

SD-WAN 구축에서 NTP 동기화에 대한 모범 사례 구성

목차

[소개](#)

[배경](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[주요 이유](#)

[구성](#)

[문제 해결](#)

소개

이 문서에서는 NTP가 SD-WAN 패브릭의 디바이스 간 시간 동기화를 정확하게 유지하는 데 어떻게 중요한지 설명합니다.

배경

적절한 시간 동기화가 없으면 보안 통신, 인증서 검증 및 로깅과 같은 중요한 작업이 실패할 수 있습니다. SD-WAN은 인증서 기반, 보안 및 정책 기반 네트워크 솔루션입니다. NTP를 사용한 시간 동기화는 SD-WAN 패브릭의 무결성, 보안 및 기능을 유지 관리하기 위한 기본 사항입니다.

사전 요구 사항

요구 사항

Cisco SDWAN(Software Defined Wide Area Network) 솔루션에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- C8000V 버전 17.15.03a
- vManage 버전 20.15.03.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

주요 이유

- SD-WAN은 장치 인증에 디지털 인증서를 사용합니다. 이러한 인증서에는 유효 시작 날짜와 만료 날짜가 있습니다. 디바이스 클럭이 정확하지 않으면 인증서가 만료되었거나 아직 유효하지 않은 것으로 생각할 수 있습니다.

```
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	PEER PUBLIC
0	vmanage	dtls	10.1.1.7	101019	0	10.1.2.190	12646	192

CRTVERFL - 피어 인증서를 확인하지 못했습니다.

이 경우 시간이 인증서 유효 날짜를 초과하므로 피어 인증서 확인 실패 오류가 발생합니다.

- 에지 라우터와 컨트롤러 간의 DTLS/TLS 터널은 인증서 기반 인증에 따라 달라집니다. 시간 불일치로 인해 핸드셰이크 오류가 발생하여 제어 연결이 끊어질 수 있습니다.
- 에지 디바이스 및 컨트롤러의 로그에 타임스탬프가 기록됩니다. 시간이 동기화되지 않으면 서로 다른 디바이스의 로그가 잘못 정렬되어 이벤트 상관관계 분석 및 트러블슈팅이 어려워집니다.
- vAnalytics 및 외부 모니터링 시스템과 같은 툴은 SLA 모니터링, 성능 보고서 및 이벤트 상관관계에 대한 정확한 타임스탬프를 사용합니다.

구성

이 문서에서는 기능 템플릿, 컨피그레이션 그룹 및 CLI를 사용하여 NTP를 구성하는 방법에 대해 설명합니다.

<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>

참조 구성

컨트롤러

```
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 에지 라우터

```
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
```

 참고: VPN 0이 NTP 컨피그레이션에 사용되는 경우 터널 인터페이스에서 NTP 서비스를 허용해야 합니다. FQDN 호스트가 NTP 서버에 사용되는 경우 디바이스에는 FQDN을 IP 주소로 확인할 수 있도록 구성된 DNS가 있어야 합니다.

문제 해결

이 문서는 NTP를 확인하고 NTP 동기화의 여러 단계를 파악하여 컨트롤러 및 에지 디바이스의 문제를 해결하는 데 사용할 수 있습니다.

컨트롤러:

<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>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서([링크 제공됨](#))를 참조할 것을 권장합니다.