzugsweise einem lokalen Benutzer) an, ändern Sie den NX-OS CLI-Kontext, und starten Sie den Terminalmonitor.

<#root>

```
UCS-A#
connect nxos

UCS-A(nx-os)#
terminal monitor
```

- Aktivieren Sie Debug-Flags, und überprüfen Sie die SSH-Sitzungsausgabe in der Protokolldatei.

<#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
```

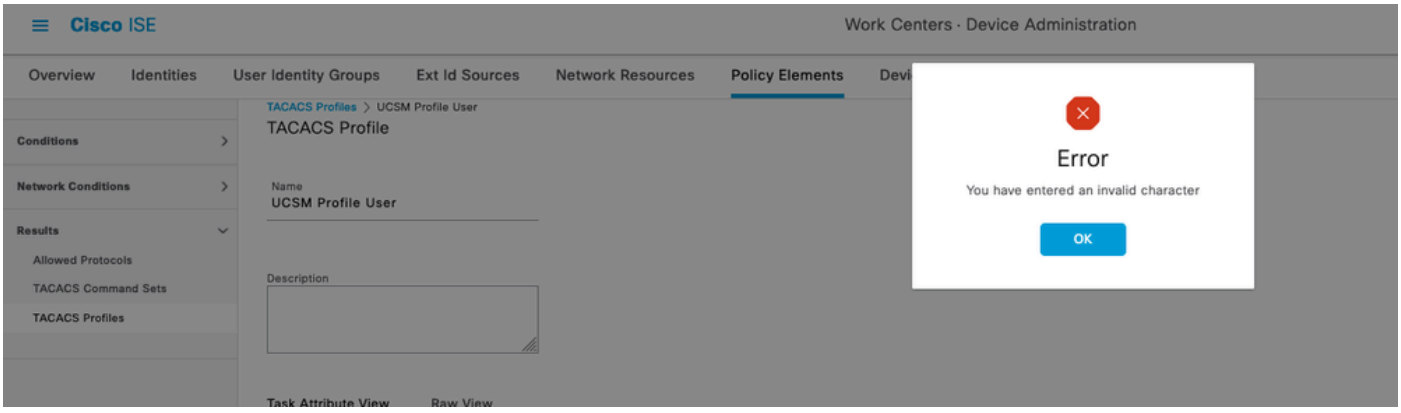
```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and 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)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all
```

- Öffnen Sie nun eine neue GUI- oder CLI-Sitzung, und versuchen Sie, sich als Remote-Benutzer (TACACS+) anzumelden.
- Sobald Sie eine Meldung über einen Anmeldefehler erhalten haben, deaktivieren Sie die Debugs, die die Sitzung oder mit diesem Befehl schließen.

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

Häufige Fragen im Zusammenhang mit TACACs und ISE

- In der ISE wird dieses Verhalten angezeigt, wenn versucht wird, ein TACACS-Profil in den Attributen zu konfigurieren, die für UCSM zum Zuweisen der entsprechenden Rollen für den Administrator oder eine andere Rolle erforderlich sind. Wählen Sie diese Option auf der Schaltfläche zum Speichern aus, um dieses Verhalten anzuzeigen:



Dieser Fehler ist auf den folgenden Fehler zurückzuführen: https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917 , bitte stellen Sie sicher, dass Sie den Ort gefunden haben, an dem dieser Fehler behoben wurde.

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 Administration > 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.

<#root>

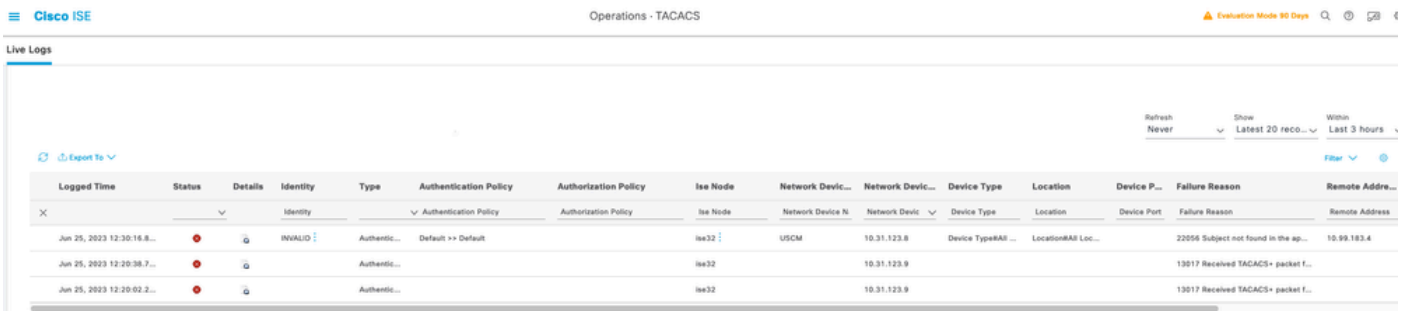
```
ise32/admin#
```

show ports | include 49

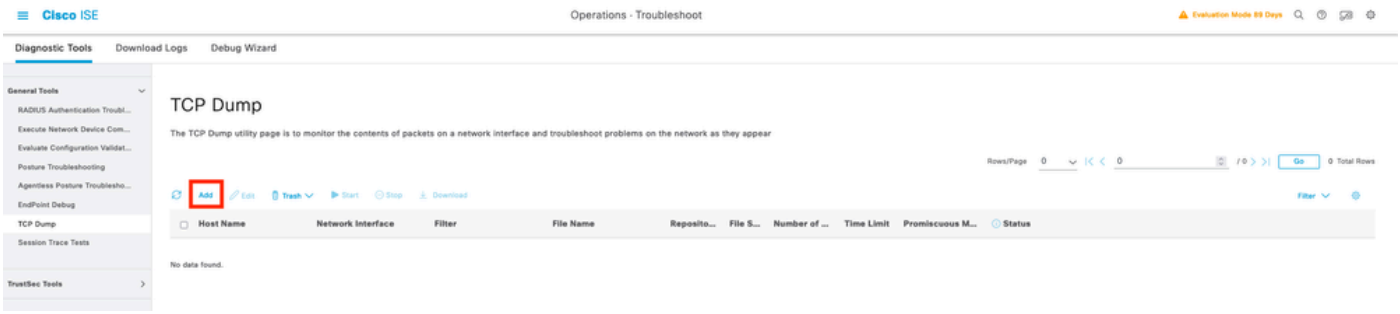
```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Schritt 2. Bestätigen Sie, ob Livelogs zu TACACS+-Authentifizierungsversuchen vorhanden sind: Dies kann im Menü Vorgänge > TACACS > Live-Protokolle überprüft werden.

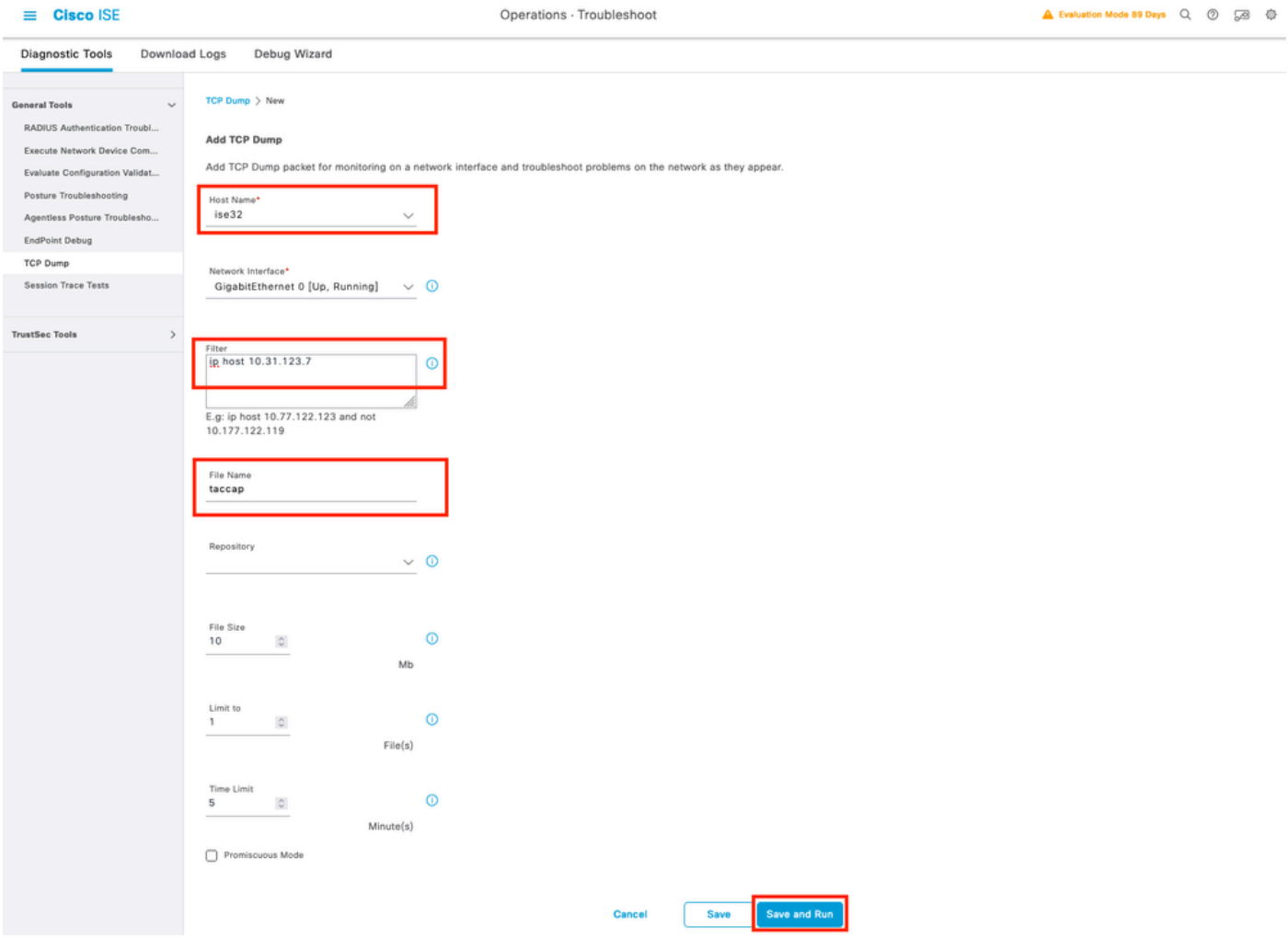
Abhängig vom Fehlergrund können Sie die Konfiguration anpassen oder die Fehlerursache beheben.



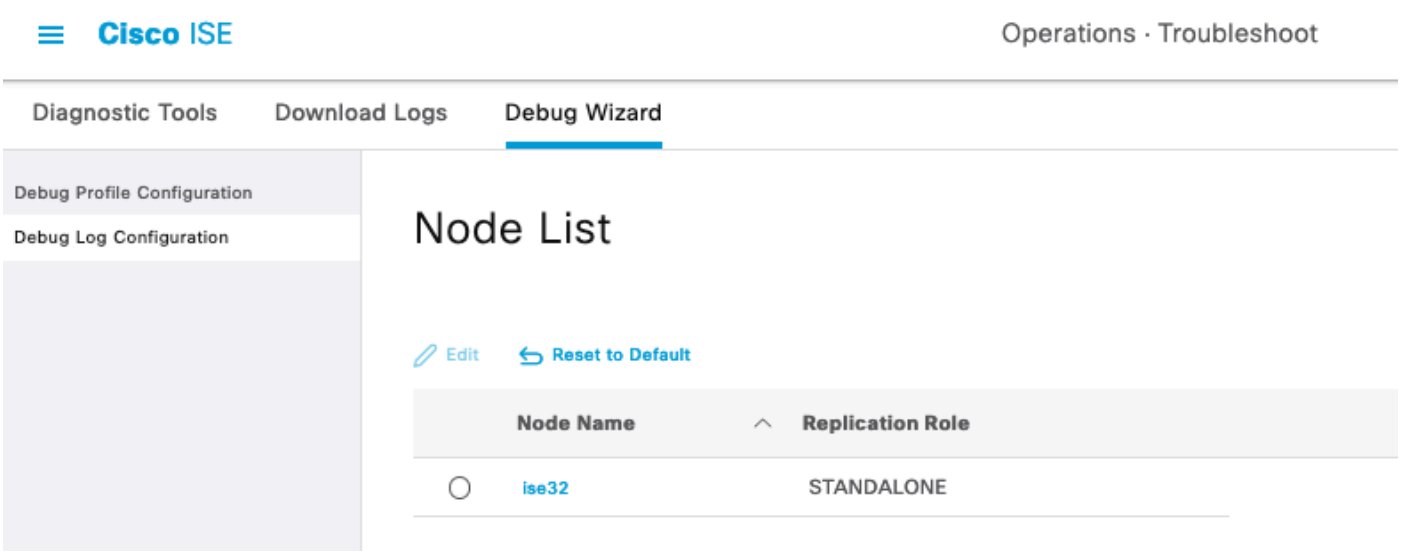
Schritt 3. Falls kein Livelog angezeigt wird, fahren Sie mit der Paketerfassung fort, navigieren Sie zum Menü Vorgänge > Fehlerbehebung > Diagnosetools > Allgemeine Tools > TCP-Dump, und wählen Sie beim Hinzufügen



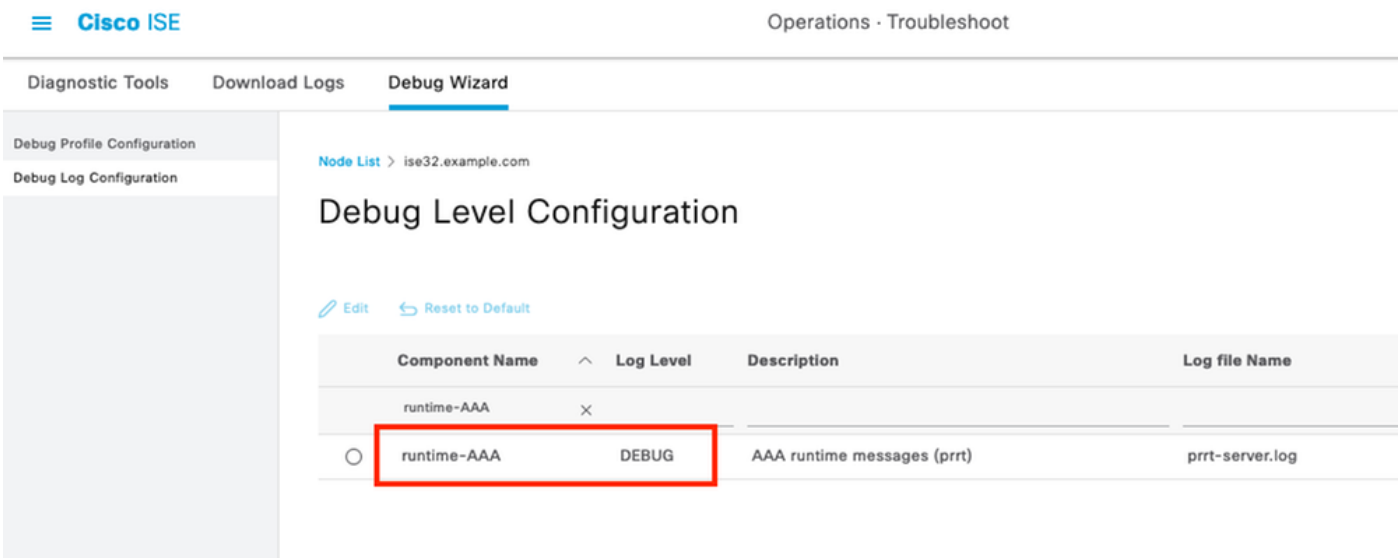
Wählen Sie den Policy Service-Knoten aus, von dem aus UCSM die Authentifizierung sendet, und fahren Sie dann in Filtern mit dem Eingabe-IP-Host X.X.X.X fort, der der IP des UCSM entspricht, von dem aus die Authentifizierung gesendet wird. Benennen Sie die Erfassung, und scrollen Sie nach unten, um zu speichern, führen Sie die Erfassung aus, und melden Sie sich bei UCSM an.



Schritt 4. Aktivieren Sie die Komponente Runtime-AAA im Debugging innerhalb des PSN, von wo aus die Authentifizierung in Operationen ausgeführt wird > Fehlerbehebung > Debug-Assistent > Debug-Protokollkonfiguration, wählen Sie PSN-Knoten aus, und wählen Sie dann Weiter in der Bearbeitungsschaltfläche .



Suchen Sie nach der Komponente Runtime-AAA, ändern Sie deren Ebene zu debug, um das Problem dann erneut zu reproduzieren, und fahren Sie mit der Analyse der Protokolle fort.



Anmerkung: Weitere Informationen finden Sie im Video auf dem Cisco Youtube-Kanal How to Enable Deubgs on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8 .

Zugehörige Informationen

Administrationsleitfaden für Cisco UCS Manager

Cisco UCS CIMC Konfigurationsleitfaden TACACS+

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.