Solucionar problemas de conexões de controle SD-WAN

Contents

Introduction

Este documento descreve algumas das causas prováveis que levam a um problema com as Conexões de Controle e como solucioná-las.

Informações de Apoio

> **Observação**: a maioria das saídas de comando apresentadas neste documento são de roteadores vEdge. No entanto, a abordagem é a mesma para roteadores que executam o software Cisco IOS® XE SD-WAN. Digite o **sdwan** para obter as mesmas saídas no software Cisco IOS XE SD-WAN. Por exemplo, **show sdwan control connections** em vez de **show control connections** .

Antes de solucionar o problema, verifique se a borda da WAN em questão foi configurada corretamente.

Ele inclui:

- Um certificado válido instalado.
- Essas configurações são implementadas sob o comando **system** bloqueio:
  - IP do sistema
  - ID do local

    - Nome da organização
    - Endereço vBond
  - Interface de transporte VPN 0 configurada com a opção Tunnel e o endereço IP.
  - Relógio do sistema que é configurado corretamente no vEdge e aqueles que correspondem com outros dispositivos/controladores:

O **show clock** confirma a hora atual definida.

Digite o **clock set** para definir a hora correta no dispositivo.

Para todos os casos mencionados anteriormente, certifique-se de que o Transport Locator (TLOC) esteja ativado. Verifique isso com o comando **show control local-properties** comando.

Um exemplo de uma saída válida é mostrado aqui:

```
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
```

No software vEdge versão 16.3 e posterior, a saída tem alguns campos adicionais:

```
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
```

Cenários de problemas

Falha de conexão DTLS (DCONFAIL)

Essa é uma das questões comuns da conectividade de controle que não aparece. As causas prováveis incluem um firewall ou alguns outros problemas de conectividade.

Pode ser que alguns ou todos os pacotes sejam descartados/filtrados em algum lugar. O exemplo com os maiores é dado em**tcpdump** resultados aqui.

- O roteador do próximo salto (NH) não está acessível.
- O gateway padrão não está instalado na base de informações de roteamento (RIB).
- A porta DTLS (Datagram Transport Layer Security) não está aberta nos controladores.

Estes comandos show podem ser usados:

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

Quando houver uma falha de conexão DTLS, você poderá vê-la na **show control connections-history** Saída do 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
```

Isso é o que acontece quando pacotes grandes não alcançam o vEdge quando você usa **tcpdump** , por exemplo, no lado 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
```

Um exemplo do lado do vEdge é mostrado aqui:

```
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
```

> **Observação**: no software Cisco IOS XE SD-WAN, você pode usar o Embedded Packet Capture (EPC) em vez de **tcpdump**.

Você pode usar **traceroute** or **nping** utilitários também para gerar tráfego com diferentes tamanhos de pacote e marcas de Differentiated Services Code Point (DSCP) para verificar a conectividade, pois o provedor de serviços pode ter problemas com a entrega de pacotes UDP maiores, pacotes UDP fragmentados (especialmente fragmentos pequenos de UDP) ou pacote marcado por DSCP. Aqui está um exemplo com **nping** quando a conectividade for bem-sucedida.

Da 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
```

Um exemplo do vEdge é mostrado aqui:

```
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
```

E aqui está um exemplo de conectividade malsucedida com o **traceroute** (executado a partir do vShell) no 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 * * *
```

O vEdge não recebe pacotes enviados do vSmart (apenas algum outro tráfego ou fragmentos):

```
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 desativado (DISTLOC)

Os disparadores para mensagens de TLOC desativado podem ser causados pelas seguintes causas prováveis:

- Limpar Conexões de Controle.
- Altere a cor em TLOC.
- Alteração no IP do sistema.

Alteração em qualquer uma das configurações mencionadas no bloco do sistema ou nas propriedades do túnel no**show control connections-history**Saída do 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 da placa não inicializada (BIDNTPR)

Em uma rede altamente instável, onde as conexões de rede oscilam continuamente, você pode ver TXCHTOBD - failed to send a challenge to Board ID failed e/ou RDSIGFBD - Read Signature from Board ID failed. Além disso, às vezes devido a problemas de bloqueio, um desafio enviado para board-id falha e quando isso acontece, redefina o board-ID e tente novamente. Isso não acontece com frequência e atrasa a forma das conexões de controle. Isso é corrigido em versões 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 - Falha de assinatura de ID de placa

Isso indica que o número do chassi/id exclusivo/número de série do vEdge foi rejeitado pelo vBond. Quando isso ocorrer, confirme as informações do vEdge mostradas na **show control local-properties** saída do comando e compare essa saída com **show orchestrator valid-vedges** no vBond.

Se não existir uma entrada para o vEdge, verifique se você tem:

- vEdge adicionado à Smart Account.
- Carregou o arquivo corretamente no vManage.

Clique em **Send to Controllers** sob **Configuration > Certificates**.

Se ele existir, verifique se há entradas duplicadas na tabela válida do vEdge e entre em contato com o Centro de assistência técnica da Cisco (TAC) para solucionar esse problema

Preso em 'Connect': Problemas de roteamento

As conexões de controle não serão ativadas se houver problemas de roteamento na rede. Certifique-se de que haja uma rota válida na RIB com o NH/TLOC correto.

Os exemplos incluem:

- Uma rota mais específica para vBond na RIB aponta para um NH/TLOC que não é usado

para estabelecer conexões de controle.
- O IP TLOC é vazado entre o provedor de serviço upstream, o que causa roteamento incorreto.

Digite estes comandos para verificação:

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

Procure o valor da distância e o protocolo para o IP-Prefix.

O vEdge tenta estabelecer uma conexão de controle sem sucesso ou as conexões com os controladores continuam oscilando.

Verifique com o comando **show control connections** ou a **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
```

Erros de soquete (LISFD)

Se houver um IP duplicado na rede, as conexões de controle não serão ativadas. Você verá o LISFD - Listener Socket FD Error mensagem. Isso também pode acontecer por outros motivos, como corrupção de pacotes, um RESET, uma incompatibilidade entre vEdge e controladores em portas TLS versus DTLS, se as portas FW não estiverem abertas e assim por diante.

A causa mais comum é um IP de transporte duplicado. Verifique a conectividade e assegure-se de que os endereços sejam exclusivos.

```
                                                                    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 tempo limite de peer (VM_TMO)

Uma condição de tempo limite de peer é acionada quando um vEdge perde a acessibilidade para o controlador em questão.

Neste exemplo, ele captura um**vManage Timeout msg (peer VM_TMO)**. Outros incluem timeouts de vBond, vSmart e/ou vEdge de mesmo nível (**VB_TMO, VP_TMO, VS_TMO**).

Como parte da solução de problemas, verifique se você tem conectividade com o controlador. Usar o ICMP (Internet Control Message Protocol) e/ou **traceroute** ao endereço IP em questão. Casos em que há muitos descartes de tráfego (a perda é alta). Rápida **ping** e garantir que seja bom.

```
                                                                                    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
```

Além disso, verifique a caixa de seleção **show control connections-history detail** para examinar as estatísticas de controle de TX/RX para ver se há alguma discrepância significativa nos contadores. Observe na saída a diferença entre os números de pacotes hello RX e 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
```

Números de série ausentes (CRTREJSER, BIDNTVRFD)

Se o número de série não estiver presente nos controladores de um determinado dispositivo, as conexões do controle falharão.

Pode ser verificado com **show controllers [valid-vsmarts | valid-vedges]** e corrigido na maior parte do tempo. Navegue até **Configuration > Certificates > Send to Controllers or Send to vBond** nas guias do vManage. No vBond, marque **show orchestrator valid-vedges** / **show orchestrator valid-vsmarts.**

Nos registros do vBond, você observa estas mensagens com razão 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"
```

Ao solucionar esse problema, verifique se o número de série e o modelo do dispositivo corretos foram configurados e provisionados no portal PnP (software.cisco.com) e no vManage.

Para verificar o número do chassi e o número de série do certificado, este comando pode ser usado em roteadores vEdge:

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

Em um roteador que execute o software Cisco IOS XE SD-WAN, digite este comando:

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

Ou 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 com vEdge/vSmart

Esta é a aparência do erro no vEdge/vSmart no **show control connections-history** Saída do 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
```

No vBond no **show orchestrator connections-history** Saída do 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
```

Além disso, o número de série do dispositivo no vBond não está na lista de vEdges válidas:

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

Para problemas com controladores

Se o arquivo serial entre os controladores não corresponder, o erro local no vBond é o número serial que não está presente em comparação com o certificado revogado para o vSmarts/vManage.

No 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
```

No vSmart/vManage afetado:

```
                                                                                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
```

Além disso, você verá mensagens ORPTMO no vSmart afetado com relação ao 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
```

No vEdge afetado pelo vSmart, no **show control connections-history** saída do erro "SERNTPRES" é visto:

```
                                                                        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 Chassi/Id Exclusiva Incorretos

Outro exemplo do mesmo erro "CRTREJSER/NOERR" pode ser visto se a ID de produto (modelo) incorreta for usada no portal PnP. Por exemplo:

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

No entanto, o modelo do dispositivo real é diferente (observe que o sufixo "DNA" não está no nome):

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

Incompatibilidade de Organização (CTORGNMMIS)

O Nome da Organização é um componente crítico para ativar a conexão de controle. Para uma determinada sobreposição, o nome da organização deve corresponder a todos os controladores e bordas para que as conexões de controle possam surgir.

Caso contrário, haverá um erro de "Incompatibilidade de nome da Org. do Certificado", como mostrado aqui:

```
                                                                          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 revogado/invalidado (VSCRTREV/CRTVERFL)

Nos casos em que o certificado é revogado nos controladores ou o número de série do vEdge é invalidado, uma mensagem vSmart ou vEdge Certification revoked, respectivamente, é exibida.

Aqui estão exemplos de saídas de mensagens de revogação de certificado vSmart. Este é o certificado revogado no 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
```

Da mesma forma, em outro vSmart na mesma sobreposição, é assim que ele vê o vSmart cujo certificado é revogado:

```
                                                                                                    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
```

E aqui está como vBond vê isso:

```
                                                                                                          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
```

A falha na verificação de certificação ocorre quando o certificado não pode ser verificado com o certificado raiz instalado:

1. Verifique a hora com o comando **show clock** comando. Deve estar pelo menos dentro do intervalo de validade do certificado vBond (verifique com o comando **show orchestrator local-properties**).

2. Isso pode ser causado pela corrupção do certificado raiz no vEdge.

Em seguida **show control connections-history** no roteador vEdge mostra uma saída semelhante:

```
                                                                                                    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
```

Nesse caso, o vEdge também não pode validar o certificado do controlador. Para corrigir esse problema, você pode reinstalar a cadeia de certificados raiz. Caso a Symantec Certificate Authority seja usada, você poderá copiar a cadeia de certificados Raiz do sistema de arquivos somente leitura:

```
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
```

Modelo do vEdge não anexado no vManage

No momento em que o dispositivo é ativado, se o dispositivo não estiver conectado com um modelo no vManage, o **NOVMCFG - No Config in vManage for device** é exibida.

```
                                                                    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
```

Condições transitórias (DISCVBD, SYSIPCHNG)

Aqui estão algumas condições transitórias em que as conexões de controle oscilam. Eles incluem:

- System-IP alterado no vEdge.
- Mensagem de destruição para vBond (a conexão de controle para vBond é transitória).

```
                                                                                                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
```

Falha de DNS

Quando nenhuma tentativa de conexão é vista no **show control connection-history** , você pode verificar a falha de resolução DNS em direção ao vBond com estas etapas:

- Faça ping em direção ao endereço DNS do vBond.

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

- Faça ping no google DNS (8.8.8.8) a partir da interface de origem para verificar a acessibilidade da 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 pacotes incorporada para tráfego DNS na porta 53 para verificar o tráfego DNS enviado e recebido.

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

Documento de referência: Embedded Packet Capture.

Inicie a captura do monitor, deixe-a funcionar por alguns minutos e, em seguida, interrompa a captura. Continue para examinar a captura de pacotes para ver se as consultas DNS são enviadas e recebidas.

Informações Relacionadas

- Configurar parâmetros básicos para formar conexões de controle no cEdge
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.