# Nexus 9000 - Mise à l'échelle du cloud ASIC NX-OS - Procédure SPAN-to-CPU

## Contenu



## Introduction

Ce document décrit les étapes utilisées pour effectuer une capture de paquets SPAN (Switched Port Analyzer) vers CPU sur une série de modules ASIC Cisco Nexus 9000 à l'échelle du cloud. Ce document décrit également les mises en garde courantes rencontrées lors de l'utilisation d'une capture de paquets SPAN à CPU pour dépanner le flux de paquets via un commutateur Cisco Nexus 9000 Cloud Scale.

## Informations générales

Une capture de paquets SPAN-to-CPU permet aux administrateurs réseau de valider rapidement et facilement si des paquets spécifiques entrent et sortent d'un commutateur Cisco Nexus 9000 Cloud Scale. De la même manière qu'une session SPAN ou ERSPAN (Encapsulated Remote SPAN) normale, une session de surveillance SPAN-CPU implique la définition d'une ou de plusieurs interfaces source et directions de trafic. Tout trafic correspondant à la direction (TX, RX ou les deux) définie sur une interface source est répliqué sur le plan de contrôle du périphérique Cisco Nexus 9000. Ce trafic répliqué peut être filtré et analysé à l'aide de l'utilitaire de capture de paquets du plan de contrôle Ethanalyzer ou enregistré sur un périphérique de stockage local pour examen ultérieur.

Cette fonctionnalité est destinée à une utilisation temporaire lors du dépannage du flux de paquets via les commutateurs de la gamme Cisco Nexus 9000. Cisco recommande vivement que les sessions de surveillance SPAN-CPU soient désactivées ou supprimées administrativement lorsqu'elles ne sont pas utilisées activement pour résoudre un problème de flux de paquets. Si vous ne le faites pas, les performances du trafic répliqué sur le réseau risquent d'être dégradées et l'utilisation CPU du commutateur Cisco Nexus 9000 peut être accrue.

### Matériel applicable

La procédure décrite dans ce document s'applique uniquement à ce matériel :

- **Commutateurs fixes Nexus 9200/9300** N9K-C92160YC-XN9K-C92300YCN9K-C92304QCN9K-C92348GC-XN9K-C9236CN9K-C9272QN9K-C9332CN9K-C9364CN9K-C93108TC-EXN9K-C93108TC-EX-24N9K-C93180LC-EXN9K-C93180YC-EXN9K-C93180YC-EX-24N9K-C93108TC-FXN9K-C93108TC-FX-24N9K-C93180YC-FXN9K-C93180YC-FX-24N9K-C9348GC-FXPN9K-C93240YC-FX2N9K-C93216TC-FX2N9K-C9336C-FX2N9K-C9336C-FX2-EN9K-C93360YC-FX2N9K-C93180YC-FX3N9K-C93108TC-FX3PN9K-C93180YC-FX3SN9K-C9316D-GXN9K-C93600CD-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C9332D-GX2B
- **Cartes de ligne de commutation modulaires Nexus 9500** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

## Conditions préalables

### Conditions requises

Cisco vous recommande de comprendre les principes de base de la fonctionnalité SPAN (Ethernet Switched Port Analyzer) sur les commutateurs de la gamme Cisco Nexus 9000. Pour plus d'informations sur cette fonctionnalité, reportez-vous aux documents suivants :

- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 9.3(x)
- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 9.2(x)
- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 7.0(3)I7(x)

### Components Used

Les informations de ce document sont basées sur les commutateurs de la gamme Cisco Nexus 9000 avec l'ASIC évolutif du cloud exécutant la version 9.3(3) du logiciel NX-OS.

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Cavaliers et limitations

Les sessions de surveillance SPAN-CPU comportent certaines restrictions et certaines restrictions à prendre en compte lors du dépannage des flux de paquets. Ce document aborde quelques mises en garde courantes. Pour obtenir une liste complète des directives et des limites, reportez-vous aux documents suivants :

- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 9.3(x)
- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 9.2(x)
- Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 7.0(3)I7(x)

## Limiteur de débit matériel par défaut de 50 kbits/s

Par défaut, les commutateurs de la gamme Cisco Nexus 9000 limitent à 50 kbits/s le débit du trafic répliqué au plan de contrôle via une session de surveillance SPAN-CPU. Cette limitation de débit est effectuée au niveau du moteur ASIC/transfert de l'échelle de cloud et est un mécanisme d'autoprotection permettant de s'assurer que le plan de contrôle du périphérique n'est pas submergé par le trafic répliqué.

La commande **show hardware rate-limiter span** peut être utilisée pour afficher le paramètre actuel du limiteur de débit de la session de surveillance SPAN-to-CPU.

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+------------------
-+  span 50  0 0 0
```

Si le trafic répliqué est abandonné par le limiteur de débit matériel, alors la colonne Abandonné sera une valeur non nulle, comme indiqué dans le résultat ci-dessous :

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+------------------
-+  span 50 0 499136  499136
```

Le limiteur de débit matériel de la session de surveillance SPAN-CPU peut être modifié à l'aide de la commande de configuration globale **hardware rate-limiter span {kbps}**, comme indiqué dans le résultat ci-dessous.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# hardware rate-limiter span 250 N9K-1(config)# end N9K# show running-config | inc
rate-limiter hardware rate-limiter span 250 N9K# show hardware rate-limiter span Units for
Config: kilo bits per second Allowed, Dropped & Total: aggregated bytes since last clear
counters Module: 1 R-L Class Config Allowed Dropped Total +----------------+----------+---------
----------+--------------------+--------------------+  span 250  0 0 0
```

> **Attention** : Cisco ne recommande pas de modifier le limiteur de débit matériel de la session de surveillance SPAN-CPU en l'éloignant de sa valeur par défaut de 50 kbits/s, sauf si le TAC Cisco l'y a explicitement demandé. L'augmentation de ce limiteur de débit à une valeur élevée peut entraîner une augmentation de l'utilisation du CPU et une instabilité du plan de contrôle sur le commutateur de la gamme Cisco Nexus 9000, ce qui pourrait avoir un impact significatif sur le trafic de production.

## Le compteur autorisé du limiteur de débit matériel SPAN-CPU n'est pas pris en charge

La sortie de la commande **show hardware rate-limitspan** contient un compteur Allowed. Sur d'autres limiteurs de débit matériel, ce compteur indique le nombre d'octets qui passent correctement par le limiteur de débit matériel. Cependant, le compteur Allowed du limiteur de débit matériel SPAN-CPU ne s'incrémente pas en raison d'une limitation logicielle. Un exemple de ceci est illustré dans le résultat ci-dessous :

```
N9K# show hardware rate-limiter span

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters


Module: 1
R-L Class Config Allowed             Dropped               Total
+---------------+---------+-------------------+-------------------+-------------------+
span 50 0              499136              499136
```

Cette limitation logicielle affecte toutes les versions du logiciel NX-OS et est documentée par CSCva37512.

Afin de déterminer la quantité de trafic répliquée sur le plan de contrôle d'un périphérique Nexus 9000 configuré avec une session de surveillance SPAN-CPU active, utilisez la commande **show system internal access-list tcam ingress region span**. Un exemple de sortie filtrée de la commande susmentionnée qui montre les compteurs de paquets et d'octets pertinents est présenté ci-dessous.

```
N9K# show system internal access-list tcam ingress region span | include pkts:
<snip>
pkts: 56582127, bytes: 4119668263
```

## Les paquets générés par le plan de contrôle n'apparaissent pas dans les sessions de surveillance TX SPAN-to-CPU

Les paquets créés par le plan de contrôle et transmis depuis une interface source pour une session de surveillance SPAN-CPU ne seront pas capturés par la session de surveillance SPAN-CPU. Ces paquets sortent correctement de l'interface, mais ne peuvent pas être capturés via une session de surveillance SPAN-CPU sur le même périphérique où le paquet est généré.

Prenons par exemple un périphérique de la gamme Cisco Nexus 9000 où Ethernet1/1 est une interface L3/routée connectée à un autre routeur. Le processus OSPF 1 est activé sur Ethernet1/1, qui est la seule interface activée par OSPF sur le périphérique Cisco Nexus 9000.

```
N9K# show running-config ospf  !Command: show running-config ospf !Running configuration last
done at: Wed Feb 26 16:16:30 2020 !Time: Wed Feb 26 16:16:37 2020 version 9.3(3) Bios:version
05.39 feature ospf router ospf 1 interface Ethernet1/1 ip router ospf 1 area 0.0.0.0 N9K# show
ip ospf interface brief  OSPF Process ID 1 VRF default Total number of interface: 1 Interface ID
Area Cost State Neighbors Status Eth1/1 1 0.0.0.0 4 DR 0 up
```

L'utilitaire de capture de paquets du plan de contrôle Ethanalyer montre que les messages Hello OSPF sont générés par le plan de contrôle du périphérique une fois toutes les 10 secondes.

```
N9K# ethanalyzer local interface inband display-filter ospf limit-captured-frames 0 Capturing on
inband 2020-02-26 16:19:13.041255 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26
16:19:22.334692 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26 16:19:31.568034
192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  ^C 3 packets captured
```

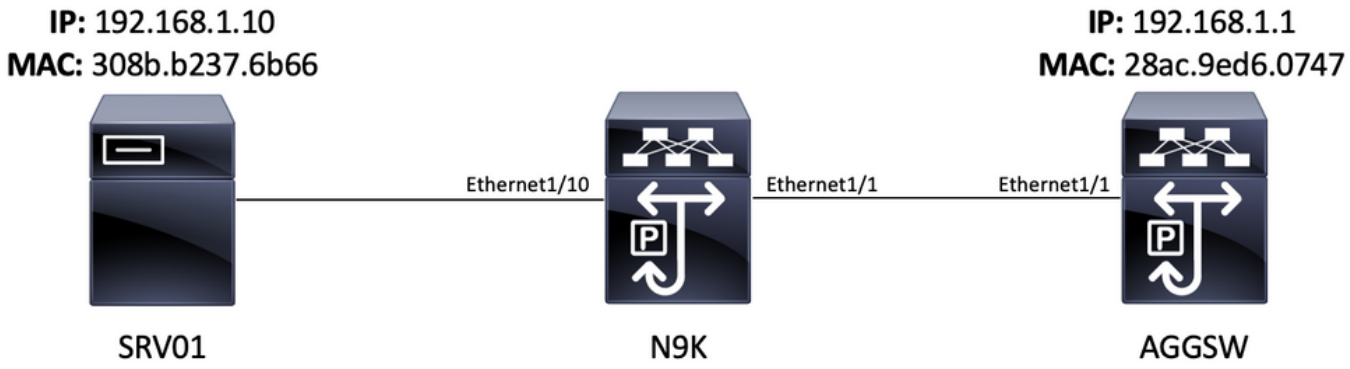
Cependant, une sortie/TX SPAN-to-CPU sur l'interface Ethernet1/1 n'affiche pas ces paquets Hello OSPF (Open Shortest Path First) transmis sur cette interface après 60 secondes de temps.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Wed Feb 26 16:20:48 2020 !Time: Wed Feb 26 16:20:51 2020 version 9.3(3)
Bios:version 05.39 monitor session 1 source interface Ethernet1/1 tx destination interface sup-
eth0 no shut N9K# show monitor  Session State Reason Description ------- ----------- -----------
---------- ------------------------------- 1 up The session is up N9K# ethanalyzer local
interface inband mirror display-filter ospf autostop duration 60 Capturing on inband 0 packets
captured
```

Afin de vérifier si les paquets générés par le plan de contrôle d'un périphérique Cisco Nexus 9000 sont transmis depuis une interface spécifique, Cisco recommande d'utiliser un utilitaire de capture de paquets sur le périphérique distant connecté à l'interface.

# Procédure SPAN-to-CPU évolutive pour le cloud Cisco Nexus 9000

Considérez la topologie suivante :




Un paquet ICMP (Internet Control Message Protocol) provenant du serveur SRV01 dans VLAN 10 (192.168.10.10) est destiné à la passerelle VLAN 10 192.168.10.1. Une session de surveillance SPAN-to-CPU sera utilisée pour confirmer que ce paquet ICMP traverse le périphérique N9K (un Cisco Nexus 93180YC-EX qui exécute le logiciel NX-OS version 9.3(3)), qui agit comme un commutateur de couche 2 qui connecte SRV01 à AGGSW dans VLAN 10.

## Étape 1. Confirmer les ressources suffisantes pour la nouvelle session SPAN

Les commutateurs de la gamme Cisco Nexus 9000 avec ASIC évolutif en nuage qui exécutent le logiciel NX-OS prennent en charge un maximum de quatre sessions SPAN ou ERSPAN actives par ASIC/moteur de transfert. En outre, si les trois premières sessions SPAN ou ERSPAN sont configurées avec des interfaces source bidirectionnelles (TX et RX), l'interface source de la quatrième session SPAN ou ERSPAN doit être une source d'entrée/RX.

Avant de configurer une session de surveillance SPAN-CPU, vérifiez la quantité d'autres sessions SPAN ou ERSPAN actuellement configurées sur le périphérique. Cela peut être fait avec les

commandes **show running-config monitor** et **show monitor**. L'exemple ci-dessous montre le résultat des deux commandes lorsqu'aucune autre session SPAN ou ERSPAN n'est configurée sur le périphérique.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:34:04 2020 !Time: Tue Feb 25 20:34:06 2020 version 9.3(3)
Bios:version 07.66 N9K# show monitor  Note: No sessions configured
```

> **Note**: Des informations supplémentaires sur le nombre maximal de sessions SPAN/ERSPAN et d'autres limitations sont disponibles dans le Guide d'évolutivité vérifiée NX-OS de la gamme Cisco Nexus 9000 pour le logiciel NX-OS Version 9.3(3).

## Étape 2. Configuration de la session de surveillance SPAN-to-CPU

L'élément de configuration clé qui définit une session de surveillance SPAN-to-CPU est une interface de destination de « sup-eth0 », qui est l'interface intrabande du superviseur. L'exemple ci-dessous montre la configuration d'une session de surveillance SPAN-to-CPU où les paquets d'entrée/RX d'Ethernet1/10 sont répliqués au superviseur du commutateur de la gamme Cisco Nexus 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# source interface Ethernet1/10 rx N9K-
1(config-monitor)# destination interface sup-eth0 N9K-1(config-monitor)# no shut N9K-1(config-
monitor)# end N9K#
```

## Étape 3. Vérifier que la session de surveillance SPAN-to-CPU est active

Utilisez les commandes **show running-config monitor** et **show monitor** afin de vérifier que la session SPAN-to-CPU monitor est configurée et opérationnelle. La configuration de la session de surveillance SPAN-to-CPU peut être vérifiée à l'aide de la sortie de la commande **show running-config monitor**, comme indiqué dans l'exemple ci-dessous.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:47:50 2020 !Time: Tue Feb 25 20:49:35 2020 version 9.3(3)
Bios:version 07.66 monitor session 1 source interface Ethernet1/10 rx destination interface sup-
eth0 no shut
```

L'état opérationnel de la session de surveillance SPAN-CPU peut être vérifié à l'aide de la sortie de la commande **show monitor**. Le résultat doit indiquer que l'état de la session de surveillance SPAN-to-CPU est « up » avec la raison « The session is up », comme indiqué dans l'exemple ci-dessous.

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 up The session is up
```

## Étape 4. Afficher les paquets répliqués dans le plan de contrôle

L'utilitaire de capture de paquets du plan de contrôle Ethanalyer peut être utilisé pour afficher le trafic répliqué sur le plan de contrôle du périphérique Cisco Nexus 9000. Le mot clé **mirroir** de la commande Ethanalyzer filtre le trafic de telle sorte que seul le trafic répliqué par une session de surveillance SPAN-CPU est affiché. Les filtres de capture et d'affichage de l'analyseur peuvent

être utilisés pour limiter davantage le trafic affiché. Vous trouverez des informations supplémentaires sur les filtres de capture et d'affichage d'Ethanalyzer utiles dans le Guide de dépannage d'Ethanalyzer sur Nexus 7000. Notez que bien que ce document ait été écrit pour la plate-forme Cisco Nexus 7000, il s'applique principalement à la plate-forme Cisco Nexus 9000 également.

Un exemple d'utilisation de l'utilitaire de capture de paquets du plan de contrôle Ethanalyzer pour filtrer le trafic répliqué par une session de surveillance SPAN-CPU est présenté ci-dessous. Notez que le mot clé **miroir** est utilisé, ainsi qu'un filtre d'affichage définissant les paquets ICMP provenant ou destinés à 192.168.10.10 (l'adresse IP de SRV01 dans la topologie susmentionnée).

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0
Capturing on inband
2020-02-25 21:01:07.592838 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.046682 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.047720 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.527646 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.528659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.529500 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530082 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.531244 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request ^C 9 packets captured
```

> **Note**: Utilisez la combinaison de touches Control-C afin de quitter l'utilitaire de capture de paquets du plan de contrôle Ethanalyzer.

Vous pouvez afficher des informations détaillées sur ce trafic en incluant le mot clé **detail** dans la commande Ethanalyzer. Un exemple de ceci pour un seul paquet ICMP Echo Request est montré ci-dessous.

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0 detail
Capturing on inband Frame 2 (114 bytes on wire, 114 bytes captured) Arrival Time: Feb 25, 2020
21:56:40.497381000 [Time delta from previous captured frame: 1.874113000 seconds] [Time delta
from previous displayed frame: 1.874113000 seconds] [Time since reference or first frame:
1.874113000 seconds] Frame Number: 2 Frame Length: 114 bytes Capture Length: 114 bytes [Frame is
marked: False] [Protocols in frame: eth:ip:icmp:data] Ethernet II, Src: 30:8b:b2:37:6b:66
(30:8b:b2:37:6b:66), Dst: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) Destination: 28:ac:9e:d6:07:47
(28:ac:9e:d6:07:47) Address: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) .... ...0 .... .... .... ....
= IG bit: Individual address (unicast) .... ..0. .... .... .... .... = LG bit: Globally unique
address (factory default) Source: 30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) Address:
30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) .... ...0 .... .... .... .... = IG bit: Individual address
(unicast) .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Type
: IP (0x0800) Internet Protocol, Src: 192.168.10.10 (192.168.10.10), Dst: 192.168.10.1
(192.168.10.1) Version : 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP
0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) ....
..0. = ECN-Capable Transport (ECT): 0 .... ...0 = ECN-CE: 0 Total Length: 100 Identification:
0x00e1 (225) Flags: 0x00 0.. = Reserved bit: Not Set .0. = Don't fragment: Not Set ..0 = More
fragments: Not Set Fragment offset: 0 Time to live: 254 Protocol: ICMP (0x01) Header checksum :
0x265c [correct] [Good: True] [Bad : False] Source: 192.168.10.10 (192.168.10.10) Destination:
192.168.10.1 (192.168.10.1) Internet Control Message Protocol Type : 8 (Echo (ping) request)
Code: 0 () Checksum : 0xf1ed [correct] Identifier: 0x0004 Sequence number: 0 (0x0000) Data (72
bytes) 0000 00 00 00 00 ed 9e 9e b9 ab cd ab cd ab cd ab cd ................ 0010 ab cd ab cd ab
cd ab cd ab cd ab cd ab cd ab cd ................ 0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
ab cd ................ 0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ................
0040 ab cd ab cd ab cd ab cd ........ Data: 00000000ED9E9EB9ABCDABCDABCDABCDABCDABCDABCD...
```

```
[Length: 72] ^C 1 packet captured
```

### Étape 5. Arrêter administrativement la session de surveillance SPAN-to-CPU

Utilisez la commande de configuration **shutdown** dans le contexte de la session de surveillance SPAN-to-CPU pour arrêter la session de surveillance SPAN-to-CPU et arrêter la réplication du trafic vers le plan de contrôle du périphérique Cisco Nexus 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# shut N9K-1(config-monitor)# end N9K#
```

Vérifiez l'état de fonctionnement de la session de surveillance SPAN-to-CPU à l'aide de la commande **show monitor**. L'état de fonctionnement de la session de surveillance SPAN-CPU doit apparaître comme « arrêté » avec une raison de « fermeture de l'administrateur de session », comme indiqué dans l'exemple ci-dessous :

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 down Session admin shut
```

### Étape 6. Supprimer la configuration de session de surveillance SPAN-to-CPU (facultatif)

Si vous le souhaitez, supprimez la configuration de la session de surveillance SPAN-CPU avec la commande de configuration **no monitor session {id}**. Le résultat ci-dessous en donne un exemple.

```
N9K# configure terminal Enter configuration commands, one per line . End with CNTL/Z. N9K-
1(config)# no monitor session 1 N9K-1(config)# end
```

Vérifiez que la configuration de la session de surveillance SPAN-to-CPU a été supprimée avec succès à l'aide de la commande **show running-config monitor**, comme indiqué dans l'exemple ci-dessous.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 21:46:25 2020 !Time: Tue Feb 25 21:46:29 2020 version 9.3(3)
Bios:version 07.66 N9K#
```

## Analyser les résultats d'une capture de paquets SPAN-to-CPU

L'exemple ci-dessus de cette procédure montre que les paquets ICMP Echo Request provenant de 192.168.10.10 (SRV01) et destinés à 192.168.10.1 (AGGSW) entrent dans l'interface Ethernet1/10 du périphérique Cisco Nexus 9000 avec un nom d'hôte N 9K. Cela prouve que SRV01 envoie ce trafic depuis sa carte d'interface réseau. Cela prouve également que le paquet ICMP Echo Request progresse suffisamment dans le pipeline de transfert de Cisco Cloud Scale ASIC pour qu'il soit répliqué sur le plan de contrôle du périphérique.

Cependant, cela ne prouve pas que le périphérique Cisco Nexus 9000 transfère le paquet ICMP Echo Request d'Ethernet1/1 vers AGGSW. Un dépannage supplémentaire doit être effectué pour vérifier si le paquet est transféré d'Ethernet1/1 vers AGGSW. Par ordre de fiabilité :

1. Si le périphérique distant de l'interface de sortie attendue (Ethernet1/1 de N9K dans l'exemple) est un périphérique de la gamme Cisco Nexus 9000 avec un ASIC évolutif en nuage, vous pouvez effectuer une session de surveillance SPAN/RX SPAN-to-CPU sur le périphérique distant (Eth1/1

d'AGGSW dans l'exemple précédent). Si le périphérique distant de l'interface de sortie attendue n'est pas un périphérique de la gamme Cisco Nexus 9000 avec un ASIC à l'échelle du cloud, alors un SPAN, un miroir de ports ou une autre capture de paquets similaire sur le périphérique distant est équivalent.

2. Exécutez un ELAM d'entrée/de réception sur l'interface d'entrée (Ethernet1/10 de N9K dans l'exemple ci-dessus) du périphérique Cisco Nexus 9000. Des informations supplémentaires sur cette procédure sont disponibles dans la note technique de dépannage ELAM de Nexus 9000 sur l'échelle du cloud ASIC NX-OS.

3. Effectuez une sortie/TX SPAN-to-CPU sur l'interface de sortie du périphérique Cisco Nexus 9000 (Ethernet1/1 de N9K dans l'exemple ci-dessus).

## Informations connexes

- Guide de dépannage NX-OS de la gamme Cisco Nexus 9000, version 9.3(x)
- Guide de dépannage NX-OS de la gamme Cisco Nexus 9000, version 9.2(x)
- Guide de dépannage NX-OS de la gamme Cisco Nexus 9000, version 7.0(3)I7(x)
- Ethanalyzer on Nexus 7000 Guide de dépannage
- ELAM NX-OS Nexus 9000 - Evolutivité du cloud ASIC (Tahoe)