阿里云
VPN网关

SSL-VPN入门

文档版本：20200428

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击**设置** > **网络** > **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid Instance_ID
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig [-all|-t]
{}或者{a|b}	表示必选项，至多选择一个。	switch {active|stand}

目录

1 教程概述

本教程为您介绍如何通过SSL-VPN功能远程接入VPC。

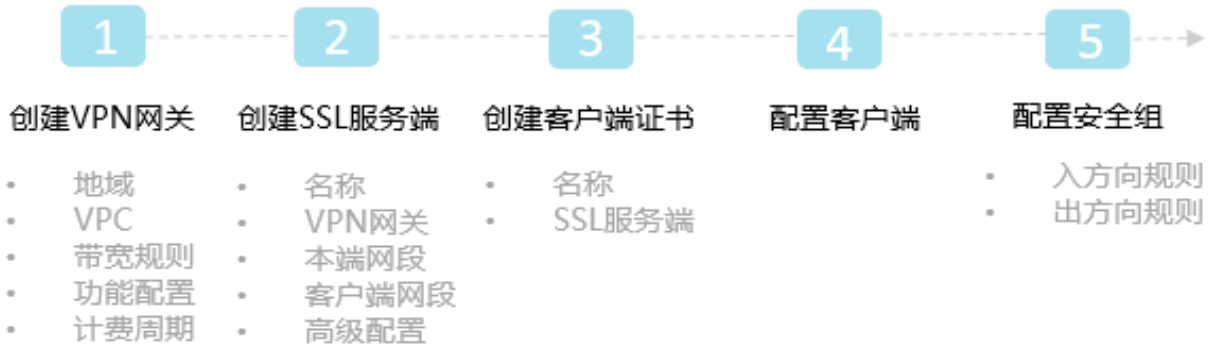
前提条件

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

配置流程说明

通过SSL-VPN功能远程接入VPC的流程图如下：



1. 创建VPN网关

   创建VPN网关并开启SSL-VPN功能。

2. 创建SSL服务端

   在SSL服务端中指定要连接的IP地址段和客户端连接时使用的IP地址段。

3. 创建客户端证书

   根据服务端配置，创建客户端证书，下载客户端证书和配置。

4. 配置客户端

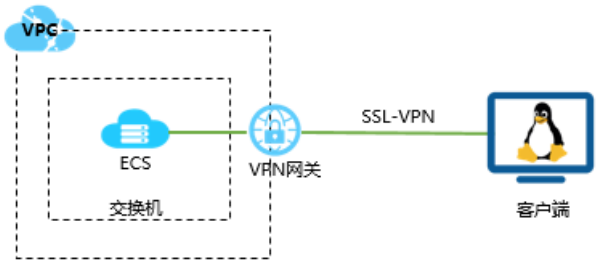
   在客户端中下载安装客户端VPN软件，加载客户端证书和配置，发起连接即可。

5. 配置安全组

   确保ECS的安全组规则允许客户端访问。

2 Linux客户端远程连接

本文以Linux操作系统的客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

步骤一：创建VPN网关

完成以下操作，创建用户网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**VPN** > **VPN网关** 。
3. 在VPN网关页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域**：选择VPN网关的地域。

> **说明：**

确保VPC的地域和VPN网关的地域相同。

- **VPC**： 选择要连接的VPC。
- **带宽规格**：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
- **IPsec-VPN**： 选择是否开启IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。
- **SSL-VPN**： 选择开启SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。
- **SSL连接数**： 选择您需要同时连接的客户端最大规格。

说明:
本选项只有在选择开启了SSL-VPN功能后才可配置。

- **计费周期**：选择购买时长。

5. 返回VPN网关页面，查看创建的VPN网关。

刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明VPN网关完成了初始化，可以正常使用了。

说明:
VPN网关的创建一般需要1-5分钟。

步骤二：创建SSL服务端

完成以下操作，创建SSL服务端。

1. 在左侧导航栏，单击**VPN** > **SSL服务端**。
2. 选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**。
4. 在**创建SSL服务端**页面，根据以下信息配置SSL服务端，然后单击**确定**。

- **名称**：输入SSL服务端的名称。
- **VPN网关**：选择已创建的VPN网关。
- **本端网段**：以CIDR地址块的形式输入要连接的网络。单击**添加本端网段**添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
- **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。
- **高级配置**：使用默认高级配置。

步骤三：创建并下载SSL客户端证书

1. 在左侧导航栏，单击**VPN** > **SSL客户端**。

2. 选择SSL客户端的地域。
3. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
4. 在**创建客户端证书**页面，输入客户端证书名称并选择对应的SSL服务端，然后单击**确定**。
5. 在**SSL客户端**页面，找到已创建的客户端证书，然后单击**操作**列下的**下载**。

步骤四：客户端配置

完成以下操作，配置Linux客户端。

1. 执行以下命令安装OpenVPN客户端。

```
yum install -y openvpn
```

2. 将步骤三中下载的证书解压拷贝到/etc/openvpn/conf/目录。
3. 执行以下命令启动Openvpn客户端软件。

```
openvpn --config /etc/openvpn/conf/config.ovpn --daemon
```

步骤五：连接测试

在客户端**ping**已连接的VPC内的一台ECS实例，测试连通性。

说明：

确保测试的ECS实例的安全组规则允许客户端远程连接。详细信息，请参见#unique_5。

3 linux客户端远程连接（双因子认证）

本文以Linux客户端为例介绍如何通过SSL-VPN双因子认证后接入专有网络VPC。

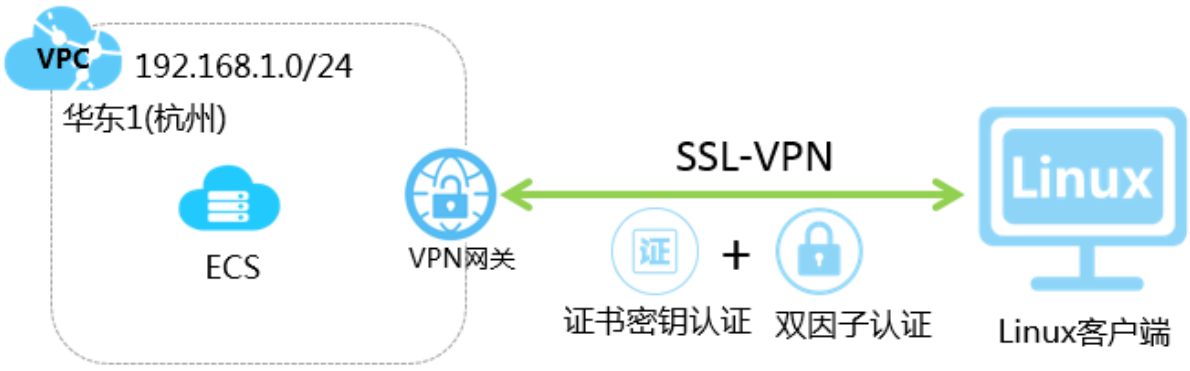
前提条件

开始前，请确保满足以下条件：

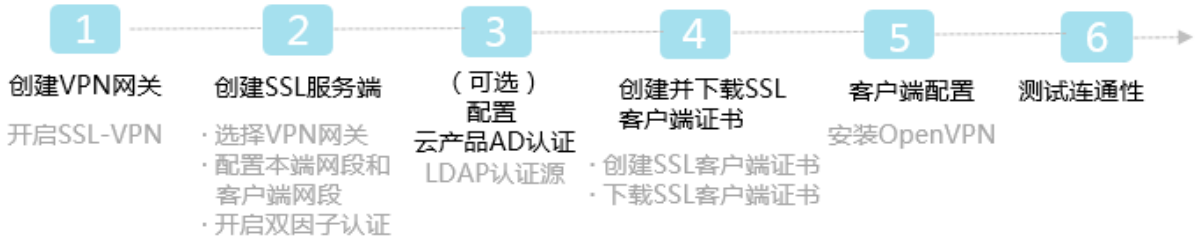
- 您已经购买了应用身份服务（IDaaS）实例，并且已经在阿里云上维护了IDaaS的用户信息。详细信息，请参见#unique_7。
- 您已经创建了专有网络。详细信息，请参见#unique_8。

背景信息

某公司在华东1（杭州）地域创建了专有网络VPC，出差员工通过SSL-VPN接入云上VPC。公司为了数据安全和集中管理，开启了SSL服务端双因子认证，SSL拨号客户端不仅要完成证书认证，在启动OpenVPN后还需要用户名和密码认证，认证通过后才可以访问云上资源。



配置流程



步骤一：创建VPN网关

VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络安全可靠的连接。

> **说明:**
> 请确保您的VPN网关是2020年3月5日00时00分之后创建的，否则不支持双因子认证功能。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**VPN** > **VPN网关** 。
3. 在**VPN网关**页面，单击**创建VPN网关**。
4. 在VPN网关的购买页面，根据以下信息配置VPN网关，然后单击**立即购买**完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域**：选择VPN网关的地域。 本示例选择**华东1（杭州）**。

     > **说明:**
     > 确保VPC的地域和VPN网关的地域相同。
   - **VPC**： 选择要连接的VPC。
   - **带宽规格**：选择VPN网关的带宽规格，带宽规格是VPN网关所具备的公网带宽。本示例选择**5Mbps**。
   - **IPsec-VPN**： 选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**关闭**。
   - **SSL-VPN**： 选择开启或关闭SSL-VPN功能，SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。本示例选择**开启**。
   - **SSL连接数**： 选择您需要同时连接的客户端最大规格。 本示例选择**5**。

     > **说明:**
     > 本选项只有在选择开启了SSL-VPN功能后才可配置。
   - **计费周期**：选择购买时长。

步骤二：创建SSL服务端

SSL-VPN基于OpenVPN架构，您需要通过SSL-VPN服务端来指定要连接的IP地址段和客户端连接时使用的IP地址段，并开启双因子认证。

1. 在左侧导航栏，单击**VPN** > **SSL服务端**。
2. 在顶部状态栏处，选择SSL服务端的地域。

   本示例选择**华东1（杭州）**。
3. 在**SSL服务端**页面，单击**创建SSL服务端**。

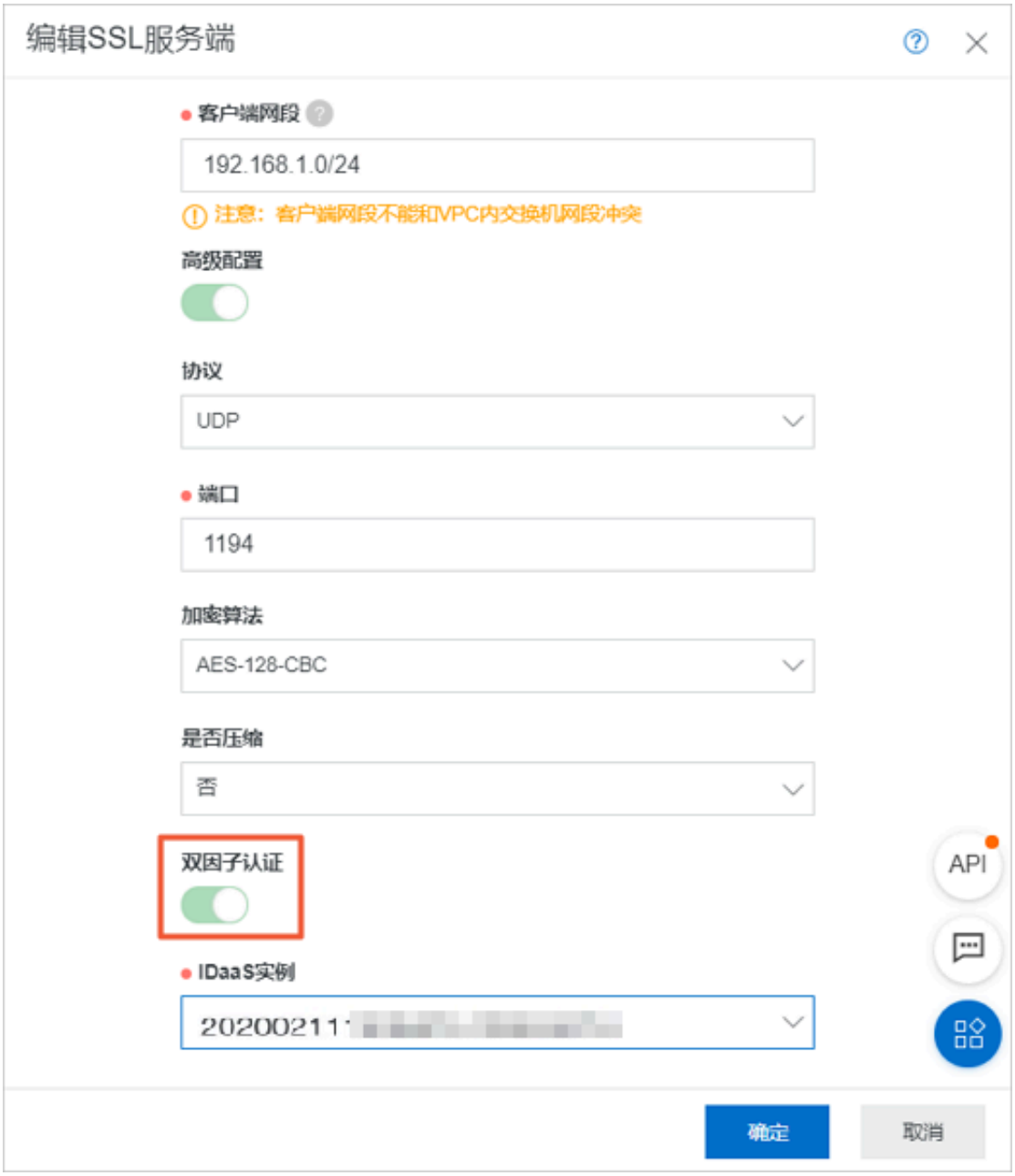
4. 在**创建SSL服务端**对话框，根据以下信息配置SSL服务端，然后单击**确定**。

   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入客户端通过SSL-VPN连接要访问的网段。本示例输入**192.168.1.0/24**。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。本示例输入**10.10.10.0/24**。
   - **高级配置**：打开高级配置，并完成以下配置。
     - **协议**：选择SSL连接使用的协议，支持UDP和TCP。本示例使用默认配置。
     - **端口**：SSL连接使用的端口。本示例使用默认配置。
     - **加密算法**：SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。本示例使用默认配置。
     - **是否压缩**：是否对传输数据进行压缩处理。本示例使用默认配置。
     - **双因子认证**：打开双因子认证，然后选择IDaaS实例。

       阿里云云盾应用身份服务IDaaS（Alibaba Cloud Identity as a Service）致力于统一身份认证领域，实现一个账号打通所有应用服务。开启并选择IDaaS实例后，SSL拨号客户端不仅要完成证书密钥认证，在启动OpenVPN后还需要用户名和密码的认证，认证通过后才可以访问云上资源，减少SSL-VPN登录认证风险。

       说明：

如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。



（可选）步骤三：配置云产品AD认证

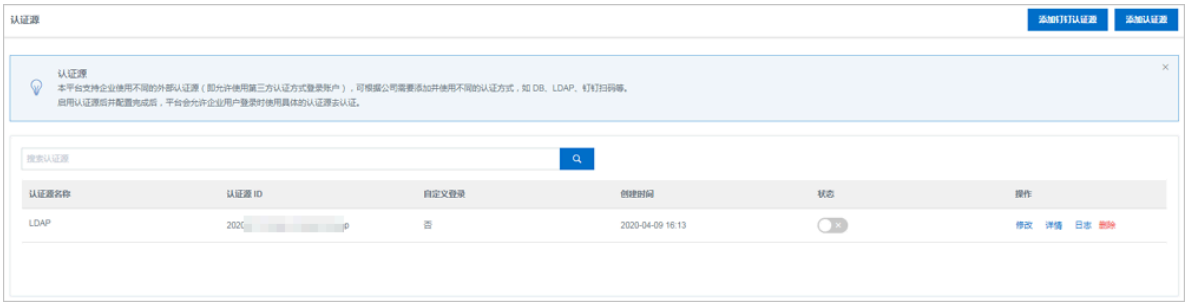
双因子认证默认支持使用IDaaS的用户名和密码进行认证，您可以选择配置AD认证。配置成功后，SSL-VPN具备AD认证能力。如果您仅需要使用IDaaS的用户名和密码进行认证，请忽略该步骤。

1. 以IT管理员账号登录云盾IDaaS管理控制台。
2. 在**实例列表**页面，找到目标IDaaS实例，单击**操作**列下的**管理**。
3. 在左侧导航栏，单击**认证** > **认证源**，然后单击**添加认证源**。
4. 在**添加认证源**页面，找到**LDAP**，单击其**操作**列下的**添加认证源**。

5. 在**添加认证源（LDAP）**页面，创建LDAP认证源。

   详细信息，请参见#unique_9。

   认证源创建成功后，您可以查看创建的认证源。



6. 在**认证源**页面，找到目标认证源，单击其**状态**列下的 图标，然后在弹出的对话框中，单击**确定**。

7. 在左侧导航栏，单击**设置** > **安全设置**。

8. 在**安全设置**页面，单击**云产品AD认证**页签。

9. 选择创建的AD认证源，启用该功能并单击**保存配置**。

步骤四：创建并下载SSL客户端证书

根据SSL服务端配置，创建并下载SSL客户端证书。

1. 在左侧导航栏，单击**VPN** > **SSL客户端**。

2. 在顶部状态栏处，选择SSL客户端的地域。

   本示例选择**华东1（杭州）**。

3. 在**SSL客户端**页面，单击**创建SSL客户端证书**。

4. 在**创建SSL客户端证书**对话框，根据以下信息配置SSL客户端证书，然后单击**确定**。

   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。

5. 在**SSL客户端**页面，找到已创建的SSL客户端证书，然后单击**操作**列下的**下载**。

   SSL客户端证书会下载到本地。

步骤五：客户端配置

完成以下操作，配置Linux客户端。

1. 执行以下命令安装OpenVPN客户端。

   ```
   yum install -y openvpn
   ```

2. 将步骤三中下载的证书解压拷贝到/etc/openvpn/conf/目录。

3. 执行以下命令启动Openvpn客户端软件，并完成用户名密码验证。

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```

   ```
   [root@iZ8ps[redacted] conf]# openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   Enter Auth Username: dgtt
   Enter Auth Password: **********
   ```

步骤六：测试连通性

完成以下操作，测试Linux客户端与云上VPC的连通性。

1. 登录Linux客户端。

2. 通过ping命令ping VPC下的ECS实例的IP地址，验证通信是否正常。

   说明：

   请确保测试的ECS实例的安全组规则允许Linux客户端远程连接。详细信息，请参见#unique_5。

   经测试，Linux客户端可以正常访问ECS实例。

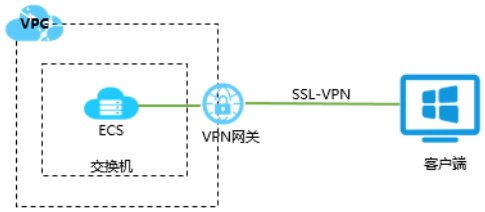
   ```
   C:\Users\25513>ping 192.[redacted].1

   Pinging 192.[redacted].1 with 32 bytes of data:
   Reply from 192.[redacted].1: bytes=32 time=4ms TTL=64
   Reply from 192.[redacted].1: bytes=32 time=4ms TTL=64
   Reply from 192.[redacted].1: bytes=32 time=22ms TTL=64
   Reply from 192.[redacted].1: bytes=32 time=11ms TTL=64

   Ping statistics for 192.[redacted].1:
       Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
       Minimum = 4ms, Maximum = 22ms, Average = 10ms
   ```

4 Windows客户端远程连接

本文以Windows操作系统的客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

步骤一：创建VPN网关

完成以下操作，创建用户网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**VPN** > **VPN网关** 。
3. 在VPN网关页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域**：选择VPN网关的地域。

     说明：
     确保VPC的地域和VPN网关的地域相同。
   - **VPC**： 选择要连接的VPC。
   - **带宽规格**：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
   - **IPsec-VPN**： 选择是否开启IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。
   - **SSL-VPN**： 选择开启SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。
   - **SSL连接数**： 选择您需要同时连接的客户端最大规格。

     说明：

本选项只有在选择开启了SSL-VPN功能后才可配置。

- **计费周期**：选择购买时长。

5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明VPN网关完成了初始化，可以正常使用了。

   说明：
   VPN网关的创建一般需要1-5分钟。

步骤二：创建SSL服务端

完成以下操作，创建SSL服务端。

1. 在左侧导航栏，单击**VPN** > **SSL服务端**。
2. 选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**。
4. 在**创建SSL服务端**页面，根据以下信息配置SSL服务端，然后单击**确定**。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择已创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入要连接的网络。单击**添加本端网段**添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。
   - **高级配置**：使用默认高级配置。

步骤三：创建并下载SSL客户端证书

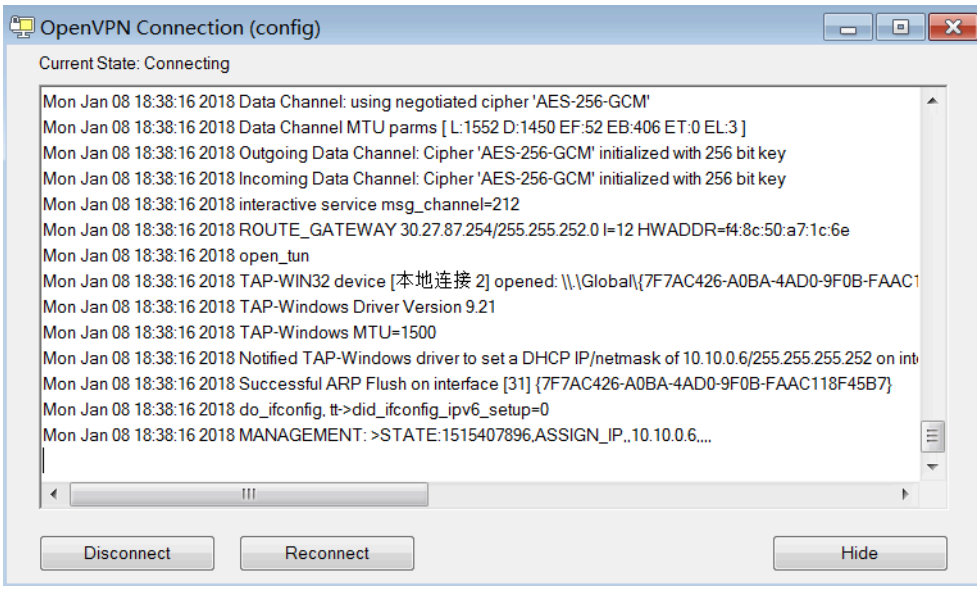
1. 在左侧导航栏，单击**VPN** > **SSL客户端**。
2. 选择SSL客户端的地域。
3. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
4. 在**创建客户端证书**页面，输入客户端证书名称并选择对应的SSL服务端，然后单击**确定**。
5. 在**SSL客户端**页面，找到已创建的客户端证书，然后单击**操作**列下的**下载**。

步骤四：客户端配置

完成以下操作，配置Windows客户端。

注意：
需要以管理员身份运行客户端。

1. 下载并安装OpenVPN客户端。
2. 将步骤三中下载的证书解压后复制到OpenVPN安装目录中的config文件夹中。
3. 单击**Connect**发起连接。



步骤五：连接测试

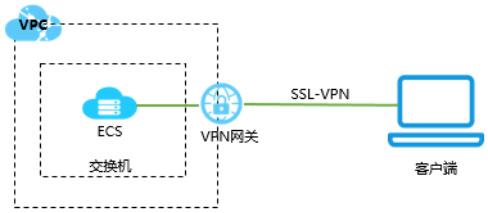
在客户端**ping**已连接的VPC内的一台ECS实例，测试连通性。

说明：

确保测试的ECS实例的安全组规则允许客户端远程连接。详细信息，请参见#unique_5。

5 Mac客户端远程连接

本文以Mac客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

步骤一：创建VPN网关

完成以下操作，创建用户网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击**VPN** > **VPN网关** 。
3. 在VPN网关页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域**：选择VPN网关的地域。

     说明:
     确保VPC的地域和VPN网关的地域相同。
   - **VPC**： 选择要连接的VPC。
   - **带宽规格**：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
   - **IPsec-VPN**： 选择是否开启IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。
   - **SSL-VPN**： 选择开启SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。
   - **SSL连接数**： 选择您需要同时连接的客户端最大规格。

     说明:

本选项只有在选择开启了SSL-VPN功能后才可配置。

- **计费周期**：选择购买时长。

5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明VPN网关完成了初始化，可以正常使用了。

   说明：
   VPN网关的创建一般需要1-5分钟。

步骤二：创建SSL服务端

完成以下操作，创建SSL服务端。

1. 在左侧导航栏，单击**VPN** > **SSL服务端**。
2. 选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**。
4. 在**创建SSL服务端**页面，根据以下信息配置SSL服务端，然后单击**确定**。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择已创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入要连接的网络。单击**添加本端网段**添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。
   - **高级配置**：使用默认高级配置。

步骤三：创建并下载SSL客户端证书

1. 在左侧导航栏，单击**VPN** > **SSL客户端**。
2. 选择SSL客户端的地域。
3. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
4. 在**创建客户端证书**页面，输入客户端证书名称并选择对应的SSL服务端，然后单击**确定**。
5. 在**SSL客户端**页面，找到已创建的客户端证书，然后单击**操作**列下的**下载**。

步骤四：客户端配置

完成以下操作，配置Mac客户端。

1. 执行以下命令安装OpenVPN客户端。

```
brew install openvpn
```

> **说明:**
> 如果尚未安装homebrew，先安装homebrew。

2. 将步骤三中下载的证书解压拷贝到配置目录并建立连接：

   a. 备份默认配置文件。

   b. 执行以下命令删除默认配置文件：

   ```
   rm /usr/local/etc/openvpn/*
   ```

   c. 执行以下命令将文件拷贝到配置目录：

   ```
   cp cert_location /usr/local/etc/openvpn/
   ```

   cert_location是步骤三中下载的证书路径，例如： /Users/example/Downloads/certs6.zip。

   d. 执行以下命令解压证书文件：

   ```
   cd  /usr/local/certificates
   unzip /usr/local/etc/openvpn/certs6.zip
   ```

   e. 执行以下命令发起连接：

   ```
   sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
   ```

步骤五：连接测试

在客户端**ping**已连接的VPC内的一台ECS实例，测试连通性。

> **说明:**
> 确保测试的ECS实例的安全组规则允许客户端远程连接。详细信息，请参见#unique_5。