Problemen met de prestaties van C8000v-routers oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met de prestaties van C8000v-bedrijfsrouters in openbare clouds en ESXi-scenario's kunt oplossen.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwarecomponenten:

- C8000v met versie 10 .12
- ESXI versie 7.0 U3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Algemene probleemoplossing

Hoewel u uw C8000v in verschillende omgevingen kunt laten hosten, zijn er nog steeds een paar stappen voor probleemoplossing die u kunt doorlopen die identiek zijn, ongeacht waar de C8000v

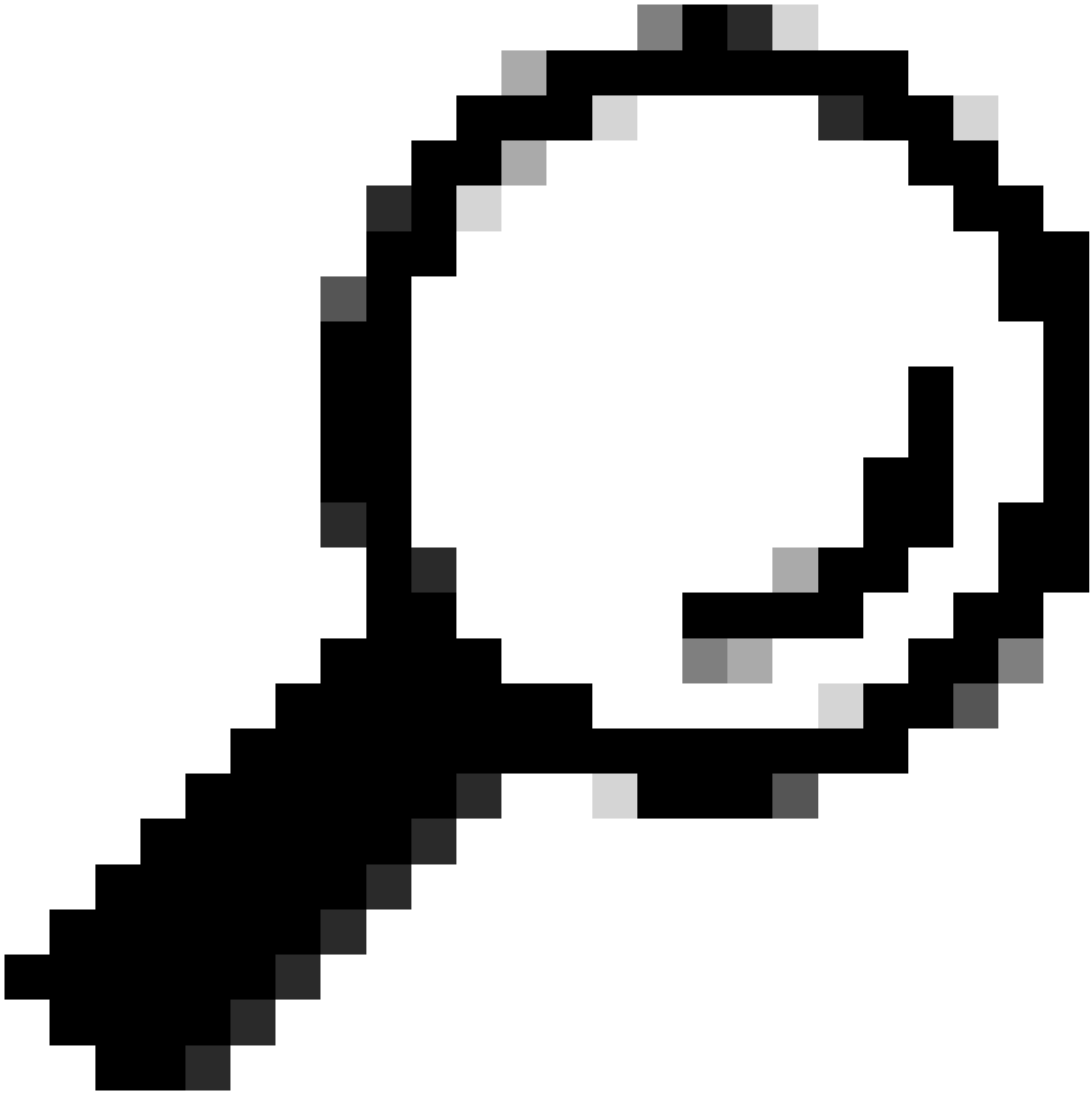
wordt gehost. Laten we beginnen met de basis. Het eerste wat u moet controleren is of het apparaat zijn capaciteitslimieten bereikt of niet. Hiervoor kunt u beginnen met het controleren van deze twee uitgangen:

1. Platform hardware qfp active datapath util samenvatting weergeven – Deze opdracht geeft u de volledige informatie van de invoer/uitvoer die de C8000v ontvangt en verzendt vanuit elke poort. U moet uw aandacht richten op het percentage verwerkingsbelasting. Als u zich in een scenario bevindt waarin u 100% bereikt, betekent dit dat u de capaciteitslimiet bereikt

```
------------------ 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. toon platformhardware qfp active datapath infrastructure sw-cio – Beschouw deze opdracht als een meer diepgaande versie van de bovenstaande. Het biedt meer details over de afzonderlijke cores, waaronder de IO- en crypto-cores die geen deel uitmaken van het QFP-gebruiksnummer. Het is erg handig in een scenario waarin u wilt zien of een specifieke kern van een gegevensvliegtuig een knelpunt veroorzaakt.



Tip: Een zeer belangrijk detail bij het gebruik van deze opdracht, altijd twee keer uitvoeren. Als het berekent het percentage core gebruik tussen de tijd dat de opdracht werd uitgevoerd.

```
------------------ 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.
```

Nu heb je bepaald of je de platformlimiet bereikt of niet. De volgende stap zou zijn om te controleren op druppels. Deze zijn inherent verbonden met prestatieproblemen. Er zijn drie soorten druppels die u kunt overwegen, afhankelijk van waar ze zich voordoen.

- Overschrijdingen: Dit type pakketdrop vindt plaats aan het Rx-einde. Dit gebeurt omdat de verwerkingscapaciteit van een of meer kernen is overschreden.
- Feature drops: Dit type packet drop komt voor in de PPE. Ze zijn gerelateerd aan functies in de router zoals een ACL of QoS.
- Staartdruppels: Dit type pakketdruppels vindt plaats in het Tx-uiteinde. Ze ontstaan door congestie in de Tx-buffers.

Om te bepalen welke druppels u ervaart, kunt u de volgende uitgangen gebruiken:

- Platform Hardware QFP Active Drop State Wissen weergeven
- show interface
- interface voor beleidskaart weergeven

U controleert hoe u kunt identificeren welke druppels u tegenkomt en hoe u ze kunt verzachten. Toch zal de grootste focus in dit artikel de druppels zijn die bekend staan als Taildrops, omdat ze bijzonder lastig zijn om problemen op te lossen in virtuele routers.

overschrijdingen

Een overschrijding van Cisco IOS XE treedt op wanneer de netwerkinterface pakketten sneller ontvangt dan deze kan verwerken of opslaan in de buffer. Concreet worden de interne buffers van de interfaces (FIFO-wachtrij) vol omdat de binnenkomende gegevenssnelheid groter is dan de capaciteit van de hardware om deze aan te kunnen. Als gevolg hiervan kunnen nieuwe inkomende pakketten niet worden opgeslagen en worden verwijderd, waardoor de overschrijdingsteller wordt verhoogd. Dit is in wezen een pakketverlies dat wordt veroorzaakt doordat de interface tijdelijk wordt overweldigd.

Dit soort pakketdruppels komen voor op het Rx-uiteinde. Ze gebeuren omdat de verwerkingscapaciteit van een of meer kernen is overschreden en Rx-thread niet in staat is om inkomende pakketten te distribueren naar de relevante PP-thread en de ingangsbuffers al vol zijn. Om een eenvoudige analogie te maken, kun je het zien als een wachtrij bij een kassa die te vol

wordt omdat pakketten sneller aankomen dan de kassier (interface-hardware) ze kan bedienen. Wanneer de wachtrij vol is, moeten nieuwe klanten vertrekken zonder te worden bediend - dit zijn de overschrijdingen.

Hoewel hardware in dit gedeelte wordt genoemd, is de C8000v een op software gebaseerde router. In dit geval kunnen overschrijdingen worden veroorzaakt door:

- Hoog gebruik van het gegevensvliegtuig: als het gebruik van het gegevensvliegtuig hoog is, kunnen de pakketten niet snel genoeg worden gepolst, wat leidt tot overschrijdingen. De aanwezigheid van "olifantenstromen" (grote, continue gegevensstromen) kan bijvoorbeeld verwerkingsbronnen verzadigen en overschrijdingen op interfaces veroorzaken.
- Onjuist apparaatsjabloon: het gebruik van een ongeschikte apparaatsjabloon kan leiden tot inefficiënt bufferbeheer en overschrijdingen. Dit kan worden gecontroleerd met de opdracht Toon platform software cpu toegewezen en het kan worden gewijzigd met de platform resource <template> opdracht.

Elke interface krijgt een beperkte pool van credits toegewezen, dit mechanisme voorkomt een drukke interface en overbelasting van de systeembronnen. Elke keer dat een nieuw pakket in het dataplane arriveert, is een tegoed vereist. Wanneer de pakketverwerking is voltooid, wordt het tegoed geretourneerd zodat Rx thread het opnieuw kan gebruiken. Als er geen krediet beschikbaar is voor de interface, moet het pakket wachten in de Rx-ring van de interface. Over het algemeen verwacht je dat de prestatiegrens gerelateerd aan dalingen Rx-overschrijdingen zijn omdat de verwerkingscapaciteit van een of meer kernen is overschreden.

Om overschrijdingen te identificeren, controleert u meestal de interfacestatistieken op invoerfouten, met name de overschrijdingsteller:

- Gebruik de opdracht show platform hardware qfp active datapath infrastructure sw-cio om het kerngebruik te identificeren en als het aantal credits voor een specifieke interface is overschreden.
- Gebruik de opdracht show interface <interface-naam> en zoek naar de overschrijding telling in de uitvoer.

Overschrijdingen worden weergegeven als onderdeel van invoerfouten, bijvoorbeeld:

```
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 <<<<<<<<<<<
```

Laten we een geval veronderstellen waarin Gig2 prestatieproblemen observeert die worden veroorzaakt door overschrijdingen. Om de werkthread te bepalen die aan deze interface is gekoppeld, kunt u de volgende opdracht gebruiken:

```
#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
```

Vervolgens kunt u het gebruik van de specifieke thread analyseren die verantwoordelijk is voor het Rx-verkeer van deze interface en het aantal credits.

In een scenario waarin Gig2 prestatieproblemen als gevolg van overschrijdingen observeert, kunt u verwachten dat de PP # 2 constant volledig wordt gebruikt (Inactief = 0%) en lage / nul credits voor interface Gig2:

```
#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
```

Feature Drops

Pakketten worden behandeld door elke beschikbare data plane thread en worden strikt verdeeld op basis van de beschikbaarheid van QFP-cores via software Rx-functie (x86) - Load Based Distribution (LBD). Pakketten die in de PPE aankomen, kunnen worden gedropt met een specifieke QFP-dropreden, die kan worden gecontroleerd met behulp van deze uitvoer:

```
#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
```

De redenen voor de druppels zijn divers en zijn meestal voor zichzelf sprekend. Om verder te onderzoeken kan een packet trace worden gebruikt.

Staartdruppels

Zoals eerder vermeld, vallen vallen op waar het apparaat pakketten probeert te verzenden, maar de transmissiebuffers zijn vol.

In deze subsectie gaat u kijken naar welke uitgangen u kunt onderzoeken wanneer u met dit soort situaties wordt geconfronteerd. Welke waarden u erin kunt zien, betekenen en wat u kunt doen om het probleem te beperken.

Eerst moet je weten hoe je ze kunt identificeren. Een van die manieren is om gewoon naar de showinterface te kijken. Houd een oogje in het zeil voor elke output druppels verhogen:

```
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
```

Deze opdracht is vooral handig om te begrijpen of u congestie ervaart of niet:

- Toon platformhardware qfp active datapath infrastructure - HQF staat voor `Hierarchical Queueing Framework`. Dit is een functie die Quality of Service (QoS)-beheer op verschillende niveaus (fysiek, logisch en klasse) mogelijk maakt met behulp van de modulaire QoS-opdrachtregelinterface (MQC). Het toont de huidige RX- en TX-kosten. Wanneer de TX-wachtrij vol is, zoals de uitvoer laat zien (volledig 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
```

De output suggereert dat de onderliggende hardware niet bijhoudt met het verzenden van pakketten. Om de onderliggende interface te debuggen, moet u mogelijk buiten de C8000v kijken en naar de onderliggende omgeving waar de C8000v wordt uitgevoerd om te zien of er extra fouten zijn gemeld op de onderliggende fysieke interfaces.

Om de omgeving te controleren, kunt u één stap doen voordat u controleert welke hypervisor de C8000v-router wordt uitgevoerd. Dit is om de uitvoer van de controleur te controleren. Toch kun je jezelf verloren vinden op wat elke teller betekent of waar je naar moet kijken.

Ten eerste is een belangrijk detail dat u in gedachten moet houden wanneer u naar deze uitvoer kijkt, dat de informatie meestal afkomstig is van de vNIC's zelf. Elke NIC-driver heeft een specifieke set tellers die ze gebruiken, die natuurlijk per driver kunnen verschillen. Verschillende hypervisors hebben ook een soort effect op wat wordt gepresenteerd. Sommige tellers, zoals mbuf-tellers, zijn statistieken van het DPDK-stuurprogramma. Deze kunnen variëren voor verschillende DPDK-stuurprogramma's. Het werkelijke aantal wordt meestal geteld door de hypervisor op de virtualisatielaag.

```
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
```

Neem hier een minuut de tijd om te leren hoe u deze tellers kunt interpreteren en lezen:

1. Als u subX ziet, betekent dit dat het een sub-interface is - een logische verdeling van de hoofdinterface. De sub0 is over het algemeen de primaire / standaardversie. Deze worden vaak gebruikt wanneer er meerdere VLAN's bij betrokken zijn.
2. Dan heb je "rx = ontvangen" en "tx = verzenden".
3. Ten slotte verwijst q0 naar de eerste/standaardwachtrij die door die interface wordt gebruikt

Hoewel er geen beschrijving is voor elke teller, beschrijft het artikel enkele van hen, die relevant kunnen zijn voor uw probleemoplossing:

- "RX_MISSED_ERRORS:" wordt weergegeven wanneer de NIC-buffer (Rx FIFO) overvol raakt. Deze aandoening leidt tot dalingen en een toename van de latentie. Een mogelijke oplossing hiervoor is het verhogen van de NIC-buffer (wat in ons geval onmogelijk is) of het wijzigen van het NIC-stuurprogramma.
- "tx_q0_drop_total" en "tx_q0_tx_ring_full": Deze kunnen u vertellen dat de host pakketten laat vallen en dat de C8000v Tail Drops in de C8000v ervaart omdat de host de C8000v onder druk zet

In de bovenstaande uitvoer zien we geen "rx_missed_errors". Echter, aangezien we ons richten op taildrops zien we zowel "tx_q0_drop_total" als "tx_q0_tx_ring_full". Hiermee kunnen we concluderen dat er inderdaad congestie is veroorzaakt door de onderliggende hardware van de host.

Zoals eerder vermeld, heeft elke hypervisor een soort effect op wat wordt gepresenteerd. Het artikel richt zich op dit in de volgende sectie als het gaat over de verschillen tussen de verschillende hypervisors waar de C8000v kan worden gehost. U kunt ook de verschillende aanbevelingen vinden om te proberen dit soort problemen in elk van hen te verminderen.

Hypervisors

Een hypervisor is een softwarelaag waarmee meerdere besturingssystemen (virtuele machines of

VM's genoemd) op één fysieke hardwarehost kunnen worden uitgevoerd door de hardwarebronnen zoals CPU, geheugen en opslag aan elke VM te beheren en toe te wijzen. Het zorgt ervoor dat deze virtuele machines onafhankelijk van elkaar werken zonder elkaar te verstoren.

In het kader van de Cisco Catalyst 8000V (C8000v) is de hypervisor het platform waarop de C8000v virtuele machine wordt gehost. Hoe weet u welke hypervisor uw C8000v host? Er is een vrij nuttige output die ons die informatie geeft. Bovendien kunt u ook controleren tot welke bronnen onze virtuele router toegang heeft:

```
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
```

ESXi van VMware

ESXi is een type-1 hypervisor ontwikkeld door VMware die direct op fysieke servers is geïnstalleerd om virtualisatie mogelijk te maken. Hiermee kunnen meerdere virtuele machines (VM's) op één fysieke server worden uitgevoerd door de hardwarebronnen te abstraheren en aan elke VM toe te wijzen. De C8000v-router is een van die VM's.

U kunt beginnen met het doorlopen van een gemeenschappelijk scenario waar congestie optreedt. Dit kan worden bevestigd door de tx_q0_tx_ring_full-teller te controleren:

Voorbeeld:

```
------------------ 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 <------
```

Deze congestie treedt op wanneer de C8000V probeert pakketten via de VMXNET3-interface te verzenden. De bufferring zit echter al vol met pakketten, die in vertragingen of dalingen terechtkomen.

Onder deze omstandigheden gebeuren die druppels aan de hypervisorzijde zoals we eerder hebben vermeld. Als aan alle aanbevelingen is voldaan, wordt aanbevolen om VMware-ondersteuning te raadplegen om te begrijpen wat er op de NIC gebeurt.

Hier zijn enkele suggesties om de prestaties te verbeteren:

- Gebruik een speciale vSwitch en uplink voor optimale prestaties
- Door de C8000V toe te wijzen aan een speciale vSwitch die wordt ondersteund door zijn eigen fysieke uplink, kunnen we het verkeer van luidruchtige buren isoleren en knelpunten met gedeelde bronnen voorkomen.

Er zijn een paar commando's die de moeite waard zijn om te bekijken vanaf de ESXi-kant. Om

bijvoorbeeld te controleren op pakketverlies via de ESXi-interface, kunnen we het volgende doen:

1. SSH inschakelen.
2. Maak verbinding met ESXi via SSH.
3. Voer de desktop uit.
4. Type n.

De opdracht esxtop kan pakketten weergeven die zijn gedropt op de virtuele switch als het netwerkstuurprogramma van de virtuele machine geen Rx-buffergeheugen meer heeft. Hoewel esxtop laat zien dat de pakketten zijn gedropt bij de virtual switch, worden ze eigenlijk gedropt tussen de virtual switch en het gaststuurprogramma van het besturingssysteem.

Zoek naar pakketten die worden verwijderd onder %DRPTX en %DRPRX:

```
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 (
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
```

Met deze opdracht worden alle NIC's weergegeven die op een host zijn geconfigureerd:

```
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
```

Er is ook een handige opdracht om de status te controleren van de vNIC die aan een bepaalde VM is toegewezen.

```
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:~]
```

Kijkend naar de c8kv-gw-mgmt, dat is een C8000v VM, zijn er 2 Netwerken toegewezen:

- C8KV-T/M-9200L
- C8KV-naar-Cisco

U kunt de wereld-ID gebruiken om meer informatie over deze VM te zoeken:

```
[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:~]
```

Zodra u deze informatie hebt, kunt u identificeren aan welk netwerk de vSwitch is toegewezen.

Om enkele verkeersstatistieken van de fysieke NIC die aan de vSwitch is toegewezen te controleren, hebben we de volgende opdracht:

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

Deze opdracht geeft informatie weer zoals ontvangen pakketten, ontvangen bytes, gedropte pakketten en ontvangen fouten. Dit kan helpen om vast te stellen of er druppels optreden bij de NIC.

```
[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
```

Er zijn een paar configuraties die moeten worden geverifieerd om de prestaties van de Cisco Catalyst 8000V in een ESXi-omgeving te verbeteren door de instellingen op de host en de virtuele machine aan te passen:

- Stel de virtuele hardware: CPU-reserveringsinstelling in op Maximum.
- Reserveer al het gastgeheugen in Virtual Hardware: Memory.
- Selecteer VMware Paravirtual van Virtual Hardware: SCSI-controller.
- Selecteer SR-IOV voor de ondersteunde NIC's in de optie Virtuele hardware: netwerkadapter: adaptertype
- Stel de optie General Guest OS Version > VM Options in op Other 3.x of later Linux (64-

bits).
- Stel de optie VM-opties onder Geavanceerde latentiegevoeligheid in op Hoog.
- Voeg onder VM-opties > Geavanceerde configuratie bewerken "numa.nodeAffinity" toe aan dezelfde NUMA-node als de SRIOV-NIC
- Schakel de hypervisorinstellingen in.
- Beperk de overhead van vSwitch door SR-IOV in te schakelen op de ondersteunde fysieke NIC's.
- De vCPU's van de VM configureren om op dezelfde NUMA-node als fysieke NIC's te worden uitgevoerd.
- Stel de VM-latentiegevoeligheid in op Hoog.

AWS

De C8000v ondersteunt implementatie op AWS door te starten als een Amazon Machine Image (AMI) binnen een Amazon Virtual Private Cloud (VPC), waardoor gebruikers een logisch geïsoleerd gedeelte van de AWS-cloud kunnen bieden voor hun netwerkbronnen.

Multi-TX wachtrijen

In een C8000v die op AWS draait, is het gebruik van Multi-TX Queues (Multi-TXQs) een belangrijke functie. Deze wachtrijen helpen de interne verwerkingsoverhead te verminderen en de schaalbaarheid te verbeteren. Meerdere wachtrijen maken het sneller en eenvoudiger om inkomende en uitgaande pakketten toe te wijzen aan de juiste virtuele CPU (vCPU).

In tegenstelling tot sommige systemen waarin RX/TX-wachtrijen per vCPU worden toegewezen, worden deze wachtrijen in de C8000v toegewezen per interface. De RX- (ontvangst) en TX-wachtrijen (verzenden) dienen als de verbindingspunten tussen de Catalyst 8000V-toepassing en de AWS-infrastructuur of -hardware en beheren hoe netwerkverkeer wordt verzonden en ontvangen. AWS bepaalt het aantal en de snelheid van RX/TX-wachtrijen die beschikbaar zijn voor elke interface, afhankelijk van het instantietype.

Om meerdere TX-wachtrijen te maken, moet de Catalyst 8000V meerdere interfaces hebben. Wanneer meerdere TX-wachtrijen zijn ingeschakeld, behoudt het apparaat de volgorde van pakketstromen door een hashingmethode te gebruiken die is gebaseerd op de 5-voudige van de stroom (bron-IP, bestemming-IP, bronpoort, bestemmingspoort en protocol). Deze hashing bepaalt welke TX-wachtrij moet worden gebruikt voor elke stroom.

Gebruikers kunnen meerdere interfaces op de Catalyst 8000V maken met dezelfde fysieke netwerkinterfacekaart (NIC) die is aangesloten op de AWS-instantie. Dit wordt gedaan door loopback-interfaces te configureren of secundaire IP-adressen toe te voegen.

Met Multi-TXQ's zijn er meerdere zendwachtrijen om uitgaand verkeer af te handelen. In het voorbeeld zijn er twaalf TX wachtrijen (genummerd 0 tot 11). Met deze instelling kunt u elke wachtrij afzonderlijk controleren om te zien of er wachtrijen vol raken.

Als u naar de uitvoer kijkt, ziet u dat TX Queue 8 een zeer hoge "volledige" teller heeft (56.406.998), wat betekent dat de buffer vaak wordt gevuld. De andere TX-wachtrijen tonen nul voor de "volledige" teller, wat aangeeft dat ze niet overbelast zijn.

```
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
```

Door de "volledige" tellers van TX-wachtrijen te bewaken, kunt u vaststellen of een verzendwachtrij overbelast is. Een constant toenemende "volledige" telling op een bepaalde TX-

wachtrij wijst op een verkeersstroom die het apparaat benadrukt. Om dit aan te pakken, kan het gaan om het balanceren van het verkeer, het aanpassen van configuraties of het schalen van bronnen om de prestaties te verbeteren.

Statistieken overschreden

AWS stelt bepaalde netwerklimieten in op instantieniveau om consistente en hoogwaardige netwerkprestaties voor verschillende instantiegroottes te garanderen. Deze limieten helpen een stabiel netwerk voor alle gebruikers te behouden.

U kunt deze limieten en bijbehorende statistieken controleren met de opdracht Controllers weergeven op uw apparaat. De output bevat veel tellers, maar hier richten we ons alleen op de belangrijkste voor het bewaken van netwerkprestaties:

```
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>
```

Je kunt nu induiken en zien waar die tellers precies naar verwijzen:

- bw_in_allowance_exceeded: Aantal pakketten dat in de wachtrij staat of is gevallen omdat de binnenkomende bandbreedte de limiet van de instantie heeft overschreden.
- bw_out_allowance_exceeded: Aantal pakketten dat in de wachtrij staat of is weggevallen omdat de uitgaande bandbreedte de limiet van de instantie heeft overschreden.
- pps_allowance_exceeded: Aantal pakketten dat in de wachtrij staat of is gevallen omdat het totaal aantal pakketten per seconde (PPS) de limiet van de instantie heeft overschreden.
- conntrack_allowance_exceeded: Aantal getraceerde verbindingen dat het maximaal toegestane aantal voor het instantietype heeft bereikt.
- linklocal_allowance_exceeded: Aantal pakketten is gedaald omdat het verkeer naar lokale proxyservices (zoals Amazon DNS, Instance Metadata Service en Time Sync Service) de PPS-limiet voor de netwerkinterface heeft overschreden. Dit heeft geen invloed op aangepaste DNS-resolvers.

Wat dit betekent voor uw C8000v-prestaties:

- Als u merkt dat deze tellers toenemen en prestatieproblemen ondervinden, betekent dit niet altijd dat de C8000v-router het probleem is. In plaats daarvan geeft het vaak aan dat de AWS-instantie die u gebruikt zijn capaciteitslimieten heeft bereikt. U kunt de specificaties van uw AWS-instantie controleren om ervoor te zorgen dat deze uw verkeersbehoeften aankan.

Microsoft Azure

Ontdek in dit gedeelte hoe Microsoft Azure en de Cisco C8000v virtuele router samenwerken om schaalbare, veilige en krachtige virtuele netwerkoplossingen in de cloud te leveren.

Bekijk hoe Accelerated Networking (AN) en pakketfragmentatie de prestaties kunnen beïnvloeden. Naast het belang van het gebruik van een ondersteund instantietype voor Microsoft Azure.

Versnelde netwerken

In gevallen van prestatieproblemen waarbij de C8000v wordt gehost in de Microsoft Azure Cloud. Een aspect dat u niet over het hoofd kunt zien, is of Versneld netwerk is ingeschakeld of niet. Dit verhoogt de prestaties van de router aanzienlijk. In een notendop, versnelde netwerken maakt single root I / O virtualisatie (SR-IOV) op VM's zoals een Cisco Catalyst 8000V VM. Het versnelde netwerkpad omzeilt de virtuele switch, verhoogt de netwerksnelheid, verbetert de netwerkprestaties en vermindert de netwerklatentie en -jitter.

Er is een eenvoudige manier om te controleren of Accelerated Network is ingeschakeld. Dat is om de output van de show controllers te controleren en te controleren of een bepaalde tellers aanwezig is of niet:

```
------------------ 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
```

De tellers die u zoekt zijn degenen die beginnen met vf zoals vf_rx_good_packets. Als u controleert of deze tellers aanwezig zijn, kunt u er absoluut zeker van zijn dat versnelde netwerken is ingeschakeld.

Azure en fragmentatie

Fragmentatie kan negatieve gevolgen hebben voor de prestaties. Een van de belangrijkste redenen voor het effect op de prestaties is het CPU / geheugeneffect van de fragmentatie en hermontage van pakketten. Wanneer een netwerkapparaat een pakket moet fragmenteren, moet het CPU-/geheugenbronnen toewijzen om fragmentatie uit te voeren.

Hetzelfde gebeurt wanneer het pakket opnieuw wordt samengesteld. Het netwerkapparaat moet alle fragmenten opslaan totdat ze zijn ontvangen, zodat het ze opnieuw kan samenvoegen in het oorspronkelijke pakket.

Azure verwerkt geen gefragmenteerde pakketten met Accelerated Networking. Wanneer een VM een gefragmenteerd pakket ontvangt, verwerkt het niet-versnelde pad het. Als gevolg hiervan missen gefragmenteerde pakketten de voordelen van versnelde netwerken, zoals lagere latentie, minder jitter en hogere pakketten per seconde. Daarom wordt aanbevolen fragmentatie indien mogelijk te voorkomen.

Azure laat gefragmenteerde pakketten die bij de VM aankomen standaard buiten de orde vallen, wat betekent dat de pakketten niet overeenkomen met de transmissiesequentie van het broneindpunt. Dit probleem kan optreden wanneer pakketten over het internet of andere grote WAN's reizen.

Ondersteunde instantietypen voor Microsoft Azure

Het is belangrijk dat de C8000v een ondersteund instantietype gebruikt volgens Cisco-standaarden. U vindt ze in de installatie- en configuratiehandleiding van de Cisco Catalyst 8000V Edge-software.

De reden hiervoor is dat de instantietypen in die lijst de typen zijn waarbij de C8KV naar behoren is getest. Nu is er de geldige vraag of de C8000v werkt op een instantietype dat niet wordt vermeld? Het antwoord is hoogstwaarschijnlijk ja. Wanneer u echter problemen oplost met iets dat zo complex is als prestatieproblemen, wilt u geen andere onbekende factor toevoegen aan het probleem. Alleen al om die reden raadt Cisco TAC u altijd aan om in een ondersteund instantietype te blijven.

Aanvullende bronnen

Een prestatieprobleem kan alleen echt worden opgelost wanneer het op het moment gebeurt. Dit kan echter moeilijk te vangen zijn, omdat het op elk moment kan gebeuren. Daarom bieden wij dit EEM-script aan. Het helpt om belangrijke outputs vast te leggen op het moment dat pakketten worden weggegooid en prestatieproblemen ontstaan:

```
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 bootflas
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 bootfla
action 0136 cli command "show platform hardware qfp active data infrastructure sw-nic | append bootflas
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.