Configurazione di ASR9k TACACS con Cisco Secure ACS 5.x Server

Sommario

Introduzione

In questo documento viene descritta la configurazione di ASR serie 9000 Aggregation Services Router (ASR) per l'autenticazione e l'autorizzazione tramite TACACS+ con il server Cisco Secure Access Control Server (ACS) 5.x.

In questo esempio viene implementato il modello amministrativo di autorizzazione basata su attività utilizzato per controllare l'accesso degli utenti nel sistema software Cisco IOS XR. Le attività principali necessarie per implementare l'autorizzazione basata su attività riguardano la configurazione dei gruppi di utenti e dei gruppi di attività. I gruppi di utenti e i gruppi di attività vengono configurati tramite il set di comandi del software Cisco IOS XR utilizzato per i servizi di autenticazione, autorizzazione e accounting (AAA). I comandi di autenticazione vengono utilizzati per verificare l'identità di un utente o di un'entità. I comandi di autorizzazione vengono utilizzati per verificare che a un utente autenticato (o entità) venga concessa l'autorizzazione per eseguire un'attività specifica. I comandi di accounting vengono utilizzati per registrare le sessioni e per creare un riepilogo di controllo registrando determinate azioni generate dall'utente o dal sistema.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di ASR 9000 e configurazione di base
- Installazione e configurazione di ACS 5.x.
- Protocollo TACACS+

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASR 9000 con software Cisco IOS XR, versione 4.3.4
- Cisco Secure ACS 5.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali modifiche alla configurazione.

Configurazione

Componenti predefiniti di IOS XR

In IOS XR sono disponibili gruppi di utenti e di attività predefiniti. L'amministratore può utilizzare questi gruppi predefiniti o definire gruppi personalizzati in base ai requisiti.

Gruppi di utenti predefiniti

I seguenti gruppi di utenti sono predefiniti in IOS XR:

Gruppo utenti	Privilegi
supporto cisco	Funzioni di debug e risoluzione dei problemi (in genere, utilizzate dal personale del support tecnico Cisco).
netadmin	Configurare i protocolli di rete, ad esempio Open Shortest Path First (OSPF), generalmente utilizzati dagli amministratori di rete.
operatore	Eseguire attività di monitoraggio quotidiane e disporre di diritti di configurazione limitati.
root-lr	Visualizzare ed eseguire tutti i comandi all'interno di un singolo RP.
sistema radice	Visualizzare ed eseguire tutti i comandi per tutti i RP nel sistema.
sysadmin	Eseguire attività di amministrazione del sistema per il router, ad esempio mantenere la posizione in cui sono archiviati i dump di base o configurare l'orologio NTP (Network Time Protocol).
serviceadmin	Eseguire attività di amministrazione del servizio, ad esempio SBC (Session Border Controll

Il gruppo di utenti del sistema radice dispone di autorizzazioni predefinite; in altre parole, è completamente responsabile delle risorse gestite dagli utenti del sistema radice e di alcune responsabilità in altri servizi.

Utilizzare questi comandi per verificare i gruppi di utenti predefiniti:

```
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>
```

Gruppi di task predefiniti

Gli amministratori possono utilizzare questi gruppi di task predefiniti, in genere per la configurazione iniziale:

- supporto cisco: Attività del personale di supporto Cisco
- netadmin: Attività dell'amministratore di rete
- operatore: Attività quotidiane dell'operatore (a scopo dimostrativo)
- root-lr: Attività di amministrazione del router di dominio sicuro
- sistema radice: Attività di amministratore a livello di sistema
- sysadmin Attività dell'amministratore di sistema
- serviceadmin: Attività di amministrazione dei servizi, ad esempio SBC

Utilizzare questi comandi per verificare i gruppi di operazioni predefiniti:

```
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>
```

Utilizzare questo comando per verificare le attività supportate:

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

Di seguito sono elencate le attività supportate:

Aaa	Acl	Admin	Ancp	Atm	servizi di base	Bcdl	Bfd	bgp
Avvio	Pacchetto	call-home	Cdp	Cef	Cgn	supporto cisco	config-mgmt	servizi di configurazione
Crittografia	Diag	Non consentito	Driver	Dwdm	Eem	EIGRP	servizi ethernet	accesso esterno
Fabric	fault-mgr	File system	Firewall	Fr	Hdlc	servizi host	Hsrp	interfaccia
Inventario	servizi ip	IPv4	Ipv6	Isis	L2vpn	Li	Lisp	registrazione

Lpt	Monitor (Monitora)	mpls-ldp	mpls-static	mpls-te	Multicast	NetFlow	Rete	nps
OSPF	Ouni	Pbr	pkg-mgmt	pos-dpt	Ppp	Qos	Rcmd	costola
RIP	root-lr	sistema radice	route-map	route-policy	Sbc	Snmp	sonet-sdh	statico
Sysmgr	Sistema	Trasporto	tty-access	Tunnel	Universale	VLAN	Vpdn	vrp

Ognuna delle attività sopra indicate può essere assegnata con una di queste o tutte e quattro le autorizzazioni.

Lettura	Specifica una designazione che consente solo un'operazione di lettura.
Scrittura	Specifica una designazione che consente un'operazione di modifica e un'operazione lettura.
Immettere il comando	Specifica una designazione che consente un'operazione di accesso; ad esempio, pi Telnet.
Debug	Specifica una designazione che consente un'operazione di debug.

Componenti definiti dall'utente su IOS XR

Gruppi di utenti definiti dall'utente

L'amministratore può configurare i propri gruppi di utenti per soddisfare esigenze particolari. Di seguito è riportato l'esempio di configurazione:

```
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
```

Gruppi di task definiti dall'utente

L'amministratore può configurare i propri gruppi di task per soddisfare esigenze particolari. Di seguito è riportato l'esempio di configurazione:

```
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
```

Se non si è certi di come trovare il gruppo di attività e l'autorizzazione necessari per un determinato comando, è possibile utilizzare il comando **description** per individuarlo. Di seguito è riportato un esempio:

Esempio 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#
```

Per consentire a un utente di eseguire il comando **show aaa usergroup**, è necessario consentire questa riga nel gruppo di operazioni:

operazione read aaa

Esempio 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)#
```

Per consentire a un utente di eseguire il comando **aaa authentication login default group tacacs+** dalla modalità di configurazione, è necessario consentire questa riga nel gruppo di operazioni:

operazione lettura/scrittura aaa

Èpossibile definire il gruppo di utenti che può importare diversi gruppi di operazioni. Di seguito è riportato l'esempio di configurazione:

```
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
```

Configurazione AAA sul router

Definire un server TACACS sul router:

In questa sezione, l'indirizzo IP del server ACS viene definito come server TACACS con la chiave 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
!
```

Puntare l'autenticazione e l'autorizzazione al server TACACS esterno.

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

Autorizzazione comando (facoltativa):

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

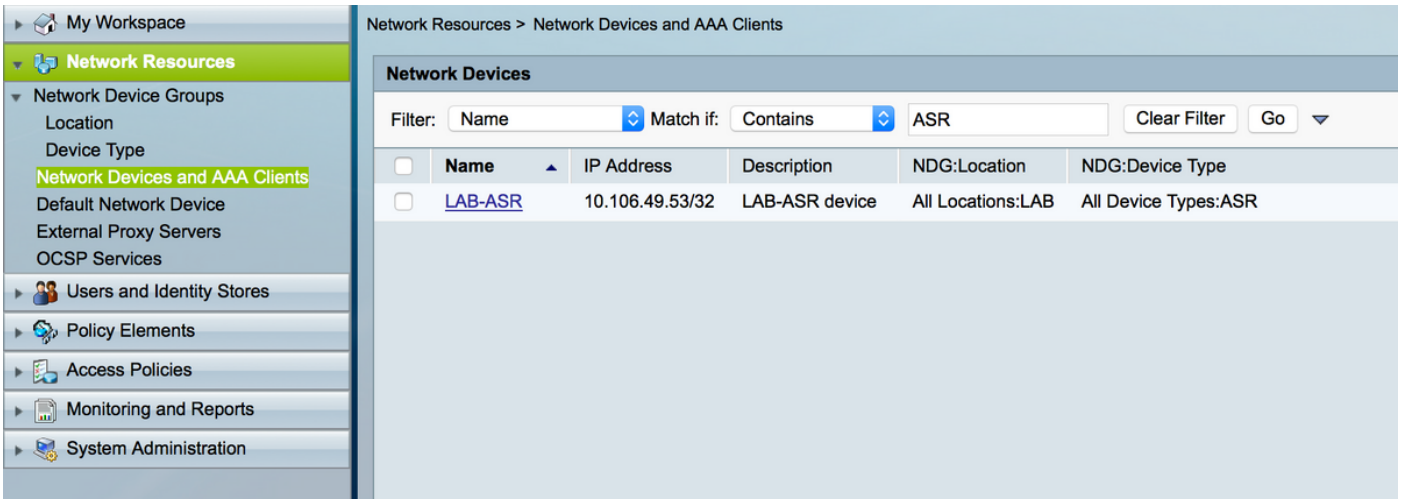
Puntare l'accounting al server esterno (facoltativo).

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

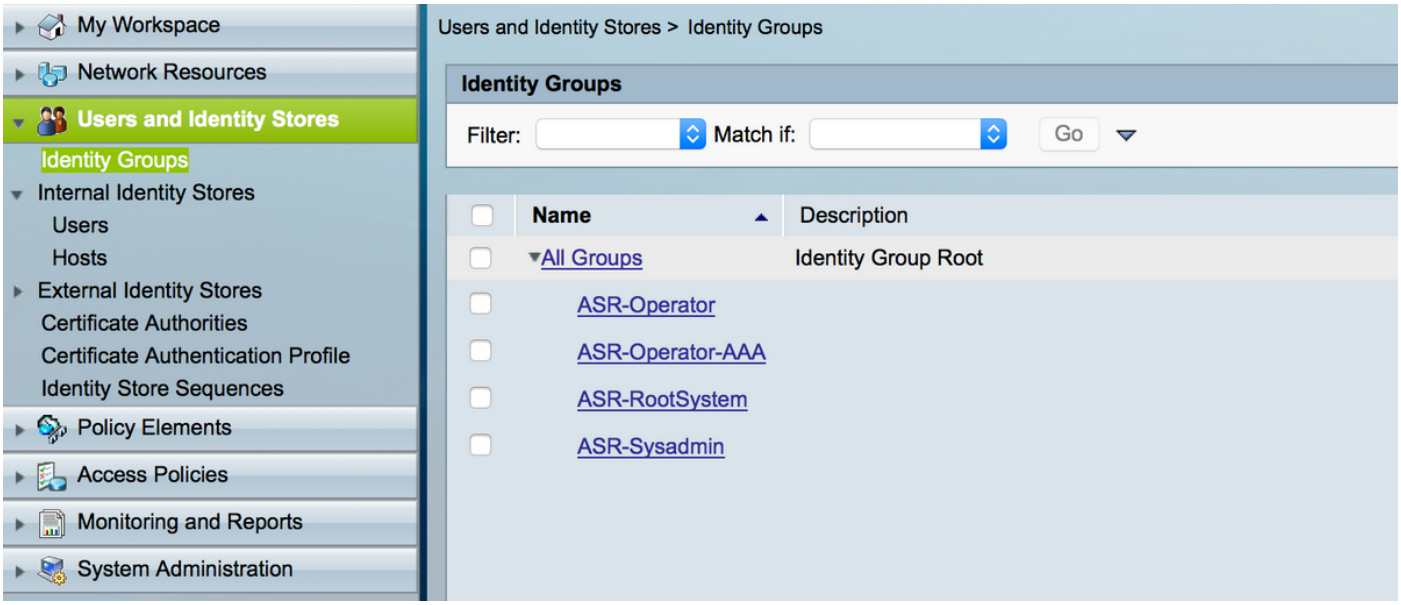
Configurazione server ACS

Passaggio 1. Per definire l'indirizzo IP del router nell'elenco dei client AAA sul server ACS,

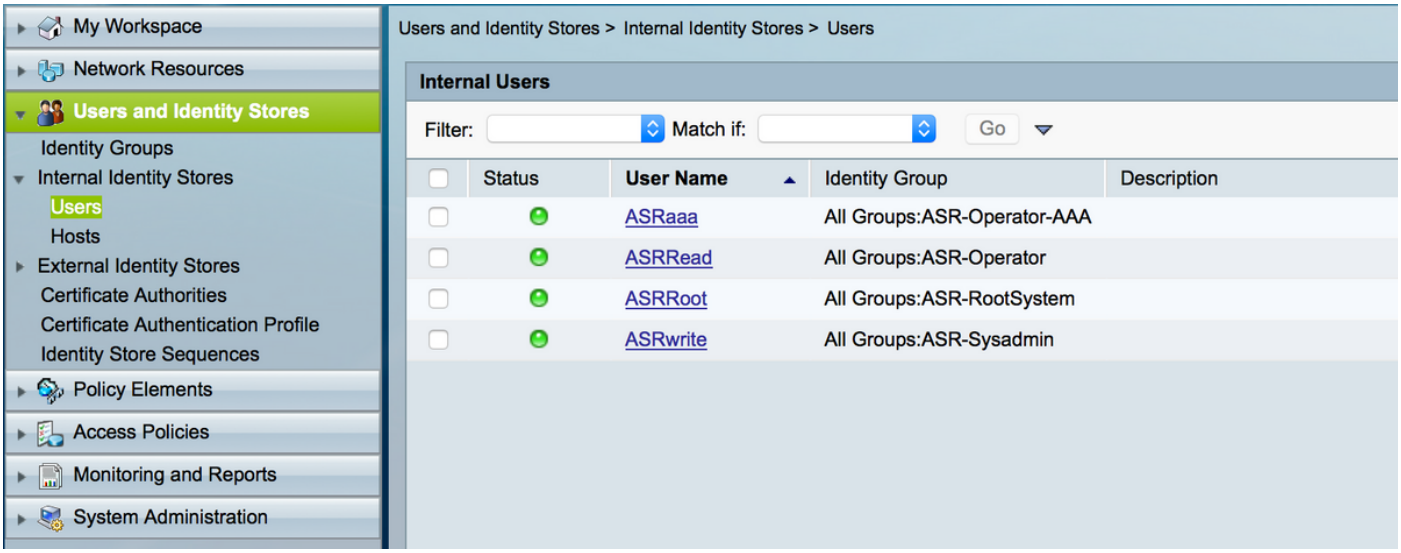
selezionare **Risorse di rete > Dispositivi di rete e client AAA**, come mostrato nell'immagine. In questo esempio, il segreto condiviso **cisco** viene definito come configurato nell'ASR.



Passaggio 2. Definire i gruppi di utenti in base alle proprie esigenze. Nell'esempio, come mostrato in questa immagine, si utilizzano quattro gruppi.

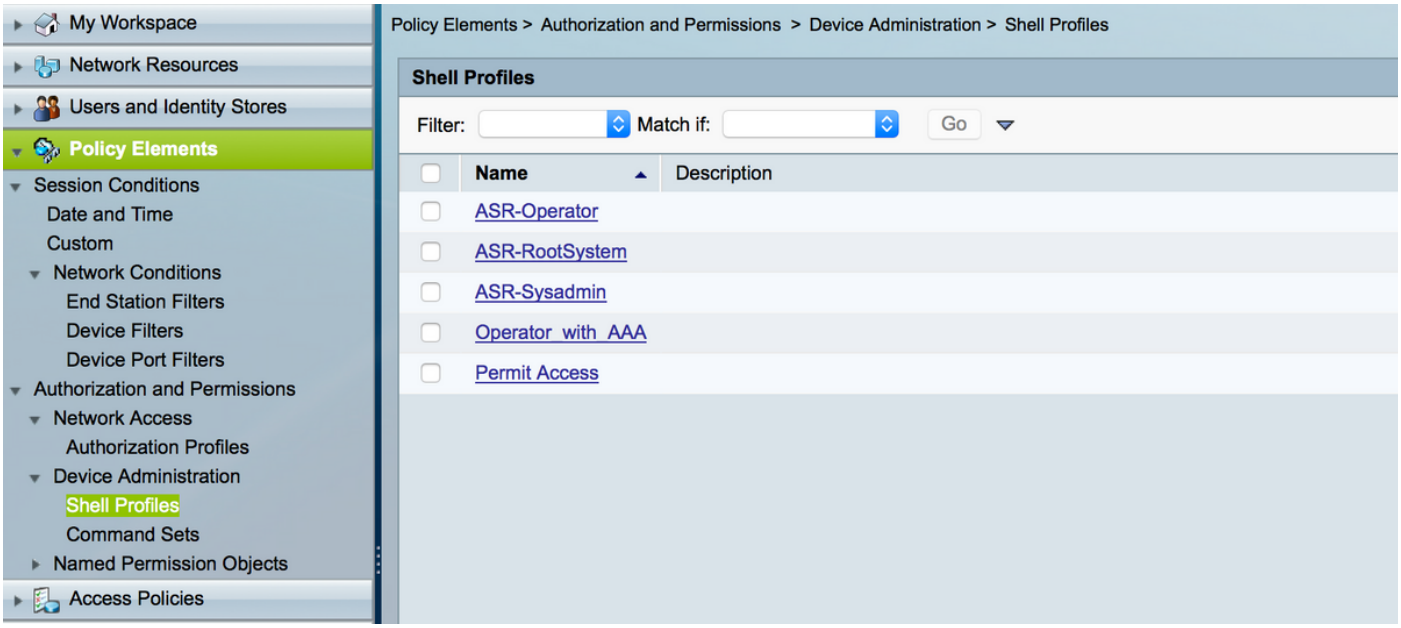


Passaggio 3. Come mostrato nell'immagine, creare gli utenti e mapparli al rispettivo gruppo di utenti creato in precedenza.

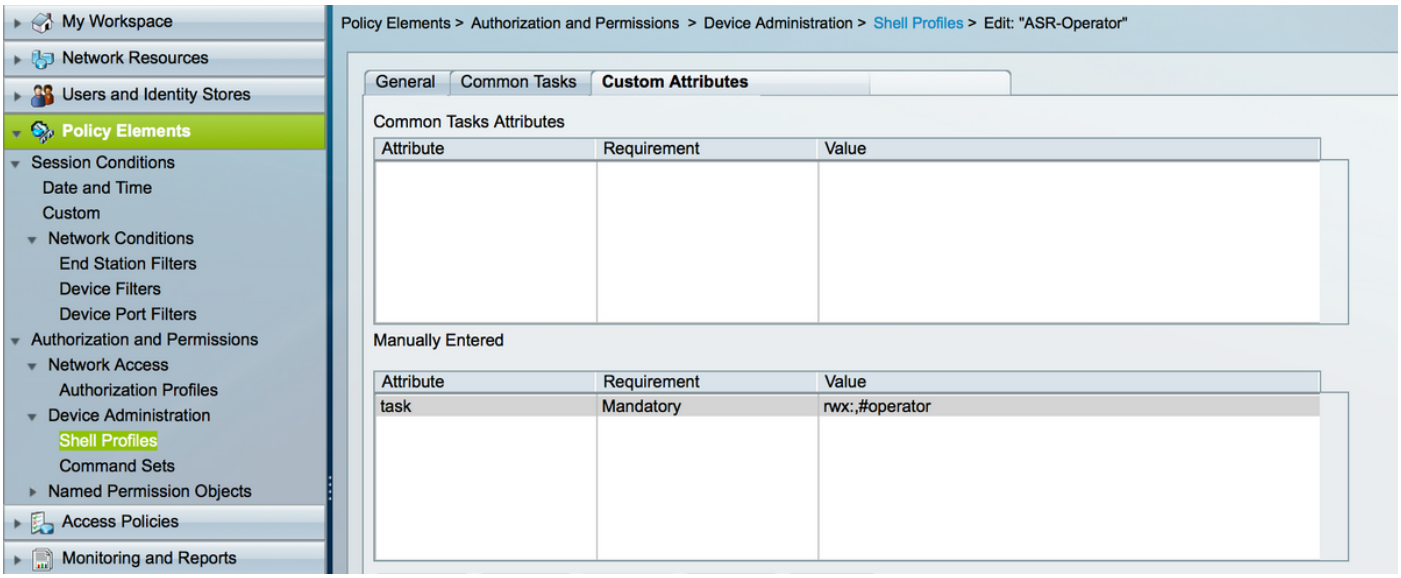


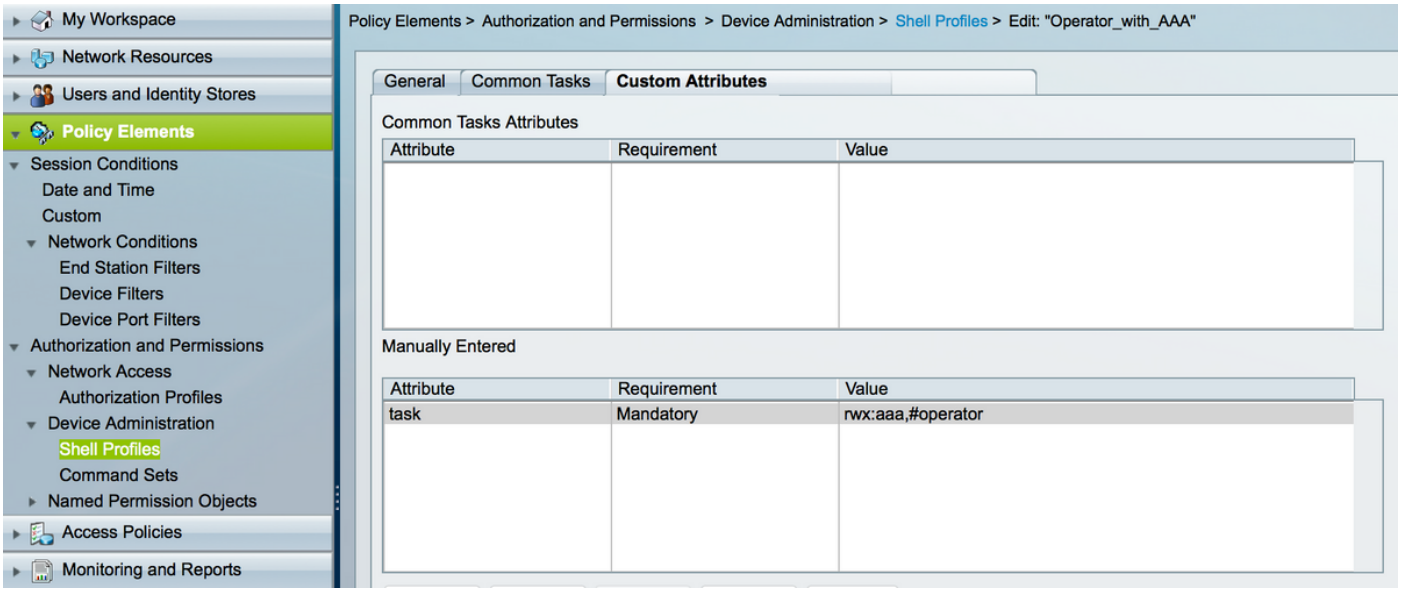
Nota: In questo esempio, vengono utilizzati gli utenti interni ACS per l'autenticazione. Se si desidera utilizzare gli utenti creati negli archivi identità esterni, è possibile utilizzarli anche loro. In questo esempio, gli utenti dell'origine identità esterna non sono inclusi. .

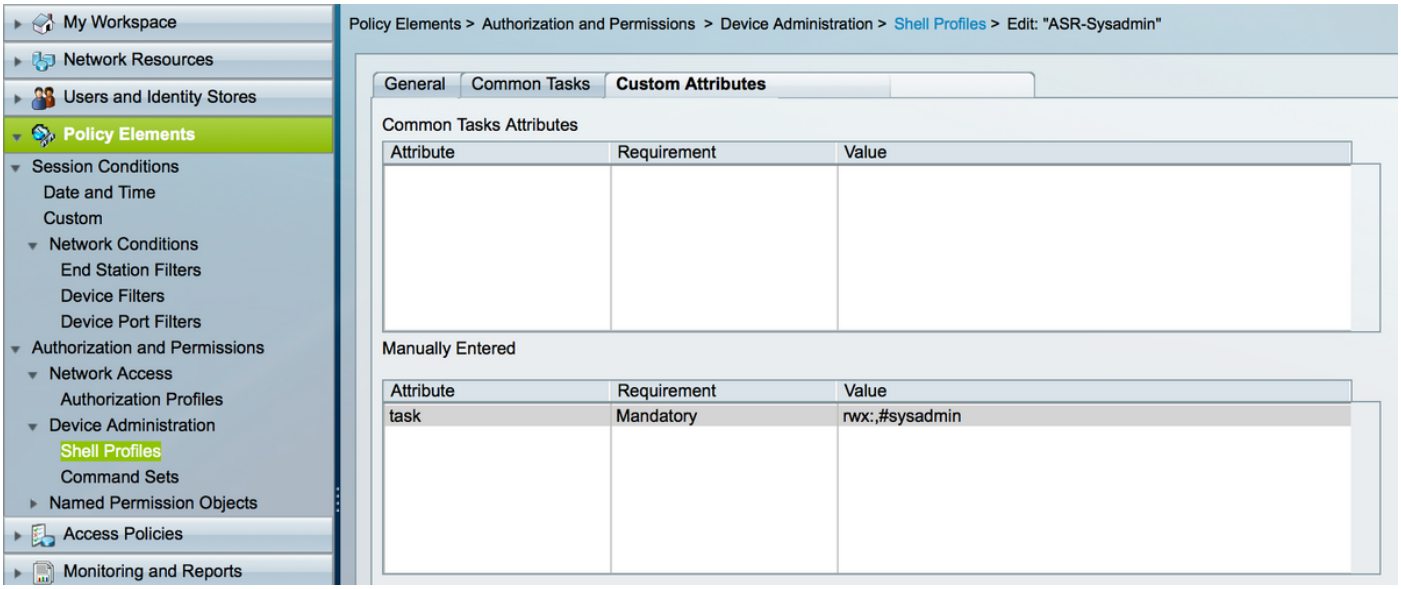
Passaggio 4. Definire il profilo di guscio da sottoporre a push per i rispettivi utenti.

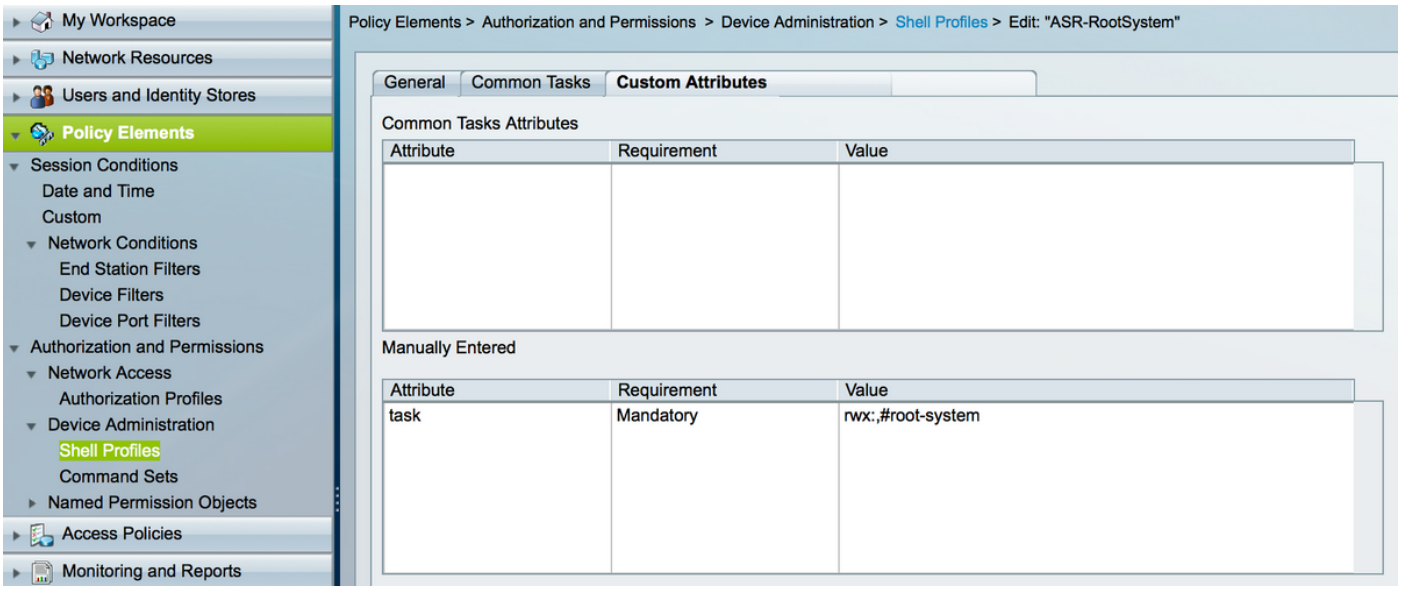


Nel profilo della shell già creato, è possibile configurare per eseguire il push dei rispettivi gruppi di attività, come mostrato nell'immagine.

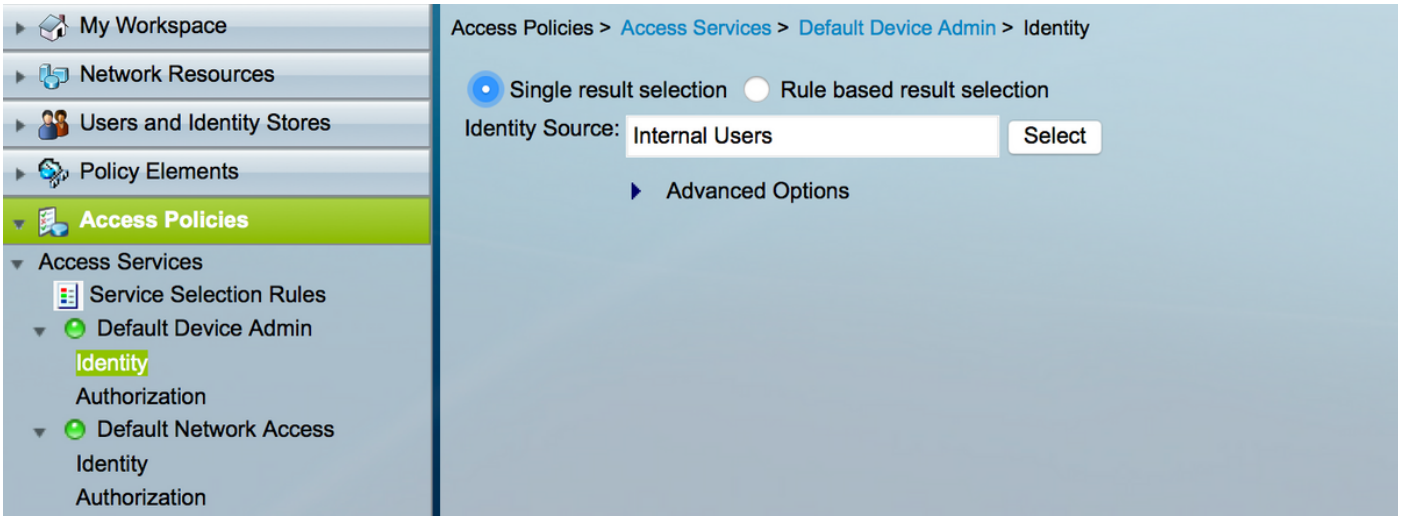




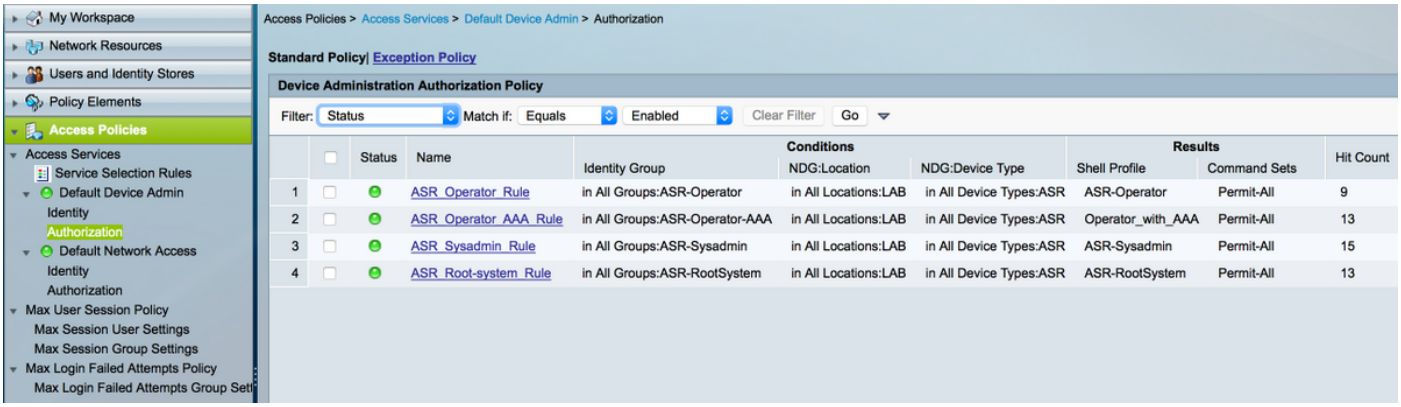




Passaggio 5. Definire il criterio di accesso. L'autenticazione viene eseguita sugli utenti interni.



Passaggio 6. Configurare l'autorizzazione in base al requisito utilizzando i gruppi di identità utente creati in precedenza e mappare i rispettivi profili di shell, come mostrato nell'immagine.



Verifica

Operatore

Per accedere, viene usato **username asrread**. Questi sono i comandi di verifica.

```
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
```

Operatore con AAA

Per accedere, usare il nome utente **asraaa**. Questi sono i comandi di verifica.

> **Nota: asraa** è l'operazione dell'operatore inviata dal server TACACS insieme all'operazione aaa: lettura, scrittura ed esecuzione delle autorizzazioni.

```
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
```

Sysadmin

Per eseguire il login, viene utilizzato **username asrwrite**. Questi sono i comandi di verifica.

```
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 )
```

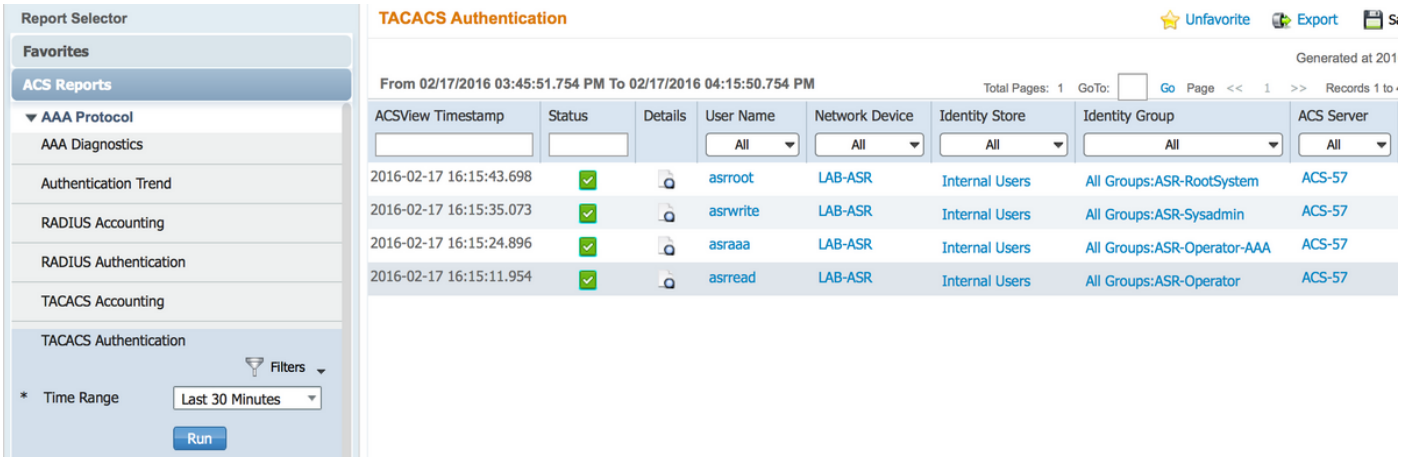
Sistema radice

Per effettuare il login, viene usato **username asrroot**. Questi sono i comandi di verifica.

```
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 )
```

Risoluzione dei problemi

Èpossibile verificare il report ACS dalla pagina di monitoraggio e reporting. Come mostrato nell'immagine, è possibile fare clic sul riepilogo della lente di ingrandimento per visualizzare il report dettagliato.



Di seguito sono riportati alcuni comandi utili per risolvere i problemi relativi a ASR:

- mostra utente
- mostra gruppo utenti
- mostra attività utente
- mostra tutti gli utenti