Fehlerbehebung bei Leistungsproblemen mit C8000v-Routern

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Leistungsprobleme bei C8000v-Unternehmensroutern in Public Clouds und ESXi-Szenarien behoben werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Softwarekomponenten:

- C8000v mit 17.12-Version
- ESXI Version 7.0 U3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Allgemeine Fehlerbehebung

Obwohl Sie Ihren C8000v in verschiedenen Umgebungen hosten können, gibt es immer noch

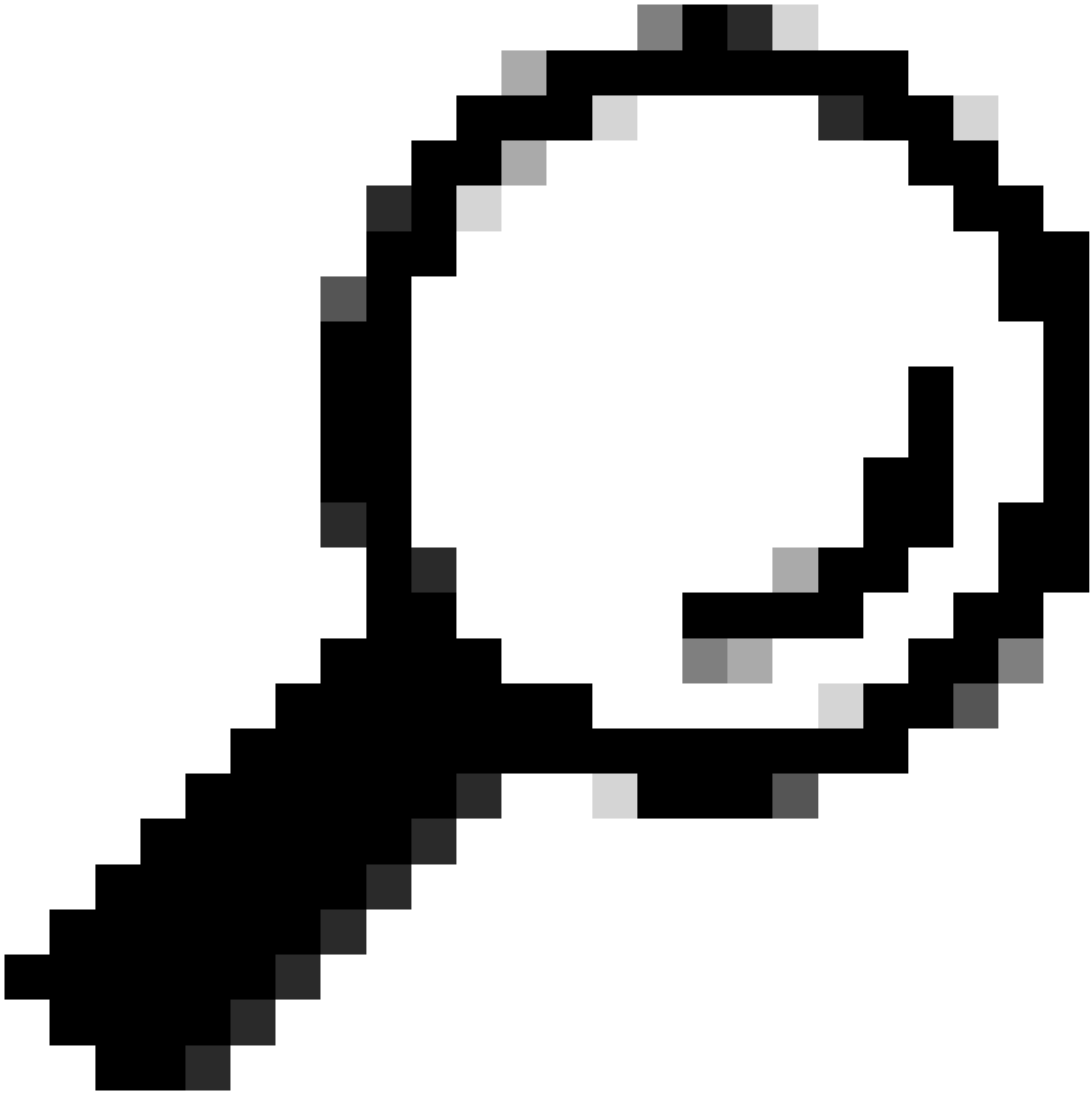
einige Schritte zur Fehlerbehebung, die identisch sind, unabhängig davon, wo der C8000v gehostet wird. Lassen Sie uns mit den Grundlagen beginnen. Als Erstes müssen Sie sicherstellen, dass das Gerät seine Kapazitätsgrenzen erreicht hat. Dazu können Sie zunächst die folgenden beiden Ausgaben überprüfen:

1. show platform hardware qfp active datapath util summary - Dieser Befehl liefert Ihnen die vollständigen Informationen über die Ein-/Ausgabe, die der C8000v von jedem Port empfängt und überträgt. Konzentrieren Sie sich auf den prozentualen Anteil der Verarbeitungslast. Wenn Sie sich in einem Szenario befinden, in dem Sie 100 % erreichen, bedeutet dies, dass Sie die Kapazitätsgrenze erreichen.

```
------------------ show platform hardware qfp active datapath utilization summary  ------------------

  CPP 0:                      5 secs        1 min        5 min       60 min
Input:     Total (pps)         93119        92938        65941        65131
                 (bps)     997875976   1000204000    708234904    699462016
Output:    Total (pps)         93119        92949        65944        65131
                 (bps)    1052264704   1054733128    746744264    737395744
Processing: Load (pct)            14           14           10           10
```

2. show platform hardware qfp active datapath infrastructure sw-cio - Dieser Befehl ist eine detailliertere Version des obigen Befehls. Er liefert genauere Informationen zu den einzelnen Cores, einschließlich der E/A- und Krypto-Cores, die nicht Teil der QFP-Nutzungsnummer sind. Dieses Szenario ist sehr nützlich, wenn Sie sehen möchten, ob ein bestimmter Datenebenenkern einen Engpass verursacht.



Tipp: Ein sehr wichtiges Detail bei der Verwendung dieses Befehls, immer zweimal ausführen. Berechnet die prozentuale Core-Auslastung zwischen der Ausführung des Befehls.

```
------------------ show platform hardware qfp active datapath infrastructure sw-cio  ------------------

Credits Usage:

  ID      Port  Wght  Global WRKR0  WRKR1  WRKR2  WRKR3  WRKR4  WRKR5  WRKR6  WRKR7  WRKR8  WRKR9  WRKR
   1      rcl0    16:    492      0      0      0      0      0      0      0      0      0      0
   1      rcl0    32:    496      0      0      0      0      0      0      0      0      0      0
   2       ipc     1:    489      0      0      0      0      0      0      0      0      0      0
   3 vxe_punti     4:    490      0      0      0      0      0      0      0      0      0      0
   4       Gi1     4:   1999      0      0      0      0      0      0      0      0      0      0
   5       Gi2     4:   1991      0      0      0      0      0      0      0      0      0      0
   6       Gi3     4:   1991      0      0      0      0      0      0      0      0      0      0
```

```
  7       Gi4     4:   1993     0      0      0      0      0      0      0      0      0      0
  8       Gi5     4:   2009     0      0      0      0      0      0      0      0      0      0
  9       Gi6     4:   2015     0      0      0      0      0      0      0      0      0      0
 10       Gi7     4:   2002     0      0      0      0      0      0      0      0      0      0
 11      vpg0   400:    490     0      0      0      0      0      0      0      0      0      0

Core Utilization over preceding 107352.2729 seconds
---------------------------------------------------
      ID:      0      1      2      3      4      5      6      7      8      9     10      1
    % PP:   2.98   2.01   1.81   1.67   1.60   1.53   1.35   1.30   1.25   1.19   2.19   1.
    % RX:   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.
    % TM:   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.
  % IDLE:  97.02  97.99  98.19  98.33  98.40  98.47  98.65  98.70  98.75  98.81  97.81  98.
```

Jetzt haben Sie festgestellt, ob Sie die Plattformgrenze erreichen oder nicht. Der nächste Schritt wäre, auf Tropfen zu prüfen. Diese sind grundsätzlich mit Leistungsproblemen verbunden. Es gibt drei Arten von Tropfen, die Sie in Betracht ziehen können, je nachdem, wo sie auftreten.

- Überschreitungen: Dieser Paketverwerfungstyp tritt am Rx-Ende auf. Sie treten auf, weil die Verarbeitungskapazität eines oder mehrerer Kerne überschritten wurde.
- Verworfene Funktionen: Dieser Paketverlust tritt im PPE-System auf. Sie hängen mit Funktionen im Router zusammen, z. B. mit einer ACL oder QoS.
- Heckklappe: Dieser Paketverwerfungstyp tritt am Tx-Ende auf. Sie passieren aufgrund von Überlastung in den Tx-Puffern.

Um festzustellen, welche Tropfen Sie erleben, können Sie die folgenden Ausgaben verwenden:

- show plattform hardware qfp active drop state clear
- show interface
- Richtlinienzuordnungsschnittstelle anzeigen

Sie überprüfen, wie Sie feststellen können, welchen Angriffen Sie ausgesetzt sind, und wie Sie diese vermeiden können. Der größte Fokus in diesem Artikel sind jedoch die Drops, die als Taildrops bezeichnet werden, da sie besonders bei virtuellen Routern schwierig zu beheben sind.

Überläufe

Ein Overrun-Drop in Cisco IOS XE tritt auf, wenn die Netzwerkschnittstelle Pakete schneller empfängt, als sie diese verarbeiten oder in ihrem Puffer speichern kann. Insbesondere die internen Puffer der Schnittstellen (FIFO-Warteschlange) werden voll, da die Datenübertragungsrate die Fähigkeit der Hardware zur Verarbeitung übersteigt. Daher können neue eingehende Pakete nicht gespeichert werden, und sie werden verworfen, wodurch der Zähler für die Überschreitung erhöht wird. Dies ist im Wesentlichen ein Paketverlust, der durch die vorübergehende Überlastung der Schnittstelle verursacht wird.

Diese Art von Paketverlust tritt am Rx-Ende auf. Sie treten auf, weil die Verarbeitungskapazität eines oder mehrerer Kerne überschritten wurde und der Rx-Thread eingehende Pakete nicht an den entsprechenden PP-Thread verteilen kann und die Eingangspuffer bereits voll sind. Um eine einfache Analogie zu machen, können Sie es sich als eine Warteschlange an einem

Kassenschalter vorstellen, der zu voll wird, weil Pakete schneller ankommen, als die Kassierer (Schnittstellen-Hardware) sie bedienen können. Wenn die Warteschlange voll ist, müssen neue Kunden gehen, ohne bedient zu werden - das sind die Überschreitungen.

Obwohl Hardware in diesem Abschnitt erwähnt wird, ist der C8000v ein softwarebasierter Router. In diesem Fall können Überläufe verursacht werden durch:

- Hohe Auslastung der Datenebene: Wenn die Auslastung der Datenebene hoch ist, können die Pakete nicht schnell genug abgerufen werden, was zu Überläufen führt. Das Vorhandensein von "Elefantenflüssen" (großen, kontinuierlichen Datenflüssen) kann beispielsweise Verarbeitungsressourcen belasten und zu Überläufen an den Schnittstellen führen.
- Falsche Gerätevorlage: Die Verwendung einer ungeeigneten Gerätevorlage kann zu ineffizientem Puffermanagement und Überläufen führen. Dies kann mit dem Befehl show platform software cpu alloc überprüft und mit dem Befehl platform resource **<template>** geändert werden.

Jeder Schnittstelle wird ein begrenzter Pool von Credits zugewiesen. Dieser Mechanismus verhindert, dass die Schnittstelle ausgelastet ist und die Systemressourcen überlastet werden. Jedes Mal, wenn ein neues Paket auf dem Datenflugzeug eingeht, ist eine Gutschrift erforderlich. Wenn die Paketverarbeitung abgeschlossen ist, wird die Gutschrift zurückgegeben, sodass der Rx-Thread sie erneut verwenden kann. Wenn für die Schnittstelle kein Guthaben verfügbar ist, muss das Paket im Rx-Ring der Schnittstelle warten. Im Allgemeinen erwarten Sie, dass das Leistungslimit aufgrund der Überschreitung der Verarbeitungskapazität eines oder mehrerer Kerne überschritten wird.

Um Überläufe zu identifizieren, überprüfen Sie in der Regel die Schnittstellenstatistiken auf Eingabefehler, insbesondere den Überlauffähigkeitszähler:

- Verwenden Sie den Befehl show platform hardware qfp active datapath infrastructure sw-cio, um die Core-Nutzung zu identifizieren und zu ermitteln, ob die Anzahl der Gutschriften für eine bestimmte Schnittstelle überschritten wurde.
- Verwenden Sie den Befehl show interface **<Schnittstellenname>**, und suchen Sie in der Ausgabe nach der Anzahl der Überläufe.

Überläufe werden als Teil von Eingabefehlern angezeigt, z. B.:

```
Gig2 is up, line protocol is up
241302424557 packets input, 168997587698686 bytes, 0 no buffer
20150 input errors, 0 CRC, 0 frame, 20150 overrun, 0 ignored <<<<<<<<<<<
```

Nehmen wir an, Gig2 beobachtet Leistungsprobleme, die durch Überläufe verursacht werden. Um den Arbeitsthread zu bestimmen, der dieser Schnittstelle zugeordnet ist, können Sie den folgenden Befehl verwenden:

```
#show platform hardware qfp active datapath infra binding
Port Instance Bindings:

ID Port IOS Port WRKR 2
1 rcl0 rcl0 Rx+Tx
2 ipc ipc Rx+Tx
3 vxe_punti vxe_puntif Rx+Tx
4 Gi1 GigabitEthernet1 Rx+Tx
5 Gi2 GigabitEthernet2 Rx+Tx <<< in this case, WRKR2 is the thread responsible for both Rx and Tx
```

Anschließend können Sie die Nutzung des spezifischen Threads analysieren, der für den Rx-Datenverkehr dieser Schnittstelle verantwortlich ist, sowie die Anzahl der Credits.

In einem Szenario, in dem Gig2 Leistungsprobleme aufgrund von Überläufen beobachtet, können Sie davon ausgehen, dass der PP#2 ständig voll ausgelastet ist (Idle = 0 %) und dass die Schnittstelle Gig2 mit niedrigen oder null Credits ausgestattet ist:

```
#show platform hardware qfp active datapath infrastructure sw-cio
Credits Usage:

ID Port Wght Global WRKR0 WRKR1 WRKR2 Total
1 rcl0 16: 487 0 0 25 512
1 rcl0 32: 496 0 0 16 512
2 ipc 1: 490 0 0 21 511
3 vxe_punti 4: 459 0 0 53 512
4 Gi1 4: 477 0 0 35 512
5 Gi2 4: 474 0 0 38 512 <<< low/zero credits for interface Gig2:

Core Utilization over preceding 1.0047 seconds
-----------------------------------------------
ID: 0 1 2
% PP: 0.77 0.00 0.00
% RX: 0.00 0.00 0.44
% TM: 0.00 0.00 5.63
% IDLE: 99.23 99.72 93.93 <<< the core ID relevant in this case would be PP#2
```

Verwerfen von Funktionen

Pakete werden von jedem verfügbaren Datenebenen-Thread verarbeitet und ausschließlich auf Basis der Verfügbarkeit von QFP-Cores über die Software-Rx-Funktion (x86) - Load Based Distribution (LBD) verteilt. Pakete, die im PPE ankommen, können mit einem bestimmten QFP-Verwerfungsgrund verworfen werden, der mit der folgenden Ausgabe überprüft werden kann:

```
#show drops
------------------ show platform hardware qfp active statistics drop detail ------------------

Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------------
   ID  Global Drop Stats                          Packets                 Octets
```

```
------------------------------------------------------------------------------
  319  BFDoffload                              403                  31434
  139  Disabled                                105                   7487
   61  Icmp                                    135                   5994
   94  Ipv4NoAdj                                 1                    193
   33  Ipv6NoRoute                            2426                 135856
  215  UnconfiguredIpv4Fia                 1937573              353562196
  216  UnconfiguredIpv6Fia                 8046173             1057866418


------------------ show platform hardware qfp active interface all statistics drop_summary ------------

-----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
         reads the interface stats.
      2) the interface stats include the subinterface

Interface                                       Rx Pkts             Tx Pkts
-------------------------------------------------------------------------
GigabitEthernet1                                9980371                   0
GigabitEthernet2                                   4012                   0
```

Die Gründe für die Tropfen sind vielfältig und in der Regel selbsterklärend. Für weitere Untersuchungen kann eine Paketverfolgung verwendet werden.

Heckklappe

Wie bereits erwähnt, treten Aussetzer dort auf, wo das Gerät versucht, Pakete zu übertragen, die Übertragungspuffer jedoch voll sind.

In diesem Unterabschnitt werden Sie sehen, welche Ausgaben Sie überprüfen können, wenn Sie mit dieser Art von Situation konfrontiert sind. Welche Werte Sie darin erkennen können, und was Sie tun können, um das Problem zu beheben.

Zunächst müssen Sie wissen, wie Sie diese identifizieren können. Eine solche Möglichkeit ist, einfach auf die Show-Schnittstelle zu schauen. Achten Sie darauf, dass die Ausgangsleistung sinkt:

```
GigabitEthernet2 is up, line protocol is up
Hardware is vNIC, address is 0050.56ad.c777 (bia 0050.56ad.c777)
Description: Connected-To-ASR Cloud Gateway
Internet address is 10.6.255.81/29
MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 2/255, rxload 3/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 10000Mbps, link type is force-up, media type is Virtual
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 03:16:21
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 7982350 <<<<<<<<
```

```
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 150449000 bits/sec, 20461 packets/sec
5 minute output rate 89116000 bits/sec, 18976 packets/sec
```

Dieser Befehl ist besonders nützlich, um zu verstehen, wenn bei Ihnen Staus auftreten oder nicht:

- show platform hardware qfp active datapath infrastructure - HQF steht für "Hierarchical Queueing Framework". Diese Funktion ermöglicht das QoS-Management auf verschiedenen Ebenen (physisch, logisch und Klasse) mithilfe der modularen QoS-Kommandozeile (MQC). Sie zeigt die aktuellen RX- und TX-Kosten an. Wenn die TX-Warteschlange voll ist, wie die Ausgabe anzeigt (volle 1959)

```
pmd b1689fc0 device Gi1
RX: pkts 5663120 bytes 1621226335 return 0 badlen 0
Out-of-credits: Hi 0 Lo 0
pkts/burst 1 cycl/pkt 1565 ext_cycl/pkt 1173
Total ring read 12112962299, empty 12107695202
TX: pkts 8047873582 bytes 11241140363740
pri-0: pkts 8047873582 bytes 11241140363740
pkts/send 3
Total: pkts/send 3 cycl/pkt 452
send 2013612969 sendnow 1810842
forced 2013274797 poll 724781 thd_poll 0
blocked 2197451 retries 7401 mbuf alloc err 0
TX Queue 0: full 1959 current index 0 hiwater 224
```

Die Ausgabe deutet darauf hin, dass die zugrunde liegende Hardware mit dem Senden von Paketen nicht Schritt hält. Um die zugrunde liegende Schnittstelle zu debuggen, müssen Sie möglicherweise außerhalb des C8000v und der zugrunde liegenden Umgebung suchen, in der das C8000v ausgeführt wird, um festzustellen, ob auf den zugrunde liegenden physischen Schnittstellen zusätzliche Fehler gemeldet werden.

Um die Umgebung zu überprüfen, können Sie zunächst prüfen, auf welchem Hypervisor der C8000v-Router ausgeführt wird. Dies ist, um die Ausgabe des Befehls show controller zu überprüfen. Trotzdem kann man sich auf dem, was jeder Zähler bedeutet oder wo man sich ansehen verloren.

Zunächst einmal sollten Sie bei dieser Ausgabe berücksichtigen, dass die Informationen größtenteils von den vNICs selbst stammen. Jeder Netzwerkkartentreiber verfügt über einen bestimmten Satz von Zählern, die er verwendet. Diese können natürlich je nach Treiber variieren. Verschiedene Hypervisoren haben auch einen gewissen Einfluss auf die Darstellung. Einige Zähler, z. B. mbuf-Zähler, sind Statistiken vom DPDK-Treiber. Diese können je nach DPDK-Treiber variieren. Die eigentliche Zählung wird in der Regel vom Hypervisor auf Virtualisierungsebene vorgenommen.

```
GigabitEthernet2 - Gi2 is mapped to UIO on VXE
```

```
rx_good_packets 1590
tx_good_packets 1402515
rx_good_bytes 202860
tx_good_bytes 1857203911
rx_missed_errors 0
rx_errors 0
tx_errors 0
rx_mbuf_allocation_errors 0
rx_q0_packets 1590
rx_q0_bytes 202860
rx_q0_errors 0
tx_q0_packets 1402515
tx_q0_bytes 1857203911
rx_q0_drop_total 0
rx_q0_drop_err 0
rx_q0_drop_fcs 0
rx_q0_rx_buf_alloc_failure 0
tx_q0_drop_total 976999540797
tx_q0_drop_too_many_segs 0
tx_q0_drop_tso 0
tx_q0_tx_ring_full 30901211518
```

Nehmen Sie sich einen Moment Zeit, um zu erfahren, wie Sie diese Zähler interpretieren und lesen können:

1. Wenn Sie subX sehen, bedeutet das, dass es eine Subschnittstelle ist - eine logische Unterteilung der Hauptschnittstelle. Der sub0 ist im Allgemeinen der primäre/standardmäßige Wert. Diese werden häufig verwendet, wenn mehrere VLANs beteiligt sind.
2. Dann haben Sie "rx = Empfangen" und "tx = Senden".
3. Schließlich bezieht sich q0 auf die erste/Standardwarteschlange, die von dieser Schnittstelle verwendet wird.

Auch wenn es nicht für jeden Zähler eine Beschreibung gibt, werden einige davon beschrieben, die für die Fehlerbehebung relevant sein können:

- "RX_MISSED_ERRORS:" wird angezeigt, wenn der NIC-Puffer (Rx FIFO) zu voll wird. Dies führt zu Einbrüchen und einer Erhöhung der Latenz. Eine mögliche Lösung hierfür ist die Erhöhung des NIC-Puffers (was in unserem Fall nicht möglich ist) oder die Änderung des NIC-Treibers.
- "tx_q0_drop_total" und "tx_q0_tx_ring_full": Diese können Ihnen mitteilen, dass der Host Pakete verwirft und dass beim C8000v Schwanzverluste im C8000v auftreten, da der Host den C8000v-Router mit einem Gegendruck beaufschlagt.

In der obigen Ausgabe wird kein "rx_missing_errors" angezeigt. Da wir uns jedoch auf die Taildrops konzentrieren, sehen wir sowohl "tx_q0_drop_total" als auch "tx_q0_tx_ring_full". Daraus können wir schließen, dass es in der Tat eine Überlastung durch die zugrunde liegende Hardware des Hosts verursacht.

Wie bereits erwähnt, hat jeder Hypervisor einen gewissen Einfluss auf die Darstellung. Der Artikel konzentriert sich im nächsten Abschnitt darauf, während er die Unterschiede zwischen den

verschiedenen Hypervisoren behandelt, auf denen der C8000v gehostet werden kann. Sie können auch die verschiedenen Empfehlungen finden, um zu versuchen, diese Art von Problem in jedem von ihnen zu mildern.

Hypervisoren

Ein Hypervisor ist eine Softwareschicht, die die Ausführung mehrerer Betriebssysteme (virtuelle Systeme oder VMs) auf einem einzelnen physischen Hardware-Host ermöglicht, indem die Hardwareressourcen wie CPU, Arbeitsspeicher und Speicher verwaltet und jedem VM zugewiesen werden. Es stellt sicher, dass diese virtuellen Systeme unabhängig voneinander arbeiten, ohne sich gegenseitig zu stören.

Im Kontext des Cisco Catalyst 8000V (C8000v) ist der Hypervisor die Plattform, die das virtuelle C8000v-System hostet. Wie finden Sie heraus, welcher Hypervisor Ihr C8000v hostet? Es gibt eine ziemlich nützliche Ausgabe, die uns diese Informationen gibt. Zusätzlich können Sie überprüfen, auf welche Ressourcen unser virtueller Router Zugriff hat:

```
C8000v#show platform software system all
Processor Details
=================
Number of Processors : 8
Processor : 1 - 8
vendor_id : GenuineIntel
cpu MHz : 2593.906
cache size : 36608 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz

Memory Details
==============
Physical Memory : 32817356KB

VNIC Details
============
Name Mac Address Driver Name Status Platform MTU
GigabitEthernet1 0022.480d.7a05 net_netvsc UP 1500
GigabitEthernet2 6045.bd69.83a0 net_netvsc UP 1500
GigabitEthernet3 6045.bd69.8042 net_netvsc UP 1500

Hypervisor Details
==================
Hypervisor: AZURE
Manufacturer: Microsoft Corporation
Product Name: Virtual Machine
Serial Number: 0000-0002-0201-5310-5478-4052-71
UUID: 8b06091c-f1d3-974c-85a5-a78dfb551bf2
Image Variant: None
```

VMware ESXi

ESXi ist ein Hypervisor vom Typ 1, der von VMware entwickelt wurde und direkt auf physischen

Servern installiert wird, um die Virtualisierung zu ermöglichen. Es ermöglicht die Ausführung mehrerer virtueller Systeme (VMs) auf einem einzigen physischen Server, indem die Hardwareressourcen abstrahiert und jeder VM zugewiesen werden. Der C8000v-Router ist eine dieser VMs.

Sie können damit beginnen, ein allgemeines Szenario zu durchsuchen, in dem eine Überlastung auftritt. Dies kann durch Überprüfung des Zählers tx_q0_tx_ring_full bestätigt werden:

Beispiel:

```
------------------ show platform software vnic-if interface-mapping ------------------

---------------------------------------------------------------
Interface Name Driver Name Mac Addr
---------------------------------------------------------------
GigabitEthernet3 net_vmxnet3 <-- 0050.5606.2239
GigabitEthernet2 net_vmxnet3 0050.5606.2238
GigabitEthernet1 net_vmxnet3 0050.5606.2237
---------------------------------------------------------------

GigabitEthernet3 - Gi3 is mapped to UIO on VXE
rx_good_packets 99850846
tx_good_packets 24276286
rx_good_bytes 78571263015
tx_good_bytes 14353154897
rx_missed_errors 0
rx_errors 0
tx_errors 0
rx_mbuf_allocation_errors 0
rx_q0packets 99850846
rx_q0bytes 78571263015
rx_q0errors 0
tx_q0packets 24276286
tx_q0bytes 14353154897
rx_q0_drop_total 0
rx_q0_drop_err 0
rx_q0_drop_fcs 0
rx_q0_rx_buf_alloc_failure 0
tx_q0_drop_total 160945155
tx_q0_drop_too_many_segs 0
tx_q0_drop_tso 0
tx_q0_tx_ring_full 5283588 <------
```

Diese Überlastung tritt auf, wenn der C8000V versucht, Pakete über die VMXNET3-Schnittstelle zu senden. Der Pufferring ist jedoch bereits voll mit Paketen, die entweder verzögert werden oder verloren gehen.

Unter diesen Bedingungen erfolgt der Ausfall auf der Hypervisorseite, wie bereits erwähnt. Wenn alle Empfehlungen erfüllt werden, wird empfohlen, sich an den VMware-Support zu wenden, um zu erfahren, was auf der Netzwerkkarte geschieht.

Nachstehend finden Sie einige Vorschläge zur Verbesserung der Leistung:

- Verwendung eines dedizierten vSwitches und Uplinks für optimale Leistung
- Durch die Zuweisung des C800V zu einem dedizierten vSwitch, der durch einen eigenen physischen Uplink unterstützt wird, können wir den Datenverkehr von lauten Nachbarn isolieren und Engpässe bei gemeinsam genutzten Ressourcen vermeiden.

Es gibt einige Befehle, die es wert sind, von ESXi-Seite betrachtet zu werden. Um beispielsweise zu prüfen, ob von der ESXi-Schnittstelle Paketverluste auftreten, führen Sie die folgenden Schritte aus:

1. Aktivieren Sie SSH.
2. Stellen Sie über SSH eine Verbindung mit ESXi her.
3. Starten Sie esxtop.
4. Geben Sie n ein.

Der Befehl esxtop kann Pakete anzeigen, die am virtuellen Switch verworfen wurden, wenn dem Netzwerktreiber des virtuellen Systems der Rx-Pufferspeicher ausgeht. Obwohl esxtop die Pakete als am virtuellen Switch verworfen anzeigt, werden sie zwischen dem virtuellen Switch und dem Gast-Betriebssystemtreiber verworfen.

Suchen Sie nach Paketen, die unter %DRPTX und %DRPRX verworfen werden:

```
12:34:43pm up 73 days 16:05, 907 worlds, 9 VMs, 53 vCPUs; CPU load average: 0.42, 0.42, 0.42

PORT-ID USED-BY TEAM-PNIC DNAME PKTTX/s MbTX/s PSZTX PKTRX/s MbRX/s PSZRX %DRPTX %DRPRX
67108870 Management n/a vSwitch-to-9200 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
67108872 Shadow of vmnic1 n/a vSwitch-to-9200 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
67108876 vmk1 vmnic1 vSwitch-to-9200 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
67108890 2101719:c8kv-gw-mgmt vmnic1 vSwitch-to-9200 76724.83 792.35 1353.00 16180.39 9.30 75.00 0.00 0
100663305 Management n/a vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
100663307 Shadow of vmnic0 n/a vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
100663309 vmk0 vmnic0 vSwitch-to-Cisc 3.64 0.01 280.00 3.29 0.00 80.00 0.00 0.00
100663310 2100707:gsoaresc-On_Prem vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 2.43 0.00 60.00 0.00 0.00
100663311 2100993:cats-vmanage void vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
100663312 2100993:cats-vmanage void vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
100663313 2100993:cats-vmanage vmnic0 vSwitch-to-Cisc 5.38 0.01 212.00 9.71 0.01 141.00 0.00 0.00
100663314 2101341:cats-vsmart void vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
100663315 2101341:cats-vsmart vmnic0 vSwitch-to-Cisc 2.60 0.00 164.00 6.94 0.01 124.00 0.00 0.00
100663316 2101522:cats-vbond vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 100.00
100663317 2101522:cats-vbond vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 0.00 0.00 0.00 0.00 100.00
100663318 2101522:cats-vbond vmnic0 vSwitch-to-Cisc 4.33 0.01 174.00 7.80 0.01 162.00 0.00 0.00
100663319 2101522:cats-vbond vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 4.16 0.00 90.00 0.00 0.00
100663320 2101547:gdk-backup vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 3.12 0.00 77.00 0.00 0.00
100663321 2101703:sevvy vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 3.12 0.00 77.00 0.00 0.00
100663323 2101719:c8kv-gw-mgmt vmnic0 vSwitch-to-Cisc 16180.91 9.09 73.00 76755.87 792.44 1353.00 0.00 0
100663324 2137274:telemetry-server vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 3.12 0.00 77.00 0.00 0.00
100663335 2396721:netlab vmnic0 vSwitch-to-Cisc 0.00 0.00 0.00 3.12 0.00 77.00 0.00 0.00
2214592519 vmnic1 - vSwitch-to-9200 76727.26 792.38 1353.00 16182.64 9.30 75.00 0.00 0.00
2248146954 vmnic0 - vSwitch-to-Cisc 16189.05 9.32 75.00 76736.97 792.38 1353.00 0.00 0.00
```

Dieser Befehl listet alle NICs auf, die auf einem Host konfiguriert sind:

```
esxcli network nic list
Name PCI Device Driver Admin Status Link Status Speed Duplex MAC Address MTU Description
------ ------------ ------ ------------ ----------- ----- ------ ----------------- ---- -----------
vmnic0 0000:01:00.0 igbn Up Up 1000 Full fc:99:47:49:c5:0a 1500 Intel(R) I350 Gigabit Network Connectio
vmnic1 0000:01:00.1 igbn Up Up 1000 Full fc:99:47:49:c5:0b 1500 Intel(R) I350 Gigabit Network Connectio
vmnic2 0000:03:00.0 ixgben Up Up 1000 Full a0:36:9f:1c:1f:cc 1500 Intel(R) Ethernet Controller 10 Gigab
vmnic3 0000:03:00.1 ixgben Up Up 1000 Full a0:36:9f:1c:1f:ce 1500 Intel(R) Ethernet Controller 10 Gigab
```

Es gibt auch einen nützlichen Befehl, um den Status der vNIC zu überprüfen, die einem bestimmten virtuellen System zugewiesen ist.

```
esxcli network vm list
World ID Name Num Ports Networks
-------- ---------------- --------- --------
2137274 telemetry-server 1 Cisco Backbone 10.50.25.0/24
2101703 sevvy 1 Cisco Backbone 10.50.25.0/24
2396721 netlab 1 Cisco Backbone 10.50.25.0/24
2101547 gdk-backup 1 Cisco Backbone 10.50.25.0/24
2101522 cats-vbond 4 VPN0, VPN0, VPN0, VPN0
2101719 c8kv-gw-mgmt 2 c8kv-to-9200l, c8kv-to-cisco
2100707 gsoaresc-On_Prem 1 Cisco Backbone 10.50.25.0/24
2100993 cats-vmanage 3 VPN0, VPN0, VPN0
2101341 cats-vsmart 2 VPN0, VPN0
[root@localhost:~]
```

Wenn Sie sich c8kv-gw-mgmt ansehen, bei dem es sich um ein virtuelles System mit C8000v handelt, werden Ihnen 2 Netzwerke zugewiesen:

- c8kv-bis-9200l
- c8kv-zu-Cisco

Sie können die Welt-ID verwenden, um nach weiteren Informationen zu diesem virtuellen System zu suchen:

```
[root@localhost:~] esxcli network vm port list -w 2101719
Port ID: 67108890
vSwitch: vSwitch-to-9200L
Portgroup: c8kv-to-9200l
DVPort ID:
MAC Address: 00:0c:29:31:a6:b6
IP Address: 0.0.0.0
Team Uplink: vmnic1
Uplink Port ID: 2214592519
Active Filters:
```

```
Port ID: 100663323
vSwitch: vSwitch-to-Cisco
Portgroup: c8kv-to-cisco
DVPort ID:
MAC Address: 00:0c:29:31:a6:ac
IP Address: 0.0.0.0
Team Uplink: vmnic0 <----
Uplink Port ID: 2248146954
Active Filters:
[root@localhost:~]
```

Sobald Ihnen diese Informationen vorliegen, können Sie bestimmen, welchem Netzwerk der vSwitch zugeordnet ist.

Um einige Statistiken zum Datenverkehr der dem vSwitch zugewiesenen physischen NICs zu überprüfen, verwenden Sie den folgenden Befehl:

```
# esxcli network nic stats get -n <vmnic>
```

Dieser Befehl zeigt Informationen wie empfangene Pakete, empfangene Bytes, verlorene Pakete und empfangene Fehler an. Auf diese Weise kann leichter festgestellt werden, ob die Netzwerkkarte verloren geht.

```
[root@localhost:~] esxcli network nic stats get -n vmnic0
NIC statistics for vmnic0
Packets received: 266984237
Packets sent: 123640666
Bytes received: 166544114308
Bytes sent: 30940114661
Receive packets dropped: 0
Transmit packets dropped: 0
Multicast packets received: 16773454
Broadcast packets received: 36251726
Multicast packets sent: 221108
Broadcast packets sent: 1947649
Total receive errors: 0
Receive length errors: 0
Receive over errors: 0
Receive CRC errors: 0
Receive frame errors: 0
Receive FIFO errors: 0
Receive missed errors: 0
Total transmit errors: 0
Transmit aborted errors: 0
Transmit carrier errors: 0
Transmit FIFO errors: 0
Transmit heartbeat errors: 0
Transmit window errors: 0
```

Es gibt einige Konfigurationen, die überprüft werden müssen, um die Leistung von Cisco Catalyst 8000V in einer ESXi-Umgebung zu verbessern, indem die Einstellungen auf dem Host und dem virtuellen System geändert werden:

- Legen Sie die virtuelle Hardware fest: Die CPU-Reservierungseinstellung ist Maximum.
- Reservieren Sie den gesamten Gastspeicher in der virtuellen Hardware: Arbeitsspeicher.
- Wählen Sie VMware Paravirtual unter Virtual Hardware: SCSI-Controller
- Über die virtuelle Hardware: Netzwerkadapter: Option "Adaptertyp": Wählen Sie SR-IOV für die unterstützten NICs aus.
- Legen Sie die Option General Guest OS Version > VM Options (Allgemeine Gastbetriebssystem-Version > VM-Optionen) auf Other 3.x oder höher Linux (64-Bit) fest.
- Legen Sie die Option VM-Optionen unter Erweiterte Latenzempfindlichkeit auf Hoch fest.
- Fügen Sie unter VM Options > Advanced Edit Configuration "numa.nodeAffinity" zum gleichen NUMA-Knoten wie die SRIOV NIC hinzu.
- Aktivieren Sie die Hypervisor-Leistungseinstellungen.
- Begrenzen Sie den Overhead von vSwitch, indem Sie SR-IOV auf den unterstützten physischen NICs aktivieren.
- Konfigurieren Sie die vCPUs des virtuellen Systems so, dass sie auf demselben NUMA-Knoten wie die physischen NICs ausgeführt werden.
- Stellen Sie die Latenzempfindlichkeit der virtuellen Systeme auf Hoch ein.

AWS

Der C8000v unterstützt die Bereitstellung auf AWS, indem er als Amazon Machine Image (AMI) in einer Amazon Virtual Private Cloud (VPC) startet. So können Benutzer einen logisch isolierten Abschnitt der AWS-Cloud für ihre Netzwerkressourcen bereitstellen.

Multi-TX-Warteschlangen

In einem C8000v, der auf AWS ausgeführt wird, ist die Verwendung von Multi-TX-Warteschlangen (Multi-TXQs) ein wichtiges Merkmal. Diese Warteschlangen reduzieren den internen Verarbeitungsaufwand und verbessern die Skalierbarkeit. Mehrere Warteschlangen machen es schneller und einfacher, eingehende und ausgehende Pakete der richtigen virtuellen CPU (vCPU) zuzuweisen.

Im Gegensatz zu einigen Systemen, bei denen RX/TX-Warteschlangen pro vCPU zugewiesen werden, werden diese Warteschlangen beim C8000v pro Schnittstelle zugewiesen. Die RX- (Receive-) und TX- (Transmit-) Warteschlangen dienen als Verbindungspunkte zwischen der Catalyst 8000V-Anwendung und der AWS-Infrastruktur oder -Hardware und verwalten das Senden und Empfangen von Netzwerkverkehr. AWS steuert die Anzahl und Geschwindigkeit der RX-/TX-Warteschlangen, die je nach Instanztyp für jede Schnittstelle verfügbar sind.

Um mehrere TX-Warteschlangen zu erstellen, benötigt der Catalyst 8000V mehrere Schnittstellen. Wenn mehrere TX-Warteschlangen aktiviert sind, behält das Gerät die Reihenfolge der

Paketflüsse bei, indem es eine Hash-Methode verwendet, die auf dem 5-Tupel des Flusses (Quell-IP, Ziel-IP, Quell-Port, Ziel-Port und Protokoll) basiert. Dieses Hashing entscheidet, welche TX-Warteschlange für die einzelnen Datenflüsse verwendet wird.

Benutzer können mehrere Schnittstellen auf dem Catalyst 8000V erstellen, indem sie die gleiche physische Netzwerkkarte (NIC) verwenden, die mit der AWS-Instanz verbunden ist. Hierzu werden Loopback-Schnittstellen konfiguriert oder sekundäre IP-Adressen hinzugefügt.

Bei Multi-TXQs gibt es mehrere Übertragungswarteschlangen für den ausgehenden Datenverkehr. Im Beispiel gibt es zwölf TX-Warteschlangen (mit den Nummern 0 bis 11). Mit dieser Konfiguration können Sie jede Warteschlange einzeln überwachen, um festzustellen, ob sie voll ist.

Wenn man sich die Ausgabe anschaut, sieht man, dass die TX Queue 8 einen sehr hohen "Voll"-Zähler (56.406.998) hat, was bedeutet, dass ihr Puffer sich häufig füllt. Die anderen TX-Warteschlangen zeigen Null für den Zähler "Voll" an, was darauf hinweist, dass sie nicht überlastet sind.

```
Router#show platform hardware qfp active datapath infrastructure sw-cio
pmd b17a2f00 device Gi2
RX: pkts 9525 bytes 1229599 return 0 badlen 0
Out-of-credits: Hi 0 Lo 0
pkts/burst 1 cycl/pkt 560 ext_cycl/pkt 360
Total ring read 117322273, empty 117312792
TX: pkts 175116324 bytes 246208197526
pri-0: pkts 157 bytes 10238
pkts/send 1
pri-1: pkts 75 bytes 4117
pkts/send 1
pri-2: pkts 91 bytes 6955
pkts/send 1
pri-3: pkts 95 bytes 8021
pkts/send 1
pri-4: pkts 54 bytes 2902
pkts/send 1
pri-5: pkts 75 bytes 4082
pkts/send 1
pri-6: pkts 104 bytes 8571
pkts/send 1
pri-7: pkts 74 bytes 4341
pkts/send 1
pri-8: pkts 175115328 bytes 246208130411
pkts/send 2
pri-9: pkts 85 bytes 7649
pkts/send 1
pri-10: pkts 106 bytes 5784
pkts/send 1
pri-11: pkts 82 bytes 7267
pkts/send 1
Total: pkts/send 2 cycl/pkt 203
send 68548581 sendnow 175024880
forced 1039215617 poll 1155226129 thd_poll 0
blocked 2300918060 retries 68534370 mbuf alloc err 0
TX Queue 0: full 0 current index 0 hiwater 0
TX Queue 1: full 0 current index 0 hiwater 0
```

```
TX Queue 2: full 0 current index 0 hiwater 0
TX Queue 3: full 0 current index 0 hiwater 0
TX Queue 4: full 0 current index 0 hiwater 0
TX Queue 5: full 0 current index 0 hiwater 0
TX Queue 6: full 0 current index 0 hiwater 0
TX Queue 7: full 0 current index 0 hiwater 0
TX Queue 8: full 56406998 current index 224 hiwater 224 <<<<<<<<<<
TX Queue 9: full 0 current index 0 hiwater 0
TX Queue 10: full 0 current index 0 hiwater 0
TX Queue 11: full 0 current index 0 hiwater 0
```

Durch die Überwachung der vollständigen Zähler von TX-Warteschlangen kann festgestellt werden, ob eine Übertragungswarteschlange überlastet ist. Eine konstant steigende "vollständige" Zählung einer bestimmten TX-Warteschlange deutet auf einen Datenverkehrsfluss hin, der das Gerät belastet. Hierzu gehören Datenverkehrsausgleich, das Anpassen von Konfigurationen oder das Skalieren von Ressourcen zur Verbesserung der Leistung.

Kennzahlen überschritten

AWS legt bestimmte Netzwerkgrenzen auf Instanzebene fest, um eine konsistente und qualitativ hochwertige Netzwerkleistung über verschiedene Instanzgrößen hinweg sicherzustellen. Diese Einschränkungen tragen dazu bei, die Stabilität des Netzwerks für alle Benutzer aufrechtzuerhalten.

Sie können diese Grenzwerte und zugehörige Statistiken mit dem Befehl show controllers (Controller anzeigen) auf Ihrem Gerät überprüfen. Die Ausgabe enthält viele Zähler. Hier konzentrieren wir uns jedoch nur auf die wichtigsten Zähler für die Überwachung der Netzwerkleistung:

```
c8kv-2#sh control | inc exceed
<snipped>
bw_in_allowance_exceeded 0
bw_out_allowance_exceeded 0
pps_allowance_exceeded 0
conntrack_allowance_exceeded 0
linklocal_allowance_exceeded 0
<snipped>
```

Sie können jetzt eintauchen und sehen, worauf sich diese Zähler genau beziehen:

- bw_in_zuschlag_überschritten: Anzahl der Pakete, die in die Warteschlange eingereiht oder wegen Überschreitung der Instanzgrenze durch die eingehende Bandbreite verworfen wurden
- bw_out_limit_überschritten: Anzahl der Pakete, die in die Warteschlange eingereiht oder verworfen wurden, weil die ausgehende Bandbreite den Grenzwert der Instanz überschritten hat.
- pps_zuschlag_überschritten: Anzahl der in die Warteschlange eingereihten oder

verworfenen Pakete, da die Gesamtpaketanzahl pro Sekunde (PPS) den Grenzwert der Instanz überschreitet.
- conntrack_limit_überschritten: Anzahl der verfolgten Verbindungen, die den für den Instanztyp maximal zulässigen Wert erreicht haben.
- linklocal_limit_überschritten: Anzahl der wegen Überschreitung des PPS-Grenzwerts für die Netzwerkschnittstelle durch den Datenverkehr zu lokalen Proxydiensten (wie Amazon DNS, Instance Metadata Service und Time Sync Service) verworfenen Pakete Benutzerdefinierte DNS-Resolver sind davon nicht betroffen.

Dies bedeutet für Ihre C8000v-Leistung Folgendes:

- Wenn Sie feststellen, dass diese Zähler ansteigen und Leistungsprobleme auftreten, bedeutet dies nicht immer, dass der C8000v-Router das Problem ist. Stattdessen weist es häufig darauf hin, dass die von Ihnen verwendete AWS-Instanz ihre Kapazitätsgrenzen erreicht hat. Sie können die Spezifikationen Ihrer AWS-Instanz überprüfen, um sicherzustellen, dass sie Ihren Datenverkehrsanforderungen gerecht werden kann.

Microsoft Azure

In diesem Abschnitt erfahren Sie, wie Microsoft Azure und der virtuelle Router Cisco C8000v gemeinsam skalierbare, sichere und leistungsstarke virtuelle Netzwerklösungen in der Cloud bereitstellen.

Gehen Sie durch, wie sich Accelerated Networking (AN) und Paketfragmentierung auf die Leistung auswirken können. Außerdem müssen Sie überprüfen, wie wichtig die Verwendung eines unterstützten Instanzentyps für Microsoft Azure ist.

Schnellere Netzwerke

Bei Leistungsproblemen, bei denen der C8000v in der Microsoft Azure Cloud gehostet wird. Ein Aspekt, den Sie nicht übersehen können, ist, ob Accelerated Network aktiviert ist. da dies die Leistung des Routers erheblich steigert. Auf den Punkt gebracht: Beschleunigte Netzwerkfunktionen ermöglichen eine Single-Root-E/A-Virtualisierung (SR-IOV) auf VMs wie dem Cisco Catalyst 8000V VM. Der beschleunigte Netzwerkpfad umgeht den virtuellen Switch, erhöht die Geschwindigkeit des Netzwerkverkehrs, verbessert die Netzwerkleistung und reduziert Netzwerklatenz und Jitter.

Es gibt eine sehr einfache Möglichkeit zu überprüfen, ob Accelerated Network aktiviert ist. Mit dieser Funktion können Sie die Ausgabe der Kontroller anzeigen und überprüfen, ob bestimmte Zähler vorhanden sind:

```
------------------ show controllers ------------------

GigabitEthernet1 - Gi1 is mapped to UIO on VXE
  rx_good_packets 6497723453
  tx_good_packets 14690462024
  rx_good_bytes 2271904425498
  tx_good_bytes 6276731371987
```

```
rx_q0_good_packets 58576251
rx_q0_good_bytes 44254667162
```

```
vf_rx_good_packets 6439147188
vf_tx_good_packets 14690462024
vf_rx_good_bytes 2227649747816
vf_tx_good_bytes 6276731371987
```

Die gesuchten Leistungsindikatoren sind diejenigen, die mit vf beginnen, z. B. vf_rx_good_packages. Wenn Sie überprüfen, ob diese Leistungsindikatoren vorhanden sind, können Sie absolut sicher sein, dass die beschleunigte Netzwerkfunktion aktiviert ist.

Azure und Fragmentierung

Eine Fragmentierung kann negative Auswirkungen auf die Leistung haben. Einer der Hauptgründe für die Auswirkungen auf die Leistung ist der CPU-/Speichereffekt der Fragmentierung und Reassemblierung von Paketen. Wenn ein Netzwerkgerät ein Paket fragmentieren muss, muss es CPU-/Speicherressourcen zuweisen, um die Fragmentierung durchzuführen.

Das Gleiche geschieht, wenn das Paket wieder zusammengesetzt wird. Das Netzwerkgerät muss alle Fragmente speichern, bis sie empfangen werden, damit es sie wieder in das ursprüngliche Paket einbauen kann.

Azure verarbeitet keine fragmentierten Pakete mit Accelerated Networking. Wenn eine VM ein fragmentiertes Paket empfängt, wird es vom nicht beschleunigten Pfad verarbeitet. Daher verpassen fragmentierte Pakete die Vorteile von Accelerated Networking, wie z. B. geringere Latenz, weniger Jitter und höhere Pakete pro Sekunde. Aus diesem Grund wird empfohlen, eine Fragmentierung möglichst zu vermeiden.

Azure verwirft standardmäßig fragmentierte Pakete, die nicht in der richtigen Reihenfolge an das virtuelle System gesendet werden, was bedeutet, dass die Pakete nicht mit der Übertragungssequenz vom Quellendpunkt übereinstimmen. Dieses Problem kann auftreten, wenn Pakete über das Internet oder andere große WANs übertragen werden.

Unterstützte Instanztypen für Microsoft Azure

Es ist wichtig, dass der C8000v einen unterstützten Instanztyp gemäß den Cisco Standards verwendet. Sie finden sie im Cisco Catalyst 8000V Edge Software Installation And Configuration

Guide.

Der Grund dafür ist, dass die Instanztypen in dieser Liste diejenigen sind, bei denen C8KV ordnungsgemäß getestet wurde. Nun stellt sich die gültige Frage, ob der C8000v mit einem Instanztyp funktioniert, der nicht aufgeführt ist. Die Antwort ist höchstwahrscheinlich ja. Wenn Sie jedoch eine so komplexe Fehlerbehebung wie Leistungsprobleme durchführen, möchten Sie dem Problem keinen weiteren unbekannten Faktor hinzufügen. Allein aus diesem Grund empfiehlt Cisco TAC Ihnen stets, in einem unterstützten Instanzentyp zu bleiben.

Zusätzliche Ressourcen

Ein Leistungsproblem kann nur dann wirklich behoben werden, wenn es gerade auftritt. Dies kann jedoch schwierig zu erfassen sein, da es zu einem bestimmten Zeitpunkt passieren kann. Aus diesem Grund stellen wir dieses EEM-Skript bereit. Es hilft, wichtige Ausgaben zu erfassen, sobald Pakete verworfen werden und Leistungsprobleme auftreten:

```
ip access-list extended TAC
permit ip host  host



permit ip host



          host



conf t
event manager applet CONNECTIONLOST1 authorization bypass
event track 100 state down maxrun 500
action 0010 syslog msg "Logging information to file bootflash:SLA-DROPS.txt and bootflash:FIASLA_Decode
action 0020 cli command "enable"
action 0021 cli command "term length 0"
action 0022 cli command "term exec prompt timestamp"
action 0023 cli command "term exec prompt expand"
action 0095 cli command "show clock | append bootflash:SLA-DROPS.txt"
action 0096 cli command "show platform hardware qfp active statistics drop detail | append bootflash:SL
action 0097 cli command "show logging | append bootflash:SLA-DROPS.txt"
action 0099 cli command "show interfaces summary | append bootflash:SLA-DROPS.txt"
action 0100 cli command "show interfaces | append bootflash:SLA-DROPS.txt"
action 0101 cli command "show platform hardware qfp active statistics drop clear"
action 0102 cli command "debug platform packet-trace packet 2048 fia-trace"
action 0103 cli command "debug platform packet-trace copy packet both"
action 0104 cli command "debug platform condition ipv4 access-list TAC both"
action 0105 cli command "debug platform condition start"
action 0106 cli command "show platform hardware qfp active data infrastructure sw-cio | append bootflas
action 0110 wait 60
action 0111 cli command "debug platform condition stop"
action 0112 cli command "show platform packet-trace packet all decode | append bootflash:FIASLA_Decode.
action 0120 cli command "show platform packet-trace statistics | append bootflash:FIASLA_Decode.txt"
action 0121 cli command "show platform packet-trace summary | append bootflash:FIASLA_Decode.txt"
action 0122 cli command "show platform hardware qfp active datapath utilization summary | append bootfl
```

```
action 0123 cli command "show platform hardware qfp active statistics drop detail | append bootflash:SL
action 0124 cli command "show platform hardware qfp active infrastructure bqs queue output default all
action 0125 cli command "show platform software status control-processor brief | append bootflash:SLA-D
action 0126 cli command "show platform hardware qfp active datapath infrastructure sw-pktmem | append b
action 0127 cli command "show platform hardware qfp active infrastructure punt statistics type per-caus
action 0128 cli command "show platform hardware qfp active statistics drop | append bootflash:SLA-DROPS
action 0129 cli command "show platform hardware qfp active infrastructure bqs queue output default all
action 0130 cli command "show platform hardware qfp active data infrastructure sw-hqf config 0 0 | appe
action 0131 cli command "show platform hardware qfp active feature lic-bw oversubscription | append boo
action 0132 cli command "show platform hardware qfp active data infrastructure sw-hqf config 0 0 | appe
action 0133 cli command "show platform hardware qfp active data infrastructure sw-cio | append bootfla
action 0134 cli command "show platform hardware qfp active data infrastructure sw-hqf sched | append bo
action 0135 cli command "show platform hardware qfp active data infrastructure sw-dist | append bootfl
action 0136 cli command "show platform hardware qfp active data infrastructure sw-nic | append bootfla
action 0137 cli command "show platform hardware qfp active data infrastructure sw-pktmem | append bootf
action 0138 cli command "show controllers | append bootflash:SLA-DROPS.txt"
action 0139 cli command "show platform hardware qfp active datapath pmd controllers | append bootflash:
action 0140 cli command "show platform hardware qfp active datapath pmd system | append bootflash:SLA-D
action 0141 cli command "show platform hardware qfp active datapath pmd static-if-config | append bootf
action 0150 cli command "clear platform condition all"
action 0151 cli command "clear platform packet-trace statistics"
action 0152 cli command "clear platform packet-trace configuration"
action 0153 cli command "show log | append bootflash:througput_levelinfoSLA.txt"
action 0154 cli command "show version | append bootflash:througput_levelinfoSLA.txt"
action 0155 cli command "show platform software system all | append bootflash:througput_levelinfoSLA.tx
action 0156 syslog msg "EEM script and FIA trace completed."
action 0180 cli command "conf t"
action 0181 cli command "no event manager applet CONNECTIONLOST1"
end
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.