配置SD-WAN部署中的NTP同步最佳实践

目录

简介

- 背景

先决条件

- 要求
- 使用的组件

主要原因

配置

故障排除

简介

本文档介绍NTP如何在SD-WAN交换矩阵中跨设备保持准确的时间同步。

背景

如果没有正确的时间同步，安全通信、证书验证和日志记录等关键操作可能会失败。SD-WAN是基于证书的安全、策略驱动的网络解决方案。使用NTP的时间同步是维护SD-WAN交换矩阵的完整性、安全性和功能的基础。

先决条件

要求

思科建议您了解思科软件定义广域网(SDWAN)解决方案。

使用的组件

本文档中的信息基于以下软件版本：

- C8000V版本17.15.03a
- vManage版本20.15.03.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

主要原因

- SD-WAN使用数字证书进行设备身份验证。这些证书具有有效开始日期和到期日期。如果设备时钟不准确，它可能认为证书已过期或尚未生效。

```
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 — 无法验证对等证书

在这种情况下，由于时间在证书有效日期之外，将会出现Fail to Verify Peer Certificate错误。

- 边缘路由器和控制器之间的DTLS/TLS隧道取决于基于证书的身份验证。时间不匹配可能导致握手失败，导致控制连接中断。
- 边缘设备和控制器上的日志带有时间戳。如果时间不同步，来自不同设备的日志将失调，使得事件关联和故障排除非常困难。
- vAnalytics和外部监控系统等工具依赖精确的时间戳进行SLA监控、性能报告和事件关联。

配置

本文档介绍如何使用功能模板、配置组和CLI配置NTP。

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

参考配置

控制器

```
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
 !
!
```

思科边缘路由器

```
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
```



注意：如果将VPN 0用于NTP配置，则必须在隧道接口上允许NTP服务。如果FQDN主机用于NTP服务器，设备必须配置DNS才能将FQDN解析为IP地址。

故障排除

本文档可用于验证NTP并了解NTP同步的不同阶段，以便解决控制器和边缘设备上的问题：

控制器：
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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。