Fehlerbehebung bei NTP-Problemen (Network Time Protocol) in vEdge

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Beispiele für NTP-Probleme
NTP-Befehle anzeigen
NTP-Zuordnungen anzeigen
NTP-Peer anzeigen
Fehlerbehebung bei NTP mit vManager und Paketerfassungstools
Überprüfen des Ausgangs mit "Flow simulieren" auf vManage
TCPDump von vEdge sammeln
Durchführung von Wireshark Capture über vManage
Häufige NTP-Probleme
NTP-Pakete nicht empfangen
Synchron-Verlust
Die Geräteuhr wurde manuell eingestellt.
Referenzen und zugehörige Informationen

Einleitung

In diesem Dokument wird die Fehlerbehebung bei NTP-Problemen (Network Time Protocol) mit **show ntp**-Befehlen und Paketerfassungstools auf vEdge-Plattformen beschrieben..

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Softwareversionen oder vEdge-Modelle beschränkt.

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.

Beispiele für NTP-Probleme

Der Verlust der NTP-Synchronisierung mit einem vEdge kann auf verschiedene Weise auftreten, z. B.:

- Falsche Uhrzeit in **Anzeige** der **Taktausgabe** auf dem Gerät.

- Zertifikate werden aufgrund einer falschen Zeit außerhalb des Gültigkeitsbereichs als ungültig angesehen.
- Falsche Zeitstempel in Protokollen.

NTP-Befehle anzeigen

Um mit der Isolierung von NTP-Problemen zu beginnen, müssen Sie die Verwendung und Ausgabe von zwei Hauptbefehlen verstehen:

- NTP-Zuordnungen anzeigen
- NTP-Peer anzeigen

Weitere Einzelheiten zu bestimmten Befehlen finden Sie in der SD-WAN-Befehlsreferenz.

NTP-Zuordnungen anzeigen

```
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	lokale Indexnummer
ASSOCID	Zuordnungs-ID
STATUS	Peer-Statuswort (im Hexadezimalformat)
KONF	Konfiguration (persistent oder ephemer)
ERREICHBARKEIT	Erreichbarkeit (ja oder nein)
AUTH	Authentifizierung (OK, Ja, Schlecht oder Keine)
BEDINGUNG	Auswahlstatus
VERANSTALTUNG	Letzte Veranstaltung für diesen Peer
ANZAHL	Ereigniszählung

NTP-Peer anzeigen

```
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
```

INDEX	lokale Indexnummer
ENTFERNT	NTP-Serveradresse

NEU	Aktuelle Quelle der Synchronisierung durch den Peer
ST	Schicht Das NTP nutzt das Schichtenkonzept, um zu beschreiben, wie weit (in NTP-Hops) ein Rechner von einer maßgeblichen Zeitquelle entfernt ist. Beispielsweise ist ein Schicht-1-Zeitserver direkt mit einer Funk- oder Atomuhr verbunden. Es sendet seine Zeit über NTP an einen Schicht-2-Zeitserver usw. bis Schicht 16. Ein Computer, der NTP ausführt, wählt automatisch den Computer mit der niedrigsten Schicht-Nummer aus, mit dem er kommunizieren kann, und verwendet NTP als Zeitquelle.
TYP	typ
WANN	Die Zeit seit dem Empfang des letzten NTP-Pakets von einem Peer wird in Sekunden gemeldet. Dieser Wert muss kleiner als das Abfrageintervall sein.
UMFRAGE	Abfrageintervall (Sekunden)
REICHWEITE	Reichweite, wie durch Oktalwert auf Basis der letzten 8 Verbindungen angegeben 377 (1 1 1 1 1 1 1) - Die letzten 8 waren alle OK 376 (1 1 1 1 1 1 1 0) - Letzte fehlerhafte Verbindung .... 177 (0 1 1 1 1 1 1) - Älteste Verbindung war schlecht, alle seit gut und so weiter
VERZÖGERUNG	Die Round-Trip-Verzögerung zum Peer wird in Millisekunden gemeldet. Um den Takt genauer einzustellen, wird diese Verzögerung bei der Einstellung der Taktzeit berücksichtigt.
OFFSET	Offset (in Millisekunden) Offset ist die Zeitdifferenz zwischen den Peers oder zwischen dem primären und dem Client. Dieser Wert ist die Korrektur, die auf eine Client-Uhr angewendet wird, um diese zu synchronisieren. Ein positiver Wert zeigt an, dass die Serveruhr höher ist. Ein negativer Wert zeigt an, dass die Client-Uhr höher ist.
JITTER	Jitter (in Millisekunden)

Fehlerbehebung bei NTP mit vManager und Paketerfassungstools

Überprüfen des Ausgangs mit "Flow simulieren" auf vManage

1. Wählen Sie das Dashboard für Netzwerkgeräte über **Monitor > Network aus.**
2. Wählen Sie den gewünschten vEdge aus.
3. Klicken Sie auf die Option **Fehlerbehebung**, gefolgt von **Flusssimulation**.
4. Geben Sie das Quell-VPN und die Schnittstelle aus den Dropdown-Menüs an, legen Sie die Ziel-IP fest, und legen Sie die Anwendung als NTP fest.
5. Klicken Sie auf **Simulieren.**

Dadurch wird das erwartete Weiterleitungsverhalten für NTP-Datenverkehr vom vEdge angezeigt.

TCPDump von vEdge sammeln

Wenn NTP-Datenverkehr die Kontrollebene von vEdge passiert, kann er über TCP-Dump erfasst werden. Bei der Übereinstimmungsbedingung muss der Standard-UDP-Port 123 verwendet werden, um speziell nach NTP-Datenverkehr zu filtern.

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
```

Fügen Sie das Flag verbose **-v hinzu**, um die Zeitstempel aus den NTP-Paketen zu dekodieren.

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
```

Durchführung von Wireshark Capture über vManage

Wenn die Paketerfassung von vManage aktiviert wurde, kann der NTP-Datenverkehr auch direkt in eine von Wireshark lesbare Datei erfasst werden.

1. Wählen Sie das Dashboard für Netzwerkgeräte über **Monitor > Network aus.**
2. Wählen Sie den gewünschten vEdge aus.
3. Klicken Sie auf die Option **Fehlerbehebung**, gefolgt von **Paketerfassung**.
4. Wählen Sie VPN 0 und die externe Schnittstelle aus den Dropdown-Menüs aus.
5. Klicken Sie auf **Datenverkehrsfilter**. Hier können Sie den Zielport 123 und ggf. einen bestimmten Zielserver angeben.

> **Hinweis**: Bei der Filterung nach IP-Adresse werden Pakete nur in eine Richtung erfasst, da der IP-Filter nach Quelle oder Ziel gefiltert wird. Da der Layer-4-Zielport in beide Richtungen den Wert 123 aufweist, wird nur nach dem Port gefiltert, um bidirektionalen Datenverkehr zu erfassen.

---

6. Klicken Sie auf **Start**.

vManage kommuniziert nun mit dem vEdge, um eine Paketerfassung entweder für 5 Minuten oder bis zum Auffüllen des 5-MB-Puffers zu sammeln, je nachdem, welcher Fall zuerst eintritt. Nach Fertigstellung kann diese Aufzeichnung zur Überprüfung heruntergeladen werden.

Häufige NTP-Probleme

NTP-Pakete nicht empfangen

Paketerfassungen zeigen ausgehende Pakete, die an den/die konfigurierten Server gesendet wurden, aber keine Antworten erhalten.

```
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
```

Wenn Sie bestätigen, dass keine NTP-Pakete empfangen wurden, haben Sie folgende Möglichkeiten:

- Überprüfen Sie, ob das NTP richtig konfiguriert ist.
- Wenn Datenverkehr in VPN 0 einen Tunnel durchläuft, stellen Sie sicher, dass **allow-service ntp** oder **allow-service all** unter der Tunnelschnittstelle aktiviert ist.
- Überprüfen Sie, ob NTP von einer Zugriffsliste oder einem zwischengeschalteten Gerät blockiert wird.
- Suchen Sie nach Routing-Problemen zwischen der NTP-Quelle und dem -Ziel.

Synchron-Verlust

Ein Verlust der Synchronisierung kann auftreten, wenn der Dispersions- und/oder Verzögerungswert für einen Server sehr hoch wird. Hohe Werte zeigen an, dass die Pakete zu lange dauern, bis sie vom Server/Peer in Bezug auf den Stamm der Uhr an den Client gesendet werden. Das lokale System kann daher der Genauigkeit der im Paket enthaltenen Zeit nicht vertrauen, da es nicht weiß, wie lange es bis zum Eintreffen des Pakets gedauert hat.

Wenn der Pfad eine überlastete Verbindung enthält, die eine Pufferung verursacht, werden die Pakete verzögert, sobald sie an den NTP-Client gesendet werden.

Wenn Sie einen Verlust der Synchronisierung feststellen, müssen Sie die folgenden Links überprüfen:

- Ist der Pfad überlastet/überbelegt?
- Wurden verworfene Pakete beobachtet?
- Handelt es sich um Verschlüsselung?

Der Reichweitenwert in **show ntp peer** kann auf einen Verlust von NTP-Datenverkehr hinweisen. Wenn der Wert kleiner als 377 ist, werden Pakete gelegentlich empfangen, und der Client wird nicht mehr synchronisiert.

Die Geräteuhr wurde manuell eingestellt.

Die vom NTP bezogenen Uhrenwerte können mit dem Befehl **clock set** überschrieben werden. In diesem Fall werden die Offsetwerte für alle Peers deutlich erhöht.

```
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
```

Ausführliche Aufnahmen zeigen auch, dass die Referenz-Zeitstempel und die Originator-Zeitstempel nicht übereinstimmen.

```
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
```

Um zu erzwingen, dass der vEdge den NTP-Status als Zeitquelle wieder einstellt, löschen Sie die Konfiguration unter **System ntp,** führen Sie einen Commit aus, fügen Sie sie erneut hinzu, und führen Sie einen neuen Commit aus.

Referenzen und zugehörige Informationen

- Fehlerbehebung und Fehlerbehebung bei NTP-Problemen (Cisco IOS-Geräte)
- Cisco SD-WAN-Befehlsreferenz
- Überprüfen des NTP-Status mit dem Befehl show ntp associations

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.