Dépannage des problèmes NTP (Network Time Protocol) sur vEdge

Table des matières

Introduction

Ce document décrit comment dépanner les problèmes de NTP (Network Time Protocol) avec les commandes show ntp et les outils de capture de paquets sur les plates-formes vEdge.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions logicielles ou des modèles vEdge spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Exemples de symptômes de problèmes NTP

La perte de synchronisation NTP avec un vEdge peut se manifester de différentes manières, par exemple :

- Heure incorrecte dans la sortie de show clock sur le périphérique.
- Certificats considérés comme non valides en raison d'une heure incorrecte en dehors de la plage de validité.
- Horodatages incorrects dans les journaux.

Commandes show NTP

Pour commencer à isoler les problèmes NTP, vous devez comprendre l'utilisation et la sortie de deux commandes principales :

- show ntp associations
- show ntp peer

Vous trouverez plus de détails sur des commandes spécifiques dans le Guide de référence des commandes SD-WAN.

Afficher les associations 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	numéro d'index local
ASSOCIÉ	ID d'association
STATUS (ÉTAT)	mot d'état homologue (au format hexadécimal)
CONF	configuration (persistante ou éphémère)
ACCESSIBILITÉ	accessibilité (oui ou non)
AUTH	authentification (ok, yes, bad ou none)
CONDITIONNER	état de sélection
ÉVÉNEMENT	dernier événement pour cet homologue
COMPTE	compte d'événements

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
```

INDEX	numéro d'index local
ÉLOIGNÉ	Adresse du serveur NTP
REFID	Source actuelle de synchronisation de l'homologue
ST	strate NTP utilise le concept d'une strate afin de décrire la distance (en sauts NTP) d'une machine par rapport à une source temporelle faisant autorité. Par exemple, un serveur de temps de strate 1 est directement relié à une horloge radio ou atomique. Il envoie son temps à un serveur de temps de strate 2 via NTP, et ainsi de suite jusqu'à la strate 16. Une machine qui exécute NTP choisit automatiquement la machine avec le numéro de strate le plus bas avec laquelle elle peut communiquer et utilise NTP comme source de temps.
CARACTÈRE	type
QUAND	Le temps écoulé depuis la réception du dernier paquet NTP d'un homologue est indiqué en secondes. Cette valeur doit être inférieure à l'intervalle d'interrogation.
SONDAGE	intervalle d'interrogation (secondes)
ATTEINDRE	portée, spécifiée par une valeur octale basée sur les 8 dernières connexions 377 (1 1 1 1 1 1 1 1) - Les 8 derniers étaient tous corrects 376 (1 1 1 1 1 1 1 0) - Dernière connexion incorrecte .... 177 (0 1 1 1 1 1 1 1) - La connexion la plus

	ancienne était mauvaise, car elle était bonne etc.
RETARD	Le délai de transmission aller-retour vers l'homologue est signalé en millisecondes. Afin de régler l'horloge avec plus de précision, ce retard est pris en compte lors du réglage de l'heure d'horloge.
COMPENSATION	offset (en millisecondes) Le décalage est la différence de temps d'horloge entre les homologues ou entre le principal et le client. Cette valeur est la correction qui est appliquée à une horloge client afin de la synchroniser. Une valeur positive indique que l'horloge du serveur est plus élevée. Une valeur négative indique que l'horloge du client est plus élevée.
GIGUE	gigue (en millisecondes)

Dépannage de NTP avec les outils vManage et de capture de paquets

Vérification de la sortie avec simulation des flux sur vManage

1. Sélectionnez le tableau de bord Périphérique réseau via Monitor > Network
2. Sélectionnez le serveur vEdge approprié.
3. Cliquez sur l'option Troubleshooting, suivie de Simulate Flows.
4. Spécifiez le VPN source et l'interface à partir des listes déroulantes, définissez l'IP de destination et définissez l'application comme ntp.
5. Cliquez sur Simuler.

Cela donne le comportement de transfert attendu pour le trafic NTP à partir du vEdge.

Collecter TCPDump depuis vEdge

Lorsque le trafic NTP traverse le plan de contrôle du vEdge, il peut être capturé via TCPdump. La condition de correspondance devrait utiliser le port UDP standard 123 pour filtrer spécifiquement le trafic 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
```

Ajoutez l'indicateur détaillé -v pour décoder les horodatages à partir des paquets 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 (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
```

Effectuer une capture Wireshark à partir de vManage

Si les captures de paquets ont été activées à partir de vManage, le trafic NTP peut également être capturé de cette manière directement dans un fichier lisible par Wireshark.

1. Sélectionnez le tableau de bord Périphérique réseau via Monitor > Network
2. Sélectionnez le serveur vEdge approprié.
3. Cliquez sur l'option Troubleshooting, suivie de Packet Capture.
4. Sélectionnez VPN 0 et l'interface externe dans les menus déroulants.
5. Cliquez sur Traffic Filter. Vous pouvez spécifier ici le port de destination 123 et, si vous le

souhaitez, un serveur de destination spécifique.

> Remarque : le filtre par adresse IP ne capture les paquets que dans une seule direction, car le filtre IP est par source ou destination. Comme le port de couche 4 de destination est 123 dans les deux directions, filtrez par le port uniquement pour capturer le trafic bidirectionnel.

6. Cliquez sur Démarrer.

vManage communique désormais avec vEdge pour collecter une capture de paquets pendant 5 minutes ou jusqu'à ce que la mémoire tampon de 5 Mo se remplisse, selon la première éventualité. Une fois terminée, cette capture peut être téléchargée pour révision.

Problèmes NTP courants

Paquets NTP non reçus

Les captures de paquets affichent les paquets sortants envoyés aux serveurs configurés, mais aucune réponse n'est reçue.

```
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
```

Une fois que vous avez confirmé que les paquets NTP ne sont pas reçus, vous pouvez :

- Vérifiez si le protocole NTP est correctement configuré.
- Si le trafic traverse un tunnel dans VPN 0, assurez-vous que allow-service ntp ou allow-service all est activé sous l'interface de tunnel.
- Vérifiez si le protocole NTP est bloqué par une liste d'accès ou un périphérique intermédiaire.
- Vérifiez les problèmes de routage entre la source et la destination NTP.

Perte de synchronisation

Une perte de synchronisation peut se produire si la valeur de dispersion et/ou de délai d'un serveur devient très élevée. Les valeurs élevées indiquent que les paquets mettent trop de temps pour parvenir au client à partir du serveur/homologue en référence à la racine de l'horloge. Ainsi,

la machine locale ne peut pas faire confiance à la précision du temps présent dans le paquet, car elle ne sait pas combien de temps il a fallu pour que le paquet arrive.

S'il y a une liaison encombrée dans le chemin qui provoque la mise en mémoire tampon, les paquets sont retardés lorsqu'ils arrivent au client NTP.

Si vous rencontrez une perte de synchronisation, vous devez vérifier les liens :

- Le chemin est-il encombré/surabonné ?
- Des paquets abandonnés ont-ils été observés ?
- Y a-t-il chiffrement ?

La valeur reach dans show ntp peer peut indiquer la perte du trafic NTP. Si la valeur est inférieure à 377, les paquets sont reçus par intermittence et le client se désynchronise.

L'horloge du périphérique a été réglée manuellement

Les valeurs d'horloge apprises de NTP peuvent être remplacées par la commande clock set. Dans ce cas, les valeurs de décalage pour tous les homologues augmentent de manière significative.

```
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
```

Les captures détaillées montrent également que les horodatages de référence et d'origine ne sont pas alignés.

```
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
```

Pour forcer le serveur vEdge à reprendre la préférence pour NTP en tant que source temporelle, supprimez, validez, ajoutez à nouveau et validez à nouveau la configuration sous system ntp.

Références et informations connexes

- Dépannage et débogage des problèmes NTP (périphériques Cisco IOS)
- Référence des commandes Cisco SD-WAN
- Vérification de l'état NTP avec la commande show ntp associations

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.