Cisco Secure ACS 5.x Server로 ASR9k TACACS 구성

목차

소개

이 문서에서는 Cisco Secure ACS(Access Control Server) 5.x 서버에서 TACACS+를 통해 인증 및 권한을 부여하기 위한 ASR 9000 Series ASR(Aggregation Services Router)의 구성에 대해 설명합니다.

다음은 Cisco IOS XR 소프트웨어 시스템에서 사용자 액세스를 제어하는 데 사용되는 작업 기반 권한 부여의 관리 모델 구현의 예입니다. 작업 기반 권한 부여를 구현하는 데 필요한 주요 작업에는 사용자 그룹 및 작업 그룹을 구성하는 방법이 포함됩니다. 사용자 그룹 및 작업 그룹은 AAA(Authentication, Authorization and Accounting) 서비스에 사용되는 Cisco IOS XR 소프트웨어 명령 집합을 통해 구성됩니다. 인증 명령은 사용자 또는 보안 주체의 ID를 확인하는 데 사용됩니다. 권한 부여 명령은 인증된 사용자(또는 주도자)에게 특정 작업을 수행할 수 있는 권한이 부여되었는지 확인하는 데 사용됩니다. 어카운팅 명령은 세션 로깅에 사용되며 특정 사용자 또는 시스템에서 생성된 작업을 기록하여 감사 추적을 생성합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASR 9000 구축 및 기본 컨피그레이션
- ACS 5.x 구축 및 구성.
- TACACS+ 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASR 9000 with Cisco IOS XR Software, 버전 4.3.4
- Cisco Secure ACS 5.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 컨피그레이션 변경의 잠재적 영향을 알고 있는지 확인하십시오.

설정

IOS XR의 사전 정의 구성 요소

IOS XR에는 사전 정의된 사용자 그룹 및 작업 그룹이 있습니다. 관리자는 이러한 미리 정의된 그룹을 사용하거나 요구 사항에 따라 사용자 지정 그룹을 정의할 수 있습니다.

미리 정의된 사용자 그룹

이러한 사용자 그룹은 IOS XR에서 미리 정의됩니다.

사용자 그룹	권한
cisco 지원	디버그 및 문제 해결 기능(일반적으로 Cisco 기술 지원 담당자가 사용)
netadmin	OSPF(Open Shortest Path First)와 같은 네트워크 프로토콜을 구성합니다(일반적으로 네트워크 관리자가 사용).
연산자	일상적인 모니터링 활동을 수행하고 제한된 구성 권한을 보유합니다.
루트-lr	단일 RP 내의 모든 명령을 표시하고 실행합니다.
루트 시스템	시스템의 모든 RP에 대한 모든 명령을 표시하고 실행합니다.
시사민	코어 덤프가 저장되는 위치를 유지하거나 NTP(Network Time Protocol) 시계를 설정하는 등의 라우터에 대한 시스템 관리 작업을 수행합니다.
서비스 관리자	SBC(Session Border Controller)와 같은 서비스 관리 작업을 수행합니다.

루트 시스템 사용자 그룹에는 사전 정의된 권한 부여가 있습니다. 즉, 루트 시스템 사용자 관리 리소

스에 대한 전체 권한과 기타 서비스에서의 특정 권한이 있습니다.

다음 명령을 사용하여 미리 정의된 사용자 그룹을 확인합니다.

```
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>
```

사전 정의 작업 그룹

관리자가 일반적으로 초기 컨피그레이션에 사용할 수 있는 다음과 같은 사전 정의 작업 그룹을 사용할 수 있습니다.

- cisco-support: Cisco 지원 담당자 작업
- netadmin: 네트워크 관리자 작업
- operator: 작업자 일상적인 작업(데모용)
- root-lr: 보안 도메인 라우터 관리자 작업
- root-system: 시스템 전체 관리자 작업
- sysadmin: 시스템 관리자 작업
- serviceadmin: 서비스 관리 작업(예: SBC)

다음 명령을 사용하여 미리 정의된 작업 그룹을 확인합니다.

```
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>
```

이 명령을 사용하여 지원되는 작업을 확인합니다.

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

지원되는 작업 목록은 다음과 같습니다.

AAA	Acl	관리자	취소	Atm	기본 서비스	Bcdl	Bfd	BGP
부팅	번들	콜홈	Cdp	Cef	Cgn	cisco 지원	구성 관리	컨피그레이션 서비스
암호화	당나귀	허용되지 않음	드라이버	Dwdm	이엠	Eigrp	이더넷 서비스	외부 액세스
패브릭	결함 관리자	파일 시스템	방화벽	Fr	Hdlc	호스트 서비스	Hsrp	인터페이스
인벤토리	IP 서비스	Ipv4	Ipv6	이시스	L2vpn	리	리스프	로깅
Lpts	모니터링	mpls-ldp	mpls 고정	mpls-te	멀티캐스트	Netflow	네트워크	nps
OSPF	우니	Pbr	pkg-관리	pos-dpt	Ppp	Qos	Rcmd	늑골
RIP	루트-lr	루트 시스템	경로 지도	경로 정책	Sbc	SNMP	소네트-sdh	고정
Sysmgr	시스템	전송	tty 액세스	터널	유니버설	Vlan	Vpdn	vrrp

위에서 언급 한 각 작업은 이러한 권한 중 하나 또는 모든 4 가지 권한으로 제공 할 수 있습니다.

읽기	읽기 작업만 허용하는 지정을 지정합니다.

쓰기	변경 작업을 허용하고 암시적으로 읽기 작업을 허용하는 지정을 지정합니다.
실행	액세스 작업을 허용하는 지정(예: ping 및 텔넷)을 지정합니다.
디버그	디버그 작업을 허용하는 지정을 지정합니다.

IOS XR의 사용자 정의 구성 요소

사용자 정의 사용자 그룹

관리자는 특정 요구 사항을 충족하기 위해 자신의 사용자 그룹을 구성할 수 있습니다. 구성 예는 다음과 같습니다.

```
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
```

사용자 정의 작업 그룹

관리자는 특정 요구 사항을 충족하기 위해 자신의 작업 그룹을 구성할 수 있습니다. 구성 예는 다음과 같습니다.

```
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
```

특정 명령에 필요한 작업 그룹 및 권한을 찾는 방법을 잘 모르는 경우 describe 명령을 사용하여 작업 그룹을 찾을 수 있습니다. 예를 들면 다음과 같습니다.

예 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#
```

사용자가 show aaa usergroup 명령을 실행하도록 허용하려면 작업 그룹에서 다음 행을 허용해야 합니다.

작업 읽기 aaa

예 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)#
```

사용자가 config 모드에서 aaa authentication login default group tacacs+ 명령을 실행할 수 있도록 하려면 작업 그룹에서 다음 행을 허용해야 합니다.

작업 읽기 쓰기 aaa

여러 작업 그룹을 가져올 수 있는 사용자 그룹을 정의할 수 있습니다. 구성 예는 다음과 같습니다.

```
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
```

라우터의 AAA 컨피그레이션

라우터에서 TACACS 서버를 정의합니다.

여기서 ACS 서버 IP 주소를 key cisco가 포함된 tacacs-server로 정의합니다

```
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
!
```

외부 TACACS 서버에 대한 인증 및 권한 부여를 가리킵니다.

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

명령 권한 부여(선택 사항):

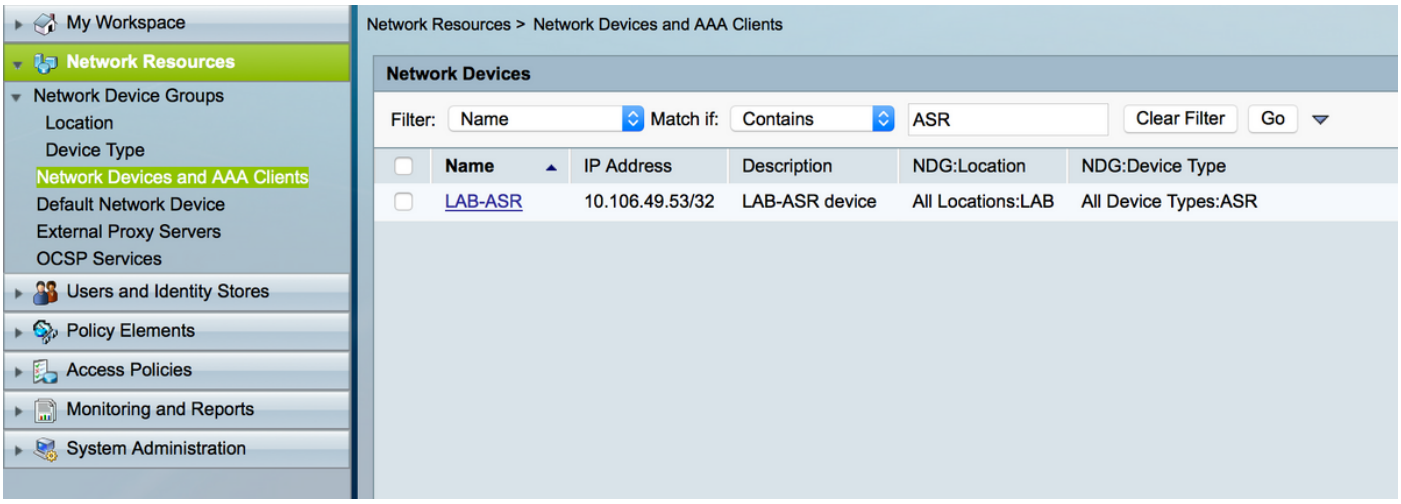
```
#aaa authorization commands default group tacacs+
```

외부 서버에 어카운팅을 지정합니다(선택 사항).

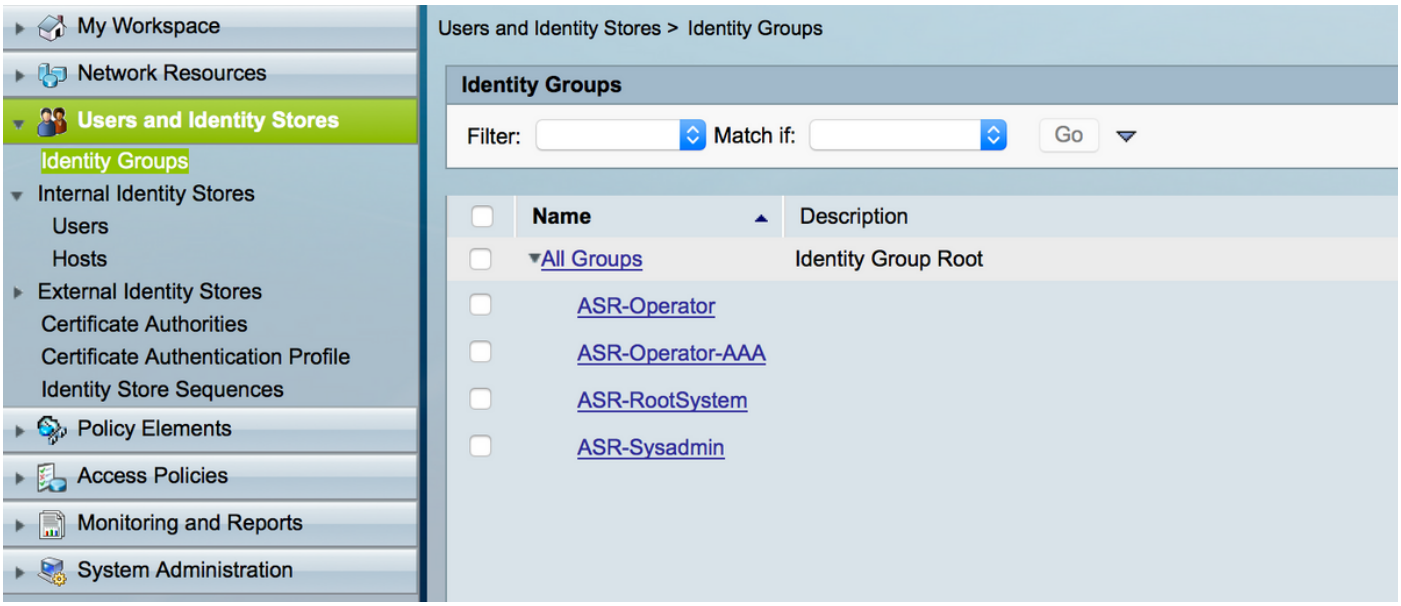
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ACS 서버 컨피그레이션

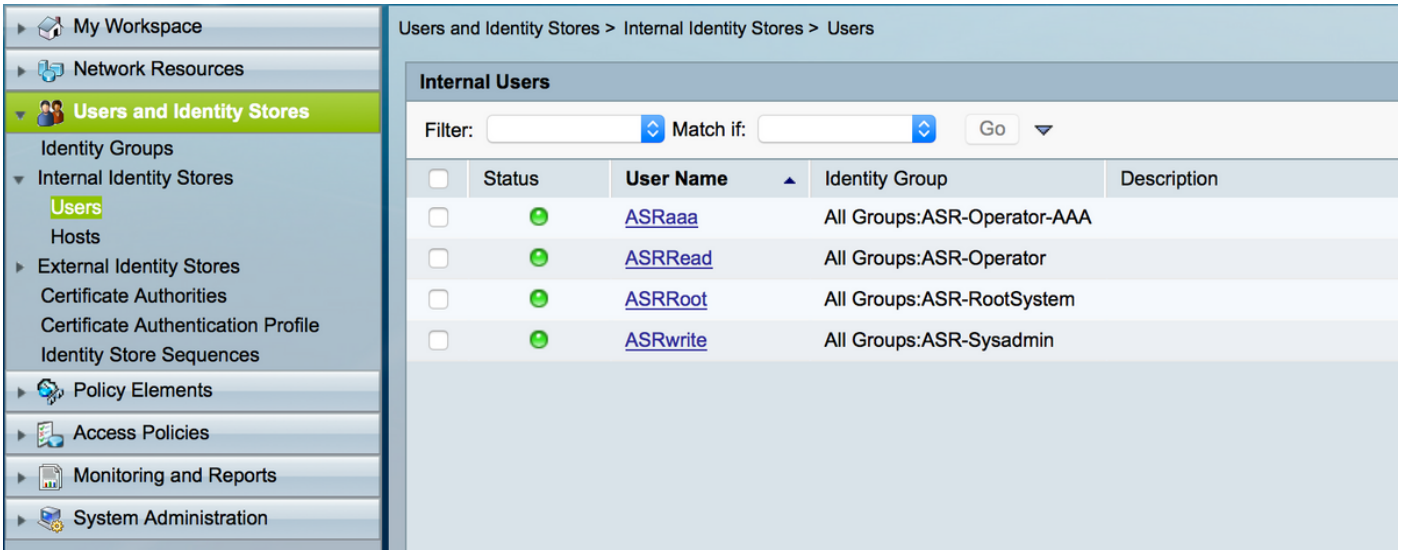
1단계. ACS 서버의 AAA 클라이언트 목록에서 라우터 IP를 정의하려면 이미지에 표시된 대로 Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)로 이동합니다. 이 예에서는 ASR에 구성된 대로 cisco를 공유 암호로 정의합니다.



2단계. 요구 사항에 따라 사용자 그룹을 정의합니다. 이 예에서는 이 이미지에 표시된 대로 4개의 그룹을 사용합니다.

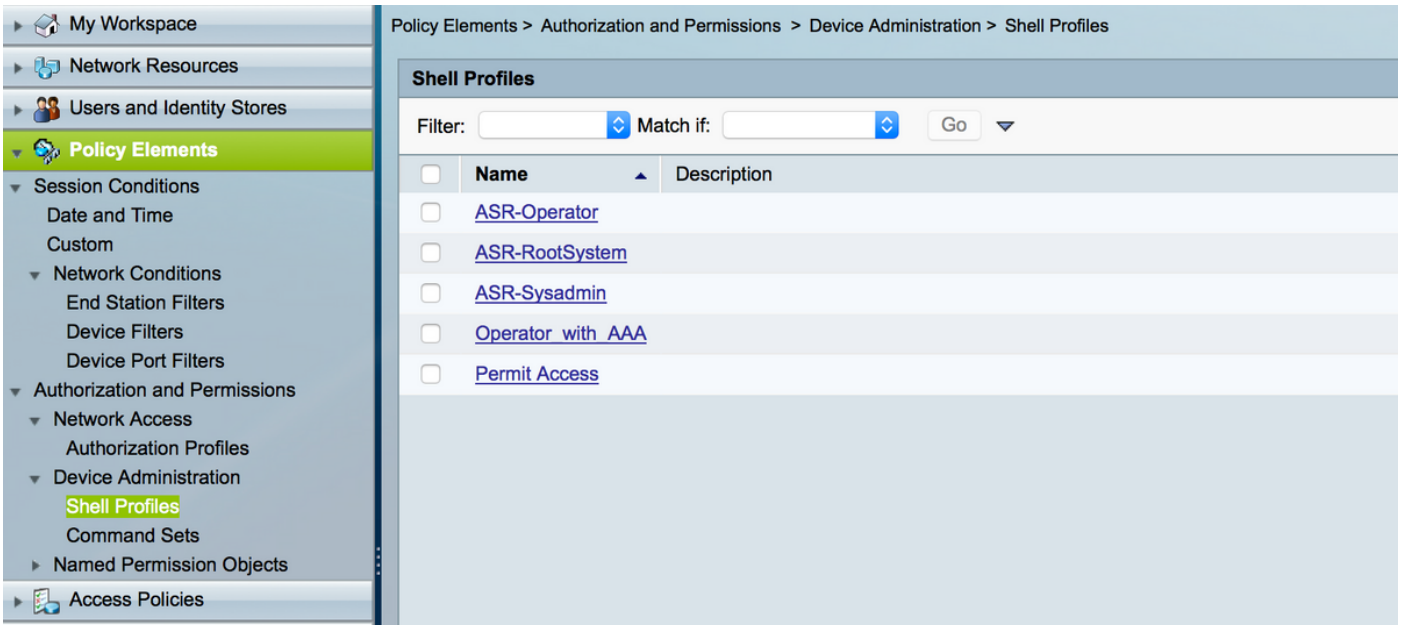


3단계. 이미지에 표시된 대로 사용자를 생성하고 위에서 생성한 각 사용자 그룹에 매핑합니다.

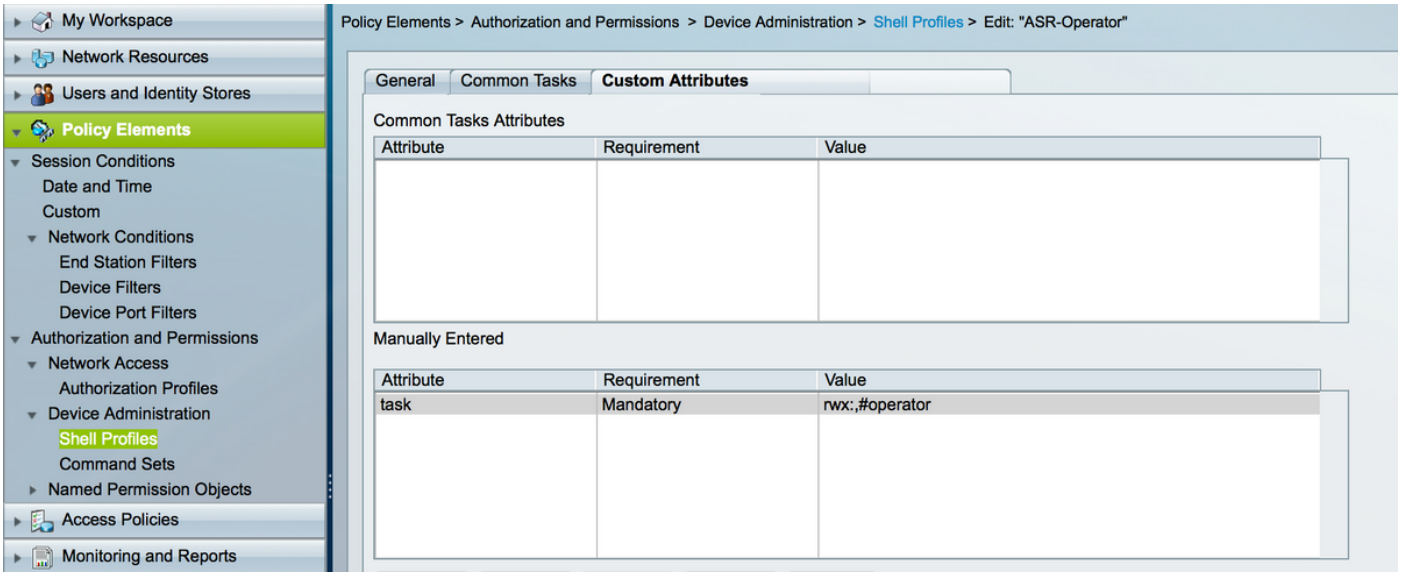


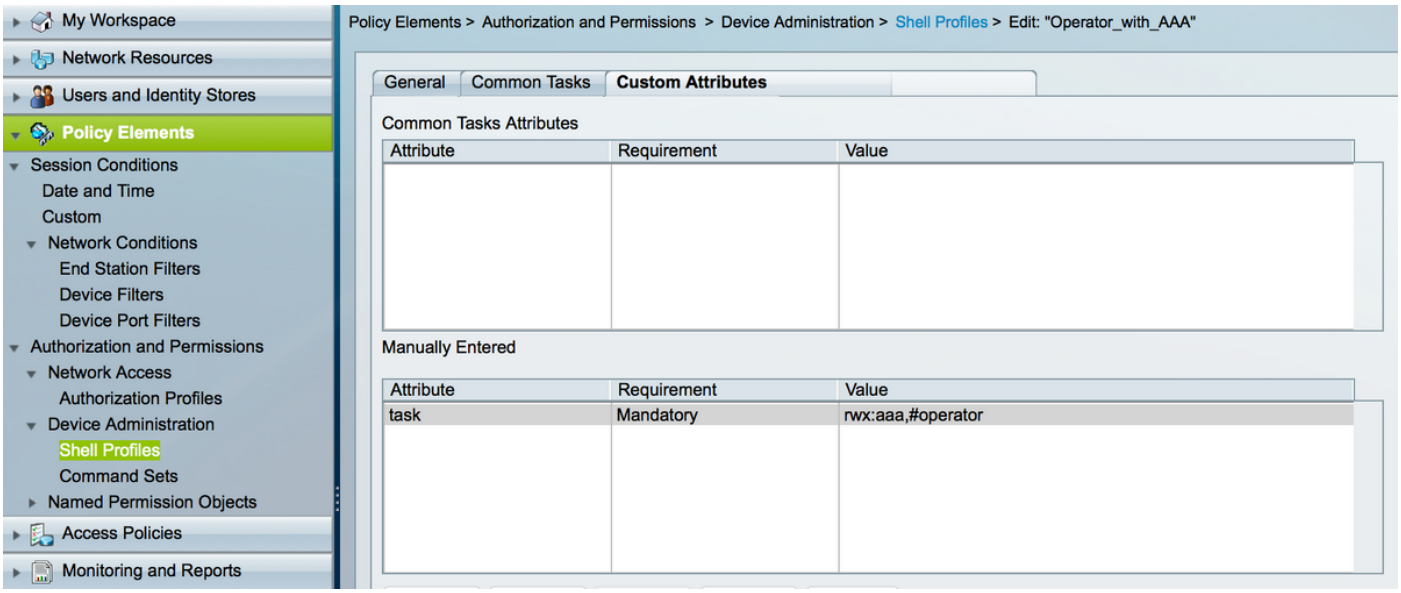
참고: 이 예에서는 인증을 위한 ACS 내부 사용자가 사용됩니다. 외부 ID 저장소에서 생성된 사용자를 사용하려면 해당 사용자도 사용할 수 있습니다. 이 예에서는 외부 ID 소스 사용자가 지원되지 않습니다. .

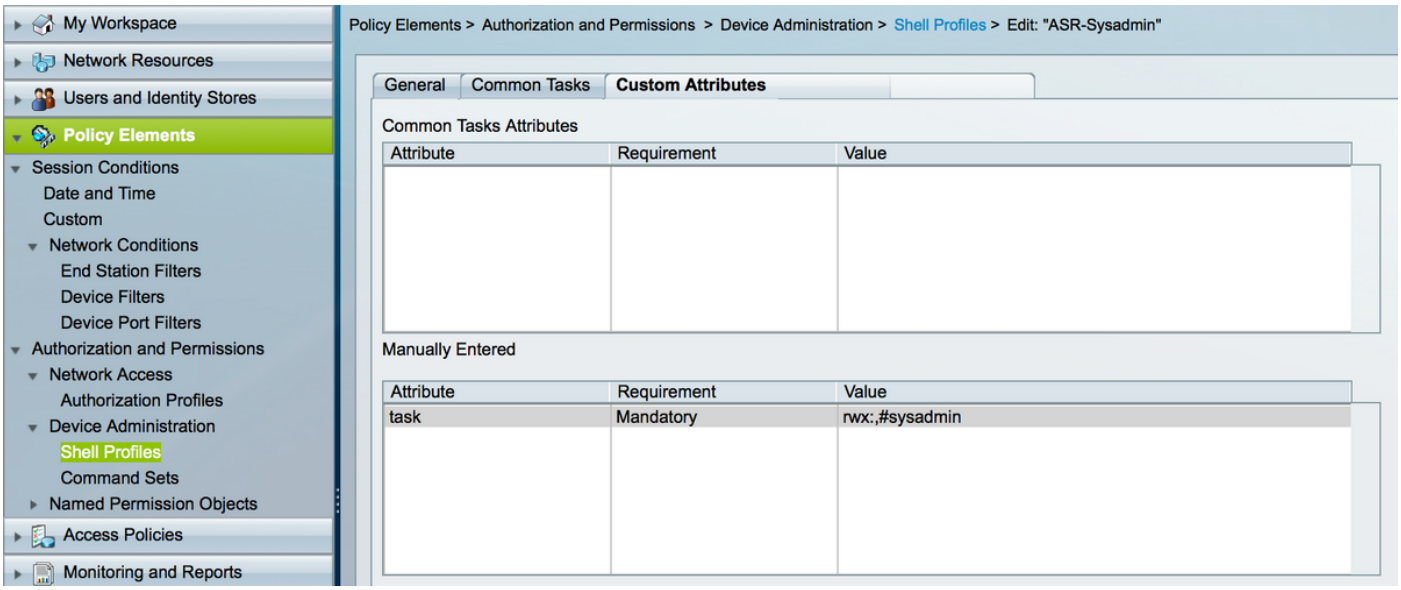
4단계. 각 사용자에 대해 푸시할 셸 프로필을 정의합니다.

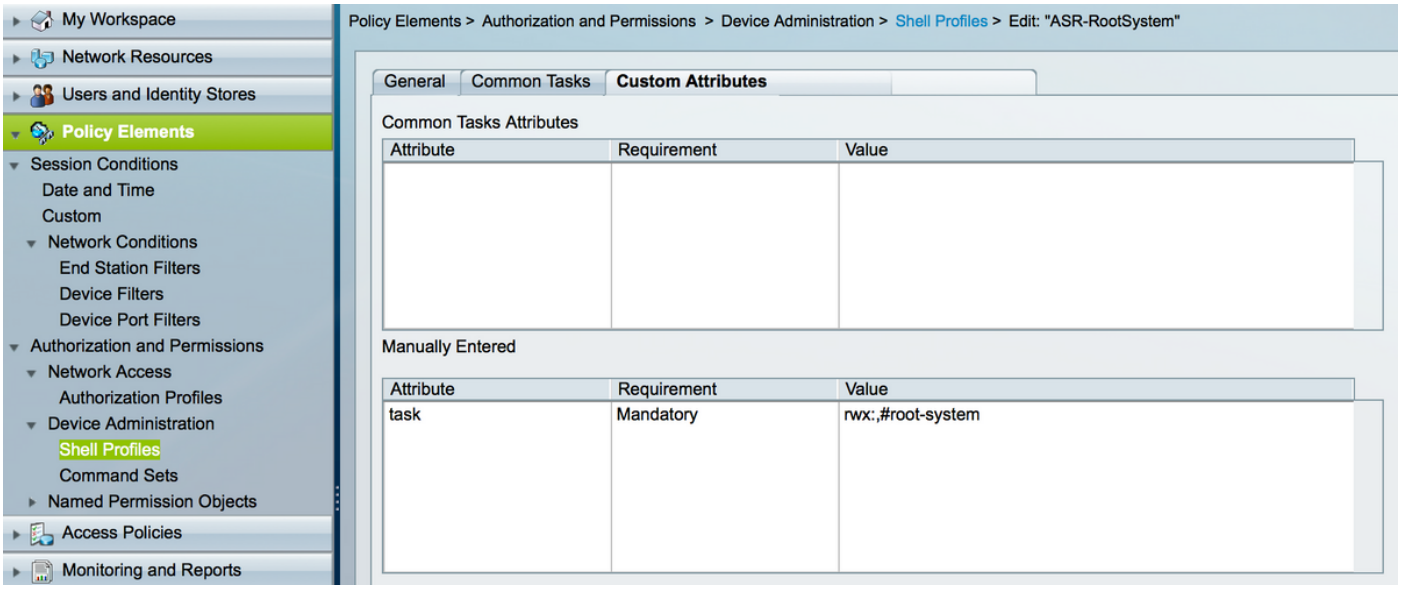


이미 생성된 셸 프로필에서는 이미지에 표시된 대로 각 작업 그룹을 푸시하도록 구성합니다.

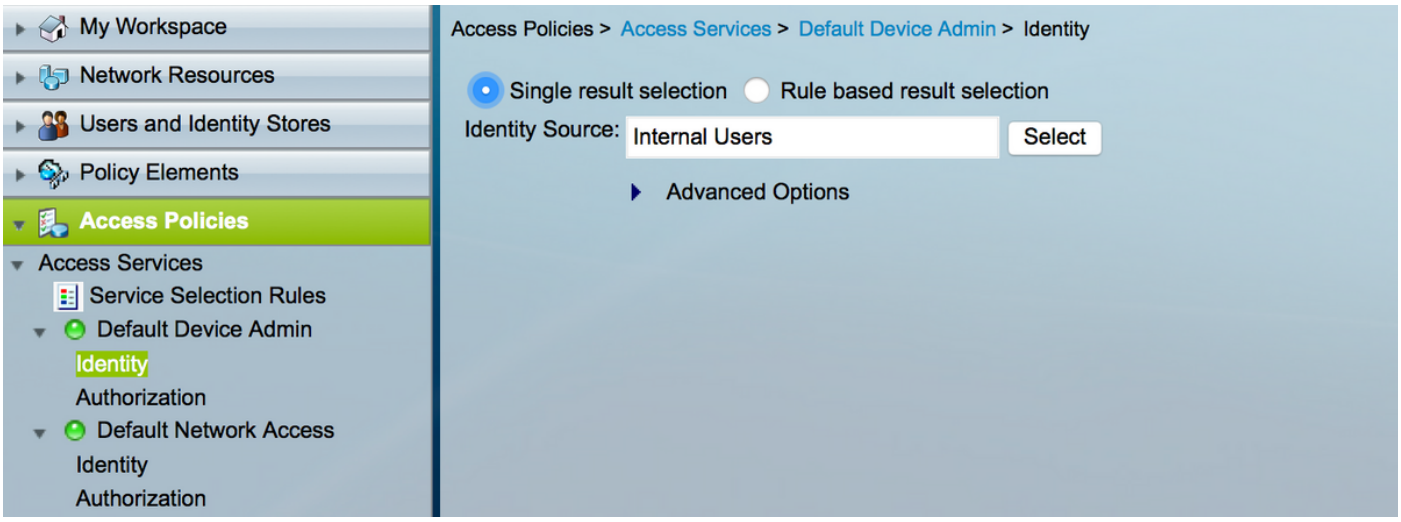




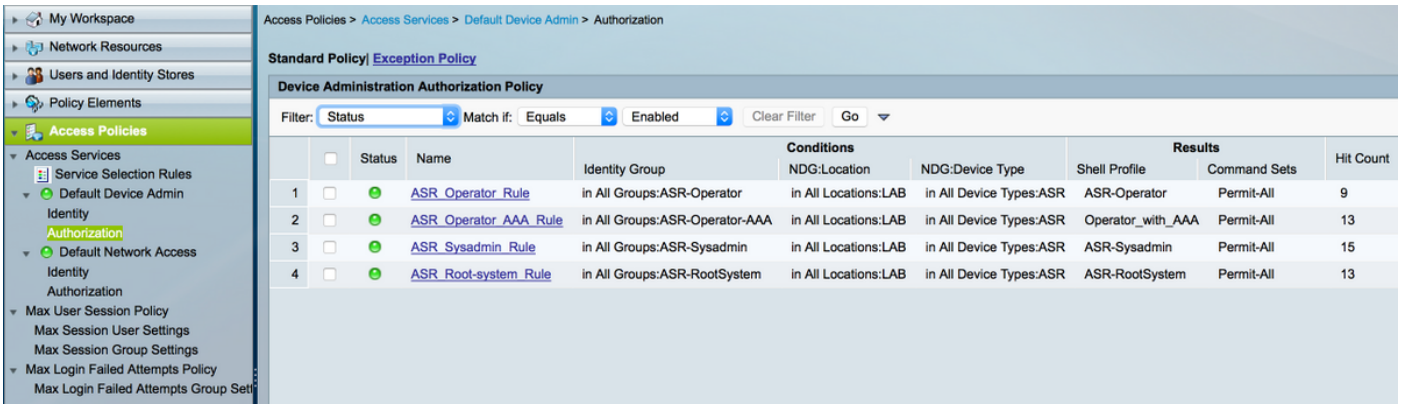




5단계. 액세스 정책을 정의합니다. 내부 사용자에 대해 인증이 수행됩니다.



6단계. 이미지에 표시된 대로 이전에 생성한 사용자 ID 그룹을 사용하여 요구 사항에 따라 권한 부여를 구성하고 각 셸 프로필을 매핑합니다.



다음을 확인합니다.

운영자

로그인하려면 사용자 이름 asrread가 사용됩니다. 다음은 확인 명령입니다.

```
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
```

AAA가 있는 연산자

로그인하기 위해 사용자 이름 asraaa가 사용됩니다. 다음은 확인 명령입니다.

> 참고: asraaa는 aaa 작업 읽기 쓰기 및 실행 권한과 함께 TACACS 서버에서 푸시되는 운영자 작업입니다.

```
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
```

시사민

로그인하려면 사용자 이름 asrwrite가 사용됩니다. 다음은 확인 명령입니다.

```
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 )
```

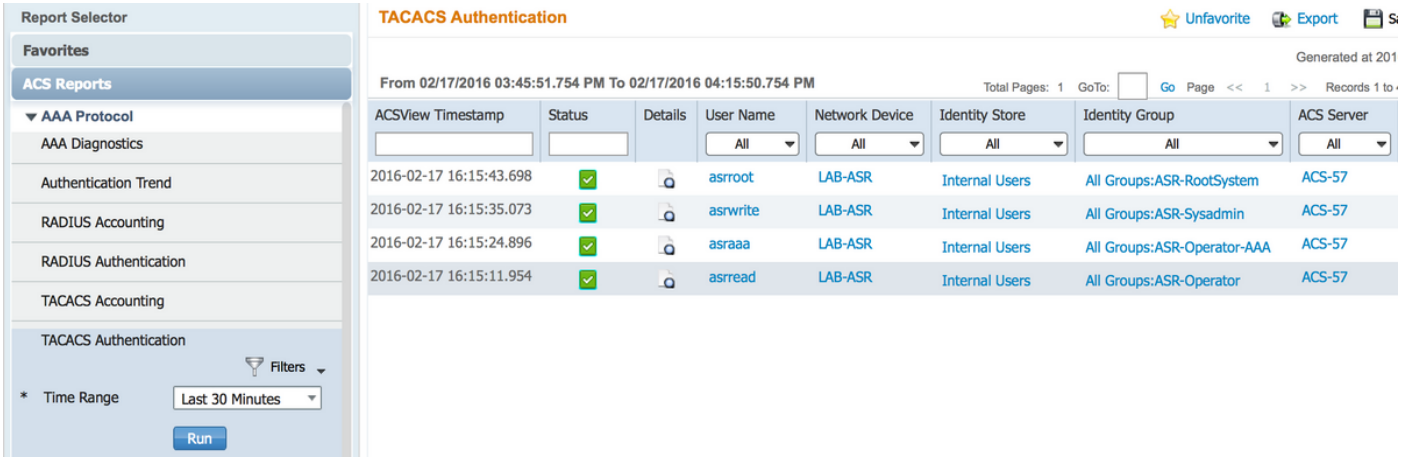
루트 시스템

로그인하려면 사용자 이름 asrroot가 사용됩니다. 다음은 확인 명령입니다.

```
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 )
```

문제 해결

Monitoring and Reporting(모니터링 및 보고) 페이지에서 ACS 보고서를 확인할 수 있습니다. 그림과 같이 돋보기 요약판을 클릭하면 상세 보고서를 볼 수 있습니다.



다음은 ASR에서 문제를 해결하는 데 도움이 되는 몇 가지 명령입니다.

- 사용자 표시
- 사용자 그룹 표시
- 사용자 작업 표시
- 사용자 모두 표시

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.