

Nexus 7000の異常なTCAM使用率レベルについて

内容

[概要](#)

[背景](#)

[前提条件](#)

[使用するコンポーネント](#)

[観察](#)

[メインインターフェイスとサブインターフェイスで設定された出力RACLに対して、Netflowはメインインターフェイスでのみ有効になっている](#)

[RACLとNetflowの両方がメインインターフェイスとサブインターフェイスに設定されている場合](#)

[解決方法](#)

[要約](#)

[関連する不具合](#)

[関連記事](#)

概要

このドキュメントでは、Nexus 7000シリーズスイッチで有効になっている機能セットに応じて、TCAMが不意に過剰に使用される仕組みについて説明します。

問題の説明

アトミックアップデートが有効な場合、RACLなどの複数の機能が異なるインターフェイスにNetFlowが適用されると、50%の制限に達していなくてもTCAMのオーバーユースエラーが発生する可能性があります。

例：使用率が29.57であるのに対し、上限が50%（アトミックアップデートが有効な場合）で、次のエラーがスローされるにもかかわらず、後続のサブインターフェイスに複数の機能を適用できません。

```
ERROR:1TCAM
```

また、リロード後、すべてのインターフェイスの設定が失われ、この理由からVDC 0に割り当てられます。

背景

Nexus 7000でデフォルトで有効になっているアトミックアップデートでは、TCAM全体の50%しか使用できません。その他の50%は、ACLの変更に対応するように予約されており、ACLの無停止アップデートを提供します。詳細については、次のセクションのリンクを参照してください。推奨書籍。

前提条件

次の項目について理解しておくことをお勧めします。

アトミックアップデート
N7000のTCAM

使用するコンポーネント

観察

メインインターフェイスとサブインターフェイスで設定された出力ACLに対して、Netflowはメインインターフェイスでのみ有効になっている

初期設定:

```
Interface Ethernet 11/2: Layer-3; RACL
Interface Ethernet 11/2.300-302: Layer-3; RACL
```

RACLのみを適用したTCAM使用率は次のとおりです。

```
N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0" across all instances:
```

```
Tcam 1, Bank 0 1211 2885 29.57
Tcam 1, Bank 0 1211 2885 29.57
Tcam 1, Bank 0 1211 2885 29.57
```

注: このドキュメントの出力ACLのTCAMスペース使用率は29.57%と想定されています

NetFlowがメインインターフェイスにのみ適用されると、インターフェイスの使用率は倍増しますが、この状況でのNetFlowの設定には1%のスペースしか必要としません。

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow
Interface Ethernet 11/2.300-302: Layer-3; RACL
```

ここで、メインインターフェイスにはNetFlowが設定されていますが、サブインターフェイスにはNetFlow (この動作を確認するために無効にするアトミックアップデート) がありません。

```
N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0"
Tcam 1, Bank 0 2394 1702 58.45
Tcam 1, Bank 0 2394 1702 58.45
Tcam 1, Bank 0 2394 1702 58.45
```

注: アトミックアップデートがまだ有効な場合、アトミックアップデートの制限が50%に過ぎず、次のエラーが発生するため、この倍増動作は不可能です。

```
ERROR:1TCAM
```

説明:

この例では、2つの異なるポリシーセットが存在します。1つの宛先にはRACLが単独で、別の宛先にはRACL +NFが存在するため、2つのTCAMエントリが同じ機能に割り当てられ、実際の消費が29.57の動作になるはずですが。

デバイスは、次に示すように、両方のインターフェイスに2つの個別のラベルを生成することによって、これを実現します。

```
module-11# show system internal access-list interface e11/2 out statistics
```

```
INSTANCE 0x0
```

```
-----
```

```
Tcam 1 resource usage:
```

```
-----
```

```
Label_b = 0x801 >>> LABEL is 0x801
```

```
module-11# show system internal access-list interface e11/2.300 out statistics
```

```
INSTANCE 0x0  
-----
```

```
Tcam 1 resource usage:  
-----
```

```
Label_b = 0x802 >>> NEW LABEL 0x802 IS GENERATED
```

RACLとNetflowの両方がメインインターフェイスとサブインターフェイスに設定されている場合

ケース1の設定はすでに存在します。

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow  
Interface Ethernet 11/2.300-302: Layer-3; RACL  
次に、他のサブインターフェイスにもNetFlowを適用します。
```

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow  
Interface Ethernet 11/2.300-302: Layer-3; RACL; NetFlow
```

すべての宛先にRACL + Netflowが設定されているため、同じラベルが宛先ごとに共有されます (すべてのインターフェイスで参照されるTCAMエントリの単一セット)。

```
N7718(config-if)# show system internal access-list resource utilization module 11 | in "Tcam 1, Bank 0"
```

```
Tcam 1, Bank 0 1211 2885 29.57
```

```
Tcam 1, Bank 0 1211 2885 29.57
```

```
Tcam 1, Bank 0 1211 2885 29.57
```

```
module-11# show system internal access-list interface ethernet11/2 out statistics |in Label_b p 5 n 4
```

```
INSTANCE 0x0
```

```
Tcam 1 resource usage:  
-----
```

```
Label_b = 0x802 >>> LABEL is 0x802
```

```
module-11# show system internal access-list interface ethernet11/2.300 out statistics |in Label_b p 5 n 4
```

```
INSTANCE 0x0
```

```
Tcam 1 resource usage:  
-----
```

```
Label_b = 0x802 >>> SAME LABEL IS MAINTAINED
```

注：この動作は、物理インターフェイス、サブインターフェイスにも拡張されます。すべての宛先に同じ設定セットが存在する場合にのみ、TCAMの使用率が2倍になることはありません。

すでにRACLを持つすべてのインターフェイスでNetflowを適用した後に限り、TCAMが元の29.57%に低下することに注意してください

1. インターフェイス「1」にRACLを適用します。29.57%
2. 後続のインターフェイスにRACLを適用します。29.57%
3. インターフェイス「1」でRACL適用後にNFを適用します。58.45%
4. 後続のインターフェイスにNFを適用します。58.45%
5. 最後のインターフェイスにNFを適用します。29.57%

解決方法

1.アトミックアップデートを無効にする。

<OR>

2. ACLのサイズを小さくして、制限を25 %未満に維持します。

要約

アトミックアップデート：

最初のインターフェイスにNetflowが適用されると、最初のインターフェイスには両方のACL、NFが設定され、2番目のインターフェイスにはRACLのみが設定されているため、別のTCAMインスタンスの作成が試行されます。

ただし、アトミックな更新が有効になっているため、個別のインスタンスの作成が失敗し、使用率が50を超えます。その結果、TCAMの使用済みエラーがスローされます。

アトミックアップデートなし：

1.すべてのインターフェイスにACLを適用する場合：他の機能がないため、29のままです。

2.最初のインターフェイスにNetFlowを適用します。スイッチは、これを機能の個別の設定/組み合わせ（個別の内部ラベルを保持）と想定しているため、同じバンクに個別のインスタンスを作成します。

3. ACLが設定されている他のすべてのインターフェイスにNetFlowが適用されると、機能の設定と組み合わせが同じになります（ラベルは両方のインターフェイスで同じになります）。そのため、再シャッフルが発生します

4. TCAMが両方のインターフェイスで共有され、使用率が29.57 %に低下します。

これは、機能の組み合わせが異なるインターフェイスで使用される場合の最適化方法です。

[CSCvs50014](#) ACLNetflow2TCAM

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/security/config/cisco_nexus7000_security_config_guide_8x/configuring_ip_acls.html

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide_Release_6-x/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide_Release_6-x_chapter_01110.html#con_1458580