虚拟专用网络

故障排除

文档版本	01
发布日期	2025-11-13

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

1 站点入云 VPN 企业版

1.1 VPN 连接状态显示“未连接”

故障现象

在“虚拟专用网络 > 企业版-VPN连接”页面，VPN连接状态显示为“未连接”。

可能原因

- VPN连接两端的连接配置不正确。
- 华为云安全组和客户设备侧ACL配置不正确。
- IPsec-VPN连接协商失败或连接断连。

处理步骤

1. 重置VPN连接。

   如果重置VPN连接后仍无法解决该问题，请继续步骤**2**。
2. 检查VPN连接两端的连接配置。
   a. 确认两端配置的网关IP参数是否为镜像。
      i. VPN网关的主/备EIP可以选择“虚拟专用网络 > 企业版-VPN网关”，在网关IP栏下查看。
      ii. 客户设备侧网关的公网IP可以选择“虚拟专用网络 > 企业版-对端网关”，在标识栏下查看。
         - 如果两端配置的网关IP参数不是镜像，请修改对应参数。
         - 如果两端配置的网关IP参数是镜像，请继续步骤**b**。

   b. 确认IKE策略、IPsec策略协商参数是否一致。

      IKE策略、IPsec策略协商参数可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改策略配置”查看。

      如果IKE策略、IPsec策略协商参数不一致，请修改对应策略。

      如果IKE策略、IPsec策略协商参数一致，请继续步骤**c**。

   c. 确认预共享密钥是否一致。

预共享密钥无法在云上直接查看。如果不确认预共享密钥，建议根据客户设备侧的预共享密钥对VPN连接的预共享密钥进行重置。

可以选择“虚拟专用网络 > 企业版-VPN连接”，选择“更多 > 重置密钥”进行重置。

d. 如果连接模式采用策略模式，请确认两端策略规则中的源网段和目的网段是否为镜像。

策略规则可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”查看。

e. 如果连接模式采用静态路由模式且云侧开启了NQA功能，请确认客户设备侧是否已经正确配置Tunnel隧道的IP地址。

- 查看是否开启NQA功能，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击VPN连接名称，在“基本信息”页签查看“检测机制”。
- 客户设备侧在华为云VPN连接已设置的Tunnel隧道的IP地址，可以选择“虚拟专用网络 > 企业版-VPN连接”，单击“修改连接信息”，查看本端接口地址和对端接口地址。

  华为云VPN连接的本端接口地址和对端接口地址需要和客户设备的本端接口地址和对端接口地址互为镜像配置。

f. 如果连接模式采用BGP路由模式，请确认两端的BGP ASN是否为镜像。

- VPN网关的BGP ASN可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
- 客户设备侧网关的BGP ASN可以选择“虚拟专用网络 > 企业版-对端网关”，在BGP ASN栏下查看。

3. 检查华为云安全组和客户设备侧ACL配置。

a. 确认华为云default安全组已经放通客户设备侧公网IP的端口。

b. 华为云default安全组查看步骤如下：

i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。

ii. 单击VPC对应的路由表。

iii. 单击路由表的名称。

iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。

v. 在“关联安全组”页签，检查端口放通情况。

c. 确认客户设备侧ACL已经放通VPN网关主备EIP的端口。

4. 查看IPsec连接日志。

a. 登录管理控制台。

b. 在管理控制台左上角单击 图标，选择区域和项目。

c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。

e. 在“VPN连接”界面，找到目标VPN连接，单击“查看日志”，查看相关日志信息。

查看IPsec连接日志的过程中，您可以根据日志关键字对照**表 VPN未连接的常见原因**中的错误码自主排查问题。

表 1-1 VPN 未连接的常见原因

分类	序号	错误信息	描述	处理步骤
IPsec-VPN连接协商失败	1	phase1 proposal mismatch	两端IKE安全提议参数不匹配。仅隧道发起端可见。	请查看两端的IKE安全提议参数，并执行相应的命令将不匹配的参数修改一致。
	2	phase1 proposal encryption algorithm mismatch	两端IKE安全提议加密算法参数不匹配。仅隧道接收端可见。	
	3	phase1 proposal authentication method mismatch	两端IKE安全提议认证方法参数不匹配。仅隧道接收端可见。	
	4	phase1 proposal authentication algorithm mismatch	两端IKE安全提议认证算法参数不匹配。仅隧道接收端可见。	
	5	phase1 proposal dh mismatch	两端IKE安全提议DH组参数不匹配。仅隧道接收端可见。	
	6	phase1 proposal integrity algorithm mismatch	两端IKE安全提议完整性算法参数不匹配。仅隧道接收端可见。	
	7	phase1 proposal prf mismatch	两端IKE安全提议PRF算法参数不匹配。仅隧道接收端可见。	
	8	phase2 proposal or pfs mismatch	两端IPSec安全提议参数、PFS算法或Security ACL不匹配。	请查看两端的IPsec安全提议参数或PFS算法，并执行相应的命令将不匹配的参数修改一致。
	9	responder dh mismatch	响应方的DH算法不匹配。	请查看两端的DH算法，并执行相应的命令将DH算法修改一致。
	10	initiator dh mismatch	发起方的DH算法不匹配。	

分类	序号	错误信息	描述	处理步骤
	11	encapsulation mode mismatch	封装模式不匹配。	请联系技术工程师进行处理。
	12	flow mismatch	两端Security ACL不匹配。	请联系技术工程师进行处理。
	13	version mismatch	两端IKE版本号不匹配。	请联系技术工程师进行处理。
	14	peer address mismatch	两端的IKE Peer地址不匹配。	请查看两端的IKE对等体地址，并执行相应的命令修改不匹配的IKE对等体地址。
	15	config ID mismatch	根据ID未找到匹配的IKE Peer。	请联系技术工程师进行处理。
	16	exchange mode mismatch	两端的协商模式不匹配。	请查看两端的IKE协商模式，并执行相应的命令将两端的协商模式修改一致。
	17	authentication fail	身份认证失败。	请查看两端的IKE安全提议参数或IKE对等体参数，并执行相应的命令将两端的参数修改一致。
	18	construct local ID fail	构造本端ID失败。	请联系技术工程师进行处理。
	19	rekey no find old sa	重协商时找不到旧的SA。	请联系技术工程师进行处理。
	20	rekey fail	重协商时旧的SA正在下线。	请联系技术工程师进行处理。
	21	first packet limited	首包限速。	请联系技术工程师进行处理。
	22	unsupported version	不支持的IKE版本号。	请联系技术工程师进行处理。
	23	malformed message	畸形消息。	请联系技术工程师进行处理。
	24	malformed payload	畸形载荷。	请联系技术工程师进行处理。
	25	malformed payload or psk mismatch	畸形载荷或两端预共享密钥不一致。	请联系技术工程师进行处理。

分类	序号	错误信息	描述	处理步骤
	26	critical drop	未识别的critical载荷。	请联系技术工程师进行处理。
	27	cookie mismatch	Cookie不匹配。	请联系技术工程师进行处理。
	28	invalid cookie	无效Cookie。	请联系技术工程师进行处理。
	29	invalid length	报文长度非法。	请联系技术工程师进行处理。
	30	unknown exchange type	未知的协商模式。	请联系技术工程师进行处理。
	31	short packet	超短包。	请联系技术工程师进行处理。
	32	uncritical drop	未识别的非critical载荷。	请联系技术工程师进行处理。
	33	route limit	路由注入的数目达到规格。	请更换路由注入规格更高的设备，并合理规划网络。
	34	ip assigned fail	IP地址分配失败。	请确保AAA和IPsec的相关配置正确，例如IP Pool、AAA业务方案、为IKE用户分配的IP地址。
	35	eap authentication timeout	EAP认证超时。	请确保客户端的用户名和密码正确，以及确保用户接入的相关配置正确。
	36	eap authentication fail	EAP认证失败。	
	37	xauth authentication fail	XAUTH认证失败。	
	38	xauth authentication timeout	XAUTH认证超时。	
	39	license or specification limited	License限制。	请联系技术工程师进行处理。

分类	序号	错误信息	描述	处理步骤
	40	local address mismatch	IKE协商时的本端IP地址和接口IP地址不匹配。	请查看IKE协商时的本端IP地址和接口IP地址，并执行相应的命令将地址修改一致。
	41	dynamic peers number reaches limitation	IKE对等体数达到规格。	请联系技术工程师进行处理。
	42	ipsec tunnel number reaches limitation	IPSec隧道数达到规格。	请联系技术工程师进行处理。
	43	netmask mismatch	开启IPSec掩码过滤功能后，掩码不匹配。	请联系技术工程师进行处理。
	44	flow confict	数据流冲突。	请联系技术工程师进行处理。
	45	proposal mismatch or use sm in ikev2	IPSec安全提议不匹配或者IKEv2使用SM算法。	请查看IPsec安全提议中IKEv2使用的算法，并执行相应的命令将算法修改正确。
	46	ikev2 not support sm in ipsec proposal ikev2	IKEv2不支持IPSec安全提议的SM算法。	
	47	no policy applied on interface	没有策略应用到接口上。	请联系技术工程师进行处理。
	48	nat detection fail	NAT探测失败。	请联系技术工程师进行处理。
	49	fragment packet limit	分片报文超规格。	请联系技术工程师进行处理。
	50	fragment packet reassemble timeout	分片报文重组超时。	请确保两端链路正常及设备状态正常。
	51	peer cert is expired	对端证书过期。	请联系技术工程师进行处理。
	52	peer cert is revoked by CRL	对端证书被吊销。	请联系技术工程师进行处理。

分类	序号	错误信息	描述	处理步骤
	53	sa with same user exists	相同用户已存在sa。	请联系技术工程师进行处理。
	54	max transmit reached	重传报文达到最大次数。	请联系技术工程师进行处理。
IPsec-VPN连接断连	1	dpd timeout	DPD探测超时。	请执行Ping操作检查链路是否可达，如果链路不可达，请排查链路和网络配置是否正确。
	2	peer request	对端发送删除消息。	请确认对端的日志信息，并根据其信息确认IPSec隧道故障的原因。
	3	config modify or manual offline	修改配置导致SA被删除或者手动清除SA。	1. 请检查是否手动执行Reset SA操作，如果是，则无需处理。 2. 请检查本端修改的IPsec配置是否正确，如果不正确，则请修改正确。 3. 请检查手动取消IPsec策略是否合理，如果不合理，则请重新在接口上应用IPsec策略。
	4	phase1 hard expiry	第一阶段硬超时（没有新的SA协商成功）。	请检查IKE SA的生存周期是否合理，如果不合理，请修改IKE SA的生存周期。
	5	phase2 hard expiry	第二阶段硬超时。	请检查IPsec SA的生存周期是否合理，如果不合理，请修改IPsec SA的生存周期。
	6	heartbeat timeout	heartbeat探测超时。	请联系技术工程师进行处理。
	7	re-auth timeout	重认证超时导致SA被删除。	无需处理。

分类	序号	错误信息	描述	处理步骤
	8	aaa cut user	AAA模块强制用户下线导致SA被删除。	无需处理。
	9	ip address syn failed	IP地址同步失败。	请确保链路正常、IPsec相关配置正确。
	10	hard expiry triggered by port mismatch	NAT端口不匹配导致硬超时。	请联系技术工程师进行处理。
	11	kick old sa with same flow	相同的流接入时删除老的SA。	请联系技术工程师进行处理。
	12	cpu table updated	插拔SPU板时删除非本CPU的SA。	无需处理。
	13	flow overlap	加密流中的IP地址与对端的IP地址冲突。	请检查两端配置的Security ACL信息，修改流冲突的ACL规则。
	14	spi conflict	SPI冲突。	无需处理。
	15	admin down	VPN隧道的管理down。	请联系技术工程师进行处理。
	16	peer address switch	对端地址变化。	请联系技术工程师进行处理。
	17	forward down	fwd群组down。	请联系技术工程师进行处理。
	18	sa with same user exists	相同用户已存在sa。	请联系技术工程师进行处理。
	19	reset sa by ike user	用户重置sa下线。	请联系技术工程师进行处理。
	20	phase1 sa replace	新IKE SA替换老的IKE SA。	无需处理。
	21	phase2 sa replace	新IPSec SA替换老的IPSec SA。	无需处理。
	22	manual offline	手动下线。	请联系技术工程师进行处理。
	23	nhrp notify	NHRP通知删除SA。	无需处理。
	24	receive backup delete info	备机收到主机的SA备份删除消息。	无需处理。

分类	序号	错误信息	描述	处理步骤
	25	eap delete old sa	对端设备重复进行EAP认证时本端设备删除老的SA。	无需处理。
	26	receive invalid spi notify	收到无效SPI通知。	如果频繁出现此现象，请检查对端设备状态、配置等是否异常。
	27	dns resolution status change	DNS解析状态发生改变。	1. 请确保DNS服务器的服务正常。 2. 请确保配置的域名正确。 如果上述操作仍然无法解决问题，请联系技术工程师进行处理。
	28	ikev1 phase1-phase2 sa dependent offline	设备删除IKEv1 SA时删除其关联的IPSec SA。	请联系技术工程师进行处理。
	29	exchange timeout	报文交互超时。	请确保链路正常、IPsec相关配置正确。
	30	hash gene adjusted	Hash因子调整导致IPSec隧道被删除。	请联系技术工程师进行处理。
	31	ipsec tunnel recover	隧道自愈重建。	无需处理。
	32	hash except	Hash分流算法调整导致IPsec隧道被删除。	请联系技术工程师进行处理。

如果上述场景均正确且异常仍然存在，请**提交工单**联系华为工程师。

1.2 云上云下无法 Ping 通

故障现象

- 云下数据中心服务器无法Ping通华为云VPC上的ECS服务器。
- 华为云VPC上的ECS服务器无法Ping通云下数据中心服务器。

可能原因

- 华为云安全组配置不正确。

- 互联子网的ACL规则配置不正确。
- 客户设备侧放通策略配置不正确。
- 客户设备侧路由配置不正确。

处理步骤

1. 重置VPN连接。

   如果重置VPN连接后仍无法解决该问题，请继续步骤**2**。
2. 检查华为云安全组配置。
   a. 确认华为云default安全组已经放通去往对端子网数据流。
   b. 华为云default安全组查看步骤如下：
      i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击关联的VPC名称。
      ii. 单击VPC对应的路由表。
      iii. 单击路由表的名称。
      iv. 找到VPN网关主或备EIP的下一跳，单击下一跳名称。
      v. 在“关联安全组”页签，检查端口放通情况。
   c. 确认华为云default安全组已经放通来自对端子网数据流。
   d. 确认华为云default安全组已经放通去往本端子网数据流。
   e. 确认华为云default安全组已经放通来自本端子网数据流。
   f. 确认华为云ECS所在的安全组已经放通去往对端子网数据流。
   g. ECS安全组可以选择“计算 > 虚拟弹性云服务器”，单击ECS名称，选择“安全组”，单击“配置规则”查看。
   h. 确认华为云ECS所在的安全组已经放通来自对端子网数据流。
3. 互联子网的ACL规则配置不正确。
   a. 确认互联子网的ACL规则中，是否已放通所有本端子网到对端子网的端口。
      i. 选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称。
      ii. 在“基本信息”页签，记录互联子网信息。
      iii. 在“基本信息”页签，单击关联模式对应的VPC名称。
      iv. 在VPC“基本信息”页签右边“网络互通概览”区域，单击子网个数。
      v. 根据网段匹配互联子网，并单击“网络ACL”的ACL名称。
      vi. 放通所有本端子网到对端子网的端口。
4. 检查客户设备侧放通策略。
   a. 确认客户设备侧已经放通去往华为云VPN本端子网的数据流。
   b. 确认客户设备侧已经放通来自华为云VPN本端子网的数据流。
5. 华为云本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。
6. 检查客户设备侧路由配置。
   a. 确认公网路由配置正确：目的地址为华为云VPN网关EIP地址，下一跳为设备出口地址。
   b. 确认私网路由配置正确：目的地址为华为云VPN本端子网，下一跳为设备出口地址。

c. 华为云本端子网可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称，在“基本信息”页签查看。

1.3 流量丢包

故障现象

- 云下数据中心服务器对华为云VPC上的ECS服务器执行Ping操作时，存在流量丢包。
- 华为云VPC上的ECS服务器对云下数据中心服务器执行Ping操作时，存在流量丢包。

处理步骤

- 检查客户侧组网和带宽情况
  - 确认客户网络的组网是否多出口，是否因为负载分担组网将流量分配到非VPN连接出口导致流量丢包，确保数据流恒定走特定出口访问华为云。
  - 使用客户侧VPN网关地址Ping华为云VPN网关IP以及其他公网（例如：114.114.114.114），检查公网时延、丢包率。

    如果公网网络质量存在问题，建议向所在网络提供运营商进行求助。
  - 检查客户出口设备带宽是否超限。
- 检查华为云侧组网和带宽情况
  - 检查华为云VPN网关的带宽是否超限。
    i. VPN网关主/备EIP带宽规格大小，可以选择“虚拟专用网络 > 企业版-VPN网关”，单击VPN网关名称查看。
    ii. VPN网关实际带宽使用情况可以选择“虚拟专用网络 > 企业版-VPN网关”，单击网关IP栏主/备EIP对应的  ，查看带宽是否达到上限。

    如果超限，可以通过扩容VPN网关的带宽进行解决。
- 如果上述场景均正确且异常仍然存在，请**提交工单**联系华为工程师。

2 站点入云 VPN 经典版

2.1 常规检查项

用户在华为云VPN产品使用过程中，通常会出现由于配置错误（华为云侧或用户侧协商策略、防火墙、路由表、域间策略、NAT配置、安全组等信息配置）而导致连接故障或无法PING通。

通常可使用以下方式排除故障：

- **检查VPN两侧协商信息**
- **检查客户防火墙ACL和云端安全组配置**
- **检查防火墙路由表**
- **检查客户防火墙域间策略**
- **检查防火墙NAT配置**

检查 VPN 两侧协商信息

- 确认PSK共享密钥是否一致。
- 确认IKE策略、IPsec策略协商参数是否一致。
- 确认两侧的本地子网和远端子网配置是否互为镜像。

检查客户防火墙 ACL 和云端安全组配置

- 确认放行去往华为云VPC子网的数据流。
- 确认放行来自华为云VPC子网的数据流。

检查防火墙路由表

确认存在目标地址为华为云VPC子网的路由信息：

- 确认配置去往华为云目标网络的路由信息，路由表或VPN路由表中存在路由信息。
- 确认路由转发表状态正常。

说明

路由易错配置：

1. 目的网段与华为云VPC网段不一致，导致前往华为云的流量无法路由到配置IPsec策略的公网口。
2. 配置静态路由时指定出接口，而非指定下一跳。

   在ethernet类型的网络中，出接口会因为无法学习到对端的ARP信息而导致路由转发失败。
3. 将路由的下一跳地址指定为华为云端的VPN网关地址。

   部分友商设备会因为路由信息无法自动迭代而不可行；由于VPN流量是要从公网口发出的，因此下一跳地址必须是运营商提供的网关地址。

检查客户防火墙域间策略

- trust到untrust：放行本地VPC到云上VPC子网访问策略。
- untrust到trust：放行云上VPC到本地VPC子网访问策略。

检查防火墙 NAT 配置

确认本地VPN网关是否在NAT设备后（一般是边界防火墙）进行部署，即VPN网关的出接口使用私有地址，然后在NAT设备上做公网地址转换。

这种场景也被称为IPsec nat穿越。

2.2 常见配置问题及解决方案

- PSK不一致：单独更新预共享密钥会在下一次IKE协商时生效，最长等待一个IKE的生命周期，须确认两端更新密钥一致。
- 协商策略不一致：请仔细排查IKE中的认证算法、加密算法、版本、DH组、协商模式和IPsec中的认证算法、加密算法、封装格式、PFS算法，特别注意PFS和云下配置一致，部分设备默认关闭了PFS配置。
- 感兴趣流：两端ACL配置不互为镜像，特别注意云下的ACL配置不能采用地址组名称，要使用真实的IP地址+掩码。
- NAT配置：云下子网访问云上子网配置为NONAT，云下公网IP不能被二次NAT为设备的接口IP。
- 安全策略：放行云下子网访问云上子网的所有协议，放行两个公网IP间的ESP、AH及UDP的500和4500端口。
- 路由配置：添加访问云上子网的出接口路由为隧道接口或IPsec协商出口，注意出接口的下一跳ARP解析要可达。

  更多故障排除案例请详细查看**连接故障或无法PING通**。

3 终端入云 VPN

3.1 客户端连接失败

3.1.1 客户端日志显示“Connection failed to establish within given time”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Connection failed to establish within given time
```

可能原因

- 客户端设备无法正常访问Internet网络。
- 用户修改服务端配置后，没有重新下载新的客户端配置文件，导致客户端配置文件与VPN网关“服务端”页签中的客户端配置文件不一致。

处理步骤

1. 在客户端设备上尝试访问其他Internet服务，查看网络是否正常。
   - 如果无法访问，请联系运营商排除网络问题。
   - 如果可以正常访问，请继续步骤2。
2. 登录管理控制台。
3. 在管理控制台左上角单击 图标，选择区域和项目。
4. 在页面左上角单击 图标，选择“网络 > 虚拟专用网络 VPN”。
5. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

6. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
7. 在服务端页签的基本信息中查看服务端ID，在高级配置中查看服务端的端口和协议。
8. 在客户端配置文件中查看“proto”和“remote”参数。示例如下：

   ```
   ......
   proto tcp    # 协议类型
   remote XXX.XX.XX.XX XXX    # 服务端公网IP和端口
   ......
   ```

   如果服务端和客户端配置文件信息不一致，请参考以下方式修改。

   - 方式1：修改服务端的信息。
     i. 在服务端配置页签，修改对应的信息。
     ii. 下载新的客户端配置文件。
     下载的客户端配置文件为“client_config.zip”。
     iii. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
     解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
     iv. 以记事本或Notepad++打开“client_config.ovpn”文件。
     v. 添加客户端证书及私钥。
     在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

     ```
     <cert>
     -----BEGIN CERTIFICATE-----
     此处添加客户端证书
     -----END CERTIFICATE-----
     </cert>

     <key>
     -----BEGIN PRIVATE KEY-----
     此处添加客户端私钥
     -----END PRIVATE KEY-----
     </key>
     ```

     vi. 保存ovpn配置文件。
   - 方式2：修改客户端配置文件。
     i. 以记事本或Notepad++打开“client_config.ovpn”文件。
     ii. 修改客户端配置文件中对应的信息。
     iii. 保存ovpn配置文件。
9. 打开OpenVPN Connect客户端。
10. 导入新的客户端配置文件。
11. 使用客户端重新连接VPN网关。
12. 按**Win+R**，输入cmd，打开命令窗口。
13. 执行以下命令，验证连通性。

    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

    ```
    64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
    64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
    64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
    ```



```
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

3.1.2 客户端日志显示“Cannot load CA certificate file [[INLINE]](no entries were read)”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Cannot load CA certificate file [[INLINE]](no entries were read)
```

可能原因

客户端配置文件中缺少客户端证书和私钥。

处理步骤

1. 重新生成客户端证书和私钥。如何生成证书，具体请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。本示例中生成客户端证书文件为“p2cclient.com.crt”，私钥文件为“p2cclient.com.key”。
2. 以记事本或Notepad++打开“client_config.ovpn”、“p2cclient.com.crt”和“p2cclient.com.key”文件。
3. 将客户端证书和私钥复制到“client_config.ovpn”文件中。

   在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

   ```
   <cert>
   -----BEGIN CERTIFICATE-----
   此处添加客户端证书
   -----END CERTIFICATE-----
   </cert>

   <key>
   -----BEGIN PRIVATE KEY-----
   此处添加客户端私钥
   -----END PRIVATE KEY-----
   </key>
   ```
4. 保存ovpn配置文件。
5. 打开OpenVPN客户端。
6. 导入新的客户端配置文件。
7. 使用客户端重新连接VPN网关。
8. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

   Linux系统，以**root**用户登录，打开命令行窗口。
9. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

3.1.3 客户端日志显示“error:068000A8:asn1 encoding routines:wrong tag”

适用的客户端

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
error:068000A8:asn1 encoding routines:wrong tag
```

可能原因

客户端证书和私钥不匹配。

处理步骤

1. 以记事本或Notepad++打开“client_config.ovpn”、“p2cclient.com.crt”和“p2cclient.com.key”文件。

   本示例中的客户端证书为“p2cclient.com.crt”，客户端私钥为“p2cclient.com.key”。

2. 将客户端证书和私钥复制到“client_config.ovpn”文件中。

   在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

   ```
   <cert>
   -----BEGIN CERTIFICATE-----
   此处添加客户端证书
   -----END CERTIFICATE-----
   </cert>

   <key>
   -----BEGIN PRIVATE KEY-----
   此处添加客户端私钥
   -----END PRIVATE KEY-----
   </key>
   ```


3. 保存ovpn配置文件。
4. 打开OpenVPN客户端。
5. 导入新的客户端配置文件。
6. 使用客户端重新连接VPN网关。
7. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

   Linux系统，以**root**用户登录，打开命令行窗口。
8. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

   说明

   XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

   回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

3.1.4 客户端日志显示“OpenSSL: error:0A000086:SSL routines::certificate verify failed”

适用的客户端

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
OpenSSL: error:0A000086:SSL routines::certificate verify failed
```

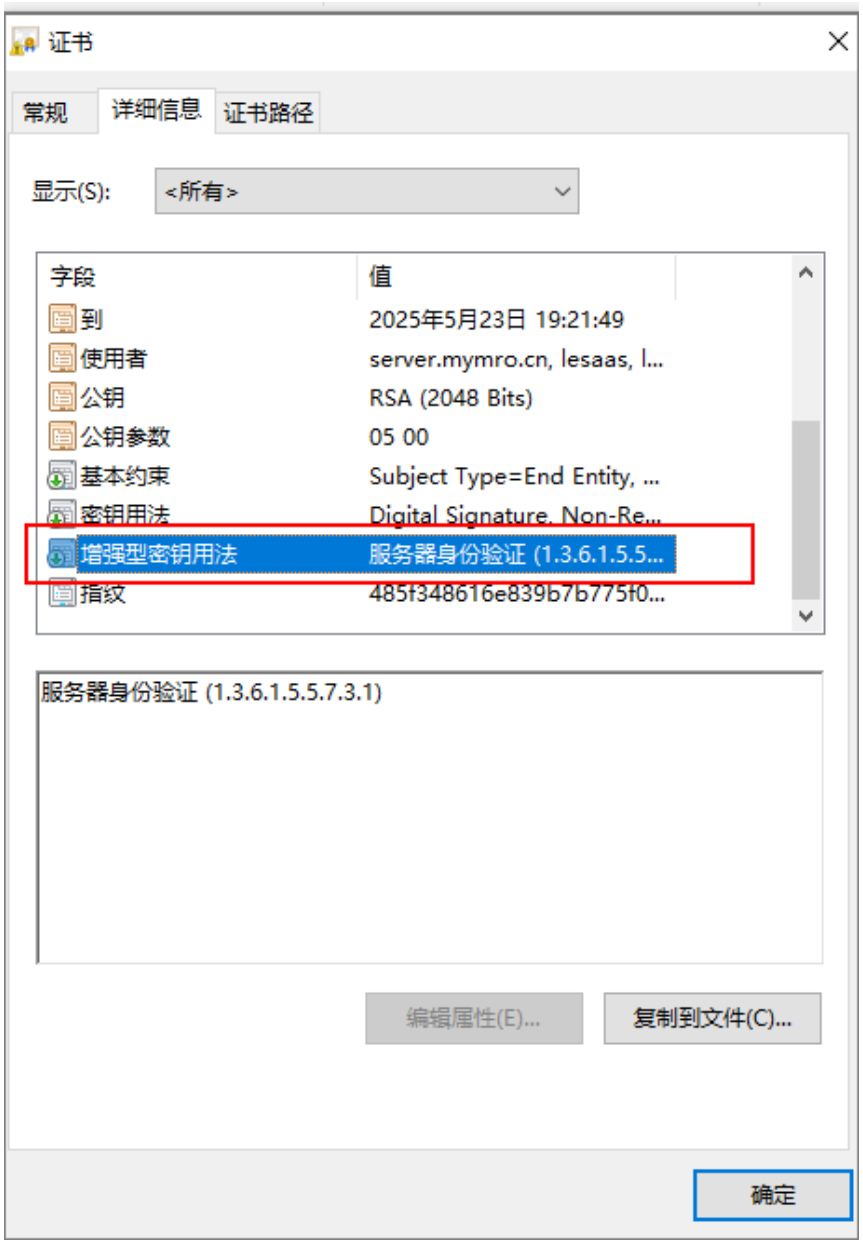
可能原因

VPN网关使用的服务端证书中缺少“服务器身份验证”扩展属性，导致验证失败。

处理步骤

1. 找到目标服务端证书，双击打开。
2. 单击“详细信息”，查看证书中是否包含“服务器身份验证”的值。如**图 服务端证书**所示。

图 3-1 服务端证书



如果证书中不包含“服务器身份验证”扩展属性，需要重新生成服务端证书。如何生成服务端证书，请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。

如果使用的服务端证书是OpenSSL自签发生成的，默认不携带此扩展属性。需要在OpenSSL配置文件中补充配置**extendedKeyUsage = serverAuth**。示例如下粗体：

```
.....
keyUsage = nonRepudiation，digitalSignature，keyEncipherment
extendedKeyUsage = serverAuth
.....
```

3. 登录管理控制台。
4. 在管理控制台左上角单击 图标，选择区域和项目。

5. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
6. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
7. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
8. 在VPN网关的“服务端”页签中，单击“更换”。
9. 在更换证书的弹窗中，单击“上传证书”。

   将新的服务端证书上传到CCM。如何上传请参考**通过云证书与管理服务CCM托管服务端证书**。
10. 下载新的客户端配置文件。

    下载的客户端配置文件为“client_config.zip”。
11. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

    解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
12. 添加客户端证书及私钥。
    a. 以记事本或Notepad++打开“client_config.ovpn”文件。
    b. 在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

    c. 保存ovpn配置文件。
13. 打开OpenVPN客户端。
14. 导入新的客户端配置文件。
15. 使用客户端重新连接VPN网关。
16. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

    Linux系统，以**root**用户登录，打开命令行窗口。
17. 执行以下命令，验证连通性。

    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.5 客户端日志显示“TLS Error: TLS handshake failed”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
TLS Error: TLS handshake failed
```

可能原因

客户端配置文件中的证书和私钥与VPN网关“服务端”页签中导入的客户端CA证书不匹配。

处理步骤

1. 检查导入的客户端CA证书是否正确。
   a. 登录管理控制台。
   b. 在管理控制台左上角单击 图标，选择区域和项目。
   c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
   d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
   e. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
   f. 在服务端页签中，查看客户端CA证书的颁发者信息。
   g. 双击目标客户端CA证书，单击详细信息，查看颁发者信息。
      - 如果两边的颁发者信息一致，请继续步骤2。
      - 如果两边的颁发者信息不一致，请参考以下步骤，重新导入客户端CA证书。

      i. 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证”，单击“上传CA证书”。
      ii. 根据界面提示填写相关信息。

      表 3-1 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-xxxx

参数	说明	取值样例
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** • 推荐使用强密码算法的证书，如RSA3072/4096。 • RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----

iii. 单击确定。

iv. 在错误的客户端CA证书的操作列，单击“删除”。

v. 在“删除CA证书”的弹窗中，单击确定。

h. 下载新的客户端配置文件。

i. 下载的客户端配置文件为“client_config.zip”。

j. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

k. 以记事本或Notepad++打开“client_config.ovpn”文件。

l. 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

m. 保存ovpn配置文件。

n. 打开OpenVPN客户端。

o. 导入新的客户端配置文件。

p. 使用客户端重新连接VPN网关。

2. 检查配置文件中的客户端证书和私钥是否匹配。

如果步骤1中导入的客户端CA证书是正确的，表示配置文件中的客户端证书和私钥不匹配。请参考以下步骤，重新复制客户端证书和私钥到客户端配置文件中。

a. 以记事本或Notepad++打开“client_config.ovpn”、“p2cclient.com.crt”和“p2cclient.com.key”文件。本示例中的客户端证书为“p2cclient.com.crt”，客户端私钥为“p2cclient.com.key”。

b. 将客户端证书和私钥复制到“client_config.ovpn”文件中。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：


```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

c. 保存ovpn配置文件。

d. 打开OpenVPN客户端。

e. 导入新的客户端配置文件。

f. 使用客户端重新连接VPN网关。

g. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

Linux系统，以**root**用户登录，打开命令行窗口。

h. 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.6 客户端日志显示“Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco”

适用的客户端

Linux

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco
```

可能原因

OpenVPN 2.5及以下版本的客户端软件，无法识别**disable-dco**配置项。

处理步骤

1. 在Windows系统，以记事本或Notepad++打开“client_config.conf”文件。
2. 注释“disable-dco”。
   a. 按**Ctrl+F**定位“disable-dco”参数的所在位置。
   b. 在参数所在行前输入**#**注释该行信息。

   ```
   .....
   .....
   # disable-dco
   .....
   .....
   ```
3. 保存conf配置文件。
4. 将conf配置文件用Xftp文件传输工具上传到Linux系统。本示例中上传至“/opt/”目录下。
5. 在Linux系统，执行以下命令，进入客户端配置文件所在目录。

   cd /opt/
6. 执行以下命令，启动OpenVPN客户端并连接VPN网关。

   openvpn --config /opt/openvpn_config_user-01.conf

   回显如下粗体信息，表示OpenVPN连接建立成功。

   ```
   2025-02-27 19:22:41 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
   2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
   2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
   ......
   ......
   ......
   2025-02-27 19:22:42 Initialization Sequence Completed
   ......
   ......
   ```
7. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

   说明

   XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

   回显如下信息，表示网络已通。

   ```
   64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
   64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
   64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
   64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
   64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
   64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
   ```

3.1.7 客户端日志显示“TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：


```
TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error
```

可能原因

- 客户端设备无法正常访问Internet网络。
- 现有客户端配置文件中的协议或端口与VPN网关的“服务端”页签中配置的不一致。

处理步骤

1. 在客户端设备上尝试访问其他Internet服务，查看网络是否正常。
   - 如果无法访问，请联系运营商排除网络问题。
   - 如果可以正常访问，请继续步骤2。
2. 登录管理控制台。
3. 在管理控制台左上角单击 图标，选择区域和项目。
4. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
5. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
6. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
7. 在服务端页签的基本信息中查看服务端ID，在高级配置中查看服务端的端口和协议。
8. 在客户端配置文件中查看“proto”和“remote”参数。示例如下：

   ```
   ......
   proto tcp    # 协议类型
   remote XXX.XX.XX.XX XXX    # 服务端公网IP和端口
   ......
   ```

   如果服务端和客户端配置文件信息不一致，请参考以下方式修改。
   - 方式1：修改服务端的信息。
     i. 在服务端配置页面，修改对应的信息。
     ii. 下载新的客户端配置文件。
     iii. 下载的客户端配置文件为“client_config.zip”。
     iv. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
     v. 解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
     vi. 以记事本或Notepad++打开“client_config.ovpn”文件。
     vii. 添加客户端证书及私钥。

     在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

     ```
     <cert>
     -----BEGIN CERTIFICATE-----
     此处添加客户端证书
     -----END CERTIFICATE-----
     </cert>

     <key>
     -----BEGIN PRIVATE KEY-----
     此处添加客户端私钥
     -----END PRIVATE KEY-----
     </key>
     ```

     viii. 保存ovpn配置文件。

- 方式2：修改客户端配置文件。
  i. 以记事本或Notepad++打开“client_config.ovpn”文件。
  ii. 修改客户端配置文件中对应的信息。
  iii. 保存ovpn配置文件。

9. 打开OpenVPN Connect客户端。
10. 导入新的客户端配置文件。
11. 使用客户端重新连接VPN网关。
12. Windows系统，按**Win+R**，输入cmd，打开命令窗口。
    Linux系统，以**root**用户登录，打开命令行窗口。
13. 执行以下命令，验证连通性。
    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

3.1.8 客户端日志显示“AUTH: Received control message: AUTH_FAILED”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
AUTH: Received control message: AUTH_FAILED
```

可能原因

- 如果用户配置了静态IP，用户只能建立1个客户端连接，其他的客户端连接会建连失败。
- 使用同一个用户名连续输入5次错误密码后，用户会被锁定。
- 用户名和用户密码不匹配。

处理步骤

1. 检查客户端是否配置了静态IP。
   a. 登录管理控制台。
   b. 在管理控制台左上角单击 图标，选择区域和项目。
   c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
   d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
   e. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
   f. 选择“用户管理 > 用户”，查看用户是否配置了静态IP。
      - 如果显示没有配置静态IP，请继续步骤2。
      - 如果显示已经配置了静态IP，表示当前正被其他用户占用，请断开客户端连接，重新连接。
2. 检查客户端是否因多次输入错误密码而被系统锁定。
   如果不是用户因为多次输入错误密码而被系统锁定，请继续步骤3。
   如果是用户在多次输入错误密码而被系统锁定，请5分钟后重新登录客户端。
3. 检查登录客户端使用的用户名和密码是否匹配。
   如果用户名和密码不匹配，请重置用户密码，使用新的密码登录客户端。如何重置用户密码，请参考以下步骤重置用户密码。
   a. 登录管理控制台。
   b. 在管理控制台左上角单击 图标，选择区域和项目。
   c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
   d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
   e. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
   f. 选择“用户管理 > 用户”，单击目标用户所在行操作列的“重置密码”。
   g. 填写新密码并确认新密码，单击确定。

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.9 客户端日志显示“AUTH_FAILED”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
AUTH_FAILED
```


可能原因

- 如果用户配置了静态IP，用户只能建立1个客户端连接，其他的客户端连接会建连失败。
- 使用同一个用户名连续输入5次错误密码后，用户会处于被锁定中。
- 用户名和用户密码不匹配。
- 客户端配置文件中的证书和私钥与VPN网关“服务端”页签中导入的客户端CA证书不匹配。

处理步骤

- 在口令认证的方式下，请参考以下步骤处理。
  a. 检查客户端是否配置了静态IP。
     i. 登录管理控制台。
     ii. 在管理控制台左上角单击 图标，选择区域和项目。
     iii. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
     iv. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
     v. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
     vi. 选择“用户管理 > 用户”，查看用户是否配置了静态IP。
        - 如果显示没有配置静态IP，请继续步骤2。
        - 如果显示已经配置了静态IP，表示当前正被其他用户占用，请断开客户端连接，重新连接。
  b. 检查客户端是否因多次输入错误密码而被系统锁定。
     如果不是用户因为多次输入错误密码而被系统锁定，请继续步骤3。
     如果是用户在多次输入错误密码而被系统锁定，请5分钟后重新登录客户端。
  c. 检查登录客户端使用的用户名和密码是否匹配。
     如果用户名和密码不匹配，请重置用户密码，使用新的密码登录客户端。如何重置用户密码，请参考以下步骤重置用户密码。
     i. 登录管理控制台。
     ii. 在管理控制台左上角单击 图标，选择区域和项目。
     iii. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
     iv. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
     v. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
     vi. 选择“用户管理 > 用户”，单击目标用户所在行操作列的“重置密码”。
     vii. 填写新密码并确认新密码，单击确定。
- 在证书认证的方式下，请参考以下步骤处理。
  a. 检查导入的客户端CA证书是否正确。
     i. 登录管理控制台。

ii. 在管理控制台左上角单击 图标，选择区域和项目。

iii. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

iv. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

v. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。

vi. 在服务端页签中，查看客户端CA证书的颁发者信息。

vii. 双击目标客户端CA证书，单击详细信息，查看颁发者信息。

如果两边的颁发者信息一致，请继续步骤2。

如果两边的颁发者信息不一致，请参考以下步骤，重新导入客户端CA证书。

1) 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证 ”，单击“上传CA证书”。

2) 根据界面提示填写相关信息。

表 3-2 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-xxxx
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** • 推荐使用强密码算法的证书，如RSA3072/4096。 • RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----

3) 单击确定。

4) 在错误的客户端CA证书的操作列，单击“删除”。

5) 在“删除CA证书”的弹窗中，单击确定。

6) 下载新的客户端配置文件。

7) 下载的客户端配置文件为“client_config.zip”。

8) 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

9) 以记事本或Notepad++打开“client_config.ovpn”文件。

10) 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
```



```
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

11) 保存ovpn配置文件。

12) 打开OpenVPN客户端。

13) 导入新的客户端配置文件。

14) 使用客户端重新连接VPN网关。

b. 检查配置文件中的客户端证书和私钥是否匹配。

如果配置文件中的证书和私钥不匹配，请重新复制客户端证书和私钥到客户端配置文件中。

i. 以记事本或Notepad++打开“client_config.ovpn”、客户端证书和客户端私钥文件。

ii. 将客户端证书和私钥复制到“client_config.ovpn”文件中。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

iii. 保存ovpn配置文件。

iv. 打开OpenVPN客户端。

v. 导入新的客户端配置文件。

vi. 使用客户端重新连接VPN网关。

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.10 客户端日志显示“error=unable to get issuer certificate: ”

适用的客户端

Windows OpenVPN GUI

故障现象

客户端连接时无法正常连接终端入云VPN网关。客户端日志中记录如下错误：

```
error=unable to get issuer certificate:
```

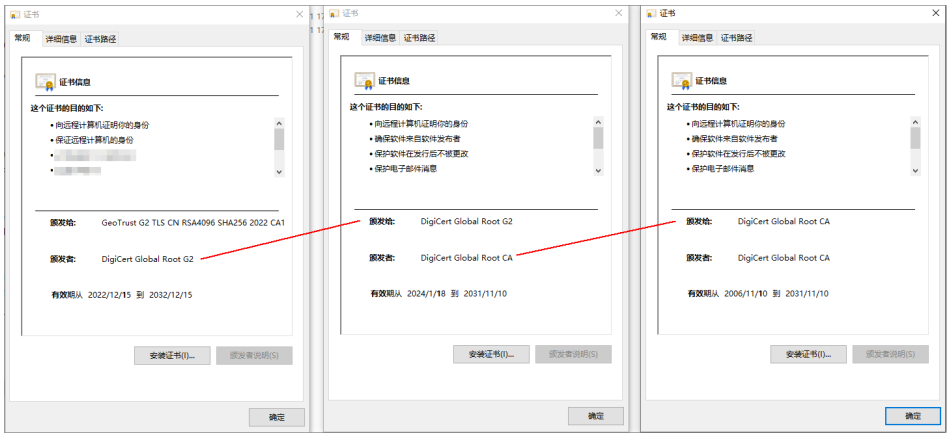

可能原因

服务端证书自带的证书链不完整，证书的颁发者和使用者未能形成完整的上下级关系，导致客户端无法认证配置文件中CA证书的有效性。

处理步骤

1. 以记事本或Notepad++打开“client_config.ovpn”文件。
2. 查看客户端配置文件中的CA证书数量。
3. 双击打开所有配置文件中的CA证书，单击“证书路径”，查看证书的颁发者和使用者是否能形成完整的上下级关系。
   - 如果最上级证书的颁发者和使用者是同一个，说明证书链完整，完整的证书链如**图 完整的CA证书链**。

     图 3-2 完整的 CA 证书链

   - 如果最上级证书的颁发者和使用者不是同一个，说明证书链不完整，请参考以下步骤补充证书链信息。

   a. 新建一个空白的记事本文件。
   b. 将“client_config.ovpn”中的CA证书内容复制粘贴到新的记事本文件中。证书内容如下：

      ```
      <ca>
      -----BEGIN CERTIFICATE-----
      CA证书
      -----END CERTIFICATE-----
      </ca>
      ```

   c. 保存新文件，并命名为“ca.crt”。
   d. 导出当前使用的CA证书的上级证书。
      i. 双击CA证书，单击“证书路径”，可以看到该证书的上级证书。
      ii. 选择上级证书，单击“查看证书”，会弹出上级证书的新窗口。
      iii. 在“详细信息”页签中，单击“复制到文件”。
      iv. 单击“下一步”。
      v. 选择“Base64编码”，单击“下一步”。
      vi. 输入文件名，如“root-ca.cer”。
      vii. 选择“下一步 > 完成”。

      如果配置文件中的CA证书有两个，需要将两个CA证书的上级证书都导出。

e. 将“root-ca.cer”上级证书的内容复制到客户端配置文件中。

i. 以记事本或Notepad++打开“root-ca.cer”和“client_config.ovpn”文件。

ii. 将上级证书内容复制粘贴到“client_config.ovpn”文件中的已有CA证书下面。

证书内容格式如下：

```
-----BEGIN CERTIFICATE-----
已有CA证书
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
上级CA证书
-----END CERTIFICATE-----
```

iii. 保存ovpn配置文件。

f. 打开OpenVPN客户端。

g. 导入新的客户端配置文件。

h. 使用客户端重新连接VPN网关。

i. 按**Win+R**，输入cmd，打开命令窗口。

j. 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.11 客户端日志显示“peer certificate verification failure”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
peer certificate verification failure
```

可能原因

- 服务端证书自带的证书链不完整，导致客户端无法认证配置文件中CA证书的有效性。
- 客户端配置中的CA证书链长度超过了3个。

处理步骤

1. 检查客户端配置中的CA证书链的长度是否过长。
   a. 以记事本或Notepad++打开“client_config.ovpn”文件。
   b. 查看客户端配置文件中的CA证书数量。
      - 如果CA证书的数量不超过3个，请继续步骤2。
      - 如果CA证书的数量超过3个，表示长度过长，需要重新生成CA证书。如何生成CA证书，请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。
   c. 登录管理控制台。
   d. 在管理控制台左上角单击 图标，选择区域和项目。
   e. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
   f. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
   g. 选择“终端入云VPN网关”页签，单击目标VPN网关操作列的“查看服务端”。
   h. 上传CA证书。
      i. 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证”，单击“上传CA证书”。
      ii. 根据界面提示填写相关信息。

      表 3-3 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-xxxx
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** • 推荐使用强密码算法的证书，如RSA3072/4096。 • RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----

      iii. 单击确定。
   i. 删除错误的CA证书。
      i. 在“服务端”界面，选择错误的客户端CA证书的操作列，单击“删除”。
      ii. 在“删除CA证书”的弹窗中，单击确定。
   j. 下载新的客户端配置文件。
      下载的客户端配置文件为“client_config.zip”。
   k. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

l. 以记事本或Notepad++打开“client_config.ovpn”文件。

m. 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

n. 保存ovpn配置文件。

o. 打开OpenVPN客户端。

p. 导入新的客户端配置文件。

q. 使用客户端重新连接VPN网关。

2. 检查服务端证书链是否完整。

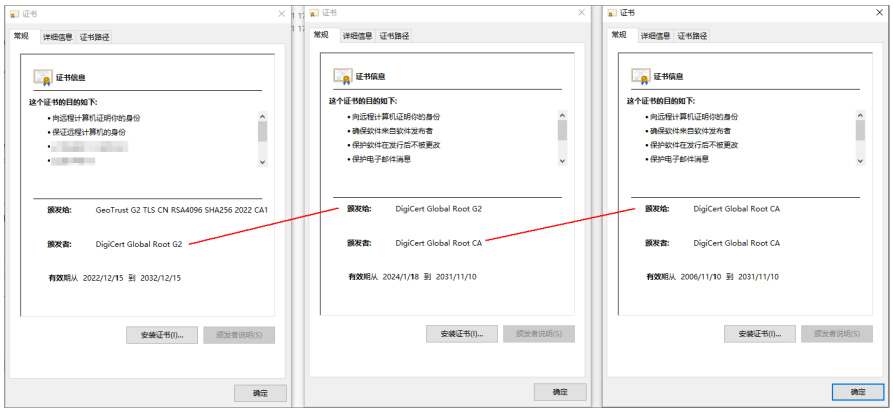
a. 以记事本或Notepad++打开“client_config.ovpn”文件。

b. 查看客户端配置文件中的CA证书数量。

c. 双击打开所有配置文件中的CA证书，单击“证书路径”，查看证书的颁发者和使用者是否能形成完整的上下级关系。

- 如果最上级证书的颁发者和使用者是同一个，说明证书链完整。完整的证书链如**图 完整的CA证书链**。

图 3-3 完整的 CA 证书链



- 如果最上级证书的颁发者和使用者不是同一个，说明证书链不完整，请参考以下步骤补充证书链信息。

i. 新建一个空白的记事本文件。

ii. 将“client_config.ovpn”中的CA证书内容复制粘贴到新的记事本文件中。证书内容如下：

```
<ca>
-----BEGIN CERTIFICATE-----
CA证书
```



```
-----END CERTIFICATE-----
</ca>
```

iii. 保存新文件，并命名为“ca.crt”。
iv. 双击CA证书，单击“证书路径”，可以看到该证书的上级证书。
v. 选择上级证书，单击“查看证书”，会弹出上级证书的新窗口。
vi. 在“详细信息”页签中，单击“复制到文件”。
vii. 单击“下一步”。
viii. 选择“Base64编码”，单击“下一步”。
ix. 输入文件名，如“root-ca.cer”。
x. 选择“下一步 > 完成”。

如果配置文件中的CA证书有两个，需要将两个CA证书的上级证书都导出。

xi. 以记事本或Notepad++打开“root-ca.cer”和“client_config.ovpn”文件。
xii. 将上级证书内容复制粘贴到“client_config.ovpn”文件中的已有CA证书下面。

证书内容格式如下：

```
-----BEGIN CERTIFICATE-----
已有CA证书
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
上级CA证书
-----END CERTIFICATE-----
```

xiii. 保存cer证书文件。
xiv. 打开OpenVPN客户端。
xv. 导入新的客户端配置文件。
xvi. 使用客户端重新连接VPN网关。
xvii. 按**Win+R**，输入cmd，打开命令窗口。
xviii. 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.12 客户端日志显示“error=path length constraint exceeded”

适用的客户端

Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
error=path length constraint exceeded
```

可能原因

客户端配置中的CA证书链长度超过了3个。

处理步骤

1. 重新生成CA证书。如何生成CA证书，请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。
2. 登录管理控制台。
3. 在管理控制台左上角单击 图标，选择区域和项目。
4. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
5. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
6. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
7. 上传CA证书。
   a. 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证 ”，单击“上传CA证书”。
   b. 根据界面提示填写相关信息。

      表 3-4 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-xxxx
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** • 推荐使用强密码算法的证书，如RSA3072/4096。 • RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----

   c. 单击确定。
8. 删除错误的CA证书。
   a. 在“服务端”界面，在错误的客户端CA证书的操作列，单击“删除”。
   b. 在“删除CA证书”的弹窗中，单击确定。
9. 下载新的客户端配置文件。
   下载的客户端配置文件为“client_config.zip”。

10. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
    解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
11. 以记事本或Notepad++打开“client_config.ovpn”文件。
12. 添加客户端证书及私钥。
    在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

13. 保存ovpn配置文件。
14. 打开OpenVPN客户端。
15. 导入新的客户端配置文件。
16. 使用客户端重新连接VPN网关。
17. 按**Win+R**，输入cmd，打开命令窗口。
18. 执行以下命令，验证连通性。
    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.13 客户端日志显示“Certificate does not have key usage extension”

适用的客户端

Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Certificate does not have key usage extension
```

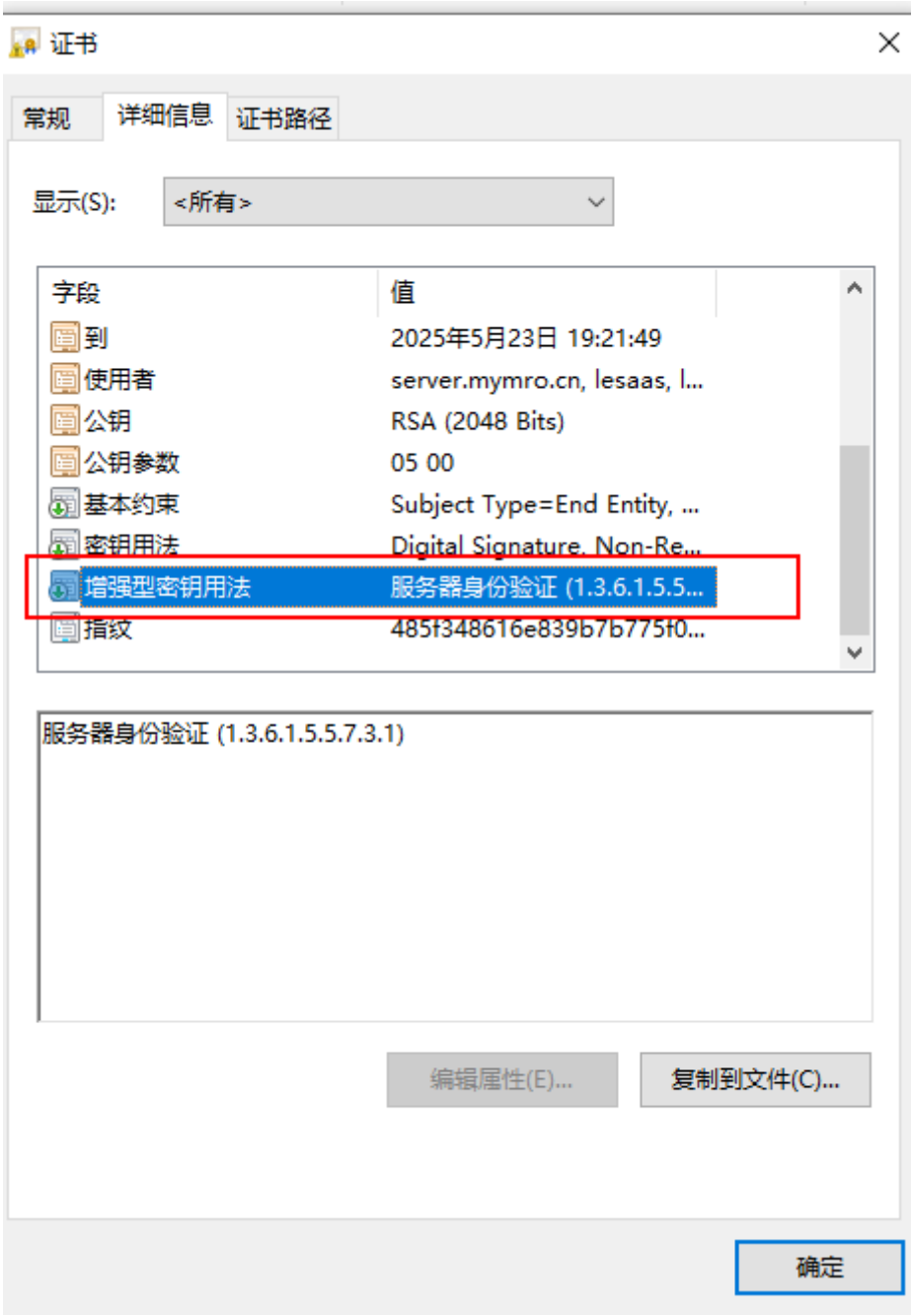
可能原因

VPN网关使用的服务端证书缺少“服务器身份验证”的扩展属性，导致验证失败。

处理步骤

1. 找到目标服务端证书，右键单击属性。
2. 单击“详细信息”，查看证书中是否包含“服务器身份验证”的值。如**图 服务端证书**所示。

图 3-4 服务端证书



如果证书中不包含“服务器身份验证”扩展属性，需要重新生成服务端证书。如何生成服务端证书，请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。

如果使用的服务端证书是OpenSSL自签发生成的，默认不携带此扩展属性。需要在OpenSSL配置文件中补充配置**extendedKeyUsage = serverAuth**。示例如下粗体：

```
.....
keyUsage = nonRepudiation，digitalSignature，keyEncipherment
extendedKeyUsage = serverAuth
.....
```

3. 登录管理控制台。
4. 在管理控制台左上角单击 图标，选择区域和项目。
5. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
6. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
7. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
8. 在VPN网关的“服务端”页签中，单击“更换”。
9. 在更换证书的弹窗中，单击“上传证书”。

   将新的服务端证书上传到CCM。如何上传服务端证书，请参考**上传服务端证书**。
10. 下载新的客户端配置文件。

    下载的客户端配置文件为“client_config.zip”。
11. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

    解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
12. 添加客户端证书及私钥。
    a. 以记事本或Notepad++打开“client_config.ovpn”文件。
    b. 在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

    ```
    <cert>
    -----BEGIN CERTIFICATE-----
    此处添加客户端证书
    -----END CERTIFICATE-----
    </cert>

    <key>
    -----BEGIN PRIVATE KEY-----
    此处添加客户端私钥
    -----END PRIVATE KEY-----
    </key>
    ```

    c. 保存ovpn配置文件。
13. 打开OpenVPN客户端。
14. 导入新的客户端配置文件。
15. 使用客户端重新连接VPN网关。
16. 按**Win+R**，输入cmd，打开命令窗口。
17. 执行以下命令，验证连通性。

    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

    ```
    64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
    64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
    ```



```
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.14 客户端日志显示“Error message: ovpnagent:request error”

适用的客户端

Windows OpenVPN Connect

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
Error message: ovpnagent:request error
```

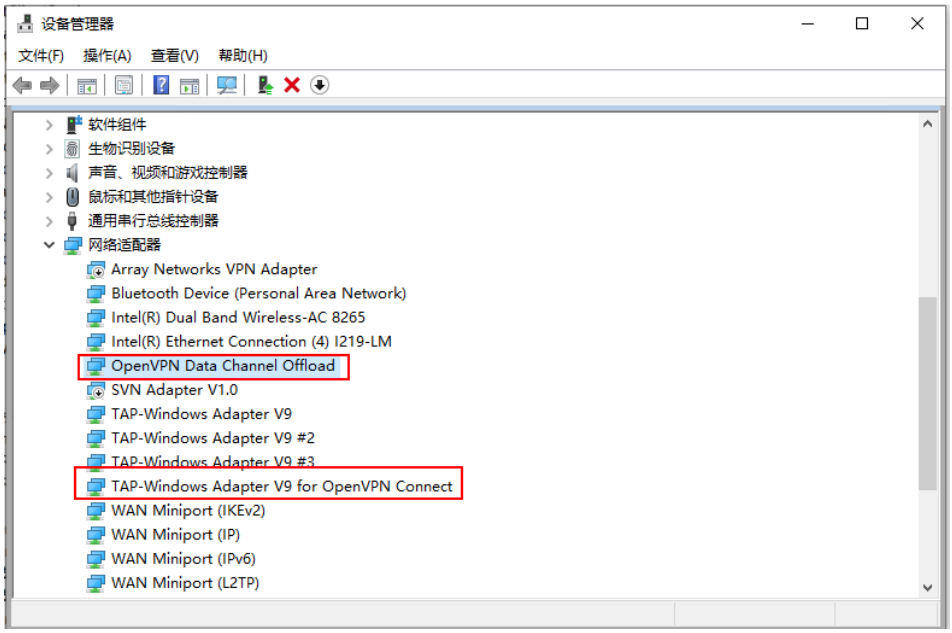
可能原因

OpenVPN客户端软件运行异常。

处理步骤

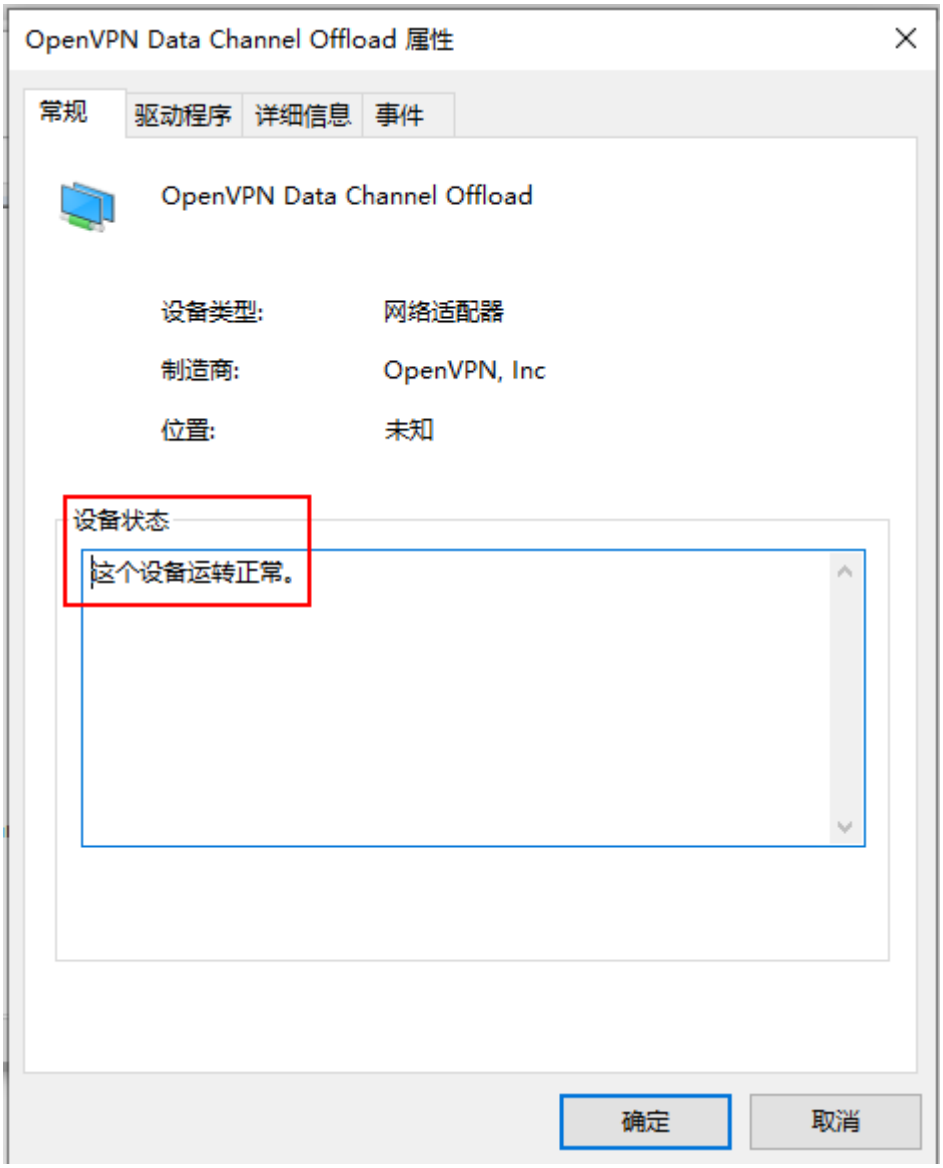
1. 检查OpenVpn网络适配器。
   a. 按**Win+R**键，输入**devmgmt.msc**，按回车，打开“设备管理器”。
   b. 选择“网络适配器”，找到“TAP-Windows Adapter V9 for OpenVPN Connect”和“OpenVPN Data Channel Offload”。如**图 设备管理器**所示。

图 3-5 设备管理器



c. 右键单击“属性”，查看设备状态是否运转正常。如图 查看设备状态所示。

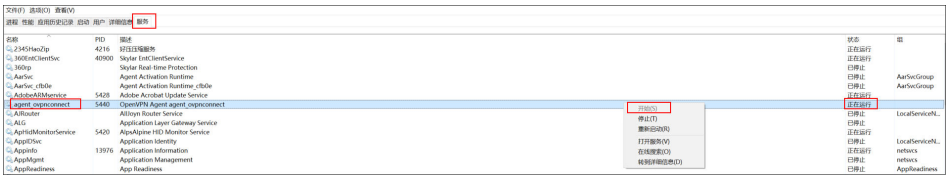
图 3-6 查看设备状态



如果运转不正常，需要卸载OpenVPN Connect，重新安装。

2. 检查"agent_ovpnconnect"服务是否正常运行。
   a. 在开始菜单栏中输入“任务管理器”，单击打开。
   b. 单击“服务”，找到“agent_ovpnconnect”服务。
   如果该服务状态为“已停止”，右键单击“开始”。如图 任务管理器所示。

图 3-7 任务管理器



3. 使用客户端重新连接。
4. 按**Win+R**，输入cmd，打开命令窗口。
5. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

   说明

   XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

   回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

3.1.15 客户端日志显示“X509::parse_pem: error in cert::error:0480006C:PEM routines::no start line”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
X509::parse_pem: error in cert::error:0480006C:PEM routines::no start line
```

可能原因

在证书认证的方式下，客户端配置文件中缺少客户端证书和私钥。

处理步骤

1. 重新生成客户端证书和私钥。如何生成证书，具体请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。本示例中生成客户端证书文件为“p2cclient.com.crt”，私钥文件为“p2cclient.com.key”。
2. 以记事本或Notepad++打开“p2cclient.com.crt”、“p2cclient.com.key”和“client_config.ovpn”文件。
3. 将重新生成的客户端证书和私钥复制粘贴到客户端配置文件。

   在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```


4. 保存ovpn配置文件。
5. 打开OpenVPN客户端。
6. 导入新的客户端配置文件。
7. 使用客户端重新连接VPN网关。
8. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

   Linux系统，以**root**用户登录，打开命令行窗口。
9. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

   说明

   XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

   回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

3.1.16 客户端日志显示“certReadError”

适用的客户端

- Linux
- Windows OpenVPN GUI

故障现象

客户端无法正常连接终端入云VPN网关，日志中记录如下错误：

```
certReadError
```

可能原因

在证书认证的方式下，客户端配置文件中缺少客户端证书和私钥。

处理步骤

1. 重新生成客户端证书和私钥。如何生成证书，具体请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。本示例中生成客户端证书文件为“p2cclient.com.crt”，私钥文件为“p2cclient.com.key”。
2. 以记事本或Notepad++打开“p2cclient.com.crt”、“p2cclient.com.key”和“client_config.ovpn”文件。
3. 将重新生成的客户端证书和私钥复制粘贴到客户端配置文件。

   在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：


```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

4. 保存ovpn配置文件。
5. 打开OpenVPN客户端。
6. 导入新的客户端配置文件。
7. 使用客户端重新连接VPN网关。
8. Windows系统，按**Win+R**，输入cmd，打开命令窗口。

   Linux系统，以**root**用户登录，打开命令行窗口。
9. 执行以下命令，验证连通性。

   ping XX.XX.XX.XX

   说明

   XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

   回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

说明

Linux系统需要将“client_config.conf”配置文件用“Xftp”文件传输工具上传到Linux系统，替换原有配置文件。具体操作请参考**配置客户端**。

3.1.17 客户端日志显示“OPTIONS ERROR:failed to negotiate cipher with server.Add the server's cipher('AES-XXX-GCM') to --data-ciphers(currently 'AES-XXX-GCM') if you want to connect to this server.”

适用的客户端

Windows OpenVPN GUI

故障现象

连接时报错，无法正常连接，客户端日志中记录如下错误：

```
OPTIONS ERROR:failed to negotiate cipher with server.Add the server's cipher('AES-XXX-GCM') to --data-ciphers(currently 'AES-XXX-GCM') if you want to connect to this server.    # AES-XXX-GCM为配置的加密算法，请根据实际配置判断
```

可能原因

客户端加密套件与服务端不匹配。

处理步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
6. 在服务端页签的高级配置中查看服务端加密算法和认证算法。
7. 在客户端配置文件中查看“data-ciphers”和“auth”参数。示例如下：

   ```
   ......
   data-ciphers AES-XXX-GCM     # 加密算法
   auth SHAXXX     # 认证算法
   ......
   ```

   如果服务端和客户端配置文件信息不一致，请参考以下方式修改。

   - 方式1：修改服务端的加密算法。
     i. 在服务端配置页面，单击“高级配置”右侧的按钮，修改加密算法。
     ii. 下载新的客户端配置文件。
     下载的客户端配置文件为“client_config.zip”。
     iii. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
     解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
     iv. 以记事本或Notepad++打开“client_config.ovpn”文件。
     v. 添加客户端证书及私钥。
     在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

     ```
     <cert>
     -----BEGIN CERTIFICATE-----
     此处添加客户端证书
     -----END CERTIFICATE-----
     </cert>

     <key>
     -----BEGIN PRIVATE KEY-----
     此处添加客户端私钥
     -----END PRIVATE KEY-----
     </key>
     ```

     vi. 保存ovpn配置文件。
   - 方式2：修改客户端配置文件。
     i. 以记事本或Notepad++打开“client_config.ovpn”文件。
     ii. 修改“data-ciphers”和“auth”参数参数。

     ```
     ......
     data-ciphers AES-XXX-GCM     # 配置的加密算法需要与服务端的加密算法保持一致
     auth SHAXXX          # 配置的认证算法需要与服务端的认证算法保持一致
     ......
     ```


iii. 保存ovpn配置文件。

8. 打开OpenVPN Connect客户端。
9. 导入新的客户端配置文件。
10. 使用客户端重新连接VPN网关。
11. 按**Win+R**，输入cmd，打开命令窗口。
12. 执行以下命令，验证连通性。

    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请提交工单联系华为工程师。

3.1.18 客户端日志显示“Session invalidated: DECRYPT_ERROR”

适用的客户端

Windows OpenVPN Connect

故障现象

连接时显示连接成功，但是1s内会立刻断连，不断重复上述过程，客户端日志中记录如下错误：

```
Session invalidated: DECRYPT_ERROR
```

可能原因

客户端加密套件与服务端不匹配。

处理步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。
6. 在服务端页签的高级配置中查看服务端加密算法和认证算法。
7. 在客户端配置文件中查看“data-ciphers”和“auth”参数。示例如下：

```
.....
data-ciphers AES-XXX-GCM     #加密算法
auth SHAXXX     #认证算法
.....
```


如果服务端和客户端配置文件信息不一致，请参考以下方式修改。

- 方式1：修改服务端的加密算法。
  i. 在服务端配置页面，单击“高级配置”右侧的按钮，修改加密算法。
  ii. 下载新的客户端配置文件。
  下载的客户端配置文件为“client_config.zip”。
  iii. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
  解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
  iv. 以记事本或Notepad++打开“client_config.ovpn”文件。
  v. 添加客户端证书及私钥。
  在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

  vi. 保存ovpn配置文件。
- 方式2：修改客户端配置文件。
  i. 以记事本或Notepad++打开“client_config.ovpn”文件。
  ii. 修改“data-ciphers”和“auth”参数。

```
......
data-ciphers AES-XXX-GCM      # 配置的加密算法需要与服务端的加密算法保持一致
auth SHAXXX          # 配置的认证算法需要与服务端的认证算法保持一致
......
```

  iii. 保存ovpn配置文件。

8. 打开OpenVPN Connect客户端。
9. 导入新的客户端配置文件。
10. 使用客户端重新连接VPN网关。
11. 按**Win+R**，输入cmd，打开命令窗口。
12. 执行以下命令，验证连通性。
    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.1.19 客户端日志显示“Unrecognized option or missing or extra parameter(s) in xxx.ovpn:108: data-ciphers (2.4.12)”

适用的客户端

Linux

故障现象

连接时报错，无法正常连接，客户端日志中记录如下错误：

```
Unrecognized option or missing or extra parameter(s) in xxx.ovpn:108: data-ciphers (2.4.12)
```

可能原因

OpenVPN 2.4.12 版本的客户端软件，无法识别**data-ciphers**和“disable-dco”配置项。

处理步骤

1. 在Windows系统，登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。
6. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

   解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
7. 以记事本或Notepad++打开“client_config.conf”文件。
8. 配置客户端配置文件。
   a. 添加客户端证书及私钥。

      在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。示例如下：

      ```
      <cert>
      -----BEGIN CERTIFICATE-----
      此处添加客户端证书
      -----END CERTIFICATE-----
      </cert>

      <key>
      -----BEGIN PRIVATE KEY-----
      此处添加客户端私钥
      -----END PRIVATE KEY-----
      </key>
      ```

   b. 在**data-ciphers**和“disable-dco”参数所在行前输入**#**注释该行信息。

      ```
      ......
      ......
      # data-ciphers AES-XXX-XXX
      ......
      ......
      # disable-dco
      ```

```
.....
.....
```

9. 保存conf配置文件。
10. 将conf配置文件用Xftp文件传输工具上传到Linux系统。本示例中上传至“/opt/”目录下。
11. 在Linux系统，执行以下命令，进入客户端配置文件所在目录。

    cd /opt/
12. 执行以下命令，启动OpenVPN客户端并连接VPN网关。

    openvpn --config /opt/openvpn_config_user-01.conf

    回显如下粗体信息，表示OpenVPN连接建立成功。

```
2025-02-27 19:22:41 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
.....
.....
.....
2025-02-27 19:22:42 Initialization Sequence Completed
.....
.....
```

13. 执行以下命令，验证连通性。

    ping XX.XX.XX.XX

    说明

    XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

    回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

3.1.20 使用联邦认证登录客户端时，浏览器页面显示“错误信息：用户缺少 vpn:system:loginP2cVpnBySSO 权限，请联系管理员添加。”

故障现象

用户使用联邦认证登录客户端时，浏览器连接显示认证失败。

错误信息：用户缺少vpn:system:loginP2cVpnBySSO权限，请联系管理员添加。

可能原因

当前登录的用户缺少vpn:system:loginP2cVpnBySSO权限。

处理步骤

请联系管理员添加“VPN SSOAccessPolicy”权限。具体步骤如下：

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤4 在左侧导航栏，单击“用户组”。

步骤5 选择目标用户组，单击操作列的“授权”。

步骤6 在右上方搜索“VPN SSOAccessPolicy”，勾选该权限。

步骤7 单击“下一步”，根据实际情况选择授权范围方案。

步骤8 单击“确定”。

----结束

3.2 客户端连接成功，业务无法正常使用

3.2.1 客户端无法 ping 通 ECS 的私网 IP 地址

故障现象

客户端正常连接终端入云VPN网关，但不能ping通需要访问的ECS的私网IP地址。

可能原因

- 客户端设备或ECS禁止ping探测。
- ECS安全组禁止ping探测。
- VPN网关本端网段未包含需要访问的ECS的私网IP地址。
- 没有配置用户所属用户组，或者用户组没有配置对应访问策略。
- 当用户修改指定IP，客户端自动重连后，Windows系统的路由表中未生成目的地为本端子网的路由。

处理步骤

1. 确认客户端设备和ECS的访问控制策略是否禁止ping探测。
   如果禁止，请修改策略放通ping探测。Windows操作系统还需要修改防火墙的入站规则，允许ICMPv4-In。
2. 确认ECS安全组的出方向和入方向规则都放通ICMP。
3. 确认本端网段包含需要访问的ECS的私网IP地址。
   a. 在VPN网关的“服务端”页签中修改本端网段。
   b. 断开客户端连接，重新接入。
   c. 查看客户端设备是否可以接收到VPN网关推送的路由。
      - Windows：使用**route print**命令。
      - Linux：使用**ip route show all**命令。
4. 确认用户管理中已经配置用户所属用户组和访问策略。
   访问策略的目的网段中需要包含被访问的ECS的私网IP地址。

5. 服务端配置的本端网段和客户端地址池需要符合以下规则。
   - 本端网段为192.168.1.XX。
   - 客户端地址池为172.16.0.0。
6. 在客户端系统上查看本端网段对应的路由是否生成。
   - 如果生成对应的路由，客户端分配到的IP为172.16.0.5。

     回显信息如下：

     ```
     IPv4 路由表
     ===========================================================================
     活动路由:
     网络目标        网络掩码          网关       接口   跃点数
         192.168.1.XX   255.255.255.0         172.16.0.0     172.16.0.5    281
         192.168.2.XX   255.255.255.0         172.16.0.0     172.16.0.5    281
         192.168.3.XX   255.255.255.0         172.16.0.0     172.16.0.5    281
     ===========================================================================
     ```

   - 如果未生成对应的路由，请断开客户端连接，重新接入。

   如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

3.2.2 客户端业务访问过程中出现丢包

故障现象

客户端正常连接终端入云VPN网关，但业务访问过程中出现丢包。

可能原因

- 业务流量有突发或持续超过VPN网关实例的带宽规格。
- VPN网关绑定的EIP带宽不足。
- Internet网络质量不佳。

处理步骤

1. 在VPN网关列表页跳转到流量监控视图，确认流量是否突发或持续接近VPN网关的带宽规格。
2. 在VPN网关的“基本信息”页面查看EIP带宽大小，并结合流量监控视图，排查是否超过EIP的带宽规格。

   如果因EIP带宽规格偏小导致流量超限，请修改EIP的带宽。
3. 通过在客户端ping VPN网关的公网IP地址探测公网链路质量。

   若探测结果不佳，请联系运营商进行网络问题排查。

3.2.3 客户端流量不通，且连接时有报错

适用的客户端

OpenVPN GUI

故障现象

客户端成功连接，无法ping通ECS的IP地址，当关闭OpenVpn GUI客户端，重新打开时，有"OPENVPNServiceInteractive" is not started. 的提示信息。日志中记录如下错误：


```
ERROR: route addition failed using CreateIpForwardEntry: 拒绝访问
```

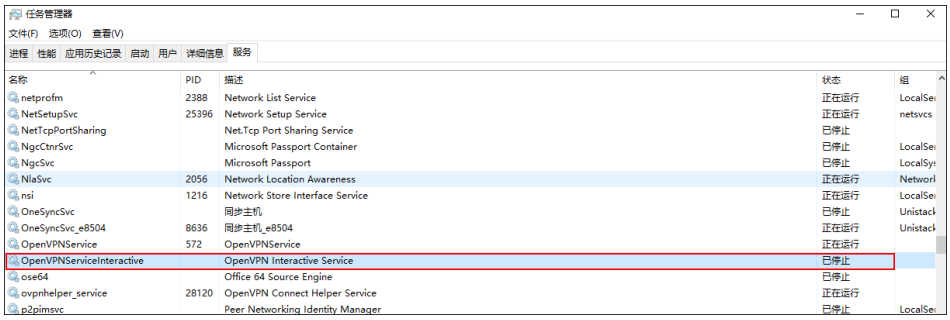
可能原因

OpenVPN客户端软件运行有问题。

处理步骤

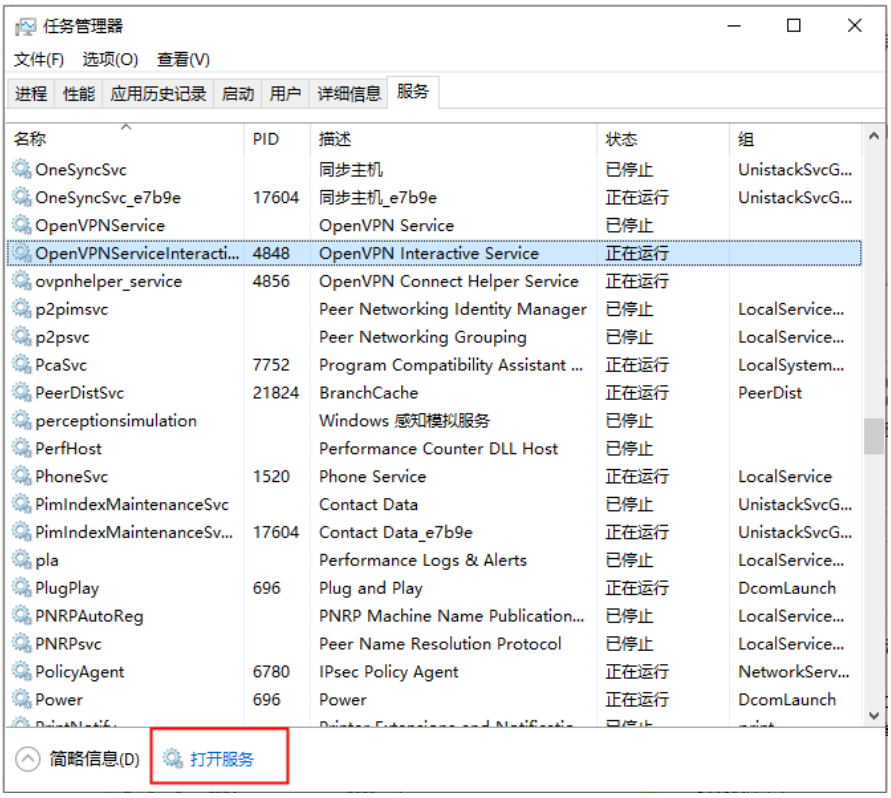
1. 在开始菜单栏中输入“任务管理器”，单击打开。
2. 单击“服务”，找到OPENVPNServiceInteractive服务，查看运行状态。如图 任务管理器所示。

图 3-8 任务管理器



- 如果状态是正在运行，请继续步骤3。
- 如果状态是已停止，请参考以下步骤，修改该服务的启动类型。
  i. 右键单击该服务的“开始”，运行服务。
  ii. 单击任务管理器下方的“打开服务”。如图 打开服务所示。

图 3-9 打开服务



iii. 找到“OpenVPN Interactive Service”服务，右键单击“属性”。

iv. 将该服务的“启动类型”修改为“自动”。如图 修改启动类型所示。

图 3-10 修改启动类型

v. 单击确定。

3. 将OpenVpn GUI客户端断开，重新连接。

