

Configurar práticas recomendadas para sincronização de NTP em implantações de SD-WAN

Contents

[Introdução](#)

[Background](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Principais motivos](#)

[Configurar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como o NTP é crucial para manter a sincronização de tempo precisa entre dispositivos na estrutura SD-WAN.

Background

Sem a sincronização de tempo adequada, operações críticas como comunicação segura, validação de certificado e registro podem falhar. A SD-WAN é uma solução de rede baseada em certificado, segura e orientada por políticas. A sincronização de tempo usando NTP é fundamental para manter a integridade, a segurança e a funcionalidade da estrutura SD-WAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da solução Cisco Software Defined Wide Area Network (SDWAN).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- C8000V versão 17.15.03a
- vManage versão 20.15.03.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Principais motivos

- A SD-WAN usa o certificado digital para autenticação do dispositivo. Esses certificados têm datas válidas de e de expiração. Se o relógio do dispositivo não estiver preciso, ele pode achar que o certificado expirou ou ainda não é 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    PUBLIC
-----
```

INSTANCE	TYPE	PROTOCOL	SYSTEM	IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PRIVATE PORT	PUBLIC
0	vmanage	dtls		10.1.1.7	101019	0	10.1.2.190	12646	192

CRTVERFL - Falha ao verificar Certificado de Mesmo Nível

Nesse caso, como a hora está fora da data de validade do certificado, ocorre o erro Falha ao Verificar Certificado de Mesmo Nível.

- Os túneis DTLS/TLS entre o Roteador de Borda e os controladores dependem da autenticação baseada em certificado. A incompatibilidade de tempo pode causar falhas de handshake, interrompendo a conexão de controle.
- Registros em dispositivos de borda e controladores são carimbados com data e hora. Se o tempo estiver fora de sincronia, os registros de dispositivos diferentes estariam desalinhados, dificultando a correlação de eventos e a solução de problemas.
- Ferramentas como vAnalytics e sistemas de monitoramento externo dependem de carimbos de data e hora precisos para monitoramento de SLA, relatórios de desempenho e correlação de eventos.

Configurar

Este documento descreve como você pode configurar o NTP usando o modelo de recurso, os grupos de configuração e a 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>

Configuração de referência

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
!
!
```

Roteador Cisco Edge

```
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: Se a VPN 0 for usada para a configuração NTP, o serviço NTP deverá ser permitido na interface de túnel. Se os hosts FQDN forem usados para servidores NTP, o dispositivo deverá ter o DNS configurado para poder resolver o FQDN para o endereço IP.

Troubleshooting

Este documento pode ser usado para verificar o NTP e entender diferentes estágios de sincronização do NTP para solucionar problemas em controladores e dispositivos de borda:

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>

Borda:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.