# ACL ロギングに最適化された Nexus 7000 と 7700 シリーズ スイッチの設定例

## 目次



## 概要

このドキュメントでは、Cisco Nexus 7000 および 7700 シリーズ スイッチの最適化されたアクセス コントロール リスト（ACL）のロギング（OAL）を設定する方法について説明します。

## 前提条件

### 要件

このドキュメントで説明する設定を開始する前に、基本的な ACL を使用した Nexus の設定を理解しておくことをお勧めします。

### 使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco Nexus 7000 シリーズ スイッチ

- Cisco Nexus 7700 シリーズ スイッチ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

# 背景説明

ロギング対応 ACL により、ネットワークを通過する、またはネットワーク デバイスによって廃棄されたときのトラフィックを詳細に理解できます。 残念ながら、ACL ロギングは CPU 負荷が大きく、ネットワーク デバイスのその他の機能に悪影響を与える可能性があります。 CPU サイクルを短縮するために、Cisco Nexus 7000 シリーズ スイッチは OAL を使用します。

OAL を使用すると、ACL ロギングはハードウェアでサポートされます。 OAL では、ハードウェアのパケットを許可またはドロップして、スーパバイザに情報を送信するために最適化されたルーチンを使用し、ロギング メッセージを生成できるようにします。 たとえば、パケットがハードウェアで転送される際にそのパケットがロギングを有効にした ACL にヒットした場合、パケットのコピーがハードウェアで作成され、パケットは設定された時間間隔に従ってロギングのためスーパバイザにパントされます。

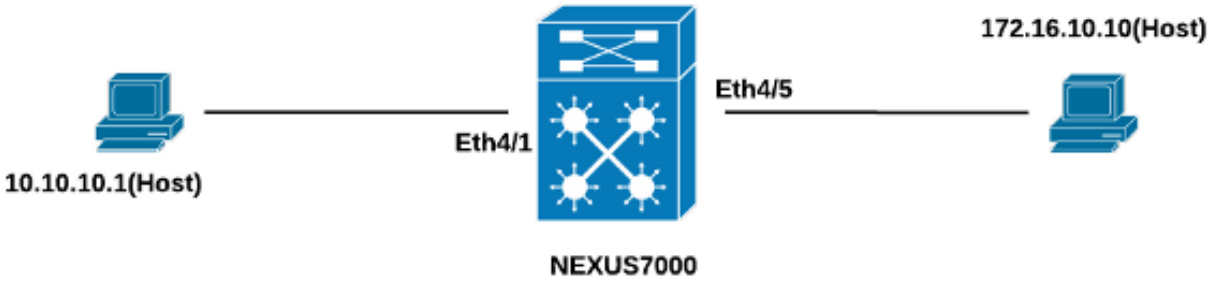
# 設定

この項では OAL を使用する Nexus スイッチを設定するために使用できる情報を提供します。

この項に記載する例では、IP アドレス 10.10.10.1 のホストが、トラフィックを IP アドレス 172.16.10.10 の別のホストに送信し、その際に ACL のロギングが設定された Nexus 7000 シリーズのインターフェイスを使用します。

## ネットワーク図

ホストと Nexus 7000 シリーズのスイッチの間の接続は、次のトポロジに従って発生します。




## 設定

OAL を使用するようにスイッチを設定するには、次の手順を実行します。

1. OAL を有効にするには、次のグローバル コマンドを設定します。

```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
logging ip access-list cache threshold 0
```

次に例を示します。

```
Nexus-7000# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. ロギングに次の設定を適用します。

```
Nexus-7000# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

次に例を示します。

```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level  5
Nexus-7000(config)# logging logfile acllog 5
```

3. ロギングを有効にするように ACL を設定します。 エントリは、次の例に示すように、**log キーワード**を有効にして設定する必要があります。

```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
Nexus-7000(config-acl)#
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
10 permit ip 10.10.10.1/32 172.16.10.10/32 log
20 deny ip any any log
Nexus-7000(config-acl)#
```

4. 前の手順で設定した ACL を必用なインターフェイスに適用します。

```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
Nexus-7000(config-if)#
Nexus-7000(config-if)# show run int ethernet 4/1
!Command: show running-config interface Ethernet4/1
!Time: Mon Jun 30 16:30:38 2014
version 6.2(6)
interface Ethernet4/1
 ip access-group test1 in
 ip access-group test1 out
 ip address 10.10.10.2/24
 no shutdown
Nexus-7000(config-if)#
```

# 確認

設定が適切に機能することを確認するために、この項に記載する情報を活用してください。

このドキュメントで使用されている例では、ping は IP アドレス 10.10.10.1 のホストから IP アドレス 172.16.10.1 のホストに向けて開始されます。 トラフィック フローを確認するには、CLI に **show logging ip access-list cache コマンド**を入力します。

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

300 秒ごとに口ギングを確認できますが、これはこれがデフォルトの間隔です。

```
Nexus-7000# show logging logfile
2014 Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog)
cleared by user
2014 Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on console0
2014 Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 2589
2014 Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 4561
```

# トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

# 設定に関する注意事項

この項では、このドキュメントで説明されている設定に関する追加情報を提供します。

## 詳細な ACL 口ギング

Nexus Operating System（NX-OS）リリース 6.2(6)以降では、*詳細な* ACL 口ギングを使用できます。 この機能は、次の情報を記録します。

- 発信元および宛先 IP アドレス
- 送信元と送信先ポート
- 送信元インターフェイス
- プロトコル
- ACL 名
- ACL のアクション（許可または拒否）
- 適用されたインターフェイス
- パケット数

詳細ロギングを有効にするには、CLI に **logging ip access-list detailed** コマンドを入力します。次に例を示します。

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

詳細ログを有効にした後のログ出力の例を次に示します。

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

## グローバル OAL コマンドの説明

この項では、OAL を使用できるように Nexus 7000 シリーズ スイッチを設定するために使用するグローバル OAL コマンドについて説明します。

| コマンド | 説明 |
|---|---|
| Switch(config)# logging ip access-list cache {{entries number_of_entries} \| {interval seconds} \| {rate-limit number_of_packets} \| {threshold number_of_packets}} | このコマンドは OAL グローバル パラメータを設定します。 |
| Switch(config)# no logging ip access-list cache {entries \| 間隔 \| rate-limit \| threshold} | このコマンドは、OAL グローバル パラメータをデフォルト設定に<br>ます。 |
| entries<br>num_entries | これらのパラメータは、ソフトウェア内にキャッシュされるログ<br>リの最大数を指定します。 値の範囲は 0 ~ 1,048,576 です。 デフ<br>ト値は 8,000 エントリです。 |
| 間隔<br>秒 | これらのパラメータは、エントリが Syslog に送信されるまでの最<br>間を指定します。 値の範囲は 5 ~ 86,400 です。 デフォルト値は<br>秒です。 |
| threshold<br>num_packets | これらのパラメータは、エントリが Syslog に送信されるまでのパ<br>トー致（ヒット）の数を指定します。 値の範囲は 0 ~ 1,000,000<br>。 デフォルト値は 0 パケット（レート制限なし）です。つまり、<br>ォルトでは、パケット マッチ個数によってシステム ログがトリガ<br>れることはありません。 |

**注:** 次の CLI コマンドの *no form* は、パラメータが変更されている場合にのみデフォルト設定に戻します。 Nexus 7000 シリーズ スイッチには、OAL のオプションがあるため、設定は削除されません。

## ロギング コマンドの説明

この項では、OAL を使用できるように Nexus 7000 シリーズ スイッチを設定するために使用するロギング コマンドについて説明します。

| コマンド | 説明 |
|---|---|

| | |
|---|---|
| switch(config)# acllog match-log- level number<br>例：<br>switch(config)# acllog match-log- level 3 | このコマンドは、エントリが ACL ログ（acllog）に記録される前に一致している必要があ<br>レベルを指定します。 値の範囲は 0 ~ 7 です。 デフォルト値は 6 です。 |
| Switch(config)# no acllog match-log-level number<br>例：<br>switch(config)# no acllog match-log-level 6 | このコマンドはデフォルト設定（6）にログ レベルを戻します。 |
| Switch(config)# logging level facility severity-level<br>例：<br>switch(config)# logging level acllog 3 | このコマンドは、指定された重大度またはそれ以上の重大度である指定のファシリティか<br>メッセージを有効にします。 このドキュメントで使用する例では、デフォルト設定が 2<br>し、*acllog* レベルは 3 に設定されます。 |
| Switch(config)# no logging level [facility severity-level]<br>例：<br>switch(config)# no logging level acllog 3 | このコマンドは、指定されたファシリティのロギング重大度をデフォルト レベルにリセ<br>ファシリティと重大度のレベルを指定しない場合、<br>すべてのファシリティがそれぞれのデフォルト レベルにリセットされます。 このドキュ<br>する例では、acllog はデフォルト（2）に戻ります。 |
| Switch(config)# logging logfile logfile-name severity-level [size bytes]<br>例：<br>switch(config)# logging logfile acllog 3 | このコマンドは、ロギングが発生する前に、システム メッセージと最小の重大度を保存<br>用されるログ ファイルの名前を設定します。 任意で最大ファイル サイズを指定できます<br>トの重大度は 5 です。デフォルトのファイル サイズは 10,485,760 です。 |
| Switch(config)# no logging logfile [logfile-name severity-level [size bytes]]<br>例：<br>switch(config)# no logging logfile acllog 3 | このコマンドは、ログ ファイルへのロギングを無効にします。 |

**注:** ログ メッセージがログに入力されるためには、ACL ログ ファシリティ（acllog）のログ レベルとログ ファイルのロギング重大度が、ACL ログの *match-log-level* 設定よりも大きいか、同じでなければなりません。

## ガイドラインと制限事項

このドキュメントで説明した設定を適用する前に、考慮する必要がある重要なガイドラインと制限を次に示します。

- Nexus 7000 および 7700 シリーズ スイッチは OAL のみサポートします。
- ACL ロギングは、ACL キャプチャ機能を使用しません。
- 出力 ACL の *log* オプションはマルチキャスト パケットではサポートされません。
- 詳細なロギングのサポートは、IPv6 パケットでは利用できません。
- *acllog* ファシリティのログ レベルと*ログファイルのロギング*の重大度は、*acllog match-log-level* の設定よりも大きいか等しくなるように設定する必要があります。
- OAL が使用されている場合は、ハードウェアのアクセス リストの capture コマンドを使用しないでください。 このコマンドが、OAL とともに使用され、ACL キャプチャを有効にすると、すべての仮想デバイス コンテキスト（VDC）で ACL のロギングが無効であることを示す警告メッセージが表示されます。 ACL キャプチャをディセーブルにすると、ACL ロギングはイネーブルになります。 このプロセスが正しく動作するには、**no hardware access-list capture** コマンドの使用を無効にします。