# Nexus 7000 ACL捕獲/VACL支援和限制常見問題

## 目錄



## 簡介

本檔案介紹存取控制清單(ACL)擷取功能，此功能是用來選擇性監控介面或VLAN上的流量。為ACL規則啟用capture選項時，會根據指定的操作轉發或丟棄與此規則匹配的資料包，並且還可能會將其複製到備用目標埠以進行進一步分析。

## 問： ACL捕獲的使用情形是什麼？

**A.此**功能類似Catalyst 6000系列交換器平台支援的VLAN存取控制清單(VACL)擷取功能。您可以設定ACL擷取，以選擇性地監控介面或VLAN上的流量。為ACL規則啟用capture選項時，會根據指定的permit或deny操作轉發或丟棄與此規則匹配的資料包，並且還可能將其複製到備用目標埠以進行進一步分析。

## 問：在Nexus 7000交換機上可以配置多少個ACL捕獲會話？

**A.在**系統中的任意指定時間，只能跨虛擬裝置環境(VDC)啟用一個ACL捕獲會話。 ACL三重內容可定址儲存器(TCAM)在VACL中可具有儘可能多的應用控制引擎(ACE)。

## 問： M1模組是否支援ACL捕獲？

**A.**是。Cisco NX-OS版本5.2(1)及更高版本支援M1模組上的ACL捕獲。

## 問： M2模組是否支援ACL捕獲？

**A.**是。Cisco NX-OS版本6.1(1)及更高版本支援M2模組上的ACL捕獲。

## 問：F1模組是否支援ACL捕獲？

**A.** F1系列模組不支援ACL捕獲。

## 問：F2模組是否支援ACL捕獲？

**答：**F2系列模組目前不支援ACL捕獲，但可能會在規劃圖中提供此功能。請諮詢業務部門(BU)確認。

## 問：ACL捕獲可以應用到哪些介面和方向？

**A.可**以應用帶捕獲選項的ACL規則：

- 在VLAN上
- 在所有介面的輸入方向上
- 在所有第3層介面上處於輸出方向

## 問：ACL捕獲功能是否存在任何明顯的限制？

**是的**。ACL擷取功能有一些限制，如下所示：

- ACL擷取是硬體輔助功能，管理介面或來自監督器的控制封包不支援。此外，SNMP社群ACL和vty ACL等軟體ACL也不支援此功能。
- 不支援將埠通道和Supervisor帶內埠作為ACL捕獲的目標。
- ACL捕獲會話目標介面不支援入口轉發和入口MAC學習。如果目的地介面已使用以下選項設定，監控器會保持ACL擷取作業階段關閉。使用**show monitor session all**命令以確定是否已啟用輸入轉送和MAC學習。
- 封包的來源連線埠和ACL擷取目的地連線埠不能是同一封包復寫ASIC的一部分。如果兩個連線埠屬於同一個ASIC，則不會擷取封包。**show monitor session**命令會列出與ACL擷取目的地連線埠連線到同一ASIC的所有連線埠。
- 如果在輸入**hardware access-list capture**命令之前配置ACL捕獲監控器會話，則必須關閉監控器會話並將其恢復正常才能啟動會話。
- 啟用ACL捕獲後，將禁用記錄所有VDC的ACL並使用速率限制器的功能。

## 問：是否可執行ACL捕獲，使特定流量流出目標介面X，特定流量流出目標介面Y，而其他流量流出目標介面Z?

**答：**否。目標只能是使用**hardware access**-list capture命**令配置的一個接**口。

## 問：是否將ACL捕獲應用到多個源VLAN?

**A.**是。一個VLAN清單中可以指定多個VLAN。例如：

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action forward
  statistics per-entry
  vlan filter acl-vlan-first vlan-list 1,2,3
```

## 問：在Nexus 7010上可以配置多少個活動L2 VACL?

**A.** 對於沒有XL線卡的裝置，支援的最大IP ACL條目數是64,000，而對於有XL線卡的裝置，則是128,000。

## 問： VACL捕獲如何處理路由流量？

**A.重**寫後會發生VACL捕獲，因此進入VLAN X和退出VLAN Y的幀會被捕獲到VLAN Y中。

## 問：機箱中混合使用M1和M2卡是否會影響VACL的使用？

**A.**機箱中混合使用M1和M2卡不應對VACL的使用產生任何影響。

## 問：Nexus 7000上的ACL捕獲功能有哪些配置示例？

**答：**ACL捕獲准則可在Cisco Nexus 7000系列NX-OS安全配置指南6.x版中檢視。

以下示例展示如何在預設VDC中啟用ACL捕獲並為ACL捕獲資料包配置目標：

```
hardware access-list capture
    monitor session 1 type acl-capture
    destination interface ethernet 2/1
    no shut
    exit
    show ip access-lists capture session 1
```

以下範例顯示如何為ACL的ACE啟用捕獲作業階段，然後將ACL套用到介面：

```
ip access-list acl1
      permit tcp any any capture session 1
      exit
      interface ethernet 1/11
      ip access-group acl1 in
      no shut
      show running-config aclmgr
```

以下範例顯示如何對具有擷取作業階段ACE的ACL套用到VLAN:

```
vlan access-map acl-vlan-first
      match ip address acl-ipv4-first
      match mac address acl-mac-first
      action foward
      statistics per-entry
      vlan filter acl-vlan-first vlan-list 1
      show running-config vlan 1
```

以下範例顯示如何為整個ACL啟用擷取作業階段，然後將ACL套用到介面：

```
ip access-list acl2
      capture session 2
      exit
      interface ethernet 7/1
      ip access-group acl1 in
      no shut
      show running-config aclmg
```

# 相關資訊

- 技術支援與文件 - Cisco Systems