Fehlerbehebung bei Endgeräten der Catalyst Serie 9000, die keine DHCP-Adresse erhalten, wenn sie von ISE umgeleitet werden

Inhalt

Problem

Nach der Aktivierung der Authentifizierung mithilfe der Umleitung von der Cisco Identity Services Engine (ISE) auf einem Switch der Cisco Catalyst Serie 9000 können kabelgebundene Endpunkte gelegentlich keine IP-Adressen über das Dynamic Host Configuration Protocol (DHCP) abrufen. Bei Switches, die nicht zu den Catalyst Switches der Serie 9000 gehören, wurden keine Probleme bei Verwendung derselben Konfigurationen festgestellt.

Umwelt

- Produktfamilie: Catalyst Serie 9000
- Windows-Computer mit DHCP-Erfassungsfehlern
- Die Umleitungszugriffskontrollliste (Redirect Access Control List, ACL) auf dem Catalyst Switch der Serie 9000 verweigert nicht explizit den DHCP-Datenverkehr.

Auflösung

1. Fügen Sie der Umleitungszugriffskontrollliste die folgenden deny-Anweisungen hinzu, um den DHCP-Datenverkehr explizit zu behandeln:

```
deny udp any eq boott any
```

```
deny udp any eq bootpc

deny udp any eq bootpc any
```

2. Nachdem Sie die ACL geändert haben, authentifizieren Sie ein zuvor ausgefallenes Gerät erneut, um sicherzustellen, dass es nun erfolgreich eine IP-Adresse über DHCP abrufen kann.

Ursache

Die Catalyst Switches der Serie 9000 verarbeiten Pakete anders als ältere Switch-Modelle, wenn die Authentifizierung aktiviert ist. Die Paketverarbeitungsreihenfolge für Catalyst Switches der Serie 9000 ist wie folgt:

1. Pakete, die einer ACE-Regel (permit access control entry) entsprechen, werden zur Umleitung an den AAA-Server an die CPU gesendet.

2. Pakete, die einer deny-ACE-Regel entsprechen, werden über den Switch weitergeleitet.

3. Pakete, die weder mit Zulassen- noch mit Ablehnungs-ACE-Regeln übereinstimmen, werden von der nächsten herunterladbaren Zugriffskontrollliste (DACL) verarbeitet. Wenn keine DACL vorhanden ist, werden Pakete von der implizit-deny-ACL verarbeitet und verworfen.

Diese Verarbeitungsmethode unterscheidet sich von älteren Switch-Modellen, die Standard-ACLs verwenden, die standardmäßig DHCP-Datenverkehr zulassen und vor Umleitungs-ACLs verarbeitet werden. Catalyst 9000-Modelle verwenden diese Standard-ACLs nicht und verlassen sich stattdessen vollständig auf die Umleitungs-ACL und DACL, die in der Sitzung vorhanden sind. Die Standard-ACL für geschlossene Modussitzungen auf Vorgänger-Catalyst-Switches sieht folgendermaßen aus:

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

Erweiterte IP-Zugriffsliste Auth-Default-ACL

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

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

```
30 deny ip any
```

Verwandte Inhalte

- Standard-ACLs für die 802.1X-Authentifizierung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.