

Solucionar problemas de pontos de extremidade do Catalyst 9000 Series que não recebem endereço DHCP quando redirecionados pelo ISE

Contents

Problema

Após habilitar a autenticação usando o redirecionamento do Cisco Identity Services Engine (ISE) em um switch Cisco Catalyst 9000 Series, os pontos finais com fio não conseguem obter endereços IP por meio do Dynamic Host Configuration Protocol (DHCP). Nenhum problema é observado em switches não Catalyst 9000 Series usando as mesmas configurações.

Ambiente

- Família de produtos: Catalyst 9000 Series
- Computadores Windows com falhas de aquisição de DHCP
- A ACL (Access Control List, lista de controle de acesso) redirecionada no switch Catalyst 9000 Series não nega explicitamente o tráfego DHCP

Resolução

1. Adicione as seguintes instruções deny à ACL de redirecionamento para tratar explicitamente o tráfego DHCP:

```
deny udp any eq bootps any
```

```
deny udp any any eq bootp
```

```
deny udp any eq bootpc any
```

2. Depois de modificar a ACL, autentique novamente um dispositivo que anteriormente estava falhando para verificar se agora pode recuperar com êxito um endereço IP através do DHCP.

Causa

Os Catalyst 9000 Series Switches processam pacotes de forma diferente dos modelos de switch mais antigos quando a autenticação é habilitada. A ordem de processamento de pacotes nos Catalyst 9000 Series Switches é a seguinte:

1. Os pacotes que correspondem a uma regra de entrada de controle de acesso (ACE) de permissão são enviados à CPU para redirecionamento ao servidor AAA.
2. Os pacotes que correspondem a uma regra de negação de entrada são encaminhados através do switch.
3. Os pacotes que não corresponderem às regras ACE de permissão ou de negação serão processados pela próxima lista de controle de acesso para download (DACL) e, se não houver nenhuma DACL, os pacotes chegarão à ACL de negação implícita e serão descartados.

Este método de processamento difere de modelos de switch mais antigos que usam ACLs padrão que permitem o tráfego DHCP por padrão e são processados antes de redirecionar ACLs. Os modelos da série Catalyst 9000 não usam essas ACLs padrão e, em vez disso, dependem inteiramente da ACL e da DACL de redirecionamento no lugar na sessão. A ACL padrão para sessões de modo fechado em switches Catalyst predecessores segue:

```
3750#sh ip access-lists Auth-Default-ACL
```

Lista de acesso IP estendida Auth-Default-ACL

```
10 permit udp any range bootps 65347 any range bootpc 65348 (22 correspondências)
```

```
20 permit udp any any range bootps 65347 (12 correspondências)
```

```
30 deny ip any any
```

Conteúdo relacionado

- [ACLs padrão para autenticação 802.1X](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.