Solucionar problemas de Network Time Protocol (NTP) no vEdge

Contents

Introduction

Este documento descreve como solucionar problemas do Network Time Protocol (NTP) com comandos **show ntp** e ferramentas de captura de pacotes em plataformas vEdge.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não está restrito a versões de software ou modelos vEdge específicos.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Exemplo de sintomas de problemas de NTP

A perda de sincronização de NTP para um vEdge pode se manifestar de algumas maneiras diferentes, por exemplo:

- Tempo incorreto na saída de **show clock** no dispositivo.

- Certificados considerados inválidos devido a um tempo incorreto fora do intervalo de validade.
- Carimbos de data/hora incorretos nos logs.

Comandos show do NTP

Para iniciar o isolamento de problemas de NTP, você deve entender o uso e a saída de dois comandos principais:

- show ntp associations
- show ntp peer

Mais detalhes sobre comandos específicos podem ser encontrados na Referência de comandos da SD-WAN.

Mostrar associações NTP

```
vedge1# show ntp associations

                                                                    LAST
IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  EVENT      COUNT
------------------------------------------------------------------------------
1    56368    8011    yes   no            none  reject     mobilize   1
2    56369    911a    yes   yes           none  falsetick  sys_peer   1
3    56370    9124    yes   yes           none  falsetick  reachable  2
```

IDX	número de índice local
ASSOCID	ID de associação
STATUS	palavra de status de peer (em hexadecimal)
CONF.	configuração (persistente ou efêmera)
ALCANÇABILIDADE	alcançabilidade (sim ou não)
AUTH	autenticação (ok, sim, inválida ou nenhuma)
CONDIÇÃO	status da seleção
EVENTO	último evento para este par
CONTAGEM	contagem de eventos

Show NTP Peer

```
vedge1# show ntp peer | tab

INDEX  REMOTE          REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
------------------------------------------------------------------------------------
1      192.168.18.201  .STEP.    16  u     37    1024  0      0.000    0.000    0.000
2      x10.88.244.1    LOCAL(1)  2   u     7     64    377    108.481  140.642  20.278
3      x172.18.108.15  .GPS.     1   u     66    64    377    130.407  -24883.  55.334
```

ÍNDICE	número de índice local
REMOTO	endereço do servidor NTP
REFID	Fonte atual de sincronização do par

ST	stratum O NTP usa o conceito de um stratum para descrever a distância (em saltos de NTP) que uma máquina está de uma fonte de tempo autoritativa. Por exemplo, um servidor de tempo stratum 1 tem um rádio ou relógio atômico diretamente conectado a ele. Ele envia seu horário para um servidor de horário de estrato 2 através do NTP e assim por diante até o estrato 16. Uma máquina que executa o NTP escolhe automaticamente a máquina com o menor número de stratum com a qual pode se comunicar e usa o NTP como sua origem de tempo.
TIPO	tipo
QUANDO	O tempo desde que o último pacote NTP foi recebido de um peer é relatado em segundos. Este valor deve ser inferior ao intervalo de sondagem.
VOTAÇÃO	intervalo de sondagem (segundos)
ALCANCE	alcance, conforme especificado pelo valor octal com base nas últimas 8 conexões 377 (1 1 1 1 1 1) - As últimas 8 foram todas OK 376 (1 1 1 1 1 1 0) - Última conexão inválida ... 177 (0 1 1 1 1 1) - A conexão mais antiga estava ruim, desde que ela estava boa etc
ATRASO	O atraso de ida e volta para o peer é relatado em milissegundos. Para ajustar o relógio com mais precisão, esse atraso é levado em conta quando a hora do relógio é definida.
DESLOCAMENTO	deslocamento (em milissegundos) Deslocamento é a diferença de tempo do relógio entre os peers ou entre o primário e o cliente. Esse valor é a correção aplicada a um relógio do cliente para sincronizá-lo. Um valor positivo indica que o relógio do servidor está mais alto. Um valor negativo indica que o relógio do cliente está mais alto.
TREMULAÇÃO	jitter (em milissegundos)

Solucionar problemas de NTP com ferramentas vManage e Packet

Capture

Verificar saída com simular fluxos no vManage

1. Escolha o painel Network Device via **Monitor > Network**
2. Escolha o vEdge aplicável.
3. Clique na opção **Troubleshooting**, seguida por **Simulate Flows**.
4. Especifique a interface e a VPN de origem nos menus suspensos, defina o IP de destino e o aplicativo como ntp.
5. Clique em **Simular.**

Isso fornece o comportamento de encaminhamento esperado para o tráfego NTP do vEdge.

Coletar TCPDump do vEdge

Quando o tráfego NTP atravessa o plano de controle do vEdge, ele pode ser capturado via TCPdump. A condição de correspondência precisaria usar a porta UDP padrão 123 para filtrar especificamente o tráfego NTP.

tcpdump vpn 0 options "dst port 123"

```
vedge1# tcpdump interface ge0/0 options "dst port 123"
tcpdump -p -i ge0_0 -s 128 dst port 123 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:05:44.364567 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:05:44.454385 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:05:45.364579 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:05:45.373547 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:52.364470 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:06:52.549536 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:54.364486 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:06:54.375065 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
```

Adicione o flag detalhado **-v** para decodificar os timestamps de dentro dos pacotes NTP.

tcpdump vpn 0 options "dst port 123 -v"

```
vedge1# tcpdump interface ge0/0 options "dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:10:13.364515 IP (tos 0xb8, ttl 64, id 62640, offset 0, flags [DF], proto UDP (17), length 76)
    192.168.19.55.123 > 192.168.18.201.123: NTPv4, length 48
        Client, Leap indicator: clock unsynchronized (192), Stratum 3 (secondary reference), poll 6 (64s
        Root Delay: 0.103881, Root dispersion: 1.073425, Reference-ID: 10.88.244.1
          Reference Timestamp:  3889015198.468340729 (2023/03/28 17:59:58)
          Originator Timestamp: 3889019320.559000091 (2023/03/28 19:08:40)
          Receive Timestamp:    3889019348.377538353 (2023/03/28 19:09:08)
          Transmit Timestamp:   3889019413.364485614 (2023/03/28 19:10:13)
            Originator - Receive Timestamp:  +27.818538262
            Originator - Transmit Timestamp: +92.805485523
19:10:13.365092 IP (tos 0xc0, ttl 255, id 7977, offset 0, flags [none], proto UDP (17), length 76)
```

```
192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
    Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
    Root Delay: 0.000000, Root dispersion: 0.002166, Reference-ID: 127.127.1.1
      Reference Timestamp:  3889019384.881000144 (2023/03/28 19:09:44)
      Originator Timestamp: 3889019413.364485614 (2023/03/28 19:10:13)
      Receive Timestamp:    3889019385.557000091 (2023/03/28 19:09:45)
      Transmit Timestamp:   3889019385.557000091 (2023/03/28 19:09:45)
        Originator - Receive Timestamp:  -27.807485523
        Originator - Transmit Timestamp: -27.807485523
```

Executar a Captura do Wireshark a partir do vManage

Se as capturas de pacotes tiverem sido ativadas a partir do vManage, o tráfego NTP também pode ser capturado dessa maneira diretamente para um arquivo legível pelo Wireshark.

1. Escolha o painel Network Device via **Monitor > Network**
2. Escolha o vEdge aplicável.
3. Clique na opção **Troubleshooting**, seguida de **Captura de Pacotes**.
4. Escolha VPN 0 e a interface externa nos menus suspensos.
5. Clique em **Traffic Filter**. Aqui você pode especificar a porta de destino 123 e, se desejar, um servidor de destino específico.

> **Observação**: o filtro por endereço IP captura apenas pacotes em uma direção, pois o filtro IP é por origem ou destino. Como a porta da camada 4 de destino é 123 em ambas as direções, filtre pela porta apenas para capturar o tráfego bidirecional.

---

6. Clique em Iniciar.

Agora, o vManage comunica-se com o vEdge para coletar uma captura de pacotes por 5 minutos ou até que o buffer de 5 MB seja preenchido, o que ocorrer primeiro. Após a conclusão, o download dessa captura pode ser feito para revisão.

Problemas comuns de NTP

Pacotes NTP não recebidos

As capturas de pacotes mostram os pacotes de saída enviados para o(s) servidor(es) configurado(s), mas nenhuma resposta recebida.

```
vedge1# tcpdump interface ge0/0 options "dst 192.168.18.201 && dst port 123 -n"
tcpdump -p -i ge0_0 -s 128 dst 192.168.18.201 && dst port 123 -n in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
14:24:49.364507 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:25:55.364534 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:27:00.364521 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

Depois de confirmar que os pacotes NTP não foram recebidos, você pode:

- Verifique se o NTP está configurado corretamente.
- Se o tráfego atravessa um túnel na VPN 0, certifique-se de que **allow-service ntp** ou **allow-service all** esteja habilitado na interface do túnel.
- Verifique se o NTP está bloqueado por uma lista de acesso ou dispositivo intermediário.
- Verifique problemas de roteamento entre a origem e o destino do NTP.

Perda de sincronização

Pode ocorrer perda de sincronização se o valor de dispersão e/ou atraso de um servidor for muito alto. Valores altos indicam que os pacotes demoram muito para chegar ao cliente a partir do servidor/peer em referência à raiz do relógio. Portanto, a máquina local não pode confiar na precisão do tempo presente no pacote, porque não sabe quanto tempo levou para o pacote chegar.

Se houver um link congestionado no caminho que cause buffer, os pacotes serão atrasados à medida que chegarem ao cliente NTP.

Se ocorrer uma perda de sincronização, você deverá verificar os links:

- Há congestionamento/excesso de assinaturas no caminho?
- São observados pacotes descartados?
- Há criptografia envolvida?

O valor de alcance em **show ntp peer** pode indicar perda de tráfego NTP. Se o valor for menor que 377, os pacotes são recebidos intermitentemente e o cliente sai de sincronia.

O relógio do dispositivo foi definido manualmente

Os valores de clock aprendidos do NTP podem ser substituídos através do comando **clock set**. Quando isso acontece, os valores de deslocamento para todos os peers aumentam significativamente.

```
vedge1# show ntp peer | tab

INDEX  REMOTE           REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
-------------------------------------------------------------------------------------
1      x10.88.244.1     LOCAL(1)  2   u     40    64    1      293.339  -539686  88.035
2      x172.18.108.15   .GPS.     1   u     39    64    1      30.408   -539686  8.768
3      x192.168.18.201  LOCAL(1)  8   u     38    64    1      5.743    -539686  2.435
```

Capturas detalhadas também mostram que os carimbos de data/hora de referência e os carimbos de data/hora do originador não estão alinhados.

```
vedge1# tcpdump interface ge0/0 options "src 192.168.18.201 && dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 src 192.168.18.201 && dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
00:01:28.156796 IP (tos 0xc0, ttl 255, id 8542, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002365, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889091263.881000144 (2023/03/29 15:07:43)
          Originator Timestamp: 133810392.155976055 (2040/05/05 00:01:28)
```

```
          Receive Timestamp:    3889091277.586000096 (2023/03/29 15:07:57)
          Transmit Timestamp:   3889091277.586000096 (2023/03/29 15:07:57)
            Originator - Receive Timestamp:  -539686410.569975959
            Originator - Transmit Timestamp: -539686410.569975959
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
```

Para forçar o vEdge a retomar a preferência por NTP como sua origem de tempo, exclua, confirme, adicione novamente e confirme novamente a configuração em **system ntp**.

Referências e informações relacionadas

- Solucionar problemas e depurar problemas de NTP (dispositivos Cisco IOS)
- Referência de comandos do Cisco SD-WAN
- Verificação do Status do NTP com o Comando show ntp associations

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.