SD-WAN 제어 연결 문제 해결

목차

소개

이 문서에서는 제어 연결에 문제를 일으킬 수 있는 몇 가지 가능한 원인과 문제 해결 방법에 대해 설명합니다.

배경 정보

> **참고**: 이 문서에 제시된 대부분의 명령 출력은 vEdge 라우터에서 가져온 것입니다. 그러나 이 접근 방식은 Cisco IOS® XE SD-WAN 소프트웨어를 실행하는 라우터에서도 동일합니다. 다음을 입력합니다. **sdwan** 키워드를 사용하면 Cisco IOS XE SD-WAN 소프트웨어에서 동일한 출력을 얻을 수 있습니다. 예를 들면 다음과 같습니다. **show sdwan control connections** 대신 **show control connections** .

문제를 해결하기 전에 문제의 WAN 에지가 올바르게 구성되었는지 확인하십시오.

여기에는 다음이 포함됩니다.

- 설치된 유효한 인증서.
- 이러한 컨피그레이션은 **system** 차단:
  - 시스템 IP
  - 사이트 ID
  - 조직 이름
  - vBond 주소
- 터널 옵션 및 IP 주소로 구성된 VPN 0 전송 인터페이스.

• vEdge에서 올바르게 구성된 시스템 클럭 및 다른 디바이스/컨트롤러와 일치하는 시스템 클럭: 이 **show clock** 명령에서 현재 시간 집합을 확인합니다.

다음을 입력합니다. **clock set** 명령을 사용하여 디바이스에서 올바른 시간을 설정합니다.

앞에서 언급한 모든 사례의 경우 TLOC(Transport Locator)가 설정되어 있는지 확인합니다. 이 내용을 확인하려면 **show control local-properties** 명령을 실행합니다.

다음은 유효한 출력의 예입니다.

```
branch-vE1# show control local-properties
personality                   vedge
organization-name             vIPtela Inc Regression
certificate-status            Installed
root-ca-chain-status          Installed

certificate-validity          Valid
certificate-not-valid-before Sep 06 22:39:01 2018 GMT
certificate-not-valid-after  Sep 06 22:39:01 2019 GMT

dns-name                      vbond-dns-name.cisco.com site-id                      10 domain-id
                   1 protocol                     dtls tls-port                       0 system-ip
                   10.1.10.1 chassis-num/unique-id        66cb2a8b-2eeb-479b-83d0-0682b64d8190
serial-num                    12345718 vsmart-list-version          0 keygen-interval
             1:00:00:00 retry-interval               0:00:00:17 no-activity-exp-interval
    0:00:00:12 dns-cache-ttl                0:00:02:00 port-hopped                   TRUE time-
since-last-port-hop     20:16:24:43 number-vbond-peers           2  INDEX   IP
                PORT ------------------------------ 0       10.3.25.25          12346   1
      10.4.30.30          12346   number-active-wan-interfaces 2    PUBLIC      PUBLIC  PRIVATE
    PRIVATE                                    RESTRICT/   LAST         MAX   SPI TIME    LAST-
RESORT   INTERFACE  IPv4        PORT    IPv4        PORT     VS/VM COLOR       CARRIER  STATE
CONTROL     CONNECTION   CNTRL REMAINING   INTERFACE ----------------------------------------
-------------------------------------------------------------------------------------------
-- ge0/1      10.1.7.11    12346   10.1.7.11    12346     2/1  gold        default  up
     no/yes    0:00:00:16   2     0:07:33:55  No ge0/2      10.2.9.11    12366   10.2.9.11
   12366     2/0  silver      default  up      no/yes    0:00:00:12   2     0:07:35:16  No
```

vEdge 소프트웨어 버전 16.3 이상에서는 출력에 몇 가지 추가 필드가 있습니다.

```
number-vbond-peers           1
number-active-wan-interfaces 1

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
               PRIVATE                          MAX   RESTRICT/           LAST         SPI TIME
   NAT  VM INTERFACE  IPv4          PORT   IPv4         IPv6                   PORT   VS/VM
COLOR         STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON
                                                                                          STU
N                                             PRF ----------------------------------------
-------------------------------------------------------------------------------------------
------- ge0/4  172.16.0.20   12386  192.168.0.20  2601:647:4380:ca75::c2  12386  2/1  public-
internet  up   2  no/yes/no   No/Yes 0:10:34:16  0:03:03:26  E    5
```

문제 시나리오

DTLS 연결 실패(DCONFAIL)

이는 제어 연결의 일반적인 문제 중 하나이며, 이는 발생하지 않습니다. 방화벽이나 기타 연결 문제가 원인일 수 있습니다.

일부 또는 모든 패킷이 어딘가에서 삭제/필터링될 수 있습니다. 더 큰 것의 예는**tcpdump** 결과를 확인하십시오.

- 다음 홉(NH) 라우터에 연결할 수 없습니다.
- 기본 게이트웨이가 RIB(Routing Information Base)에 설치되지 않았습니다.
- DTLS(Datagram Transport Layer Security) 포트가 컨트롤러에서 열려 있지 않습니다.

다음 show 명령을 사용할 수 있습니다.

```
#Check that Next hop
show ip route vpn 0
#Check ARP table for Default GW
show arp
#Ping default GW
ping <...>
#Ping Google DNS
ping 8.8.8.8
#Ping vBond if ICMP is allowed on vBond
ping <vBond IP>
#Traceroute to vBond DNS
traceroute <...>
```

DTLS 연결 실패의 경우 **show control connections-history** 명령 출력입니다.

```
                                                                                                    PEER
PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                   LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
IP         PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
---
0        vsmart   tls      10.0.1.5          160000000   1      10.0.2.73        23456
10.0.2.73        23456   default          trying          DCONFAIL   NOERR      10407 2019-04-
07T22:03:45+0000
```

이는 사용 시 큰 패킷이 vEdge에 도달하지 않을 때 발생합니다 **tcpdump** 예를 들어 SD-WAN(vSmart) 측에서 다음을 수행합니다.

```
tcpdump vpn 0 interface eth1 options "host 198.51.100.162 -n"

13:51:35.312109 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 1 (packet
number)
13:51:35.312382 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached
vEdege
13:51:35.318654 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 <<< not reached
vEdege
13:51:35.318726 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 853 <<< not reached
vEdege
13:51:36.318087 IP 198.51.100.162.9536 > 172.18.10.130.12546: UDP, length 140 <<<< 5
13:51:36.318185 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 79 <<<< 6
13:51:36.318233 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 1024 << not reached
vEdege
13:51:36.318241 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 879 << not reached
vEdege
```

```
13:51:36.318257 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 804 << not reached
vEdege
13:51:36.318266 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 65 <<<< 10
13:51:36.318279 IP 172.18.10.130.12546 > 198.51.100.162.9536: UDP, length 25 <<<< 11
```

vEdge 측의 예는 다음과 같습니다.

```
tcpdump vpn 0 interface ge0/1 options "host 203.0.113.147 -n"
13:51:35.250077 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 1
13:51:36.257490 IP 198.51.100.162.12426 > 203.0.113.147.12746: UDP, length 140 <<<< 5
13:51:36.325456 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 79 <<<< 6
13:51:36.325483 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 65 <<<< 10
13:51:36.325538 IP 203.0.113.147.12746 > 198.51.100.162.12426: UDP, length 25 <<<< 11
```

> **참고**: Cisco IOS XE SD-WAN 소프트웨어에서 EPC(Embedded Packet Capture)를 대신 사용할 수 있습니다. **tcpdump**.

다음을 사용할 수 있습니다. **traceroute** 또는 **nping** 또한 서비스 공급자는 더 큰 UDP 패킷, 조각화된 UDP 패킷(특히 UDP 작은 조각) 또는 DSCP 표시된 패킷의 전달에 문제가 있을 수 있으므로 다른 패킷 크기의 트래픽을 생성하고 연결을 확인하기 위해 DSCP(Differentiated Services Code Point) 마크를 표시합니다. 다음 예는 **nping** 성공적으로 연결할 수 있습니다.

vSmart에서

```
vSmart# tools nping vpn 0 198.51.100.162 options "--udp -p 12406 -g 12846 --source-ip
172.18.10.130 --df --data-length 555 --tos 192"
Nping in VPN 0
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2019-05-17 23:28 UTC
SENT (0.0220s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
SENT (1.0240s) UDP 172.18.10.130:12846 > 198.51.100.162:12406 ttl=64 id=16578 iplen=583
```

vEdge의 예는 다음과 같습니다.

```
vEdge# tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"
tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:29:43.492632 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
18:29:44.494591 IP 203.0.113.147.12846 > 198.51.100.162.12406: UDP, length 555
```

다음은 ISE와의 연결이 실패한 예입니다 **traceroute** vSmart의 명령(vShell에서 실행):

```
vSmart$ traceroute 198.51.100.162 1400 -F -p 12406 -U -t 192 -n -m 20
traceroute to 198.51.100.162.162 (198.51.100.162.162), 20 hops max, 1400 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  10.65.14.177  0.435 ms 10.65.13.225  0.657 ms  0.302 ms
 7  10.10.28.115  0.322 ms 10.93.28.127  0.349 ms 10.93.28.109  1.218 ms
 8  * * *
 9  * * *
10  * 10.10.114.192  4.619 ms *
11  * * *
12  * * *
13  * * *
14  * * *
```

```
15  * * *
16  10.68.72.61  2.162 ms * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

vEdge는 vSmart에서 보낸 패킷을 수신하지 않습니다(일부 다른 트래픽 또는 프래그먼트만).

```
vEdge# tcpdump vpn 0 interface ge0/1 options "-n host 203.0.113.147 and udp"
tcpdump -i ge0_1 -s 128 -n host 203.0.113.147 and udp in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 128 bytes
18:16:30.232959 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 65
18:16:30.232969 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 25
18:16:33.399412 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:34.225796 IP 198.51.100.162.12386 > 203.0.113.147.12846: UDP, length 140
18:16:38.406256 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
18:16:43.413314 IP 203.0.113.147.12846 > 198.51.100.162.12386: UDP, length 16
```

TLOC 사용 안 함(DISTLOC)

TLOC Disabled 메시지로 트리거되는 원인은 다음과 같습니다.

- 제어 연결을 지웁니다.
- TLOC의 색상을 변경합니다.
- 시스템 IP를 변경합니다.

시스템 블록에 언급된 컨피그레이션 또는 의 터널 속성에서 변경**show control connections-history**명령 출력입니다.

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------
vmanage  dtls     192.168.30.101   1           0      192.168.20.101   12346    192.168.20.101
12346   biz-internet     tear_down       DISTLOC    NOERR      3     2019-06-01T14:43:11+0200
vsmart   dtls     192.168.30.103   1           1      192.168.20.103   12346    192.168.20.103
12346   biz-internet     tear_down       DISTLOC    NOERR      4     2019-06-01T14:43:11+0200
vbond    dtls     0.0.0.0          0           0      192.168.20.102   12346    192.168.20.102
12346   biz-internet     tear_down       DISTLOC    NOERR      4     2019-06-01T14:43:11+0200
```

보드 ID가 초기화되지 않음(BIDNTPR)

네트워크 연결이 지속적으로 플랩하는 매우 불안정한 네트워크에서 다음을 확인할 수 있습니다 TXCHTOBD - failed to send a challenge to Board ID failed 및/또는 RDSIGFBD - Read Signature from Board ID failed. 또한 잠

금 문제로 인해 보드 ID로 보낸 챌린지가 실패하는 경우가 종종 있으며, 그러한 경우 보드 ID를 재설정하고 다시 시도하십시오. 자주 발생하지 않으며, 제어 연결의 형태를 지연시킵니다. 이는 이후 버전에서 수정되었습니다.

```
                                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC                                  LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
vbond    dtls     -               0           0           203.0.113.109    12346
203.0.113.109    12346   silver           challenge       TXCHTOBD   NOERR      2     2019-05-
22T05:53:47+0000
vbond    dtls     -               0           0           203.0.113.56     12346
203.0.113.56     12346   silver           challenge       TXCHTOBD   NOERR      0     2019-05-
21T09:50:41+0000
```

BDSGVERFL - 보드 ID 서명 실패

이는 vEdge chassis-num/unique-id/serial number가 vBond에서 거부되었음을 나타냅니다. 이 경우, vEdge 정보가 **show control local-properties** 명령 출력 및 해당 출력을 **show orchestrator valid-vedges** vBond에 있습니다.

vEdge에 대한 항목이 없는 경우 다음 항목이 있는지 확인합니다.

- vEdge를 smart account에 추가했습니다.
- 해당 파일을 vManage에 올바르게 업로드했습니다.

클릭 **Send to Controllers** 의 밑에 **Configuration > Certificates.**

유효한 vEdge 테이블의 중복 항목이 있는지 확인하고 Cisco TAC(Technical Assistance Center)에 문의하여 추가 트러블슈팅을 요청하십시오

'Connect'에서 고착: 라우팅 문제

제어 연결은 네트워크에 라우팅 문제가 있는 경우 표시되지 않습니다. 올바른 NH/TLOC를 사용하여 RIB에 올바른 경로가 있는지 확인합니다.

예를 들면 다음과 같습니다.

- RIB의 vBond에 대한 보다 구체적인 경로는 제어 연결을 설정하는 데 사용되지 않는 NH/TLOC를 가리킵니다.
- 업스트림 서비스 공급자 간에 TLOC IP가 유출되어 라우팅이 올바르지 않습니다.

확인을 위해 다음 명령을 입력합니다.

```
show ip route
show ip routes vpn 0 <prefix/mask>
ping <vBond IP>
```

IP-Prefix에 대한 거리 값 및 프로토콜을 찾습니다.

vEdge는 성공하지 못하거나 컨트롤러에 대한 연결이 계속 깜박이는 상태에서 제어 연결을 설정하려고 시도합니다.

다음을 사용하여 확인합니다. **show control connections** 및/또는 **show sdwan control connections-history** 명령을 사용합니다.

```
vedge1# show control connections
                                                                                    PEER
PEER                                        CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV
PEER                                       PUB                                      GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT
PUBLIC IP                                  PORT  LOCAL COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      192.168.20.102                       12346
192.168.20.102                             12346 biz-internet    -     connect          0
```

소켓 오류(LISPD)

네트워크에 중복된 IP가 있으면 제어 연결이 나타나지 않습니다. Cisco의 LISFD - Listener Socket FD Error 메시지. 이 문제는 패킷 손상, RESET, TLS의 vEdge와 컨트롤러 간 불일치, DTLS 포트(FW 포트가 열려 있지 않은 경우) 등 다른 이유로 발생할 수 있습니다.

가장 일반적인 원인은 중복 전송 IP입니다. 연결을 확인하고 주소가 고유한지 확인합니다.

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
vbond    dtls     -                0           0           203.0.113.21     12346
203.0.113.21     12346   default          up              LISFD      NOERR      0     2019-04-
30T15:46:25+0000
```

피어 시간 초과 문제(VM_TMO)

피어 시간 초과 조건은 vEdge가 해당 컨트롤러에 대한 연결 능력을 상실할 때 트리거됩니다.

이 예에서는 Firepower Threat Defense**vManage Timeout msg (peer VM_TMO)**. 기타 항목에는 피어 vBond, vSmart 및/또는 vEdge 시간 초과가 포함됩니다(**VB_TMO, VP_TMO, VS_TMO**).

트러블슈팅의 일환으로 컨트롤러에 연결되어 있는지 확인합니다. ICMP(Internet Control Message Protocol) 및/또는 **traceroute** IP 주소를 입력합니다. 트래픽 감소가 많은 경우(손실이 높음) 급속 **ping** 우수한 성능을 보장합니다.

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
```

```
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
vmanage  tls      10.0.1.3          3           0           10.0.2.42        23456
203.0.113.124   23456   default          tear_down       VM_TMO     NOERR      21    2019-04-
30T15:59:24+0000
```

또한 **show control connections-history detail** 카운터에 심각한 불일치가 있는지 확인하기 위해 TX/RX 제어 통계를 살펴보기 위한 명령 출력 출력에서 RX 및 TX hello 패킷 번호의 차이를 확인합니다.

```
-------------------------------------------------------------------------------------------
 LOCAL-COLOR- biz-internet SYSTEM-IP- 192.168.30.103   PEER-PERSONALITY- vsmart
-------------------------------------------------------------------------------------------
site-id             1
domain-id           1
protocol            dtls
private-ip          192.168.20.103
private-port        12346
public-ip           192.168.20.103
public-port         12346
UUID/chassis-number 4fc4bf2c-f170-46ac-b217-16fb150fef1d
state               tear_down [Local Err: ERR_DISABLE_TLOC] [Remote Err: NO_ERROR]
downtime            2019-06-01T14:52:49+0200
repeat count        5
previous downtime   2019-06-01T14:43:11+0200

  Tx Statistics-
  --------------
    hello                   597
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                1
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0
  Rx Statistics-
  --------------
    hello                   553
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0
```

일련 번호 없음(CRTREJSER, BIDNTVRFD)

지정된 디바이스의 컨트롤러에 일련 번호가 없으면 제어 연결이 실패합니다.

다음을 사용하여 확인할 수 있습니다. **show controllers [valid-vsmarts | valid-vedges]** 대부분의 경우 출력 및 고정됩니다. 탐색 **Configuration > Certificates > Send to Controllers or Send to vBond** vManage 탭의 버튼 vBond에서 확인 **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts.**

vBond의 로그에서는 이러한 메시지를 이유가 있는 상태로 관찰합니다 ERR_BID_NOT_VERIFIED:

```
messages:local7 info: Dec 21 01:13:31 vBond-1 VBOND[1677]: %Viptela-vBond-1-vbond_0-6-INFO-
1400002: Notification: 12/21/2018 1:13:31 vbond-reject-vedge-connection severit
y-level:major host-name:"vBond-1" system-ip:10.0.1.11 uuid:"11OG301234567" organization-
name:"Example_Orgname" sp-organization-name:"Example_Orgname"" reason:"ERR_BID_NOT_VERIFIED"
```

이러한 문제를 해결할 때 PnP 포털(software.cisco.com) 및 vManage에서 올바른 일련 번호 및 디바이스 모델이 구성 및 프로비저닝되었는지 확인합니다.

섀시 번호 및 인증서 일련 번호를 확인하기 위해 vEdge 라우터에서 다음 명령을 사용할 수 있습니다.

```
vEdge1# show control local-properties | include  "chassis-num|serial-num"
chassis-num/unique-id        11OG528180107
serial-num                   1001247E
```

Cisco IOS XE SD-WAN 소프트웨어를 실행하는 라우터에서 다음 명령을 입력합니다.

```
cEdge1#show sdwan control local-properties | include chassis-num|serial-num
chassis-num/unique-id            C1111-4PLTEEA-FGL223911LK
serial-num                       016E9999
```

또는 다음 명령을 사용합니다.

```
Router#show crypto pki certificates CISCO_IDEVID_SUDI | s ^Certificate
Certificate
  Status: Available
  Certificate Serial Number (hex): 016E9999
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: C1111-4PLTEEA
    Serial Number: PID:C1111-4PLTEEA SN:FGL223911LK
    cn=C1111-4PLTEEA
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:C1111-4PLTEEA SN:FGL223911LK
  Validity Date:
    start date: 15:33:46 UTC Sep 27 2018
    end   date: 20:58:26 UTC Aug 9 2099
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

vEdge/vSmart 관련 문제

다음은 vEdge/vSmart에서 발생한 오류의 모습입니다 **show control connections-history** 명령 출력:

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                 LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
```

```
vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346    192.168.0.231
12346   biz-internet     challenge_resp  RXTRDWN    BIDNTVRFD  0     2019-06-01T16:40:16+0200
```

의 vBond에서 **show orchestrator connections-history** 명령 출력:

```
                                                                                                  PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                      REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE              LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0
192.168.10.234   12346   default          tear_down        BIDNTVRFD/NOERR     1     2019-06-
01T18:44:34+0200
```

또한 vBond의 디바이스 일련 번호가 유효한 vEdge 목록에 없습니다.

```
vbond1# show orchestrator valid-vedges | i 11OG528180107
```

컨트롤러 문제

컨트롤러 간 직렬 파일이 일치하지 않을 경우 vBond의 로컬 오류는 vSmarts/vManage에 대해 폐기된 인증서와 비교하여 없는 일련 번호입니다.

vBond에서:

```
                                                                                                  PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                      REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE              LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
0        unknown  dtls     -                0           0           ::               0
192.168.0.229    12346   default          tear_down        SERNTPRES/NOERR     2     2019-06-
01T19:04:51+0200

vbond1# show orchestrator valid-vsmarts

SERIAL
NUMBER  ORG
-----------------------
0A      SAMPLE - ORGNAME
0B      SAMPLE - ORGNAME
0C      SAMPLE - ORGNAME
0D      SAMPLE - ORGNAME
```

영향을 받는 vSmart/vManage에서:

```
                                                                                  PEER
PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                  LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
IP        PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------------------------
---
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346
192.168.0.231    12346   default          tear_down       CRTREJSER  NOERR      9     2019-06-
01T19:06:32+0200

vsmart# show control local-properties| i serial-num
serial-num                          0F
```

또한 vEdge와 관련하여 영향을 받는 vSmart에서 ORPTMO 메시지가 표시됩니다.

```
                                                                                    PEER
PEER
         PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
IP         PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
---
0        unknown  tls      -               0           0      ::               0
192.168.10.238   54850   default          tear_down       ORPTMO     NOERR      0     2019-06-
01T19:18:16+0200
0        unknown  tls      -               0           0      ::               0
192.168.10.238   54850   default          tear_down       ORPTMO     NOERR      0     2019-06-
01T19:18:16+0200
0        unknown  tls      -               0           0      ::               0
198.51.100.100   55374   default          tear_down       ORPTMO     NOERR      0     2019-06-
01T19:18:05+0200
0        unknown  tls      -               0           0      ::               0
198.51.100.100   59076   default          tear_down       ORPTMO     NOERR      0     2019-06-
01T19:18:03+0200
0        unknown  tls      -               0           0      ::               0
192.168.10.240   53478   default          tear_down       ORPTMO     NOERR      0     2019-06-
01T19:18:02+0200
```

vEdge에서 영향을 받는 vSmart, **show control connections-history** "SERNTPRES" 오류가 표시됩니다.

```
                                                                      PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
23456   biz-internet     tear_down       SERNTPRES  NOERR      29    2019-06-01T19:18:51+0200
vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456    192.168.0.229
23456   mpls             tear_down       SERNTPRES  NOERR      29    2019-06-01T19:18:32+0200
```

잘못된 섀시 번호/고유 Id

PnP 포털에서 잘못된 제품 ID(모델)가 사용되면 동일한 오류 "CRTREJSER/NOERR"의 또 다른 예를 볼 수 있습니다. 예를 들면 다음과 같습니다.

```
vbond# show orchestrator valid-vedges | include ASR1002
ASR1002-HX-DNA-JAE21050110            014EE30A                          valid     Cisco SVC N1
```

그러나 실제 디바이스 모델은 다릅니다("DNA" 후위 정보는 이름에 없습니다).

```
ASR1k#show sdwan control local-properties | include chassis-num
chassis-num/unique-id        ASR1002-HX-JAE21050110
```

조직 불일치(CTORGNMIS)

Organization Name(조직 이름)은 제어 연결을 시작하는 데 중요한 구성 요소입니다. 지정된 오버레이의 경우 제어 연결이 가동될 수 있도록 조직 이름이 모든 컨트롤러와 vEdge에서 일치해야 합니다 .

그렇지 않은 경우 다음과 같은 "Certificate Org. name mismatch" 오류가 발생합니다.

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vbond    dtls     -                0           0      203.0.113.197    12346    203.0.113.197
12346   biz-internet     tear_down       CTORGNMMIS NOERR      14    2019-04-08T00:26:19+0000
vbond    dtls     -                0           0      198.51.100.137   12346    198.51.100.137
12346   biz-internet     tear_down       CTORGNMMIS NOERR      13    2019-04-08T00:26:04+0000
```

vEdge/vSmart 인증서 취소/무효화(VSCRTREV/CRTVERFL)

컨트롤러에서 인증서가 해지되거나 vEdge 일련 번호가 무효화되는 경우 각각 vSmart 또는 vEdge Certification 해지 메시지가 표시됩니다.

다음은 vSmart 인증서 취소 메시지의 출력 예입니다. vSmart에서 해지된 인증서입니다.

```
                                                                      PEER
PEER
        PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
IP        PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
0        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346
192.168.0.231    12346   default          up              RXTRDWN    VSCRTREV   0     2019-06-
01T18:13:22+0200
1        vbond    dtls     0.0.0.0          0           0      192.168.0.231    12346
192.168.0.231    12346   default          up              RXTRDWN    VSCRTREV   0     2019-06-
01T18:13:22+0200
```

마찬가지로, 동일한 오버레이의 다른 vSmart에서는 인증서가 해지된 vSmart가 다음과 같이 표시됩니다.

```
                                                                      PEER
PEER
        PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                    LOCAL      REMOTE     REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC
```

```
IP        PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
---
0        vsmart   tls      10.10.10.229     1           1      192.168.0.229    23456
192.168.0.229    23456   default          tear_down       VSCRTREV   NOERR      0     2019-06-
01T18:13:24+0200
```

그리고 여기 vBond가 이것을 보는 방법이 있다:

```
                                                                                    PEER
PEER             PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
PEER             PUBLIC                                                  REPEAT
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
PUBLIC IP        PORT    REMOTE COLOR     STATE             LOCAL/REMOTE    COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
0        vsmart   dtls     10.10.10.229     1           1           192.168.0.229    12346
192.168.0.229    12346   default          tear_down         VSCRTREV/NOERR     0     2019-06-
01T18:13:14+0200
```

인증서 확인 실패는 설치된 루트 인증서로 인증서를 확인할 수 없는 경우입니다.

1. 시간을 **show clock** 명령을 실행합니다. 적어도 vBond 인증서 유효 범위 내에 있어야 합니다. **show orchestrator local-properties** 명령).

2. vEdge에서 루트 인증서가 손상되었기 때문에 발생할 수 있습니다.

그 다음 **show control connections-history** vEdge 라우터의 명령도 비슷한 출력을 보여 줍니다.

```
                                                                        PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER
PUBLIC                                  LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
---
vbond    dtls     -                0           0           203.0.113.82     12346
203.0.113.82     12346   default          tear_down       CRTVERFL   NOERR      32    2018-11-
16T23:58:22+0000
vbond    dtls     -                0           0           203.0.113.81     12346
203.0.113.81     12346   default          tear_down       CRTVERFL   NOERR      31    2018-11-
16T23:58:03+0000
```

이 경우 vEdge는 컨트롤러 인증서도 검증할 수 없습니다. 이 문제를 해결하려면 루트 인증서 체인을 다시 설치할 수 있습니다. Symantec Certificate Authority를 사용하는 경우 읽기 전용 파일 시스템에서 루트 인증서 체인을 복사할 수 있습니다.

```
vEdge1# vshell
vEdge1:~$ cp /rootfs ro/usr/share/viptela/root-ca-sha1-sha2.crt /home/admin/
vEdge1:~$ exit
exit
vEdge1# request root-cert-chain install /home/admin/root-ca-sha1-sha2.crt
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root-ca-sha1-sha2.crt via VPN 0
```

```
Installing the new root certificate chain
Successfully installed the root certificate chain
```

vEdge 템플릿이 vManage에 연결되지 않음

디바이스가 vManage의 템플릿과 연결되어 있지 않은 경우 디바이스가 가동될 때 **NOVMCFG - No Config in vManage for device** 메시지가 표시됩니다.

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                 LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT D                OWNTIME
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------- ---------
----------
vmanage  dtls     10.0.1.1          1           0      10.0.2.80        12546    203.0.113.128
12546   default          up              RXTRDWN    NOVMCFG    35    2               019-02-
26T12:23:52+0000
```

과도 상태(DISCVBD, SYSIPCHNG)

다음은 제어 연결이 플랩하는 몇 가지 일시적인 조건입니다. 여기에는 다음이 포함됩니다.

- vEdge에서 System-IP가 변경되었습니다.
- vBond에 대한 해제 메시지입니다(vBond에 대한 제어 연결은 일시적입니다).

```
                                                                    PEER
PEER
PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER
PUBLIC                                 LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP
PORT    LOCAL COLOR      STATE           ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
vmanage  dtls     10.0.0.1         1           0      198.51.100.92   12646     198.51.100.92
12646   default          tear_down       SYSIPCHNG  NOERR      0     2018-11-02T16:58:00+0000
```

DNS 실패

에 연결 시도가 표시되지 않는 경우 **show control connection-history** 명령을 사용하면 다음 단계를 통해 vBond에 대한 DNS 확인 실패를 확인할 수 있습니다.

- vBond의 DNS 주소로 ping합니다.

```
ping vbond-dns-name.cisco.com
ping vbond-dns-name.cisco.com: Temporary failure in name resolution
```

- 소스 인터페이스에서 Google DNS(8.8.8.8)에 Ping을 수행하여 인터넷 연결 가능성을 확인합니다.

```
ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

- 송신 및 수신된 DNS 트래픽을 확인하기 위해 포트 53의 DNS 트래픽용 임베디드 패킷 캡처.

```
monitor capture mycap interface <interface that forms control>
monitor capture mycap match ipv4 <source IP> <vBond IP>
```

참조 문서: 임베디드 패킷 캡처.

모니터 캡처를 시작하고 2분 정도 실행한 다음 캡처를 중지합니다. 패킷 캡처를 검사하여 DNS 쿼리가 전송 및 수신되는지 확인합니다.

관련 정보

- cEdge에서 제어 연결을 형성하기 위한 기본 매개변수 구성
- 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.