在Nexus上将网络时间协议配置为服务器和客户端

目录

简介

本文档介绍对Nexus 9000平台进行简单配置和验证，以同时充当网络时间协议(NTP)服务器和客户端。

先决条件

要求

Cisco建议您了解以下主题：

- Nexus NX-OS 软件。
- 网络时间协议(NTP)。

使用的组件

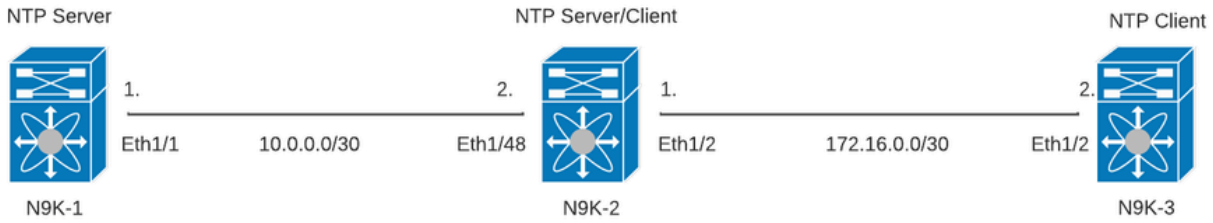
本文档中的信息基于NXOS版本10.2(5)的Cisco Nexus 9000。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

NTP是一种网络协议，用于同步网络中一组设备的时间，以便在从多个网络设备接收系统日志和其他特定时间事件时关联事件。

网络图



配置

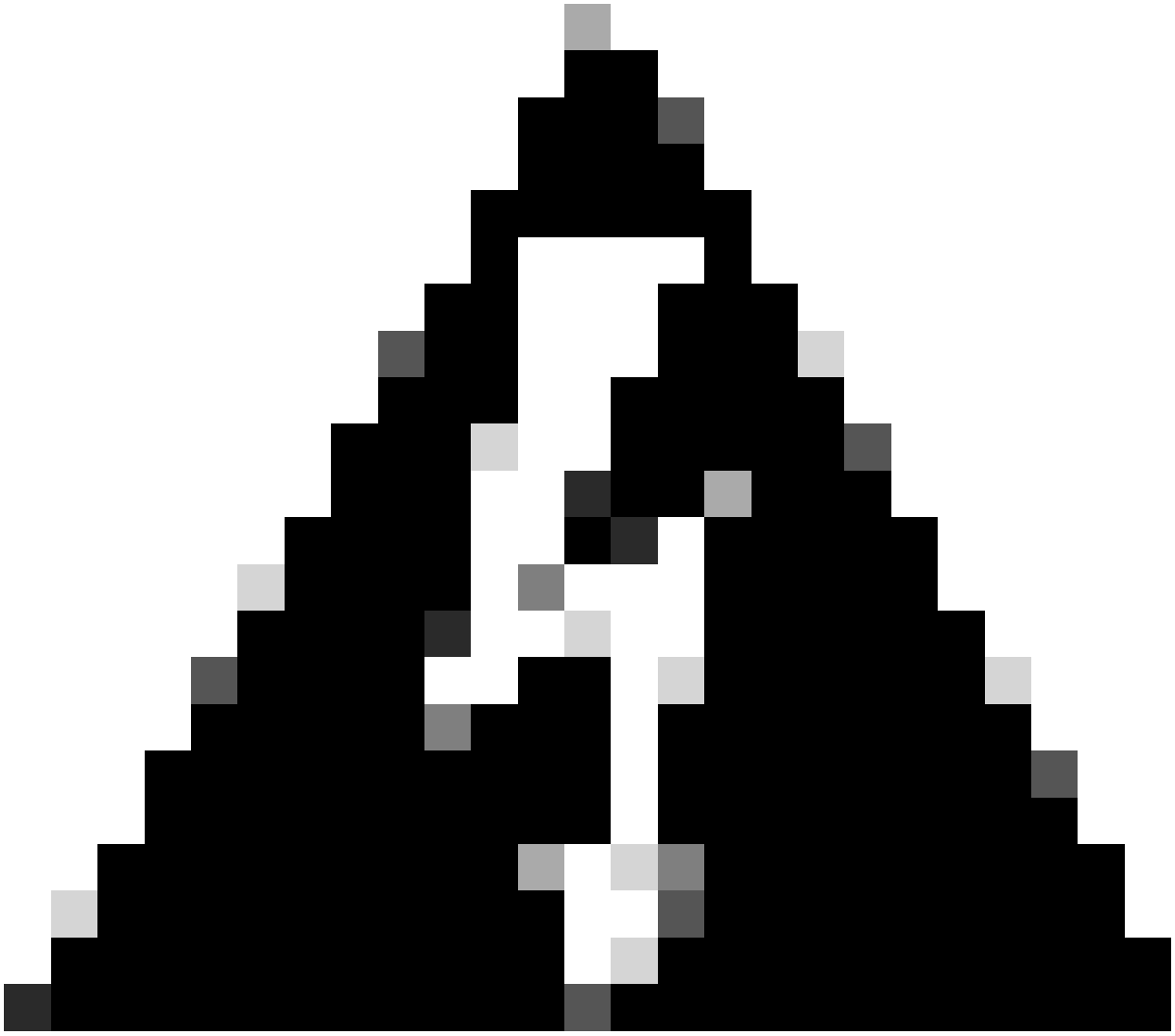
步骤1:启用NTP。

```
feature ntp
```

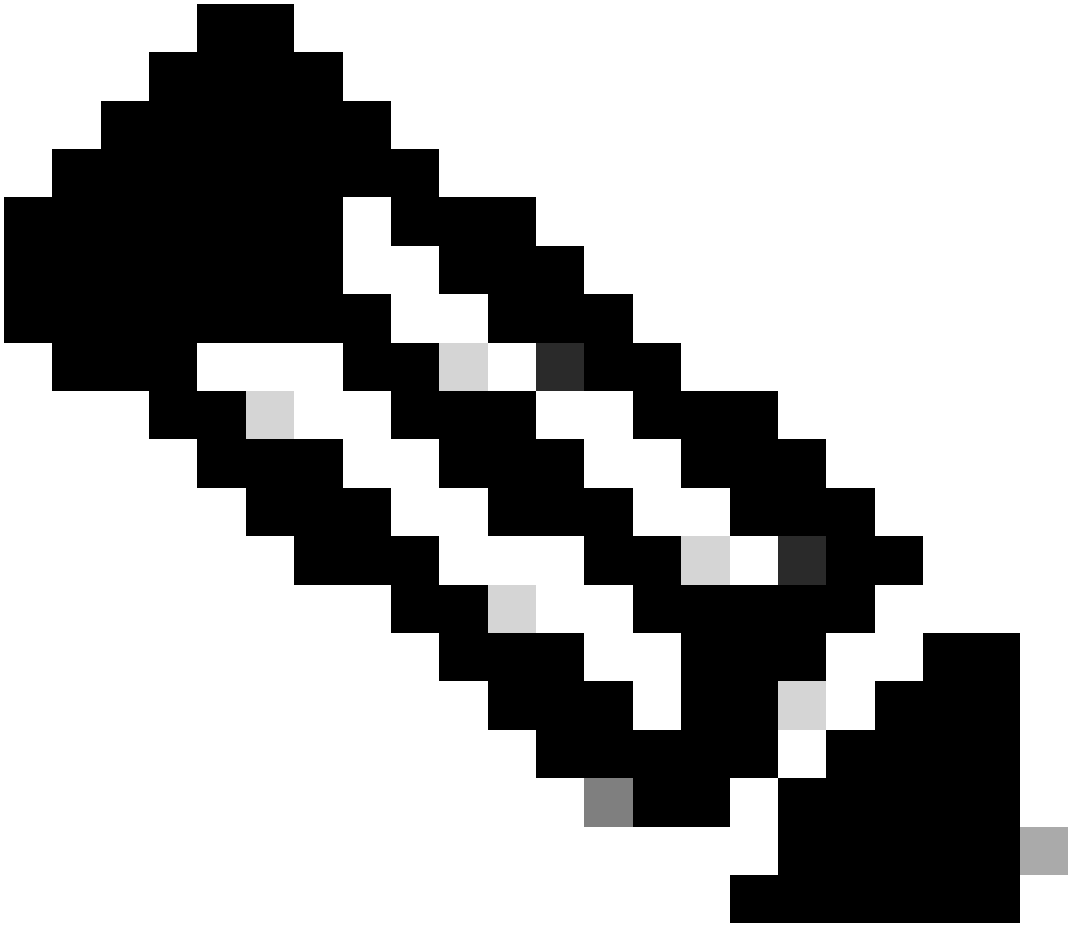
第二步：将时钟协议设置为NTP。

```
clock protocol ntp
```

第三步：将Nexus定义为NTP客户端和服务器。



警告：即使是在从服务器到客户端交换数据包后，此协议仍可能需要几分钟才能同步。



注意：NTP采用层的概念来表示机器和权威时间源之间的距离（以NTP跳为单位）。在使用“ntp master <stratum>”命令在Nexus上启用NTP服务器时，可以配置此值。

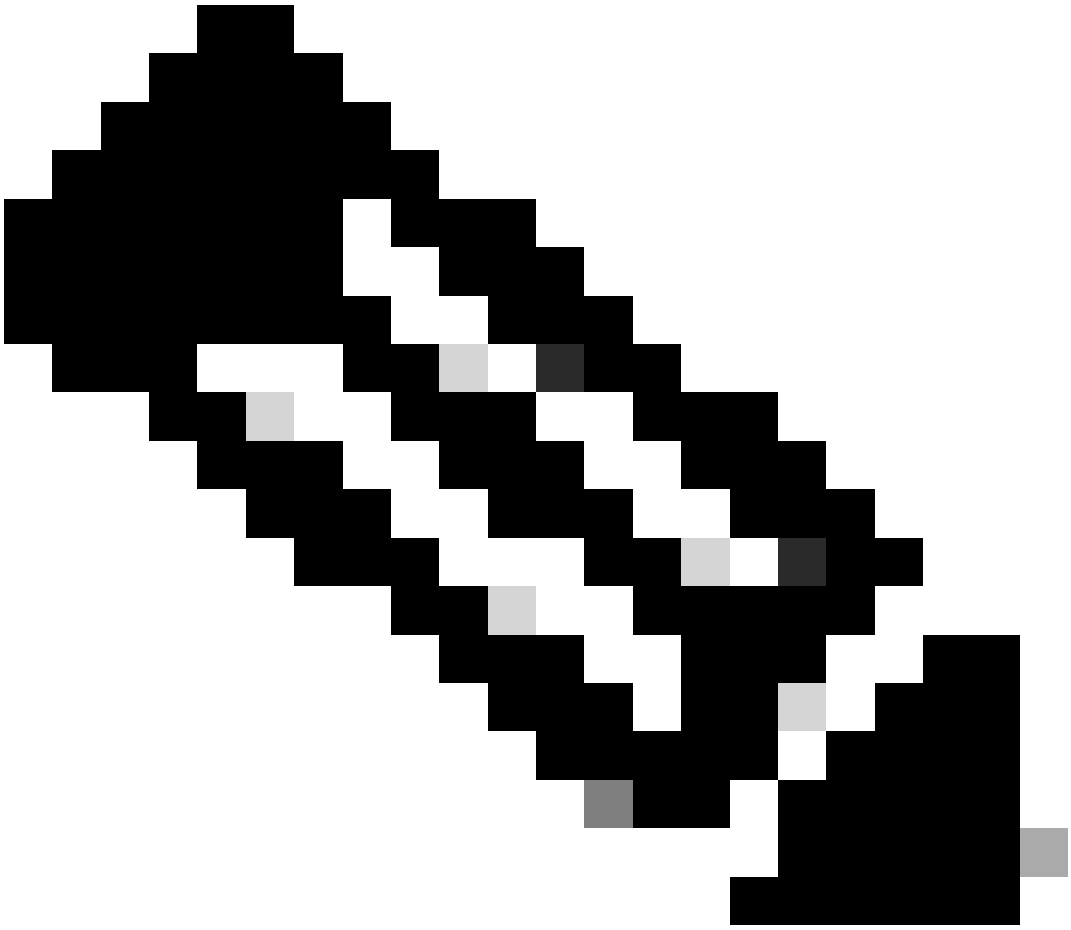
```
N9K-1# show running-config ntp
ntp source 10.0.0.1
ntp master 1
```

```
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
```

验证

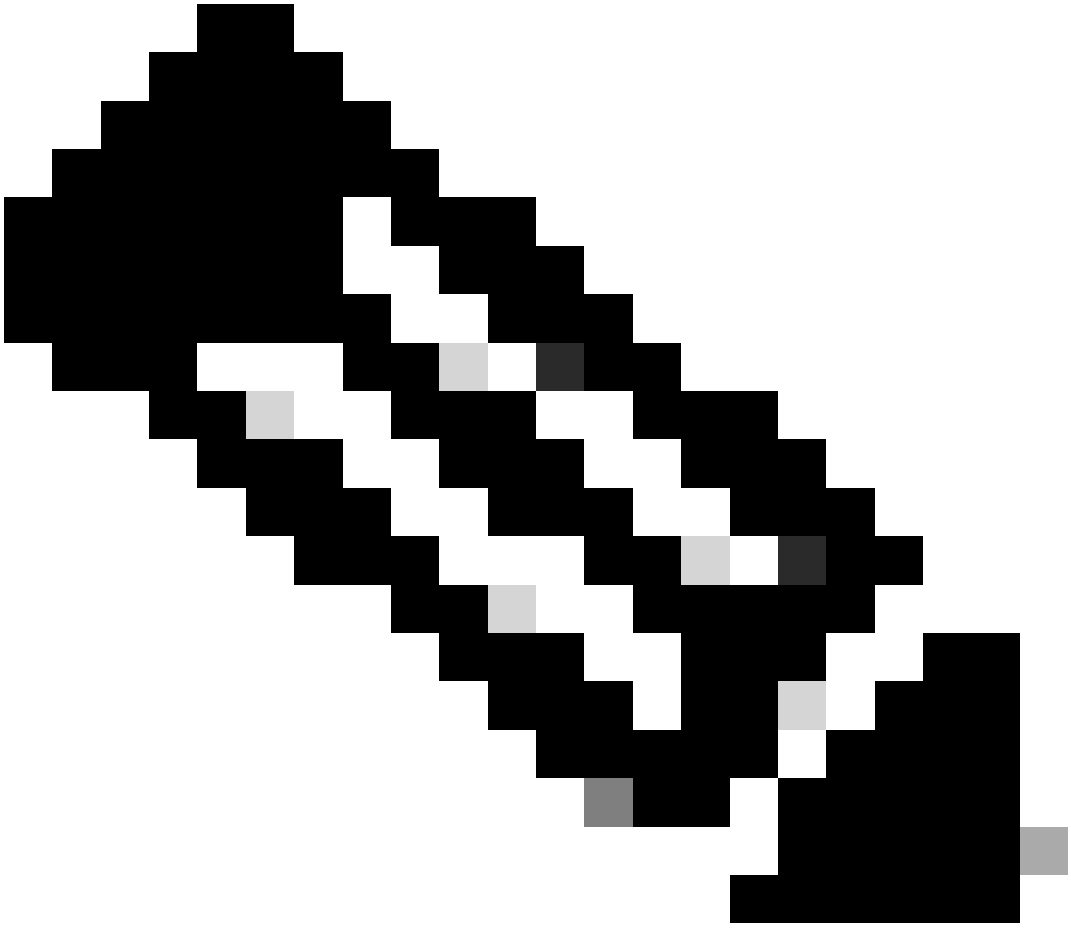


注意：出于验证目的，验证仅关注N9K-2，因为它同时运行NTP服务器和客户端角色。

1. 确认时钟已配置了NTP协议。

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

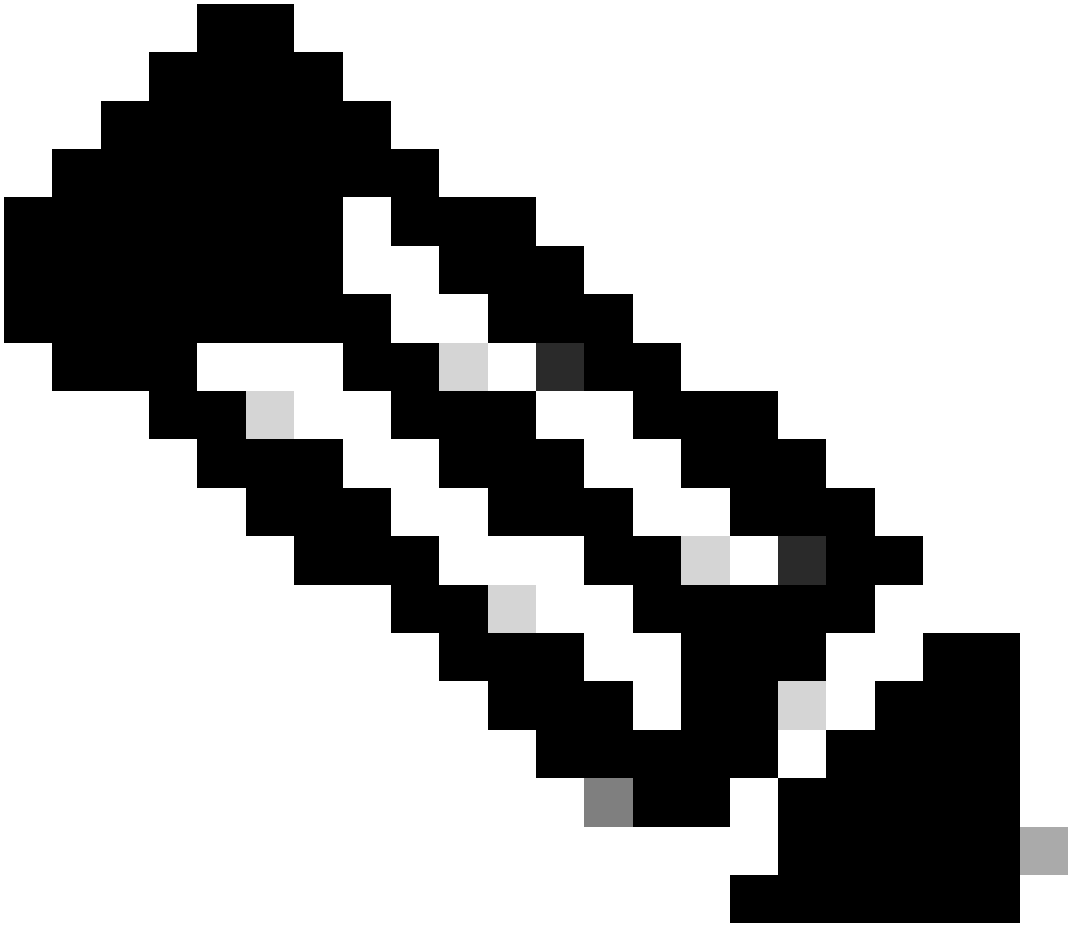
2. 确认NTP服务器和Nexus IP已列出。



注意：IP地址为127.127.1.0的条目是本地IP，指示Nexus已与自身同步，表示作为NTP服务器角色一部分的本地生成的参考时钟源。

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

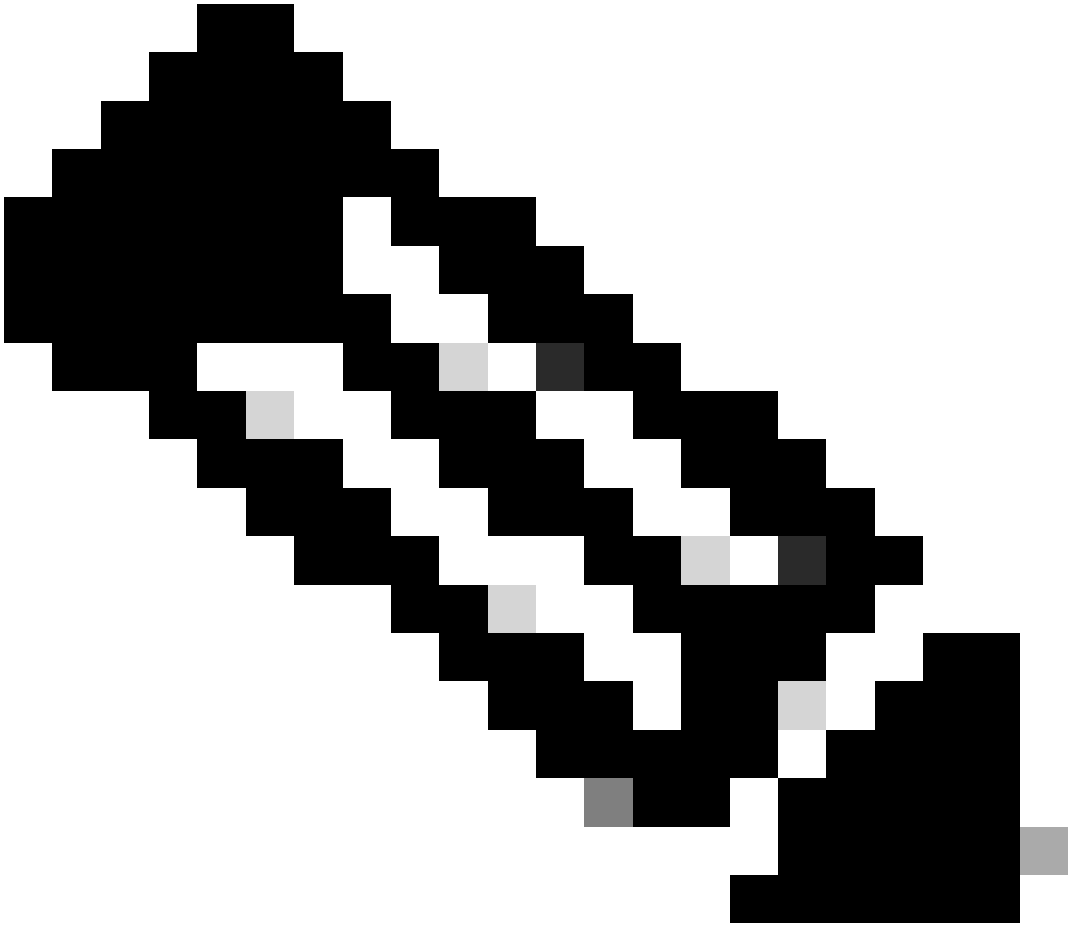
3. 确认已选择配置的NTP服务器进行同步。



注意：第16层表示服务器当前未同步到可靠的时间源，并且永远不会选择服务器进行同步。从Cisco NX-OS版本10.1(1)开始，只有13层或更低层可以同步。

```
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. 验证NTP数据包是否已接收并发送至服务器。



注意：命令“show ntp statistics peer ipaddr <ntp-server>”仅适用于NTP客户端。如果计数器上有非默认值，可以使用命令“clear ntp statistics all-peers”清除它们。

```
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
```

双向NTP数据包流的数据包捕获示例：

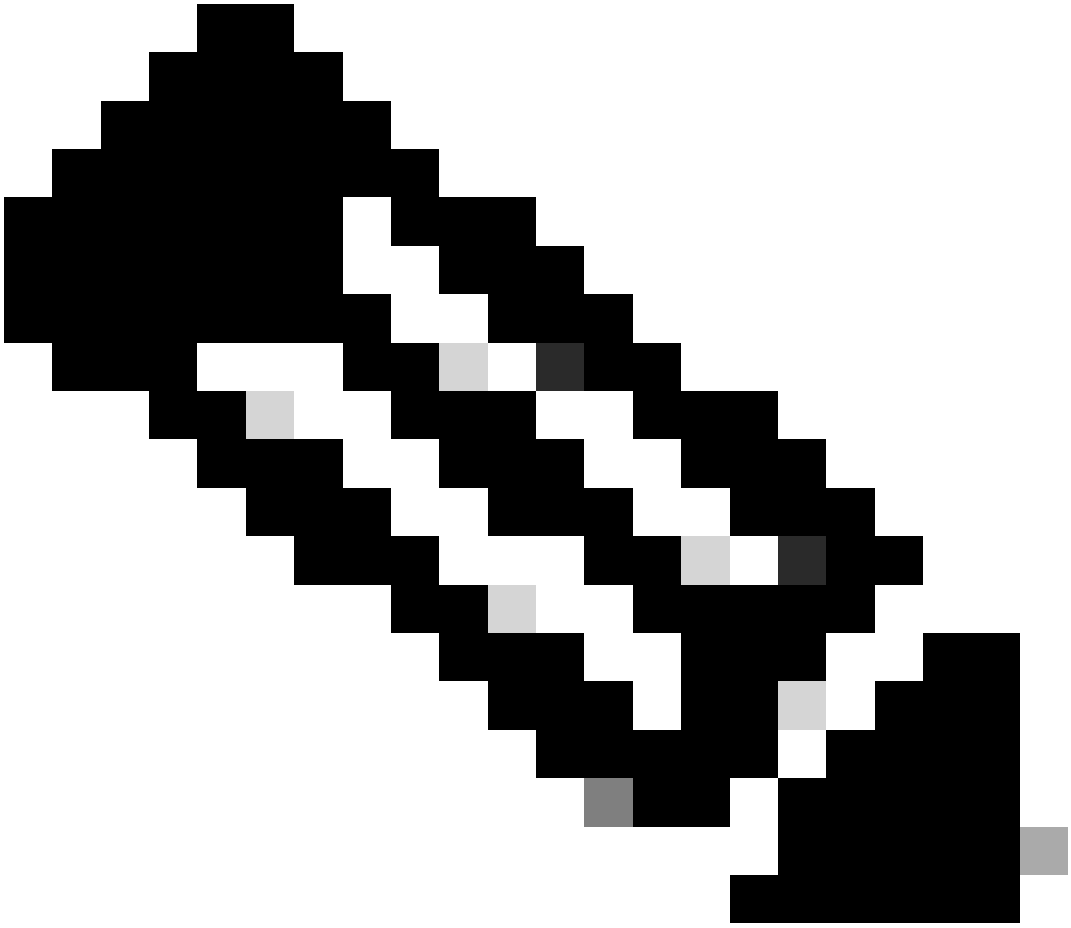
```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0
Capturing on 'ps-inb'
    4 2024-01-01 03:23:47.900233043   172.16.0.2 → 172.16.0.1   NTP 90 NTP Version 4, client
2     5 2024-01-01 03:23:47.900863464   172.16.0.1 → 172.16.0.2   NTP 90 NTP Version 4, server
    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. 搜索从Nexus发送到其NTP客户端的数据包，以使用配置的NTP服务器作为参考来确认该数据包：

```
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. 运行ELAM以验证是否已将数据包正确分配给管理引擎(COPP)重定向ACL的统计信息：



注意：NTP流量必须传送到CPU，因此它设置了sup_hit标志。

```
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
```

相关信息

[Cisco Nexus 9000系列NX-OS系统管理配置指南，版本10.2(x)]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。