Prise en charge et limitations des listes de contrôle d'accès Nexus 7000 - FAQ

Contenu

Introduction

Ce document décrit la fonction de capture de liste de contrôle d'accès (ACL), qui est utilisée afin de surveiller sélectivement le trafic sur une interface ou un VLAN. Lorsque vous activez l'option de capture pour une règle de liste de contrôle d'accès, les paquets qui correspondent à cette règle sont transférés ou abandonnés en fonction de l'action spécifiée et peuvent également être copiés vers un port de destination alternatif pour une analyse plus approfondie.

Q. Quel est le cas d’utilisation de la capture des listes de contrôle d’accès ?

A. Cette fonctionnalité est analogue à la fonctionnalité de capture VACL (VLAN Access Control List) prise en charge sur les plates-formes de commutation de la gamme Catalyst 6000. Vous pouvez configurer une capture de liste de contrôle d'accès afin de surveiller sélectivement le trafic

sur une interface ou un VLAN. Lorsque vous activez l'option de capture pour une règle de liste de contrôle d'accès, les paquets qui correspondent à cette règle sont transférés ou abandonnés en fonction de l'action d'autorisation ou de refus spécifiée et peuvent également être copiés vers un port de destination alternatif pour une analyse plus approfondie.

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

A. Une seule session de capture de liste de contrôle d'accès peut être active à un moment donné dans le système à travers les contextes de périphérique virtuel (VDC). La mémoire TCAM (Ternary Content Addressable Memory) de la liste de contrôle d'accès peut contenir autant de moteurs de contrôle d'application (ACE) que possible.

Q. Les modules M1 prennent-ils en charge la capture des listes de contrôle d’accès ?

A. Oui. La capture des listes de contrôle d'accès sur les modules M1 est prise en charge par Cisco NX-OS version 5.2(1) et ultérieure.

Q. Les modules M2 prennent-ils en charge la capture des listes de contrôle d’accès ?

A. Oui. La capture des listes de contrôle d'accès sur les modules M2 est prise en charge par Cisco NX-OS version 6.1(1) et ultérieure.

Q. Les modules F1 prennent-ils en charge la capture des listes de contrôle d’accès ?

A. Les modules de la gamme F1 ne prennent pas en charge la capture des listes de contrôle d’accès.

Q. Les modules F2 prennent-ils en charge la capture des listes de contrôle d’accès ?

A. Les modules de la gamme F2 ne prennent pas en charge la capture des listes de contrôle d'accès à ce jour, mais cela peut se trouver dans la feuille de route. Consultez l'unité commerciale (BU) pour confirmer.

Q. Sur quelles interfaces et directions une capture de liste de

contrôle d’accès peut-elle être appliquée ?

A. Une règle 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 toutes les interfaces de couche 3

Q. Existe-t-il des limitations notables avec la fonction de capture des listes de contrôle d’accès ?

A. Oui. La fonction de capture des listes de contrôle d’accès présente certaines limitations :

- Une capture de liste de contrôle d'accès est une fonction assistée par 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 non plus pris en charge pour les listes de contrôle d'accès logicielles, telles que les listes de contrôle d'accès de communauté SNMP et les listes de contrôle d'accès vty.
- Les canaux de port et les ports intrabande du superviseur ne sont pas pris en charge en tant que destination de la capture des listes de contrôle d’accès.
- Les interfaces de destination de la session de capture ACL ne prennent pas en charge le transfert d’entrée et l’apprentissage MAC d’entrée. Si une interface de destination est configurée avec ces options, le moniteur maintient la session de capture de liste de contrôle d’accès hors service. Utilisez la commande **show monitor session all** pour déterminer si le transfert d'entrée et l'apprentissage MAC sont activés.
- Le port source du paquet et le port de destination de capture de liste de contrôle d'accès ne peuvent pas faire partie du même ASIC de réplication de paquets. Si les deux ports appartiennent au même ASIC, le paquet n'est pas capturé. La commande **show monitor session** répertorie tous les ports connectés au même ASIC que le port de destination de capture ACL.
- Si vous configurez une session de moniteur de capture ACL avant d'entrer la commande **hardware access-list capture**, vous devez arrêter la session de surveillance et la réactiver afin de démarrer la session.
- Lorsque la capture des listes de contrôle d'accès est activée, la possibilité d'enregistrer les listes de contrôle d'accès pour tous les VDC et d'utiliser le limiteur de débit est désactivée.

Q. Pouvez-vous effectuer une capture de liste de contrôle d’accès et faire sortir un certain trafic de l’interface de destination X, de l’interface de destination Y et de l’interface de destination Z ?

A. Non. La destination ne peut être qu'une seule interface configurée avec la commande **hardware access-list capture**.

Q. Pouvez-vous appliquer la capture ACL à plusieurs VLAN source ?

A. Oui. Plusieurs VLAN peuvent être spécifiés dans une liste de VLAN. 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 VACL de couche 2 actives peuvent être configurées sur un Nexus 7010 ?

A. Le nombre maximal d'entrées de liste de contrôle d'accès IP prises en charge est de 64 000 pour les périphériques sans carte de ligne XL et de 128 000 pour les périphériques avec carte de ligne XL.

Q. Comment la capture VACL fonctionne-t-elle pour le trafic routé ?

A. La capture VACL se produit après une réécriture, de sorte que les trames qui entrent dans VLAN X et en sortent VLAN Y sont capturées dans VLAN Y.

Q. Un mélange de cartes M1 et M2 dans le châssis a-t-il un impact sur l'utilisation des VACL ?

A. Un mélange de cartes M1 et M2 dans le châssis ne doit pas avoir d'impact sur l'utilisation des VACL.

Q. Quels sont les exemples de configuration de la fonction de capture des listes de contrôle d'accès sur Nexus 7000 ?

A. Les directives de capture des listes de contrôle d'accès sont affichées dans le Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 7000, version 6.x.

Cet exemple montre comment activer une capture ACL dans le VDC par défaut et configurer une destination pour les paquets de capture 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 montre comment activer une session de capture pour les ACE d'une liste de contrôle d'accès, puis appliquer la liste de contrôle d'accès 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 montre comment appliquer une liste de contrôle d'accès avec des entrées 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 montre comment activer une session de capture pour l'ensemble de la liste de contrôle d'accès, puis appliquer la liste de contrôle d'accès 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