ISE 2.0: ASA CLI-configuratievoorbeeld voor TACACS+ verificatie en opdracht

Inhoud

Inleiding

Dit document beschrijft hoe u TACACS+ verificatie en geautoriseerde commando's kunt configureren op Cisco adaptieve security applicatie (ASA) met Identity Services Engine (ISE) 2.0 en hoger. ISE gebruikt lokale identiteitsopslag om resources zoals gebruikers, groepen en endpoints op te slaan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA Firewall is volledig operationeel
- Connectiviteit met ASA en ISE
- ISE Server is geblokkeerd

Gebruikte componenten

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

- Cisco Identity Services Engine 2.0
- Cisco ASA-softwarerelease 9.5(1)S

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.

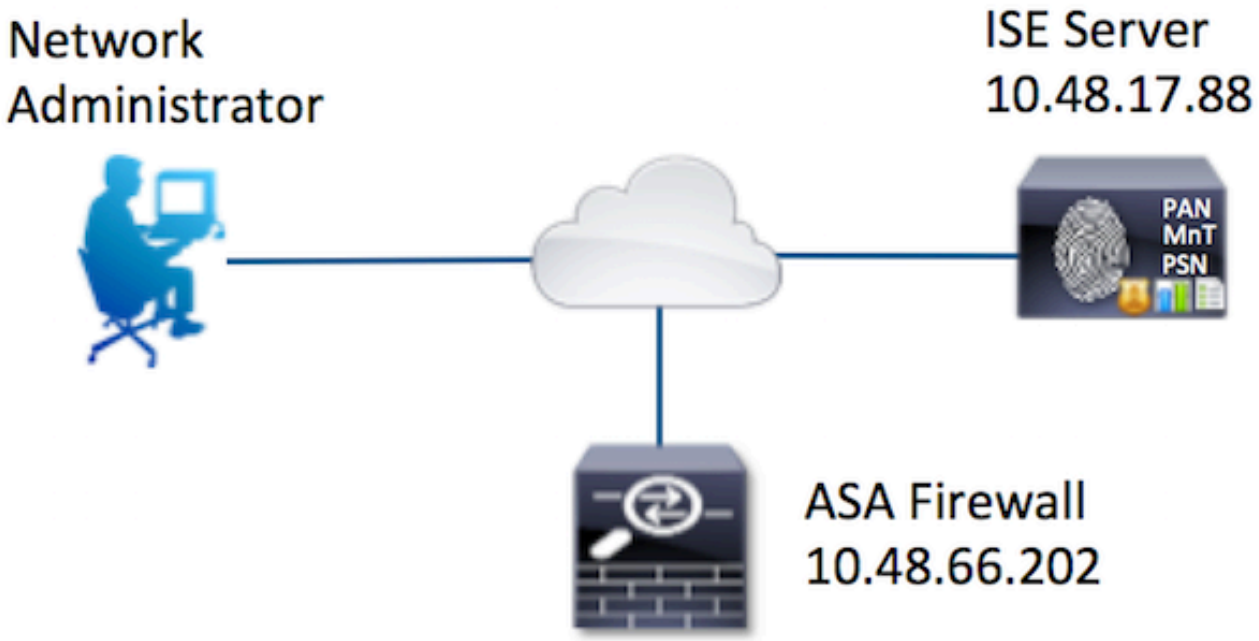
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Het doel van de configuratie is:

- Verifieer de gebruiker via Interne Identity Store
- autorisatie van de ssh-gebruiker zodat deze in de bevoorrechte EXEC-modus wordt geplaatst na de inlognaam
- Controleer en stuur elke uitgevoerde opdracht naar ISE ter verificatie

Netwerkdiagram



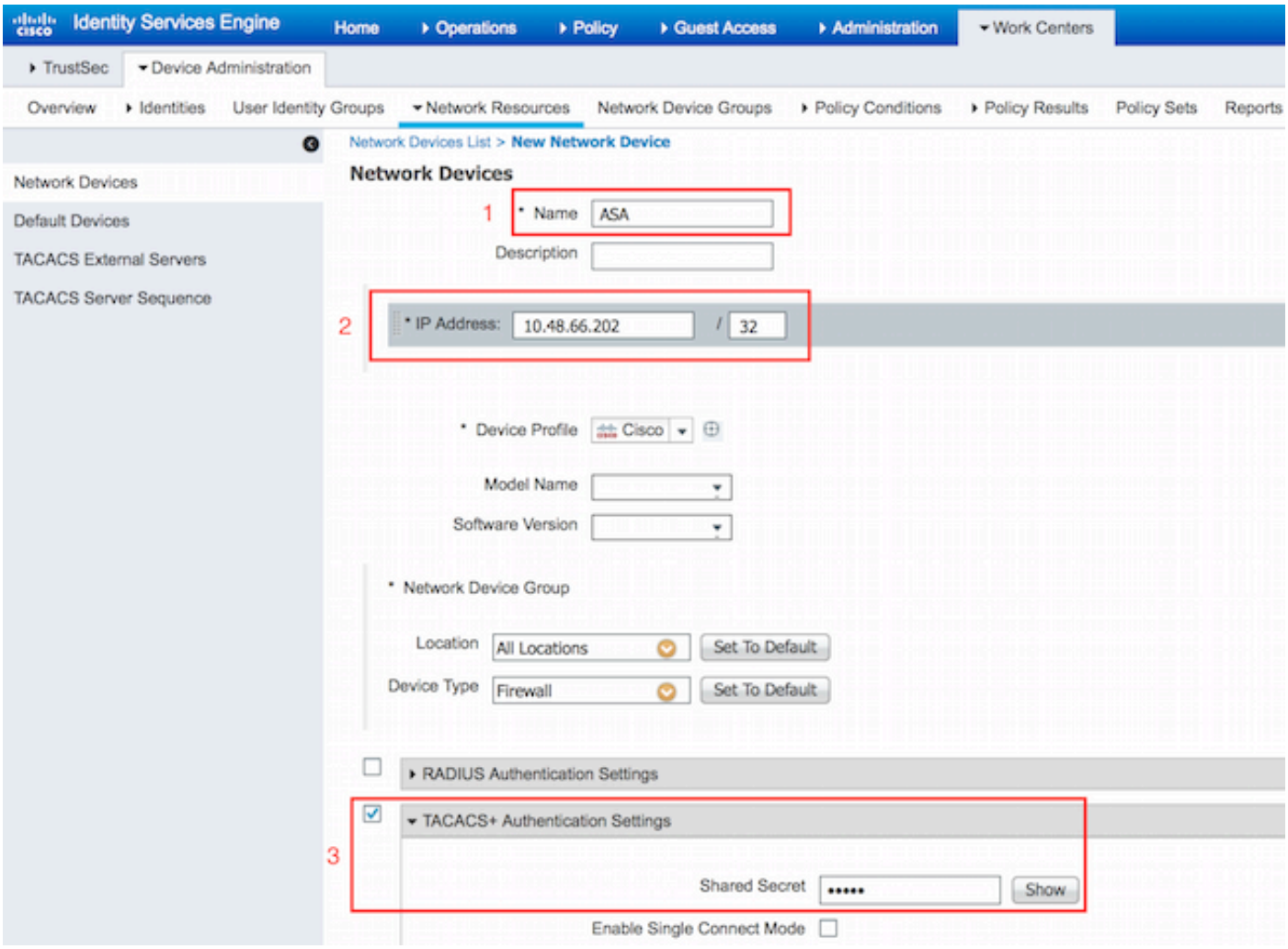
Configuraties

ISE configureren voor verificatie en autorisatie

Er worden twee gebruikers gemaakt. Gebruiker **beheerder** is een deel van **Network Admins** Local Identity Group op ISE. Deze gebruiker heeft volledige CLI privileges. Gebruiker maakt deel uit van ISE-groep voor **netwerkonderhoud**. Deze gebruiker mag alleen opdrachten tonen en pingelen.

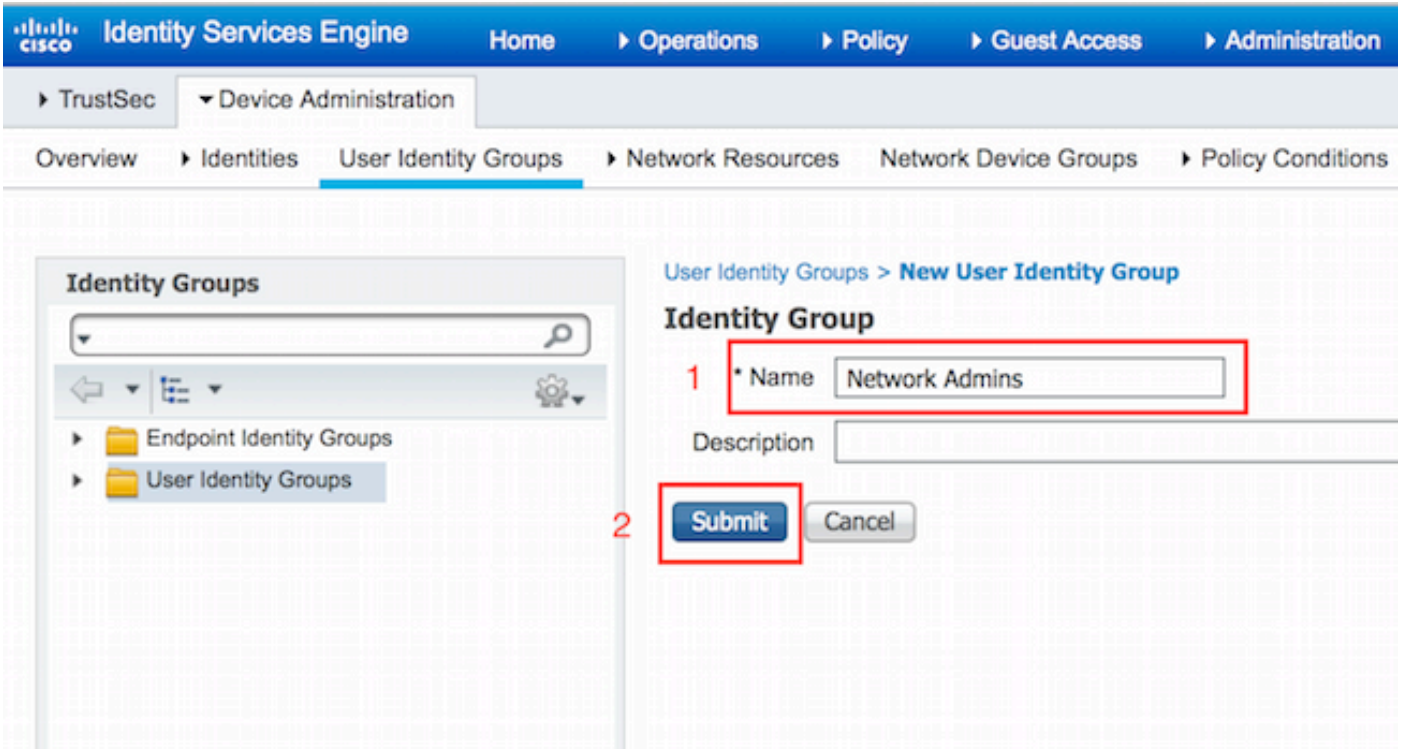
Netwerkapparaat toevoegen

Blader naar **werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten.** Klik op **Toevoegen.** Geef naam, IP-adres, selecteer het selectieteken **TACACS+ verificatie-instellingen** en specificeer **gedeelde** beveiligingstoets. U kunt desgewenst het type/de locatie van het apparaat instellen.



Gebruikersidentiteitsgroepen configureren

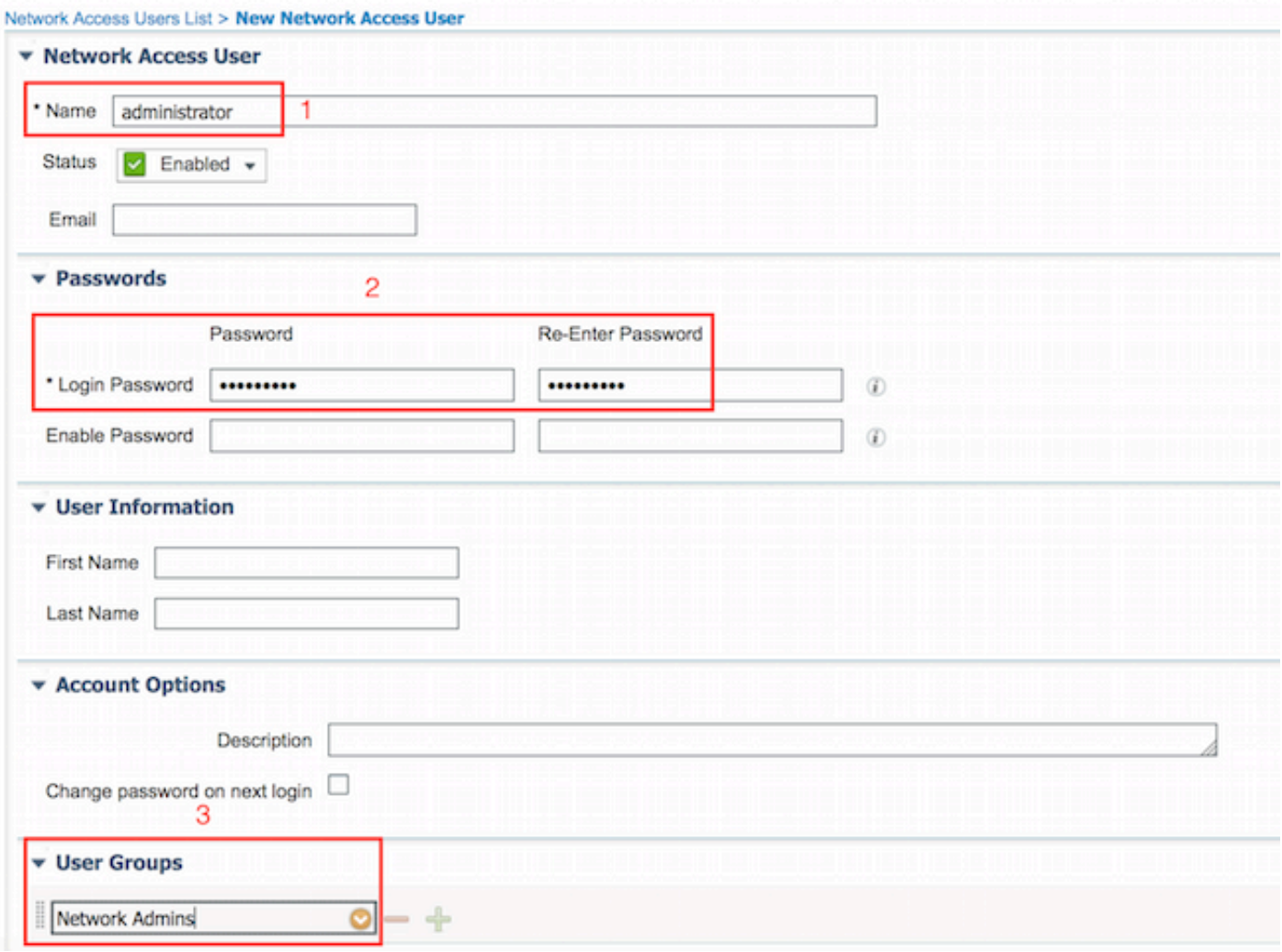
Blader naar **werkcentra > Apparaatbeheer > Gebruikersgroepen.** Klik op **Toevoegen.** Geef naam op en klik op **Indienen.**



Herhaal dezelfde stap om de gebruikersgroep **van het** Netwerk **Onderhoudsteam** te configureren.

Gebruikers configureren

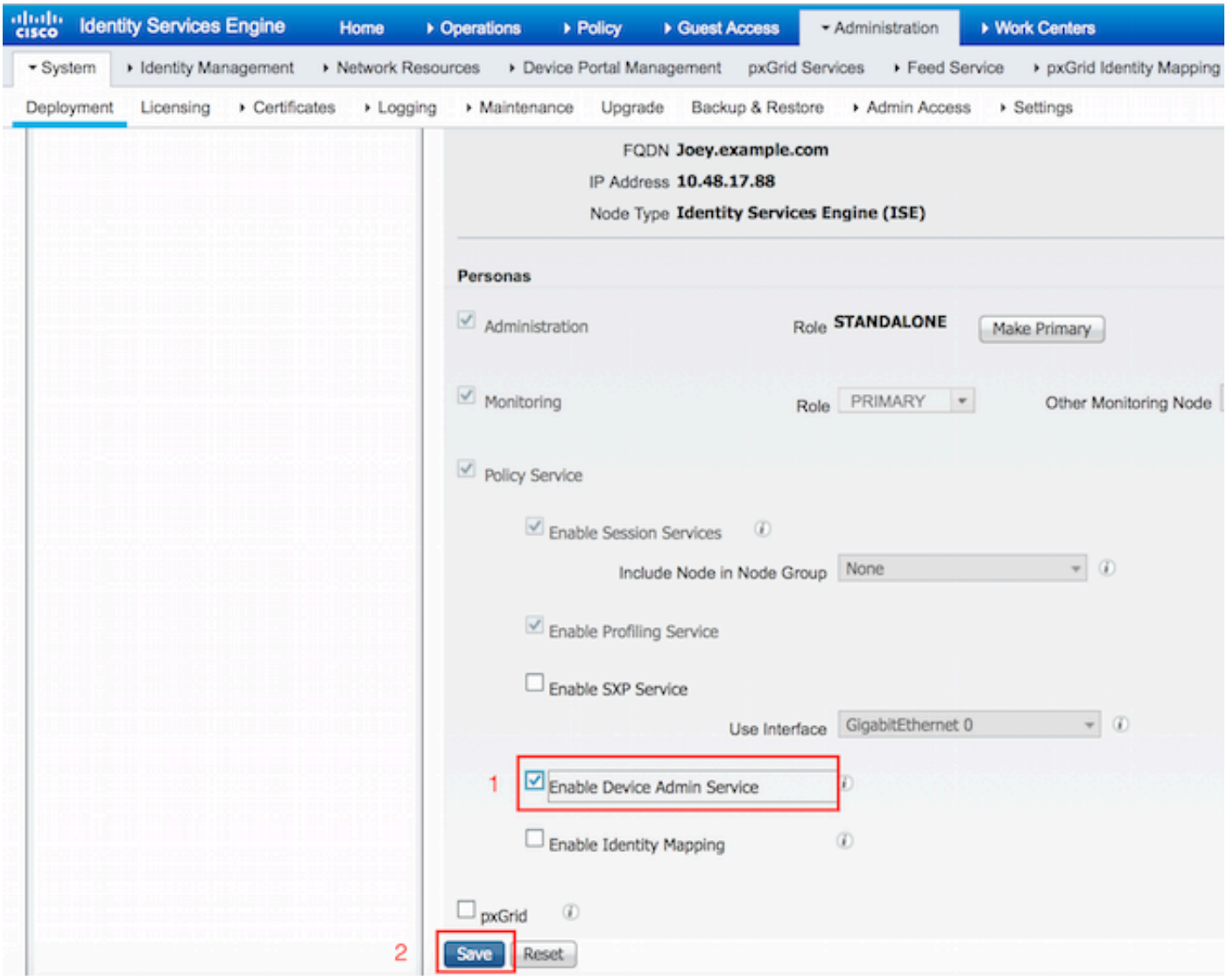
Navigeer naar **werkcentra > Apparaatbeheer > Identificaties > Gebruikers.** Klik op **Toevoegen.** Geef naam op, inlogwachtwoord specificeert gebruikersgroep en klik op **Indienen**.



Herhaal de stappen om **gebruiker** te configureren en wijs **de** gebruikersgroep **van het** Netwerk **Onderhoudsteam toe**.

Apparaatbeheerservice inschakelen

Navigeer naar **Administratie > Systeem > Plaatsing.** Selecteer het gewenste knooppunt. Selecteer het selectieteken **Apparaatbeheer inschakelen** en klik op **Opslaan.**

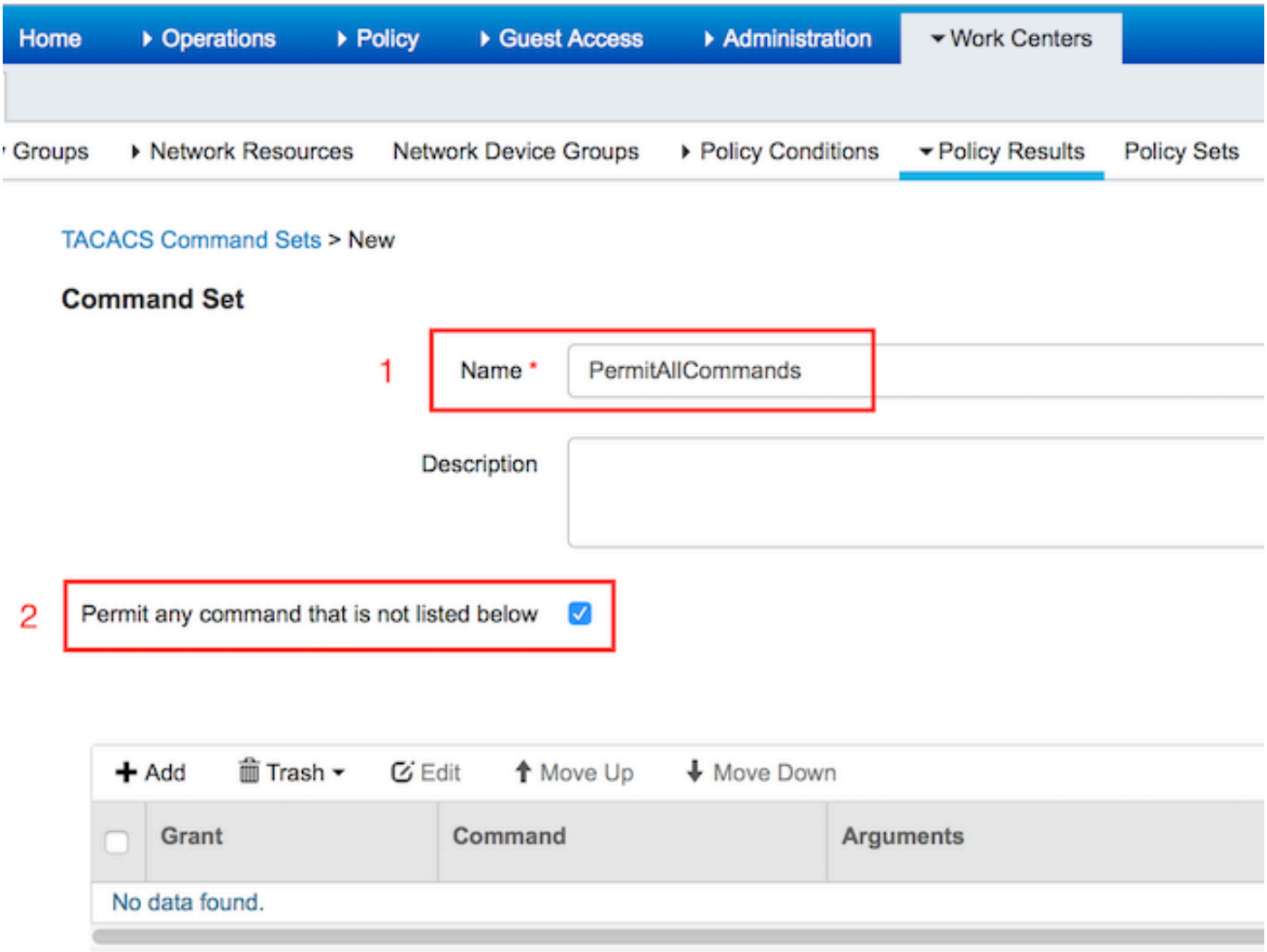


Opmerking: Voor TACACS moet er een afzonderlijke licentie zijn geïnstalleerd.

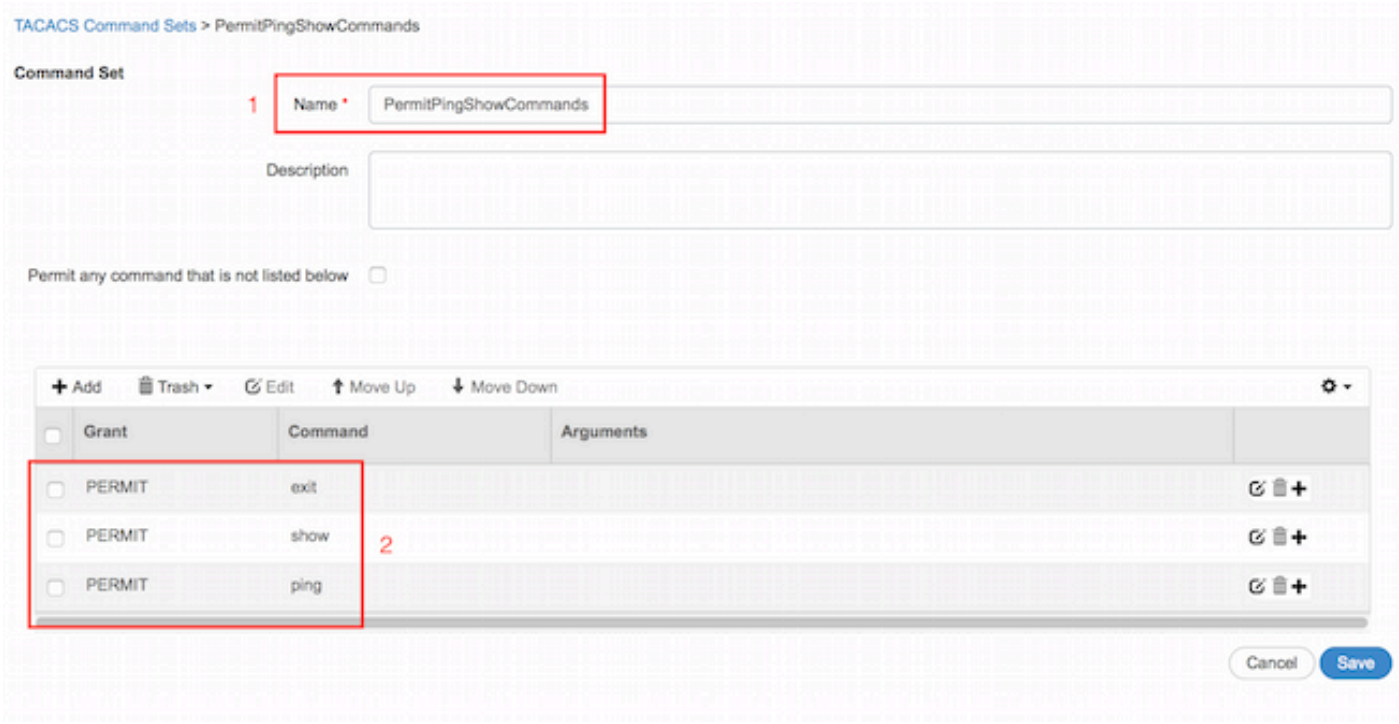
TACACS-opdrachtsets configureren

Er worden twee opdrachtsets ingesteld. Eerst **PermitAllCommands** voor de **beheerder** gebruiker die alle opdrachten op het apparaat toestaat. Tweede **PermitPingShowCommands** voor **gebruiker** die alleen opdrachten tonen en pingeren toestaat.

1. Blader naar **werkcentra > Apparaatbeheer > Beleidsuitkomsten > TACACS-opdrachtsets.** Klik op **Toevoegen.** Typ de **opdracht** Naam **toestaanAllCommands,** selecteer **Geef een opdracht toe die niet hieronder** weergegeven **is** en klik op **Indienen.**

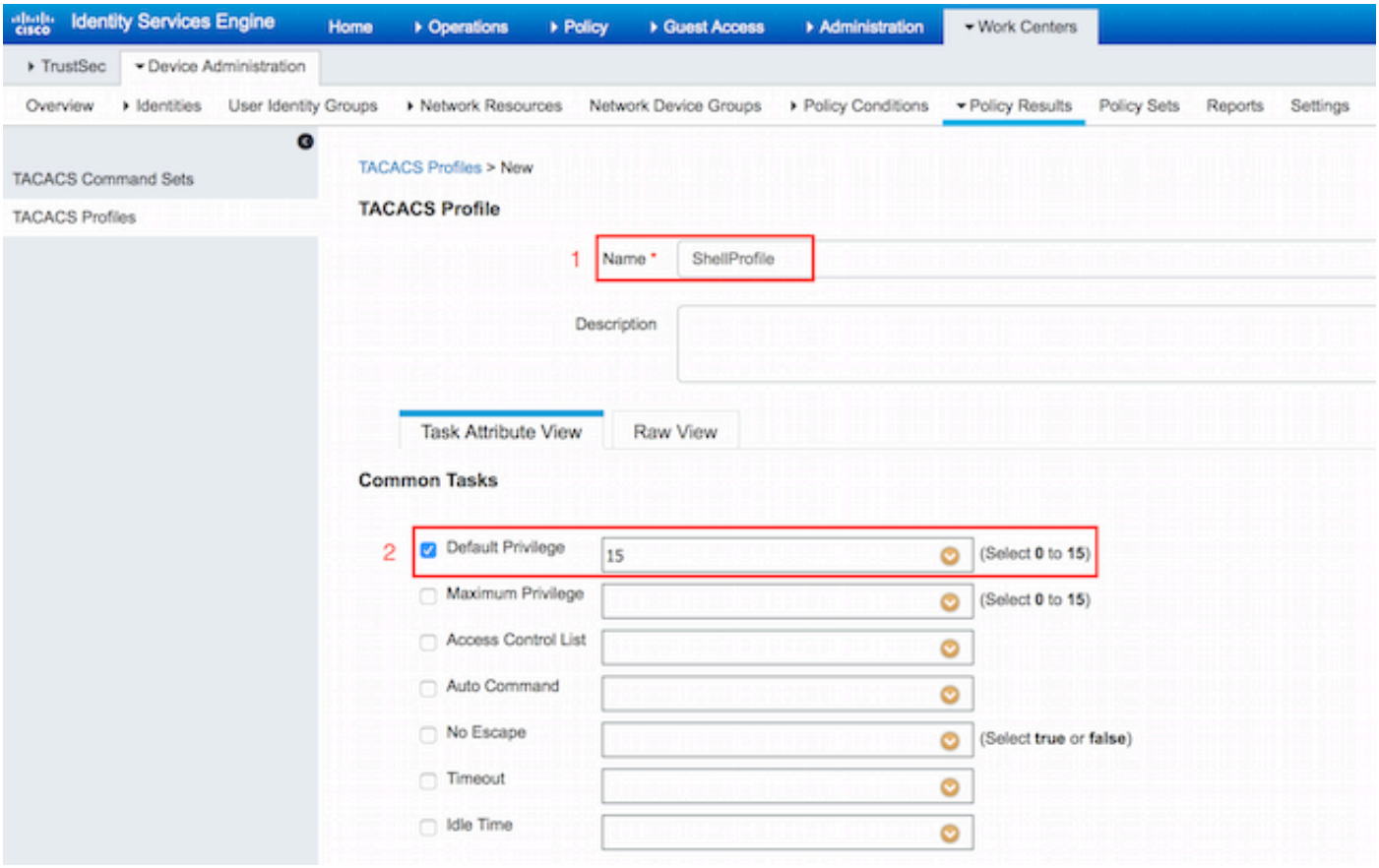


2. Blader naar **werkcentra > Apparaatbeheer > Beleidsuitkomsten > TACACS-opdrachtsets.** Klik op **Toevoegen.** Geef de **opdrachten** voor **de naamPingShowCommands op,** klik op **Add** en laat **show** toe**, ping** en **exit.** Standaard als Argumenten blanco blijven, worden alle argumenten opgenomen. Klik op **Inzenden.**



TACACS-profiel configureren

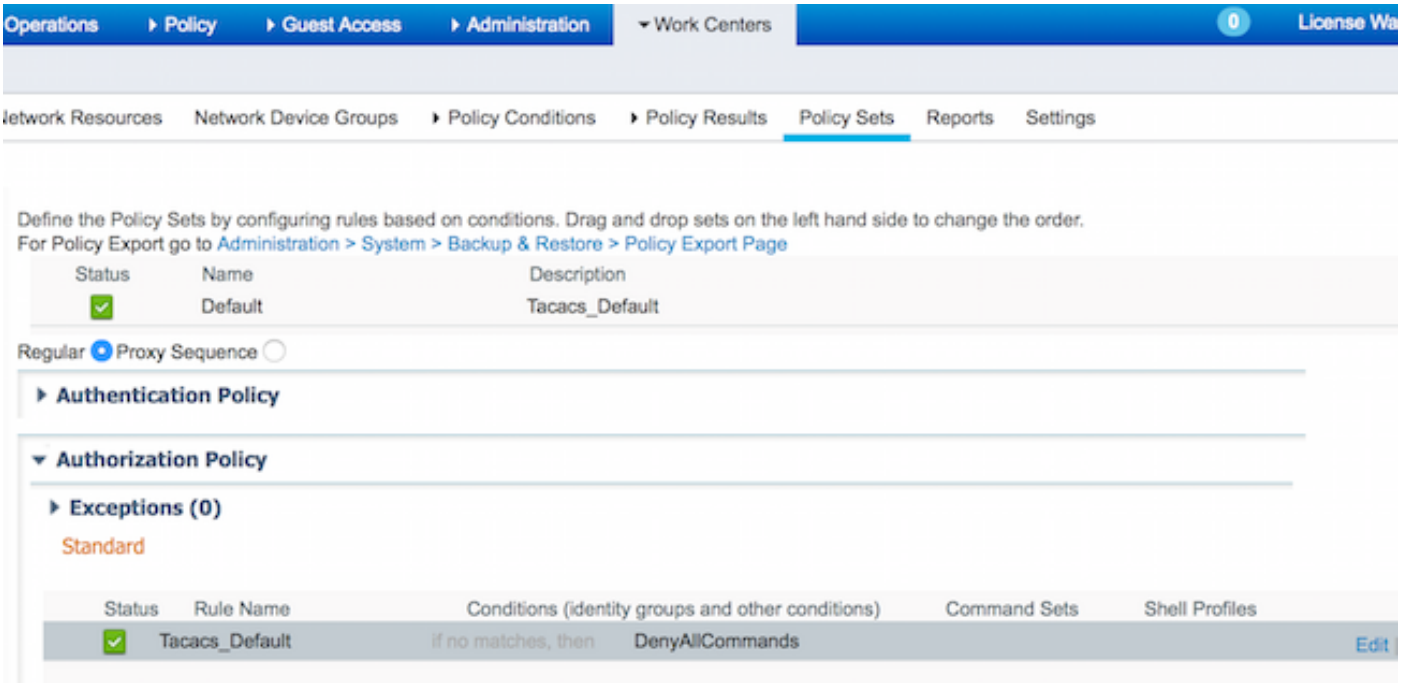
Eén TACACS-profiel wordt ingesteld. De eigenlijke opdrachtregel wordt uitgevoerd via opdrachtsets. Navigeer naar **werkcentra > Apparaatbeheer > Beleidsresultaten > TACACS profielen.** Klik op **Toevoegen.** Geef een naam op **ShellProfile,** selecteer **het** selectieteken **Default Priviool** en voer de waarde van 15 in. Klik op **Indienen**.



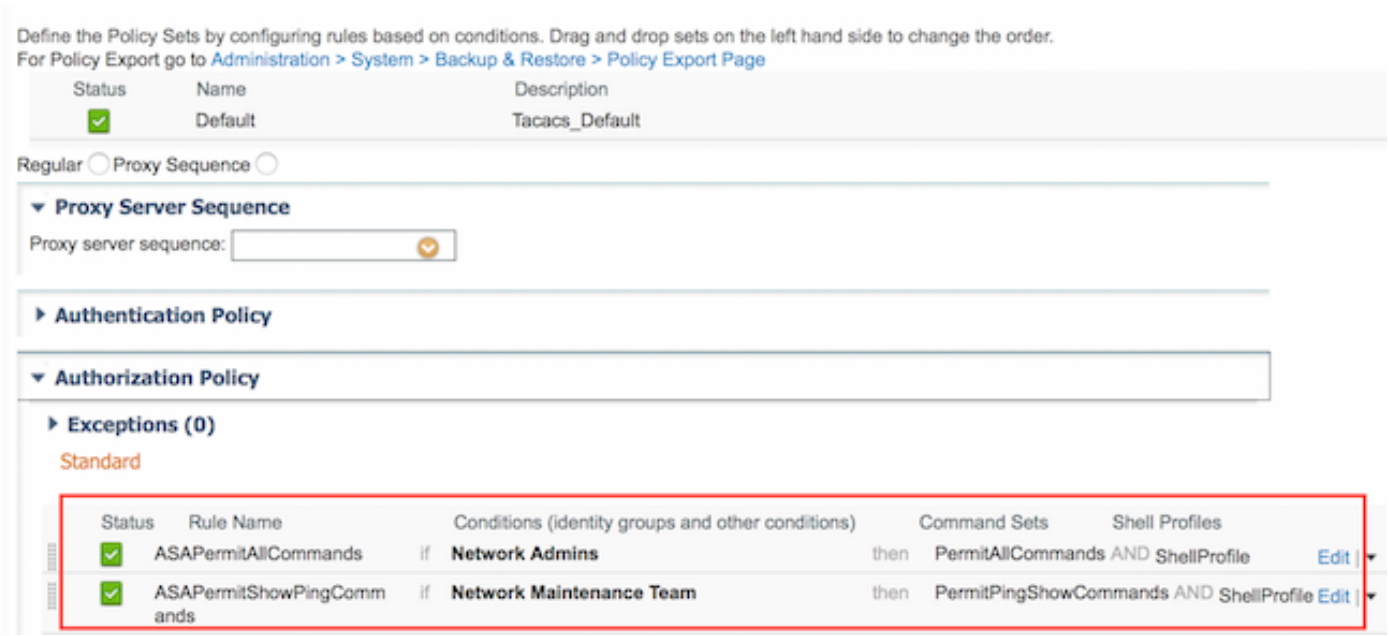
Het TACACS-machtigingsbeleid configureren

Verificatiebeleid door standaard punten naar All_User_ID_Stores, die ook de Local Store bevat, dus deze blijft ongewijzigd.

Navigeer naar **werkcentra > Apparaatbeheer > Beleidsformaten > Standaard > autorisatiebeleid > Bewerken > Nieuwe regel hierboven invoegen.**



Er worden twee goedkeuringsregels ingesteld. De eerste regel wijst TACACS-profiel **ShellProfile** toe en de opdracht Set **PermitAllCommands toe** op basis van **Network Admins** User Identity Group lidmaatschap. Tweede regel toegewezen TACACS-profiel **ShellProfile** en opdrachtset **PermitPingShowCommands** op basis van **het** lidmaatschap **van de** Gebruiker van het **Team** van de **Onderhoud**.



Configureer de Cisco ASA firewall voor verificatie en autorisatie

1. Maak een lokale gebruiker met volledig privilege voor back-up met de gebruikersnaam, zoals hier wordt getoond

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Defineer TACACS server ISE, specificeer interface, protocol ip adres en **tacacs** toets.

```
aaa-server ISE protocol tacacs+
aaa-server ISE (mgmt) host 10.48.17.88
 key cisco
```

> Opmerking: De servertoets dient overeen te komen met die welke eerder op ISE Server is gedefinieerd.

3. Test de bereikbaarheid van de TACACS-server met de opdracht test **aaa** zoals getoond.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

De uitvoer van de vorige opdracht toont aan dat de TACACS-server bereikbaar is en dat de gebruiker geauthentiseerd is.

4. Het configureren van de authenticatie voor ssh, exec autorisatie en commando vergunningen zoals hieronder wordt getoond. Met **een autorisatie exec authenticatie-server** kunt u automatisch in bevoorrechte EXEC modus worden geplaatst.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

> Opmerking: Met de bovenstaande opdrachten wordt verificatie uitgevoerd op ISE, wordt de gebruiker direct in de bevoorrechtingsmodus geplaatst en wordt de opdrachtautorisatie uitgevoerd.

5. Laat shh op de gmt-interface staan.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

Verifiëren

Cisco ASA-firewallverificatie

1. Schakel over naar de ASA Firewall als **beheerder** die deel uitmaakt van de gebruikersgroep met volledige toegang. De groep **Network Admins** is in kaart gebracht aan **ShellProfile** en Commands **All** Commands in ISE. Probeer elke opdracht uit te voeren om volledige toegang te garanderen.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
```

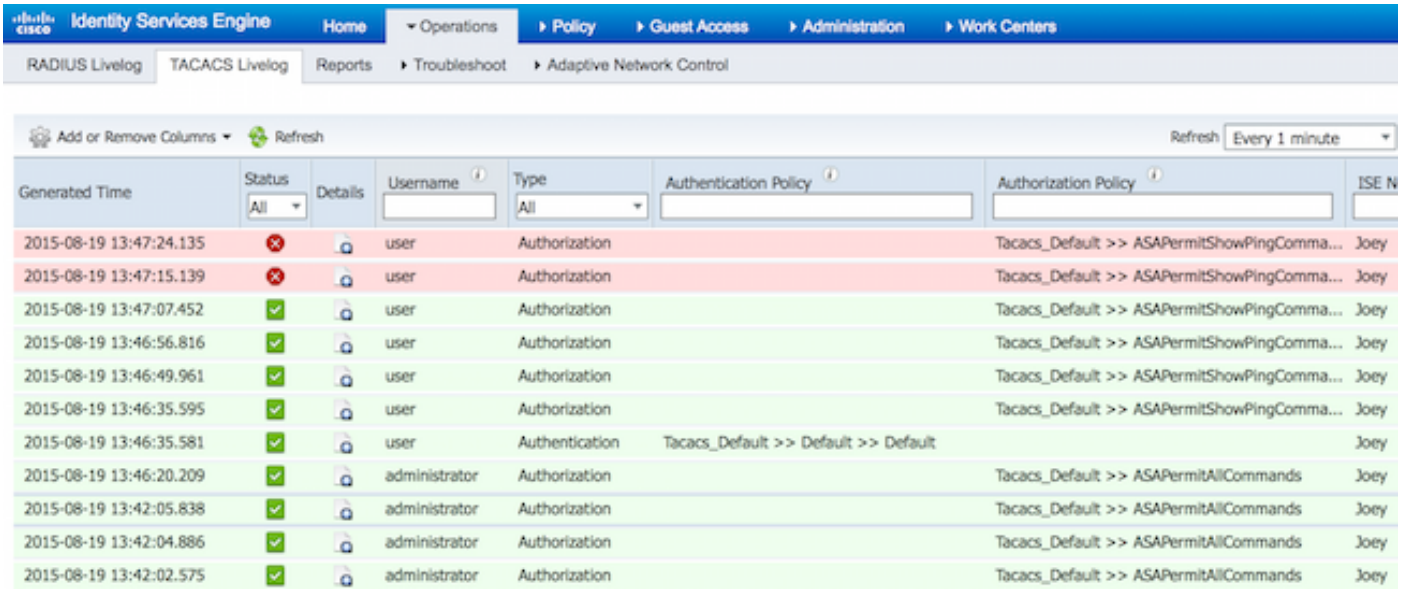
```
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. Stap naar de ASA Firewall als **gebruiker** die tot de gebruikersgroep met beperkte toegang behoort. **De** groep **van het Netwerk van Onderhoud** wordt in kaart gebracht aan **ShellProfile** en **PermitPingShowCommands** die op ISE is ingesteld. Probeer om het even welke opdracht uit te voeren om ervoor te zorgen dat slechts tonen en pingopdrachten kunnen worden afgegeven.

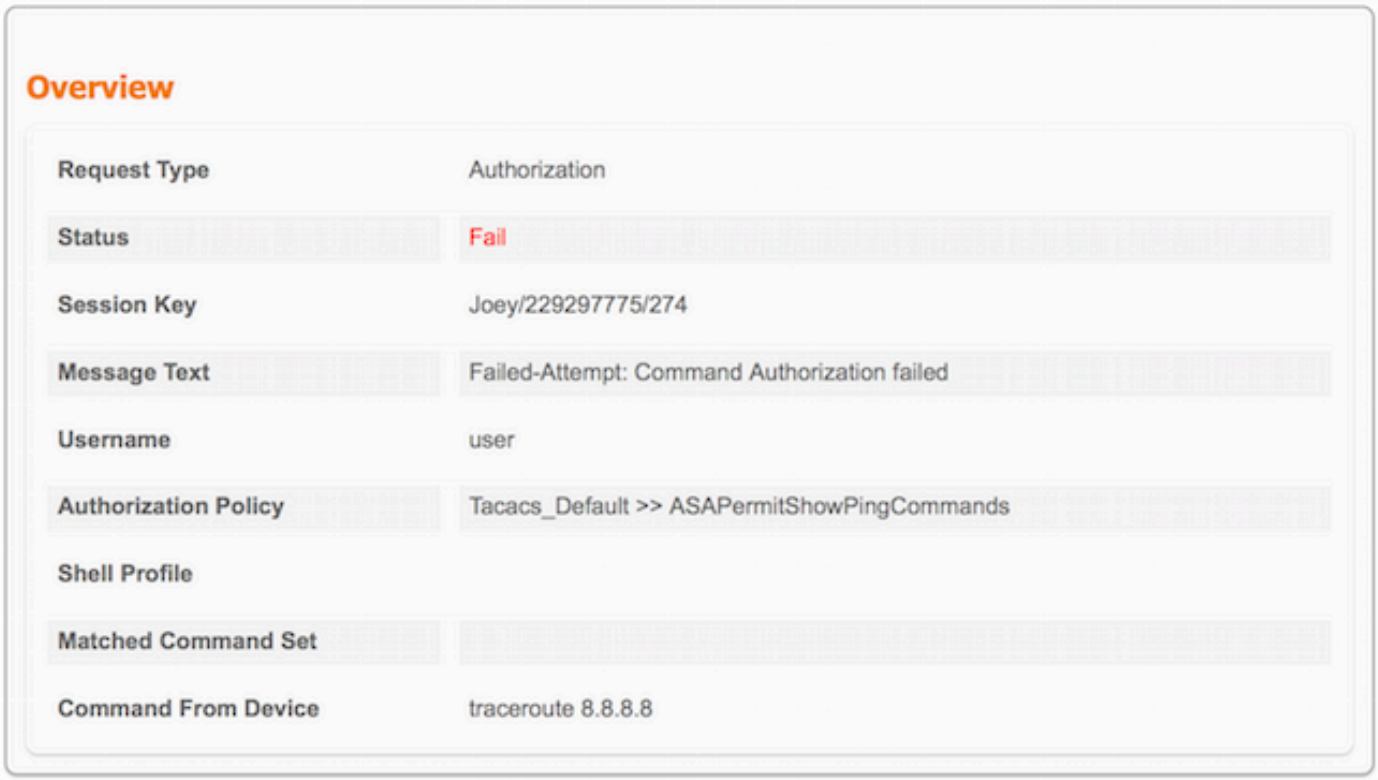
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

ISE 2.0 Verificatie

1. Navigeer naar **bewerkingen > TACACS-loggen.** Zorg ervoor dat de hierboven aangehaalde pogingen zijn gezien.



2. Klik op de details van een van de rode rapporten, de mislukte opdracht die eerder is uitgevoerd, is zichtbaar.



Problemen oplossen

Fout: Poging mislukt: Opdrachtautorisatie mislukt

Controleer de eigenschappen SelectedCommisionSet om te controleren of de verwachte commantiesets door het autorisatiebeleid zijn geselecteerd

Gerelateerde informatie

Technische ondersteuning en documentatie – Cisco Systems

ISE 2.0 Releaseopmerkingen

ISE 2.0 hardwareinstallatiehandleiding

ISE 2.0 upgrade-gids

Handleiding ACS naar ISE-migratietool

ISE 200 Active Directory Integration Guide

ISE 2.0 Engine Administrator-gids