Configurazione di best practice per la sincronizzazione NTP in implementazioni SD-WAN

Sommario

Introduzione

Questo documento descrive come l'NTP sia fondamentale per mantenere una precisa sincronizzazione dell'ora tra i dispositivi nella struttura SD-WAN.

Introduzione

Senza una corretta sincronizzazione dell'ora, operazioni critiche quali la comunicazione protetta, la convalida dei certificati e la registrazione possono avere esito negativo. SD-WAN è una soluzione di rete basata su certificati, sicura e basata su regole. La sincronizzazione dell'ora tramite NTP è fondamentale per mantenere l'integrità, la sicurezza e la funzionalità del fabric SD-WAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della soluzione SDWAN (Software Defined Wide Area Network) di Cisco.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- C800V versione 17.15.03a
- vManage versione 20.15.03.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Principali motivi

- SD-WAN utilizza il certificato digitale per l'autenticazione dei dispositivi. Questi certificati hanno date di inizio e di scadenza valide. Se l'orologio del dispositivo non è preciso, il certificato potrebbe essere scaduto o non ancora valido.

```
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 - Impossibile verificare il certificato peer

In questo caso, poiché l'ora non è compresa nella data di validità del certificato, si verificherà l'errore Impossibile verificare il certificato peer.

- I tunnel DTLS/TLS tra il router perimetrale e i controller dipendono dall'autenticazione basata sui certificati. La mancata corrispondenza dell'ora può causare errori di handshake che causano l'interruzione della connessione del controllo.
- I log sui dispositivi e i controller Edge sono contrassegnati da un timestamp. Se il tempo non è sincronizzato, i registri di dispositivi diversi non sono allineati e rendono difficile la correlazione degli eventi e la risoluzione dei problemi.
- Strumenti come vAnalytics e i sistemi di monitoraggio esterno si basano su timestamp precisi per il monitoraggio degli SLA, i report sulle prestazioni e la correlazione degli eventi.

Configurazione

In questo documento viene descritto come configurare l'NTP utilizzando il modello di funzionalità, i gruppi di configurazione e la 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

Configurazione di riferimento

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
```

Nota: Se per la configurazione NTP viene utilizzata la VPN 0, il servizio NTP deve essere autorizzato sull'interfaccia del tunnel. Se per i server NTP vengono utilizzati host FQDN, il DNS del dispositivo deve essere configurato per essere in grado di risolvere l'FQDN in indirizzo IP.

Risoluzione dei problemi

Questo documento può essere usato per verificare l'NTP e capire le diverse fasi della sincronizzazione NTP per risolvere i problemi sui controller e sui dispositivi Edge:

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

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).