Solución de problemas del protocolo de tiempo de la red (NTP) en vEdge

Contenido

Introducción

Este documento describe cómo resolver problemas del protocolo de tiempo de la red (NTP) con los comandos **show ntp** y las herramientas de captura de paquetes en las plataformas vEdge.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no se limita a versiones de software o modelos vEdge específicos.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Ejemplo de síntomas de problemas de NTP

La pérdida de sincronización NTP con un vEdge puede manifestarse de varias maneras, por ejemplo:

- Hora incorrecta en la salida **show clock** en el dispositivo.

- Certificados considerados no válidos debido a una hora incorrecta fuera del intervalo de validez.
- Marcas de tiempo incorrectas en los registros.

Comandos show del NTP

Para comenzar el aislamiento de los problemas de NTP, debe comprender el uso y la salida de dos comandos principales:

- show ntp associations
- show ntp peer

Puede encontrar más detalles de comandos específicos en la Referencia de Comandos de SD-WAN.

Show NTP Associations

```
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
ASÓCIDO	ID de asociación
ESTADO	palabra de estado de peer (en hexadecimal)
CONF	configuración (persistente o efímera)
ALCANCE	disponibilidad (sí o no)
AUTENTICACIÓN	autenticación (ok, yes, bad o none)
CONDICIÓN	estado de selección
EVENTO	último evento para este par
CUENTA	conteo 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	dirección del servidor NTP
REENCONTRAR	Fuente actual de sincronización del par

ST	estrato El NTP utiliza el concepto de estrato para describir a cuántos saltos (NTP) se encuentra una máquina de una fuente de hora autorizada. Por ejemplo, un servidor de tiempo de estrato 1 tiene una radio o un reloj atómico conectados directamente a él. Envía su tiempo a un servidor de tiempo del estrato 2 a través del NTP y así sucesivamente hasta el estrato 16. Una máquina que ejecuta NTP automáticamente elige la máquina con el número de estrato más bajo con el que puede comunicarse y utiliza NTP como su fuente de tiempo.
TIPO	tipo
WHEN (CUÁNDO)	Tiempo desde que el último paquete NTP se recibió desde el par informado en segundos. Este valor debe ser inferior al intervalo de sondeo.
POLL (SONDEO)	intervalo de sondeo (segundos)
REACH (ALCANCE)	alcance, según lo especificado por el valor octal basado en las últimas 8 conexiones 377 (1 1 1 1 1 1 1 1) - Los últimos 8 estuvieron bien 376 (1 1 1 1 1 1 1 0) - Última conexión incorrecta .... 177 (0 1 1 1 1 1 1 1) - La conexión más antigua era mala, todo desde bueno y más
DEMORA	La demora de ida y vuelta al par se informa en milisegundos. Para configurar el reloj con mayor precisión, esta demora se tiene en cuenta cuando se configura la hora del reloj.
OFFSET (DESPLAZAMIENTO)	desplazamiento (en milisegundos) El desplazamiento es la diferencia de tiempo de reloj entre los pares o entre el principal y el cliente. Este valor es la corrección que se aplica al reloj de un cliente para sincronizarlo. Un valor positivo indica que el reloj del servidor es más alto. Un valor negativo indica que el reloj del cliente es más alto.
FLUCTUACIÓN	fluctuación (en milisegundos)

Solución de problemas de NTP con vManage y herramientas de

captura de paquetes

Verificación de la salida con simulación de flujos en vManage

1. Elija el panel del dispositivo de red a través de **Monitor > Network**
2. Elija el vEdge correspondiente.
3. Haga clic en la opción **Troubleshooting**, seguido de **Simulate Flows**.
4. Especifique la VPN de origen y la interfaz de las listas desplegables, establezca la IP de destino y establezca la aplicación como ntp.
5. Haga clic en **Simular.**

Esto proporciona el comportamiento de reenvío esperado para el tráfico NTP desde el vEdge.

Recopilar TCPDump de vEdge

Cuando el tráfico NTP atraviesa el plano de control del vEdge, se puede capturar a través de TCPdump. La condición de coincidencia necesitaría utilizar el puerto UDP estándar 123 para filtrar específicamente el tráfico 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
```

Agregue el verbose flag **-v** para decodificar las marcas de tiempo desde dentro de los paquetes 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
```

Realizar captura de Wireshark desde vManage

Si se han habilitado las capturas de paquetes desde vManage, el tráfico NTP también se puede capturar de esta manera directamente en un archivo legible por Wireshark.

1. Elija el panel del dispositivo de red a través de **Monitor > Network**
2. Elija el vEdge correspondiente.
3. Haga clic en la opción **Troubleshooting**, seguido de **Packet Capture**.
4. Seleccione VPN 0 y la interfaz externa en los menús desplegables.
5. Haga clic en **Traffic Filter**. Aquí puede especificar el puerto de destino 123 y, si lo desea, un servidor de destino específico.

> **Nota**: Filtrar por dirección IP sólo captura los paquetes en una dirección, ya que el filtro IP está ordenado por origen o destino. Debido a que el puerto de la capa 4 de destino es 123 en ambas direcciones, filtre por el puerto sólo para capturar el tráfico bidireccional.

---

6. Haga clic en Start (Inicio).

vManage se comunica ahora con vEdge para recopilar una captura de paquetes durante 5 minutos o hasta que se llene el búfer de 5 MB, lo que ocurra primero. Una vez completada, la captura se puede descargar para su revisión.

Problemas comunes de NTP

Paquetes NTP no recibidos

Las capturas de paquetes muestran los paquetes salientes enviados a los servidores configurados, pero no se reciben respuestas.

```
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
```

Una vez que confirme que los paquetes NTP no se reciben, puede:

- Compruebe si el NTP está configurado correctamente.
- Si el tráfico atraviesa un túnel en VPN 0, asegúrese de que **allow-service ntp** o **allow-service all** esté habilitado en la interfaz de túnel.
- Compruebe si NTP está bloqueado por una lista de acceso o un dispositivo intermediario.
- Verifique si existen problemas de ruteo entre el origen y el destino NTP.

Pérdida de sincronización

Puede producirse una pérdida de sincronización si el valor de dispersión o retraso de un servidor es muy alto. Los valores altos indican que los paquetes tardan demasiado en llegar al cliente desde el servidor/peer en referencia a la raíz del reloj. Por lo tanto, la máquina local no puede confiar en la precisión del tiempo presente en el paquete, porque no sabe cuánto tiempo tardó en llegar el paquete.

Si hay un link congestionado en el trayecto que causa el almacenamiento en buffer, los paquetes se retrasan a medida que llegan al cliente NTP.

Si experimenta una pérdida de sincronización, debe comprobar los enlaces:

- ¿Hay congestión/sobresuscripción en la ruta?
- ¿Se observan paquetes perdidos?
- ¿Está implicada la encriptación?

El valor de alcance en **show ntp peer** puede indicar la pérdida de tráfico NTP. Si el valor es menor que 377, los paquetes se reciben intermitentemente y el cliente se desincroniza.

El reloj del dispositivo se ha establecido manualmente

Los valores de reloj aprendidos de NTP se pueden invalidar mediante el comando **clock set**. Cuando esto sucede, los valores de desplazamiento para todos los pares aumentan 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
```

Las capturas detalladas también muestran que las marcas de hora de referencia y las marcas de hora de origen no están alineadas.

```
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 forzar que vEdge reanude la preferencia por NTP como su fuente de tiempo, elimine, confirme, vuelva a agregar y vuelva a confirmar la configuración en **system ntp**.

Referencias e información relacionada

- Solución de problemas y depuración de NTP (dispositivos Cisco IOS)
- Referencia de Comandos de Cisco SD-WAN
- Verificación del estado de NTP con el comando show ntp associations

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).