Configure Best Practices for NTP Synchronization in SD-WAN Deployments

Contents

Introduction

- Background

Prerequisites

- Requirements
- Components Used

Top Reasons

Configure

Troubleshoot

Introduction

This document describes how NTP is crucial for maintaining accurate time synchronization across devices in the SD-WAN fabric.

Background

Without proper time sync, critical operations like secure communication, certificate validation, and logging can fail. SD-WAN is a certificate-based, secure, and policy-driven network solution. Time synchronization using NTP is foundational for maintaining the integrity, security, and functionality of the SD-WAN fabric.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Software Defined Wide Area Network (SDWAN) solution.

Components Used

The information in this document is based on these software versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Top Reasons

- SD-WAN uses digital certificate for device authentication. These certificates have valid-from and expiry dates. If the device clock is not accurate, it can think that the certificate is either expired or not valid yet.

```
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 - Fail to verify Peer Certificate

In this case, as the time is outside certificate validity date, Fail to Verify Peer Certificate error occurs.

- DTLS/TLS tunnels between Edge Router and controllers depend on certificate based authentication. Time mismatch can cause handshake failures causing control connection to break.
- Logs on Edge devices and controllers are timestamped. If time is out of sync, logs from different devices would be misaligned making event correlation and troubleshooting difficult.
- Tools like vAnalytics and external monitoring systems rely on precise timestamps for SLA monitoring, performance reports and event correlation.

Configure

This document describes how you can configure NTP using feature template, configuration groups and 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/config-groups/configuration-group-guide/using-config-groups.html

Reference Configuration

Controller

```
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
```



Note: If VPN 0 is used for NTP configuration, NTP service must be allowed on the tunnel interface. If FQDN hosts are used for NTP servers, the device must have DNS configured to be able to resolve the FQDN to IP address.

Troubleshoot

This document can be used to verify NTP and understand different stages of NTP synchronisation to troubleshoot issues on controllers and Edge devices:

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