Nexus 7000 ACL捕获/VACL支持和限制常见问题

目录

[简介](#)
[问：ACL捕获的使用案例是什么？](#)
[问：Nexus 7000交换机上可以配置多少个ACL捕获会话？](#)
[问：M1模块是否支持ACL捕获？](#)
[问：M2模块是否支持ACL捕获？](#)
[问：F1模块是否支持ACL捕获？](#)
[问：F2模块是否支持ACL捕获？](#)
[问：ACL捕获可应用于哪些接口和方向？](#)
[问：ACL捕获功能是否存在显着限制？](#)
[问：您能否执行ACL捕获，并让某些流量从目标接口X流出，某些流量从目标接口Y流出，而其他流量从目标接口Z流出？](#)
[问：您能否将ACL捕获应用于多个源VLAN?](#)
[问：在Nexus 7010上可以配置多少个活动L2 VACL?](#)
[问：VACL捕获如何处理路由流量？](#)
[问：机箱中M1和M2卡的混合是否影响VACL的使用？](#)
[问：Nexus 7000上ACL捕获功能的一些配置示例是什么？](#)
[相关信息](#)

简介

本文档介绍访问控制列表(ACL)捕获功能，该功能用于有选择地监控接口或VLAN上的流量。为ACL规则启用捕获选项时，匹配此规则的数据包会根据指定操作被转发或丢弃，并且可能会复制到备用目标端口以供进一步分析。

问：ACL捕获的使用案例是什么？

答：此功能类似于Catalyst 6000系列交换机平台上支持的VLAN访问控制列表(VACL)捕获功能。您可以配置ACL捕获，以选择性地监控接口或VLAN上的流量。为ACL规则启用捕获选项时，匹配此规则的数据包会根据指定的允许或拒绝操作被转发或丢弃，并且可能被复制到备用目标端口进行进一步分析。

问：Nexus 7000交换机上可以配置多少个ACL捕获会话？

答：在系统中跨虚拟设备环境(VDC)的任意给定时间，只能有一个ACL捕获会话处于活动状态。ACL三态内容可寻址存储器(TCAM)在VACL中可以拥有尽可能多的应用控制引擎(ACE)。

问：M1模块是否支持ACL捕获？

是的。Cisco NX-OS版本5.2(1)及更高版本支持M1模块上的ACL捕获。

问：M2模块是否支持ACL捕获？

是的。Cisco NX-OS版本6.1(1)及更高版本支持M2模块上的ACL捕获。

问：F1模块是否支持ACL捕获？

答：F1系列模块不支持ACL捕获。

问：F2模块是否支持ACL捕获？

答：F2系列模块目前不支持ACL捕获，但这可能在规划图中。请咨询业务部(BU)确认。

问：ACL捕获可应用于哪些接口和方向？

A.可以应用带捕获选项的ACL规则：

- 在VLAN上
- 在所有接口的入口方向
- 在所有第3层接口的出口方向

问：ACL捕获功能是否存在显着限制？

是的。ACL捕获功能的一些限制包括：

- ACL捕获是硬件辅助功能，管理接口或管理引擎中生成的控制数据包不支持该功能。软件ACL（如SNMP社区ACL和vty ACL）也不支持它。
- 不支持将端口通道和管理引擎带内端口作为ACL捕获的目标。
- ACL捕获会话目标接口不支持入口转发和入口MAC学习。如果为目标接口配置了这些选项，监控器会保持ACL捕获会话关闭。使用show monitor session **all命令确**定是否启用了入口转发和MAC学习。
- 数据包的源端口和ACL捕获目标端口不能属于同一数据包复制ASIC。如果两个端口属于同一ASIC，则不会捕获数据包。**show monitor session**命令列出了与ACL捕获目标端口连接到同一ASIC的所有端口。
- 如果在输入**hardware access-list capture**命令之前配置ACL捕获监控会话，则必须关闭监控会话并将其重新打开以启动会话。
- 启用ACL捕获后，将禁用记录所有VDC的ACL并使用速率限制器的功能。

问：您能否执行ACL捕获，并让某些流量从目标接口X流出，某些流量从目标接口Y流出，而其他流量从目标接口Z流出？

答：不。目标只能是使用hardware access-list capture命令**配置的**一个接口。

问：您能否将ACL捕获应用于多个源VLAN?

是的。可以在VLAN列表中指定多个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
```

问：在Nexus 7010上可以配置多少个活动L2 VACL?

A. 没有XL线卡的设备支持的最大IP ACL条目数为64,000，没有XL线卡的设备支持最大IP ACL条目数为128,000。

问：VACL捕获如何处理路由流量？

答：VACL捕获发生在重写之后，因此进入VLAN X并退出VLAN Y的帧会捕获在VLAN Y中。

问：机箱中M1和M2卡的混合是否影响VACL的使用？

答：机箱中M1和M2卡的混合不应对VACL的使用产生任何影响。

问：Nexus 7000上ACL捕获功能的一些配置示例是什么？

答：ACL捕获指南可在Cisco Nexus 7000系列NX-OS安[全配置指南6.x版中查看](#)。

本示例展示如何在默认VDC中启用ACL捕获并配置ACL捕获数据包的目标：

```
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
```

此示例显示如何为ACL的ACE启用捕获会话，然后将ACL应用到接口：

```
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
```

本示例展示如何将带有捕获会话ACE的ACL应用到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
```

此示例显示如何为整个ACL启用捕获会话，然后将ACL应用到接口：

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

相关信息

- 技术支持和文档 - Cisco Systems