Risoluzione dei problemi NTP (Network Time Protocol) su vEdge

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al Network Time Protocol (NTP) con i comandi **show ntp** e gli strumenti di acquisizione pacchetti sulle piattaforme vEdge.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o per tutti i modelli vEdge.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sintomi di esempio di problemi NTP

La perdita della sincronizzazione NTP con un vEdge può manifestarsi in diversi modi, ad esempio:

- Ora errata nell'output **show clock** sul dispositivo.

- Certificati considerati non validi a causa di un'ora non corretta non compresa nell'intervallo di validità.
- Timestamp non corretti nei registri.

Comandi show NTP

Per iniziare a isolare i problemi NTP, è necessario comprendere l'utilizzo e l'output di due comandi principali:

- mostra associazioni ntp
- show ntp peer

Per ulteriori informazioni su comandi specifici, consultare la guida di riferimento dei comandi SD-WAN.

Mostra associazioni 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	numero di indice locale
ASSOCIATO	ID associazione
STATO	parola di stato peer (in esadecimale)
CONF	configurazione (permanente o effimera)
RAGGIUNGIBILITÀ	raggiungibilità (sì o no)
AUTH	autenticazione (ok, sì, errata o nessuna)
CONDIZIONE	stato selezione
EVENTO	ultimo evento per questo peer
CONTEGGIO	conteggio eventi

Mostra peer NTP

```
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
```

INDICE	numero di indice locale
REMOTO	Indirizzo server NTP
REFID	Origine corrente della sincronizzazione dal peer

ST	strato La NTP utilizza il concetto di strato per descrivere quanto lontano (negli hop NTP) una macchina da una fonte temporale autorevole. Ad esempio, un server di riferimento ora di strato 1 ha un orologio radio o atomico direttamente collegato. Invia il suo tempo ad un server di tempo di strato 2 attraverso NTP, e così via fino allo strato 16. Una macchina che esegue NTP sceglie automaticamente la macchina con il numero più basso dello strato con cui può comunicare e utilizza NTP come sorgente del tempo.
TIPO	tipo
QUANDO	Il tempo trascorso dalla ricezione dell'ultimo pacchetto NTP da un peer viene segnalato in secondi. Questo valore deve essere inferiore all'intervallo di polling.
SONDAGGIO	intervallo di polling (secondi)
PORTATA	reach, come specificato dal valore ottale basato sulle ultime 8 connessioni 377 (1 1 1 1 1 1 1) - Le ultime 8 erano tutte OK 376 (1 1 1 1 1 1 0) - Ultima connessione non valida .... 177 (0 1 1 1 1 1 1) - La connessione più vecchia non era buona e così via
RITARDO	Il ritardo di andata e ritorno al peer viene segnalato in millisecondi. Per impostare l'orologio in modo più accurato, questo ritardo viene preso in considerazione quando si imposta l'ora dell'orologio.
SCOSTAMENTO	offset (in millisecondi) L'offset è la differenza di tempo tra i peer o tra il client e il server principale. Questo valore è la correzione che viene applicata a un orologio client per sincronizzarlo. Un valore positivo indica che l'orologio del server è più alto. Un valore negativo indica che l'orologio del client è più alto.
TREMOLIO	variazione (in millisecondi)

Risoluzione dei problemi NTP con vManage e gli strumenti di

acquisizione pacchetti

Verifica dell'avanzamento con simulazione dei flussi in vManage

1. Scegliete il quadro comandi Dispositivo di rete tramite **Monitor > Rete**
2. Scegliere il vEdge applicabile.
3. Fate clic sull'opzione **Risoluzione problemi (Troubleshooting)**, quindi su **Simula flussi (Simulate Flows)**.
4. Specificare la VPN di origine e l'interfaccia dagli elenchi a discesa, impostare l'IP di destinazione e impostare l'applicazione come ntp.
5. Fare clic su **Simula.**

Fornisce il comportamento di inoltro previsto per il traffico NTP dal server vEdge.

Raccogli TCPDump da vEdge

Quando il traffico NTP attraversa il control plane del vEdge, può essere acquisito tramite TCPdump. La condizione di corrispondenza deve utilizzare la porta UDP standard 123 per filtrare in modo specifico il traffico 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
```

Aggiungere il flag verbose **-v** per decodificare i timestamp dai pacchetti 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
```

Esegui acquisizione di Wireshark da vManage

Se le acquisizioni dei pacchetti sono state abilitate da vManage, il traffico NTP può essere acquisito in questo modo direttamente in un file leggibile da Wireshark.

1. Scegliete il quadro comandi Dispositivo di rete tramite **Monitor > Rete**
2. Scegliere il vEdge applicabile.
3. Fare clic sull'opzione **Risoluzione dei problemi**, quindi su **Packet Capture** (Acquisizione pacchetti).
4. Scegliere VPN 0 e l'interfaccia esterna dai menu a discesa.
5. Fare clic su **Filtro traffico**. Qui è possibile specificare la porta di destinazione 123 e, se si desidera, un server di destinazione specifico.

> **Nota**: il filtro in base all'indirizzo IP acquisisce i pacchetti solo in una direzione, poiché il filtro IP si basa sull'origine o sulla destinazione. Poiché la porta del livello 4 di destinazione è 123 in entrambe le direzioni, filtrare in base alla porta solo per acquisire il traffico bidirezionale.

---

6. Fare clic su **Start**.

vManage comunica ora con vEdge per acquisire un pacchetto per 5 minuti o fino a quando il buffer da 5 MB non si riempie, a seconda della condizione che si verifica per prima. Una volta completata, l'acquisizione può essere scaricata per la revisione.

Problemi NTP comuni

Pacchetti NTP non ricevuti

Le acquisizioni dei pacchetti mostrano i pacchetti in uscita inviati ai server configurati, ma non le risposte ricevute.

```
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
```

Dopo aver confermato che i pacchetti NTP non sono stati ricevuti, è possibile:

- Verificare che NTP sia configurato correttamente.
- Se il traffico attraversa un tunnel nella VPN 0, verificare che **allow-service ntp** o **allow-service all** sia abilitato nell'interfaccia del tunnel.
- Verificare se il protocollo NTP è bloccato da un elenco degli accessi o da un dispositivo intermedio.
- Verificare la presenza di problemi di routing tra l'origine NTP e la destinazione.

Perdita di sincronizzazione

La perdita di sincronizzazione può verificarsi se la dispersione e/o il valore di ritardo di un server diventa molto elevato. Valori alti indicano che i pacchetti impiegano troppo tempo per raggiungere il client dal server/peer in riferimento alla radice dell'orologio. Pertanto, il computer locale non può fidarsi dell'accuratezza del tempo presente nel pacchetto, perché non sa quanto tempo è stato necessario per l'arrivo del pacchetto.

Se il percorso contiene un collegamento congestionato che causa il buffering, i pacchetti vengono ritardati quando arrivano al client NTP.

Se si verifica una perdita di sincronizzazione, è necessario controllare i collegamenti:

- Nel percorso è presente una congestione/sottoscrizione in eccesso?
- Sono stati osservati pacchetti ignorati?
- C'è anche la crittografia?

Il valore REACH in **show ntp peer** può indicare la perdita di traffico NTP. Se il valore è inferiore a 377, i pacchetti vengono ricevuti in modo intermittente e il client non è più sincronizzato.

L'orologio sul dispositivo è stato impostato manualmente

I valori dell'orologio appresi dal protocollo NTP possono essere sostituiti con il comando **clock set**. In questo caso, i valori di offset per tutti i peer aumentano in modo significativo.

```
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
```

Le acquisizioni dettagliate mostrano inoltre che i timestamp di riferimento e quelli dell'iniziatore non sono allineati.

```
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
```

Per forzare vEdge a riprendere la preferenza per NTP come origine ora, eliminare, eseguire il commit, aggiungere di nuovo e ripetere il commit della configurazione in **system ntp**.

Riferimenti e informazioni correlate

- Risoluzione dei problemi e debug dei NTP (dispositivi Cisco IOS)
- Guida di riferimento ai comandi di Cisco SD-WAN
- Verifica dello stato NTP con il comando show ntp association

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).