Konfiguration des Network Time Protocol auf Nexus als Server und Client

Inhalt

Einleitung

In diesem Dokument wird eine einfache Konfiguration und Validierung für eine Nexus 9000-Plattform beschrieben, die sowohl als NTP-Server (Network Time Protocol) als auch als Client fungiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Nexus NX-OS-Software
- Network Time Protocol (NTP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Nexus 9000 mit NX-OS-Version 10.2(5).

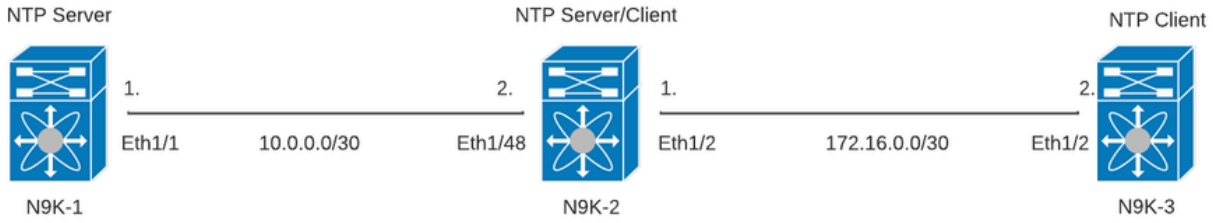
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

NTP ist ein Netzwerkprotokoll zum Synchronisieren der Uhrzeit einer Gruppe von Geräten in einem Netzwerk, um Ereignisse zu korrelieren, wenn Sie Systemprotokolle und andere zeitspezifische Ereignisse von mehreren Netzwerkgeräten empfangen.

Netzwerkdiagramm



Konfigurationen

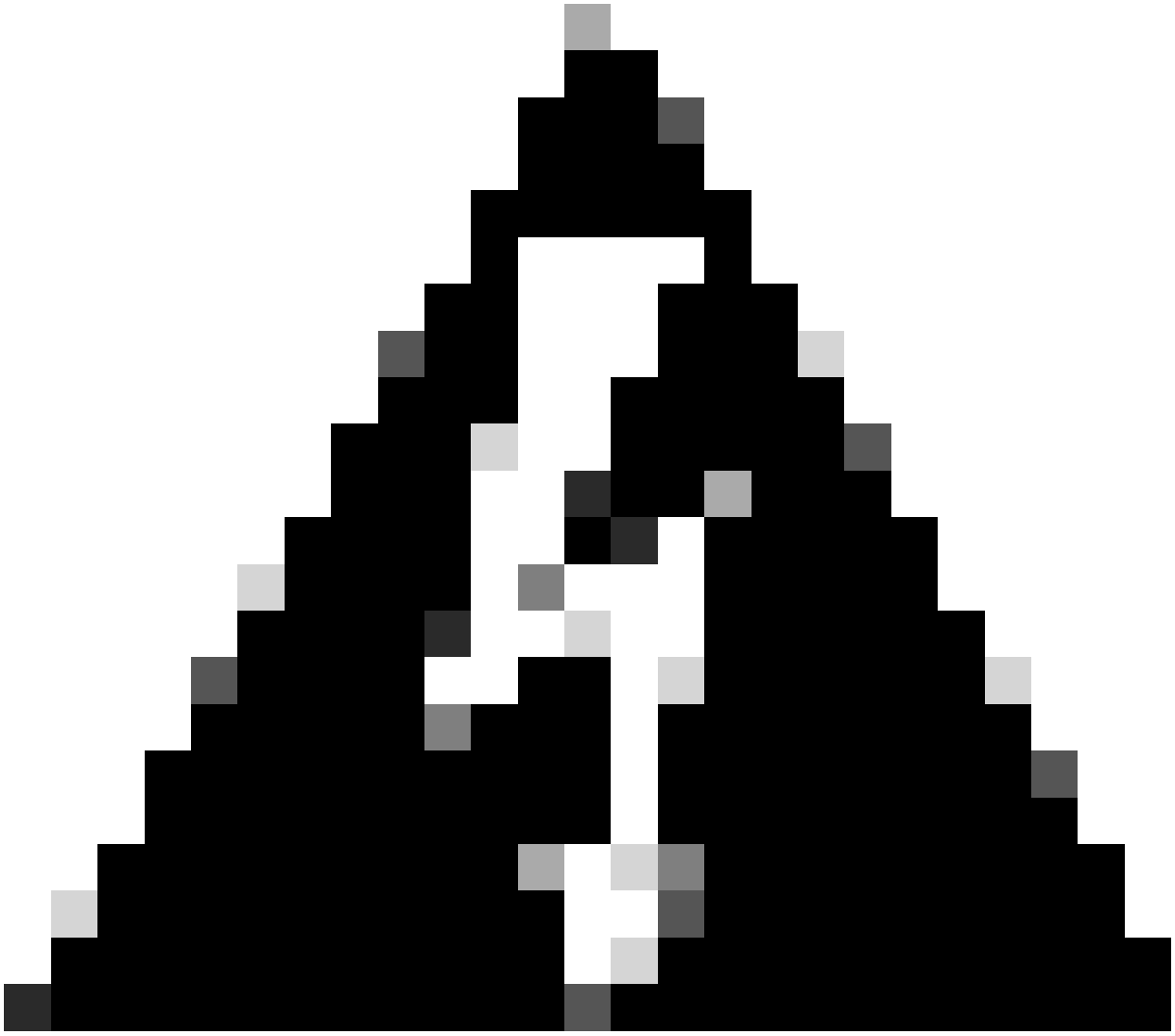
Schritt 1: NTP aktivieren.

```
feature ntp
```

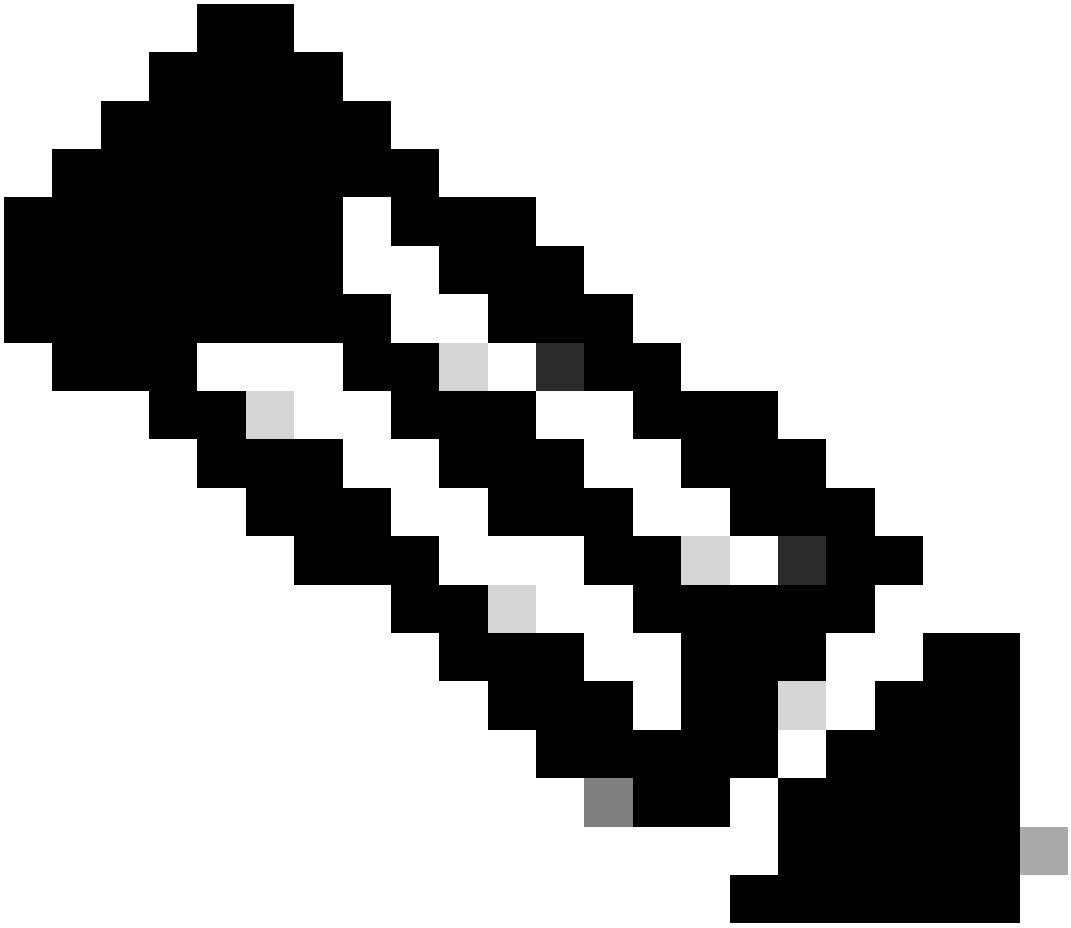
Schritt 2: Setzen Sie das Uhrenprotokoll auf NTP.

```
clock protocol ntp
```

Schritt 3: Definieren Sie Nexus als NTP-Client und -Server.



Warnung: Die Synchronisierung dieses Protokolls kann einige Minuten dauern, auch nachdem Pakete von Server zu Client ausgetauscht wurden.



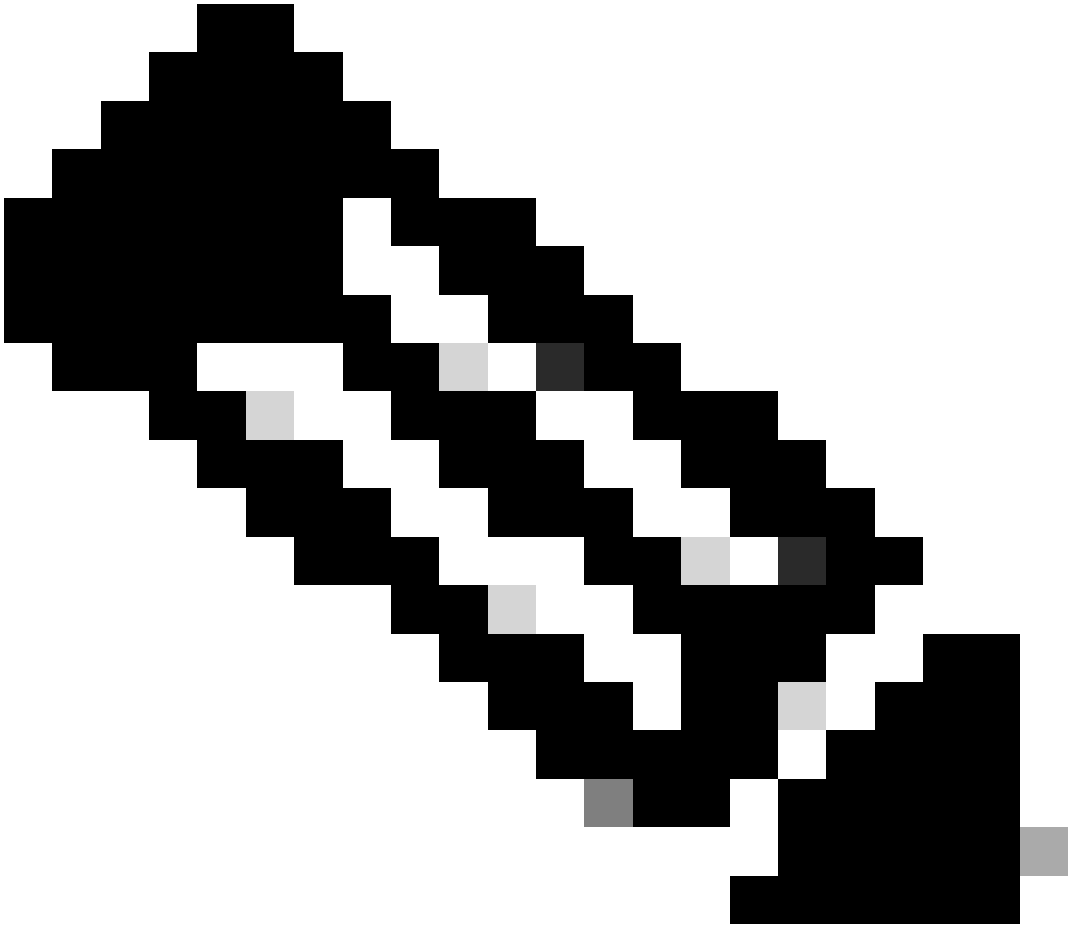
Hinweis: Das Konzept einer Schicht wird vom NTP verwendet, um den Abstand (in NTP-Hops) zwischen einer Maschine und einer maßgeblichen Zeitquelle anzugeben. Dieser Wert kann konfiguriert werden, wenn der NTP-Server auf einem Nexus mit dem Befehl "ntp master <stratum>" aktiviert wird.

```
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
```

Überprüfung

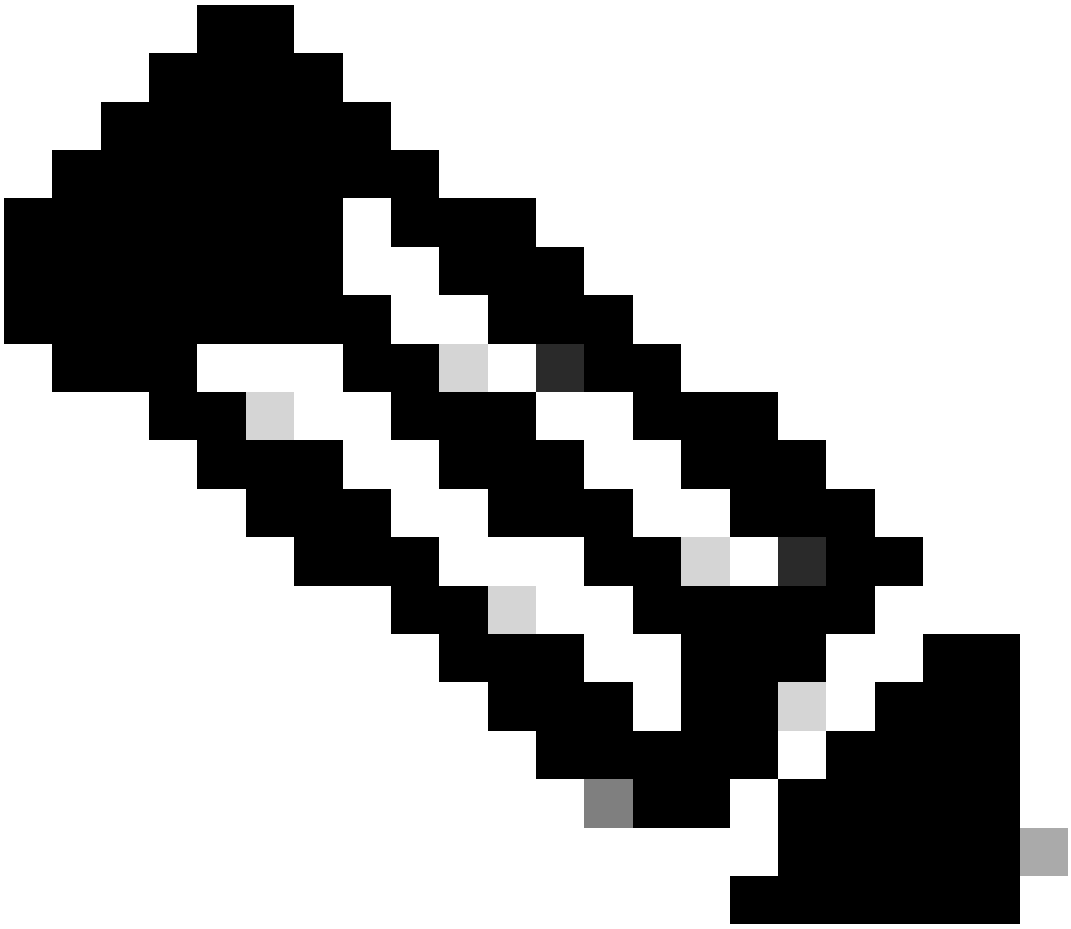


> Hinweis: Zur Veranschaulichung konzentriert sich die Verifizierung nur auf N9K-2, da NTP-Server- und Client-Rollen gleichzeitig ausgeführt werden.

1. Bestätigung, dass die Uhr mit dem NTP-Protokoll konfiguriert wurde

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

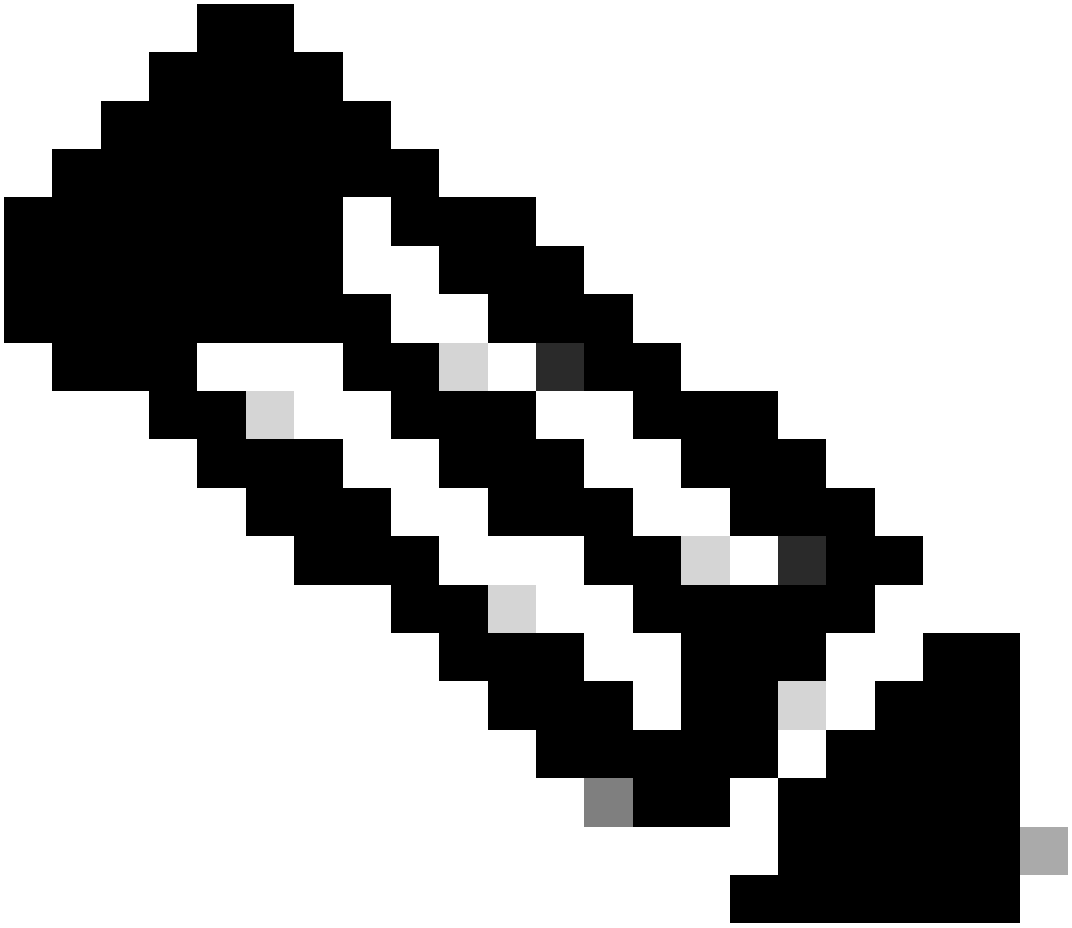
2. Bestätigen Sie, dass der NTP-Server und die Nexus IP aufgeführt sind.



Hinweis: Der Eintrag mit der IP-Adresse 127.127.1.0 ist eine lokale IP-Adresse, die angibt, dass der Nexus eine Synchronisierung mit sich selbst durchgeführt hat. Dies stellt eine lokal generierte Referenzuhr als Teil der Rolle eines NTP-Servers dar.

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

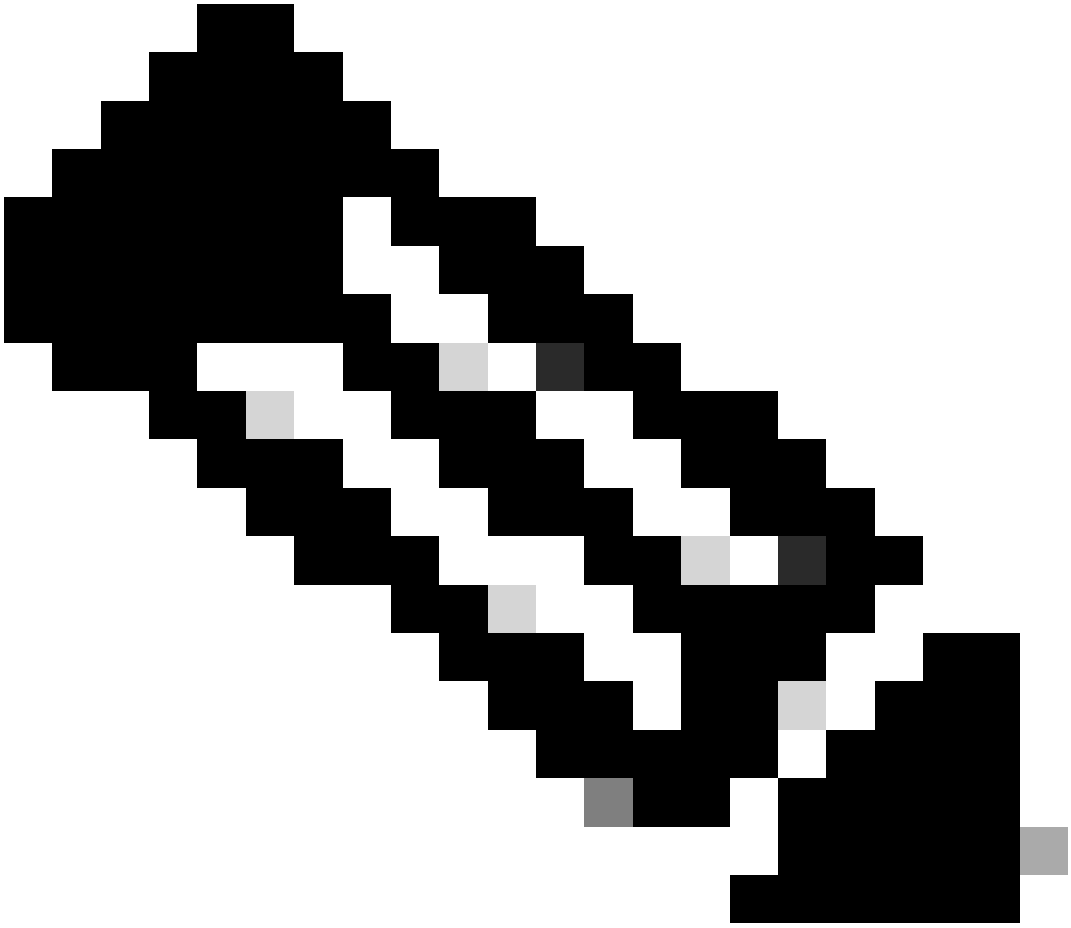
3. Bestätigen Sie, dass der konfigurierte NTP-Server für die Synchronisierung ausgewählt ist.



Hinweis: Eine Schicht (st) von 16 gibt an, dass der Server derzeit nicht mit einer zuverlässigen Zeitquelle synchronisiert ist und niemals für die Synchronisierung ausgewählt werden kann. Ab der Cisco NX-OS-Version 10.1(1) ist die Synchronisierung nur in einer Schicht von 13 oder weniger möglich.

```
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. Vergewissern Sie sich, dass NTP-Pakete empfangen und an den Server gesendet werden.



Hinweis: Der Befehl "show ntp statistics peer ipaddr <ntp-server>" funktioniert nur für NTP-Clients. Wenn Leistungsindikatoren nicht standardmäßige Werte enthalten, können Sie diese mit dem Befehl "clear ntp statistics all-peers" löschen.

```
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
```

Beispiel für die Paketerfassung für den bidirektionalen NTP-Paketfluss:

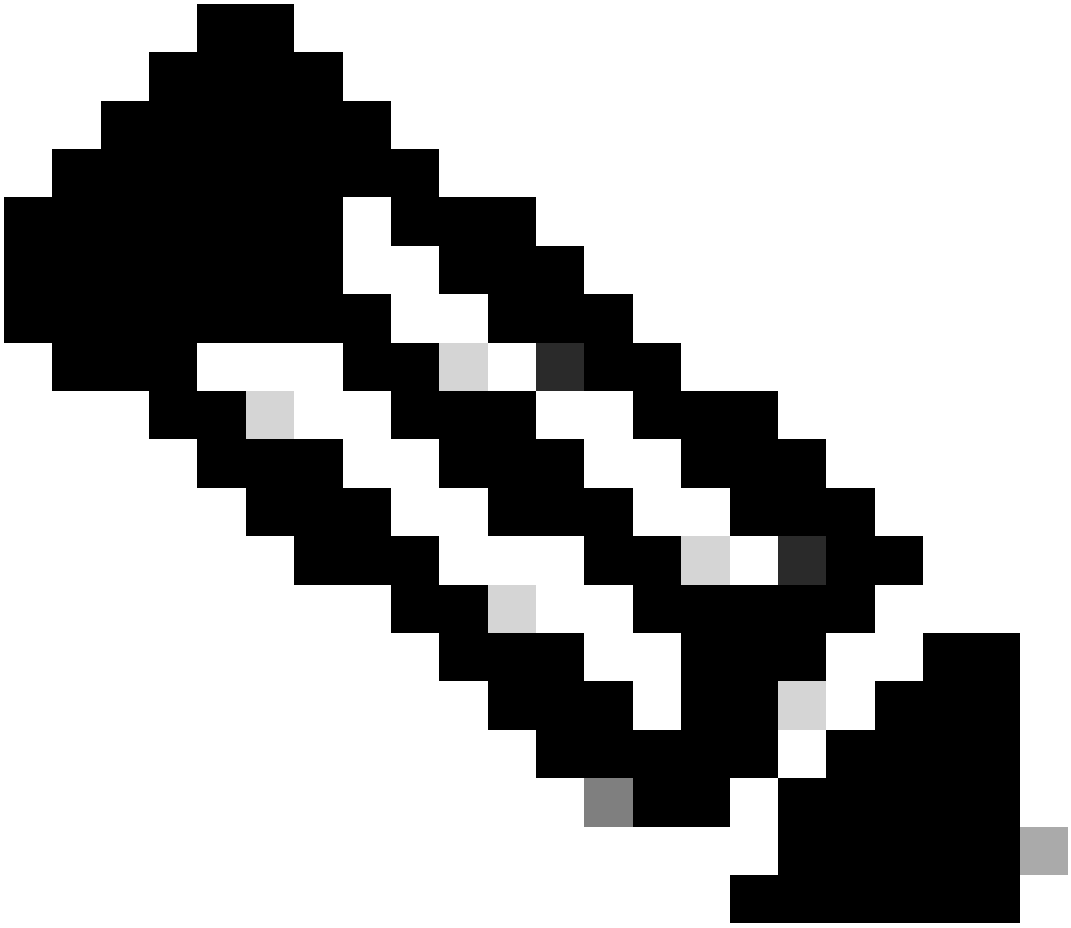
```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0
Capturing on 'ps-inb'
    4 2024-01-01 03:23:47.900233043   172.16.0.2 → 172.16.0.1   NTP 90 NTP Version 4, client
2     5 2024-01-01 03:23:47.900863464   172.16.0.1 → 172.16.0.2   NTP 90 NTP Version 4, server
    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. Suchen Sie nach dem vom Nexus an den NTP-Client gesendeten Paket, um die Verwendung des konfigurierten NTP-Servers als Referenz zu bestätigen:

```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0 detail
Capturing on 'ps-inb'
...
<output omitted>
...
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. Führen Sie ein ELAM aus, um zu überprüfen, ob die Pakete den Statistiken der ACLs für die Umleitung durch den Supervisor (COPP) richtig zugewiesen sind:



Hinweis: NTP-Datenverkehr muss an die CPU gesendet werden, daher ist das sup_hit-Flag gesetzt.

```
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
```

Zugehörige Informationen

[Cisco Nexus Serie 9000 NX-OS - Systemmanagement-Konfigurationsleitfaden, Version 10.2(x)]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.