

Configurar las prácticas recomendadas para la sincronización NTP en implementaciones SD-WAN

Contenido

[Introducción](#)

[Background](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Principales razones](#)

[Configurar](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo NTP es crucial para mantener una sincronización horaria precisa entre los dispositivos en el fabric SD-WAN.

Background

Sin una sincronización horaria adecuada, las operaciones críticas como la comunicación segura, la validación de certificados y el registro pueden fallar. SD-WAN es una solución de red basada en certificados, segura y basada en políticas. La sincronización horaria mediante NTP es fundamental para mantener la integridad, seguridad y funcionalidad del fabric SD-WAN.

Prerequisites

Requirements

Cisco recomienda conocer la solución de red de área extensa definida por software (SDWAN) de Cisco.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- C8000V versión 17.15.03a
- vManage versión 20.15.03.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Principales razones

- La SD-WAN utiliza un certificado digital para la autenticación de dispositivos. Estos certificados tienen fechas de inicio y de vencimiento válidas. Si el reloj del dispositivo no es preciso, puede pensar que el certificado ha caducado o que aún no es válido.

```
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 - Error al verificar el certificado de par

En este caso, como la hora está fuera de la fecha de validez del certificado, se produce el error Fail to Verify Peer Certificate .

- Los túneles DTLS/TLS entre el router de borde y los controladores dependen de la autenticación basada en certificados. La falta de coincidencia de tiempo puede provocar fallos de enlace que interrumpan la conexión de control.
- Los registros de los dispositivos periféricos y los controladores tienen una marca de tiempo. Si el tiempo no está sincronizado, los registros de los diferentes dispositivos se alinearían incorrectamente, lo que dificultaría la correlación de eventos y la resolución de problemas.
- Las herramientas como vAnalytics y los sistemas de supervisión externa se basan en marcas de tiempo precisas para la supervisión de SLA, los informes de rendimiento y la correlación de eventos.

Configurar

Este documento describe cómo puede configurar NTP usando la plantilla de funciones, los grupos de configuración y 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>

Configuración de referencia

Controlador

system

```

ntp
keys
  authentication 1001 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
  authentication 1002 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
  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
!
!

```

Router de extremo de Cisco

```

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: Si se utiliza VPN 0 para la configuración de NTP, se debe permitir el servicio NTP en la interfaz de túnel. Si se utilizan hosts FQDN para servidores NTP, el dispositivo debe tener DNS configurado para poder resolver el FQDN en dirección IP.

Troubleshoot

Este documento se puede utilizar para verificar el NTP y comprender las diferentes etapas de la sincronización del NTP para resolver problemas en los controladores y los dispositivos periféricos:

Controladores:

<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>

Perímetro:

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).