

# Nexus-integratie met het Configuratievoorbeeld ACS 5.2

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Nexus-apparaat voor verificatie en autorisatie met ACS 5.2-configuratie](#)

[ACS 5.x-configuratie](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document biedt een voorbeeld van de configuratie van TACACS+ verificatie in een Nexus-schakelaar. Als u de Nexus-schakelaar instelt om authenticatie door Access Control Server (ACS) te bewerkstelligen, wordt u automatisch geplaatst in de rol van netwerkoperator/vdc-operator, die alleen-lezen toegang biedt. Om in de netwerk-admin/vdc-admin rol te worden geplaatst, moet u een schelp op ACS 5.2 maken. Dit document beschrijft dat proces.

## [Voorwaarden](#)

### [Vereisten](#)

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Definieer uw Nexus-schakelaar als een client in ACS.
- Definieert het IP-adres en een identieke gedeelde geheime sleutel op de ACS en Nexus.

**Opmerking:** Maak een selectieteken of een back-up op Nexus voordat u wijzigingen aanbrengt.

### [Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ACS 5.2
- Nexus 5000, 5.2(1)N1(1)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

## Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**Opmerking:** Gebruik het [Opname Gereedschap](#) (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

### Nexus-apparaat voor verificatie en autorisatie met ACS 5.2-configuratie

Voer de volgende stappen uit:

1. Maak een lokale gebruiker op de Nexus-schakelaar met volledige rechten voor back-up:

```
username admin privilege 15 password 0 cisco123!
```

2. Schakel TACACS+ in en voer vervolgens het IP-adres van de TACACS+ server (ACS) in:

```
feature tacacs+
```

```
tacacs-server host IP-ADDRESS key KEY
```

```
tacacs-server key KEY
```

```
tacacs-server directed-request
```

```
aaa group server tacacs+ ACS
```

```
server IP-ADDRESS
```

```
use-vrf management
```

```
source-interface mgmt0
```

**Opmerking:** de toets moet overeenkomen met het gedeelde geheim dat op het ACS voor dit Nexus-apparaat is ingesteld.

3. Test de beschikbaarheid van de TACACS-server:

```
test aaa group group-name username password
```

De testauthenticatie zou moeten mislukken met een verworpen bericht van de server, omdat de server niet is geconfigureerd. Dit bericht bevestigt dat de TACACS+ server bereikbaar is.

4. Inlogverificatie configureren:

```
aaa authentication login default group ACS
```

```
aaa authentication login console group ACS
```

```
aaa accounting default group ACS
```

```
aaa authentication login error-enable
```

```
aaa authorization commands default local
```

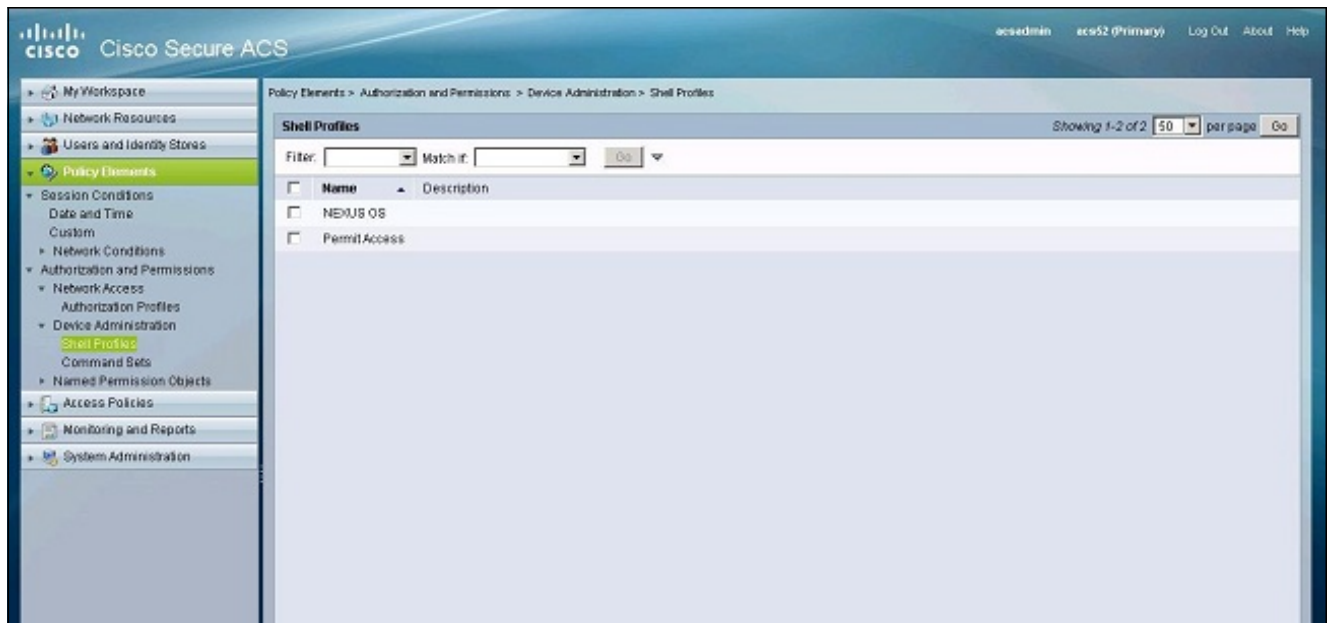
```
aaa authorization config-commands default local
```

**Opmerking:** Nexus gebruikt lokale authenticatie als de authenticatieserver onbereikbaar is.

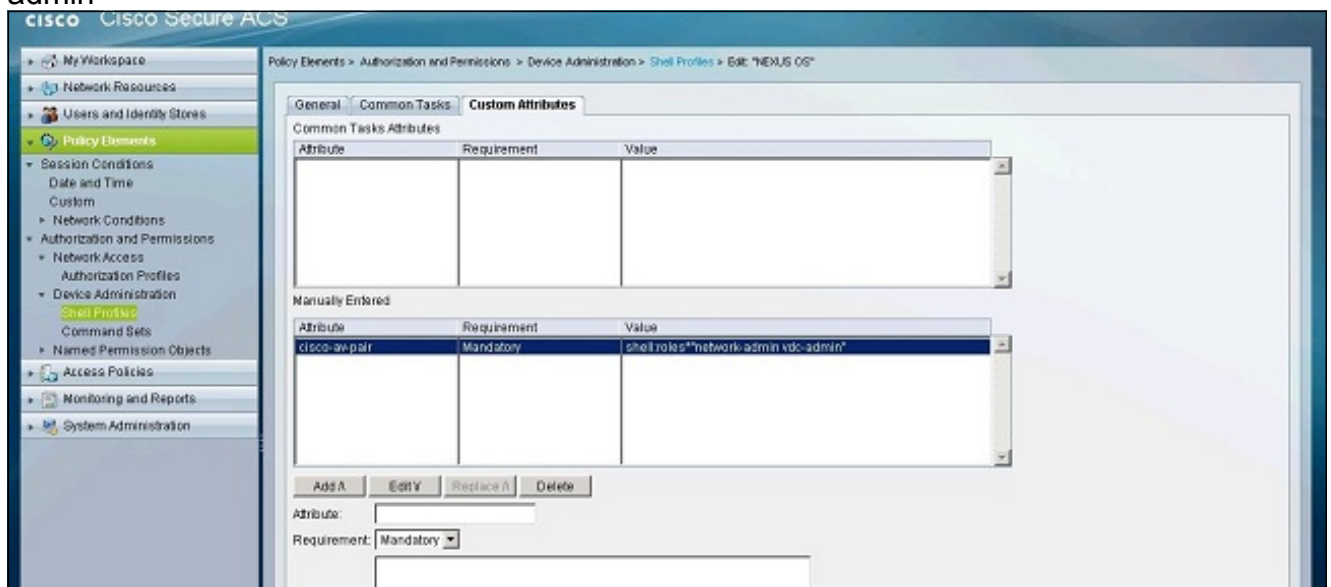
## [ACS 5.x-configuratie](#)

Voer de volgende stappen uit:

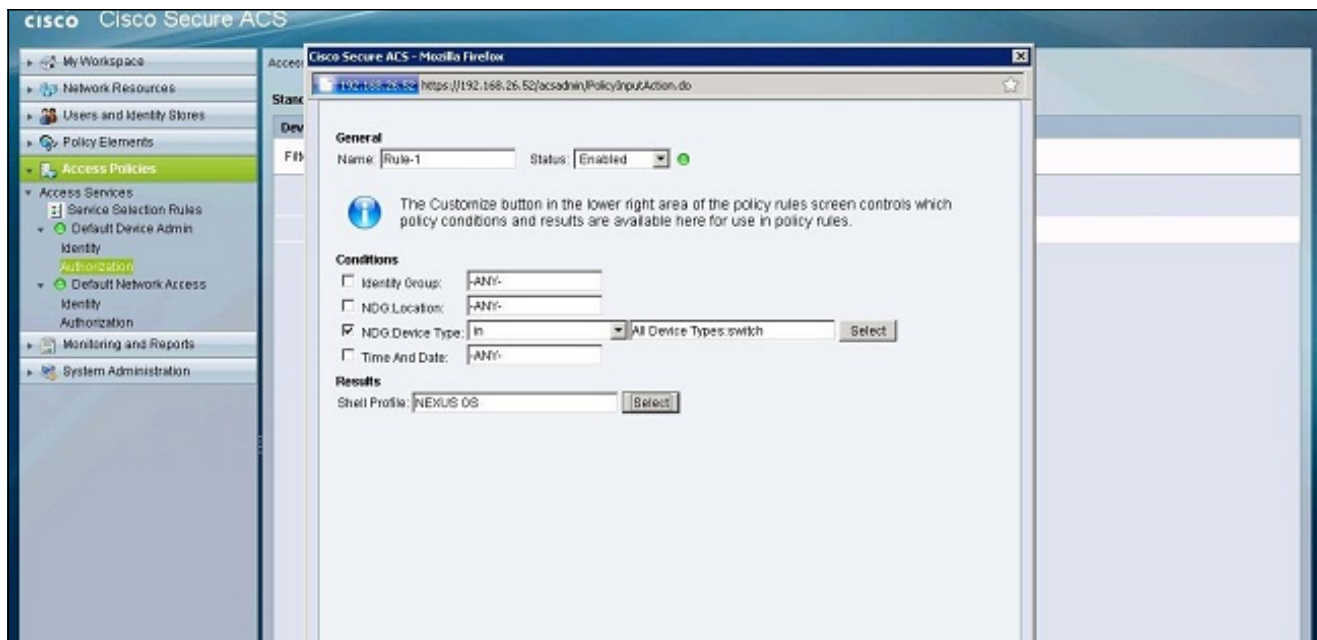
1. Navigeer naar **elementen van het beleid > Verificatie en toegangsrechten > Apparaatbeheer > Shell profielen** om een Shell-profiel te maken.



2. Voer een naam in voor het profiel.
3. Typ deze waarden onder het tabblad Eigen kenmerken: Kenmerk: cisco-av-paarVoorschrift: VerplichtValue: shell:rollen\*"netwerk-beheerder vdc-admin"



4. Breng de veranderingen in om een op eigenschap gebaseerde rol voor de Nexus schakelaar te creëren.
5. Maak een nieuwe autorisatieregel, of bewerk een bestaande regel in het juiste toegangsbeleid. Standaard worden TACACS+ verzoeken verwerkt door het beleid voor de toegang tot het standaardapparaat.
6. Kies in het gedeelte Voorwaarden de juiste voorwaarden. Kies in het gedeelte Resultaten het profiel Nexus OS shell.



7. Klik op OK.

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- [Tacacs+](#) —Hier worden de TACACS+ statistieken weergegeven.
- [toon in werking stellen-in werking stellen-configuratie tacacs+](#)-Toont de configuratie TACACS+ in de actieve configuratie.
- [toon opstarten-in-configuratie tacacs+](#)-Hiermee wordt de configuratie TACACS+ in de opstartconfiguratie weergegeven.
- [Tacacs-server](#) —Hier worden alle geconfigureerde TACACS+ serverparameters weergegeven.

## Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)