排除SD-WAN控制連線故障

目錄

簡介

本文說明導致控制連線出現問題的某些可能原因，以及如何排除這些原因。

背景資訊

> **註**：本文檔中顯示的命令輸出大多來自vEdge路由器。但是執行Cisco IOS® XE SD-WAN軟體的路由器也使用相同的方法。輸入 **sdwan** 關鍵字：在Cisco IOS XE SD-WAN軟體上取得相同的輸出。例如， **show sdwan control connections** 而不是 **show control connections** .

在排除故障之前，請確保有問題的WAN邊緣已正確配置。

它包括：

- 已安裝的有效證書。
- 這些配置位於 **system** 封鎖:
  - System-IP
  - Site-ID
  - Organization-Name
  - vBond地址
- 使用Tunnel選項和IP地址配置的VPN 0傳輸介面。
- 在vEdge上正確配置的系統時鐘以及與其他裝置/控制器匹配的系統時鐘：

其 **show clock** 命令確認當前時間設定。

輸入 **clock set** 命令設定裝置上的正確時間。

對於前面提到的所有情況，請確保傳輸定位器(TLOC)已啟動。請通過 **show control local-properties** 指令。

有效輸出的示例如下所示：

```
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軟體版本16.3和更新版本中，輸出包含幾個額外欄位：

```
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
```

問題情景

DTLS連線失敗(DCONFAIL)

這是控制連線不常出現的常見問題之一。可能的原因包括防火牆或其他一些連線問題。

有可能部分或全部資料包在某個位置被丟棄/過濾。較大的例子在文中給出**tcpdump** 結果在這裡。

- 無法訪問下一跳(NH)路由器。
- 路由資訊庫(RIB)中未安裝預設閘道。
- 控制器中的資料包傳輸層安全(DTLS)連線埠未開啟。

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 <...>
```

DTLS連線失敗時，可在 **show control connections-history** 命令輸出。

```
                                                                                                    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
```

這就是使用時大資料包無法到達vEdge時會發生的情況 **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
```

註：在Cisco IOS XE SD-WAN軟體上，您可以使用嵌入式資料包捕獲(EPC)而不是 **tcpdump**.

您可以使用 **traceroute** 或 **nping** 因為您的服務提供商可能會在傳送較大的UDP資料包、分段的UDP資料包（尤其是UDP小片段）或DSCP標籤的資料包時遇到問題，因此也可能會使用實用程式生成具有不同資料包大小和差分服務代碼點(DSCP)標籤的流量，以檢查連通性。以下是使用 **nping** 連線成功時。

在vSmart上：

```
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
```

以下是與 **traceroute** vSmart上的命令（從vShell運行）：

```
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不會接收從vSmart傳送的封包（只有某些其他流量或片段）：

```
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
```

已停用TLOC(DISTLOC)

觸發TLOC Disabled消息的可能是由於以下原因：

- 清除控制連線。
- 更改TLOC上的顏色。
- 更改系統IP。

更改系統塊或中隧道屬性中提及的任何配置**show control connections-history**命令輸出。

```
                                                                        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
```

未初始化Board-ID(BIDNTPR)

在高度不穩定的網路中，網路連線不斷擺動，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，有時由於鎖定問題，傳送到board-id的質詢失敗，當發生這種情況時，重置board-ID並重試。這種情況不經常發生，並且會延遲控制連線的形式。在更高的版本中修復了此問題。

```
                                                                          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 — 主機板ID簽名失敗

這表示vEdge chassis-num/unique-id/serial number被vBond拒絕。發生這種情況時，請確認 **show control local-properties** 命令輸出並將輸出與 **show orchestrator valid-vedges** 在vBond。

如果vEdge的條目不存在，請確保您具有：

- 已將vEdge新增到智慧帳戶。
- 已正確將該檔案上載到vManage。

按一下 **Send to Controllers** 在 **Configuration > Certificates**.

如果存在，請檢查valid-vEdge表中的重複條目，並聯絡Cisco技術支援中心(TAC)進行進一步的故障排除

停滯在「連線」中：路由問題

如果網路中出現路由問題，則不會出現控制連線。 確保RIB中有具有正確NH/TLOC的有效路由。

示例包括：

- 在RIB中到vBond的更具體的路由指向不用於建立控制連線的NH/TLOC。
- TLOC IP在上游服務提供商之間洩漏，從而導致路由不正確。

輸入以下命令進行驗證：

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

尋找IP首碼的距離值和通訊協定。

vEdge嘗試建立無成功的控制連線，或者與控制器的連線不斷抖動。

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

```
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
```

插座錯誤(LISFD)

如果網路中存在重複的IP，則控制連線不會啟動。您會看到 LISFD - Listener Socket FD Error 消息。這也可能是由於其他原因造成的，例如資料包損壞、重置、vEdge與TLS埠上的控制器與DTLS埠之間的不匹配（如果FW埠未開啟）等等。

最常見的原因是傳輸IP重複。檢查連通性並確保地址唯一。

```
                                                                                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
```

對等體超時問題(VM_TMO)

當vEdge無法連線到相關控制器時，會觸發對等超時條件。

在本範例中，它擷取**vManage Timeout msg (peer VM_TMO)**. 其他包括對等體vBond、vSmart和/或vEdge超時(**VB_TMO, VP_TMO, VS_TMO**)。

進行疑難排解時，請確保您已連線至控制器。使用網際網路控制訊息通訊協定(ICMP)和/或 **traceroute** 到相關IP地址。存在大量流量丟棄的情況（丟失率高）。快速 **ping** 確保它是良好的。

```
                                                                                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，請檢查 **show control connections-history detail** 命令輸出，以檢視TX/RX控制統計資訊，檢視計數器是否有任何明顯差異。請注意，在輸出中，RX和TX hello資料包編號之間的差異。

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

序列號不存在(CRTREJSER、BIDNTVRFD)

如果給定裝置的控制器上沒有序列號，則控制連線會失敗。

可以使用驗證 **show controllers [valid-vsmarts | valid-vedges]** 輸出並修復大部分時間。導航至 **Configuration > Certificates > Send to Controllers or Send to vBond** vManage頁籤中的按鈕。在vBond上，檢查 **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts.**

在vBond的日誌中，您觀察這些消息是有原因的 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"
```

解決此類問題時，請確保在PnP門戶(software.cisco.com)和vManage上配置並調配了正確的序列號和裝置型號。

為了檢查機箱號和證書序列號，可以在vEdge路由器上使用以下命令：

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

在執行Cisco IOS XE SD-WAN軟體的路由器上，輸入以下命令：

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

或以下命令：

```
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
```

針對vEdge/vSmart的問題

以下是vEdge/vSmart **show control connections-history** 命令輸出：

```
                                                                    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
```

關於vBond **show orchestrator connections-history** 命令輸出：

```
                                                                                  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上的裝置序列號不在有效vEdge的清單中：

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

控制器問題

如果控制器之間的串列檔案本身不匹配，vBond上的本地錯誤是vSmarts/vManage的證書被吊銷的序列號不存在。

在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
```

在受影響的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，您還會在受影響的vSmart上看到有關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vEdge受影響的vSmart上，在 **show control connections-history** 輸出出現「SERNTPRES」錯誤：

```
                                                                        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
```

Wrong Chassis-Num/Unique-Id

如果在PnP門戶上使用了錯誤的產品ID（型號），則也可以看到相同錯誤「CRTREJSER/NOERR」的另一個示例。例如：

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

然而，真正的裝置型號不同（請注意，「DNA」字尾不在名稱中）：

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

組織不匹配(CTORGNMIS)

組織名稱是啟用控制連線的重要元件。對於給定的覆蓋，「組織」名稱必須在所有控制器和vEdge之間匹配，以便控制連線可以啟動。

如果不匹配，則出現「Certificate Org. name mismatch」錯誤，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證書已吊銷/失效(VSCRTREV/CRTVERFL)

如果證書在控制器上被吊銷，或vEdge序列號被無效，則會分別顯示vSmart或vEdge認證吊銷消息。

以下是vSmart證書撤銷消息的輸出示例。這是在vSmart上吊銷的證書：

```
                                                                                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
```

同樣，在同一重疊中的另一個vSmart上，這是它檢視證書被吊銷的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如何看待這一點的：

```
                                                                                    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
```

證書驗證失敗是因為無法在安裝了根證書的情況下驗證證書：

1.檢查時間是否符合 **show clock** 指令。它必須至少在vBond證書有效範圍內(請檢視 **show orchestrator local-properties** 指令)。

2.這可能是由於vEdge上的根憑證損毀。

然後 **show control connections-history** vEdge路由器上的命令會顯示類似的輸出：

```
                                                                                    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
```

在這種情況下，vEdge無法同時驗證控制器憑證。若要解決此問題，您可以重新安裝根憑證鏈結。在使用Symantec Certificate Authority的情況下，可以從只讀檔案系統複製根證書鏈：

```
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

當啟動裝置時（如果裝置未附加vManage上的模板），將 **NOVMCFG - No Config in vManage for device** 將顯示消息。

```
                                                                          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
```

瞬態條件(DISCVBD、SYSIPCHNG)

以下是一些控制連線擺動的瞬態條件。它們包括：

- vEdge上的系統IP已更改。
- 到vBond的拆解消息（到vBond的控制連線是暫時的）。

```
                                                                                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

當在 **show control connection-history** 命令，您可以透過以下步驟檢查vBond的DNS解析失敗：

- 對vBond的DNS地址執行ping操作。

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

- 從源介面ping Google DNS(8.8.8.8)，以驗證Internet的可達性。

```
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:
```

- 針對埠53上的DNS流量的嵌入式資料包捕獲，用於檢查已傳送和已接收的DNS流量。

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

參考文檔：嵌入式資料包捕獲。

啟動監視器捕獲，讓它運行幾分鐘，然後停止捕獲。繼續檢查資料包捕獲，檢視是否傳送和接收DNS查詢。

相關資訊

- 配置基本引數以在cEdge上形成控制連線
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。