Domande frequenti sull'acquisizione di ACL Nexus 7000/supporto e limitazioni per VACL

Sommario

Introduzione

In questo documento viene descritta la funzione di acquisizione Access Control List (ACL), che viene usata per monitorare in modo selettivo il traffico su un'interfaccia o su una VLAN. Quando si abilita l'opzione di acquisizione per una regola ACL, i pacchetti che soddisfano questa regola vengono inoltrati o eliminati in base all'azione specificata e possono essere copiati su una porta di destinazione alternativa per ulteriori analisi.

D. Qual è il caso di utilizzo dell'acquisizione degli ACL?

R. Questa funzione è analoga alla funzione di acquisizione VACL (VLAN Access Control List) supportata sulle piattaforme degli switch Catalyst serie 6000. È possibile configurare un'acquisizione ACL in modo da monitorare in modo selettivo il traffico su un'interfaccia o su una VLAN. Quando si abilita l'opzione di acquisizione per una regola ACL, i pacchetti che soddisfano questa regola vengono inoltrati o eliminati in base all'azione di autorizzazione o rifiuto specificata e possono essere copiati anche su una porta di destinazione alternativa per ulteriori analisi.

D. Quante sessioni di acquisizione ACL possono essere configurate su uno switch Nexus 7000?

R. Nel sistema può essere attiva una sola sessione di acquisizione ACL alla volta nei contesti dei dispositivi virtuali (VDC). Il TCAM (Ternary Content Addressable Memory) dell'ACL può contenere il numero massimo di Application Control Engine (ACE) nel VACL.

D. I moduli M1 supportano l'acquisizione degli ACL?

R. Sì. L'acquisizione degli ACL sui moduli M1 è supportata in Cisco NX-OS versione 5.2(1) e successive.

D. I moduli M2 supportano l'acquisizione degli ACL?

R. Sì. L'acquisizione degli ACL sui moduli M2 è supportata in Cisco NX-OS versione 6.1(1) e successive.

D. I moduli F1 supportano l'acquisizione ACL?

R. I moduli della serie F1 non supportano l'acquisizione di ACL.

D. I moduli F2 supportano l'acquisizione ACL?

R. I moduli della serie F2 non supportano l'acquisizione ACL al momento, ma questa operazione potrebbe essere prevista nel piano di sviluppo. Consulta l'Unità Commerciale (UO) per confermare.

D. Su quali interfacce e direzioni è possibile applicare un'acquisizione ACL?

R. È possibile applicare una regola ACL con l'opzione di acquisizione:

- Su una VLAN
- In direzione entrata su tutte le interfacce
- In direzione di uscita su tutte le interfacce di layer 3

D. Sono previste limitazioni di rilievo per la funzione di acquisizione degli ACL?

R. Sì. Di seguito sono riportate alcune limitazioni della funzione di acquisizione degli ACL:

- L'acquisizione ACL è una funzionalità assistita da hardware e non è supportata per l'interfaccia di gestione o per i pacchetti di controllo provenienti dal supervisor. Inoltre, non è supportato sugli ACL software come gli ACL della community SNMP e gli ACL vty.
- I canali delle porte e le porte in banda del supervisore non sono supportati come destinazione per l'acquisizione degli ACL.
- Le interfacce di destinazione delle sessioni di acquisizione ACL non supportano l'inoltro in entrata e l'apprendimento di indirizzi MAC in entrata. Se un'interfaccia di destinazione è configurata con queste opzioni, il monitoraggio mantiene inattiva la sessione di acquisizione ACL. Usare il comando **show monitor session all** per determinare se l'inoltro in entrata e l'apprendimento degli indirizzi MAC sono abilitati.
- La porta di origine del pacchetto e la porta di destinazione dell'acquisizione ACL non possono far parte dello stesso ASIC di replica dei pacchetti. Se entrambe le porte appartengono allo stesso ASIC, il pacchetto non viene acquisito. Il comando **show monitor session** elenca tutte le porte collegate allo stesso ASIC della porta di destinazione dell'acquisizione ACL.
- Se si configura una sessione di monitoraggio acquisizione ACL prima di immettere il comando **hardware access-list capture**, è necessario chiudere la sessione di monitoraggio e riavviarla per avviare la sessione.
- Quando l'acquisizione ACL è abilitata, la capacità di registrare ACL per tutti i VDC e di usare il limitatore di velocità è disabilitata.

D. È possibile acquisire un ACL e far uscire un determinato traffico dall'interfaccia di destinazione X, un determinato traffico dall'interfaccia di destinazione Y e altro traffico dall'interfaccia di destinazione Z?

R. No. La destinazione può essere una sola interfaccia configurata con il comando **hardware access-list capture**.

D. È possibile applicare l'acquisizione ACL a più di una VLAN di origine?

R. Sì. In un elenco VLAN è possibile specificare più VLAN. Ad esempio:

```
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
```

D. Quanti VACL L2 attivi possono essere configurati su Nexus

7010?

R. Il numero massimo di voci ACL IP supportate è 64.000 per i dispositivi senza scheda di linea XL e 128.000 per i dispositivi con scheda di linea XL.

D. Come funziona l'acquisizione VACL per il traffico indirizzato?

R. L'acquisizione del VACL si verifica dopo una riscrittura, quindi i frame in entrata nella VLAN X e in uscita dalla VLAN Y vengono acquisiti nella VLAN Y.

D. Una combinazione di schede M1 e M2 nello chassis influisce sull'utilizzo delle VACL?

R. Una combinazione di schede M1 e M2 nello chassis non dovrebbe avere alcun impatto sull'uso dei VACL.

D. Quali sono alcune configurazioni di esempio per la funzione di acquisizione ACL su Nexus 7000?

R. Le linee guida per l'acquisizione degli ACL sono disponibili nella guida alla configurazione della sicurezza di Cisco Nexus serie 7000 NX-OS, versione 6.x.

Nell'esempio viene mostrato come abilitare un'acquisizione ACL nel controller di dominio virtuale predefinito e configurare una destinazione per i pacchetti di acquisizione 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
```

Nell'esempio viene mostrato come abilitare una sessione di acquisizione per le voci ACE di un ACL, quindi applicare l'ACL a un'interfaccia:

```
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
```

Nell'esempio viene mostrato come applicare un ACL con ACE di sessione di acquisizione a una 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
```

Nell'esempio viene mostrato come abilitare una sessione di acquisizione per l'intero ACL e quindi applicare l'ACL a un'interfaccia:

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

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems