有底安全卫士
部署操作指引

修订记录

制定日期	制定/修订 内容摘要	页数	版本	拟稿	审核	批准
20224-10-18	新建文档	14	0.1	陈致远	江峰	

目录

1. 文档使用范围

本文档介绍有底安全卫士（v1.0）客户端的部署架构、建议部署架构、部署要求以及部署操作。有关有底安全卫士的防护功能、运维和操作，请查看《有底安全卫士产品说明书》。

2. 部署架构

2.1. 部署环境要求

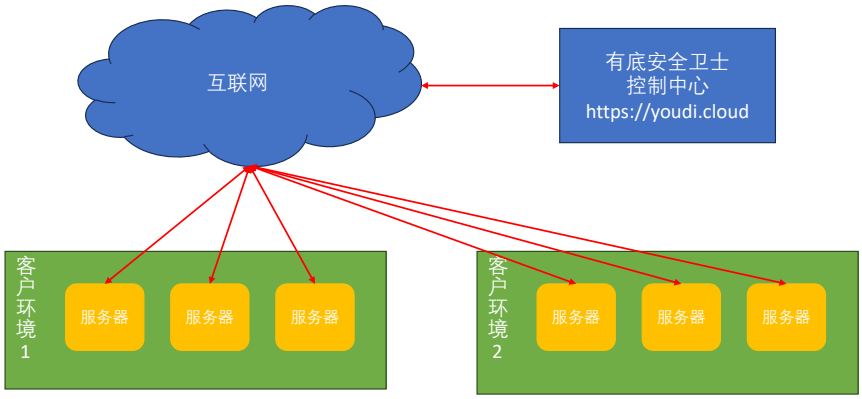
有底云安全中心可部署符合以下场景的服务器中：

- 公网部署（直连模式）
  能访问以下互联网 IP 及域名的服务器
  - https://180.184.97.186
  - https://180.184.97.105
  - https://14.103.148.114
  - https://14.103.145.223
  - http://hids-online-cn-beijing.tos-cn-beijing.volces.com
- 公网代理（代理模式）
  部署一台或多台具备符合公网部署（直连模式）要求的代理服务器，为内网服务器提供如下端口服务的场景：
  - 8080 端口
  - 6751 端口

  代理服务器性能要求：
  - 客户端少于 400 台，配置 1 核 CPU2G 内存 40GB 磁盘操作系统为 Linux、Ubuntu 的虚拟服务器；
  - 客户端大于 400 台且少于 1000 台，配置 2 核 CPU4G 内存 40GB 磁盘操作系统为 Linux、Ubuntu 的虚拟服务器；
  - 客户端大于 1000 台且少于 5000 台，配置 4 核 CPU8G 内存 40GB 磁盘操作系统为 Linux、Ubuntu 的虚拟服务器；

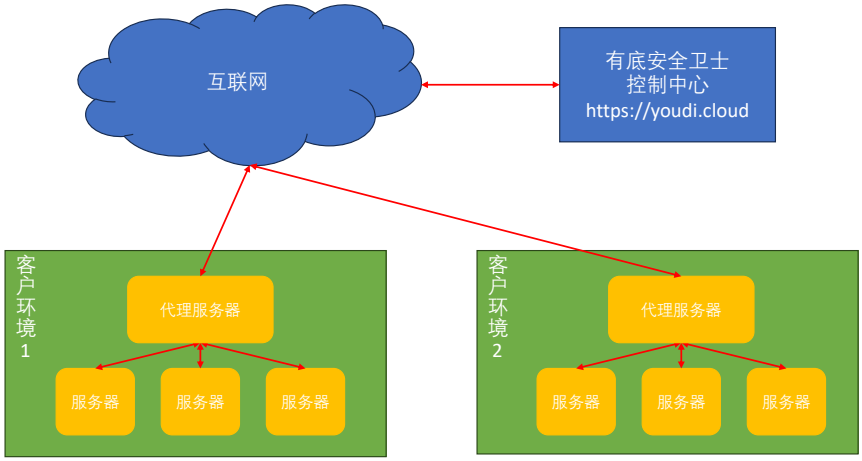
2.2. 推荐部署场景

- 服务器数量少于 20 台，且均满足互联网直连模式，使用公网部署（直连模式）部署。



公网部署（直连模式）

- 服务器数量大于 20 台，或存在无法满足互联网直连模式的服务器，推荐采用公网代理（代理模式）。



公网代理（代理模式）

2.3. 客户端操作系统兼容列表

有底安全中心对所有 ECS 公共镜像进行了适配，并会随公共镜像更新进行兼容测试与适配，确保相关功能稳定运行。如您采用自定义镜像或共享镜像，或是基于公共镜像自行升级内核版本，可能会导致镜像不适配，请参考如下信息确认兼容性。

类别	类型	大版本
Linux	CentOS	7~8
		stream 8~9
	Alibaba	2~3
	Amazon	2~3
	Velinux	1
	Ubuntu	16~24
	Debian	9~12
	Redhat	7~8
	Rocky	8
Windows	Windows Server	2012~2022
	Window	10~11

注:

1. Windows 不支持的资产类型：容器、系统服务、应用、内核模块、Web 站点、系统完整性校验;

2. Windows Server2012 停止维护，产品后续不支持新增功能模块;

3. Ubuntu 仅 16 支持系统弱口令，Debian 仅 9 支持系统弱口令;

4. 此表内容默认官方内核+intel/amd 处理器，自定义内核、非 intel/amd 处理器不适用此表，需单独评估。

3. 部署操作

3.1. 公网部署（直连模式）

3.1.1. Linux 操作系统客户端部署操作

i. 登录有底安全卫士控制台，切换到专家模式;
ii. 在总资产中心页面，点击安装客户端引导;
iii. 依次点击 Linux 标签、公网部署（直连模式），在第一步：选择厂商列表中选择服务器所在的环境（如有列表以外的环境，请选择线下 IDC）;
iv. 点击生成客户端安装命令按钮，生成安装命令;
v. 点击复制客户端安装命令中的复制按钮，完成命令的复制;

vi. 登录需要安装客户端的服务器，在 root 权限下粘贴命令执行，完成客户端安装；

vii. 刷新资产中心页面，更新客户服务器清单后，点击开启防护，完成防护的开启。

3.1.2. Windows 操作系统客户端部署操作

i. 登录有底安全卫士控制台，切换到专家模式；

ii. 在总资产中心页面，点击安装客户端引导；

iii. 依次点击 Windows 标签、公网部署（直连模式），在第一步：选择厂商列表中选择服务器所在的环境（如有列表以外的环境，请选择线下 IDC）；

iv. 点击生成客户端安装命令按钮，生成安装命令；

v. 点击复制客户端安装命令中的复制按钮，完成命令的复制；

vi. 登录需要安装客户端的服务器，在管理员用户下的命令提示符(CMD）界面，执行复制的部署命令，即可完成客户端下载及安装。；

vii. 刷新资产中心页面，更新客户服务器清单后，点击开启防护，完成防护的开启。

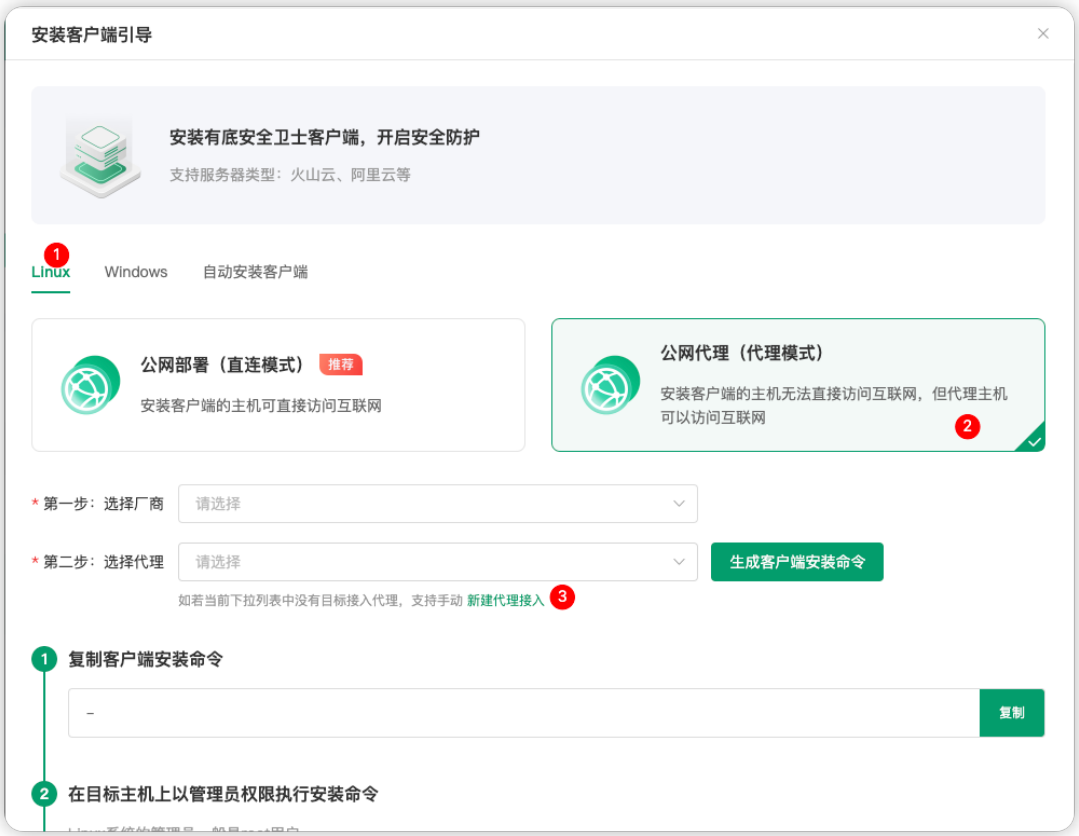
3.2. 公网代理（代理模式）

3.2.1. 代理服务器部署操作

i. 登录有底安全卫士控制台，切换到专家模式；

ii. 在总资产中心页面，点击安装客户端引导；

iii. 依次点击 Linux 标签、公网代理（代理模式）、新建代理接入；



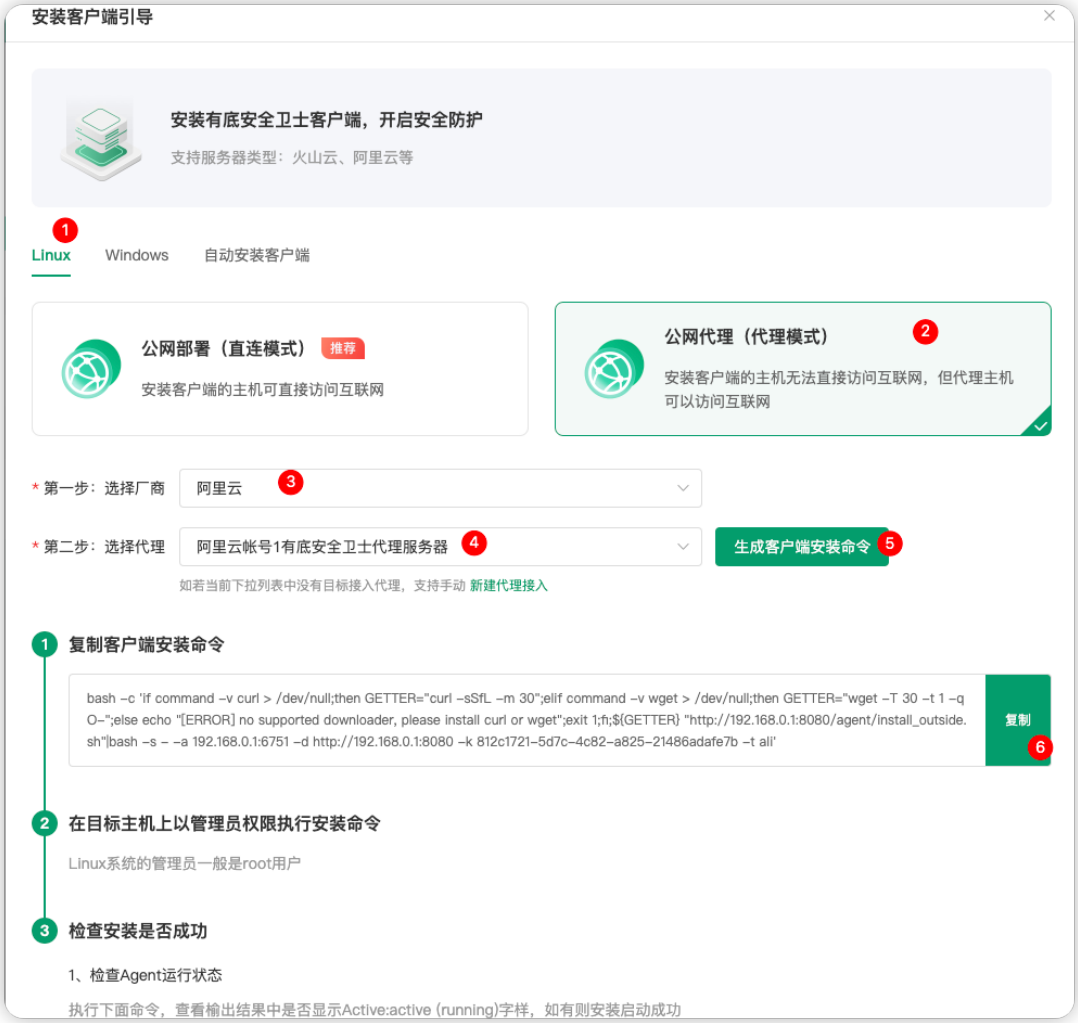
iv. 在弹出的窗口中录入代理名称、通信地址（代理服务器内网 IP 地址），点击确定并生成安装命令；

v. 点击复制，复制安装命令；

vi. 登录代理服务器，在 root 权限下运行复制的命令，完成代理服务器的安装。

3.2.2. Linux 服务器客户端部署操作

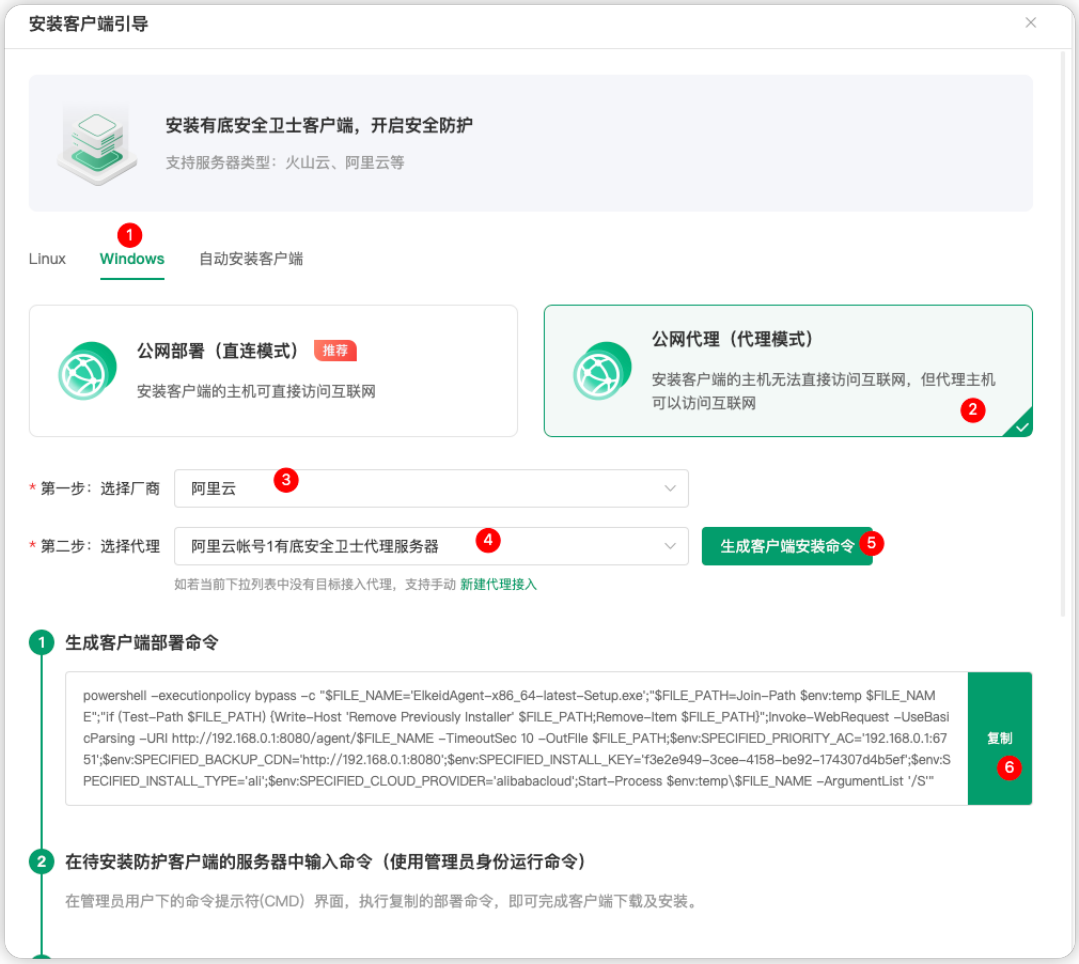
i. 登录有底安全卫士控制台，切换到专家模式；
ii. 在总资产中心页面，点击安装客户端引导；
iii. 依次点击 Linux 标签、公网代理（代理模式），在第一步：选择厂商列表中选择服务器所在的环境（如有列表以外的环境，请选择线下 IDC）；
iv. 第二步选择代理，选择对应代理；
v. 点击生成客户端安装命令按钮，生成安装命令；
vi. 点击复制客户端安装命令中的复制按钮，完成命令的复制；



vii. 登录需要安装客户端的服务器，在 root 权限下粘贴命令执行，完成客户端安装；
viii. 刷新资产中心页面，更新客户服务器清单后，点击开启防护，完成防护的开启。

3.2.3. Windows 服务器客户端部署操作

i. 登录有底安全卫士控制台，切换到专家模式；
ii. 在总资产中心页面，点击安装客户端引导；
iii. 依次点击 Windows 标签、公网代理（代理模式），在第一步：选择厂商列表中选择服务器所在的环境（如有列表以外的环境，请选择线下 IDC）；
iv. 第二步选择代理，选择对应代理；
v. 点击生成客户端安装命令按钮，生成安装命令；
vi. 点击复制客户端安装命令中的复制按钮，完成命令的复制；



viii. 登录需要安装客户端的服务器，在管理员用户下的命令提示符(CMD）界面，执行复制的部署命令，即可完成客户端下载及安装；
ix. 刷新资产中心页面，更新客户服务器清单后，点击开启防护，完成防护的开启。

4. 客户端管理操作

4.1. 检查客户端状态

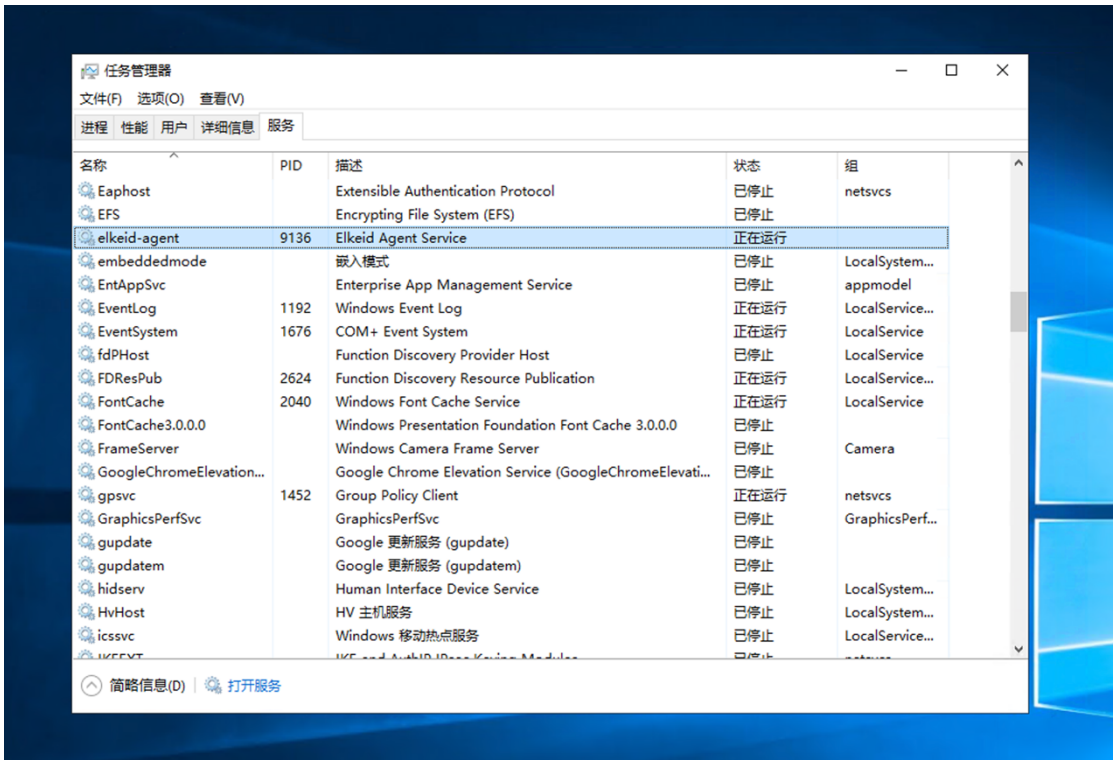
4.1.1. Linux 服务器客户端状态检查

i. 登录到服务器，执行命令 systemctl status elkeid-agent | grep 'Active'，查看输出结果中是否显示 Active:active (running)字样，如有则安装启动成功；

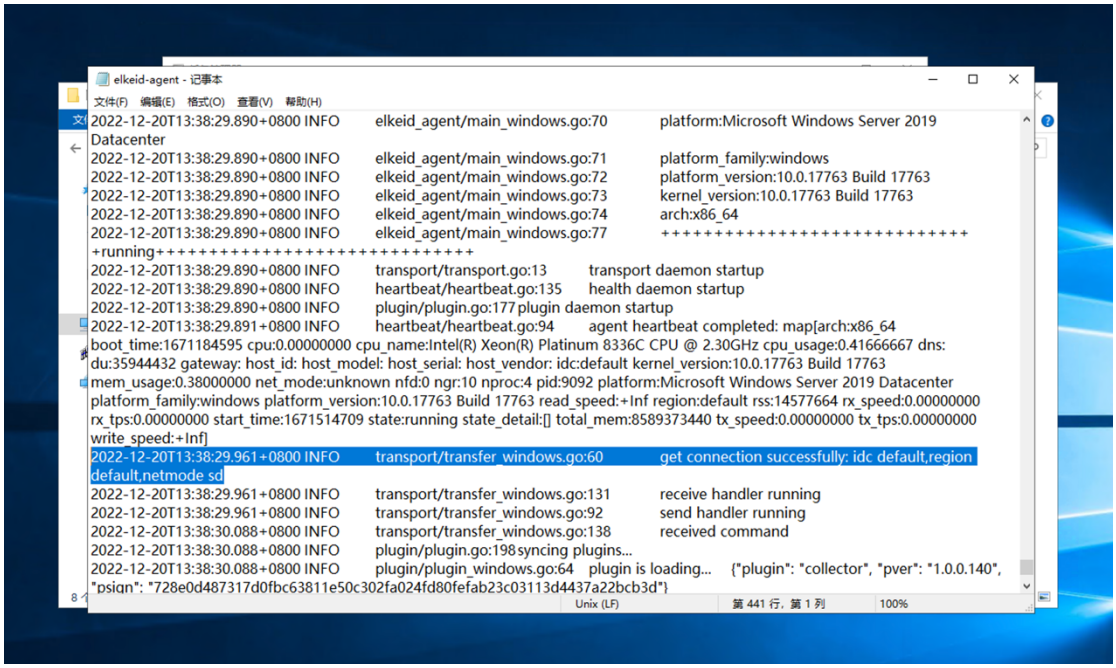
ii. 执行命令 cat /etc/elkeid/log/elkeid-agent.log | grep 'get connection successfully'，查看日志里是否显示 get connection successfully 字样，如有则视为网络通畅。

4.1.2. Windows 服务器客户端状态检查

i. 登录到服务器，打开任务管理器，选择服务 TAB，查找 elkeid-agent 服务，输出结果中是否显示正在运行字样，如有则安装且启动成功；



ii. 打开日志文件（路径：C:\Program Files\Elkeid\log\elkeid-agent.log)，确认有 get connection successfully 字样，视为网络通畅；



4.2. 卸载代理服务器

i. 登录有底安全卫士控制台，切换到专家模式；
ii. 在系统配置下代理管理页面，点击部署代理；
iii. 在弹出的窗口中复制卸载命令；

iv. 登录代理服务器，在 root 权限下运行复制的命令，完成代理服务器的卸载。

4.3. 卸载客户端

4.3.1. Linux 服务器客户端卸载命令

i. 登录服务器，在 root 权限下运行如下的命令，完成客户端的卸载，bash -c 'if command -v curl > /dev/null;then GETTER="curl -sSfL -m 30";elif command -v wget > /dev/null;then GETTER="wget -T 30 -t 1 -qO-";else echo "[ERROR] no supported downloader, please install curl or wget";exit 1;fi;DOWN_BASE=$(cat /etc/elkeid/download_base);${GETTER} "${DOWN_BASE}uninstall.sh" | bash'。

4.3.2. Windows 服务器客户端卸载命令

i. 登录服务器，在管理员用户下的命令提示符(CMD）界面，执行以下命令，即可完成客户端卸载，powershell -executionpolicy bypass -c "Start-Process $env:ProgramFiles\Elkeid\Uninstall.exe -ArgumentList '/S'"。

--（完）--