Konfigurieren von ASR9K TACACS mit der Cisco Identity Services Engine 2.4

Inhalt

Einführung

In diesem Dokument wird die Konfiguration des ASR Aggregation Services Routers (ASR) der Serie 9000 beschrieben, um die Authentifizierung und Autorisierung über TACACS+ mit dem Cisco Identity Services Engine 2.4-Server durchzuführen.

Hintergrundinformationen

Es zeigt die Implementierung des Verwaltungsmodells der aufgabenbasierten Autorisierung, das zur Kontrolle des Benutzerzugriffs im Cisco IOS® XR-Softwaresystem verwendet wird. Die wichtigsten Aufgaben für die Implementierung der aufgabenbasierten Autorisierung umfassen die Konfiguration von Benutzergruppen und Aufgabengruppen. Benutzergruppen und Aufgabengruppen werden über den Befehlssatz der Cisco IOS® XR-Software konfiguriert, der für AAA-Dienste (Authentication, Authorization and Accounting) verwendet wird. Authentifizierungsbefehle werden verwendet, um die Identität eines Benutzers oder Prinzipals zu überprüfen. Mithilfe von Autorisierungsbefehlen wird überprüft, ob einem authentifizierten Benutzer (oder Prinzipal) Berechtigungen für eine bestimmte Aufgabe erteilt werden. Accounting-Befehle werden zur Protokollierung von Sitzungen und zum Erstellen eines Prüfpfads verwendet, indem bestimmte vom Benutzer oder vom System generierte Aktionen aufgezeichnet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ASR 9000 - Bereitstellung und Basiskonfiguration
- TACACS+-Protokoll
- ISE 2.4 - Bereitstellung und Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASR 9000 mit Cisco IOS® XR Software, Version 5.3.4
- Cisco ISE 2.4

Die Informationen in diesem Dokument werden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn das Netzwerk in Betrieb ist, stellen Sie sicher, dass die potenziellen Auswirkungen von Konfigurationsänderungen vollständig verstanden werden.

Konfigurieren

Vordefinierte Komponenten auf IOS® XR

In IOS® XR gibt es vordefinierte Benutzergruppen und Aufgabengruppen. Der Administrator kann diese vordefinierten Gruppen verwenden oder benutzerdefinierte Gruppen je nach Anforderung definieren.

Vordefinierte Benutzergruppen

Diese Benutzergruppen sind in IOS® XR vordefiniert:

Benutzergruppe	Berechtigungen
Cisco Support	Funktionen zum Debuggen und Beheben von Fehlern (in der Regel von Mitarbeiter technischen Supports von Cisco verwendet).
netadmin	Konfigurieren Sie Netzwerkprotokolle wie Open Shortest Path First (OSPF) (in der von Netzwerkadministratoren verwendet).
Operator	Durchführen alltäglicher Überwachungsaktivitäten mit eingeschränkten Konfigurationsrechten.
Root-lr	Anzeigen und Ausführen aller Befehle in einem einzigen RP
Root-System	Anzeigen und Ausführen aller Befehle für alle RPs im System.
Systemadministrator	Führen Sie Systemverwaltungsaufgaben für den Router aus, z. B. zum Erhalten de Speicherorts der Core Dumps oder zum Einrichten der Network Time Protocol (NTI Uhr.
Service-Administrator	Durchführen von Dienstverwaltungsaufgaben, z. B. Session Border Controller (SBC

Jeder vordefinierten Benutzergruppe sind bestimmte Aufgabengruppen zugeordnet, die nicht

geändert werden können. Verwenden Sie diese Befehle, um die vordefinierten Benutzergruppen zu überprüfen:

```
RP/0/RSP0/CPU0:ASR9k#sh aaa usergroup ?

 |              Output Modifiers
 root-lr        Name of the usergroup
 netadmin       Name of the usergroup
 operator       Name of the usergroup
 sysadmin       Name of the usergroup
 retrieval      Name of the usergroup
 maintenance    Name of the usergroup
 root-system    Name of the usergroup
 provisioning   Name of the usergroup
 read-only-tg   Name of the usergroup
 serviceadmin   Name of the usergroup
 cisco-support  Name of the usergroup
 WORD           Name of the usergroup
 <cr>
```

Vordefinierte Aufgabengruppen

Diese vordefinierten Aufgabengruppen können von Administratoren in der Regel für die Erstkonfiguration verwendet werden:

- cisco-support: Aufgaben des Cisco Support-Personals
- netadmin: Netzwerkadministratoraufgaben
- Operator: Tagesaufgaben von Operatoren (zu Demonstrationszwecken)
- root-lr: Administratoraufgaben für sichere Domänen-Router
- Root-System: Systemweite Administratoraufgaben
- sysadmin: Systemadministratoraufgaben
- ServiceAdmin: Serviceverwaltungsaufgaben

Verwenden Sie diese Befehle, um die vordefinierten Aufgabengruppen zu überprüfen:

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?

|              Output Modifiers
root-lr        Name of the taskgroup
netadmin       Name of the taskgroup
operator       Name of the taskgroup
sysadmin       Name of the taskgroup
root-system    Name of the taskgroup
serviceadmin   Name of the taskgroup
cisco-support  Name of the taskgroup
WORD           Name of the taskgroup
<cr>
```

Verwenden Sie diesen Befehl, um die unterstützten Aufgaben zu überprüfen:

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

Die folgende Liste enthält die unterstützten Aufgaben:

Aaa	ACL	Administrator	Ancp	ATM	Basisdienste	Bcdl	BF
Booten	Paket	Call Home	CDP	CEF	Kampagnen	Cisco Support	co
Krypto	Diag	Unzulässig	Treiber	DWDM	Eem	EIGRP	Et

Fabric	Fehlermanagement	Dateisystem	Firewall	FR	HDLC	Host-Services	HS
Bestand	IP-Services	IPv4	IPv6	Isis	L2VPN	Li	Lis
Lektionen	Überwachung	mpls-ldp	mpls-statisch	mpls-te	Multicast	NetFlow	Ne
OSPF	Ouni	PBR	pkg-mgmt	POS-Punkt	PPP	QoS	RC
Rippen	Root-lr	Root-System	Route Map	Routingrichtlinie	Sbc	SNMP	sc
Sysmgr	System	Transport	Einfacher Zugriff	Tunnel	Universell	VLAN	VF

Jede dieser Aufgaben kann mit einer dieser oder allen vier Berechtigungen zugewiesen werden:

Lesen	Gibt eine Bezeichnung an, die nur eine Leseoperation zulässt.
Schreiben	Gibt eine Bezeichnung an, die eine Änderungsoperation zulässt und implizit eine Leseoperatio zulässt.
Ausführen	Gibt eine Bezeichnung an, die eine Zugriffsoperation zulässt. z. B. Ping und Telnet.
Debuggen	Gibt eine Bezeichnung an, die einen Debugvorgang zulässt.

Benutzerdefinierte Aufgabengruppen

Administratoren können benutzerdefinierte Aufgabengruppen konfigurieren, um bestimmte Anforderungen zu erfüllen. Nachfolgend finden Sie ein Konfigurationsbeispiel:

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
  debug    Specify a debug-type task ID
  execute  Specify a execute-type task ID
  read     Specify a read-type task ID
  write    Specify a read-write-type task ID

RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
Task group 'TAC-Defined-TASK'

Task IDs included directly by this group:
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE

Task group 'TAC-Defined-TASK' has the following combined set
  of task IDs (including all inherited groups):
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE
```

Mit dem Befehl Describe können Sie ermitteln, welche Aufgabengruppe und welche Berechtigungen für einen bestimmten Befehl erforderlich sind.

Beispiel 1.

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
Package:
```

```
.....
User needs ALL of the following taskids:

aaa (READ)
RP/0/RSP1/CPU0:ASR9k#
```

Damit ein Benutzer den Befehl **show aaa usergroup** ausführen kann, sollte der Benutzergruppe die Task Read aa zugewiesen werden.

Beispiel 2.

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
Package:
.....
User needs ALL of the following taskids:

aaa (READ WRITE)
RP/0/RSP1/CPU0:ASR9k(config)#
```

Damit ein Benutzer die **Standardtastenkombinationen für** die **Standardauthentifizierungsanmeldung+** im Konfigurationsmodus ausführen kann, sollte der Aufgabengruppe: **Task Read Write aa** zugewiesen werden.

Administratoren können die Benutzergruppe definieren, die mehrere Aufgabengruppen erben kann. Nachfolgend finden Sie das Konfigurationsbeispiel:

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:50:56.799 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ

RP/0/RSP1/CPU0:ASR9k#conf t
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:51:31.494 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'
  Inherits from task group 'TAC-Defined-TASK'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
```

```
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

AAA-Konfiguration auf dem Router

Konfigurieren Sie den TACACS-Server auf dem ASR-Router mit der IP-Adresse und dem gemeinsam genutzten geheimen Schlüssel.

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit
```

```
!
tacacs-server host 10.127.196.160 port 49
key 7 14141B180F0B
!
```

Konfigurieren Sie Authentifizierung und Autorisierung, um den konfigurierten TACACS-Server zu verwenden.

```
#aaa authentication login default group tacacs+ local
#aaa authorization exec default group tacacs+ local
```

Konfigurieren Sie die Befehlsautorisierung für die Verwendung des konfigurierten TACACS-Servers (optional):

> **Hinweis**: Stellen Sie sicher, dass die Authentifizierung und Autorisierung wie erwartet funktioniert, und stellen Sie sicher, dass die Befehlssätze ebenfalls korrekt konfiguriert sind, bevor Sie die Befehlsautorisierung aktivieren. Wenn die Konfiguration nicht korrekt ist, können Benutzer möglicherweise keine Befehle auf dem Gerät eingeben.

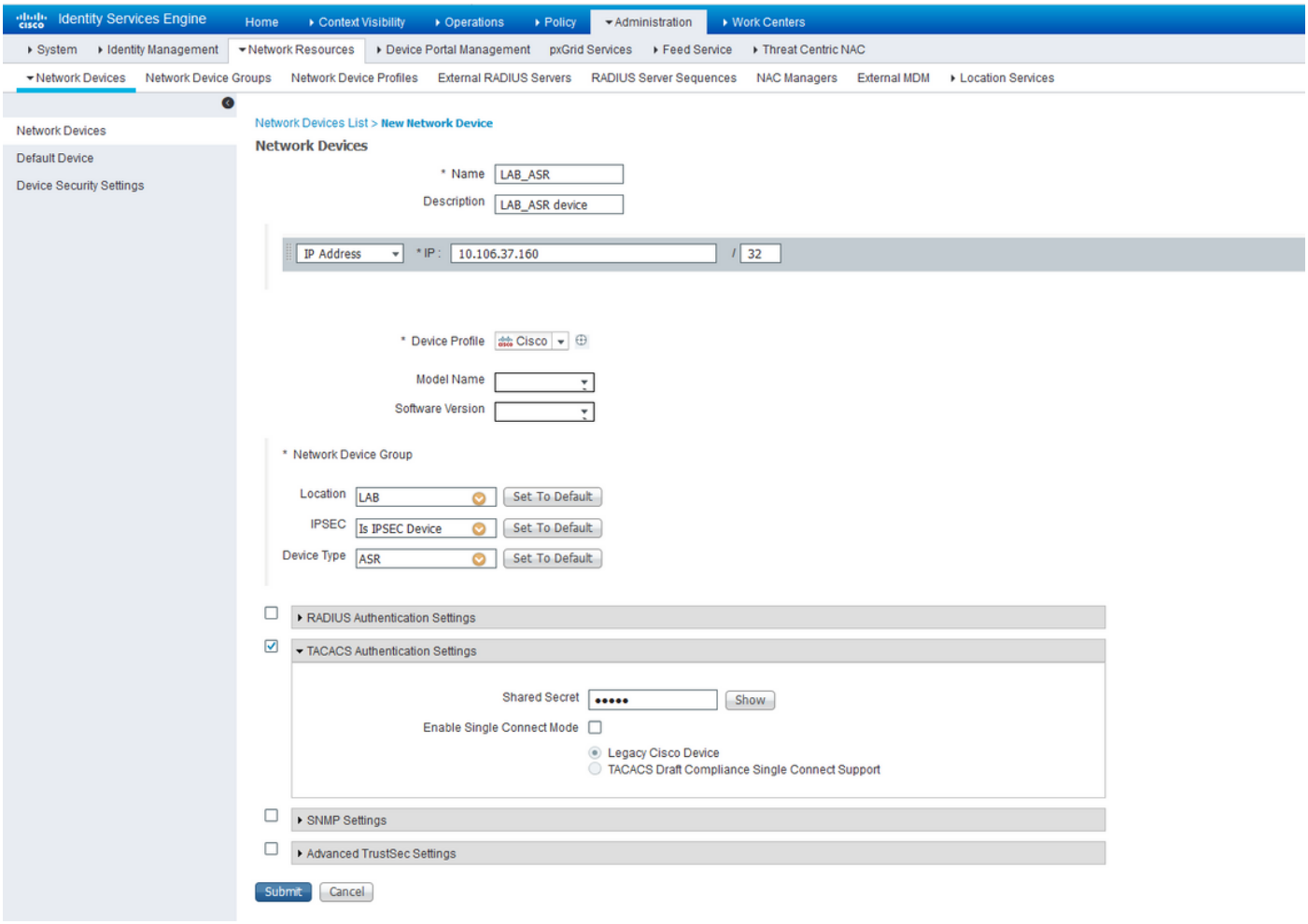
```
#aaa authorization commands default group tacacs+
```

Konfigurieren Sie die Befehlsabrechnung, um den konfigurierten TACACS-Server zu verwenden (optional).

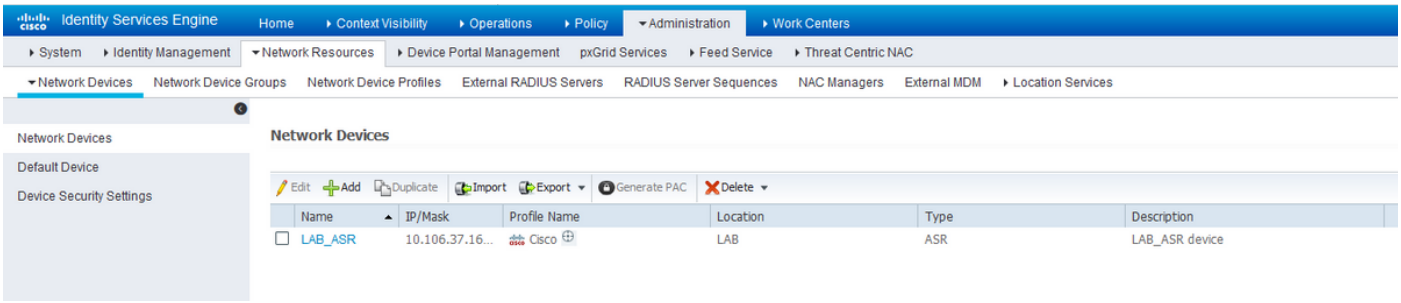
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE-Serverkonfiguration

Schritt 1: Um die Router-IP in der Liste der AAA-Clients auf dem ISE-Server zu definieren, navigieren Sie zu **Administration > N.Netzwerkressourcen > Netzwerkgeräte** wie im Bild gezeigt. Der gemeinsame geheime Schlüssel muss mit dem auf dem ASR-Router konfigurierten geheim sein, wie im Bild gezeigt.



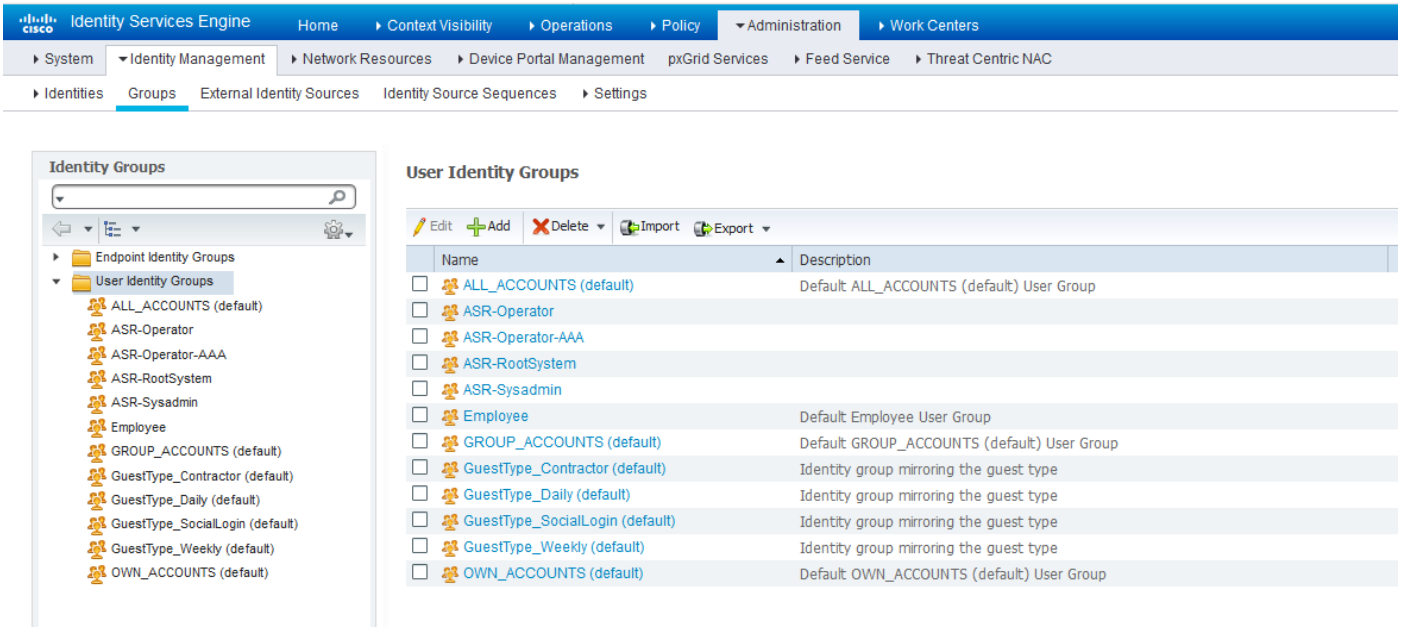
Konfiguration von Netzwerkgeräten



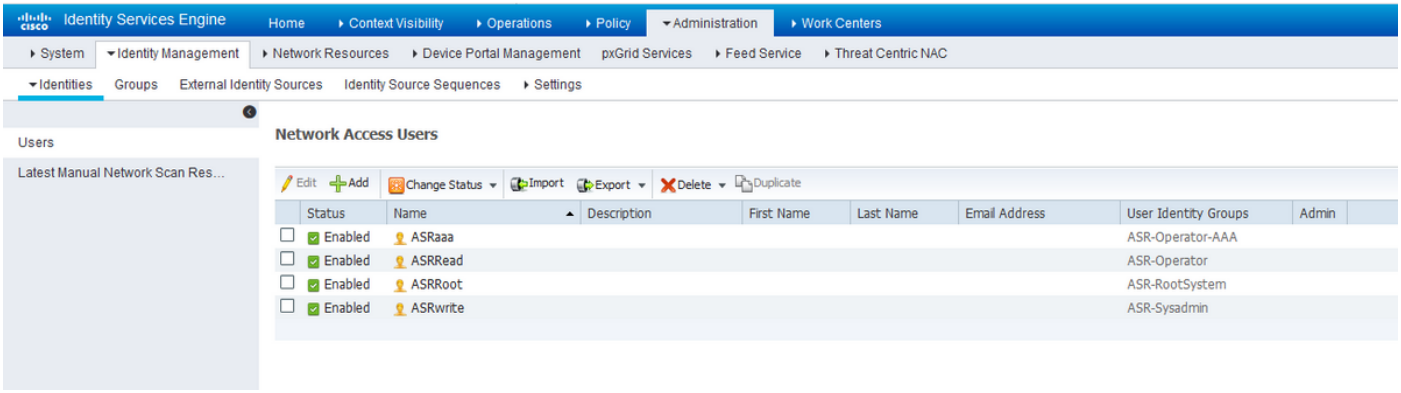
Konfiguration von Netzwerkgeräten

Schritt 2: Definieren Sie die Benutzergruppen gemäß Ihren Anforderungen, wie im Beispiel in diesem Bild gezeigt, verwenden Sie vier Gruppen. Sie können die Gruppen unter **Administration > Identity Management > Groups > User Identity Groups** definieren. In diesem Beispiel werden folgende Gruppen erstellt:

1. ASR-Operator
2. ASR-Operator-AAA
3. ASR-RootSystem
4. ASR-Systemadmin



IdentitätsgruppenSchritt 3: Erstellen Sie, wie im Bild gezeigt, die Benutzer, und ordnen Sie sie der zuvor erstellten Benutzergruppe zu.



Identitäten/Benutzer

> **Hinweis**: In diesem Beispiel werden die internen ISE-Benutzer für die Authentifizierung und Autorisierung verwendet. Authentifizierungen und Autorisierungen mit externer Identitätsquelle fallen nicht in den Anwendungsbereich dieses Dokuments.

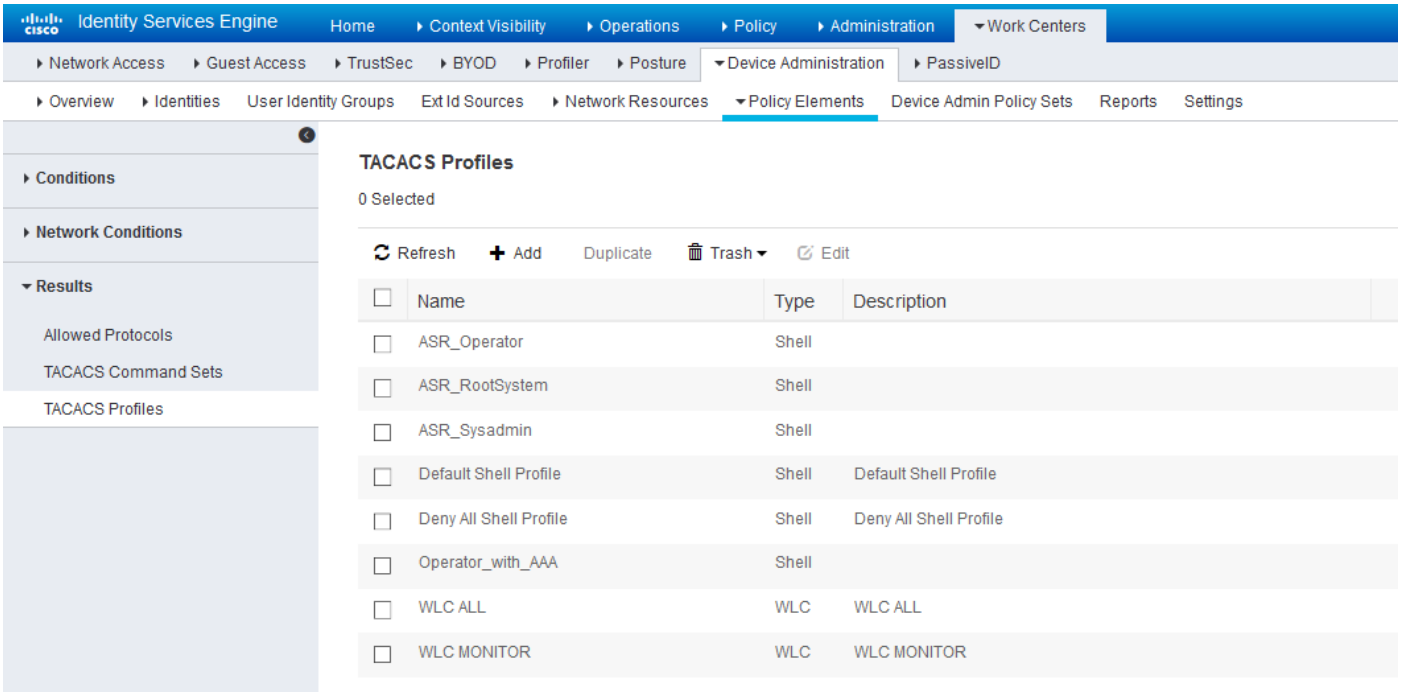
Schritt 4: Definieren Sie das Shell-Profil, das für die jeweiligen Benutzer gepush werden soll. Navigieren Sie dazu zu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Sie können ein neues Shell-Profil konfigurieren, wie in den Bildern gezeigt, sowie für frühere Versionen der ISE. Die in diesem Beispiel definierten Shell-Profile sind:

1. ASR-Operator

2. ASR_RootSystem

3. ASR_Sysadmin

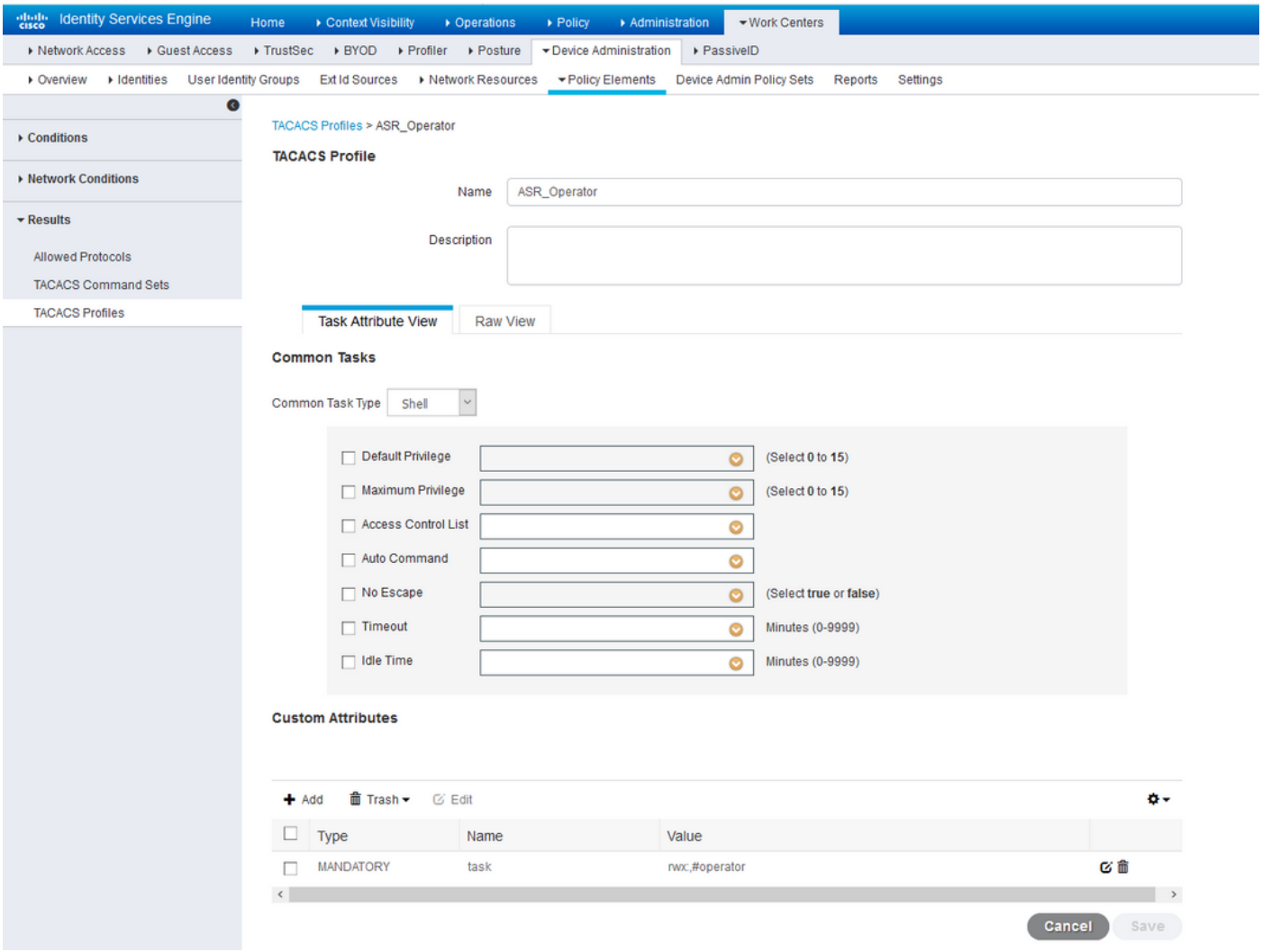
4. Operator_mit_AAA



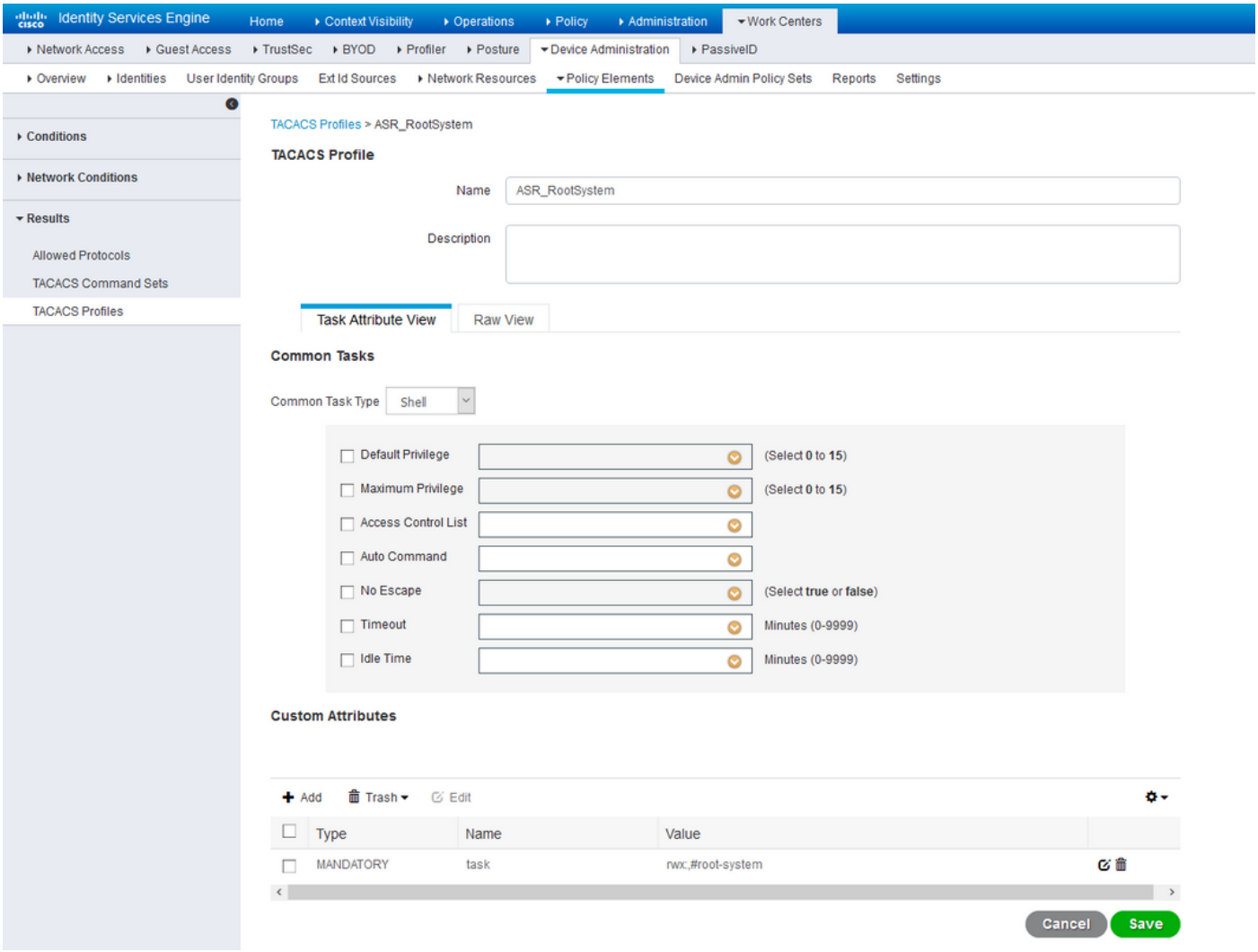
Shell-Profile für TACACS

Sie können auf die Schaltfläche **Hinzufügen** klicken, um die Felder Typ, Name und Wert einzugeben, wie in den Bildern im Abschnitt **Benutzerdefinierte Attribute** dargestellt.

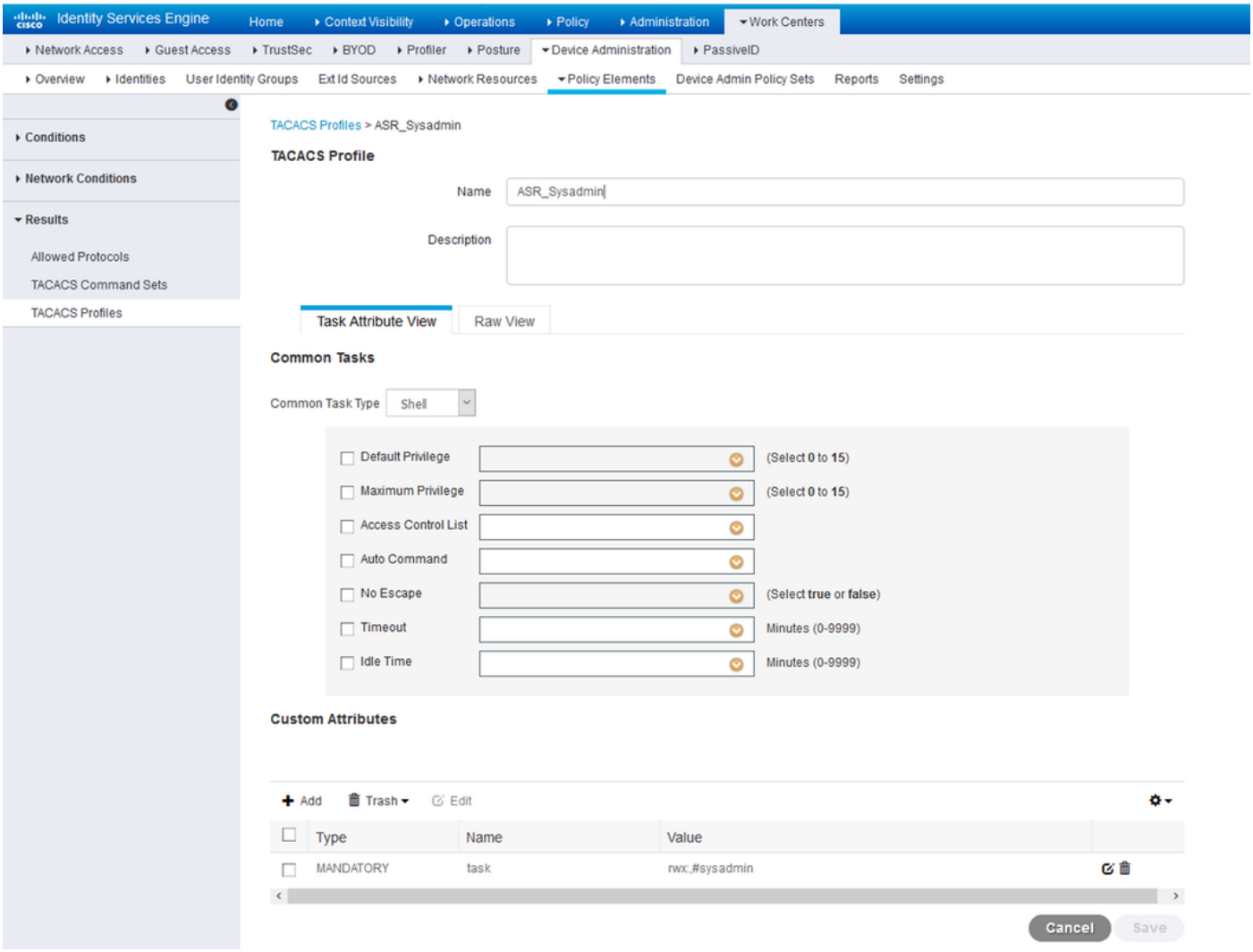
Für Operatorrolle:



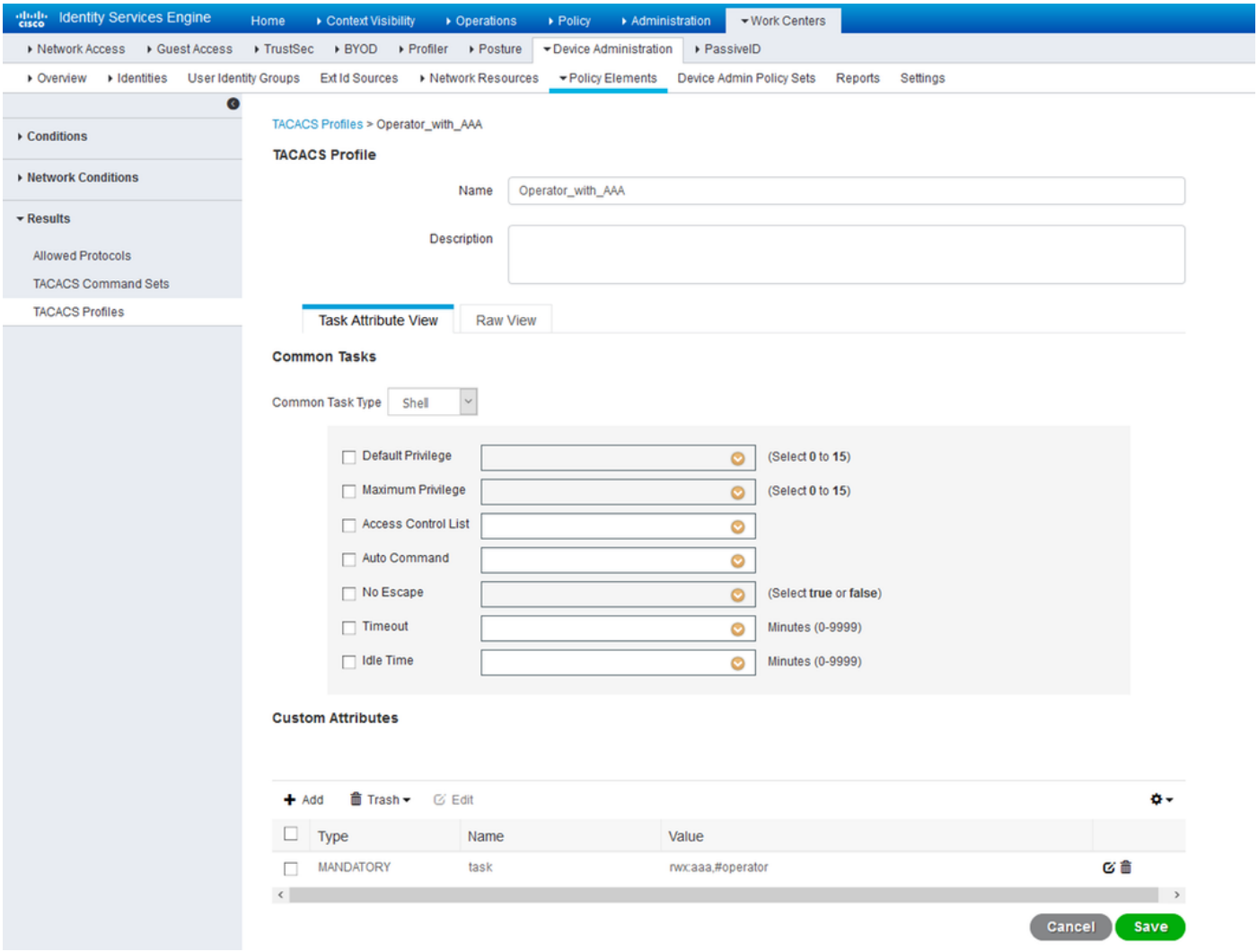
ASR Operator-Shell-ProfilFür Root-System-Rolle:



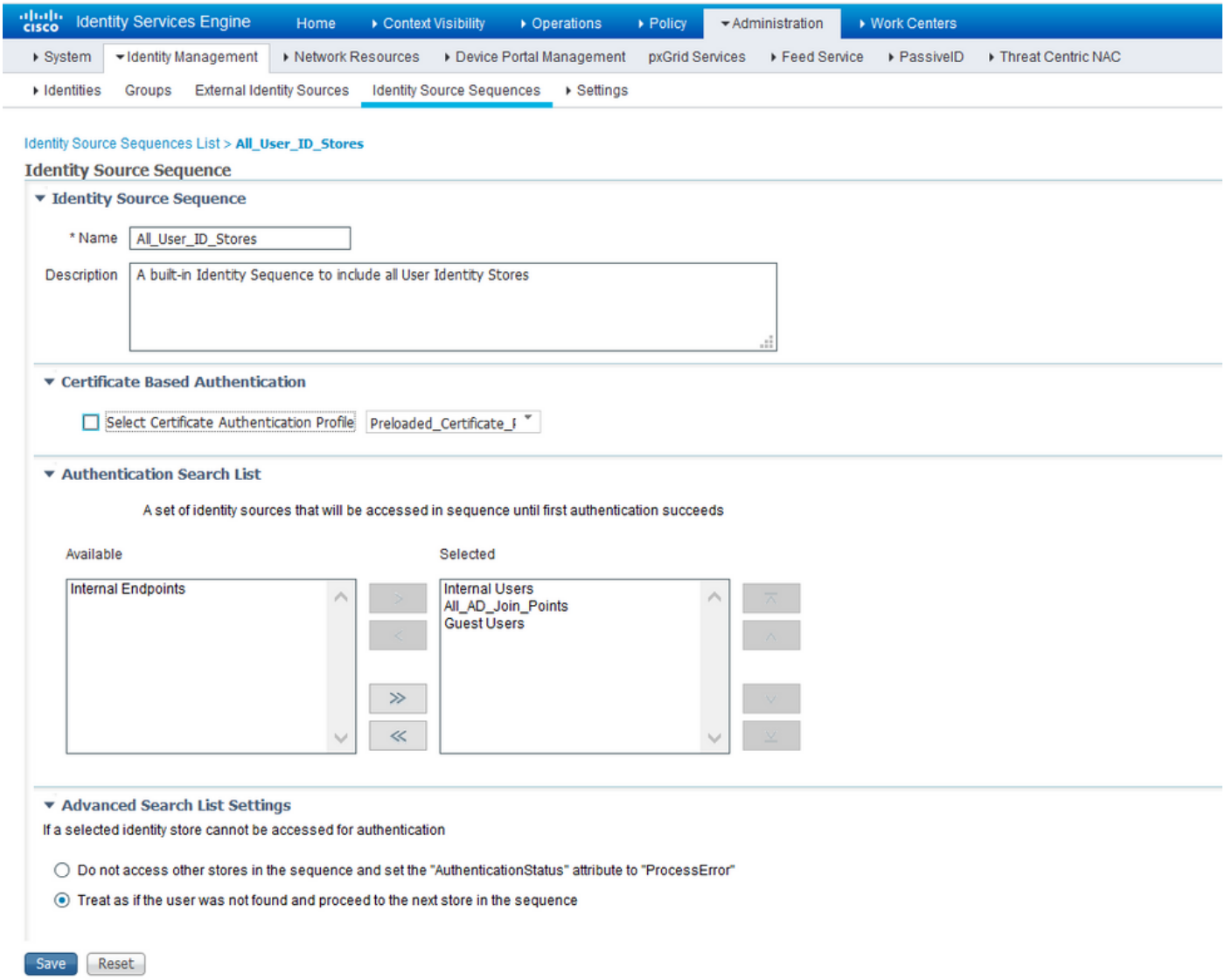
ASR Root System Shell-ProfilFür Sysadmin-Rolle:



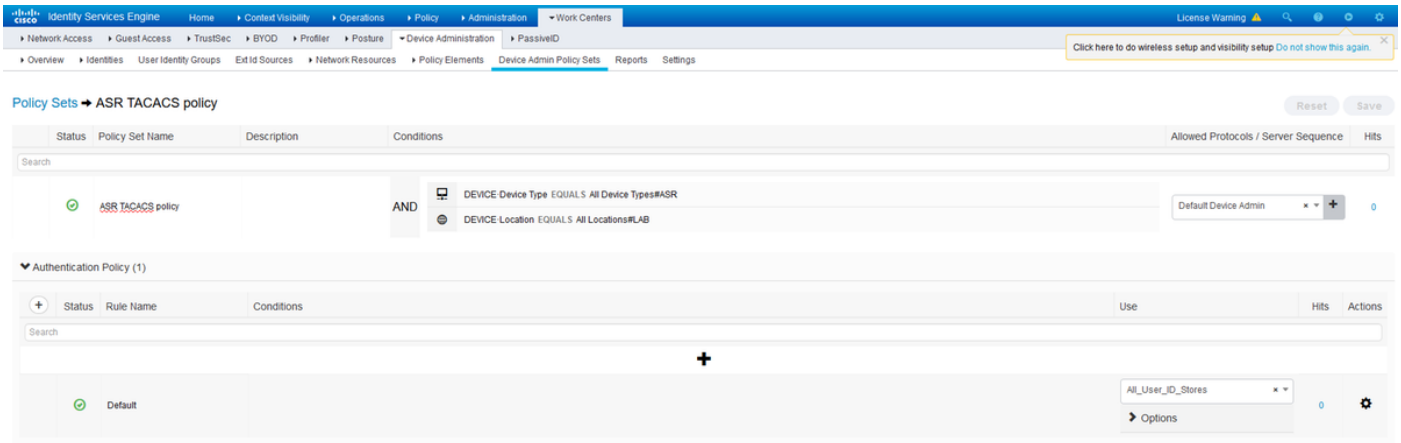
ASR Sysadmin-Shell-ProfilFür Operator- und AAA-Rolle:



Operator mit AAA-Shell-ProfilSchritt 5: Konfigurieren Sie die Identitätsquellensequenz so, dass die internen Benutzer unter **Administration > Identity Management > Identity Source Sequences** verwendet **werden.** Sie können entweder eine neue Identitätsquellensequenz hinzufügen oder die verfügbaren Sequenzen bearbeiten.



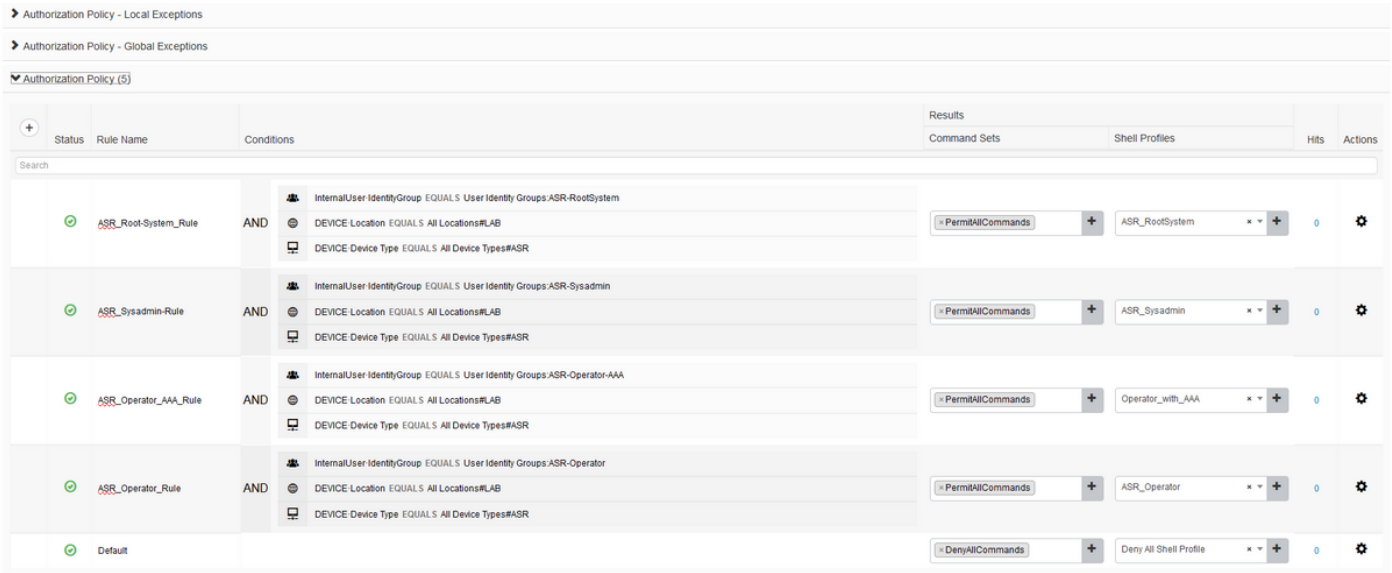
Schritt 6: Konfigurieren Sie die Authentifizierungsrichtlinie in **Work Centers > Device Administration > Device Admin Policy Sets > [Choose Policy Set],** um die Identity Store Sequence zu verwenden, die die internen Benutzer enthält. Konfigurieren Sie die Autorisierung anhand der Anforderung mithilfe der zuvor erstellten Benutzeridentitätsgruppen, und ordnen Sie die entsprechenden Shell-Profile wie im Bild gezeigt zu.



Authentifizierungsrichtlinie

Autorisierungsrichtlinien können auf verschiedene Weise je nach Anforderung konfiguriert werden. Die hier im Bild angezeigten Regeln basieren auf dem Standort des Geräts, dem Typ und der spezifischen internen Benutzeridentitätsgruppe. Die ausgewählten Shell-Profile werden bei der

Autorisierung zusammen mit den Befehlssätzen gepeilt.



Autorisierungsrichtlinie

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Operator

Überprüfen Sie, ob sich die Benutzergruppe und die zugewiesenen Aufgabengruppen beim Anmelden des Benutzers am Router anmelden.

```
username: ASRread
password:

RP/0/RSP1/CPU0:ASR9k#show user
ASRread

RP/0/RSP1/CPU0:ASR9k#show user group
operator

RP/0/RSP1/CPU0:ASR9k#show user tasks
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

Betreiber mit AAA

Überprüfen Sie die Benutzergruppe und die Aufgabengruppen, die beim**Aasra** Benutzer meldet sich beim Router an.

> **Hinweis**:asrasiert die Operatoraufgabe, die vom TACACS-Server zusammen mit den AAA-Berechtigungen für Lesen, Schreiben und Ausführen übertragen wird.

```
username: asraaa
password:

RP/0/RSP1/CPU0:ASR9k#sh user
asraaa

RP/0/RSP1/CPU0:ASR9k#sh user group
operator

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

Systemadministrator

Überprüfen Sie die Benutzergruppe und die Aufgabengruppen, die beim**verarbeiten** Benutzer meldet sich beim Router an.

```
username: asrwrite
password:

RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite

RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ
Task:                  atm  : READ
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ
Task:                  bgp  : READ
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ
Task:            call-home  : READ
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ
Task:                  cgn  : READ
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ
Task:                 dwdm  : READ
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ
Task:    ethernet-services  : READ
--More--
(output omitted )
```

Stammsystem

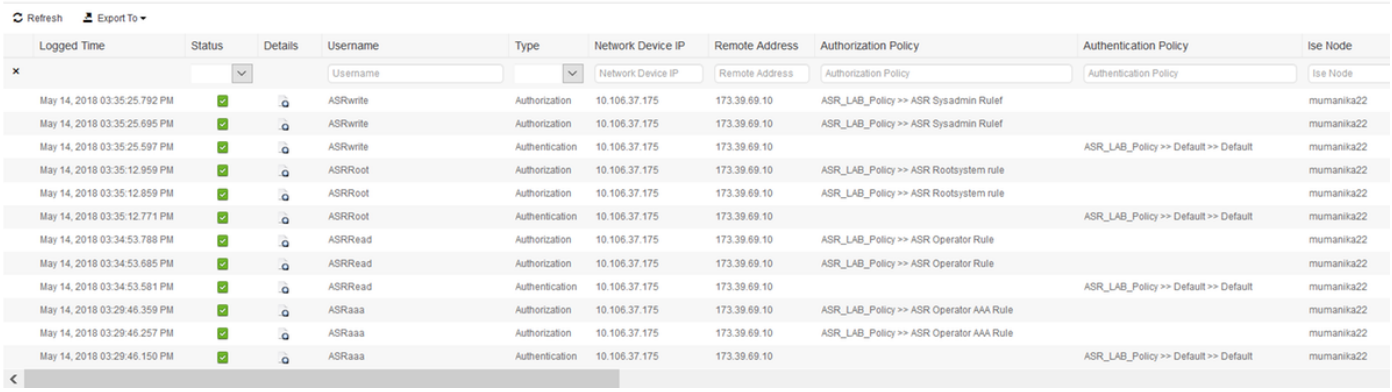
Überprüfen Sie die Benutzergruppe und die Aufgabengruppen, die beim**Asrroot** Benutzer meldet sich beim Router an.

```
username: asrroot
password:

RP/0/RSP1/CPU0:ASR9k#show user
asrroot

RP/0/RSP1/CPU0:ASR9k#show user group
root-system

RP/0/RSP1/CPU0:ios#show user tasks
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:            call-home  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                 dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
--More--
(output omitted )
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Überprüfen Sie den ISE-Bericht unter **Operations > TACACS > Live Logs (Vorgänge > TACACS > Live-Protokolle)**. Klicken Sie auf das Lupensymbol, um den detaillierten Bericht anzuzeigen.



Refresh Export To

Logged Time	Status	Details	Username	Type	Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
			Username		Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
May 14, 2018 03:35:25.792 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
May 14, 2018 03:35:25.695 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
May 14, 2018 03:35:25.597 PM	✓		ASRwrite	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:35:12.959 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
May 14, 2018 03:35:12.859 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
May 14, 2018 03:35:12.771 PM	✓		ASRRoot	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:34:53.788 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
May 14, 2018 03:34:53.685 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
May 14, 2018 03:34:53.581 PM	✓		ASRRead	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
May 14, 2018 03:29:46.359 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
May 14, 2018 03:29:46.257 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
May 14, 2018 03:29:46.150 PM	✓		ASRaaa	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22

Dies sind einige hilfreiche Befehle zur Fehlerbehebung bei ASR:

- **Benutzer anzeigen**
- **Benutzergruppe anzeigen**
- **Benutzeraufgaben anzeigen**
- **Benutzer anzeigen**