Best practices configureren voor NTP-synchronisatie in SD-WAN-implementaties

Inhoud

Inleiding

In dit document wordt beschreven hoe NTP cruciaal is voor het handhaven van nauwkeurige tijdsynchronisatie tussen apparaten in de SD-WAN-structuur.

Achtergrond

Zonder de juiste synchronisatie kunnen kritieke bewerkingen zoals veilige communicatie, certificaatvalidatie en logboekregistratie mislukken. SD-WAN is een op certificaten gebaseerde, veilige en beleidsgestuurde netwerkoplossing. Tijdsynchronisatie met behulp van NTP is fundamenteel voor het behoud van de integriteit, beveiliging en functionaliteit van de SD-WAN-structuur.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Software Defined Wide Area Network (SDWAN)-oplossing.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- C8000V versie 17.15.03a
- vManage versie 20.15.03.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Belangrijkste redenen

- SD-WAN maakt gebruik van digitaal certificaat voor apparaatverificatie. Deze certificaten hebben een geldige vervaldatum en vervaldatum. Als de klok van het apparaat niet nauwkeurig is, kan deze denken dat het certificaat is verlopen of nog niet geldig is.

```
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 - Peer Certificate niet verifiëren

In dit geval, omdat de tijd buiten de datum van geldigheid van het certificaat valt, treedt er een fout op in het Peer Certificate.

- DTLS/TLS-tunnels tussen Edge Router en controllers zijn afhankelijk van op certificaten gebaseerde verificatie. Tijdsverschil kan leiden tot handshake-fouten waardoor de besturingsverbinding wordt verbroken.
- Logs op Edge-apparaten en -controllers zijn voorzien van een tijdstempel. Als de tijd niet synchroon loopt, worden logs van verschillende apparaten verkeerd uitgelijnd, waardoor het moeilijk is om gebeurtenissen te correleren en problemen op te lossen.
- Tools zoals vAnalytics en externe monitoringsystemen vertrouwen op nauwkeurige tijdstempels voor SLA-monitoring, prestatierapporten en eventcorrelatie.

Configureren

In dit document wordt beschreven hoe u NTP kunt configureren met behulp van een functiesjabloon, configuratiegroepen en CLI.

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

Referentieconfiguratie

controleur

```
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
 !
!
```

Cisco Edge Router

```
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
```

Opmerking: Als VPN 0 wordt gebruikt voor NTP-configuratie, moet NTP-service zijn toegestaan op de tunnelinterface. Als FQDN-hosts worden gebruikt voor NTP-servers, moet DNS op het apparaat zijn geconfigureerd om de FQDN naar het IP-adres te kunnen omzetten.

Problemen oplossen

Dit document kan worden gebruikt om NTP te verifiëren en verschillende stadia van NTP-synchronisatie te begrijpen om problemen op controllers en Edge-apparaten op te lossen:

Controllers:
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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.