

# Preguntas frecuentes sobre Limitaciones y captura de ACL de Nexus 7000

## Contenido

### [Introducción](#)

[P. ¿Cuál es el caso de uso de la captura ACL?](#)

[P. ¿Cuántas sesiones de captura ACL se pueden configurar en un switch Nexus 7000?](#)

[P. ¿Los módulos M1 soportan la captura ACL?](#)

[P. ¿Los módulos M2 soportan la captura ACL?](#)

[P. ¿Los módulos F1 soportan la captura ACL?](#)

[P. ¿Los módulos F2 soportan la captura ACL?](#)

[P. ¿En qué interfaces y direcciones se puede aplicar una captura ACL?](#)

[P. ¿Hay alguna limitación notable con la función de captura de ACL?](#)

[P. ¿Puede realizar una captura ACL y hacer que cierto tráfico salga de la interfaz de destino X, que cierto tráfico salga de la interfaz de destino Y y que otro tráfico salga de la interfaz de destino Z?](#)

[P. ¿Se puede aplicar la captura ACL a más de una VLAN de origen única?](#)

[P. ¿Cuántas VACL L2 activas se pueden configurar en un Nexus 7010?](#)

[P. ¿Cómo funciona la captura de VACL para el tráfico ruteado?](#)

[P. ¿Una mezcla de tarjetas M1 y M2 en el chasis afecta al uso de VACL?](#)

[P. ¿Cuáles son algunas configuraciones de ejemplo para la función de captura de ACL en Nexus 7000?](#)

### [Información Relacionada](#)

## Introducción

Este documento describe la función de captura de la Lista de control de acceso (ACL), que se utiliza para supervisar selectivamente el tráfico en una interfaz o VLAN. Cuando habilita la opción de captura para una regla ACL, los paquetes que coinciden con esta regla se reenvían o se descartan según la acción especificada y también se pueden copiar a un puerto de destino alternativo para un análisis adicional.

## P. ¿Cuál es el caso de uso de la captura ACL?

A. Esta función es análoga a la función de captura de VLAN Access Control List (VACL) admitida en las plataformas de switches Catalyst serie 6000. Puede configurar una captura ACL para monitorear selectivamente el tráfico en una interfaz o VLAN. Cuando habilita la opción de captura para una regla ACL, los paquetes que coinciden con esta regla se reenvían o se descartan según la acción especificada permit o deny y también se pueden copiar a un puerto de destino alternativo para un análisis adicional.

## **P. ¿Cuántas sesiones de captura ACL se pueden configurar en un switch Nexus 7000?**

A. Sólo una sesión de captura de ACL puede estar activa en un momento dado del sistema a través de Virtual Device Contexts (VDC). La memoria direccionable de contenido ternario (TCAM) de ACL puede tener tantos motores de control de aplicaciones (ACE) en la VACL como sea posible.

## **P. ¿Los módulos M1 soportan la captura ACL?**

A. Yes. La captura de ACL en los módulos M1 es compatible con Cisco NX-OS versión 5.2(1) y posteriores.

## **P. ¿Los módulos M2 soportan la captura ACL?**

A. Yes. La captura de ACL en los módulos M2 es compatible con Cisco NX-OS versión 6.1(1) y posteriores.

## **P. ¿Los módulos F1 soportan la captura ACL?**

A. Los módulos de la serie F1 no admiten captura ACL.

## **P. ¿Los módulos F2 soportan la captura ACL?**

A. Los módulos de la serie F2 no admiten captura ACL hasta ahora, pero esto puede estar en la hoja de ruta. Consulte la unidad empresarial (BU) para confirmar.

## **P. ¿En qué interfaces y direcciones se puede aplicar una captura ACL?**

A. Se puede aplicar una regla ACL con la opción de captura:

- En una VLAN
- En la dirección de ingreso en todas las interfaces
- En la dirección de salida en todas las interfaces de Capa 3

## **P. ¿Hay alguna limitación notable con la función de captura de ACL?**

A. Yes. Algunas limitaciones con la función de captura ACL son:

- Una captura ACL es una función asistida por hardware y no se soporta para la interfaz de administración o para los paquetes de control que se originan en el supervisor. Tampoco es compatible con ACL de software como ACL de comunidad SNMP y ACL de vty.
- Los canales de puerto y los puertos en banda del supervisor no se soportan como destino para la captura ACL.
- Las interfaces de destino de sesión de captura de ACL no admiten el reenvío de ingreso ni el aprendizaje de MAC de ingreso. Si se configura una interfaz de destino con estas opciones, el monitor mantiene la sesión de captura ACL inactiva. Utilice el comando **show monitor session all** para determinar si el reenvío de ingreso y el aprendizaje de MAC están habilitados.
- El puerto de origen del paquete y el puerto de destino de captura ACL no pueden formar parte del mismo ASIC de replicación de paquetes. Si ambos puertos pertenecen al mismo ASIC, el paquete no se captura. El comando **show monitor session** enumera todos los puertos que están conectados al mismo ASIC que el puerto de destino de captura ACL.
- Si configura una sesión de monitor de captura de ACL antes de ingresar el comando **hardware access-list capture**, debe apagar la sesión de monitor y volver a iniciarla para iniciar la sesión.
- Cuando se habilita la captura de ACL, se inhabilita la capacidad de registrar ACL para todos los VDC y utilizar el limitador de velocidad.

**P. ¿Puede realizar una captura ACL y hacer que cierto tráfico salga de la interfaz de destino X, que cierto tráfico salga de la interfaz de destino Y y que otro tráfico salga de la interfaz de destino Z?**

A. No. El destino sólo puede ser una interfaz configurada con el comando **hardware access-list capture**.

**P. ¿Se puede aplicar la captura ACL a más de una VLAN de origen única?**

A. Yes. Se pueden especificar varias VLAN en una lista de VLAN. Por ejemplo:

```
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
```

**P. ¿Cuántas VACL L2 activas se pueden configurar en un Nexus**

## 7010?

A. El número máximo de entradas de ACL IP admitidas es de 64 000 para dispositivos sin tarjeta de línea XL y 128 000 para dispositivos con tarjeta de línea XL.

### P. ¿Cómo funciona la captura de VACL para el tráfico ruteado?

A. La captura de VACL ocurre después de una reescritura, por lo que las tramas que ingresan a VLAN X y egresan VLAN Y se capturan en VLAN Y.

### P. ¿Una mezcla de tarjetas M1 y M2 en el chasis afecta al uso de VACL?

A. Una combinación de tarjetas M1 y M2 en el chasis no debería tener ningún impacto en el uso de VACL.

### P. ¿Cuáles son algunas configuraciones de ejemplo para la función de captura de ACL en Nexus 7000?

A. Las pautas de captura de ACL se pueden ver en la [Guía de Configuración de Seguridad de Cisco Nexus 7000 Series NX-OS, Versión 6.x](#).

Este ejemplo muestra cómo habilitar una captura ACL en el VDC predeterminado y configurar un destino para los paquetes de captura ACL:

```
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
```

Este ejemplo muestra cómo habilitar una sesión de captura para las ACE de una ACL y luego aplicar la ACL a una interfaz:

```
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
```

Este ejemplo muestra cómo aplicar una ACL con ACE de sesión de captura a una VLAN:

```
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
show running-config vlan 1
```

Este ejemplo muestra cómo habilitar una sesión de captura para toda la ACL y luego aplicar la ACL a una interfaz:

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

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)