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

目录	₹	· · · · · · · · · · · · · · · · · · ·	3
1.	文権	当使用范围	4
2.	部署	署架构	4
	2.1.	部署环境要求	4
	2.2.	推荐部署场景	4
	2.3.	客户端操作系统兼容列表	5
3.	部署	署操作	5
	3.1.	公网部署(直连模式)	5
	3.1.1.	Linux 操作系统客户端部署操作	5
	3.1.2.	Windows 操作系统客户端部署操作	7
	3.2.	公网代理(代理模式)	3
	3.2.1.	代理服务器部署操作	3
	3.2.2.	Linux 服务器客户端部署操作10)
	3.2.3.	Windows 服务器客户端部署操作1	1
4.	客户	[〕] 端管理操作1	1
	4.1.	检查客户端状态12	2
	4.1.1.	Linux 服务器客户端状态检查12	2
	4.1.2.	Windows 服务器客户端状态检查12	2
	4.2.	卸载代理服务器1	3
	4.3.	卸载客户端14	4
	4.3.1.	Linux 服务器客户端卸载命令14	4
	4.3.2.	Windows 服务器客户端卸载命令14	4



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。



奇墨科技 (广州)有限公司

类别	类型	大版本
	ContOS	7~8
	Centos	stream 8~9
	Alibaba	2~3
	Amazon	2~3
Linux	Velinux	1
	Ubuntu	16~24
	Debian	9~12
	Redhat	7~8
	Rocky	8
\\/indows	Windows Server	2012~2022
windows	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;

	安装有底安全卫士客户端,	开启安全防护		
Ś	支持服务器类型:火山云、阿里	目云等		
nux Windo	ws 自动安装客户端			
			公网代理(代理模式)	
		2	安装客户端的主机无法直接访问	回互联网,但代理主机
	又不已。1997年1996年1999年1999年1999年1999年1999年1999年	~	可以访问互联网	
第一步:选择厂	商线下IDC	3	✓ 生成客户端安装命令	4
第一步:选择厂 全成客户或	商 线下IDC 端部署命令	3	∨ 生成客户端安装命令	4
第一步:选择厂 生成客户站	商 线下IDC <mark>端部署命令</mark>	3	✓ 生成客户端安装命令	
第一步:选择厂 生成客户站 powershel E";"iff (Tes	商 线下IDC 端部署命令 II -executionpolicy bypass -c "\$FILE_N t-Path \$FILE_PATH) (Write-Host "Ren UPL bhts://tide_carline_builte_	3 VAME='ElkeldAgent-x86_64-latest- nove Previously Installer' \$FILE.PAT		4 p \$FILE_NAM quest = UseBasi
第一步:选择厂 生成客户 powershel E ⁻ ;"if (Tes cParsing - ED_PRIOF	商 线下IDC 着部署命令 II -executionpolicy bypass -c "\$FILE_N tt-Path \$FILE_PATH) (Write-Host 'Rem -URI http://hids-online-cn-beijing.tos NTY_AC='csc-hids-agent.hids.volces.c	3 NAME='ElkeidAgent-x86_64-latest- nove Previously Installer' \$FILE_PAT on-beijing.volces.com/agent/\$FILL zom:443';\$env:SPECIFIED_BACKUP_		4 p \$FILE_NAM quest –UseBasi H;\$env:SPECIFI peijing_volces.co
第一步:选择厂 生成客户 銷 Powershel E [*] ;"if (Tes cParsing - ED_PRIOF m;Senv:SI _PROVIDE	商 线下IDC 端部署命令 II -executionpolicy bypass -c "\$FILE_N t-Path \$FILE_PATH) {Write-Host 'Ren -URI http://hids-online-cn-beijing.tos ITY_AC-ciosc-hids-agent-hids.volces.c PECIFIED_INSTALL_KEY='bc0f2986-4 :R='local_tob';Start-Process \$env:temp	3 VAME='ElkeldAgent-x86_64-latest- nove Prevlously Installer' \$FILE_PAT -on-beijing.volces.com/agent/\$FILI com:443';\$em:SPECIFIED_BACKUP_ la60-4be8-8e2b-56d67943e0dd';\$ p\\$FILE_NAME -ArgumentList '/S''		4 p \$FILE_NAM quest -UseBasi H;\$env:SPECIFi peljing.volces.co cciFiED_CLOUD
第一步:选择厂 生成客户 朝 powershel E";"if (Tes cParsing - ED_PRIOF m`;Senv:SI _PROVIDE	商 线下IDC #部署命令 I -executionpolicy bypass -c "\$FILE_N it-Path \$FILE_PATH) (Write-Host 'Ren -URI http://hids-online-cn-beijing.tos NTY_AC="osc-hids-agent.hids.voices.c PECIFIED_INSTALL_KEY="bc0f2986-4 :Re"local_tob';Start-Process \$env:temp	3 VAME='ElkeidAgent-x86_64-latest- move Previously Installer' \$FILE_PAT -cn-beijing.volces.com/agent/\$FILE 2007.443';\$env:SPECIFIED_BACKUP_ la60-4be8-8e2b-56d67943e0dd';\$ h}\$FILE_NAME -ArgumentList '/S''		4 p \$FILE_NAM iquest –UseBasi H;\$env:SPECIFI beijing.volces.co c:CIFIED_CLOUD
第一步:选择厂 生成客户 銷 Powershel E [*] ,"If (Tes cParsing - ED_PRIOF m';Serv:SI _PROVIDE 在待安装D	商 线下IDC #部署命令 II -executionpolicy bypass -c "\$FILE_N t-Path \$FILE_PATH) (Write-Host 'Ren -URI http://hids-online-on-beijing.tos ITY_AC-'cso-hids-agent-hids.volces.c PECIFIED_INSTALL_KEY='bc0f2986-4 :R='local_tob';Start-Process \$env:temp fifr客户端的服务器中输入命令	③ NAME='ElkeldAgent-x86_64-latest- nove Previously Installer' \$FILE_PAT -cn-beijing.volces.com/agent/\$FILI -com:443';\$em:SPECIFIED_BACKUP, la60-4be8-8e2b-56d67943e0dd';\$ p\\$FILE_NAME -ArgumentList '/S'' > (使用管理员身份运行命令)		4 p \$FILE_NAM quest -UseBasi H;\$env:SPECIFI bijng.volces.co cCIFIED_CLOUD
第一步:选择厂 生成客户 powershel E [*] ,"If (Tes cParsing - ED_PRIOV:SI _PROVIDE 在待安装即 在管理员用	商 线下IDC #部署命令 II -executionpolicy bypass -c "\$FILE_N it-Path \$FILE_PATH) (Write-Host 'Ren -URI http://hids-online-cn-beijing.tos NTY_AC='csc-hids-agent.hids.volces.c PECIFIED_INSTALL_KEY='bc0f2986-4 :Re-local_tob';Start-Process \$env:temp fifre客户端的服务器中输入命令 户下的命令提示符(CMD) 界面,执	3 VAME='ElkeidAgent-x86_64-latest- nove Previously Installer' \$FILE_PAT n-beijing.volces.com/agent/\$FILI a60-4be8-8e2b-566d67943e0dd'\$ p\\$FILE_NAME -ArgumentList '/S'' く (使用管理员身份运行命令) 切复制的部署命令,即可完成客		4 p \$FILE_NAM iquest –UseBasi H;\$env:SPECIFI beijing.volces.co :CIFIED_CLOUD
第一步:选择厂 生成客户 銷 Powershel E [*] ;"if (Tes cParsing - ED_PRIOF m;Senv:SI _PROVIDE 在待安装阳 在管理员用)	商 线下IDC #部署命令 II -executionpolicy bypass -c "\$FILE_N tt-Path \$FILE_PATH) (Write-Host 'Ren -URI http://hids-online-cn-beijing.tos ITY_AC-'cso-hids-agelth.hids.volces.c PECIFIED_INSTALL_KEY='bc0f2986-4 :R='local_tob';Start-Process \$env:temp fo护客户端的服务器中输入命令 户下的命令提示符(CMD) 界面,执	3 NAME='ElkeldAgent-x86_64-latest- move Previously Installer' \$FILE_PAT com:v43';senv:SPECIFIED_BACKUP_ la60-4be8-8e2b-56d67943e0dd';\$ p\\$FILE_NAME -ArgumentList '/S'' (使用管理员身份运行命令) 切复制的部署命令,即可完成客		4 p \$FILE_NAM quest -UseBasi H;\$env:SPECIFI ei]ing.volces.co cciFiED_CLOUD
 第一步:选择厂 生成客户號 powershel E[*],"if (Tes cParsing - ED_PRIOF m[*],Senv:Si _PROVIDE 在待安装即 在管理员用) 检查安装易 	商 线下IDC 端部署命令 II -executionpolicy bypass -c "\$FILE_N It-Path \$FILE_PATH) (Write-Host 'Ren -URI http://hids-online-cn-beijing.tos NTY_AC='csc-hids-agent.hids.volces.c PECIFIED_INSTALL_KEY='bc0f2986-4 :Re-local_tob';Start-Process \$env:temp 防护客户端的服务器中输入命令 户下的命令提示符(CMD) 界面,执 昆否成功	3 VAME='ElkeidAgent-x86_64-latest- move Previously Installer' \$FILE_PAT i-cn-beijing.volces.com/agent/\$FILI com:443';\$env:SPECIFIED_BACKUP_ la60-4be8-8e2b-56d67943e0dd',\$ p\\$FILE_NAME -ArgumentList '/S'' ★ (使用管理员身份运行命令) ¥行复制的部署命令,即可完成客	✓ 生成客户端安装命令 Setup.exe';"\$FILE_PATH=Join-Path \$env:tem +;Remove-Item \$FILE_PATH';Invoke-WebRe _NAME - TimeoutSec 10 -OutFile \$FILE_PAT CDN='http://hids-online-cn-beijing.tos-cn-t nv:SPECIFIED_INSTALL_TYPE='idc';\$env:SPE □端下载及安装。	4 p \$FILE_NAM quest –UseBasi H;\$env:SPECIFI beijing.volces.co :CIFIED_CLOUD

- 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;



安装客户端引导		
3	3装有底安全卫士客户端,开启安全防护 2持服务器类型:火山云、阿里云等	
Linux Windows	自动安装客户端	
公网 安装?	部署(直连模式) 推荐 客户端的主机可直接访问互联网	公网代理(代理模式) 安装客户端的主机无法直接访问互联网,但代理主机 可以访问互联网 2
* 第一步:选择厂商	请选择	~
* 第二步:选择代理	请选择	✓ 生成客户端安装命令
 复制客户端安: 	如若当前下拉列表中没有目标拨入代理,支持手动 新建代理接 / 凌命令	入 ³ 3 复制
2 在目标主机上!	以管理员权限执行安装命令	

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;

 1 1	^代 理新建后不可修改,通过代理集群,可将无法连接公网的服务器接入有底安全卫士,适用于无法直接连接到有底安全卫士的 [湘]是一混合示等业务场景
* 代理名称	阿里云帐号1有底安全卫士代理服务器
* 通信地址 确定并生质	192.168.0.1 10 理版分益的网 IP 地址 _{就安装命令}
* 通信地址 确定并生的 安装命令 请在服务器」	192.168.0.1 大工生加入分話 小
* 通信地址 确定并生的 安装命令 请在服务器上 bash -c "if	192.168.0.1 TVI主版分子品內MIPIULIE 改安装命令 :执行下面命令安装代理,此安装命令仅针对当前代理使用 (command -v curl); then (curl -sS http://hids-online-cn-beljing.tos-cn-beljing.volces.com/agen 复制
* 通信地址 确定并生的 安装命令 请在服务器上 bash -c "if	192.168.0.1 TUILING 分 話 小 M IP JUJI X安装命令 :执行下面命令安装代理,此安装命令仅针对当前代理使用 (command -v curl); then (curl -sS http://hids-online-cn-beijing.tos-cn-beijing.volces.com/agen 复制

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;

	安装有底安全卫士客户端,开启安全防护	
	支持服务器类型:火山云、阿里云等	
0		
inux Windows	自动安装客户端	
		公网代理 (代理模式) 2
		安装客户端的主机无法直接访问互联网,但代理主机
安装	客尸端的主机可直接访问互联网	可以访问互联网
第一步:选择厂商	阿里云 3	~
第二步:选择代理	阿里云帐号1有底安全卫士代理服务器	◇ 生成客户端安装命令 5
	如若当前下拉列表中没有目标接入代理,支持手动 新建代理接	ξ.λ
1 复制客户端安	装命令	
hash a lifea	mmand y aut > /day/aulithan CETTED_"aut a94 m 30)" all approach water / day author GETTED-"water T 20 +1 a
O-";else echo	"[ERROR] no supported downloader, please install curl or v	yet"; yet" commandv wget > / dev/ hui, then SE TEN= wget - 1 30 - t T - q wget"; exit 1; fi; \${GETTER} "http://192.168.0.1:8080/agent/install_outside.
sn Ipasn –s –	-a 192.108.0.1:0701 -d http://192.108.0.1:8060 -k 81201/21	-5070-4682-8623-214668081870 -1 811
	以做一日的四世行内社会会	
2 在目标主机上	以官理贞权限执行安装命令	
2 在目标主机上 Linux系统的管	以管理页仪限执行安装命令 里员一般是root用户	
2 在目标主机上 Linux系统的管	以管理页仪限执行安装命令 ^{至员一般是root用户}	
 2 在目标主机上 Linux系统的管: 3 检查安装是否 	以管理页权限执行安装命令 ^{聖员一般是root用户} 成功	

- 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;

오衣답/ 꽤기국		
3	2装有底安全卫士客户端,开启安全防护 2持服务器类型:火山云、阿里云等	
Linux Windows	自动安装客户端	
公网 _{安装}	部署(直连模式) 推荐 客户端的主机可直接访问互联网	·理主机 2
* 第一步:选择厂商	阿里云 3 ~	
♥第二步:选择代理	阿里云帐号1有底安全卫士代理服务器 4 生成客户端安装命 5 如若当前下拉列表中没有目标接入代理,支持手动 新建代理接入 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 <td< td=""><td></td></td<>	
1 生成客户端部	層命令	
powershell –ex E";"if (Test–Pa cParsing –URI 51';\$env:SPECI PECIFIED_INST	scutionpolicy bypass -c "\$FILE_NAME='ElkeidAgent-x86_64-latest-Setup.exe';"\$FILE_PATH=Join-Path \$env:temp \$FILE_NAM th \$FILE_PATH) (Write-Host 'Remove Previously Installer' \$FILE_PATH;Remove-Item \$FILE_PATH)";Invoke-WebRequest -UseBasi http://192.168.0.1:8080/agent/\$FILE_NAME -TImeoutSec 10 -OutFIle \$FILE_PATH;\$env:SPECIFIED_PRIORITY_AC='192.168.0.1:67 FIED_BACKUP_CDN='http://192.168.0.1:8080';\$env:SPECIFIED_INSTALL_KEY='13e2e949-3cee-4158-be92-174307d4b5ef';\$env: 'ALL_TYPE='all';\$env:SPECIFIED_CLOUD_PROVIDER='allbabacloud';Start-Process \$env:temp\\$FILE_NAME -ArgumentList '/S''	复制
2 在待安装防护 在管理员用户下	客户端的服务器中输入命令(使用管理员身份运行命令) 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。	

- 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;

文件(F) 选项(O) 查看(V)					
进程 性能 用户 详细信息	服务				
名称 ^	PID	描述	状态	组	^
🔍 Eaphost		Extensible Authentication Protocol	已停止	netsvcs	
EFS		Encrypting File System (EFS)	已停止		
🤹 elkeid-agent	9136	Elkeid Agent Service	正在运行		
🌼 embeddedmode		嵌入模式	已停止	LocalSystem	
🔍 EntAppSvc		Enterprise App Management Service	已停止	appmodel	
🔍 EventLog	1192	Windows Event Log	正在运行	LocalService	
🔍 EventSystem	1676	COM+ Event System	正在运行	LocalService	
🔍 fdPHost		Function Discovery Provider Host	已停止	LocalService	
🔍 FDResPub	2624	Function Discovery Resource Publication	正在运行	LocalService	
🔍 FontCache	2040	Windows Font Cache Service	正在运行	LocalService	
🔅 FontCache3.0.0.0		Windows Presentation Foundation Font Cache 3.0.0.0	已停止		
🔆 FrameServer		Windows Camera Frame Server	已停止	Camera	
🔆 GoogleChromeElevation		Google Chrome Elevation Service (GoogleChromeElevati	已停止		
gpsvc 🕄	1452	Group Policy Client	正在运行	netsvcs	
🔆 GraphicsPerfSvc		GraphicsPerfSvc	已停止	GraphicsPerf	
🖏 gupdate		Google 更新服务 (gupdate)	已停止		
🖏 gupdatem		Google 更新服务 (gupdatem)	已停止		
🛸 hidserv		Human Interface Device Service	已停止	LocalSystem	
🔆 HvHost		HV 主机服务	已停止	LocalSystem	
🔍 icssvc		Windows 移动热点服务	已停止	LocalService	
		IVE and Audulo IDana Kaulan Mandulan	D/Pi-		*

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;



	in circle agent - Dant			- 0	×
	文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)				
文	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:70	platform	:Microsoft Windows Server 2019	^
_	Datacenter		-		
<u>ا</u>	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:71	platform	_family:windows	
	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:72	platform	version:10.0.17763 Build 17763	
3	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:73	kernel_v	ersion:10.0.17763 Build 17763	
	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:74	arch:x86	_64	
	2022-12-20T13:38:29.890+0800 INFO	elkeid_agent/main_windows.go:77	+++++	+++++++++++++++++++++++++++++++++++++++	
-	+running++++++++++++++++++++++++++++++++++	++++++++++			
	2022-12-20T13:38:29.890+0800 INFO	transport/transport.go:13 transp	ort daemon	startup	
	2022-12-20T13:38:29.890+0800 INFO	heartbeat/heartbeat.go:135 health	daemon sta	rtup	
_	2022-12-20T13:38:29.890+0800 INFO	plugin/plugin.go:177 plugin daemon s	tartup		
-	2022-12-20T13:38:29.891+0800 INFO	heartbeat/heartbeat.go:94 agent	heartbeat co	mpleted: map[arch:x86_64	
				inpleted. mapfarenxoo_or	
18	boot_time:1671184595 cpu:0.00000000 cp	pu_name:Intel(R) Xeon(R) Platinum 8336	5C CPU @ 2.	30GHz cpu_usage:0.416666667 dns:	
3	boot_time:1671184595 cpu:0.00000000 cp du:35944432 gateway: host_id: host_mod	pu_name:Intel(R) Xeon(R) Platinum 8336 del: host_serial: host_vendor: idc:default	SC CPU @ 2. kernel_versio	30GHz cpu_usage:0.41666667 dns: pn:10.0.17763 Build 17763	
8	boot_time:1671184595_cpu:0.00000000 cp du:35944432_gateway: host_id: host_mod nem_usage:0.38000000 net_mode:unkno	pu_name:Intel(R) Xeon(R) Platinum 8336 del: host_serial: host_vendor: idc:default own nfd:0 ngr:10 nproc:4 pid:9092 platfo	SC CPU @ 2. kernel_versic orm:Microso	30GHz cpu_usage:0.41666667 dns: on:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter	
đ	boot_time:1671184595_cpu:0.00000000 cp Ju:35944432_gateway: host_id: host_mod nem_usage:0.38000000 net_mode:unkno platform_family:windows platform_versio platform_family:windows platform_versio	pu_name:Intel(R) Xeon(R) Platinum 8336 del: host_serial: host_vendor: idc:default own nfd:0 ngr:10 nproc:4 pid:9092 platfo n:10.0.17763 Build 17763 read_speed:+	5C CPU @ 2. kernel_versic orm:Microso Inf region:de	30GHz cpu usage:0.41666667 dns: 50n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000	
3	2001_time:1671184595 cpu:0.00000000 cj du:35944432 gateway: host_id: host_mod mem_usage:0.38000000 net_mode:unkno platform_family:windows platform_versio x_tps:0.000000000 start_time:1671514709	pu_name:Intel(R) Xeon(R) Platinum 833 Iel: host_serial: host_vendor: idc:default own fid:0 ngr:10 nproc:4 pid:9092 platfi n:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem:	SC CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440	30GHz cpt_usage:0.41666667 dns: n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000	
8	soot_time:167118495 cpu:0.0000000 cj du:35944432 gateway: host_id: host_mod nem_usage:0.38000000 net_mode:unkno lalfform_family:windows platform_versio x_tps:0.00000000 start_time:1671514709 write_speed:+1nf]	pu_name:Intel(R) Xeon(R) Platinum 8330 fel: host_serial: host_vendor: idc:default own nfd:0 ngr:10 nproc:4 pid:9092 platf nr:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem:	5C CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440	30GHz cpt_usage:0.41666667 dns: n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter ifault rss:14577664 rx_speed:0.0000000 tx_speed:0.0000000 tx_tps:0.0000000	
8	Doot_time:1671184595 cpu:0.00000000 cf ui:35944432 gateway: host_id: host_mod mem_usage:0.38000000 net_mode:unknc olatform_family:windows platform_versio x_tps:0.0000000 start_time:1671514709 write_speed:+1nf] 2022-12-20T13:38:29.961+0800 INFO to fault astende cf	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wom fdf:0 ngr:10 nproc:4 pid:9022 platfi nn:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:60	5C CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get conr	JoGHz cpu_usage:0.41666667 dns: on:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter ifault rss:14577664 rx_speed:0.00000000 tx_speed:0.0000000 tx_tps:0.00000000 nection successfully: idc default,region	
8	2005 time:1671184595 cpu:0.00000000 q du:35944432 gateway: host_id: host_mod mem_usage:0.38000000 net_mode:unknc olatform_family:windows platform_versio x_tps:0.00000000 start_time:1671514709 wirte_speed:+Inf] 2022-12-20113:38:29.961+0800 INFO Jefault.netmode.sd 2023-12.2013:28:29.961+0800 INFO	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wom nfd:0 ngr:10 nproc:4 pid:9022 platfi on:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:60	5C CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get com	30GHz cpr_usage:0.41666667 dns: m:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000 mection successfully: idc default,region	
8	2000 time:1671184595 cpu:0.00000000 cj diu:35944432 gateway: host_id: host_mod em_usage:0.38000000 net_mode:unkno platform_family:windows platform_versio x_tps:0.00000000 start_time:1671514709 write_speed:+Inf] 2022-12-20T13:38:29,961+0800 INFO default.netmode_sd 2022-12-20T13:38:29,961+0800 INFO 2022-12-20T13:38:29,961+0800 INFO	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wwn fdi20 ngr:10 nproc:4 pid:9092 platfi on:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:60 transport/transfer_windows.go:131 transport/transfer_windows.go:131	SC CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get conn receive h	30GHz cpt_usage:0.41666667 dns: n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000 nection successfully: idc default,region nandler running edler supping	
£	Doot_time:1671184595 cpu:0.00000000 cpu: Jui3594432 gateway: host_id: host_mod mem_usage:0.38000000 net_mode:unknc Jalform_family:windows platform_versio x_tps:0.00000000 start_time:1671514709 write_speed:+Inf] 2022-12-20T13:38:29,961+0800 INFO 2022-12-20T13:38:29,961+0800 INFO 2022-12-2000 INFO 2022-12-	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wm nfci0 ngr:10 nproc:4 pid:902 platfi n:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:50 transport/transfer_windows.go:92 transport/transfer_windows.go:92	SC CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get cont receive I send ha received	angletical magnetics 30GHz cpt_usage:0.416666667 dns: n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter ifault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000 nection successfully; idc default,region mandler running Incommend	
3 -	2000 time:1671184595 cpu:0.00000000 q du:35944432 gateway: host_id: host_mod nem_usage:0.38000000 net_mode:unknc olatform_family:windows platform_versio x_tps:0.0000000 start_time:1671514709 write_speed:+Inf] 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wom fdf:0 ngr:10 nproc:4 pid:9029 platfi on:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:60 transport/transfer_windows.go:131 transport/transfer_windows.go:132 enviroi/enviroing.go:104 generion aluging	5C CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get cont receive I send hat received	30GHz cpr_usage:0.41666667 dns: on:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000 nection successfully: idc default,region nandler running ndler running command	
武 (二)	2005 time:1671184595 cpu:0.00000000 cj diu:35944432 gateway: host_id: host_mod hem_usage:0.38000000 net_mode:unknc olatform_family:windows platform_versio x_tps:0.00000000 start_time:1671514709 wite_speed:+inf] 2022-12-20113:38:29.961+0800 INFO 2022-12-20113:38:29.961+0800 INFO 2022-12-20113:38:29.961+0800 INFO 2022-12-20113:38:30.088+0800 INFO 2022-12-20113:38:30.088+0800 INFO 2022-12-20113:38:30.088+0800 INFO	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wom fdi:0 ngr:10 nproc:4 pid:9029 platfi on:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:131 transport/transfer_windows.go:132 transport/transfer_windows.go:138 plugin/plugin.go:198 syncing plugins plugin/plugin.go:198 syncing plugins	SC CPU @ 2. kernel_versic orm:Microso Inf region:de 8589373440 get cont receive I send hat received	30GHz cpt_usage:0.41666667 dns: n:10.0.17763 Build 17763 ft Windows Server 2019 Datacenter fault rss:14577664 rx_speed:0.00000000 tx_speed:0.00000000 tx_tps:0.00000000 nection successfully: idc default,region nandler running ndler running command ("plugin": "collector." "puper:: "1.0.0.140"	
武 (二)	Doot_time:167118495 cpu:0.0000000 c1 ui:3594432 gateway: host_id: host_mod mem_usage:0.3800000 net_mode:unknc latform_family:windows platform_versio x_tps:0.0000000 start_time:1671514709 write_speed:+Inf] 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:29.961+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO 2022-12-20T13:38:30.088+0800 INFO	pu_name:Intel(R) Xeon(R) Platinum 833 del: host_serial: host_vendor: idc:default wm nfci0 ngr:10 nproc:4 pid:902 platfi n:10.0.17763 Build 17763 read_speed:+ state:running state_detail:[] total_mem: transport/transfer_windows.go:50 transport/transfer_windows.go:3131 transport/transfer_windows.go:328 plugin/plugin.go:138syncing plugins plugin/plugin.go:138syncing plugins plugin/plugin.go:138syncing plugins plugin/plugin.go:1311.adt437a23bc	5C CPU @ 2. kernel_versio orm:Microso Inf region:de 8589373440 get com receive I send hai received is loading	andler running command ("plugin": "collector", "pver": "1.0.0.140"	

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;

 通过代理集群 云等业务场景 	f,可将无法连接公网的服务器接入有底云安安全卫土,适用于无法直接连接到有底云安安全卫土的 {	I线下IDC机房、混合
安装命令		
请在服务器上执行	〒下面命令安装代理,此安装命令仅针对当前代理使用	
bash -c "if (co beijing.volces. cdn=http://hic else (wget -q proxyID= ac=csc-hid	ommand -v curl); then (curl -sS http://hids-online-cn-beijing.tos-cn- com/agent/install_proxy.sh bash -sproxyID=6718889bf3dd34805f770cd ds-online-cn-beijing.tos-cn-beijing.volces.comac=csc-hids-agent.hids.volc -O - http://hids-online-cn-beijing.tos-cn-beijing.volces.com/agent/install_pri =6718889bf3dd34805f770c0bcdn=http://hids-online-cn-beijing.tos-cn-beij s-agent.hids.volces.com:443); fi"	0b æs.com:443); oxy.sh bash -s jing.volces.com
卸载命令 _{青在服务器上执行}	丁下面命令安装代理,卸载后相关客户端将无法接入云安全中心	
	ommand -v curl); then (curl -sS http://hids-online-cn-beijing.tos-cn-	



- 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)--