Foire aux questions de support et limites de la saisie VACL d'ACL de Nexus 7000

Contenu

Introduction

Ce document décrit la caractéristique de capture de liste de contrôle d'accès (ACL), qui est utilisée surveille sélectivement le trafic sur une interface ou un VLAN. Quand vous activez l'option de capture pour une règle d'ACL, des paquets qui apparient cette règle sont expédiés ou lâchés basé sur l'action spécifiée et pourraient également être copiés sur une destination port alternative pour l'analyse approfondie.

Q. Quel est le cas d'utilisation de la capture d'ACL ?

A. Cette caractéristique est analogue à la caractéristique de saisie de la liste de contrôle d'accès VLAN (VACL) prise en charge sur des Plateformes de commutateur de gamme Catalyst 6000. Vous pouvez configurer une capture d'ACL surveillez sélectivement le trafic sur une interface ou un VLAN. Quand vous activez l'option de capture pour une règle d'ACL, des paquets qui apparient cette règle sont expédiés ou lâchés basé sur l'autorisation spécifiée ou refusent l'action et

pourraient également être copiés sur une destination port alternative pour l'analyse approfondie.

Q. Combien de sessions de capture d'ACL peuvent être configurées sur un commutateur de Nexus 7000 ?

A. Seulement une session de capture d'ACL peut être en activité à un moment donné dans le système à travers des contextes de périphérique virtuel (VDCs). La mémoire associative ternaire d'ACL (TCAM) peut avoir autant d'engines de contrôle d'application (as) dans le VACL comme peut s'adapter.

Q. L'ACL de support des modules M1 les capturent-il ?

A. Oui. La saisie d'ACL sur les modules M1 est prise en charge dans la version 5.2(1) et ultérieures de Cisco NX-OS.

Q. L'ACL de support de modules m2 les capturent-il ?

A. Oui. La saisie d'ACL sur des modules m2 est prise en charge dans la version 6.1(1) et ultérieures de Cisco NX-OS.

Q. L'ACL de support des modules F1 les capturent-il ?

A. Les modules F1-Series ne prennent en charge pas la capture d'ACL.

Q. L'ACL de support des modules F2 les capturent-il ?

A. Les modules F2-Series ne prennent en charge pas la capture d'ACL dorénavant, mais ceci peut se produire dans la feuille de route. Consultez l'unité commerciale (BU) pour confirmer.

Q. Sur quelles interfaces et directions une capture d'ACL peut-elle être appliquée ?

A. Une règle d'ACL avec l'option de capture peut être appliquée :

- Sur un VLAN
- Dans la direction d'entrée sur toutes les interfaces
- Dans la direction de sortie sur toute la couche 3 relie

Q. Y a-t-il des limites notables avec la configuration de capture

d'ACL ?

R. Oui. Quelques limites avec la configuration de capture d'ACL sont :

- Une capture d'ACL est une caractéristique assistée par le matériel et n'est pas prise en charge pour l'interface de gestion ou pour les paquets de contrôle qui proviennent du superviseur. Il n'est pas également pris en charge pour le logiciel ACLs tel que la communauté ACLs et ACLs vty SNMP.
- Des Ports canalisés et les ports d'intrabande de superviseur ne sont pas pris en charge comme destination pour la capture d'ACL.
- Les interfaces de destination de session de capture d'ACL ne prennent en charge pas l'expédition d'entrée et apprendre de MAC d'entrée. Si une interface de destination est configurée avec ces options, le moniteur réduit la session de capture d'ACL. Utilisez le **show monitor session toute la** commande de déterminer si l'expédition d'entrée et apprendre de MAC sont activés.
- Le port de source du paquet et de la destination port de capture d'ACL ne peut pas faire partie de la même réplication ASIC de paquet. Si les deux ports appartiennent au même ASIC, le paquet n'est pas capturé. Les listes de commandes de **show monitor session** tous les ports qui sont reliés au même ASIC que la destination port de capture d'ACL.
- Si vous configurez une session de surveillance de capture d'ACL avant que vous sélectionniez la commande de **capture de liste d'accès de matériel**, vous devez arrêter la session de surveillance et l'apporter sauvegardez afin de commencer la session.
- Quand la capture d'ACL est activée, la capacité de se connecter l'ACL pour tout le VDCs et d'utiliser la borne de débit est désactivée.

Q. Est-ce que vous pouvez faites effectuer une capture d'ACL et sortir certain trafic l'interface X de destination, certain trafic sortent-ils l'interface Y de destination, et l'autre trafic sortent-ils l'interface Z de destination ?

A. Non. La destination peut seulement être une interface configurée avec l'ordre de **capture de liste d'accès de matériel**.

Q. Pouvez-vous avoir la capture d'ACL appliquée à plus qu'une source unique VLAN ?

A. Oui. Le multiple VLAN peut être spécifié dans une VLAN-liste. Exemple :

```
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
```

Q. Combien de L2 actifs VACLs peuvent être configurés sur un Nexus 7010 ?

R. Le nombre maximal de rubriques de liste ACL pris en charge IP est 64,000 pour des périphériques sans linecard XL et 128,000 pour des périphériques avec un linecard XL.

Q. Comment VACL capture-il le travail pour le trafic routé ?

A. La capture VACL se produit après qu'une réécriture, ainsi encadre VLAN ingressing X et VLAN egressing Y est capturé dans VLAN Y.

Q. Est-ce qu'combinaison de cartes M1 et m2 dans le châssis affecte l'utilisation de VACLs ?

A. Un mélange de cartes M1 et m2 dans le châssis ne devrait avoir aucune incidence sur l'utilisation de VACLs.

Q. Quelles sont quelques configurations d'échantillon pour la caractéristique de capture d'ACL sur le Nexus 7000 ?

Des instructions d'Acl-capture **A.** peuvent être visualisées dans le guide de configuration de Sécurité de la gamme 7000 NX-OS de Cisco Nexus, libèrent 6.x.

Cet exemple affiche comment activer une capture d'ACL dans le par défaut volts continu et configurer une destination pour des paquets de capture d'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
```

Cet exemple affiche comment activer une session de capture pour les as d'un ACL, et puis s'applique l'ACL à une interface :

```
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
```

Cet exemple affiche comment s'appliquer un ACL avec des as de session de capture à un 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
```

Cet exemple affiche comment activer une session de capture pour l'ACL entier et puis s'appliquer l'ACL à une interface :

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

Informations connexes

- Support et documentation techniques - Cisco Systems