排除vEdge上的網路時間協定(NTP)故障

目錄

簡介

必要條件

- 需求
- 採用元件

NTP問題的症狀示例

NTP 顯示指令

- 顯示NTP關聯
- Show NTP Peer

使用vManage和資料包捕獲工具排除NTP故障

- 在vManage上使用模擬流驗證輸出
- 從vEdge收集TCPDump
- 從vManage執行Wireshark捕獲

常見NTP問題

- NTP 封包未接收
- 同步丟失
- 已手動設定裝置上的時鐘

參考和相關資訊

簡介

本檔案介紹如何在vEdge平台上使用show ntp指令和封包擷取工具來排解網路時間協定(NTP)問題的疑難問題.

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案所述內容不限於特定軟體版本或vEdge型號。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

NTP問題的症狀示例

NTP同步到vEdge的丟失可以通過幾種不同方式表現出來，例如：

- 裝置上show clock輸出中的時間不正確。
- 由於有效範圍之外的時間不正確，證書被視為無效。
- 日誌上的時間戳不正確。

NTP 顯示指令

要開始隔離NTP問題，必須瞭解兩個主要命令的使用和輸出：

- show ntp associations
- show ntp peer

有關特定命令的更多詳情，請參閱《SD-WAN命令參考》。

顯示NTP關聯

```
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	本地索引號
關聯	關聯ID
狀態	對等體狀態字（十六進位制）
會議	配置（持久或短暫）
可達性	可達性（是或否）
身份驗證	身份驗證（ok、yes、bad或none）
條件	選擇狀態
活動	此對等體的最後一個事件
計數	事件計數

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
```

索引	本地索引號
遠端	NTP伺服器地址
REFID	來自對等體的當前同步源
ST	地層 NTP 使用階層概念說明電腦與授權時間來源的距離（以 NTP 躍點為單位）。例如，第1層時間伺服器直接連線了無線電時鐘或原子時鐘。它通過NTP將其時間傳送到第2層時間伺服器，以此類推，直到第16層。運行NTP的電腦會自動選擇層數最低的電腦進行通訊，並使用NTP作為其時間源。
類型	類型
WHEN	自上次從對等接收到 NTP 封包的時間係以秒為單位報告。該值必須小於輪詢間隔。
POLL	輪詢間隔（秒）
REACH	reach，由基於前8個連線的八進位制值指定 377(1 1 1 1 1 1 1 1) — 最後8個都沒問題 376(1 1 1 1 1 1 1 0) — 最後一個連線錯誤 .... 177(0 1 1 1 1 1 1) — 最早的連線是壞的，自正常以來都是好的 等等
延遲	對等的往返延遲係以毫秒為單位報告。為更精確設定時鐘，設定時鐘時間時，會將此延遲列入考量。
OFFSET	偏移量（毫秒） Offset是對等項之間或主客戶端與客戶端之間的時鐘時間差。此值為套用至用戶端時鐘以同步化的修正值。正值表示伺服器時鐘較高。負值表示用戶端時鐘較高。
抖動	抖動（以毫秒為單位）

使用vManage和資料包捕獲工具排除NTP故障

在vManage上使用模擬流驗證輸出

1. 通過Monitor > Network選擇網路裝置控制面板
2. 選擇適用的vEdge。
3. 按一下Troubleshooting選項，然後按一下Simulate Flows。
4. 從下拉選單中指定源VPN和介面，設定目標IP，並將應用程式設定為ntp。
5. 按一下Simulate（模擬）。

這樣會為來自vEdge的NTP流量提供預期的轉發行為。

從vEdge收集TCPDump

當NTP流量通過vEdge的控制平面時，可以通過TCPdump捕獲該流量。 匹配條件需要使用標準UDP埠123專門過濾NTP流量。

tcpdump vpn 0選項「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
```

新增verbose標誌-v以從NTP資料包中解碼時間戳。

tcpdump vpn 0選項「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 (64
        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
```

從vManage執行Wireshark捕獲

如果已從vManage啟用資料包捕獲，則還可以通過這種方式將NTP流量直接捕獲到Wireshark可讀取的檔案。

1. 通過Monitor > Network選擇網路裝置控制面板
2. 選擇適用的vEdge。
3. 按一下Troubleshooting選項，然後按一下Packet Capture。
4. 從下拉選單中選擇VPN 0和外部介面。
5. 按一下「Traffic Filter」。您可以在此處指定目的地連線埠123，並在需要時指定特定目的地伺服器。

> 注意：按IP地址過濾只能捕獲一個方向的資料包，因為IP過濾器按源或目標進行過濾。由於目的地第4層連線埠兩個方向都是123，因此只能透過連線埠進行過濾以擷取雙向流量。

6. 按一下「Start」。

vManage現在與vEdge進行通訊，以收集資料包捕獲5分鐘或直到5MB緩衝區滿為止（以先發生者為準）。完成之後，可下載該捕獲以供檢視。

常見NTP問題

NTP 封包未接收

資料包捕獲顯示傳送到已配置伺服器的出站資料包，但沒有收到回覆。

```
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
```

確認未收到NTP資料包後，您可以：

- 檢查 NTP 是否正確設定。
- 如果流量通過VPN 0中的通道，請確保allow-service ntp或allow-service all在通道介面下啟用。
- 檢查NTP是否被訪問清單或中間裝置阻止。
- 檢查NTP源和目標之間的路由問題。

同步丟失

如果伺服器的色散和/或延遲值非常高，則可能會發生同步丟失。 高值表示從伺服器/對等裝置到達客戶端時所用的資料包時間太長（參考時鐘的根）。 因此，本地電腦無法信任資料包中當前時間的準確性，因為它不知道資料包到達需要多長時間。

如果路徑中存在導致緩衝的擁塞鏈路，則資料包在到達NTP客戶端時會延遲。

如果遇到同步丟失的情況，您必須檢查以下連結：

- 路徑中是否存在擁塞/超訂用？
- 是否觀察到丟棄的資料包？
- 是否涉及加密？

show ntp peer 中的到達值可能表示NTP流量丟失。 如果值小於377，則會間歇接收資料包，並且客戶端不同步。

已手動設定裝置上的時鐘

通過clock set 命令可以覆蓋從NTP獲取的時鐘值。 發生這種情況時，所有對等體的偏移值都會顯著增加。

```
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
```

詳細捕獲還顯示參考時間戳和建立者時間戳不一致。

```
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
```

要強制vEdge恢復對NTP作為其時間源的首選項，請刪除、提交、重新新增和重新提交系統ntp下的配置。

參考和相關資訊

- 對NTP問題進行故障排除和調試（Cisco IOS裝置）
- Cisco SD-WAN命令參考
- 使用show ntp associations命令檢驗NTP狀態

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。