Best Practices für die NTP-Synchronisierung in SD-WAN-Bereitstellungen konfigurieren

Inhalt

Einleitung

In diesem Dokument wird erläutert, wie das NTP für die Aufrechterhaltung einer präzisen Zeitsynchronisierung zwischen den Geräten in der SD-WAN-Fabric wichtig ist.

Hintergrund

Ohne ordnungsgemäße Zeitsynchronisierung können wichtige Vorgänge wie sichere Kommunikation, Zertifikatsvalidierung und Protokollierung fehlschlagen. SD-WAN ist eine zertifikatbasierte, sichere und richtlinienbasierte Netzwerklösung. Die Zeitsynchronisierung mithilfe von NTP ist die Grundlage für die Aufrechterhaltung der Integrität, Sicherheit und Funktionalität der SD-WAN-Fabric.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der SDWAN-Lösung (Software Defined Wide Area Network) von Cisco verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- C8000V Version17.15.03a
- vManage, Version 20.15.03.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Wichtigste Gründe

- Das SD-WAN verwendet ein digitales Zertifikat für die Geräteauthentifizierung. Diese Zertifikate haben ein Gültigkeitsdatum und ein Ablaufdatum. Wenn die Geräteuhr nicht korrekt ist, kann sie annehmen, dass das Zertifikat abgelaufen oder noch nicht gültig ist.

```
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-Zertifikat konnte nicht überprüft werden.

  In diesem Fall tritt ein Fehler "Fail to Verify Peer Certificate" auf, da die Zeit außerhalb des Gültigkeitsdatums des Zertifikats liegt.
- DTLS/TLS-Tunnel zwischen Edge-Router und Controller sind von der zertifikatbasierten Authentifizierung abhängig. Zeitliche Diskrepanz kann zu Handshake-Fehlern führen, die dazu führen, dass die Steuerverbindung unterbrochen wird.
- Protokolle auf Edge-Geräten und Controllern sind mit einem Zeitstempel versehen. Wenn die Zeit nicht mehr synchron ist, werden die Protokolle der verschiedenen Geräte falsch zugeordnet, was die Ereigniskorrelation und die Fehlerbehebung erschwert.
- Tools wie vAnalytics und externe Überwachungssysteme basieren auf präzisen Zeitstempeln für SLA-Überwachung, Performance-Berichte und Ereigniskorrelation.

Konfigurieren

In diesem Dokument wird beschrieben, wie Sie NTP mithilfe von Funktionsvorlagen, Konfigurationsgruppen und CLI konfigurieren können.

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

Referenzkonfiguration

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
```

Anmerkung: Wenn VPN 0 für die NTP-Konfiguration verwendet wird, muss der NTP-Dienst auf der Tunnelschnittstelle zugelassen werden. Wenn FQDN-Hosts für NTP-Server verwendet werden, muss DNS auf dem Gerät konfiguriert sein, damit der FQDN in eine IP-Adresse aufgelöst werden kann.

Fehlerbehebung

Dieses Dokument dient zur Überprüfung des NTP und zum Verständnis der verschiedenen Phasen der NTP-Synchronisierung, um Probleme auf Controllern und Edge-Geräten zu beheben:

Controller:
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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.