排除SD-WAN控制连接故障

目录

简介

本文档介绍导致控制连接出现问题的某些可能原因，以及如何排除这些原因的故障。

背景信息

> **注意**：本文档中介绍的大多数命令输出来自vEdge路由器。但是，运行Cisco IOS® XE SD-WAN软件的路由器采用相同的方法。输入 **sdwan** 关键字，以便在Cisco IOS XE SD-WAN软件上获得相同的输出。例如， **show sdwan control connections** 而非 **show control connections** .

在进行故障排除之前，请确保有问题的WAN Edge已正确配置。

此命令包括：

- 已安装的有效证书。
- 这些配置位于 **system** 阻止:
  - 系统IP
  - 站点ID
  - 组织名称
  - vBond address
- 使用Tunnel选项和IP地址配置的VPN 0传输接口。
- 在vEdge上正确配置的系统时钟以及与其他设备/控制器匹配的系统时钟：

此 **show clock** 命令可确认当前时间设置。

输入 **clock set** 命令，以便设置设备上的正确时间。

对于前面提到的所有情况，请确保传输定位器(TLOC)已启用。请通过 **show control local-properties** 命令。

有效输出的示例如下所示：

```
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
```

在vEdge软件版本16.3及更高版本中，输出还有几个附加字段：

```
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
```

问题场景

DTLS连接故障(DCONFAIL)

这是控制连接的常见问题之一，但无法实现。可能的原因包括防火墙或某些其他连接问题。

有可能是某些或所有数据包在某个位置被丢弃/过滤。对于较大的示例，请参阅**tcpdump** 结果在这里

。

- 下一跳(NH)路由器无法到达。
- 路由信息库(RIB)中未安装默认网关。
- 控制器中的数据报传输层安全(DTLS)端口未打开。

可以使用以下show命令：

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

当发生DTLS连接故障时，您可以在中看到它 **show control connections-history** 命令输出.

```
                                                                                                    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
```

当您使用时，如果大数据包无法到达vEdge，就会发生这种情况 **tcpdump** 例如，在SD-WAN(vSmart)端：

```
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端的示例如下所示：

```
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
```

注意：在Cisco IOS XE SD-WAN软件上，您可以使用嵌入式数据包捕获(EPC)而不是 **tcpdump**.

您只能使用 **traceroute** 或 **nping** 因为您的服务提供商可能遇到传送较大的UDP数据包、分段的UDP数据包（尤其是UDP小分段）或DSCP标记的数据包的问题，所以为了检查连接而生成具有不同数据包大小和差分服务代码点(DSCP)标记的流量。以下是一个示例 **nping** 连接成功时。

从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
```

vEdge的示例如下所示：

```
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
```

以下示例显示了与 **traceroute** 命令（从vShell运行）在vSmart上：

```
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不接收从vSmart发送的数据包（仅接收某些其他流量或分段）：

```
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禁用(DISTLOC)

对TLOC Disabled消息的触发器可能由以下原因引起：

- 清除控制连接。
- 更改TLOC上的颜色。
- 更改系统IP。

更改系统块或中隧道属性中提及的任何配置**show control connections-history**命令输出.

```
                                                                                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 not Initialized(BIDNTPR)

在高度不稳定的网络中，网络连接不断摆动，您可以看到 TXCHTOBD - failed to send a challenge to Board ID failed 和/或 RDSIGFBD - Read Signature from Board ID failed.此外，有时由于锁定问题，发送到board-id的质询失败，当发生这种情况时，重置board-ID并重试。这种情况不经常发生，而且会延迟控制连接的形式。这在后续版本中是固定的。

```
                                                                        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 — 主板ID签名失败

这表示vEdge拒绝了vBond的机箱编号/唯一id/序列号。发生这种情况时，请确认 **show control local-properties** 命令输出，并将该输出与 **show orchestrator valid-vedges** 在vBond上。

如果vEdge的条目不存在，请确保您具有：

- 已将vEdge添加到智能帐户。
- 已将该文件正确上传到vManage。

点击 **Send to Controllers** 在 **Configuration > Certificates**.

如果存在，请检查valid-vEdge表中的重复条目，并与Cisco技术支持中心(TAC)联系，进一步排除此故障

卡在“Connect”中：路由问题

如果网络中存在路由问题，则不会出现控制连接。 确保RIB中具有正确的NH/TLOC的有效路由。

示例包括：

- 在RIB中指向vBond的更具体的路由指向不用于建立控制连接的NH/TLOC。
- TLOC IP在上游服务提供商之间泄漏，从而导致路由不正确。

输入以下命令进行验证：

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

查找IP前缀的距离值和协议。

vEdge尝试建立控制连接失败，或者与控制器的连接不断抖动。

使用 **show control connections** 和/或 **show sdwan control connections-history** 命令。

```
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
```

套接字错误(LISFD)

如果网络中存在重复的IP，则控制连接不会出现。您会看到 LISFD - Listener Socket FD Error 邮件.这也可能出于其他原因，例如数据包损坏、RESET、vEdge与TLS和DTLS端口上的控制器之间的不匹配（如果FW端口未打开）等等。

最常见的原因是传输IP重复。检查连通性并确保地址唯一。

```
                                                                                  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
```

对等体超时问题(VM_TMO)

当vEdge无法与有问题的控制器连接时，会触发对等超时条件。

在本例中，它捕获了**vManage Timeout msg (peer VM_TMO)**. 其他包括对等体vBond、vSmart和/或vEdge超时(**VB_TMO, VP_TMO, VS_TMO**影响。

作为故障排除的一部分，请确保您已连接到控制器。使用互联网控制消息协议(ICMP)和/或 **traceroute** 到有问题的IP地址。存在大量流量丢弃的情况（丢失率较高）。迅速 **ping** 并确保它是良好的。

```
                                                                                  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
```

此外，请查看 **show control connections-history detail** 命令输出，以查看TX/RX控制统计信息，查看计数器中是否存在任何重大差异。注意输出中RX和TX hello数据包编号之间的差异。

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

```
 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
```

序列号不存在(CRTREJSER、BIDNTVRFD)

如果给定设备的控制器上不存在序列号，则控制连接失败。

可以通过验证 **show controllers [valid-vsmarts | valid-vedges]** 输出并修复大部分时间。导航至 **Configuration > Certificates > Send to Controllers or Send to vBond** vManage选项卡中的按钮。在vBond上，选中 **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts**.

在vBond的日志中，您观察这些消息是有原因的 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"
```

解决此类问题时，请确保在PnP门户(software.cisco.com)和vManage上配置和调配了正确的序列号和设备型号。

为了检查机箱编号和证书序列号，可以在vEdge路由器上使用此命令：

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

在运行Cisco IOS XE SD-WAN软件的路由器上，输入以下命令：

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

或此命令：

```
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
```

有关vEdge/vSmart的问题

以下是vEdge/vSmart错误在 **show control connections-history** 命令输出:

```
                                                                                  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
```

在vBond中 **show orchestrator connections-history** 命令输出:

```
                                                                                        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
```

此外，vBond上的设备序列号不在有效的vEdge列表中：

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

有关控制器的问题

如果控制器之间的串行文件本身不匹配，vBond上的本地错误是不存在与vSmarts/vManage的证书已撤销的序列号。

在vBond上：

```
                                                                                    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
```

在受影响的vSmart/vManage上：

```
                                                                          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
```

此外，您会在受影响的vSmart上看到有关vEdge的ORPTMO消息：

```
                                                                          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
```

在受vEdge影响的vSmart上，在 **show control connections-history** 输出显示“SERNTPRES”错误：

```
                                                                                  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
```

错误的Chassis-Num/Unique-Id

如果在PnP门户上使用错误的产品ID（型号），则也可以看到同一错误“CRTREJSER/NOERR”的另一个示例。例如：

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

但是，实际设备型号不同（请注意，“DNA”后缀不在名称中）：

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

组织不匹配(CTORGNMIS)

组织名称是启用控制连接的重要组件。对于给定的重叠，组织名称必须在所有控制器和vEdge之间匹配，以便控制连接可以启动。

如果不是，则出现“证书组织名称不匹配”错误，如下所示：

```
                                                                                  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证书已撤销/无效(VSCRTREV/CRTVERFL)

如果证书在控制器上被撤销，或vEdge序列号被无效，则会分别显示vSmart或vEdge认证撤销消息。

以下是vSmart证书撤销消息的示例输出。这是在vSmart上撤销的证书：

```
                                                                    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
```

同样，在同一重叠中的另一个vSmart上，这是它查看证书被撤销的vSmart的方式：

```
                                                                  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
```

下面是vBond如何看待这一点：

```
                                                                                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
```

证书验证失败是指无法通过安装根证书来验证证书：

1.使用 **show clock** 命令。它必须至少在vBond证书有效范围内(请查看 **show orchestrator local-properties** 命令)。

2.这可能是由于vEdge上的根证书损坏导致的。

然后 **show control connections-history** 命令显示类似的输出：

```
                                                                                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
```

在这种情况下，vEdge无法同时验证控制器证书。要解决此问题，您可以重新安装根证书链。如果使用Symantec Certificate Authority，您可以从只读文件系统复制根证书链：

```
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
```

vManage中未附加vEdge模板

当启动设备时，如果设备未在vManage上附加模板， **NOVMCFG - No Config in vManage for device** 将显示消息。

```
                                                                    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
```

瞬态条件(DISCVBD、SYSIPCHNG)

以下是一些瞬变情况，其中控制连接摆动。此类设备包括：

- vEdge上的系统IP已更改。
- 到vBond的拆解消息（到vBond的控制连接是临时的）。

```
                                                                    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故障

当在PC上 **show control connection-history** 命令，您可以通过以下步骤检查vBond的DNS解析故障：

- 对vBond的DNS地址执行ping操作。

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

- 从源接口Ping Google DNS(8.8.8.8)，以验证Internet可达性。

```
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:
```

- 端口53上的DNS流量的嵌入式数据包捕获，用于检查已发送和已接收的DNS流量。

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

参考文档：嵌入式数据包捕获。

启动监控器捕获，让它运行几分钟，然后停止捕获。继续检查数据包捕获，查看是否发送和接收DNS查询。

相关信息

- 配置基本参数以在cEdge上形成控制连接
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。