Solucionar problemas de conexiones de control SD-WAN

Contenido

Introducción

Este documento describe algunas de las causas probables que conducen a un problema con las conexiones de control y cómo resolverlos.

Antecedentes

> **Nota**: La mayoría de los resultados de comandos presentados en este documento provienen de routers vEdge. Sin embargo, el enfoque es el mismo para los routers que ejecutan el software Cisco IOS® XE SD-WAN. Escriba el **sdwan** para obtener los mismos resultados en el software Cisco IOS XE SD-WAN. Por ejemplo, **show sdwan control connections** en lugar de **show control connections** .

Antes de solucionar el problema, asegúrese de que el extremo de la WAN en cuestión se ha configurado correctamente.

Incluye:

- Un certificado válido que está instalado.
- Estas configuraciones se establecen en el marco del **system** bloqueo:
  - IP del sistema
  - ID del sitio

    - Organization-Name
    - Dirección vBond
- Interfaz de transporte VPN 0 configurada con la opción de túnel y la dirección IP.
- Reloj del sistema configurado correctamente en el vEdge y aquellos que coinciden con otros dispositivos/controladores:

show clock confirma la hora actual establecida.

Escriba el **clock set** para establecer la hora correcta en el dispositivo.

En todos los casos mencionados anteriormente, asegúrese de que Transport Locator (TLOC) esté activado. Compruebe esto con el **show control local-properties** comando.

Aquí se muestra un ejemplo de un resultado válido:

```
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
```

En la versión 16.3 y posteriores del software vEdge, el resultado tiene algunos campos adicionales:

```
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
```

Escenarios de problemas

Fallo en la conexión DTLS (DCONFAIL)

Este es uno de los problemas comunes de la conectividad de control que no aparece. Entre las causas probables se incluyen un firewall u otros problemas de conectividad.

Puede ser que algunos o todos los paquetes se descarten o se filtren en algún lugar. El ejemplo con los más grandes se da en**tcpdump** resultados aquí.

- No se puede alcanzar el router de salto siguiente (NH).
- La puerta de enlace predeterminada no está instalada en la Base de información de routing (RIB).
- El puerto de seguridad de la capa de transporte del datagrama (DTLS) no está abierto en los controladores.

Se pueden utilizar estos comandos show:

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

Si tiene un fallo de conexión DTLS, puede verlo en el **show control connections-history** resultado del comando.

```
                                                                                                  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
```

Esto es lo que ocurre cuando los paquetes grandes no llegan a vEdge cuando se utiliza **tcpdump** , por ejemplo, en el lado de la SD-WAN (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
```

Aquí se muestra un ejemplo del lado vEdge:

```
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
```

> **Nota**: En el software SD-WAN Cisco IOS XE, puede utilizar Embedded Packet Capture (EPC) en lugar de **tcpdump**.

Puede utilizar **traceroute** or **nping** también para generar tráfico con diferentes tamaños de paquete y marcas de punto de código de servicios diferenciados (DSCP) para comprobar la conectividad, ya que el proveedor de servicios puede tener problemas con la entrega de paquetes UDP más grandes, paquetes UDP fragmentados (especialmente fragmentos pequeños de UDP) o paquetes marcados DSCP. A continuación se muestra un ejemplo con **nping** cuando la conectividad se realiza correctamente.

Desde 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
```

Aquí se muestra un ejemplo de vEdge:

```
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
```

A continuación se incluye un ejemplo de conectividad fallida con el **traceroute** (que se ejecuta desde vShell) en 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 no recibe paquetes enviados desde vSmart (solo algunos otros fragmentos o tráfico):

```
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 desactivado (DISTLOC)

Los desencadenadores de los mensajes de TLOC inhabilitado pueden deberse a las siguientes causas probables:

- Borre las conexiones de control.
- Cambie el color en TLOC.
- Cambio en la dirección IP del sistema.

Cambio en cualquiera de las configuraciones mencionadas en el bloque del sistema o en las propiedades del túnel en el**show control connections-history**resultado del comando.

```
                                                                    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
```

ID de placa no inicializada (BIDNTPR)

En una red muy inestable, donde las conexiones de red se inestabilizan continuamente, puede ver TXCHTOBD - failed to send a challenge to Board ID failed y/o RDSIGFBD - Read Signature from Board ID failed. Además, a veces debido a problemas de bloqueo, un desafío enviado a board-id falla y cuando eso sucede, reinicia el board-ID y vuelve a intentarlo. No ocurre con frecuencia y retrasa la forma de las conexiones de control. Esto se corrige en versiones posteriores.

```
                                                                                  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 - Error de firma de ID de placa

Esto indica que vBond rechaza el número de serie/número de chasis/identificador único/vEdge. Cuando esto ocurra, confirme la información de vEdge que se muestra en la **show control local-properties** resultado del comando y comparar ese resultado con **show orchestrator valid-vedges** en vBond.

Si no existe ninguna entrada para el vEdge, asegúrese de que dispone de:

- Se ha agregado vEdge a la cuenta inteligente.
- Se ha cargado el archivo correctamente en vManage.

Haga clic en **Send to Controllers** bajo **Configuration > Certificates**.

Si existe, compruebe si hay entradas duplicadas en la tabla de vEdge válida y póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para solucionar este problema

Atascado en 'Conectar': problemas de enrutamiento

Las conexiones de control no aparecen si hay problemas de ruteo en la red. Asegúrese de que

haya una ruta válida en el RIB con el NH/TLOC correcto.

Algunos ejemplos son:

- Una ruta más específica a vBond en el RIB apunta a un NH/TLOC que no se utiliza para establecer conexiones de control.
- La IP de TLOC se filtra entre el proveedor de servicio ascendente, lo que causa un ruteo incorrecto.

Ingrese estos comandos para verificación:

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

Busque el valor de distancia y el protocolo para el prefijo IP.

vEdge intenta establecer una conexión de control sin éxito o las conexiones a los controladores siguen inestables.

Verifique con el **show control connections** y/o el **show sdwan control connections-history** comandos.

```
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
```

Errores de socket (LISFD)

Si hay una IP duplicada en la red, las conexiones de control no se activan. Puede ver la LISFD - Listener Socket FD Error mensaje. Esto también puede suceder por otras razones, como la corrupción de paquetes, un RESET, una discordancia entre vEdge y los controladores en los puertos TLS versus los puertos DTLS, si los puertos FW no están abiertos, y así sucesivamente.

La causa más común es una IP de transporte duplicada. Compruebe la conectividad y asegúrese de que las direcciones sean únicas.

```
                                                                          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
```

Problema de tiempo de espera de par (VM_TMO)

Se activa una condición de tiempo de espera del par cuando un vEdge pierde la accesibilidad al controlador en cuestión.

En este ejemplo, captura un**vManage Timeout msg (peer VM_TMO)**. Otros incluyen tiempos de espera de vBond, vSmart o vEdge del mismo nivel (**VB_TMO, VP_TMO, VS_TMO**).

Como parte de la solución de problemas, asegúrese de que tiene conectividad con el controlador. Utilizar el protocolo de mensajes de control de Internet (ICMP) y/o **traceroute** a la dirección IP en cuestión. Casos en los que se producen numerosas caídas de tráfico (las pérdidas son elevadas). Rápido **ping** y asegurarse de que es buena.

```
                                                                                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
```

Además, compruebe el **show control connections-history detail** resultado del comando para observar las estadísticas de control de TX/RX para ver si hay alguna discrepancia significativa en los contadores. Observe en la salida la diferencia entre los números de paquetes de saludo RX y TX.

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

No hay números de serie (CRTREJSER, BIDNTVRFD)

Si el número de serie no está presente en los controladores de un dispositivo determinado, las conexiones de control fallan.

Puede verificarse con **show controllers [valid-vsmarts | valid-vedges]** y se fija la mayor parte del tiempo. Desplácese hasta **Configuration > Certificates > Send to Controllers or Send to vBond** de las fichas de vManage. En vBond, marque **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts**.

En los registros de vBond, observa estos mensajes con razón 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"
```

Cuando resuelva un problema de este tipo, asegúrese de que el número de serie y el modelo de dispositivo correctos se hayan configurado y aprovisionado en el portal PnP (software.cisco.com) y vManage.

Para verificar el número de chasis y el número de serie del certificado, este comando se puede utilizar en los routers vEdge:

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

En un router que ejecute el software Cisco IOS XE SD-WAN, ingrese este comando:

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

O este comando:

```
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
```

Para problemas con vEdge/vSmart

Este es el aspecto del error en vEdge/vSmart en el **show control connections-history** resultado del comando:

```
                                                                                  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
```

En vBond en el **show orchestrator connections-history** resultado del comando:

```
                                                                                        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
```

Además, el número de serie del dispositivo en vBond no está en la lista de vEdges válidos:

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

Para problemas con controladores

Si el archivo serial entre los controladores en sí no coincide, el error local en vBond es el número de serie que no está presente frente al certificado revocado para vsmarts/vManage.

En 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
```

En vSmart/vManage afectado:

```
                                                                                    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
```

Además, verá mensajes ORPTMO en el vSmart afectado con respecto a vEdge:

```
                                                                                    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
```

En vEdge, vSmart afectado, en el **show control connections-history** resultado se ve el error "SERNTPRES":

```
                                                                                    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
```

Número De Chasis/Id Único Incorrectos

Otro ejemplo del mismo error "CRTREJSER/NOERR" puede verse si se utiliza el ID de producto (modelo) incorrecto en el portal PnP. Por ejemplo:

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

Sin embargo, el modelo del dispositivo real es diferente (tenga en cuenta que el sufijo "DNA" no está en el nombre):

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

Discordancia de la organización (CTORGNMIS)

Organization Name es un componente crítico para activar la conexión de control. Para una superposición determinada, el nombre de la organización debe coincidir en todos los controladores y vEdges para que puedan aparecer las conexiones de control.

Si no es así, hay un error de "discrepancia de nombre de organización de certificado", como se muestra aquí:

```
                                                                                    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
```

Certificado vEdge/vSmart revocado/invalidado (VSCRTREV/CRTVERFL)

En los casos en los que el certificado se revoca en los controladores o el número de serie de

vEdge se invalida, se muestra un mensaje de revocación de la certificación vSmart o vEdge, respectivamente.

A continuación se muestran ejemplos de salidas de mensajes de revocación de certificados vSmart. Este es el certificado que se revoca en 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
```

Del mismo modo, en otro vSmart de la misma superposición, es así como ve el vSmart cuyo certificado se revoca:

```
                                                                                    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
```

Y así es como vBond ve esto:

```
                                                                                                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
```

La falla de verificación de certificación se produce cuando el certificado no se puede verificar con el certificado raíz instalado:

1. Compruebe la hora con el **show clock** comando. Debe estar al menos dentro del intervalo de validez del certificado de vBond (consulte con el **show orchestrator local-properties**).

2. Esto puede deberse a la corrupción del certificado raíz en vEdge.

Luego **show control connections-history** en el router vEdge muestra un resultado similar:

```
                                                                                    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
```

En este caso, vEdge no puede validar también el certificado del controlador. Para solucionar este problema, puede reinstalar la cadena de certificados raíz. En caso de que se utilice Symantec Certificate Authority, puede copiar la cadena de certificados raíz del sistema de archivos de sólo lectura:

```
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
```

Plantilla de vEdge no conectada en vManage

En el momento en que se activa el dispositivo si éste no está conectado a una plantilla en vManage, el **NOVMCFG - No Config in vManage for device** se muestra el mensaje.

```
                                                                      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
```

Condiciones transitorias (DISCVBD, SYSIPCHNG)

Estas son algunas condiciones transitorias donde las conexiones de control se inestabilizan. Estos incluyen:

- La IP del sistema ha cambiado en vEdge.
- Mensaje de eliminación para vBond (la conexión de control a vBond es transitoria).

```
                                                                                                  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
```

Falla de DNS

Cuando no se detecta ningún intento de conexión en el **show control connection-history** , puede verificar la falla de resolución DNS hacia vBond con estos pasos:

- Haga ping hacia la dirección DNS del vBond.

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

- Haga ping a google DNS (8.8.8.8) desde la interfaz de origen para verificar la disponibilidad de Internet.

```
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:
```

- Captura de paquetes integrada para el tráfico DNS en el puerto 53 para comprobar el tráfico DNS enviado y recibido.

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

Documento de referencia: Embedded Packet Capture.

Inicie la captura de monitor y déjela funcionar durante un par de minutos y, a continuación, detenga la captura. Continúe examinando la captura de paquetes para ver si se envían y reciben consultas DNS.

Información Relacionada

- Configurar parámetros básicos para conexiones de control de formularios en cEdge
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).