Problemen oplossen met pakketdrops met ACL's op Nexus-platform

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met pakketverlies kunt oplossen met behulp van Access Control Lists (ACL's) op het Nexus-platform.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

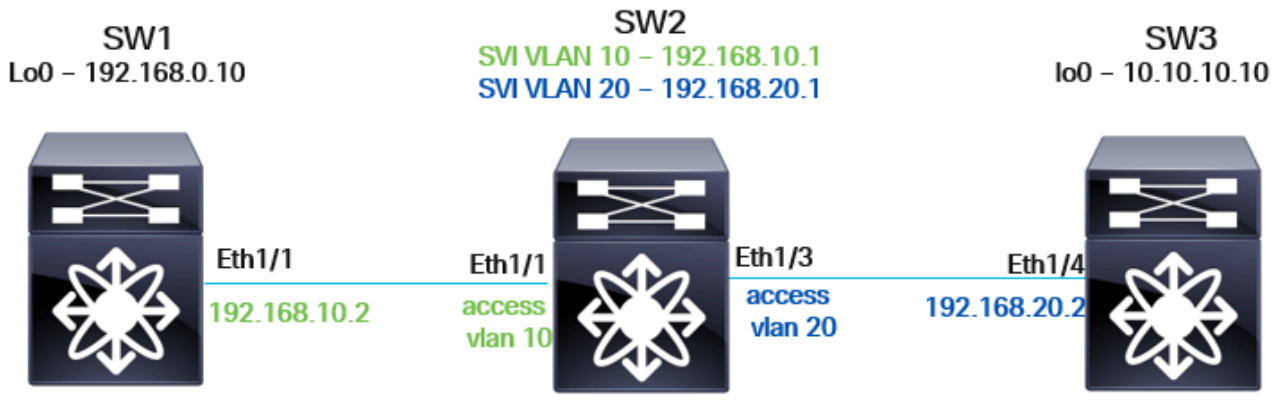
- NXOS-platform
- Toegangscontrolelijsten

Gebruikt onderdeel

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

De informatie in dit document is gemaakt op basis van Nexus-apparaten in een laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart zonder vooraf bestaande configuratie. Als je een live netwerk gebruikt, zorg er dan voor dat je de potentiële impact van een opdracht begrijpt.

Topologie



Beknopt overzicht van toegangscontrolelijsten en hun functionaliteit

Een ACL wordt in wezen gebruikt om verkeer te filteren op basis van een reeks bestelde regels en criteria (bijvoorbeeld filtering op basis van bron / bestemming IP-adressen). Deze regels bepalen of pakketten overeenkomen met specifieke voorwaarden om te beslissen of ze worden toegestaan of geweigerd. In eenvoudiger bewoordingen definieert de ACL of netwerkpakketten kunnen worden doorgelaten of geweigerd op basis van de regels die erin zijn vastgelegd. Als de pakketjes voldoen aan de vergunningsvoorwaarden, worden ze verwerkt door de Nexus-switch. Omgekeerd, als de pakketten overeenkomen met de ontkenningsvoorwaarden, moeten ze worden weggegooid.

Een belangrijk kenmerk van ACL's is hun vermogen om statistische tellers voor de pakketstroom

te bieden. Deze tellers volgen het aantal pakketten dat overeenkomt met de ACL-regels, wat erg handig kan zijn bij het oplossen van pakketverliesscenario's.

Als een apparaat bijvoorbeeld een bepaald aantal pakketten verzendt, maar minder ontvangt dan verwacht, kunnen de statistische tellers van de ACL helpen bij het isoleren van het punt waarop pakketten in het netwerk worden gedropt.

PACL en RACL

De implementatie van ACL's kan variëren, afhankelijk van of ze worden toegepast op Layer 2-interfaces (PACL), Layer 3-interfaces (RACL) of VLAN's (VACL). Hier is een korte vergelijking van deze methoden:

- Poorttoegangscontrolelijst (PACL): De ACL wordt toegepast op een Layer 2 (L2)-switchpoortinterface.
- Router Access Control List (RACL): De ACL wordt toegepast op een Layer 3 (L3) gerouteerde interface.

ACL-type	Interface	Actie	Toegepaste richting
PACL	L2	Switchport-interfaces Als de ACL wordt toegepast op een trunk-interface, filtert het verkeer voor alle VLAN's die zijn toegestaan op de trunk.	Alleen binnenkomend verkeer - verkeer dat de interface binnenkomt.
RACL	L3	SVI-, fysieke L3- en L3-subinterfaces	Zowel inbound als outbound - Inbound filtert het verkeer dat de interface binnenkomt, terwijl outbound het verkeer filtert dat de interface verlaat.

Doel

Het is noodzakelijk om te bevestigen dat alle pakketten die worden verzonden correct worden ontvangen.

Topologische uitleg

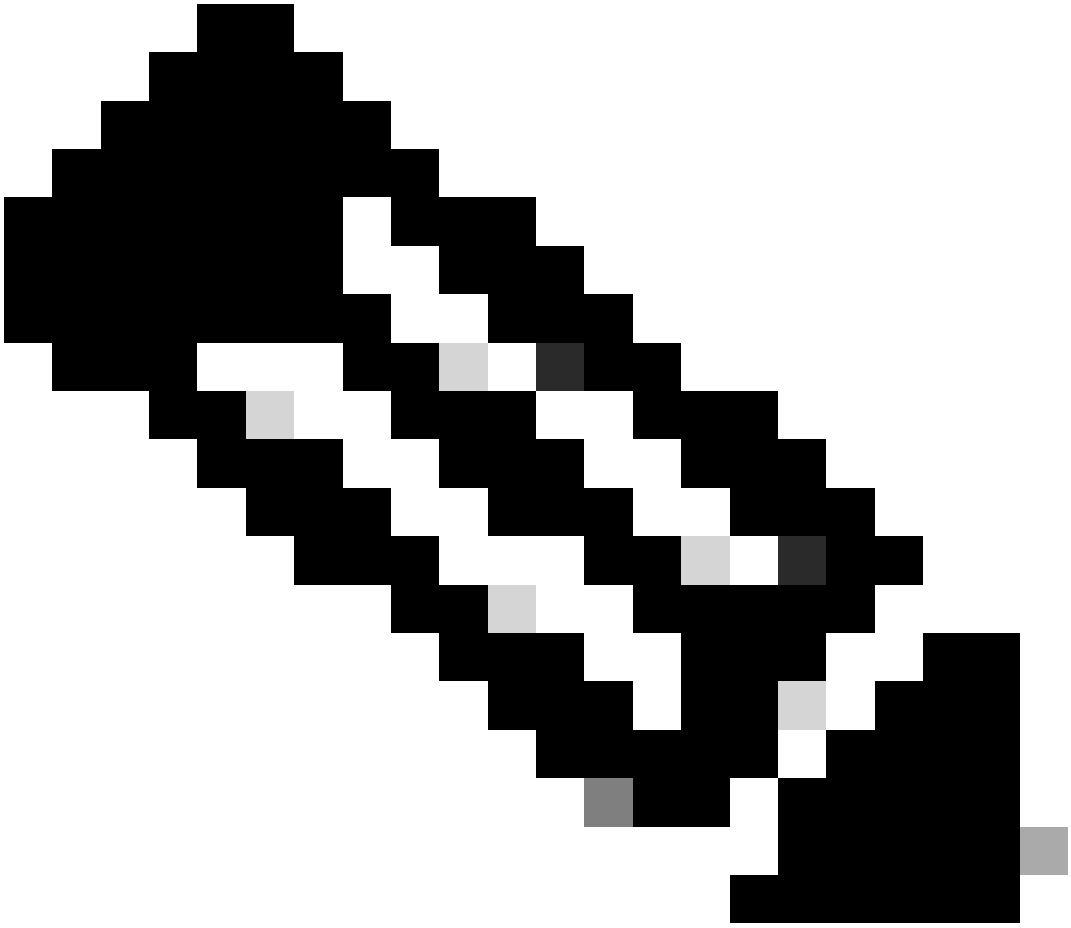
- N9K-1 heeft L3-connectiviteit met N9K-2. De Eth1/1-interface op N9K-1 is geconfigureerd als

een L3-gerouteerde interface, terwijl N9K-2's Eth1/1 een L2-switchpoortinterface is, getagd met VLAN 10.
- N9K-2 heeft ook L3-connectiviteit met N9K-3. De Eth1/3-interface op N9K-2 is een L2-switchpoortinterface getagd met VLAN 20 en N9K-3's Eth1/4 is geconfigureerd als een L3-gerouteerde interface.
- Loopback Configuratie: Zowel N9K-1 als N9K-2 hebben de Lo0-interface geconfigureerd. Deze Lo0-interfaces worden gebruikt om ICMP-pingpakketten tussen de twee apparaten te verzenden.

Probleemoplossing

Zie de gedetailleerde processtappen voor het configureren en verifiëren van RACL en PACL op de N9K-apparaten. Tijdens dit proces worden de poorttoegangscontrolelijsten en de routertoegangscontrolelijsten beoordeeld om de pakketstroom te analyseren en te bepalen of alle pakketten correct worden verzonden en ontvangen.

Stap 1. De RACL configureren op L3-interfaces van N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) en N9K-3 (Eth1/14)



Opmerking: om de uitgaande pakketstroom te observeren, is een extra ACL-configuratie nodig op N9K-2. Omdat N9K-2 geen L3 fysieke gerouteerde interfaces heeft (in plaats daarvan heeft het SVI- en L2-switchpoortinterfaces), ondersteunt PACL alleen inbound verkeer.

Om uitgaande pakketmatches vast te leggen, kan een nieuwe ACL worden gemaakt en toegepast op de L3-interfaces.

De ACL wordt toegepast op N9K-1, N9K-2 en 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
```

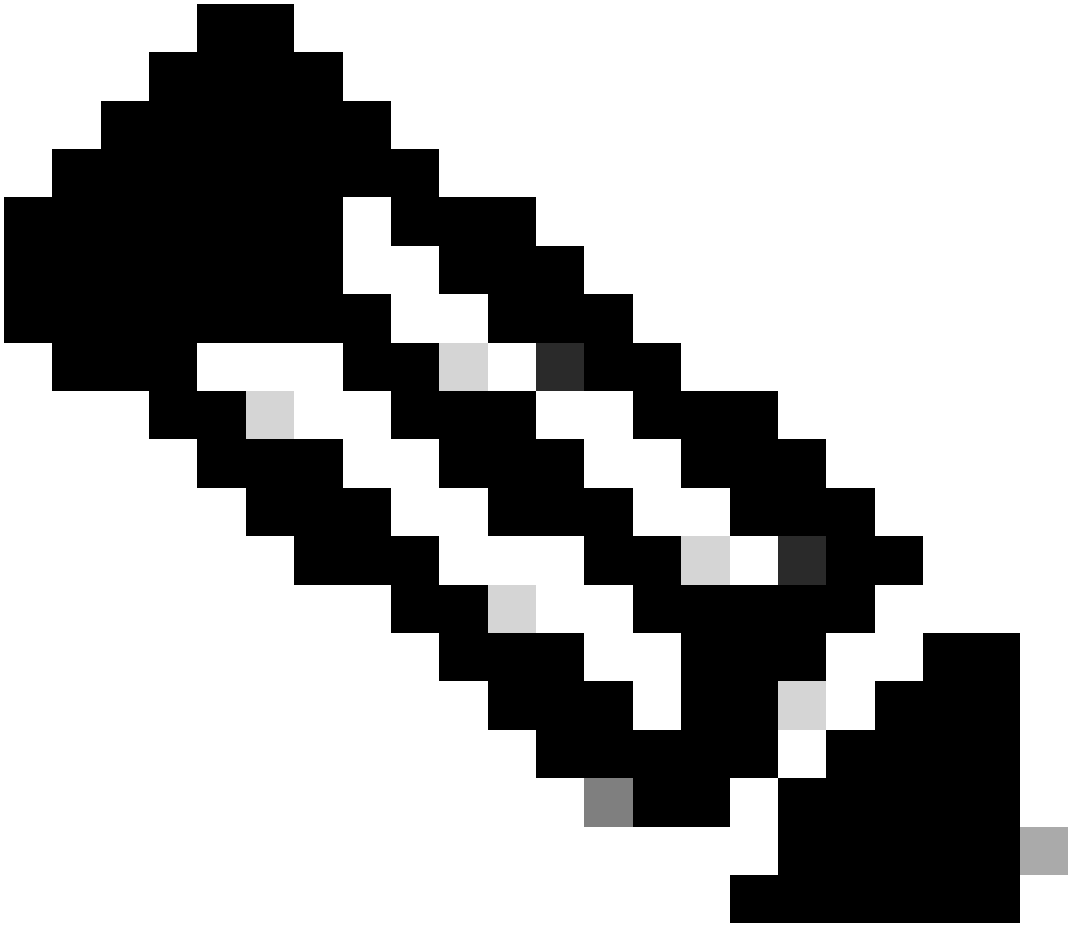
Stap 2. PACL configureren op L2-switchpoortinterfaces van N9K-2

TCAM-snijwerk

TCAM-snijwerk kan afhankelijk van het ACL-type vereist zijn, raadpleeg voor meer informatie:

Begrijp hoe Nexus 9000 TCAM-ruimte te snijden

Om de PACL toe te passen op L2 fysieke interfaces, is het noodzakelijk om een IP-poort toegangsgroep te configureren.
Het configureren van de TCAM-regio is echter ook vereist.



Opmerking: Bepaalde rijen zijn verwijderd om de uitvoer schoon te houden.

```
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)#
```

Procedure voor het configureren van de TCAM-regio

Stap 1. Wijzigingen in TCAM-regio

Evalueer welke regio vrije ruimte kan bieden, omdat dit voor elke omgeving kan verschillen.

```
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
```

Alternatieve methode voor verificatie.

```
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#
```

Stap 2. Verklein de omvang van de regio

Verklein de grootte van de regio die is toegewezen aan ing-l3-vlan-qos. (Dit verschilt per omgeving.)

N9K-C93180YC-2(config)# hardware access-list tcam region ing-l3-vlan-qos 256 **>>>** Verlaag de toewijzing van 512 naar 256.
Sla de configuratie op en laad het systeem opnieuw zodat de configuratie van kracht kan worden.

Stap 3. Verhoog de TCAM-regio voor ing-ifacl

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

Config opslaan en het systeem opnieuw laden zodat de configuratie van kracht wordt.

N9K-C93180YC-2(config)#

Stap 4. Configuratie opslaan

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

Stap 5. Opnieuw laden

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

Verificatie na opnieuw laden

Controleer na het opnieuw laden of de wijzigingen zijn doorgevoerd.

```
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
```

Alternatieve methode voor verificatie.

```
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-C93180YC-2#
```

Configuratie van IP Port Access Group

Configureer de IP-poorttoegangsgroep op L2 fysieke interfaces.

```
N9K-C93180YC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2,e1/51
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>>
N9K-C93180YC-2(config-if-range)#
```

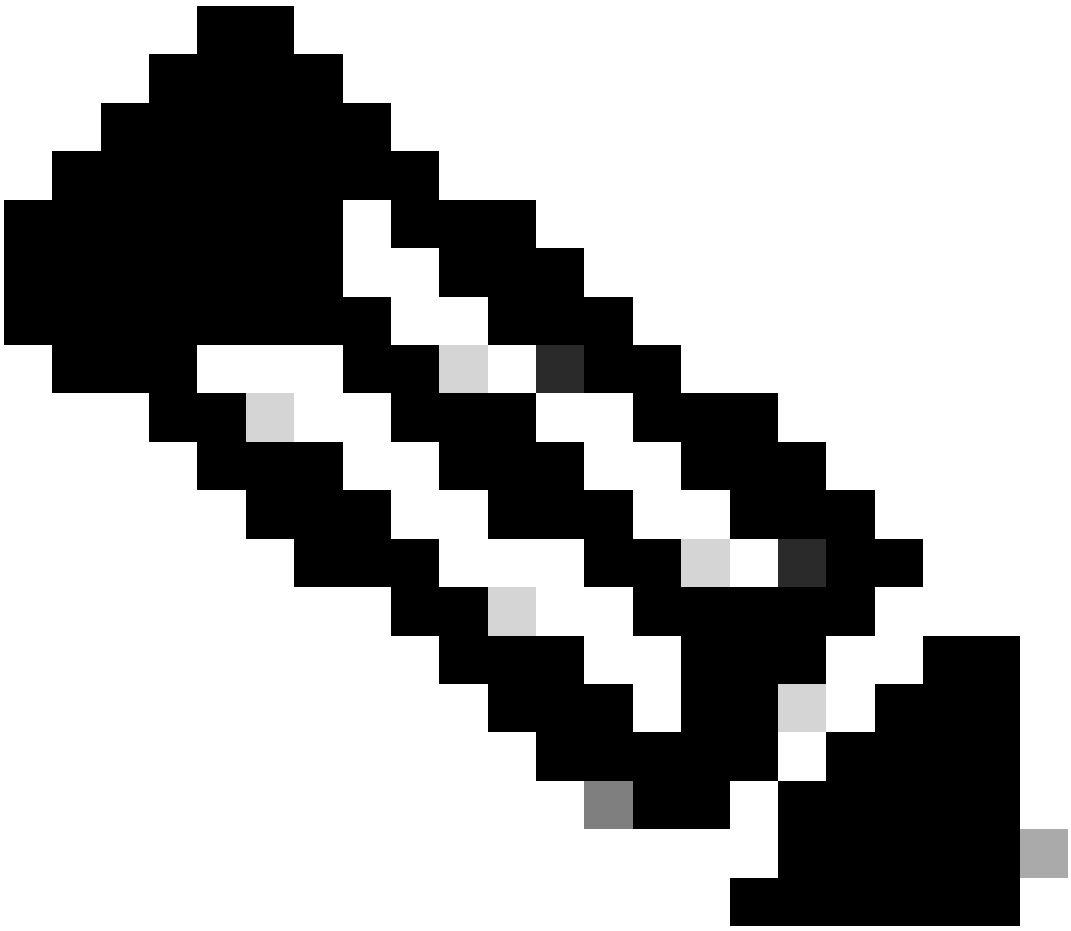
```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

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

Stap 3. loopback

N9K-1 moet zijn Loopback0 (Lo0) als bron gebruiken, terwijl N9K-3 zijn Loopback0 (Lo0) als bestemming kan gebruiken.
De actieve configuratie van de Loopback-interfaces die u gebruikt voor testdoeleinden wordt als

volgt beschreven.



Opmerking: Layer 3-connectiviteit met een routeringsprotocol is eerder geconfigureerd.

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


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

Stap 4. Genereer verkeer en verzend een Ping van N9K-3 met behulp van de bron IP 192.168.20.2 naar Lo0 192.168.0.10 van 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#
```

Stap 5. Controleer PACL- en RACL-statistische informatie over N9K-1, N9K-2 en N9K-3

- Aangezien de ICMP-pakketten afkomstig zijn van N9K-3, moet worden geverifieerd of de vijf ICMP-aanvraagpakketten door N9K-2 zijn ontvangen.
- PACL Verificatie op N9K-2: Er wordt verwacht dat vijf pakketten afkomstig van 192.168.20.2 (Eth1/4 van N9K-3) worden ontvangen, met als bestemming N9K-1's Lo0 (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]
```

Gerelateerde configuratie op Eth1/3 van 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
```

- Op N9K-2 rapporteert de RACL 5 ICMP-verzoekpakketten die N9K-2 verlaten en worden doorgestuurd naar N9K-1.
- Aangezien PACL de uitgaande richting niet ondersteunt, is het essentieel om de andere ACL (TAC-OUT-SVI) te controleren die is geconfigureerd op de SVI voor VLAN 10, die is geconfigureerd als een RACL (aangezien uitgaande richting wordt ondersteund op RACL's). VLAN 10 biedt de connectiviteit tussen N9K-2 en 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
```

Op basis van de vorige resultaten wordt bevestigd dat er geen pakketverlies is met de ICMP-verzoekpakketten die zijn verzonden vanaf N9K-3.

- De volgende stap is om door te gaan naar het volgende apparaat (bestemming N9K-1) en te controleren of hetzelfde aantal ICMP-aanvraagpakketten wordt ontvangen van N9K-3.
- De statistieken van RACL geven aan dat N9K-2 5 ICMP-aanvraagpakketten verzendt die afkomstig zijn van 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]
```

Gerelateerde configuratie op Eth1/1 van 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
```

- Op basis van de informatie wordt bevestigd dat er geen pakketverlies (ICMP-verzoek) is van N9K-3 naar Lo0 192.168.0.10 op N9K-2.

- De volgende stap is het volgen van de ICMP-antwoordpakketten afkomstig van N9K-1 Lo0 192.168.0.10 en bestemd voor N9K-3 op 192.168.20.2.
- Vervolgens is het noodzakelijk om verder te gaan naar N9K-2 en te controleren of het de vijf ICMP-antwoordpakketten ontvangt van 192.168.0.10 tot 192.168.20.2.
- Om de ICMP-antwoordpakketten van N9K-1 te volgen, moet de op Eth1/1 geconfigureerde PACL (TAC-IN) worden geverifieerd.

```
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
```

- Op basis van de eerder verstrekte informatie wordt bevestigd dat er geen pakketverlies is op het verkeer van N9K-1 naar N9K-2.
- De volgende stap is om te bevestigen dat N9K-2 de juiste ICMP-antwoordpakketten naar N9K-3 verzendt. Aangezien PACL de uitgaande richting niet ondersteunt, is het noodzakelijk om de andere ACL (TAC-OUT-SVI) te controleren die is geconfigureerd op de SVI voor VLAN 20, die is geconfigureerd als een RACL (aangezien uitgaande richting wordt ondersteund op RACL's). VLAN 20 biedt de connectiviteit tussen N9K-2 en 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
```

Gerelateerde configuratie:

```
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
```

Op basis van de ACL-tellers van bovenstaande uitgangen wordt bevestigd dat N9K-1 de vijf

ICMP-antwoordpakketten naar N9K-2 stuurt.

- Er is geen pakketverlies tussen N9K-2 en N9K-3.

- De laatste stap is om door te gaan naar de bron van het verkeer, N9K-3, en te controleren of het de vijf ICMP-antwoordpakketten ontvangt.
- Er wordt bevestigd dat de vijf ICMP-pakketten de ACL TAC-IN raken voor de ICMP-antwoorden afkomstig van N9K-1 Lo0 (192.168.0.10).
  Om verder te onderzoeken, is het noodzakelijk om de RACL (TAC-IN) geconfigureerd op Eth1/4 te herzien.

```
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]
```

Gerelateerde configuratie:

```
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
```

- Met behulp van eerder beschreven stappen voor probleemoplossing werd het inkomende en uitgaande pad van het pakket op hop-by-hop basis tussen bron en bestemming gevalideerd.

Voor dit voorbeeld werd bevestigd dat er geen pakketverlies is, omdat alle 5 ICMP-pakketten op elk apparaat correct zijn ontvangen en doorgestuurd.

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.