

瞭解Nexus 7000上不尋常的TCAM利用率級別

目錄

[簡介](#)

[背景](#)

[必要條件](#)

[採用元件](#)

[觀察](#)

[在主介面和子介面上配置輸出RACL，而僅在主介面上啟用Netflow](#)

[在主介面和子介面上配置RACL和Netflow時](#)

[解析](#)

[摘要](#)

[相關缺陷](#)

[相關文章](#)

簡介

本文檔介紹如何根據Nexus 7000系列交換機上啟用的功能集意外過度利用TCAM。

問題描述

啟用原子更新後，在多功能（例如RACL）的情況下，NetFlow應用於不同的介面，雖然未達到50%的限制，但可能會導致TCAM過度使用錯誤。

範例：無法將多個功能應用到後續的子介面，儘管使用率為29.57，但上限為50%（因為啟用了原子更新），並且引發了以下錯誤。

```
1TCAM/
```

此外，重新載入後，所有介面都會丟失配置，因此被分配給VDC 0。

背景

在Nexus 7000上預設啟用的原子更新僅允許利用整個TCAM的50%。保留其他50%以適應ACL更改，以便提供ACL的無中斷更新。有關這方面的更多資訊，請參閱一節中提供的連結：推薦閱讀。

必要條件

建議瞭解以下主題：

原子更新
N7000上的TCAM

採用元件

N77188.3(2)N77-F312CK-26
RACLNetFlow

觀察

[在主介面和子介面上配置輸出RACL，而僅在主介面上啟用Netflow](#)

初始配置：

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

僅應用RACL的TCAM利用率為：

```
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
附註：本文檔中輸出RACL的TCAM空間利用率假定為29.57%
```

一次，NetFlow僅應用於主介面，介面利用率翻倍，儘管在這種情況下NetFlow配置僅佔用1%的空間。

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow
Interface Ethernet 11/2.300-302: Layer-3; RACL
主介面配置了NetFlow，而子介面沒有NetFlow（要禁用原子更新以觀察此行為）
```

```
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
```

附註：如果仍然啟用原子更新，則此加倍行為是不可能的，因為原子更新的限制只有50%，並且會出現以下錯誤：

```
1TCAM/
```

說明：

在這種情況下，此處存在兩個不同的策略集。一個目的地單獨具有RACL，另一個目的地具有RACL +NF。因此，為相同功能分配了兩組TCAM條目，導致倍增行為（我們視為實際消耗量）應該只有29.57行為。

裝置通過為兩個介面生成兩個單獨的標籤來實現這一點，如下所示：

```
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
```

在主介面和子介面上配置RACL和Netflow時

案例1中已存在配置：

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow
Interface Ethernet 11/2.300-302: Layer-3; RACL
現在，也將NetFlow應用到其餘的子介面：
```

```
Interface Ethernet 11/2: Layer-3; RACL; NetFlow
Interface Ethernet 11/2.300-302: Layer-3; RACL; NetFlow
由於現在所有目標都配置了RACL + Netflow，因此相同的標籤被共用b/w目標（所有介面都引用一組TCAM條目）。
```

```
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
```

附註：此行為也擴展到物理介面、子介面。只有在所有相關目標具有相同的配置集時，TCAM利用率不會增加一倍。

請注意，只有在已具有RACL的所有介面上應用Netflow之後，TCAM才會降至原始的29.57%

- 1.在介面「1」上應用RACL:29.57%
- 2.在後續介面上應用RACL:29.57%
- 3.在介面「1」上的RACL應用之後應用NF:58.45%
- 4.在後續介面上應用NF:58.45%
- 5.在最後一個介面上應用NF:29.57%

解析

- 1.禁用原子更新。

<或>

- 2.減小ACL大小以使限制值保持在<25%。

摘要

使用原子更新：

一旦在第一個介面上應用Netflow，就會嘗試建立單獨的TCAM例項，因為第一個介面現在已配置了ACL(NF)，而第二個介面只配置了RACL。但是，由於啟用了原子更新，單獨例項建立會失敗，因為這樣會將利用率提高到50以上。因此，會引發TCAM過度使用錯誤。

沒有原子更新：

1. 在所有介面上應用ACL時：由於沒有其它功能，該指數仍保持在29。
2. 將NetFlow應用於第一個介面：Switch假定這是功能單獨配置/功能組合（維護單獨的內部標籤），因此會在同一銀行上建立單獨的例項。
3. 將NetFlow應用於為其配置了ACL的所有其他介面後，功能的配置/組合將相同（兩個介面的標籤現在相同），因此會發生重新洗牌
4. 兩個介面的TCAM現已共用，利用率降回29.57%。

這是當不同介面上使用特徵組合時的最佳化方法。

[CSCvs50014](#) ACLNetflowTCAM

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

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