Konfigurieren von ASR9k TACACS mit dem Cisco Secure ACS 5.x-Server

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration des ASR Aggregation Services Routers (ASR) der Serie 9000 für die Authentifizierung und Autorisierung über TACACS+ mit dem Cisco Secure Access Control Server (ACS) 5.x-Server.

Dieses Beispiel zeigt die Implementierung des Verwaltungsmodells der aufgabenbasierten Autorisierung zur Kontrolle des Benutzerzugriffs im Cisco IOS XR-Softwaresystem. 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 Principal) die Berechtigung zur Ausführung einer bestimmten Aufgabe erteilt wird. 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
- ACS 5.x - Bereitstellung und Konfiguration
- TACACS+-Protokoll

Verwendete Komponenten

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

- ASR 9000 mit Cisco IOS XR Software, Version 4.3.4
- Cisco Secure ACS 5.7

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

Konfiguration

Vordefinierte Komponenten in IOS XR

In IOS XR gibt es vordefinierte Benutzergruppen und Aufgabengruppen. Der Administrator kann diese vordefinierten Gruppen verwenden oder benutzerdefinierte Gruppen gemäß den Anforderungen 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

Die root-Benutzergruppe verfügt über eine vordefinierte Autorisierung. Das heißt, sie hat die volle Verantwortung für vom Benutzer verwaltete Root-System-Ressourcen und bestimmte Verantwortlichkeiten in anderen Diensten.

Mit diesem Befehl können Sie die vordefinierten Benutzergruppen überprüfen:

```
RP/0/RSP1/CPU0:ASR9k#show 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
  root-system    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: Service-Verwaltungsaufgaben, z. B. SBC

Mit diesem Befehl können Sie die vordefinierten Aufgabengruppen 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>
```

Mit diesem Befehl können Sie die unterstützten Aufgaben überprüfen:

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

Nachfolgend finden Sie eine Liste der 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	so
Sysmgr	System	Transport	Einfacher Zugriff	Tunnel	Universell	VLAN	VF

Jede der oben genannten Aufgaben kann mit einer dieser oder allen vier Berechtigungen erteilt 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 Komponenten auf IOS XR

Benutzerdefinierte Benutzergruppen

Der Administrator kann seine eigenen Benutzergruppen so konfigurieren, dass sie bestimmte Anforderungen erfüllen. Nachfolgend finden Sie das Konfigurationsbeispiel:

```
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup operator
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit
```

Benutzerdefinierte Aufgabengruppen

Administratoren können eigene Aufgabengruppen konfigurieren, um bestimmte Anforderungen zu erfüllen. Nachfolgend finden Sie das 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
```

Wenn Sie nicht sicher sind, wie Sie die für einen bestimmten Befehl benötigte Aufgabengruppe und Berechtigung finden, können Sie den Befehl **description** verwenden, um ihn zu finden. Hier ein Beispiel:

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, muss diese Zeile in der Aufgabengruppe zugelassen werden:

Aufgabenlesen aaa

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 den Befehl **aaa authentication login default group tacacs+** aus dem Konfigurationsmodus ausführen kann, muss diese Zeile in der Aufgabengruppe zugelassen werden:

Aufgabe lesen Schreiben aaa

Sie können die Benutzergruppe definieren, die mehrere Aufgabengruppen importieren 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

Definieren eines TACACS-Servers auf dem Router:

Hier definieren Sie die ACS-Server-IP-Adresse als takacs-Server mit der zentralen Cisco

```
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 10.106.73.233 port 49
key 7 14141B180F0B
!
```

Verweisen Sie die Authentifizierung und Autorisierung auf den externen TACACS-Server.

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

Befehlsautorisierung (optional):

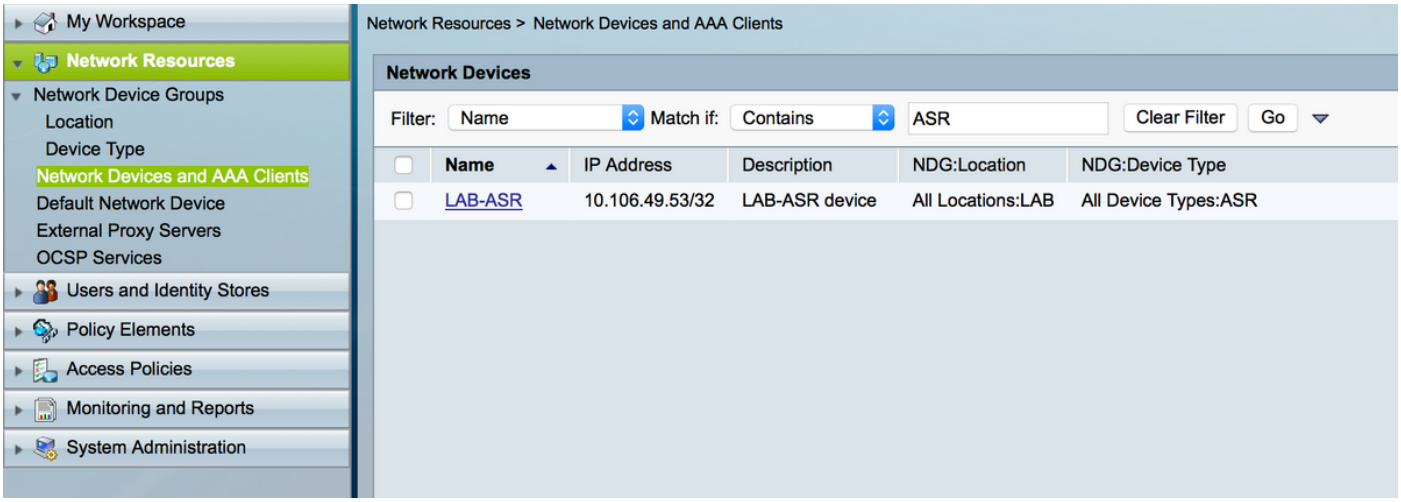
```
#aaa authorization commands default group tacacs+
```

Zeigen Sie die Accounting auf externen Server (optional).

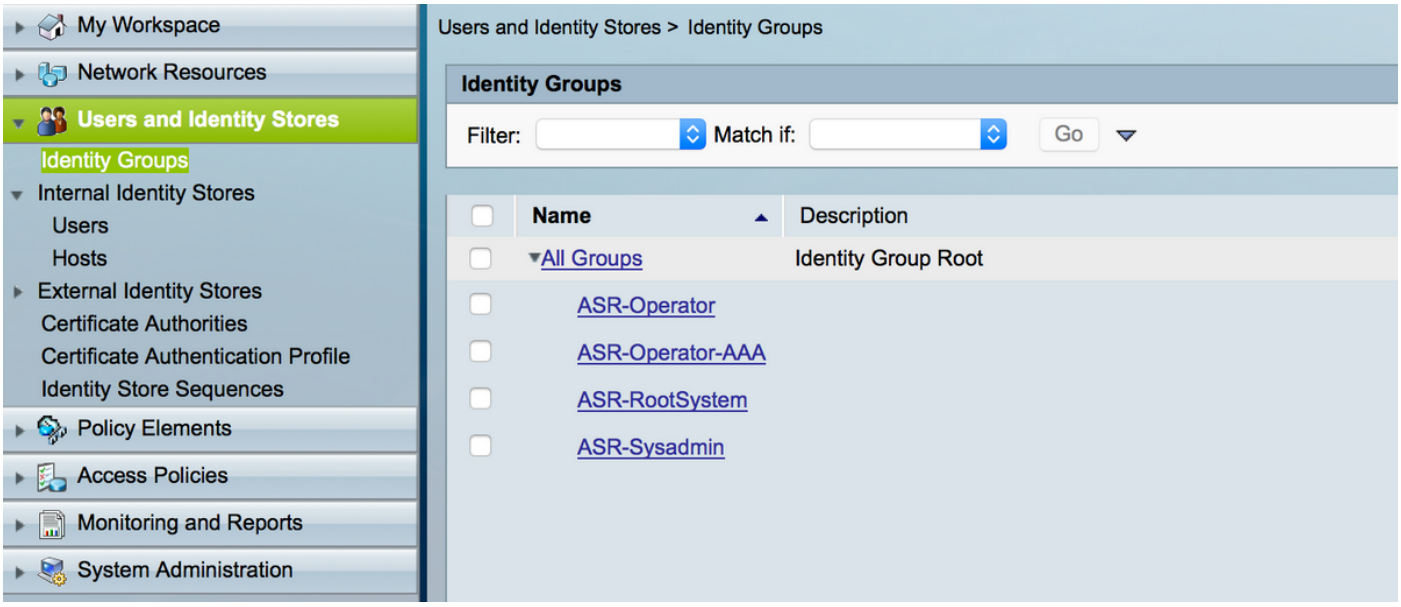
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ACS-Serverkonfiguration

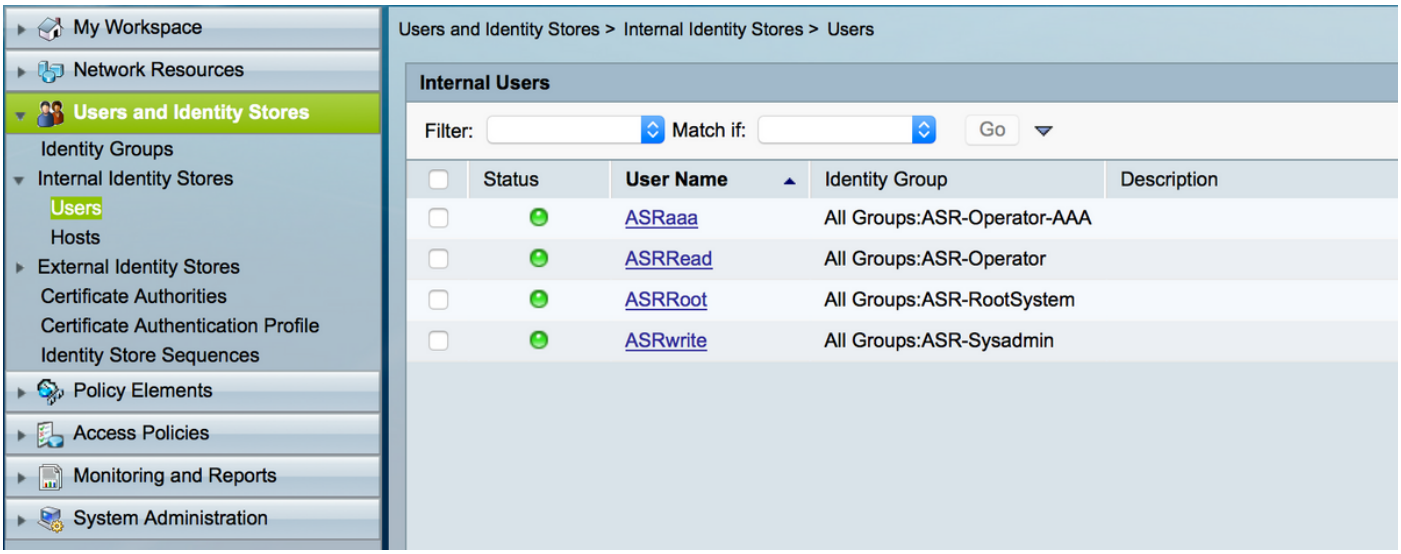
Schritt 1: Um die Router-IP in der Liste der AAA-Clients auf dem ACS-Server zu definieren, navigieren Sie zu **Network Resources > Network Devices and AAA Clients (Netzwerkressourcen > Netzwerkgeräte und AAA-Clients**, wie im Bild gezeigt. In diesem Beispiel definieren Sie **cisco** als Shared Secret (Shared Secret), wie im ASR konfiguriert.



Schritt 2: Definieren Sie die Benutzergruppen gemäß Ihren Anforderungen. Im Beispiel, wie in diesem Bild gezeigt, verwenden Sie vier Gruppen.



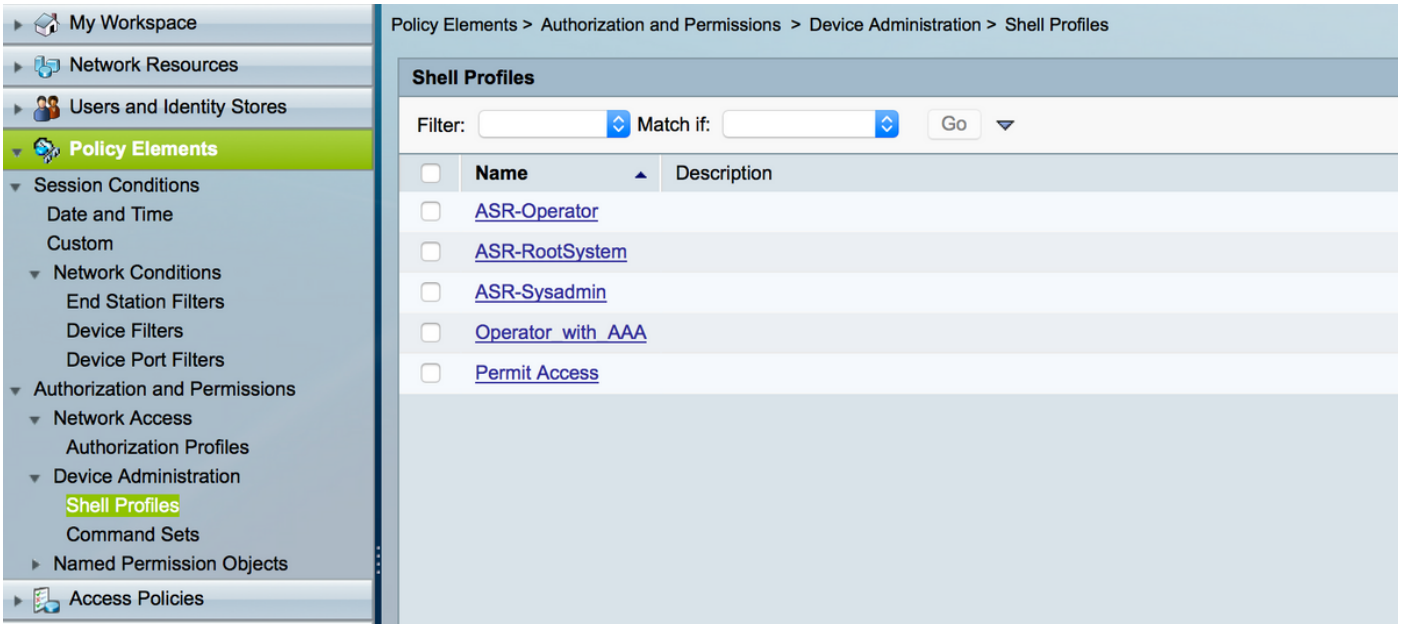
Schritt 3: Erstellen Sie, wie im Bild gezeigt, die Benutzer, und ordnen Sie sie der jeweiligen oben erstellten Benutzergruppe zu.



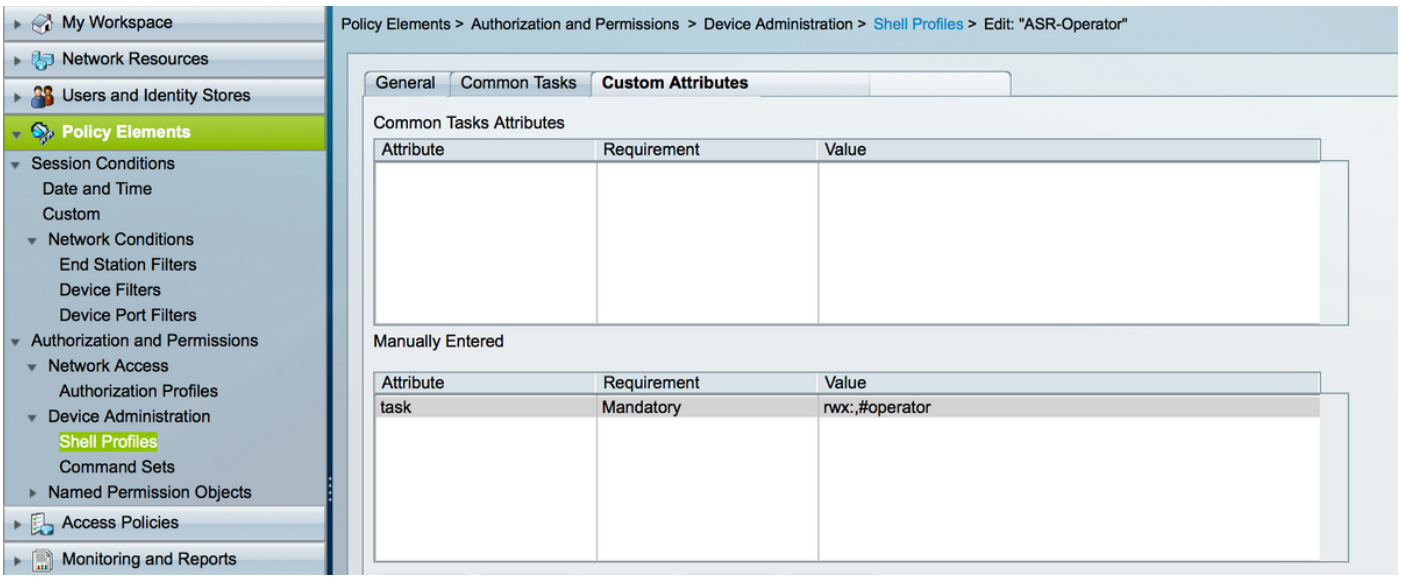
Hinweis: In diesem Beispiel werden die internen ACS-Benutzer für die Authentifizierung

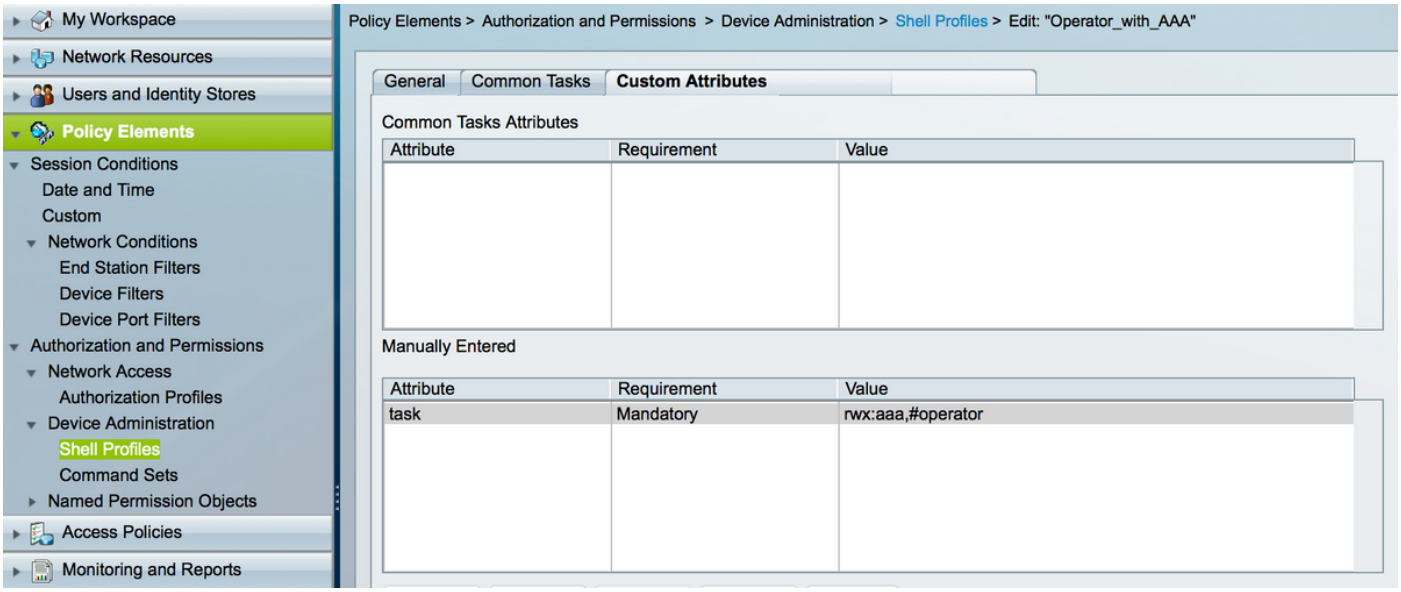
verwendet. Wenn Sie die in den externen Identitätsspeichern erstellten Benutzer verwenden möchten, können Sie diese auch verwenden. In diesem Beispiel werden die externen Identitätsquellenbenutzer nicht abgedeckt. .

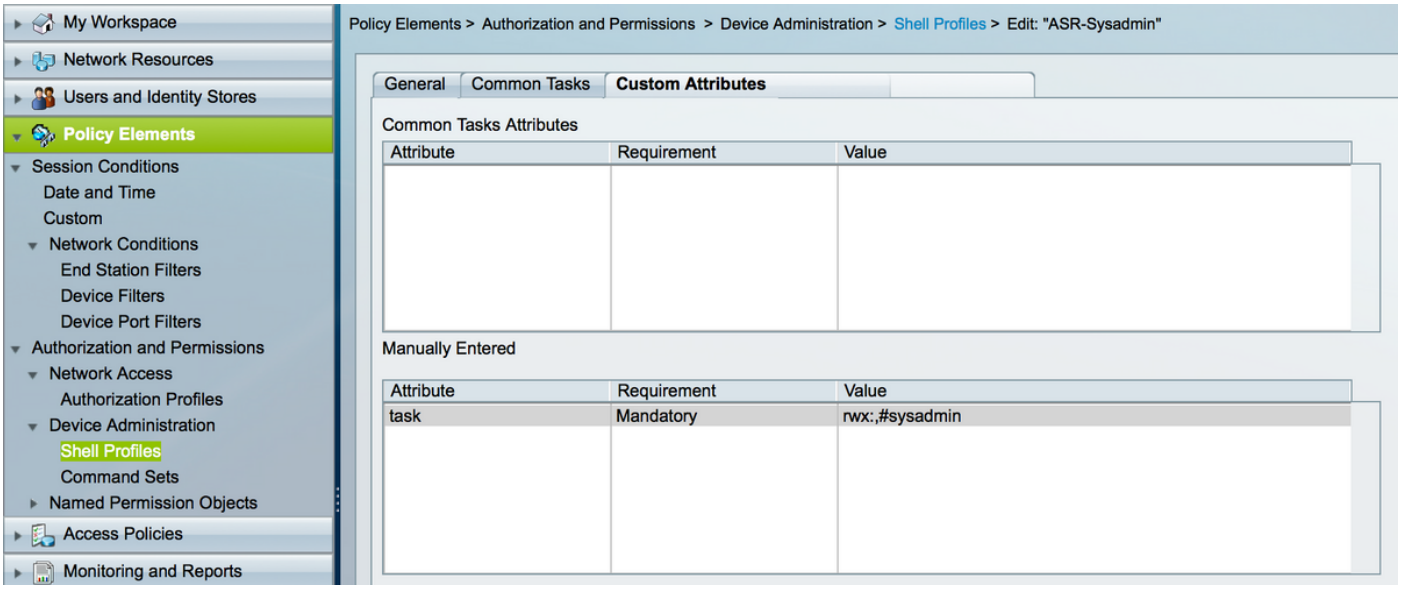
Schritt 4: Definieren Sie das Shell-Profil, das Sie für die jeweiligen Benutzer verschieben möchten.

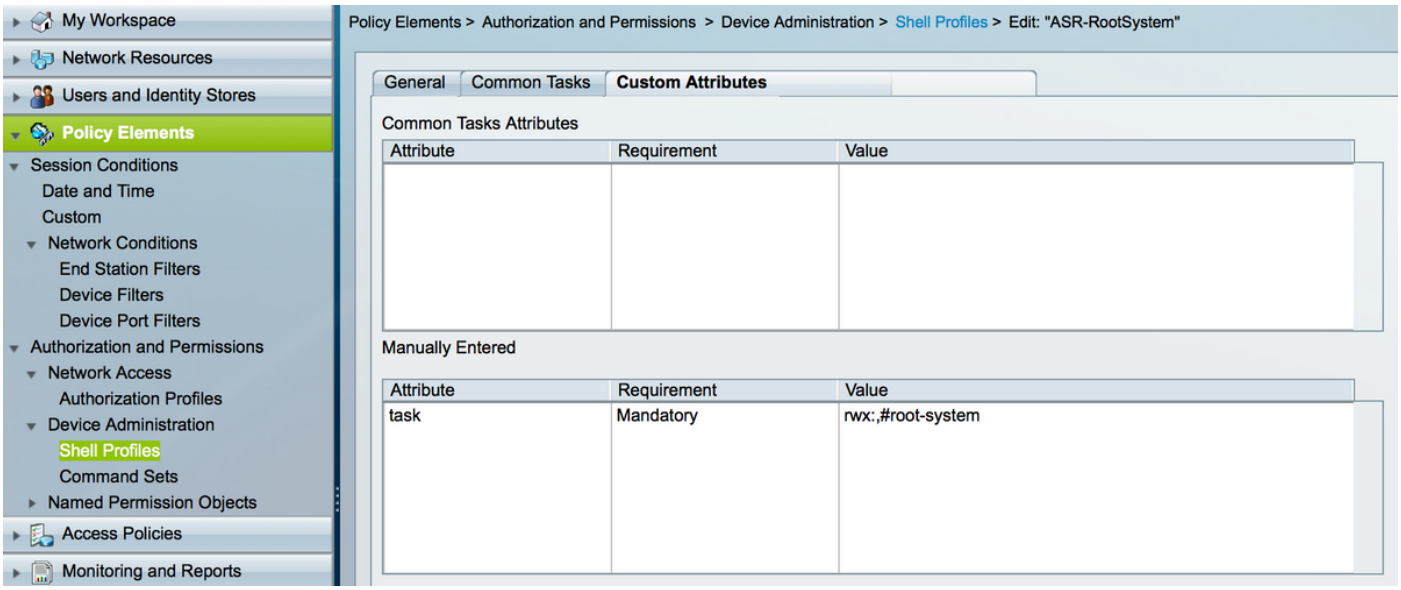


Im bereits erstellten Shell-Profil konfigurieren Sie, die entsprechenden Aufgabengruppen wie im Bild gezeigt zu verschieben.

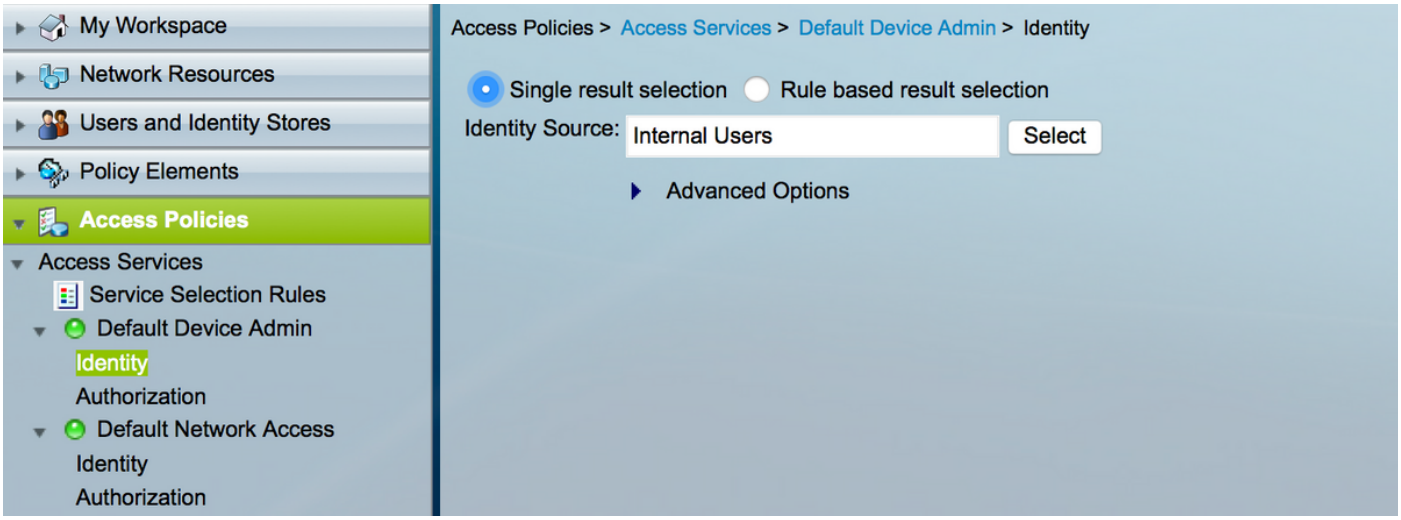




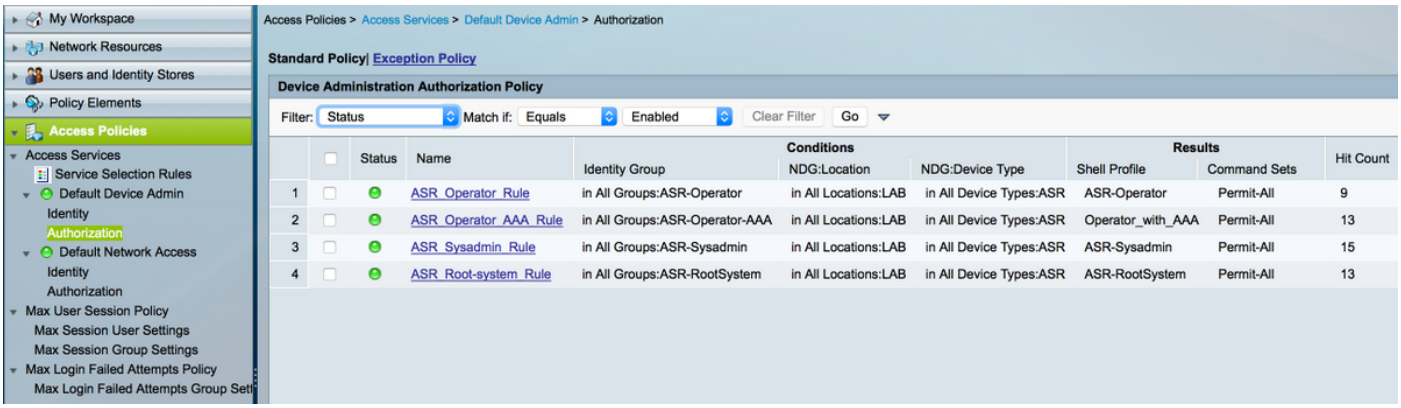




Schritt 5: Definieren Sie die Zugriffsrichtlinie. Die Authentifizierung erfolgt gegen die internen Benutzer.



Schritt 6: Konfigurieren Sie die Autorisierung anhand der Anforderung mithilfe der zuvor erstellten Benutzeridentitätsgruppen, und ordnen Sie die entsprechenden Shell-Profile zu, wie im Bild gezeigt.



Überprüfen

Operator

Für die Anmeldung wird Benutzername **asrread** verwendet. Dies sind die Überprüfungsbefehle.

```
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

Für die Anmeldung wird Benutzername **asraaa** verwendet. Dies sind die Überprüfungsbefehle.

> **Hinweis**: **asraaa** ist die Operatoraufgabe, die vom TACACS-Server zusammen mit den Berechtigungen zum Lesen und Ausführen von Aufgaben 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

Um sich anzumelden, wird Benutzername **ASR** verwendet. Dies sind die Überprüfungsbefehle.

```
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 )
```

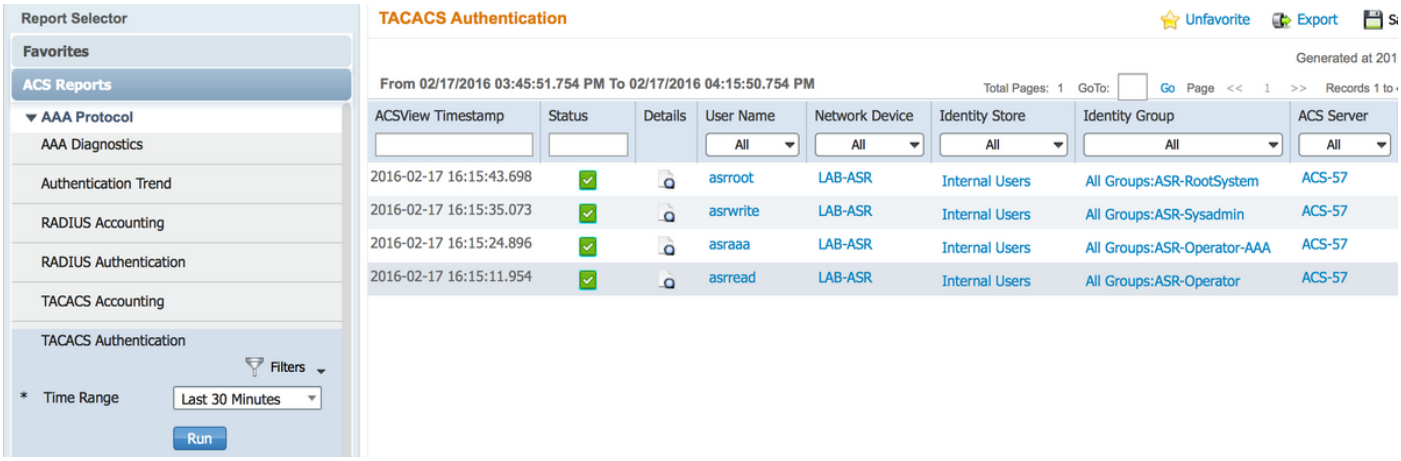
Stammsystem

Für die Anmeldung wird Benutzername **asrroot** verwendet. Dies sind die Überprüfungsbefehle.

```
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

Sie können den ACS-Bericht auf der Seite Überwachung und Reporting überprüfen. Wie im Bild gezeigt, können Sie auf die Lupe klicken, um den detaillierten Bericht anzuzeigen.



Hier einige hilfreiche Befehle zur Fehlerbehebung bei ASR:

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