# Exemplo de captura de ACL do switch Nexus 7000 Series

## Contents



## Introduction

A captura da ACL (Access Control List, lista de controle de acesso) permite capturar seletivamente o tráfego em uma interface ou na VLAN (virtual local area network, rede de área local virtual) Quando você habilita a opção de captura para uma regra de ACL, os pacotes correspondentes a essa regra são encaminhados ou descartados com base na ação de permissão ou negação especificada e também podem ser copiados para uma porta de destino alternativa para análise posterior. Uma regra de ACL com a opção de captura pode ser aplicada:

1. Em uma VLAN,
2. Na direção de entrada em todas as interfaces,
3. Na direção de saída em todas as interfaces de Camada 3.

Esse recurso é suportado no Nexus 7000 NX-OS versão 5.2 e posterior. Este documento fornece um exemplo como um guia de referência rápida sobre como configurar este recurso.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Nexus 7000 com versão 5.2.x e posterior.
- Placa de linha M1 series.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

## Exemplo de configuração de ACL

Aqui está um exemplo de configuração da captura ACL aplicada a uma VLAN, também conhecida como captura de lista de controle de acesso de LAN virtual (VACL - Virtual LAN Access Control List). Dez snifers gigabit designados podem não ser viáveis para todos os cenários. A captura seletiva de tráfego pode ser muito útil em tais cenários, especialmente durante a solução de problemas quando os volumes de tráfego estão altos.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

Você também pode verificar a programação TCAM (memória endereçável de conteúdo ternário) da lista de acesso. Esta saída é para a VLAN 500 para o Módulo 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------
```

```
Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

### Caveats

1. Apenas uma sessão de captura ACL pode estar ativa a qualquer momento no sistema em contextos de dispositivo virtual (VDCs).
2. Os módulos Nexus 7000 F1 Series não suportam captura de ACL.
3. Os módulos Nexus 7000 F2 Series não suportam atualmente a captura de ACL, mas isso pode estar no roteiro.
4. A captura de ACL nos módulos Nexus 7000 M2-Series é suportada com o Cisco NX-OS versão 6.1(1) e posterior.
5. A captura de ACL nos módulos Nexus 7000 M1-Series é suportada com o Cisco NX-OS versão 5.2(1) e posterior.
6. A captura de ACL não é compatível com o registro de ACL.  Portanto, se você tiver ACLs com uma palavra-chave **log**, elas não funcionarão depois que você tiver inserido globalmente a **captura da lista de acesso do hardware**.
7. Devido ao bug CSCug20139, o exemplo neste documento é documentado com uma **sessão de captura** por ACE em vez de por ACL, até que o bug seja resolvido.

## Informações Relacionadas

- Guia de configuração de segurança do Cisco Nexus 7000 Series NX-OS, versão 6.x, Exemplos de configuração para ACLs IP
- Suporte Técnico e Documentação - Cisco Systems