Configurer le protocole NTP sur Nexus en tant que serveur et client

Table des matières

Introduction

Ce document décrit une configuration et une validation simples d'une plate-forme Nexus 9000 pour agir à la fois comme serveur et client NTP (Network Time Protocol).

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Logiciel Nexus NX-OS.
- Protocole NTP (Network Time Protocol).

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Nexus 9000 avec NXOS version 10.2(5).

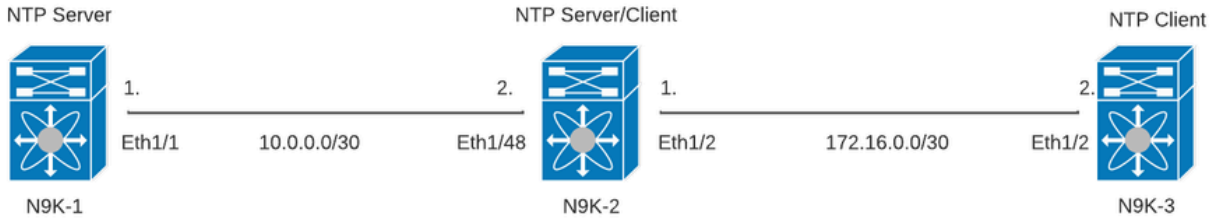
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Le protocole NTP est un protocole réseau utilisé pour synchroniser l'heure d'un ensemble de périphériques au sein d'un réseau afin de corréler les événements lorsque vous recevez des journaux système et d'autres événements spécifiques à l'heure de la part de plusieurs périphériques réseau.

Diagramme du réseau



Configurations

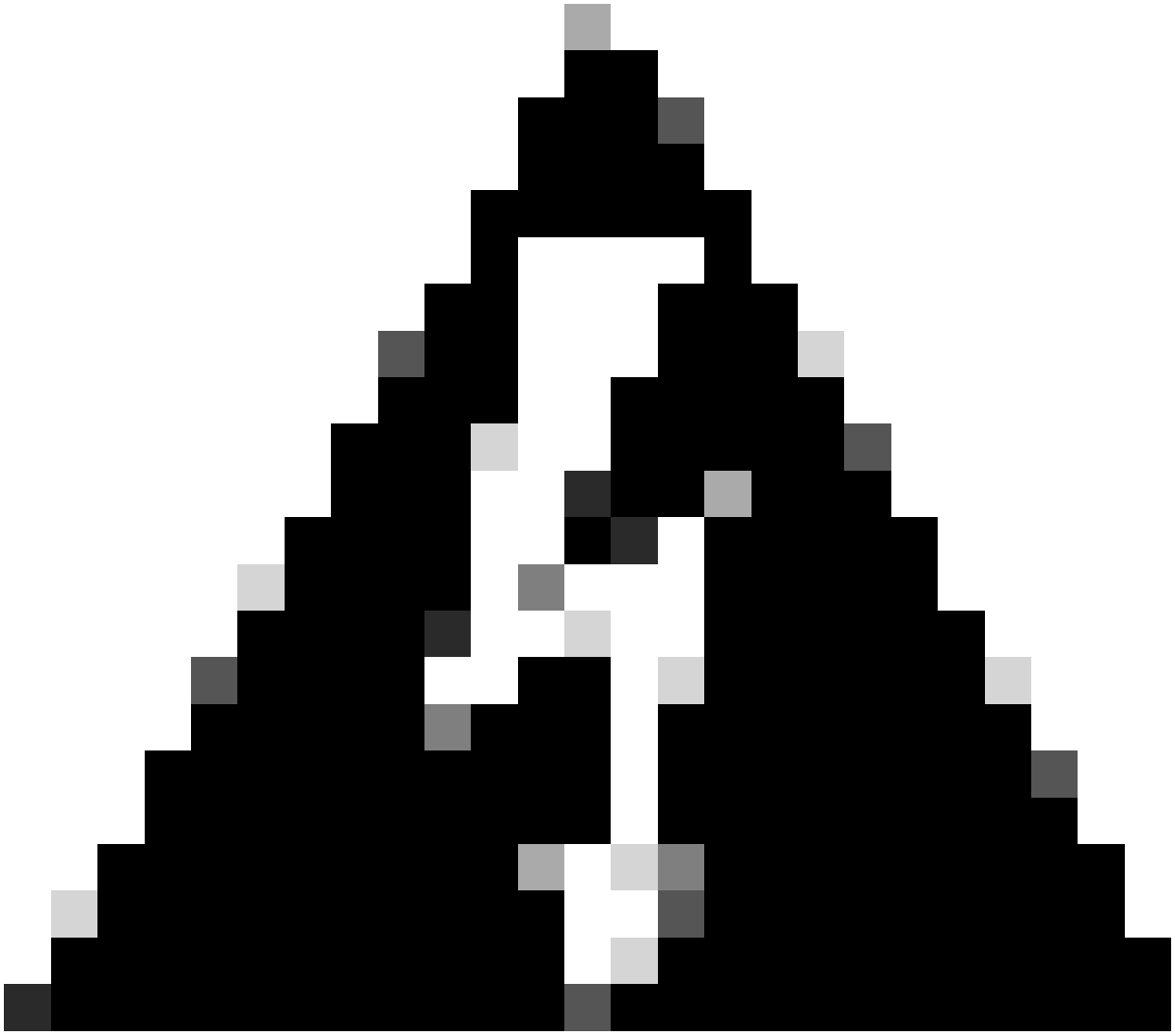
Étape 1 : activation du protocole NTP

```
feature ntp
```

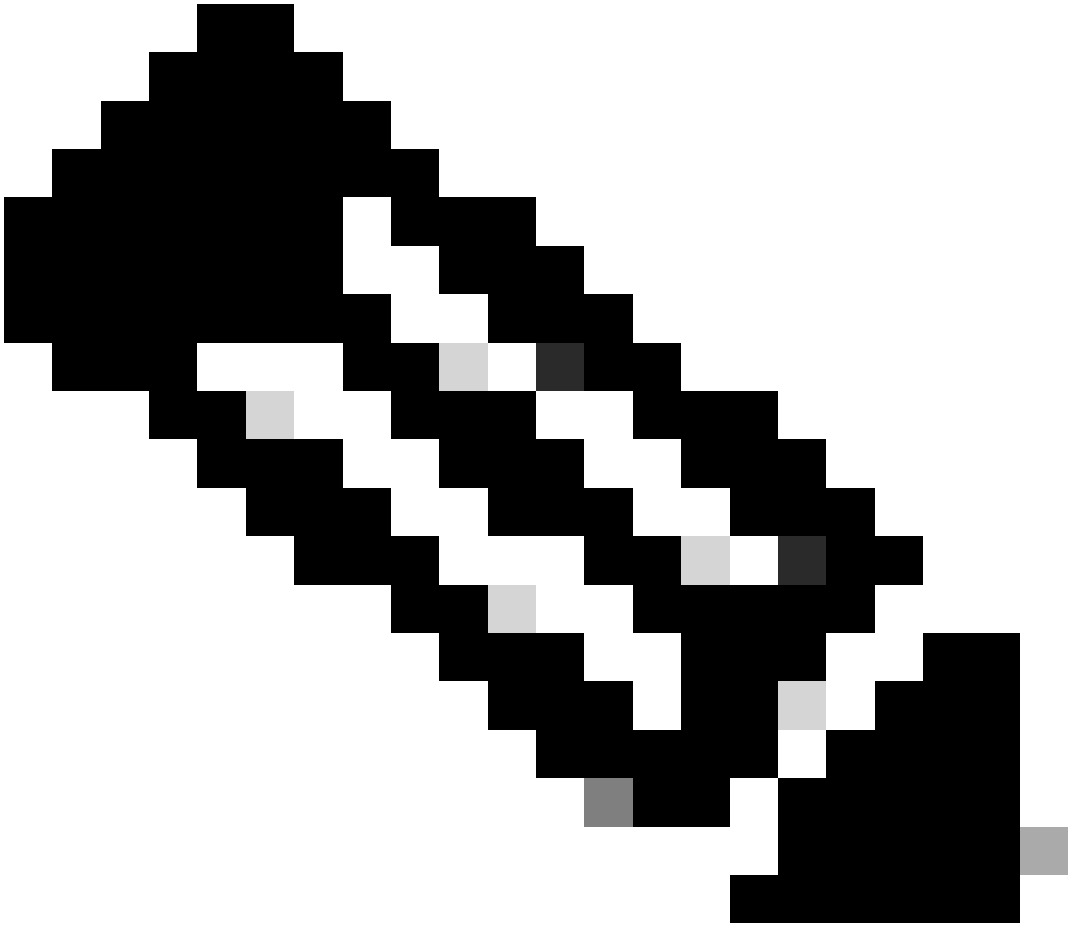
Étape 2 : définition du protocole d’horloge sur NTP

```
clock protocol ntp
```

Étape 3 : définition de Nexus comme client et serveur NTP



Avertissement : La synchronisation de ce protocole peut prendre quelques minutes, même après l’échange de paquets d’un serveur à un client.



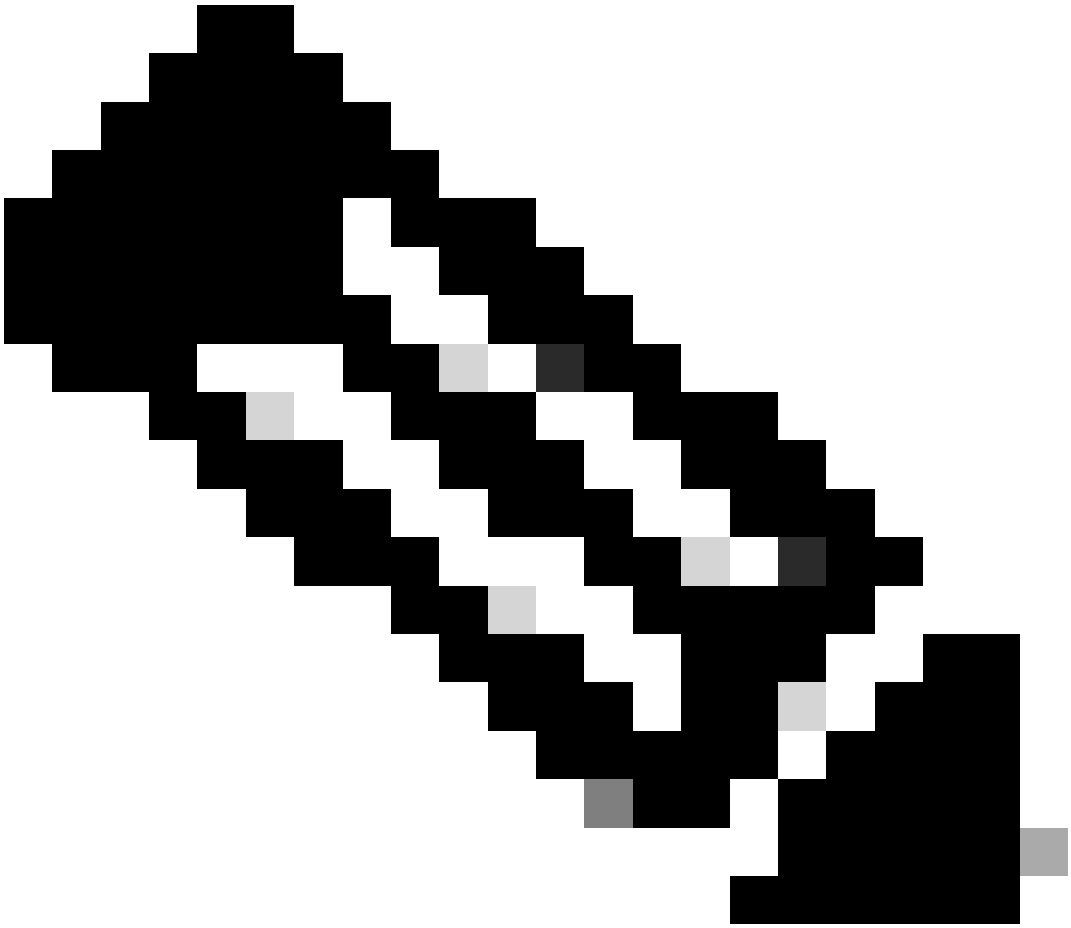
Remarque : Le concept de strate est utilisé par NTP pour indiquer la distance (en sauts NTP) entre une machine et une source temporelle faisant autorité. Cette valeur peut être configurée lors de l'activation du serveur NTP sur un Nexus avec la commande ntp master <stratum>.

```
N9K-1# show running-config ntp
ntp source 10.0.0.1
ntp master 1
```

```
N9K-2# show running-config ntp
ntp server 10.0.0.1 use-vrf default
ntp source 10.0.0.2
ntp master 8
```

```
N9K-3# show running-config ntp
ntp server 172.16.0.1 use-vrf default
ntp source 172.16.0.2
```

Vérifier

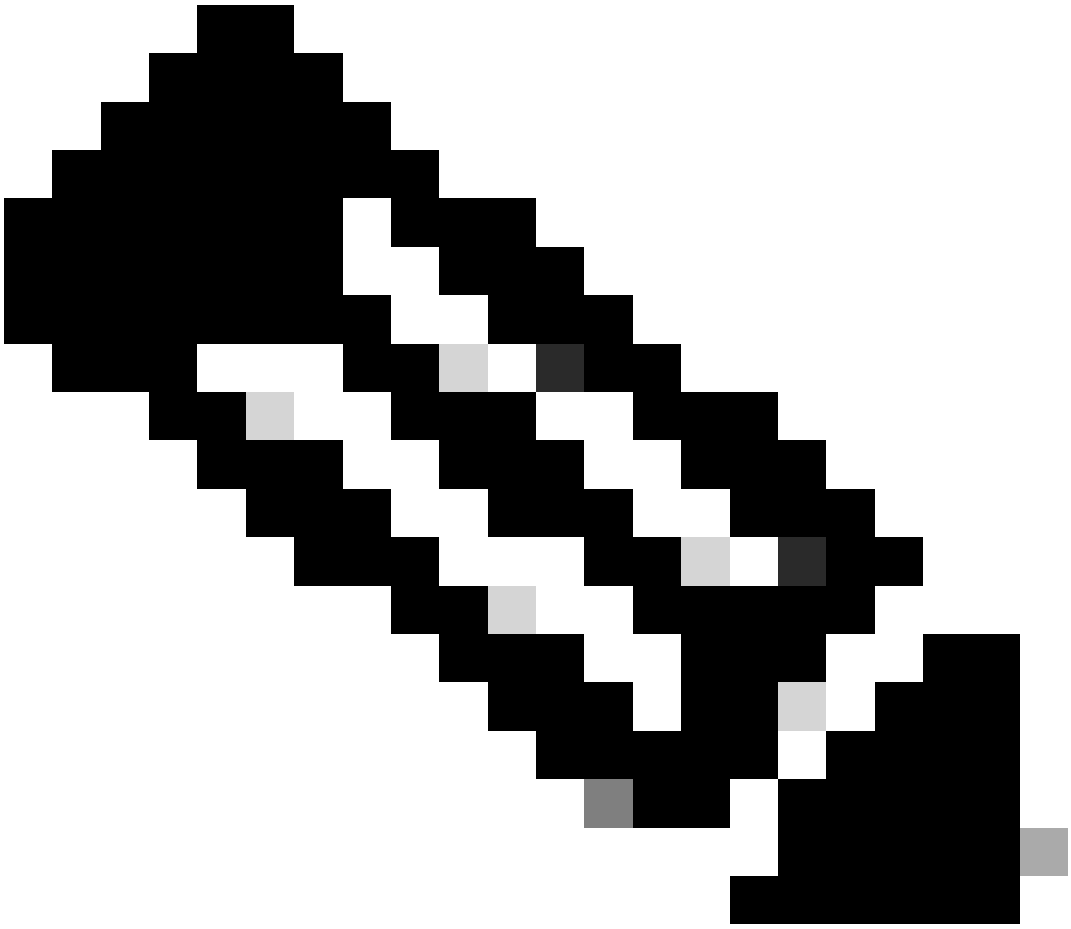


Remarque : À titre d'exemple, la vérification se concentre uniquement sur N9K-2, car il exécute les rôles serveur et client NTP simultanément.

1. Confirmer que l’horloge est configurée avec le protocole NTP

```
N9K-2# show clock
12:32:51.528 UTC Thu Sep 28 2023
Time source is NTP        <<<<<
```

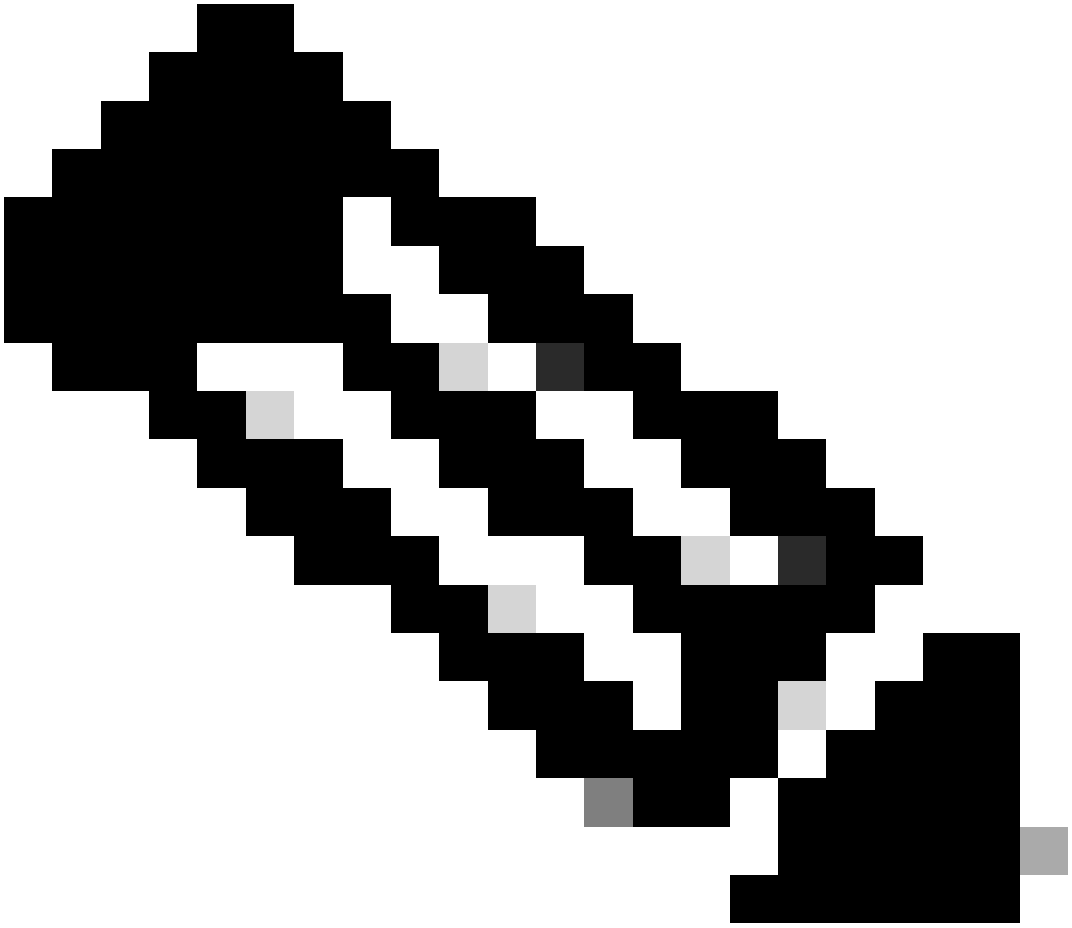
2. Confirmez que le serveur NTP et l'adresse IP Nexus sont répertoriés



Remarque : L'entrée avec l'adresse IP 127.127.1.0 est une adresse IP locale qui indique que le Nexus s'est synchronisé avec lui-même, représentant une source d'horloge de référence générée localement dans le cadre du rôle pour un serveur NTP.

```
N9K-2# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  10.0.0.1                      Server (configured)
  127.127.1.0                   Server (configured)    <<<
```

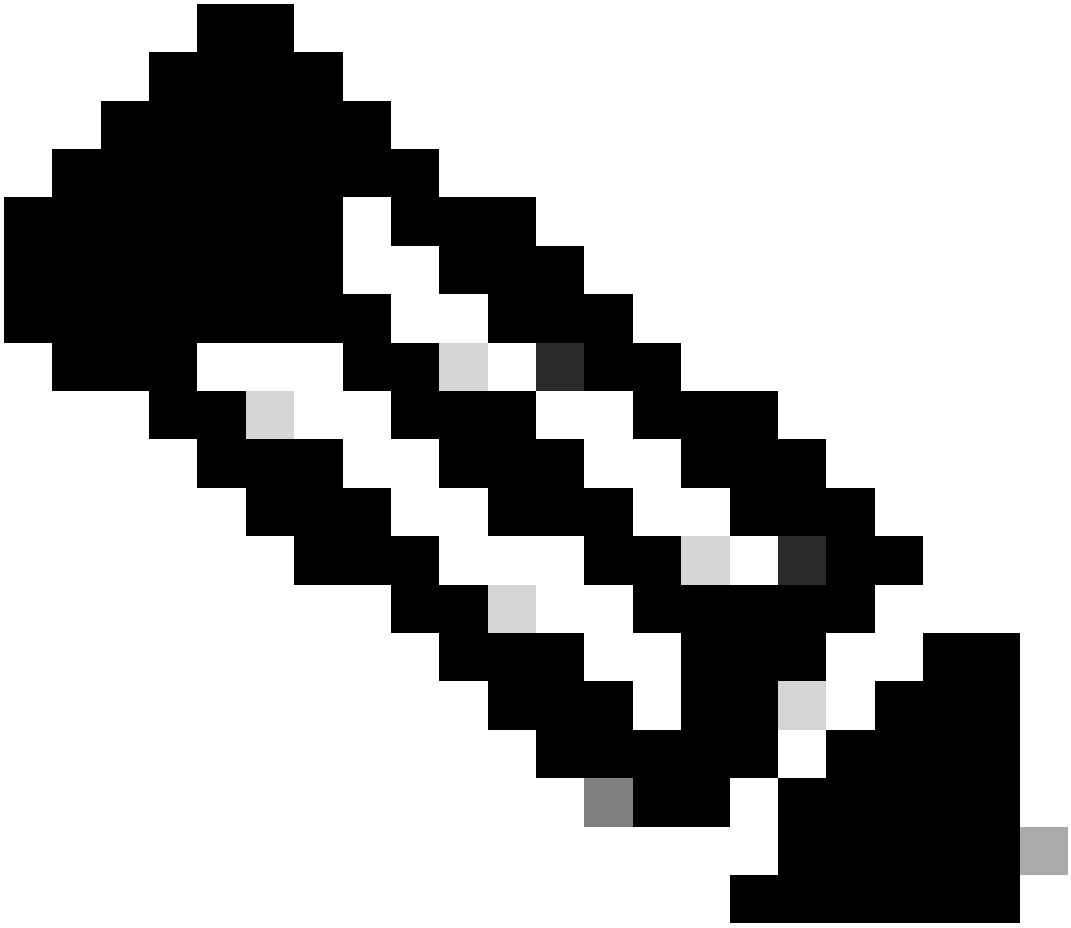
3. Confirmez que le serveur NTP configuré est sélectionné pour la synchronisation



Remarque : Une strate (st) de 16 indique que le serveur n'est pas actuellement synchronisé avec une source temporelle fiable et ne doit jamais être sélectionné pour la synchronisation. À partir de la version 10.1(1) de Cisco NX-OS, seule une strate de 13 ou moins peut être synchronisée.

```
N9K-2# show ntp peer-status
Total peers : 2
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote                                  local                                          st   poll   reach de
-------------------------------------------------------------------------------------------------------------
=127.127.1.0                              10.0.0.2                                       8   16       0   0.00
*10.0.0.1                                 10.0.0.2                                       2   32     377   0.00
```

4. Vérifiez que les paquets NTP sont reçus et envoyés au serveur



Remarque : La commande show ntp statistics peer ipaddr <ntp-server> ne fonctionne que pour les clients NTP. S'il existe des valeurs non définies par défaut sur les compteurs, vous pouvez les effacer à l'aide de la commande suivante : clear ntp statistics all-peers.

```
N9K-2# show ntp statistics peer ipaddr 10.0.0.1
remote host:          10.0.0.1
local interface:      10.0.0.2
time last received:   28s
time until next send: 5s
reachability change:  876s
packets sent:         58     <<<<<
packets received:     58     <<<<<
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      6
```

Exemple de capture de paquets pour le flux de paquets NTP bidirectionnel :

```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0
Capturing on 'ps-inb'
    4 2024-01-01 03:23:47.900233043   172.16.0.2 → 172.16.0.1   NTP 90 NTP Version 4, client
2     5 2024-01-01 03:23:47.900863464   172.16.0.1 → 172.16.0.2   NTP 90 NTP Version 4, server
    6 2024-01-01 03:23:52.926382561     10.0.0.2 → 10.0.0.1     NTP 90 NTP Version 4, client
4     7 2024-01-01 03:23:52.927169592     10.0.0.1 → 10.0.0.2     NTP 90 NTP Version 4, server
```

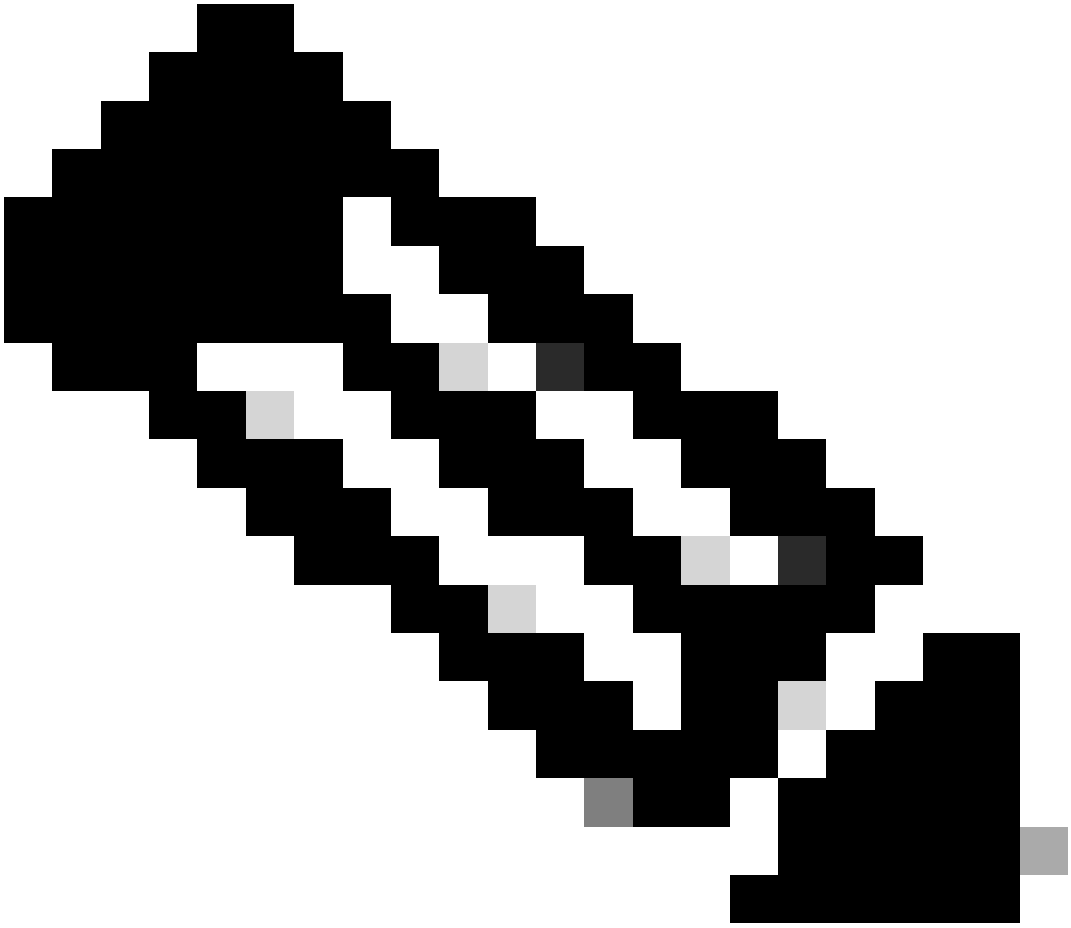
5. Recherchez le paquet envoyé de Nexus à son client NTP pour confirmer son utilisation du serveur NTP configuré comme référence

```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0 detail
Capturing on 'ps-inb'
...

...
Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface ps-inb, id 0
    Interface id: 0 (ps-inb)
        Interface name: ps-inb
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan  1, 2024 03:24:35.900699824 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1704079475.900699824 seconds
    [Time delta from previous captured frame: 0.000643680 seconds]
    [Time delta from previous displayed frame: 0.000643680 seconds]
    [Time since reference or first frame: 10.974237168 seconds]
    Frame Number: 5
    Frame Length: 90 bytes (720 bits)
    Capture Length: 90 bytes (720 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ntp]
Ethernet II, Src: d4:77:98:2b:4c:87, Dst: f8:0b:cb:e5:d9:fb
    Destination: f8:0b:cb:e5:d9:fb
        Address: f8:0b:cb:e5:d9:fb
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: d4:77:98:2b:4c:87
        Address: d4:77:98:2b:4c:87
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 76
    Identification: 0xbd85 (48517)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
```

```
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)                                    <<<<< UDP protocol number
    Header checksum: 0xa5f7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.0.1                                    <<<<<
    Destination: 172.16.0.2                               <<<<< NTP Client
User Datagram Protocol, Src Port: 123, Dst Port: 123
    Source Port: 123
    Destination Port: 123
    Length: 56
    Checksum: 0x71d5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
        [Time since first frame: 0.000643680 seconds]
        [Time since previous frame: 0.000643680 seconds]
Network Time Protocol (NTP Version 4, server)
    Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
        00.. .... = Leap Indicator: no warning (0)
        ..10 0... = Version number: NTP Version 4 (4)
        .... .100 = Mode: server (4)
    Peer Clock Stratum: secondary reference (3)
    Peer Polling Interval: 4 (16 seconds)
    Peer Clock Precision: 0.000000 seconds
    Root Delay: 0.001083 seconds
    Root Dispersion: 0.013611 seconds
    Reference ID: 10.0.0.1                                      <<<<< NTP server
    Reference Timestamp: Jan  1, 2024 03:22:32.927228435 UTC
    Origin Timestamp: Jan  1, 2024 03:24:35.896950020 UTC
    Receive Timestamp: Jan  1, 2024 03:24:35.900271042 UTC
    Transmit Timestamp: Jan  1, 2024 03:24:35.900397771 UTC
```

6. Exécutez un ELAM pour vérifier si les paquets sont correctement affectés aux statistiques des ACL de redirection du superviseur (COPP)



Remarque : Le trafic NTP doit être acheminé vers le CPU, de sorte qu'il a l'indicateur sup_hit défini.

```
N9K-2# debug platform internal tah elam
N9K-2(TAH-elam)# trigger init
Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in-select 6, out-select
N9K-2(TAH-elam-insel6)# reset
N9K-2(TAH-elam-insel6)# set outer ipv4 next-protocol 17 packet-len 76 src_ip 10.0.0.1 dst_ip 10.0.0.2
N9K-2(TAH-elam-insel6)# start
N9K-2(TAH-elam-insel6)# report
SUGARBOWL ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 0
============================

Incoming Interface: Eth1/48
Src Idx : 0xbd, Src BD : 4147
Outgoing Interface Info: dmod 0, dpid 0
Dst Idx : 0x5bf, Dst BD : 4147

Packet Type: IPv4
```

```
Dst MAC address: D4:77:98:2B:4C:87
Src MAC address: D4:77:98:2B:43:27

Sup hit: 1,  Sup Idx: 2753          <<<<< packet punt identifier, use below CLI to resolve its meaning

Dst IPv4 address: 10.0.0.2
Src IPv4 address: 10.0.0.1
Ver     =  4, DSCP    =    0, Don't Fragment = 0
Proto   = 17, TTL     =  255, More Fragments = 0
Hdr len = 20, Pkt len =   76, Checksum       = 0xae26

L4 Protocol  : 17
UDP Dst Port : 123
UDP Src Port : 123

Drop Info:
----------

LUA:
LUB:
LUC:
LUD:
Final Drops:

vntag:
vntag_valid    : 0
vntag_vir      : 0
vntag_svif     : 0

ELAM not triggered yet on slot - 1, asic - 0, slice - 1

N9K-2(TAH-elam-insel6)#  show system internal access-list sup-redirect-stats | i 2753
    2753                            copp-system-p-acl-ntp    462        <<<<< correct ACL assigned
```

Informations connexes

[Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 9000, version 10.2(x)]

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.