目录

如何卸载服务器安全

若您不再需要服务器安全防护，可将其卸载，下面介绍了卸载的具体方式

旧版服务器安全

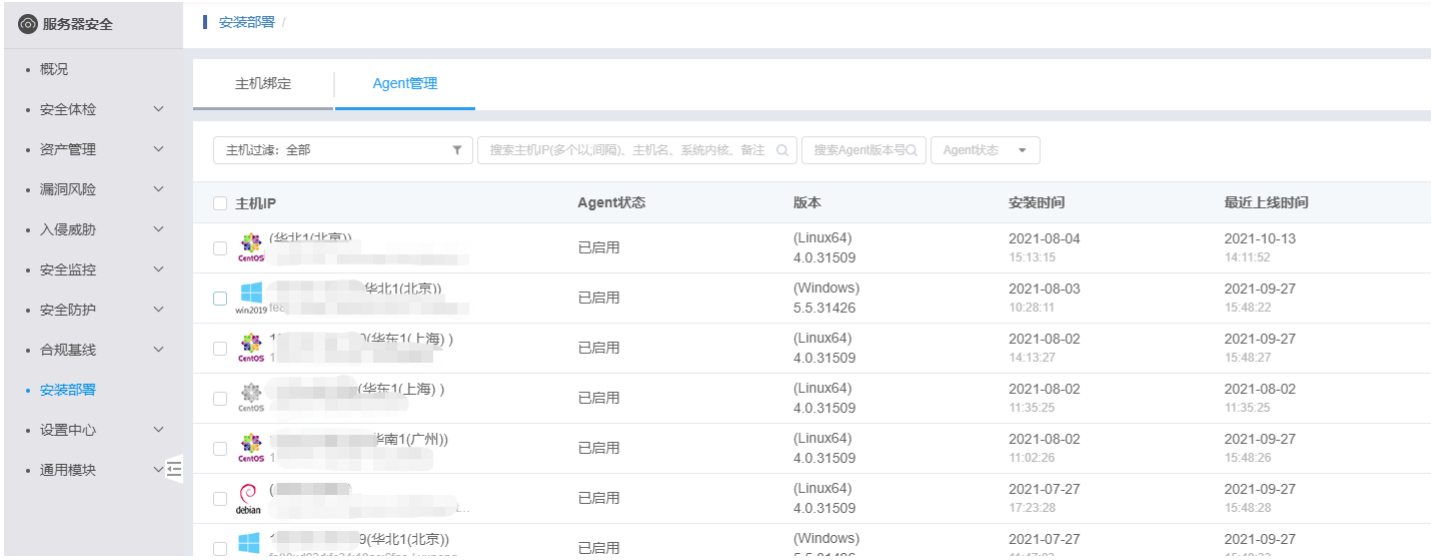
系统卸载

- Windows系统 依照路径C:Program Files\KsyunAgent\uninst.exe，找到 uninst.exe 文件，双击即可卸载。
- Linux 系统 输入命令/etc/KsyunAgent/uninstall.py 即可卸载。

新版服务器安全

控制台卸载

您可登录服务器安全控制台，进入**安装部署**页面，点击Agent管理，选择需要卸载的服务器，点击**卸载**按钮即可。



系统卸载

- Windows系统 依照路径C:Program Files(x86)\Ksyunsec\KsyunsecServer\uninst.exe，找到 uninst.exe 文件，双击即可卸载。
- Linux 系统 输入命令/etc/ksyunsec/script/uninstall.py即可卸载。

各规则库的更新机制是怎样的？

1. Windows漏洞库每月更新一次，Linux漏洞库不定期更新。
2. Windows系统漏洞补丁每月更新。
3. 应急漏洞规则库不定期更新。
4. webshell规则库不定期更新。
5. 病毒库每周四更新。
6. 插件库不定期更新。
7. 客户端安装包不定期更新。

服务器安全是怎么工作的？

用户按照金山云下载页面的提示安装客户端，安装成功后，控制台会显示服务器防护状态；

用户在控制台上可以选择开启对应的防护，并自定义选择多种告警方式。客户端检测到异常后，可以在控制台的“服务器安全”中查看详细的异常信息，同时系统会发送告警邮件和告警短信至用户注册的邮箱和手机。

Nginx该如何使用安全客户端

客户端现在只支持Apache 2.0 和IIS 的web 防护。如果用户使用其他的web 服务器，安装客户端时跳过web防护模块即可。

服务器安全客户端支持IIS7.0 及以上版本吗？

支持，需要在IIS7.0 及以上版本中安装IIS6 兼容模式。但是服务器安全客户端针对IIS7.0 及以上版本中接收Ajax 发送POST 数据的功能目前暂不支持，如需针对IIS7.0 及以上版本防护，请联系金山云技术人员进行协助安装。

不安装Apache 防护或者IIS 防护模块，其他模块能正常工作吗？

各个模块都是相互独立的，不安装Apache 防护或者IIS 防护模块，不会影响其他模块正常运行。

没有公网IP的服务器可以使用服务器安全么？

不可以，客户安装在服务器中的安全管家客户端需要通过公网IP与金山云云端服务器、病毒库服务器保持必要的心跳同步，并将客户端生成的安全告警日志上传到服务器。

服务器安全客户端可以卸载吗？

可以，如正常Windows、Linux 程序一样卸载。卸载完成后，进入控制台查看服务器安全功能，会看到对应服务器的防护状态显示为“离线”。

服务器安全客户端会收集用户信息吗？客户端会上传什么数据到服务器？

服务器安全客户端不会收集用户信息，只会与金山云云端服务器、病毒库服务器保持必要的心跳同步，并将客户端生成的安全告警日志上传到服务器。

客户端与服务端的数据传输方式是如何的？会导致数据泄露吗？

客户端采用的是SSL 加密的传输方式将数据传输至服务端，这种加密协议的安全性非常高，不会导致数据泄露。

暴力破解具体是如何识别的？

针对RDP 和SSH 的暴力破解是通过日志解析进行识别的，而针对FTP 、MySQL 的暴力破解则是通过网络报文解析进行识别。

暴力破解的检测频率是多少？

系统登录的暴力破解检测，是根据用户自定义配置的间隔时间来进行的。FTP 与MySQL 的暴力破解检测是实时进行的。系统登录暴力破解是根据日志进行事后分析阻断的，因此建议用户将检测间隔设置为一个较小的时间，建议在1-3 分钟。

暴力破解是如何进行防御的？

防暴破破解功能，在Windows系统下基于网络驱动程序在内核层实现IP的封禁；而Linux系统下则是通过维护IPtable来进行IP封禁。