Configuration des meilleures pratiques pour la synchronisation NTP dans les déploiements SD-WAN

Table des matières

Introduction

Ce document décrit comment le protocole NTP est crucial pour maintenir une synchronisation temporelle précise entre les périphériques dans la structure SD-WAN.

Fond

Sans synchronisation appropriée, les opérations critiques telles que la communication sécurisée, la validation de certificat et la journalisation peuvent échouer. SD-WAN est une solution réseau basée sur des certificats, sécurisée et basée sur des politiques. La synchronisation temporelle à l'aide du protocole NTP est essentielle pour maintenir l'intégrité, la sécurité et les fonctionnalités de la structure SD-WAN.

Conditions préalables

Exigences

Cisco vous recommande de connaître la solution Cisco SDWAN (Software Defined Wide Area Network).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- C8000V version17.15.03a
- vManage version 20.15.03.1

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.

Principales raisons

- SD-WAN utilise un certificat numérique pour l'authentification des périphériques. Ces certificats ont une date de début de validité et une date d'expiration. Si l'horloge du périphérique n'est pas précise, il peut penser que le certificat a expiré ou n'est pas encore valide.

```
vbond-west# show orchestrator connections-history
          PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
INSTANCE  TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBL
-------------------------------------------------------------------------------------------------
0         vmanage  dtls     10.1.1.7          101019      0           10.1.2.190       12646    192
```

CRTVERFL - Échec de la vérification du certificat homologue

Dans ce cas, comme l'heure est en dehors de la date de validité du certificat, l'erreur Fail to Verify Peer Certificate se produit.

- Les tunnels DTLS/TLS entre le routeur de périphérie et les contrôleurs dépendent de l'authentification basée sur les certificats. Une incohérence de temps peut entraîner des échecs de connexion entraînant l'interruption de la connexion de contrôle.
- Les journaux sur les périphériques et les contrôleurs Edge sont horodatés. Si le temps est désynchronisé, les journaux de différents périphériques ne sont pas correctement alignés, ce qui rend la corrélation des événements et le dépannage difficiles.
- Des outils tels que vAnalytics et les systèmes de surveillance externes reposent sur des horodatages précis pour la surveillance des SLA, les rapports de performances et la corrélation des événements.

Configurer

Ce document décrit comment vous pouvez configurer NTP à l'aide du modèle de fonctionnalité, des groupes de configuration et de l'interface de ligne de commande.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/vedge-20-x/systems-interfaces-book/systems-interfaces.html#c-NTP-12298
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-02system-and-interfaces.html#ntp-server-cg

Configuration de référence

Contrôleur

```
system
 ntp
  keys
   authentication 1001 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
   authentication 1002 md5 $4$KXLzYTxk6M8zj4BgLEFXKw==
   authentication 1003 md5 $4$KXLzYT1k6M8zj4BgLEFXKw==
   trusted 1001 1002
  !
  server 192.168.15.243
   key     1001
   vpn     512
   version 4
  exit
  server 192.168.15.242
   key     1002
   vpn     512
   version 4
  exit
  server us.pool.ntp.org
   vpn     512
   version 4
  exit
 !
!
```

Routeur de périphérie Cisco

```
cEdge_DC1_West_R01#show running-config | sec ntp
ntp server time.google.com prefer
ntp server pool.ntp.org

cEdge_DC1_West_R01#show sdwan running-config ntp
ntp server pool.ntp.org version 4
ntp server time.google.com prefer version 4

If Mgmt VRF is used:
ntp server vrf Mgmt-intf pool.ntp.org version 4
```

Remarque : Si le VPN 0 est utilisé pour la configuration NTP, le service NTP doit être autorisé sur l'interface du tunnel. Si des hôtes FQDN sont utilisés pour les serveurs NTP, le DNS doit être configuré sur le périphérique pour pouvoir résoudre le FQDN en adresse IP.

Dépannage

Ce document peut être utilisé pour vérifier NTP et comprendre les différentes étapes de la synchronisation NTP pour dépanner les problèmes sur les contrôleurs et les périphériques Edge :

Contrôleurs :
https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/221015-understand-ntp-association-codes-in-sd-w.html

vEdge :

https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/220330-troubleshoot-network-time-protocol-ntp.html

cEdge :
https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html

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.