Dépannage des pertes de paquets avec les ACL sur la plate-forme Nexus

Table des matières

Introduction

Ce document décrit comment dépanner la perte de paquets à l'aide des listes de contrôle d'accès (ACL) sur la plate-forme Nexus.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance des sujets suivants :

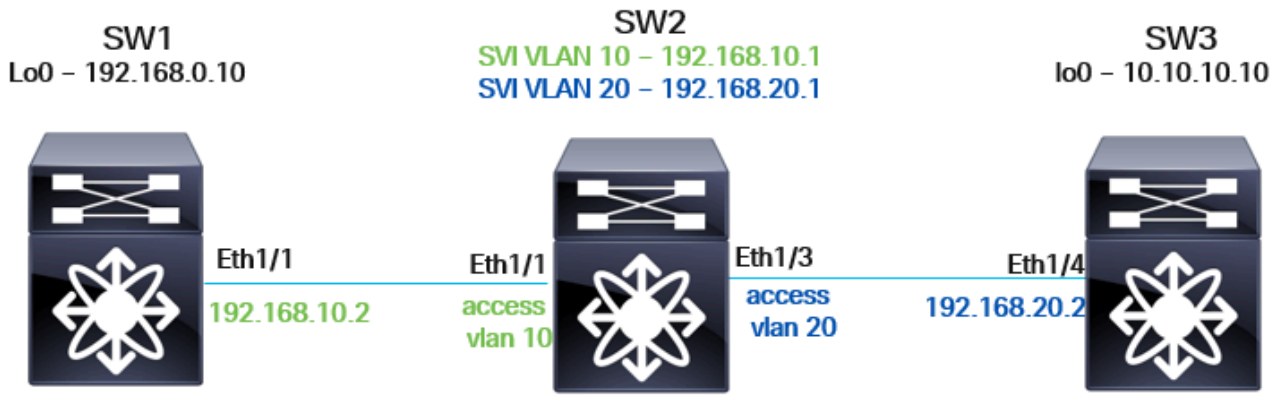
- Plate-forme NXOS
- Listes de contrôle d'accès

Composant utilisé

N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

Les informations de ce document ont été créées à partir de périphériques Nexus dans un environnement de travaux pratiques. Tous les périphériques utilisés dans ce document ont démarré sans aucune configuration préexistante. Si vous utilisez un réseau actif, assurez-vous de comprendre l'impact potentiel de toute commande.

Topologie



Brève présentation des listes de contrôle d'accès et de leurs fonctionnalités

Une liste de contrôle d'accès est essentiellement utilisée pour filtrer le trafic en fonction d'une série de règles et de critères ordonnés (par exemple, le filtrage en fonction des adresses IP source/de destination). Ces règles déterminent si les paquets correspondent à des conditions spécifiques afin de décider s'ils doivent être autorisés ou refusés. En termes plus simples, la liste de contrôle d'accès définit si les paquets réseau peuvent être autorisés à passer ou refusés en fonction des règles définies dans celle-ci. Si les paquets remplissent les conditions des règles d'autorisation, ils doivent être traités par le commutateur Nexus. Inversement, si les paquets correspondent aux conditions de refus, ils doivent être rejetés.

L'une des principales caractéristiques des listes de contrôle d'accès est leur capacité à fournir des

compteurs statistiques pour le flux de paquets. Ces compteurs suivent le nombre de paquets qui correspondent aux règles de la liste de contrôle d’accès, ce qui peut s’avérer très utile lors du dépannage de scénarios de perte de paquets.

Par exemple, si un périphérique envoie un certain nombre de paquets, mais reçoit moins de paquets que prévu, les compteurs statistiques de la liste de contrôle d’accès peuvent aider à isoler le point auquel les paquets sont abandonnés dans le réseau.

PACL et RACL

La mise en oeuvre des listes de contrôle d’accès peut varier selon qu’elles sont appliquées aux interfaces de couche 2 (PACL), aux interfaces de couche 3 (RACL) ou aux VLAN (VACL). Voici une brève comparaison de ces méthodes :

- Liste de contrôle d'accès au port (PACL) : La liste de contrôle d’accès est appliquée à une interface de port de commutation de couche 2 (L2).
- Liste de contrôle d'accès au routeur (RACL) : La liste de contrôle d’accès est appliquée à une interface routée de couche 3 (L3).

Type ACL	Interface	Action	Direction Appliquée
PACL	L2	Interfaces de port de commutation Si la liste de contrôle d’accès est appliquée à une interface d’agrégation, elle filtre le trafic pour tous les VLAN autorisés sur l’agrégation.	Entrant uniquement : trafic entrant dans l'interface.
RACL	couche 3	Sous-interfaces SVI, L3 physique et L3	Entrant et sortant : le trafic entrant filtre le trafic entrant dans l'interface, tandis que le trafic sortant filtre le trafic sortant sortant.

Objectif

Il est nécessaire de confirmer que tous les paquets envoyés sont reçus correctement.

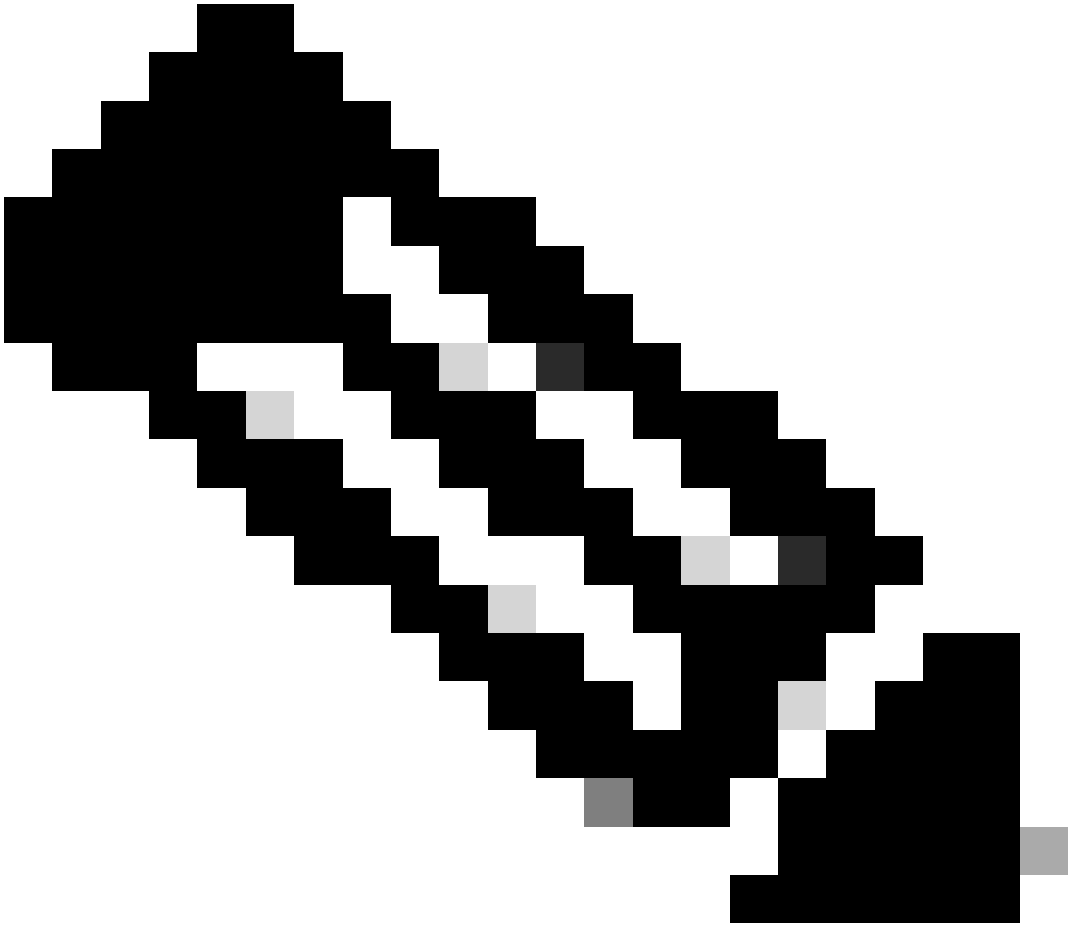
Explication de topologie

- N9K-1 a une connectivité de couche 3 avec N9K-2. L'interface Eth1/1 sur N9K-1 est configurée comme interface routée de couche 3, tandis que l'interface Eth1/1 de N9K-2 est une interface de port de commutation de couche 2, étiquetée avec VLAN 10.
- N9K-2 possède également une connectivité de couche 3 avec N9K-3. L'interface Eth1/3 sur N9K-2 est une interface de port de commutateur de couche 2 étiquetée avec VLAN 20, et l'interface Eth1/4 de N9K-3 est configurée comme interface routée de couche 3.
- Configuration du bouclage : L'interface Lo0 est configurée pour N9K-1 et N9K-2. Ces interfaces Lo0 doivent être utilisées pour envoyer des paquets ping ICMP entre les deux périphériques.

Dépannage

Retrouvez les étapes détaillées du processus de configuration et de vérification de la liste de contrôle d'accès au réseau et de la liste de contrôle d'accès au réseau sur les périphériques N9K. Au cours de ce processus, les listes de contrôle d'accès au port et les listes de contrôle d'accès au routeur sont révisées pour analyser le flux de paquets et déterminer si tous les paquets sont transmis et reçus correctement.

Étape 1 : configuration du protocole RACL sur les interfaces L3 de N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) et N9K-3 (Eth1/14)



Remarque : Pour observer le flux de paquets sortants, une configuration de liste de contrôle d'accès supplémentaire est nécessaire sur N9K-2. Comme N9K-2 ne dispose pas d'interfaces physiques routées de couche 3 (il dispose plutôt d'interfaces de port de commutation SVI et L2), la liste de contrôle d'accès prend uniquement en charge le trafic entrant.

Pour capturer les correspondances de paquets sortants, une nouvelle liste de contrôle d'accès peut être créée et appliquée aux interfaces de couche 3.

La liste de contrôle d'accès est appliquée à N9K-1, N9K-2 et N9K-3.

```
ip access-list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any
```

```
ip access-list TAC-OUT
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any


***N9K-1***
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown



***N9K-2***

interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.10.1/30

interface Vlan20
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.20.1/30

***N9K-3***

interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

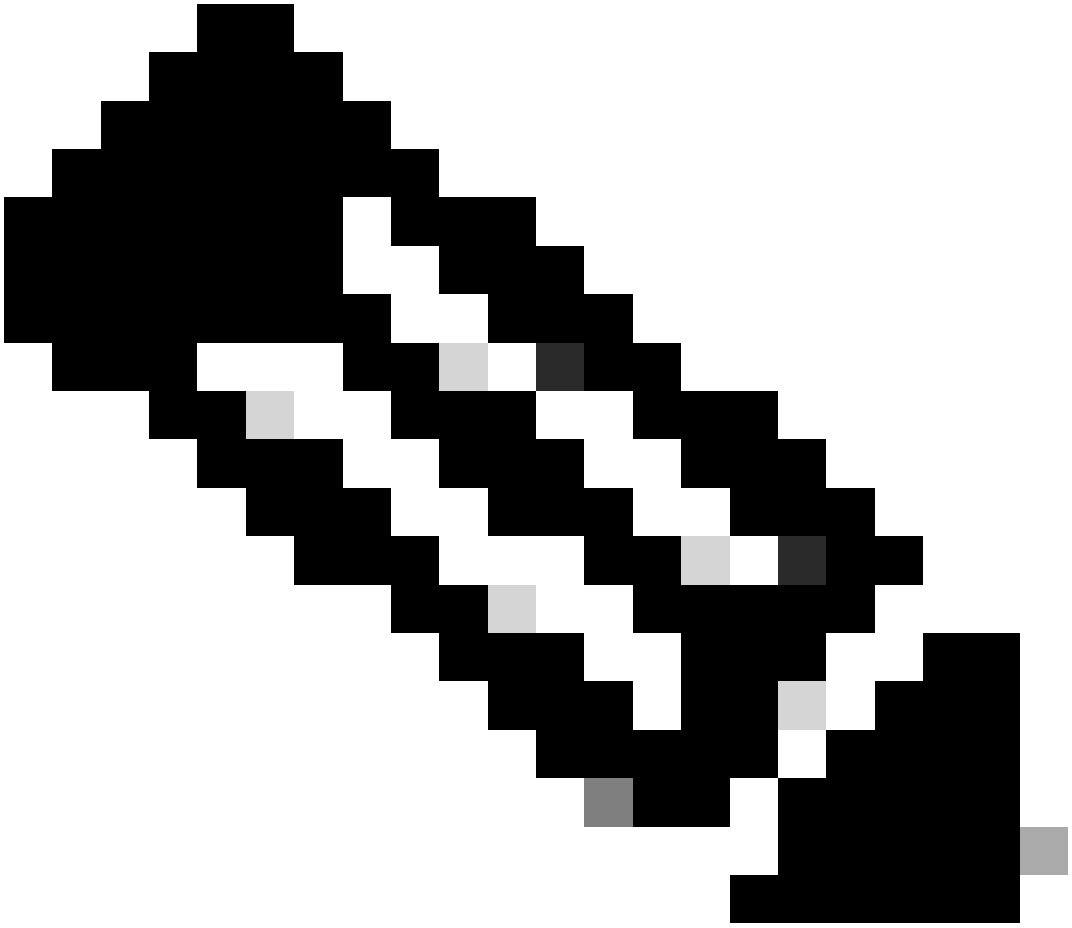
Étape 2 : configuration de la liste de contrôle d’accès sur les interfaces de port de commutation de couche 2 de N9K-2

Sculpture TCAM

La découpe TCAM peut être requise selon le type de liste de contrôle d'accès. Pour plus d'informations, consultez :

[Comprendre comment graver l'espace TCAM du Nexus 9000]

Pour appliquer la liste de contrôle d’accès aux interfaces physiques de couche 2, il est nécessaire de configurer un groupe d’accès de port ip ....
Cependant, la configuration de la région TCAM est également requise.



Remarque : Certaines lignes ont été supprimées pour garder le résultat propre.

```
N9K-C93180YC-2# conf
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2
N9K-C93180YC-2(config-if)# ip port access-group TAC-IN in
ERROR: TCAM region is not configured. Please configure TCAM region Ingress PACL [ing-ifacl] and retry t
N9K-C93180YC-2(config-if)#
```

Procédure de configuration de la région TCAM

Étape 1. Modifications de la région TCAM

Veuillez évaluer quelle région peut fournir de l'espace libre, car cela peut différer pour chaque environnement.

```
N9K-C93180YC-2# show system internal access-list globals

slot 1
=======




LOU Threshold Value : 5

----------------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
----------------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
----------------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 0 1 >>>>>>> Size of 0
Ingress VACL 2 0 0 1
Ingress RACL 3 0 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 1792 256 1
Ingress L3/VLAN QOS 6 2048 512 1 >>>>>> Size of 512
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
----------------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Une autre méthode de vérification.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 0 >>>>>>> Size of 0
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512 >>>>>> Size of 512
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#
```

Étape 2. Réduire la taille de la région

Réduisez la taille de la région allouée pour ing-l3-vlan-qos. (Ceci diffère pour chaque environnement.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 >>> Réduisez l'allocation de 512 à 256.
Enregistrez la configuration et rechargez le système pour que la configuration prenne effet.

Étape 3. Augmenter la région TCAM pour ing-ifacl

N9K-C93180YC-2(config)# hardware access-list tcam region ing-ifacl 256

Enregistrez la configuration et rechargez le système pour que la configuration prenne effet.

N9K-C93180YC-2(config)#

Étape 4 : enregistrement de la configuration

```
N9K-C93180YC-2(config)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
N9K-C93180YC-2(config)#
```

Étape 5. Recharger

```
N9K-C93180YC-2(config)# reload
This command will reboot the system. (y/n)? [n] y
```

Vérification après rechargement

Après le rechargement, vérifiez si les modifications ont pris effet.

```
N9K-C93180YC-2# sh system internal access-list globals

slot 1
=======



----------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
----------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
----------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 256 1 >>> The size value is now 256.
Ingress VACL 2 0 0 1
Ingress RACL 3 256 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 2048 256 1
Ingress L3/VLAN QOS 6 2304 256 1 >>> The size value is now 256.
```

```
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Une autre méthode de vérification.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 256 >>> The size value is now 256.
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 256 >>> The size value is now 256.
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
```

```
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C9318OYC-2#
```

Configuration du groupe d'accès au port IP

Configurez le groupe d'accès au port IP sur les interfaces physiques de couche 2.

```
N9K-C9318OYC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C9318OYC-2(config)# int e1/2,e1/51
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C9318OYC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>>
N9K-C9318OYC-2(config-if-range)#
```

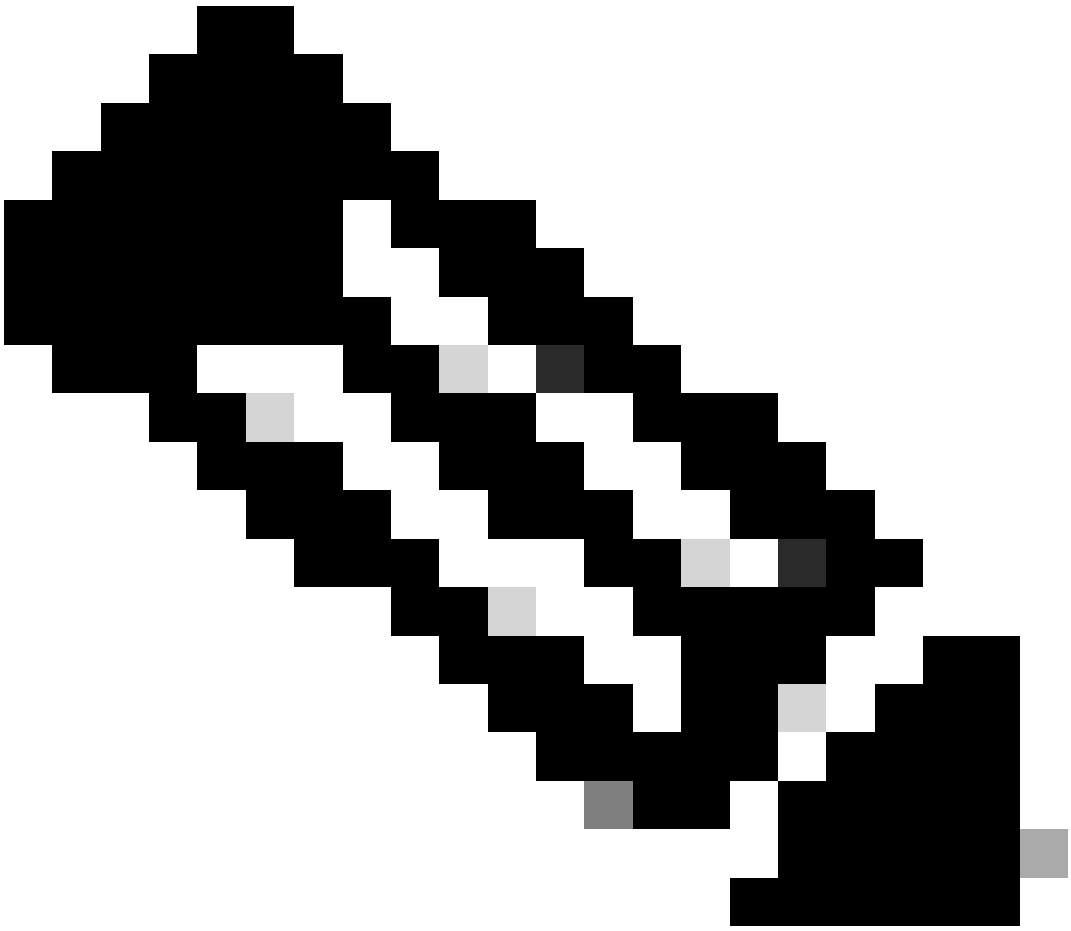
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

Étape 3. Bouclage

N9K-1 utilise son Loopback0 (Lo0) comme source, tandis que N9K-3 peut utiliser son Loopback0 (Lo0) comme destination.
La configuration en cours des interfaces de bouclage que vous utilisez à des fins de test est

détaillée comme suit.



Remarque : La connectivité de couche 3 avec un protocole de routage a déjà été configurée.

```
***N9K-1***
interface loopback0
ip address 192.168.0.10/32
```

```
***N9K-3***
interface loopback0
ip address 10.10.10.10/30
```

Étape 4 : génération du trafic et envoi d’une requête ping de N9K-3 à l’aide de l’adresse IP source 192.168.20.2 vers Lo0 192.168.0.10 de N9K-1

```
N9K-3# ping 192.168.0.10 source 192.168.20.2
PING 192.168.0.10 (192.168.0.10) from 192.168.20.2: 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=253 time=1.163 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=253 time=0.738 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=253 time=0.706 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=253 time=0.668 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=253 time=0.692 ms

--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.668/0.793/1.163 ms
N9K-3#
```

Étape 5. Vérification des informations de statistiques PACL et RACL sur N9K-1, N9K-2 et N9K-3

- Puisque les paquets ICMP proviennent de N9K-3, il est nécessaire de vérifier que les cinq paquets de requête ICMP ont été reçus par N9K-2.
- Vérification PACL sur N9K-2 : Cinq paquets provenant de 192.168.20.2 (Eth1/4 de N9K-3) doivent être reçus, la destination étant le Lo0 de N9K-1 (192.168.0.10).

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configuration associée sur Eth1/3 de N9K-2.

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> PACL
no shutdown
```

- Sur N9K-2, le RACL signale 5 paquets de requête ICMP quittant N9K-2 et étant transmis à N9K-1.
- Puisque la liste de contrôle d'accès ne prend pas en charge la direction sortante, il est essentiel de vérifier l'autre liste de contrôle d'accès (TAC-OUT-SVI) configurée sur l'interface SVI pour VLAN 10, qui est configurée en tant que RACL (puisque la direction sortante est

prise en charge sur les RACL). Le VLAN 10 fournit la connectivité entre N9K-2 et N9K-1.

```
N9K-2# show ip access-lists TAC-OUT-SVI

IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]



configuration associated:


interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>>>
ip address 192.168.10.1/30
```

D'après les résultats précédents, il est confirmé qu'il n'y a pas de perte de paquets avec les paquets de requête ICMP envoyés à partir de N9K-3.

- L'étape suivante consiste à passer au périphérique suivant (destination N9K-1) et à vérifier que le même nombre de paquets de requête ICMP sont reçus de N9K-3.
- Les statistiques RACL indiquent que N9K-2 envoie 5 paquets de requête ICMP en provenance de N9K-3.

```
N9K-1# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configuration associée sur Eth1/1 de N9K-1.

```
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>> RACL
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown
```

- Sur la base de ces informations, il est confirmé qu'il n'y a pas de perte de paquets (requête ICMP) entre N9K-3 et Lo0 192.168.0.10 sur N9K-2.
- L'étape suivante consiste à suivre les paquets de réponse ICMP provenant de N9K-1 Lo0 192.168.0.10 et destinés à N9K-3 à l'adresse 192.168.20.2.
- Ensuite, il est nécessaire de passer à N9K-2 et de vérifier s'il reçoit les cinq paquets de réponse ICMP de 192.168.0.10 à 192.168.20.2.
- Pour effectuer le suivi des paquets de réponse ICMP à partir de N9K-1, il est nécessaire de vérifier la liste de contrôle d'accès PACL (TAC-IN) configurée sur Eth1/1.

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp reply comming from 192.168.0.10 to 19
30 permit ip any any [match=0]
```

```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> PACL (Inboud direction only)
no shutdown
```

- Sur la base des informations fournies précédemment, il est confirmé qu'il n'y a pas de perte de paquets sur le trafic de N9K-1 à N9K-2.
- L'étape suivante consiste à confirmer que N9K-2 envoie correctement les paquets de réponse ICMP à N9K-3. Comme la liste de contrôle d'accès de protocole ne prend pas en charge la direction sortante, il est nécessaire de vérifier l'autre liste de contrôle d'accès (TAC-OUT-SVI) configurée sur l'interface SVI pour VLAN 20, qui est configurée en tant que liste de contrôle d'accès de protocole (car la direction sortante est prise en charge sur les listes de contrôle d'accès de protocole). Le VLAN 20 fournit la connectivité entre N9K-2 et N9K-3.

```
N9K-2# show ip access-lists TAC-OUT-SVI
IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 ICMP reply packets are being sent out to N
```

Configuration associée :

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
```

```
ip access-group TAC-OUT-SVI out >>> RACL outboud direccion
ip address 192.168.20.1/30
```

Sur la base des compteurs ACL des sorties ci-dessus, il est confirmé que N9K-1 envoie correctement les cinq paquets de réponse ICMP à N9K-2.

- Aucune perte de paquet ne se produit entre N9K-2 et N9K-3.
- La dernière étape consiste à se diriger vers la source du trafic, N9K-3, et à vérifier si elle reçoit les cinq paquets de réponse ICMP.
- Il est confirmé que les cinq paquets ICMP atteignent le TAC-IN ACL pour les réponses ICMP provenant de N9K-1 Lo0 (192.168.0.10).
  Pour approfondir l'étude, il est nécessaire de revoir le RACL (TAC-IN) configuré sur Eth1/4.

```
N9K-3# sh ip access-lists TAC-IN

IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp replies comming from Lo0 N9K-1
30 permit ip any any [match=0]
```

Configuration associée :

```
interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>>
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

- À l’aide des étapes de dépannage décrites précédemment, le chemin entrant et sortant du paquet a été validé saut par saut entre la source et la destination.

Dans cet exemple, il a été confirmé qu’il n’y a pas de perte de paquets, car les 5 paquets ICMP ont été reçus et transférés correctement sur chaque périphérique.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.