일반적인 SD-WAN 제어 및 데이터 플레인 문제 해결

목차

소개

이 문서에서는 일반적인 SD-WAN(Software Defined Wide Area Network) 제어 및 데이터 플레인 문제의 트러블슈팅을 시작하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco Catalyst 솔루션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

개요

이 문서는 전체 프로덕션 환경에서 발생하는 과제를 디버깅하기 위한 시작 지점을 제공하는 Runbook으로 설계되었습니다. 각 섹션에서는 이러한 일반적으로 발생하는 문제를 디버깅할 때 수집하거나 검색할 수 있는 일반적인 활용 사례와 예상 데이터 요소를 제공합니다.

기본 컨피그레이션

기본 컨피그레이션이 라우터에 있고 디바이스에 따른 값이 오버레이의 각 디바이스에 고유한지 확인합니다.

시스템 컨피그레이션

<#root>

```
system
 system-ip <system -ip>
 site-id <site-id>
 admin-tech-on-failure
 organization-name <organization name>
 vbond <vbond-ip>
!
```

Example:

```
system
 system-ip 10.2.2.1
 site-id 2
 admin-tech-on-failure
 organization-name "TAC - 22201"
 vbond 10.106.50.235
!
```

인터페이스 컨피그레이션

```
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit

sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec
   color blue restrict
   no allow-service all
```

```
   no allow-service bgp
   no allow-service dhcp
   no allow-service dns
   no allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
exit
```

라우터에 라우팅 테이블에서 라우트를 사용하여 컨트롤러(vBond, vManage, vSmart)와의 제어 연결을 설정할 수 있는지 확인합니다. 이 명령을 사용하여 라우팅 테이블에 설치된 모든 경로를 볼 수 있습니다.

```
show ip route
```

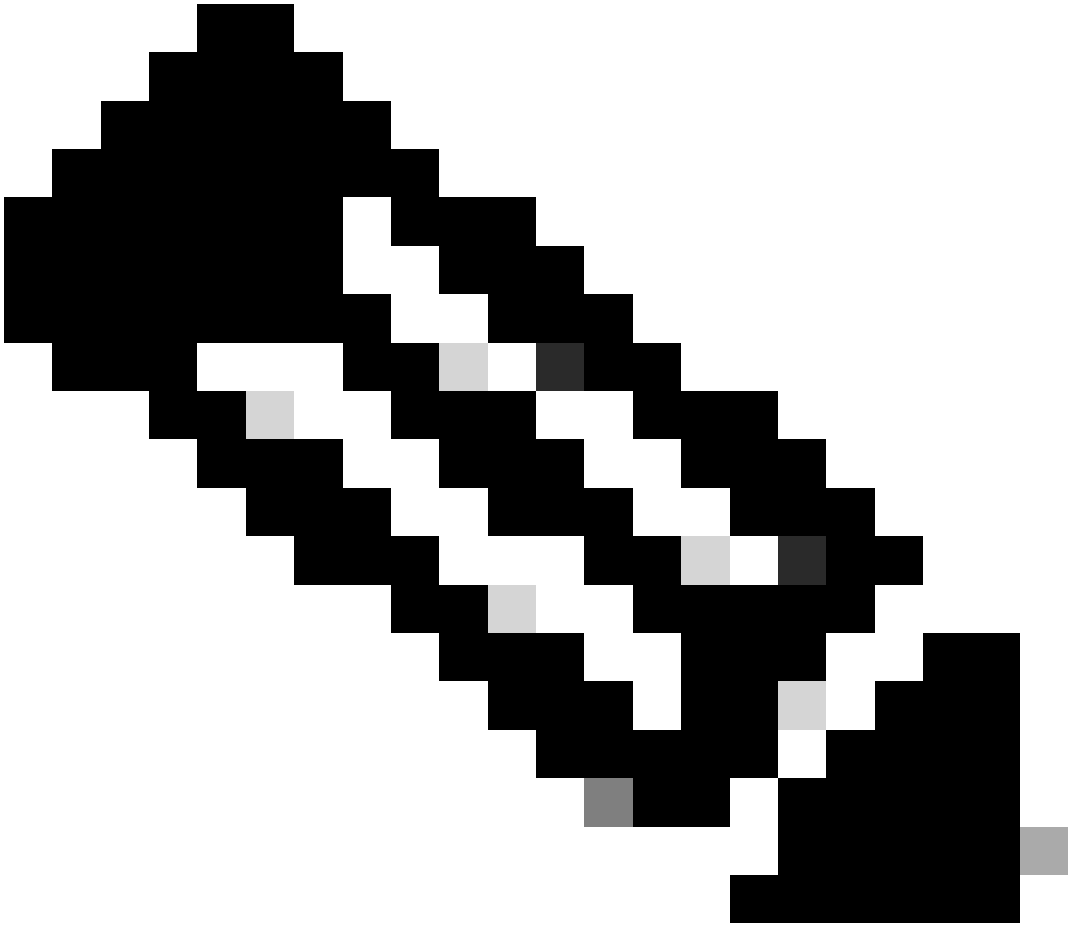
vBond FQDN을 사용하는 경우 구성된 DNS 서버 또는 이름 서버에 vBond 호스트 이름을 확인하는 항목이 있는지 확인하십시오. 다음 명령을 사용하여 어떤 DNS 서버 또는 name-server가 구성되어 있는지 확인할 수 있습니다.

```
show run | in ip name-server
```

인증서

다음 명령을 사용하여 인증서가 라우터에 설치되어 있는지 확인합니다.

```
show sdwan certificate installed
```



참고:엔터프라이즈 인증서를 사용하지 않는 경우 인증서가 라우터에서 이미 사용 가능합니다. 하드웨어 플랫폼의 경우 디바이스 인증서가 라우터 하드웨어에 내장되어 있습니다. 가상 라우터의 경우 vManage는 인증 기관의 역할을 하며 클라우드 라우터용 인증서를 생성합니다.

컨트롤러에서 엔터프라이즈 인증서를 사용하는 경우 엔터프라이즈 CA의 루트 인증서가 라우터에 설치되어 있는지 확인합니다.

다음 명령을 사용하여 루트 인증서가 라우터에 설치되어 있는지 확인합니다.

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

show sdwan control local-properties의 출력을 확인하여 필요한 컨피그레이션 및 인증서가 있는지 확인합니다.

```
SD-WAN-Router#show sdwan control local-properties
personality                          vedge
sp-organization-name                 TAC - 22201
organization-name                    TAC - 22201
root-ca-chain-status                 Installed

certificate-status                   Installed
certificate-validity                 Valid
certificate-not-valid-before         Nov 23 07:21:37 2015 GMT
certificate-not-valid-after          Nov 23 07:21:37 2025 GMT



enterprise-cert-status               Not-Applicable
enterprise-cert-validity             Not Applicable
enterprise-cert-not-valid-before     Not Applicable
enterprise-cert-not-valid-after      Not Applicable

dns-name                             10.106.50.235
site-id                              2
domain-id                            1
protocol                             dtls
tls-port                             0
system-ip                            10.2.2.1
chassis-num/unique-id                ASR1001-X-JAE194707HJ
serial-num                           983558
subject-serial-num                   JAE194707HJ
enterprise-serial-num                No certificate installed
token                                -NA-
keygen-interval                      1:00:00:00
retry-interval                       0:00:00:18
no-activity-exp-interval             0:00:00:20
dns-cache-ttl                        0:00:02:00
port-hopped                          TRUE
time-since-last-port-hop             0:00:01:26
embargo-check                        success
number-vbond-peers                   1

INDEX   IP                                       PORT
------------------------------------------------------
0       10.106.50.235                            12346

number-active-wan-interfaces         2


 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE

INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0          10.197.240.4    12426  10.197.240.4    ::
GigabitEthernet0/0/1          10.197.242.10   12406  10.197.242.10   ::
```

show sdwan control local-properties의 출력을 확인할 때 다음 조건을 모두 충족하는지 확인합니다
.

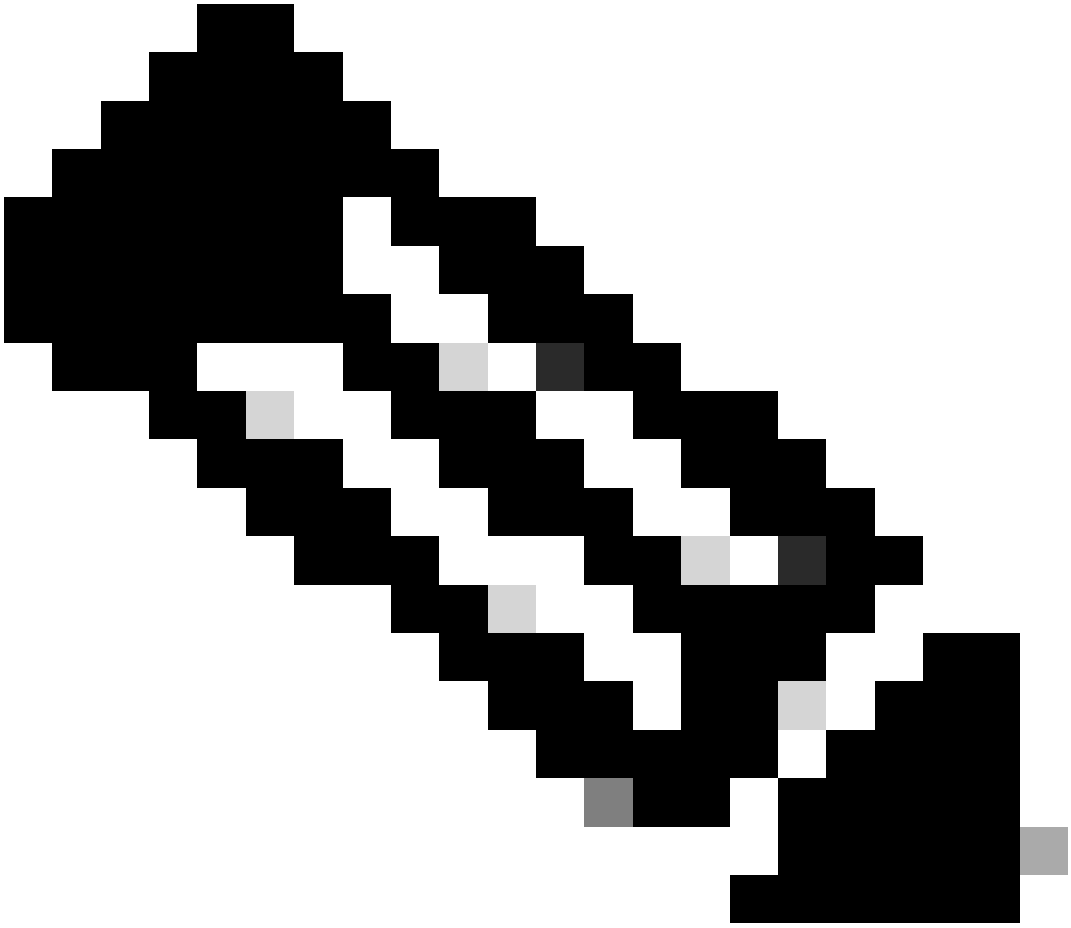
- organization-name이 올바르게 반영됩니다.
- 인증서 유효성은 출력을 확인할 때 유효합니다.
- vBond FQDN/IP 주소가 정확합니다.
- System-ip/Site-id가 정확합니다.
- vBond IP 주소는 "number-vbond-peers" 항목에 표시됩니다. vBond IP 주소가 표시되지 않으면 ping <vBond FQDN> 명령을 사용하여 DNS가 vBond URL을 확인하고 있는지 확인합니다.
- 인터페이스는 올바른 색상, IP 주소로 매핑되며 인터페이스의 상태는 UP입니다.
- 제어 연결을 형성하는 데 필요한 인터페이스의 MAX CNTRL은 0이 아닙니다.

제어 연결 상태

다음 명령을 사용하여 제어 연결의 상태를 확인합니다.

```
show sdwan control connection
```

모든 제어 연결이 가동 상태인 경우 디바이스에는 vBond, vManage 및 vSmart에 형성된 제어 연결이 있습니다. 필요한 vSmart 및 vManage 연결이 설정되면 vBond 제어 연결이 해제됩니다.



참고: 오버레이에 vSmart가 하나뿐이고 max-control 연결이 기본값인 2로 설정된 경우, vManage 및 vSmart에 대한 예상 연결과 함께 지속적 제어 연결이 vBond에 유지됩니다.

이 컨피그레이션은 sdwan 인터페이스 섹션의 tunnel-interface 컨피그레이션에서 사용할 수 있습니다. show sdwan run sdwan 명령을 사용하여 확인할 수 있습니다. 인터페이스에서 max-control-connection이 0으로 구성된 경우 라우터는 해당 인터페이스에 제어 연결을 형성하지 않습니다.

오버레이에 2개의 vSmarts가 있는 경우 라우터는 제어 연결을 위해 구성된 모든 TLOC(Transport Locator) 색상에서 각 vSmart에 대한 제어 연결을 구성합니다.

참고: 제어 연결을 형성하도록 구성된 여러 인터페이스가 라우터에 있는 시나리오에서 vManage에 대한 제어 연결은 라우터의 한 인터페이스 색상에만 형성됩니다.

```
SD-WAN-Router#show sdwan control connections
                                                                                        PEER
PEER     PEER PEER            SITE        DOMAIN PEER                                   PRIV  PEER
TYPE     PROT SYSTEM IP       ID          ID     PRIVATE IP                             PORT  PUBLIC IP
----------------------------------------------------------------------------------------------------------
vsmart   dtls 10.1.1.3        1           1      10.106.50.254                          12346 10.106.50.
vbond    dtls  0.0.0.0        0           0      10.106.50.235                          12346 10.106.50.
vmanage  dtls 10.1.1.2        1           0      10.106.65.182                          12346 10.106.65.
```

제어 연결 문제 해결

show sdwan control connections의 출력에서 필요한 모든 제어 연결이 설정되지 않은 경우 show sdwan control connection-history의 출력을 확인합니다.

```
SD-WAN-Router#show sdwan control connection-history

Legend for Errors

ACSRREJ     - Challenge rejected by peer.                    NOVMCFG    - No cfg in vmanage for device.
BDSGVERFL   - Board ID Signature Verify Failure.             NOZTPEN    - No/Bad chassis-number entry in ZTP.
BIDNTPR     - Board ID not Initialized.                      OPERDOWN   - Interface went oper down.
BIDNTVRFD   - Peer Board ID Cert not verified.               ORPTMO     - Server's peer timed out.
BIDSIG     - Board ID signing failure.                       RMGSPR     - Remove Global saved peer.
CERTEXPRD   - Certificate Expired                            RXTRDWN    - Received Teardown.
CRTREJSER   - Challenge response rejected by peer.           RDSIGFBD   - Read Signature from Board ID failed.
CRTVERFL    - Fail to verify Peer Certificate.               SERNTPRES  - Serial Number not present.
CTORGNMMIS  - Certificate Org name mismatch.                 SSLNFAIL   - Failure to create new SSL context.
DCONFAIL    - DTLS connection failure.                       STNMODETD  - Teardown extra vBond in STUN server r
DEVALC      - Device memory Alloc failures.                  SYSIPCHNG  - System-IP changed.
DHSTMO      - DTLS HandShake Timeout.                        SYSPRCH    - System property changed
DISCVBD     - Disconnect vBond after register reply.         TMRALC     - Timer Object Memory Failure.
DISTLOC     - TLOC Disabled.                                 TUNALC     - Tunnel Object Memory Failure.
DUPCLHELO   - Recd a Dup Client Hello, Reset Gl Peer.        TXCHTOBD   - Failed to send challenge to BoardID.
DUPSER      - Duplicate Serial Number.                       UNMSGBDRG  - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                            UNAUTHEL   - Recd Hello from Unauthenticated peer
HAFAIL      - SSL Handshake failure.                         VBDEST     - vDaemon process terminated.
IP_TOS      - Socket Options failure.                        VECRTREV   - vEdge Certification revoked.
LISFD       - Listener Socket FD Error.                      VSCRTREV   - vSmart Certificate revoked.
MGRTBLCKD   - Migration blocked. Wait for local TMO.         VB_TMO     - Peer vBond Timed out.
MEMALCFL    - Memory Allocation Failure.                     VM_TMO     - Peer vManage Timed out.
NOACTVB     - No Active vBond found to connect.              VP_TMO     - Peer vEdge Timed out.
NOERR       - No Error.                                      VS_TMO     - Peer vSmart Timed out.
NOSLPRCRT   - Unable to get peer's certificate.              XTVMTRDN   - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections.             XTVSTRDN   - Teardown extra vSmart.
NTPRVMINT   - Not preferred interface to vManage.            STENTRY     - Delete same tloc stale entry.
HWCERTREN   - Hardware vEdge Enterprise Cert Renewed         HWCERTREV - Hardware vEdge Enterprise Cert Revoke
EMBARGOFAIL - Embargo check failed

                                                                           PEER                     PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-----------------------------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vmanage  dtls    10.1.1.2          1           0      10.106.65.182    12346    10.106.65.182    12346
vsmart   dtls    10.1.1.3          1           1      10.106.50.254    12346    10.106.50.254    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
vbond    dtls     0.0.0.0          0           0      10.106.50.235    12346    10.106.50.235    12346
```

show sdwan control connection-history 출력에서 다음 항목을 선택합니다.

- 지정된 타임스탬프에서 제어 연결이 실패하는 컨트롤러의 유형입니다.
- 컨트롤 연결에 실패했을 때 오류가 발생했습니다. 오류, 로컬 오류 및 원격 오류에 대한 열이

2개 있습니다. 로컬 오류는 라우터에서 발생한 오류를 나타냅니다. Remote Error(원격 오류)는 해당 컨트롤러에서 발생한 오류를 나타냅니다. 출력 시작 부분에 오류 범례가 있습니다.

- Repeat count(반복 횟수) - 동일한 이유로 연결이 실패한 횟수를 나타냅니다.

일반 오류 코드 오류

- DCONFAIL(DTLS 연결 실패) : 이 오류는 라우터와 각 컨트롤러 간에 교환된 DTLS 패킷이 손실되어 DTLS 핸드셰이크를 완료할 수 없음을 나타냅니다. 이를 더 잘 이해하기 위해 라우터 및 해당 컨트롤러에서 동시 패킷 캡처를 설정할 수 있습니다. 패킷 캡처를 설정하는 다양한 방법은 Embedded Packet Capture 섹션에서 공유됩니다. 패킷 캡처를 분석하는 동안 한 쪽에서 전송된 패킷이 수정 없이 다른 쪽에서 수신되는지 확인하는 것이 중요합니다. 한쪽 끝에서 전송된 패킷이 다른 쪽 끝에서 수신되지 않는 경우, 이는 언더레이 회로에 패킷 손실이 있음을 나타내며, 이를 통신 사업자에게 확인해야 합니다. 패킷 캡처를 수행하는 방법에 대한 자세한 내용은 Underlay Issues(언더레이 문제) 섹션에서 확인할 수 있습니다.

- BIDNTVRFD(보드 ID가 확인되지 않음): 이 오류는 UUID 및 인증서 일련 번호가 컨트롤러 vEdge 목록의 유효한 항목이 아님을 나타냅니다. 다음 명령을 사용하여 컨트롤러에서 유효한 베지 목록의 출력을 확인할 수 있습니다.

<#root>

vBond:

show orchestrator valid-vedges

vManage/vSmart:

show control valid-vedges

일반적으로 BIDNTVRFD는 컨트롤러에서 생성되므로 라우터의 원격 오류입니다. 각 컨트롤러에서 다음 명령을 사용하여 /var/log/tmplog 디렉토리에 있는 vdebug 파일의 로그를 확인할 수 있습니다
.

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- CRTVERFL(Certificate Verification Failed): 이 오류는 피어가 전송한 인증서를 확인할 수 없음을 나타냅니다.

- 라우터의 로컬 오류인 경우 DTLS 핸드셰이크의 일부로 전송된 컨트롤러 인증서가 라우터에 의해 검증될 수 없음을 나타냅니다. 이 문제의 일반적인 원인 중 하나는 라우터에 컨트롤러 인증서에 서명한 인증 기관의 루트 인증서가 없다는 것입니다. 이 명령을 사용하여 인증서의 상태를 확인하여 필요한 루트 인증서가 라우터에 있는지 확인합니다.

```
show sdwan certificate root-ca-cert
show sdwan certificate root-ca-cert | inc Issuer
```

- 이 오류가 라우터의 원격 오류인 경우 각 컨트롤러의 vdebug 로그 파일을 확인하여 다음 명령을 사용하여 원인을 파악합니다.

```
vmanage# vshell
vmanage:~$ cd /var/log/tmplog/
vmanage:/var/log/tmplog$ tail -f vdebug
```

- VB_TMO(vBond Timeout) / VM_TMO(vManage Timeout) / VP_TMO(vPeer Timeout) / VS_TMO(vSmart Timeout): 이러한 오류는 디바이스 간에 패킷 손실이 발생하여 제어 연결이 시간 초과되었음을 나타냅니다. 이를 더 잘 이해하기 위해 라우터 및 해당 컨트롤러에서 동시 패킷 캡처를 설정할 수 있습니다. 패킷 캡처를 설정하는 다양한 방법은 Embedded Packet Capture 섹션에서 공유됩니다. 패킷 캡처를 분석하는 동안 한 쪽에서 보낸 패킷이 수정 없이 다른 쪽에서 수신되는지 확인하는 것이 중요합니다. 한쪽 끝에서 전송된 패킷이 다른 쪽 끝에서 수신되지 않은 경우, 이는 서비스 공급자와 확인해야 하는 언더레이 회로에 패킷 손실이 있음을 나타냅니다

기타 제어 연결 실패 오류 코드를 해결하는 방법에 대한 지침은 다음 문서를 참조하십시오.

SD-WAN 제어 연결 문제 해결

언더레이(Underlay) 문제

언더레이의 패킷 손실 문제를 해결하는 데 사용되는 툴은 디바이스마다 다릅니다. SD-WAN 컨트롤러 및 vEdge 라우터의 경우 tcpdump 명령을 사용할 수 있습니다. Catalyst IOS® XE Edge의 경우 EPC(Embedded Packet Capture) 및 FIA(Feature Invocation Array) 추적을 사용합니다.

제어 연결이 실패하는 이유와 문제의 위치를 파악하려면 패킷 손실이 발생하는 위치를 이해해야 합니다. 예를 들어, vBond 및 Edge 라우터가 제어 연결을 형성하지 않는 경우 이 설명서에서는 문제를 격리하는 방법을 설명합니다.

TCP 덤프

```
tcpdump vpn 0 interface ge0/0 options "host 10.1.1.x -vv"
```

패킷의 요청 및 응답에 따라 사용자는 삭제를 담당하는 디바이스를 이해할 수 있습니다. tcpdump 명령은 모든 컨트롤러와 vEdge 디바이스에서 사용할 수 있습니다.

임베디드 패킷 캡처

디바이스에 ACL을 생성합니다.

```
ip access-list extended TAC
10 permit ip host <edge-private-ip> host <controller-public-ip>
20 permit ip host <controller-public-ip> host <edge-private-ip>
```

모니터 캡처를 구성하고 시작합니다.

```
monitor capture CAP access-list TAC bidirectional
monitor capture CAP start
```

캡처를 중지하고 캡처 파일을 내보냅니다.

```
monitor capture CAP stop
monitor capture CAP export bootflash:<filename>
```

wireshark에서 파일의 내용을 보고 삭제를 확인합니다. 자세한 내용은 Configure and Capture Embedded Packet on Software에서 확인할 수 있습니다.

FIA 추적

FIA 추적을 구성합니다.

```
debug platform condition ipv4 <ip> both
debug platform packet-trace packet 2048 fia-trace data-size 4096
debug platform condition start
```

fia 구문 패킷 출력을 봅니다.

```
debug platform condition stop
show platform packet-trace summary
show platform packet-trace summary | i DROP
```

삭제되는 경우 삭제된 패킷에 대한 FIA 추적 출력을 구문 분석합니다.

```
show platform packet-trace packet <packet-no> decode
```

추가 FIA 추적 옵션에 대한 자세한 내용은 다음 문서를 참조하십시오. IOS-XE Datapath 패킷 추적 기능 문제 해결

FIA Trace 비디오가 포함된 Catalyst SD-WAN 에지의 정책 삭제 확인은 FIA 추적을 사용하는 예를 제공합니다.

관리 기술 생성

SD-WAN 환경에서 Collect an Admin-Tech and Upload to TAC Case - Cisco를 참조하십시오.

관련 정보

기술 지원 및 문서 – Cisco Systems

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.