ALIBABA CLOUD

阿里云

安全众测
用户指南

文档版本：20220329

阿里云

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. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，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

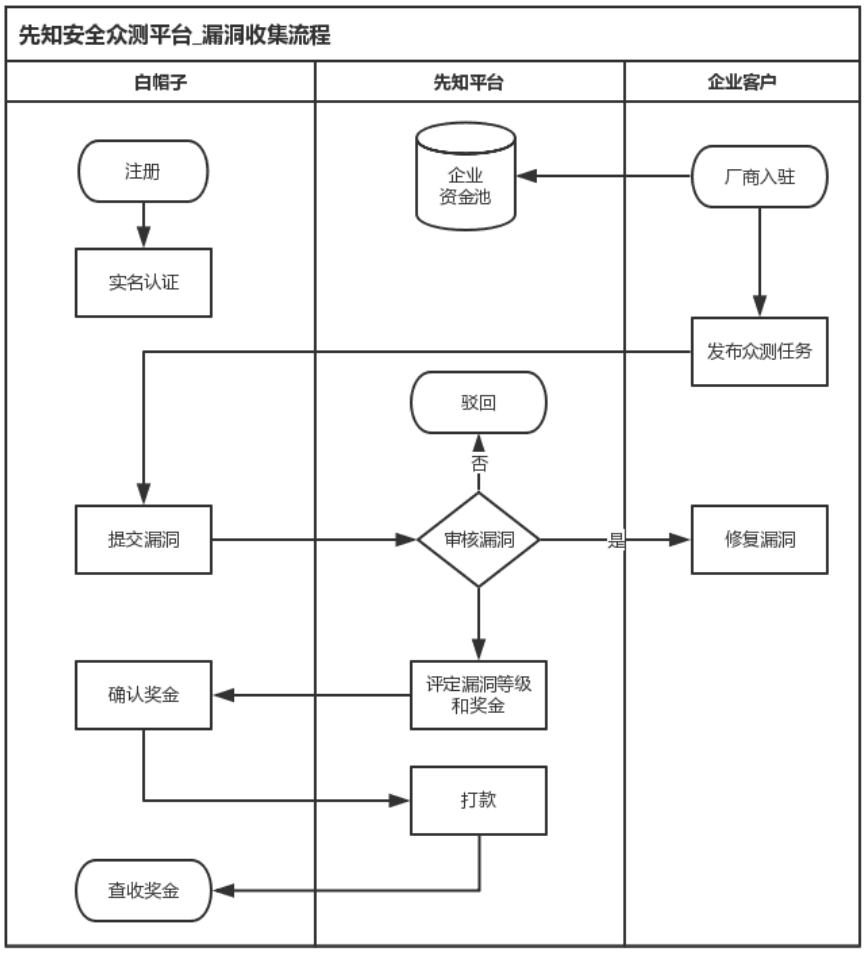
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	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.漏洞收集流程

本文介绍漏洞收集及处理流程。

漏洞收集流程图



操作步骤

1. 登录您的阿里云账号并完善个人、企业信息资料。
   - **白帽子**：使用淘宝网账号登录先知平台并完善资料和实名认证。

     > **说明**
     >
     > 请确保收款账号和个人信息真实有效，且姓名与支付宝账号一致，否则会影响奖金打款。

   - **企业**：企业入驻先知平台流程请参考企业入驻流程。
2. 白帽子根据漏洞提交页面指引，提交安全漏洞信息。

> **说明**
>
> 漏洞信息请务必详尽，漏洞描述越具体，越便于先知平台运营人员准确反馈并给出合理的奖励金额。

3. 漏洞提交后24小时内，先知平台运营人员会对所收到的漏洞报告进行内部评估。
   - 漏洞不存在或者漏洞重复上报，运营人员将驳回该漏洞，标识为**已驳回**状态，并告知驳回理由。
   - 漏洞描述不清，运营人员将返回该漏洞，并标识为**待补充**状态。请白帽子在72小时内补充漏洞信息便于运营人员进行评估，超过72小时未补充信息，平台将自动驳回该漏洞。
   - 漏洞经过验证确认存在，运营人员将在先知平台上确认该漏洞，并标识为**已审核**状态。
4. 先知平台运营人员将在漏洞确认存在后24小时内，确认漏洞等级和奖金，并标识漏洞为**已奖励**状态。
   - 通用软件漏洞将按照《漏洞验收标准》中漏洞奖励标准确定奖励金额。
   - 第三方企业漏洞将根据企业自定义奖励标准奖励。
5. 白帽子在先知官网>**我提交的漏洞**中找到**已确认价格**的漏洞，对漏洞等级和奖金进行确认，漏洞状态被标识为**奖金发放中**状态。
   - 若白帽子接受奖励金额，则进行确认操作，漏洞被标识为**奖金发放中**状态。
   - 若白帽子不接受奖励金额，可进行人工申述。先知平台运营人员将尽快与白帽子联系，共同协商奖励金额。
6. 先知平台运营人员将在白帽子确认漏洞等级和奖金后24小时内，发放奖励金额，并标识漏洞为**已奖励**状态。
7. 奖金会直接发放到白帽子入驻时填写的支付宝账号中，白帽子可登录支付宝账号查看奖金情况。
8. 企业将在漏洞被确认后根据漏洞的修复情况更新漏洞的状态，漏洞修复完成后该漏洞将标识为**已修复**。

2.企业入驻流程

本文介绍企业入驻先知（安全众测）平台的流程。

前提条件

入驻企业必须已完成**企业实名认证**。

操作步骤

1. 登录先知（安全众测）平台加入申请页面。
2. 选择充值金额，并完成预充值。

   该充值金额将直接换算为奖励基金并最终提供给白帽子。
3. 登录云盾先知（安全众测）管理控制台，填写对外展示的企业资料（企业Logo、企业名称等），并设置奖励系数制定奖励计划（高、中、低危漏洞分别奖励的金额）。

完成以上操作步骤后，您的企业已成功入驻先知（安全众测）平台，等待白帽子提交所发现的漏洞即可。

3.企业先知平台操作流程

本文介绍企业在先知（安全众测）平台中的操作流程。

操作步骤

1. 提交漏洞需求和设置奖励计划。

   在您开通先知（安全众测）服务并完成充值后，您可直接登录云盾先知（安全众测）管理平台，填写企业信息和设置奖励计划。

2. 等待白帽子提交漏洞。

   奖励计划设置完成后，先知平台会同步更新您的企业状态，并开始对外收集漏洞。

3. 查看漏洞并修复。

   待白帽子提交漏洞后，您可以登录云盾先知（安全众测）管理平台，同步查看到白帽子提交的漏洞并根据修复建议开展漏洞修复工作。

4.OpenVPN测试

本文介绍如何使用OpenVPN工具进行测试。

背景信息

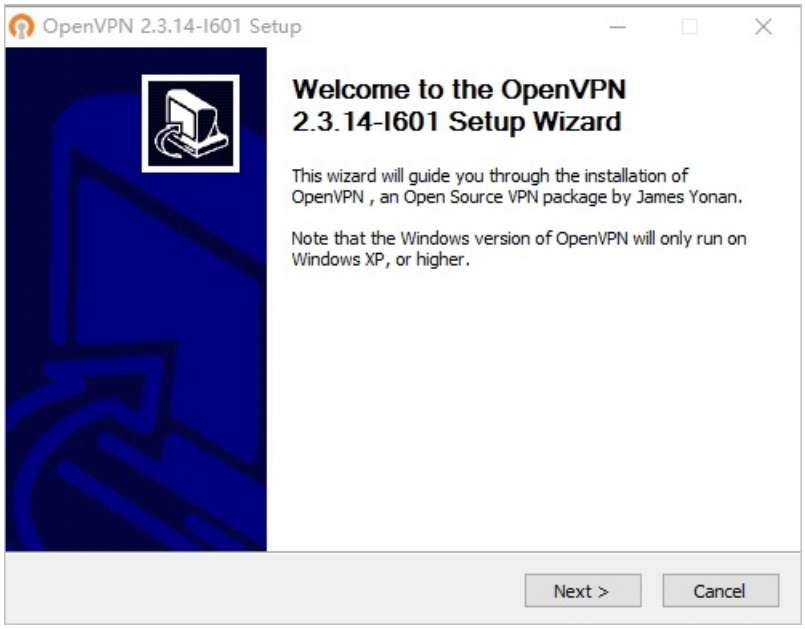
先知平台上部分项目要求必须通过VPN来进行测试。当企业页面中出现VPN测试提示说明时，企业要求必须通过专用VPN进行测试，否则将无法通过漏洞审核。

> **说明**
>
> Mac环境下使用OpenVPN可能会出现DNS问题，导致无法解析域名，建议您尝试以下解决方法：
>
> - 尝试直接通过IP对测试目标进行访问。
> - 在Mac环境下，使用Windows虚拟机进行测试。

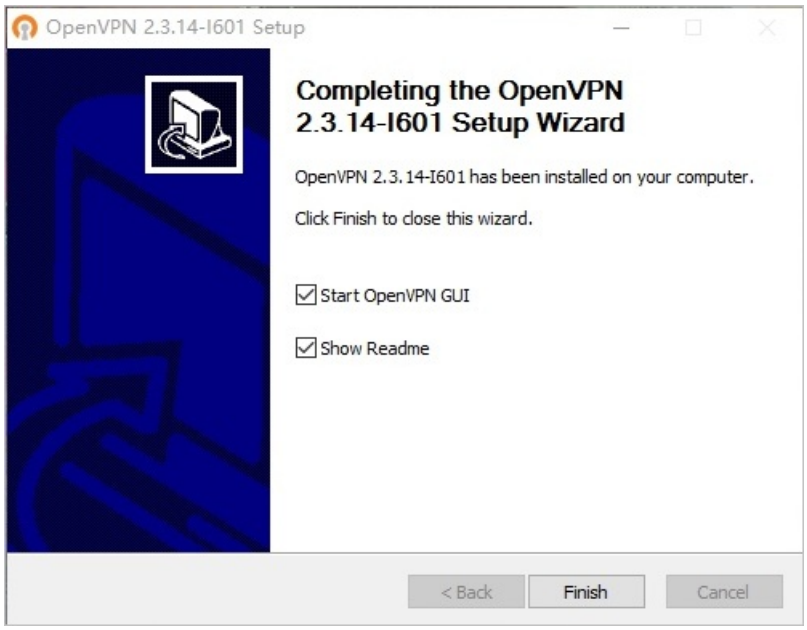
操作步骤

1. 单击下载OpenVPN工具压缩包到本地。
2. 解压已下载的压缩包。

3. 双击运行*openvpn-install-2.3.14-I601-x86_64.exe*文件，安装OpenVPN工具。



4. 安装完成后，运行OpenVPN工具。

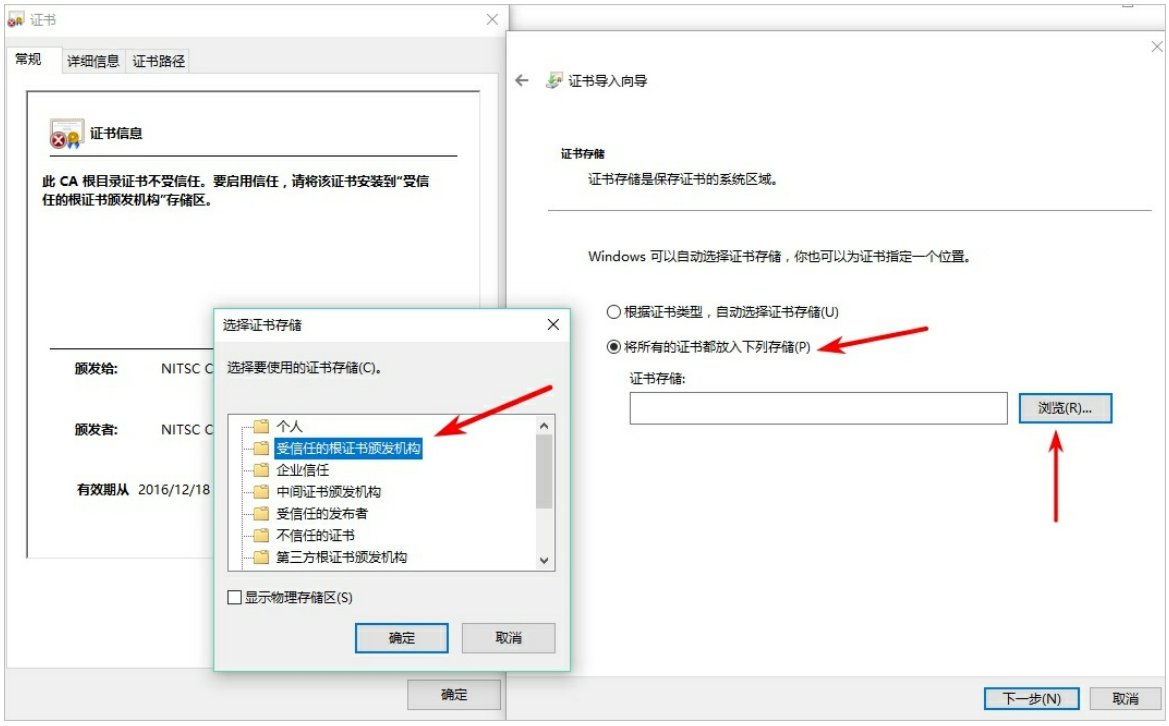


5. 将已分配给您的账号密码，填入*password.txt*文件中并保存，第一行为账号，第二行为密码。

6. 修改*client.ovpn*文件，在 `remote` 后面添加VPN服务器的IP和端口，如 `remote 1.1.1.1 1194` 。

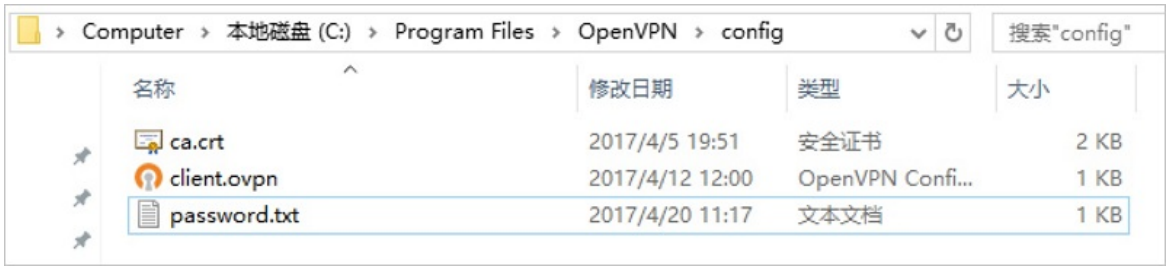
```
client
dev tun
proto udp
##########################################
# The hostname/IP and port of the server.#
# You can have multiple remote entries   #
# to load balance between the servers.   #
##########################################
remote
##########################################
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
ns-cert-type server
comp-lzo
verb 3
auth-user-pass password.txt
```

7. 安装*ca.crt*证书文件，并将该证书添加至受信任的根证书。



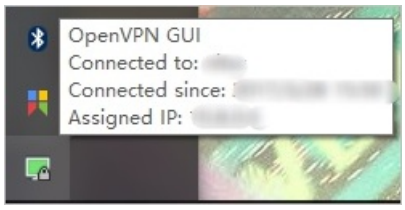
> **说明**
>
> 手机和电脑端都需要手工导入该证书。

8. 将已配置的*ca.crt*、*client.ovpn*、*password.txt*文件存放至OpenVPN安装目录下的*config*文件夹中，如*c:\Program Files\OpenVPN\config*。



9. 启动OpenVPN工具，双击菜单栏右下角图标。

连接成功。



5.先知高防管家服务

本文介绍先知高防管家服务。

服务介绍

先知高防管家服务由阿里云先知安全合作伙伴和阿里云安全专家一同提供，通过建立高防管家服务专用钉钉群的方式为您提供以下定制化服务。

- 协助您完成高防IP服务配置。
- DDoS攻击应急处置。
- 为您解答高防IP服务使用过程中遇到的问题。

您可以登录云盾先知（安全众测）管理控制台查看具体服务情况。

开通服务

在您购买阿里云高防IP服务时，可选择先知高防管家服务，合作伙伴费用将由阿里云承担。

支付完成后，先知高防管家的合作伙伴将通过电话联系您，沟通当前情况并通过建立高防服务钉钉群的方式，解决您在使用高防服务过程中遇到的问题。

6.渗透测试和安全众测的区别

阿里云安全平台提供渗透测试和安全众测两种方式帮助您对业务系统的安全性进行全方位测试。

- **安全众测**： 借助众多白帽子的力量，针对目标系统在规定时间内进行漏洞悬赏测试。您在收到有效的漏洞后，按漏洞风险等级给予白帽子一定的奖励。其最大的优势是按漏洞付费，性价比较高。同时，不同白帽子的技能研究方向可能不同，在进行测试的时候更为全面。
- **渗透测试**： 由阿里云安全团队以模拟黑客攻击的方式进行黑盒测试，多层次全面覆盖线上业务的测试，帮助您的企业发现系统中的安全隐患。根据渗透测试标准和阿里渗透测试的经验对目标测试系统定制测试方案和用例。其最大的优势是高效、专业、效果好。

同时，阿里云安全平台还提供安全扫描服务，使用扫描器对您企业的业务进行扫描，输出安全扫描报告，批量化、自动化、快速地发现较为明显的风险。对于新爆发的安全漏洞或者监控到的新的攻击方式，扫描检测规则实时更新，帮助企业第一时间排查业务是否存在风险。