Häufig gestellte Fragen zur ACL-Erfassung/VACL für Nexus 7000 - Support und Einschränkungen

Inhalt

Einführung
F. Wie sieht der Anwendungsfall der ACL-Erfassung aus?
F. Wie viele ACL-Aufzeichnungssitzungen können auf einem Nexus 7000-Switch konfiguriert werden?
F. Unterstützen M1-Module die ACL-Erfassung?
F. Unterstützen M2-Module die ACL-Erfassung?
F. Unterstützen F1-Module die ACL-Erfassung?
F. Unterstützen F2-Module die ACL-Erfassung?
F. Auf welche Schnittstellen und Richtungen kann eine ACL-Erfassung angewendet werden?
F. Gibt es beträchtliche Einschränkungen bei der ACL-Erfassung?
F. Können Sie eine ACL-Erfassung durchführen und bestimmten Datenverkehr über die Zielschnittstelle X übertragen, bestimmten Datenverkehr über die Zielschnittstelle Y weitergeleitet und anderen Datenverkehr über die Zielschnittstelle Z geleitet werden?
F. Können Sie die ACL-Erfassung auf mehr als ein einzelnes Quell-VLAN anwenden?
F. Wie viele aktive L2-VACLs können auf einem Nexus 7010 konfiguriert werden?
F. Wie funktioniert die VACL-Erfassung für gerouteten Datenverkehr?
F. Wirkt sich eine Mischung aus M1- und M2-Karten im Chassis auf die Verwendung von VACLs aus?
F. Welche Beispielkonfigurationen gibt es für die ACL-Aufzeichnungsfunktion auf dem Nexus 7000?
Zugehörige Informationen

Einführung

In diesem Dokument wird die Funktion zur Erfassung von Zugriffskontrolllisten (ACL) beschrieben, mit der der Datenverkehr an einer Schnittstelle oder einem VLAN selektiv überwacht wird. Wenn Sie die Erfassungsoption für eine ACL-Regel aktivieren, werden Pakete, die dieser Regel entsprechen, basierend auf der angegebenen Aktion entweder weitergeleitet oder verworfen und zur weiteren Analyse auch in einen alternativen Zielport kopiert.

F. Wie sieht der Anwendungsfall der ACL-Erfassung aus?

Antwort: Diese Funktion entspricht der von Catalyst Switch-Plattformen der Serie 600 unterstützten Funktion zur Erfassung von VACLs (VLAN Access Control List). Sie können eine

ACL-Erfassung konfigurieren, um den Datenverkehr auf einer Schnittstelle oder einem VLAN selektiv zu überwachen. Wenn Sie die Erfassungsoption für eine ACL-Regel aktivieren, werden Pakete, die dieser Regel entsprechen, entweder auf der Grundlage der angegebenen Zulassen- oder Ablehnungsaktion weitergeleitet oder verworfen und zur weiteren Analyse auch in einen alternativen Zielport kopiert.

F. Wie viele ACL-Aufzeichnungssitzungen können auf einem Nexus 7000-Switch konfiguriert werden?

Antwort: Im System kann jeweils nur eine ACL-Aufzeichnungssitzung über Virtual Device Contexts (VDCs) hinweg aktiv sein. Der TCAM (ACL Ternary Content Addressable Memory) kann so viele ACEs (Application Control Engines) in der VACL enthalten, wie dies möglich ist.

F. Unterstützen M1-Module die ACL-Erfassung?

Antwort: Ja. Die ACL-Erfassung auf M1-Modulen wird in Cisco NX-OS Version 5.2(1) und höher unterstützt.

F. Unterstützen M2-Module die ACL-Erfassung?

Antwort: Ja. Die ACL-Erfassung auf M2-Modulen wird in Cisco NX-OS 6.1(1) und höher unterstützt.

F. Unterstützen F1-Module die ACL-Erfassung?

Antwort: Module der F1-Serie unterstützen keine ACL-Erfassung.

F. Unterstützen F2-Module die ACL-Erfassung?

Antwort: Die Module der F2-Serie unterstützen die ACL-Erfassung zum gegenwärtigen Zeitpunkt nicht, dies ist jedoch in der Roadmap vorgesehen. Weitere Informationen erhalten Sie vom Geschäftsbereich.

F. Auf welche Schnittstellen und Richtungen kann eine ACL-Erfassung angewendet werden?

Antwort: Eine ACL-Regel mit der Erfassungsoption kann angewendet werden:

- In einem VLAN
- In Eingangsrichtung an allen Schnittstellen
- Ausgangs- und Layer-3-Schnittstellen

F. Gibt es beträchtliche Einschränkungen bei der ACL-Erfassung?

Antwort: Ja. Die ACL-Aufzeichnungsfunktion weist u. a. folgende Einschränkungen auf:

- Eine ACL-Erfassung ist eine hardwareunterstützte Funktion und wird für die Verwaltungsschnittstelle oder für vom Supervisor stammende Steuerungspakete nicht unterstützt. Software-ACLs wie SNMP Community-ACLs und vty ACLs werden nicht unterstützt.
- Port-Channels und Supervisor-In-Band-Ports werden nicht als Ziel für die ACL-Erfassung unterstützt.
- Die Zielschnittstellen für die ACL-Erfassung unterstützen keine Eingangs-Forwarding und Eingangs-MAC Learning. Wenn eine Zielschnittstelle mit diesen Optionen konfiguriert ist, wird die ACL-Aufzeichnungssitzung vom Monitor unterbrochen. Verwenden Sie den Befehl **show monitor session all**, um festzustellen, ob die Eingangs-Weiterleitung und MAC Learning aktiviert sind.
- Der Quell-Port des Pakets und der Ziel-Port für die ACL-Erfassung können nicht Teil desselben ASIC für die Paketreplikation sein. Wenn beide Ports demselben ASIC angehören, wird das Paket nicht erfasst. Der Befehl **show monitor session** listet alle Ports auf, die mit demselben ASIC wie der Ziel-Port für die ACL-Erfassung verbunden sind.
- Wenn Sie eine ACL-Überwachungssitzung konfigurieren, bevor Sie den Befehl **zur Erfassung der Hardwarezugriffsliste** eingeben, müssen Sie die Überwachungssitzung herunterfahren und wieder aktivieren, um die Sitzung zu starten.
- Wenn die ACL-Erfassung aktiviert ist, ist die Möglichkeit zur Protokollierung der ACL für alle VDCs und zur Verwendung der Durchsatzbegrenzung deaktiviert.

F. Können Sie eine ACL-Erfassung durchführen und bestimmten Datenverkehr über die Zielschnittstelle X übertragen, bestimmten Datenverkehr über die Zielschnittstelle Y weitergeleitet und anderen Datenverkehr über die Zielschnittstelle Z geleitet werden?

Antwort: Nein. Beim Ziel kann es sich nur um eine Schnittstelle handeln, die mit dem Befehl **zur Erfassung der Hardwarezugriffslisten** konfiguriert wurde.

F. Können Sie die ACL-Erfassung auf mehr als ein einzelnes Quell-VLAN anwenden?

Antwort: Ja. Mehrere VLANs können in einer VLAN-Liste angegeben werden. Beispiel:

```
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
```

F. Wie viele aktive L2-VACLs können auf einem Nexus 7010 konfiguriert werden?

Antwort: Die maximale Anzahl unterstützter IP-ACL-Einträge beträgt 64.000 für Geräte ohne XL-Linecard und 128.000 für Geräte mit XL-Linecard.

F. Wie funktioniert die VACL-Erfassung für gerouteten Datenverkehr?

Antwort: Die VACL-Erfassung erfolgt nach einer Umschreibung, sodass Frames, die VLAN X und ausgehende VLAN Y enthalten, in VLAN Y erfasst werden.

F. Wirkt sich eine Mischung aus M1- und M2-Karten im Chassis auf die Verwendung von VACLs aus?

Antwort: Eine Kombination aus M1- und M2-Karten im Chassis sollte die Verwendung von VACLs nicht beeinträchtigen.

F. Welche Beispielkonfigurationen gibt es für die ACL-Aufzeichnungsfunktion auf dem Nexus 7000?

Antwort: Richtlinien zur ACL-Erfassung finden Sie im Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x.

Dieses Beispiel zeigt, wie eine ACL-Erfassung im Standard-VDC aktiviert und ein Ziel für ACL-Erfassungspakete konfiguriert wird:

```
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
```

In diesem Beispiel wird veranschaulicht, wie eine Erfassungssitzung für die ACEs einer Zugriffskontrollliste aktiviert und anschließend die Zugriffskontrollliste auf eine Schnittstelle angewendet wird:

```
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
```

Dieses Beispiel zeigt, wie eine ACL mit ACEs für die Aufzeichnungssitzung auf ein VLAN angewendet wird:

```
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
```

In diesem Beispiel wird veranschaulicht, wie eine Erfassungssitzung für die gesamte ACL aktiviert und anschließend die ACL auf eine Schnittstelle angewendet wird:

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

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems