Fehlerbehebung bei SD-WAN-Steuerverbindungen

Inhalt

Einleitung

In diesem Dokument werden einige der wahrscheinlichen Ursachen beschrieben, die zu einem Problem mit Steuerverbindungen führen, und es wird beschrieben, wie diese behoben werden können.

Hintergrundinformationen

> **Hinweis**: Die meisten der in diesem Dokument dargestellten Befehlsausgaben stammen von vEdge-Routern. Der gleiche Ansatz wird jedoch für Router verwendet, auf denen die Cisco IOS®^{XE} SD-WAN-Software ausgeführt wird. Geben Sie **sdwan** um die gleichen Ergebnisse für die Cisco IOS XE SD-WAN-Software zu erzielen. Beispiele, **show sdwan control connections** statt **show control connections** .

Bevor Sie die Fehlerbehebung durchführen, stellen Sie sicher, dass der betreffende WAN-Edge ordnungsgemäß konfiguriert wurde.

Sie umfasst:

- Ein gültiges Zertifikat, das installiert ist.
- Diese Konfigurationen werden im Rahmen des **system** Block:
  - System-IP

    - Standort-ID
    - Unternehmensname
    - vBond-Adresse
- VPN 0-Transportschnittstelle, die mit der Tunneloption und der IP-Adresse konfiguriert wird.
- Die Systemuhr, die auf dem vEdge richtig konfiguriert ist, sowie die Systemuhr, die mit anderen Geräten/Controllern übereinstimmt:

Die Fehlermeldung **show clock** bestätigt die aktuelle eingestellte Zeit.

Geben Sie **clock set** , um die richtige Uhrzeit auf dem Gerät einzustellen.

Stellen Sie in allen oben genannten Fällen sicher, dass Transport Locator (TLOC) aktiv ist. Überprüfen Sie dies mit dem **show control local-properties** aus.

Ein Beispiel für eine gültige Ausgabe finden Sie hier:

```
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
```

In vEdge-Softwareversion 16.3 und höher enthält die Ausgabe einige zusätzliche Felder:

```
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
```

Problemszenarien

Fehler bei DTLS-Verbindung (DCONFAIL)

Dies ist eines der häufigen Probleme bei der Steuerkonnektivität, das nicht auftritt. Mögliche Ursachen sind eine Firewall oder andere Verbindungsprobleme.

Möglicherweise werden einige oder alle Pakete irgendwo verworfen/gefiltert. Das Beispiel mit den größeren wird in**tcpdump** Ergebnisse hier.

- Der Next Hop (NH)-Router ist nicht erreichbar.
- Das Standard-Gateway ist nicht in der Routing Information Base (RIB) installiert.
- Der DTLS-Port (Datagram Transport Layer Security) ist auf den Controllern nicht geöffnet.

Die folgenden Befehle können verwendet werden:

```
#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 <...>
```

Wenn eine DTLS-Verbindung ausfällt, wird sie im **show control connections-history** Befehlsausgabe.

```
                                                                                                  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
```

Dies ist der Fall, wenn große Pakete bei Verwendung von vEdge nicht erreicht werden. **tcpdump** beispielsweise auf der SD-WAN-Seite (vSmart):

```
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
```

Ein Beispiel für die vEdge-Seite ist hier dargestellt:

```
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
```

> **Hinweis**: In der Cisco IOS XE SD-WAN-Software können Sie Embedded Packet Capture (EPC) statt **tcpdump**.

Sie können **traceroute** Oder **nping** um Datenverkehr mit verschiedenen Paketgrößen und DSCP-Markierungen (Differentiated Services Code Point) zu generieren, um die Konnektivität zu überprüfen, da Ihr Service Provider Probleme bei der Bereitstellung größerer UDP-Pakete, fragmentierter UDP-Pakete (insbesondere kleiner UDP-Fragmente) oder DSCP-markierter Pakete haben kann. Hier ein Beispiel für **nping** wenn die Verbindung erfolgreich hergestellt wurde.

Von vSmart:

```
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
```

Ein Beispiel von vEdge wird hier angezeigt:

```
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
```

Und hier ist ein Beispiel für eine erfolglose Verbindung mit dem **traceroute** Befehl (der über vShell ausgeführt wird) in vSmart:

```
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 * * *
```

vEdge empfängt keine von vSmart gesendeten Pakete (nur einige andere Datenpakete oder Fragmente):

```
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 deaktiviert (DISTLOC)

Auslöser für TLOC Deaktivierte Meldungen können folgende wahrscheinliche Ursachen haben:

- Entfernen Sie die Steuerelementverbindungen.
- Ändern Sie die Farbe für TLOC.
- Änderung der System-IP.

Änderung einer der im Systemblock oder in den Tunneleigenschaften im**show control connections-history**Befehlsausgabe.

```
                                                                                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
```

Board-ID nicht initialisiert (BIDNTPR)

In einem sehr instabilen Netzwerk, in dem Netzwerkverbindungen ständig abflattern, sehen Sie TXCHTOBD - failed to send a challenge to Board ID failed und/oder RDSIGFBD - Read Signature from Board ID failed. Manchmal kann es auch aufgrund von Sperrproblemen vorkommen, dass eine Anfrage an board-id fehlschlägt und dann die board-ID zurückgesetzt wird und es dann erneut versucht wird. Es kommt nicht oft vor, und es verzögert die Form von Steuerverbindungen. Dies wurde in späteren Versionen behoben.

```
                                                                                    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 - Signaturfehler bei Motherboard-ID

Dies zeigt an, dass die vEdge-Gehäusenummer/eindeutige ID/Seriennummer vom vBond abgelehnt wurde. Bestätigen Sie in diesem Fall die vEdge-Informationen im **show control local-properties** Befehlsausgabe und vergleichen Sie diese Ausgabe mit **show orchestrator valid-vedges** auf der vBond-Website.

Wenn kein Eintrag für vEdge vorhanden ist, stellen Sie Folgendes sicher:

- vEdge dem Smart Account hinzugefügt.
- Datei richtig in vManage hochgeladen.

Klicken Sie auf **Send to Controllers** unter **Configuration > Certificates**.

Wenn es vorhanden ist, überprüfen Sie, ob doppelte Einträge in der gültigen vEdge-Tabelle vorhanden sind, und wenden Sie sich an das Cisco Technical Assistance Center (TAC), um eine weitere Fehlerbehebung durchzuführen.

In Verbindung bleiben: Routing-Probleme

Bei Routing-Problemen im Netzwerk werden keine Steuerverbindungen angezeigt. Stellen Sie sicher, dass in der RIB eine gültige Route mit dem richtigen NH/TLOC vorhanden ist.

Beispiele:

- Eine spezifischere Route zu vBond in der RIB verweist auf ein NH/TLOC, das nicht für die Herstellung von Steuerverbindungen verwendet wird.
- Die TLOC-IP-Adresse wird vom Upstream-Service-Provider weitergeleitet, was zu falschem Routing führt.

Geben Sie folgende Befehle zur Überprüfung ein:

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

Suchen Sie nach dem Abstandswert und dem Protokoll für das IP-Präfix.

vEdge versucht, eine Kontrollverbindung ohne Erfolg herzustellen, oder Verbindungen zu Controllern flattern weiter.

Überprüfen Sie mit dem **show control connections** und/oder **show sdwan control connections-history** -Befehlen.

```
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
```

Socket-Fehler (LISFD)

Wenn im Netzwerk eine doppelte IP vorhanden ist, werden keine Steuerverbindungen hergestellt. Sie sehen die LISFD - Listener Socket FD Error Nachricht. Dies kann auch aus anderen Gründen der Fall sein, z. B. Paketbeschädigung, RESET, eine Diskrepanz zwischen vEdge und Controllern auf TLS- und DTLS-Ports, wenn die FW-Ports nicht offen sind usw.

Die häufigste Ursache ist eine doppelte Transport-IP. Überprüfen Sie die Verbindung, und stellen Sie sicher, dass die Adressen eindeutig sind.

```
                                                                        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
```

Peer-Timeout (VM_TMO)

Eine Peer-Timeout-Bedingung wird ausgelöst, wenn die Erreichbarkeit eines vEdge für den betreffenden Controller verloren geht.

In diesem Beispiel wird ein**vManage Timeout msg (peer VM_TMO)**. Andere schließen Peer-vBond-, vSmart- und/oder vEdge-Timeouts ein (**VB_TMO, VP_TMO, VS_TMO**).

Stellen Sie bei der Fehlerbehebung sicher, dass eine Verbindung zum Controller besteht. Internet Control Message Protocol (ICMP) verwenden und/oder **traceroute** an die betreffende IP-Adresse. Fälle, in denen der Datenverkehr häufig verloren geht (Verluste sind hoch). Schnell **ping** und sicherzustellen, dass sie gut ist.

```
                                                                                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
```

Überprüfen Sie außerdem die **show control connections-history detail** -Befehlsausgabe, um die TX/RX-Steuerungsstatistik zu überprüfen und festzustellen, ob eine signifikante Abweichung in den Zählern vorliegt. Beachten Sie in der Ausgabe den Unterschied zwischen RX- und TX-Hello-Paketnummern.

```
-------------------------------------------------------------------------------------------
 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
```

Seriennummer(n) nicht vorhanden (CRTREJSER, BIDNTVRFD)

Wenn die Seriennummer auf den Controllern für ein Gerät nicht vorhanden ist, schlagen die Steuerverbindungen fehl.

Verifizierung mit **show controllers [valid-vsmarts | valid-vedges]** und die meiste Zeit fixiert. Navigieren Sie zu **Configuration > Certificates > Send to Controllers or Send to vBond** -Schaltflächen auf den Registerkarten vManage. Bei vBond prüfen **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts.**

In den Protokollen von vBond werden diese Meldungen mit Gründen angezeigt 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"
```

Wenn Sie ein solches Problem beheben, stellen Sie sicher, dass die richtige Seriennummer und das richtige Gerätemodell im PnP-Portal (software.cisco.com) und in vManage konfiguriert und bereitgestellt wurden.

Um die Gehäusenummer und die Seriennummer des Zertifikats zu überprüfen, kann dieser Befehl auf vEdge-Routern verwendet werden:

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

Geben Sie auf einem Router, auf dem die Cisco IOS XE SD-WAN-Software ausgeführt wird, den folgenden Befehl ein:

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

Oder dieser Befehl:

```
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
```

Bei Problemen mit vEdge/vSmart

So sieht der Fehler in vEdge/vSmart im **show control connections-history** Befehlsausgabe:

```
                                                                    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
```

Über vBond im **show orchestrator connections-history** Befehlsausgabe:

```
                                                                                  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
```

Außerdem befindet sich die Seriennummer des Geräts auf vBond nicht in der Liste der gültigen vEdges:

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

Bei Problemen mit Controllern

Wenn die serielle Datei zwischen den Controllern selbst nicht übereinstimmt, ist der lokale Fehler bei vBond die Seriennummer, die nicht vorhanden ist, und das für vSmarts/vManage widerrufene Zertifikat.

Bei vBond:

```
                                                                                  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
```

Bei betroffenem vSmart/vManage:

```
                                                                                  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
```

Außerdem werden auf dem betroffenen vSmart ORPTMO-Meldungen in Bezug auf vEdge angezeigt:

```
                                                                                  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
```

Bei vEdge betroffene vSmart im **show control connections-history** Ausgabe wird der Fehler "SERNTPRES" angezeigt:

```
                                                                                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
```

Falsche Chassis-Num/eindeutige ID

Ein weiteres Beispiel für den gleichen Fehler "CRTREJSER/NOERR" ist erkennbar, wenn im PnP-Portal die falsche Produkt-ID (Modell) verwendet wird. Beispiele:

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

Das tatsächliche Gerätemodell ist jedoch anders (beachten Sie, dass "DNA"-Postfix nicht im Namen enthalten ist):

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

Organisationskonflikt (CTORGNMMIS)

Der Name der Organisation ist eine wichtige Komponente für das Aufrufen der Steuerverbindung. Für ein bestimmtes Overlay muss der Organisationsname über alle Controller und vEdges hinweg übereinstimmen, damit Steuerverbindungen verfügbar sind.

Wenn nicht, wird der Fehler "Certificate Org. name mismatch" angezeigt:

```
                                                                                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-Zertifikat widerrufen/ungültig (VSCRTREV/CRTVERFL)

In Fällen, in denen das Zertifikat auf Controllern widerrufen wird oder die vEdge-Seriennummer ungültig ist, wird eine Meldung angezeigt, die die vSmart- bzw. vEdge-Zertifizierung widerruft.

Hier sehen Sie ein Beispiel für die Ausgabe von vSmart Certificate-Widerrufsmeldungen. Dies ist das Zertifikat, das für vSmart:

```
                                                                                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
```

Auf einem anderen vSmart im gleichen Overlay erkennt er auf diese Weise den vSmart, dessen Zertifikat widerrufen wird:

```
                                                                              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
```

Und so sieht vBond das:

```
                                                                                    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
```

Fehler bei der Zertifizierungsprüfung, wenn das Zertifikat nicht mit installiertem Stammzertifikat überprüft werden kann:

1. Überprüfen Sie die Uhrzeit mit dem **show clock** aus. Sie muss sich mindestens im Gültigkeitsbereich des vBond-Zertifikats befinden (weitere Informationen hierzu finden Sie im **show orchestrator local-properties** Befehl).

2. Dies kann durch eine Beschädigung des Stammzertifikats in vEdge verursacht werden.

dann **show control connections-history** zeigt auf dem vEdge-Router eine ähnliche Ausgabe an:

```
                                                                                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
```

In diesem Fall kann vEdge das Controller-Zertifikat nicht ebenfalls validieren. Um dieses Problem zu beheben, können Sie die Stammzertifikatkette neu installieren. Falls die Symantec Certificate Authority verwendet wird, können Sie die Root-Zertifikatskette aus dem schreibgeschützten Dateisystem kopieren:

```
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-Vorlage in vManage nicht angehängt

Wenn das Gerät nicht mit einer Vorlage in vManage verknüpft ist, wird beim Hochfahren des Geräts **NOVMCFG - No Config in vManage for device** wird angezeigt.

```
                                                                  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
```

Übergangsbedingungen (DISCVBD, SYSIPCHNG)

Hier sind einige transiente Bedingungen, bei denen die Steueranschlüsse klappen. Dazu gehören:

- System-IP auf dem vEdge geändert.
- Abreißmeldung an vBond (Kontrollverbindung zu vBond ist vorübergehend).

```
                                                                                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-Fehler

Wenn keine Verbindungsversuche im **show control connection-history** können Sie mit den folgenden Schritten prüfen, ob die DNS-Auflösung bei vBond fehlschlägt:

- Pingen Sie an die DNS-Adresse von vBond.

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

- Pingen Sie Google DNS (8.8.8.8) von der Quellschnittstelle, um die Erreichbarkeit des Internets zu überprüfen.

```
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:
```

- Integrierte Paketerfassung für DNS-Datenverkehr an Port 53 zur Überprüfung auf gesendeten und empfangenen DNS-Datenverkehr

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

Referenzdokument: Integrierte Paketerfassung.

Starten Sie die Monitoraufnahme, lassen Sie sie einige Minuten laufen, und stoppen Sie dann die Erfassung. Untersuchen Sie die Paketerfassung, um festzustellen, ob DNS-Abfragen gesendet und empfangen wurden.

Zugehörige Informationen

- Konfigurieren von Grundparametern zur Bildung von Steuerelementverbindungen auf cEdge
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.