Nexus 7000 の ACL キャプチャ/VACL のサポートと制限に関する FAQ

内容

概要

このドキュメントでは、インターフェイスまたは VLAN のトラフィックを選択的にモニタするために使用するアクセス コントロール リスト（ACL）キャプチャ機能について説明します。ACL ルールのキャプチャ オプションを有効にすると、このルールに一致したパケットは、指定されたアクションに基づいて転送またはドロップされます。また、さらに分析するために代替の宛先ポートにコピーされる可能性もあります。

Q. ACLキャプチャの使用例は何ですか。

A.この機能は、Catalyst 6000シリーズスイッチプラットフォームでサポートされているVLANアクセスコントロールリスト(VACL)キャプチャ機能に類似しています。インターフェイスまたは VLAN 上のトラフィックを選択的にモニタするために、ACL キャプチャを設定できます。ACL ルールのキャプチャ オプションを有効にすると、このルールに一致したパケットは、指定された permit または deny アクションに基づいて転送またはドロップされます。また、さらに分析するために代替の宛先ポートにコピーされる可能性もあります。

Q. Nexus 7000スイッチでは、いくつのACLキャプチャセッションを設定できますか。

A.仮想デバイス・コンテキスト(VDC)全体で、システム内の任意の時点でアクティブにできるACLキャプチャ・セッションは1つだけです。 ACL TCAM（Ternary Content Addressable Memory）には、容量いっぱいまで VACL のアプリケーション制御エンジン（ACE）を含めることができます。

Q. M1モジュールはACLキャプチャをサポートしていますか。

A.はい。M1 モジュールの ACL キャプチャは、Cisco NX-OS リリース 5.2(1) 以降でサポートされています。

Q. M2モジュールはACLキャプチャをサポートしていますか。

A.はい。M2 モジュールの ACL キャプチャは、Cisco NX-OS リリース 6.1(1) 以降でサポートされています。

Q. F1モジュールはACLキャプチャをサポートしていますか。

A. F1シリーズのモジュールでは、ACLキャプチャはサポートされていません。

Q. F2モジュールはACLキャプチャをサポートしていますか。

A. F2シリーズモジュールは、現時点ではACLキャプチャをサポートしていませんが、これはロードマップに含まれている可能性があります。営業部門（BU）にお問い合わせください。

Q. ACLキャプチャを適用できるインターフェイスと方向はどれですか。

A. captureオプションを含むACLルールを適用できます。

- VLAN 上で
- すべてのインターフェイス上の入力方向に
- すべてのレイヤ 3 インターフェイス上の出力方向に

Q. ACLキャプチャ機能に関する顕著な制限はありますか。

A.はい。ACL キャプチャ機能には次の制限があります。

- ACL キャプチャはハードウェアベース機能で、管理インターフェイスまたはスーパーバイザで発信される制御パケットではサポートされません。さらに、SNMP コミュニティ ACL および vty ACL などのソフトウェア ACL でもサポートされません。
- ポートチャネル インターフェイス、およびスーパーバイザ インバンド ポートは ACL キャプチャの宛先としてサポートされません。
- ACL キャプチャ セッションの宛先インターフェイスは、入力転送と入力の MAC の学習をサポートしません。宛先インターフェイスでこれらオプションが設定されている場合、モニタが ACL のキャプチャ セッションをダウン状態にし続けます。入力転送および MAC の学習が有効になっているかどうかを確認するには、**show monitor session all コマンドを使用します**。
- パケットの送信元ポートと ACL キャプチャの宛先ポートは、同じパケット複製 ASIC の一部であってはなりません。両方のポートが同じ ASIC に属する場合、パケットはキャプチャされません。**show monitor session コマンドにより、ACL キャプチャの宛先ポートとして同じ ASIC に接続するすべてのポートが表示されます。**
- **hardware access-list capture コマンドを入力する前に ACL キャプチャ モニタ セッションを設定する場合は、モニタ セッションをシャット ダウンし、再度起動して、セッションを開始する必要があります。**
- ACL 機能が有効な場合、すべての VDC の ACL を記録し、レート リミッタを使用することができなくなります。

Q. ACLキャプチャを実行して、特定のトラフィックを宛先インターフェイスXに、特定のトラフィックを宛先インターフェイスYに、他のトラフィックを宛先インターフェイスZに送信することはできますか。

A.いいえ。宛先は、hardware access-list captureコマンドで設定されたインターフェイスを1つだけ**使用できます**。

Q. ACLキャプチャを複数のソースVLANに適用できますか。

A.はい。複数の VLAN を VLAN リストに指定できます。以下に、いくつかの例を示します。

```
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. Nexus 7010で設定できるアクティブL2 VACLの数はいくつですか。

A. サポートされる IP ACL エントリの最大数は、XL ライン カードを使用しないデバイスで

64,000、XL ライン カードを使用するデバイスで 128,000 です。

Q. VACLキャプチャは、ルーティングされたトラフィックにどのように機能しますか。

A. VACLキャプチャは書き換え後に発生するため、VLAN Xに入ってVLAN Yに出力するフレームはVLAN Yでキャプチャされます。

Q.シャーシにM1カードとM2カードが混在していると、VACLの使用に影響しますか。

A.シャーシ内にM1カードとM2カードが混在しても、VACLの使用に影響はありません。

Q. Nexus 7000のACLキャプチャ機能の設定例を教えてください。

A. ACL キャプチャ ガイドラインについては、『Cisco Nexus 7000 シリーズ NX-OS セキュリティ コンフィギュレーション ガイド、リリース 6.x』を参照してください。

次に、デフォルト VDC で ACL キャプチャを有効にして、ACL キャプチャ パケットの宛先を設定する例を示します。

```
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
```

次に、ACL の ACE のキャプチャ セッションを有効にしてから、その ACL をインターフェイスに適用する例を示します。

```
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
```

次に、キャプチャ セッションの ACE を含む ACL を VLAN に適用する例を示します。

```
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
```

次に、ACL 全体のキャプチャ セッションを有効にしてから、その ACL をインターフェイスに適用する例を示します。

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

関連情報

- テクニカル サポートとドキュメント – Cisco Systems