

Problemen oplossen met Catalyst 9000-reeks Eindpunten die geen DHCP-adres ontvangen wanneer omgeleid door ISE

Inhoud

uitgeven

Nadat verificatie is ingeschakeld met omleiding van Cisco Identity Services Engine (ISE) op een switch uit de Cisco Catalyst 9000-reeks, kunnen bekabelde eindpunten met tussenpozen geen IP-adressen verkrijgen via het Dynamic Host Configuration Protocol (DHCP). Er zijn geen problemen waargenomen bij switches uit de niet-Catalyst 9000-reeks die dezelfde configuraties gebruiken.

milieu

- Productreeks: Catalyst 9000 reeks
- Windows-computers met DHCP-acquisitiefouten
- Redirect Access Control List (ACL) op de Catalyst 9000 Series-switch ontkent DHCP-verkeer niet expliciet

resolutie

1. Voeg de volgende weigeringsinstructies toe aan de omleiding van ACL om DHCP-verkeer expliciet af te handelen:

```
UDP geen EQ-opstartbewerkingen weigeren
```

```
UDP geen EQ-bootpc weigeren
```

UDP elke EQ BootPC weigeren

2. Nadat u de ACL hebt gewijzigd, verifieert u opnieuw een apparaat dat eerder is gefaald om te controleren of het nu met succes een IP-adres via DHCP kan ophalen.

Oorzaak

De Catalyst 9000-serie switches verwerken pakketten anders dan oudere switch modellen wanneer authenticatie is ingeschakeld. De pakketverwerkingsvolgorde op Catalyst 9000-serie switches is als volgt:

1. Pakketten die overeenkomen met een ACE-regel (Access Control Entry) voor toegangscontrole worden naar de CPU gestuurd voor doorverwijzing naar de AAA-server.
2. Pakketten die overeenkomen met een ACE-weigeringsregel worden doorgestuurd via de switch.
3. Pakketten die niet overeenkomen met de ACE-regels worden verwerkt door de volgende downloadable access control list (DACL), en als er geen DACL bestaat, raken de pakketten de impliciete ACL en worden ze verwijderd.

Deze verwerkingsmethode verschilt van oudere switch-modellen die standaard ACL's gebruiken die standaard DHCP-verkeer toestaan en worden verwerkt voordat ACL's worden omgeleid. Catalyst 9000-reeksmodellen gebruiken deze standaard ACL's niet en vertrouwen in plaats daarvan volledig op de omleiding van ACL en DACL die op de sessie aanwezig is. De standaard ACL voor gesloten modus sessies op voorganger Catalyst switches volgt:

```
3750#ship-toegangslijsten Auth-Default-ACL
```

```
Uitgebreide IP-toegangslijst Auth-Default-ACL
```

```
10 Toestaan UDP Any Range Bootps 65347 Any Range Bootpc 65348 (22 wedstrijden)
```

```
20 Toestaan UDP elke range bootps 65347 (12 wedstrijden)
```

```
30 IP-adressen weigeren
```

Verwante inhoud

- [Standaard ACL's voor 802.1X-verificatie](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.