排除Catalyst 9000系列終端在ISE重定向時無法接收DHCP地址的問題

目錄

問題

在Cisco Catalyst 9000系列交換機上啟用使用來自思科身份服務引擎(ISE)的重定向的身份驗證後，有線終端間歇性地無法通過動態主機配置協定(DHCP)獲取IP地址。在使用相同配置的非Catalyst 9000系列交換機上未發現任何問題。

環境

- 產品系列：Catalyst 9000系列
- 發生DHCP獲取失敗的Windows電腦
- Catalyst 9000系列交換器上的重新導向存取控制清單(ACL)不會明確拒絕DHCP流量

解析

1.將以下deny語句新增到重定向ACL以顯式處理DHCP流量：

```
deny udp any eq bootps any

deny udp any any eq bootpc

deny udp any eq bootpc any
```

2.修改ACL後，重新驗證以前出現故障的裝置，以驗證它現在是否可以通過DHCP成功檢索IP地址。

原因

啟用身份驗證時，Catalyst 9000系列交換機處理資料包的方式與舊交換機型號不同。Catalyst 9000系列交換機上的資料包處理順序如下：

1.將符合允許訪問控制條目(ACE)規則的資料包傳送到CPU以重定向到AAA伺服器。

2.通過交換機轉發與拒絕ACE規則匹配的資料包。

3.與permit和deny ACE規則均不匹配的資料包由下一個可下載訪問控制清單(DACL)處理，如果沒有DACL，則資料包將命中implicit-deny ACL並被丟棄。

此處理方法與使用預設ACL的舊式交換機型號不同，這些交換機型號預設允許DHCP流量，並且在重新導向ACL之前會對其進行處理。Catalyst 9000系列型號不使用這些預設ACL，而是完全依賴於會話上使用的重新導向ACL和DACL。前身Catalyst交換機上關閉模式會話的預設ACL如下：

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

延伸型IP存取清單驗證 — 預設型ACL

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

    20 permit udp any any range bootps 65347（12個匹配）

    30 deny ip any any
```

相關內容

- 用於802.1X身份驗證的預設ACL
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。