

目录

目录	1
服务器列表	2
安全客户端	2
安装Linux版客户端	2
卸载Linux版客户端	3
安装Windows版客户端	3
卸载Windows版客户端	4
防护数据	4
功能设置	5

服务器列表

进入云安全→服务器安全，可以看到如下信息



- 今日服务器安全概况

用户账号此数据中心下，所有服务器的今日安全概况，包括登录权限、后门程序、系统补丁、暴力破解、网站安全五个部分，每个部分具体对应的防护功能，详见服务器安全[产品描述](#)

- 服务器名称：

用户在创建服务器时自定义的服务器名称

- IP地址：

服务器绑定的公网IP和内网IP

- 客户端状态：

“未安装”，表示服务器还未安装安全管家客户端，安装方法详见用户手册[安全客户端](#) “在线”，表示用户服务器已安装客户端，且和云端服务器通信正常，可获取到防护数据 “离线”，表示用户服务器已安装客户端，且曾经和云端服务器通信成功过，但当前不在通信状态

- 安全情况：

此服务器今日的防护信息，若无安全情况，则显示为“服务器今日暂无安全威胁”

安全客户端

在服务器列表页点击“安装服务器管家”



进入下载页面



安装Linux版客户端

下载方法一：在Linux安装区域点击“Linux32位 点击下载”或“Linux64位 点击下载”按钮，下载服务器管家安装包，将客户端复制到服务器

下载方法二：64位系统在服务器执行命令 wget http://www.ksyun.com/sec-st/KsyunAgent_linux64.tar.gz；32位系统在服务器执行命令 wget http://www.ksyun.com/sec-st/KsyunAgent_linux32.tar.gz

进行解压，tar -zxvf KsyunAgent_linux64.tar.gz

进入解压后的目录，以root权限执行 ./install.py（或 python install.py）

```
[root@KsyunAgent_linux64]# python install.py
1.1 Start install KsyunAgent..
1.2 Install common file
1.3 Start the application
1.4 Install apache plugin

step 0/0, start install Apache Defense Module..
step 0.1, start install Apache Defend Module..
step 0.2, copy libraries
step 0.3, copy bin and set boot
step 0.4, restart the apache server..

Tips:
(1)If you want to check apache defense module log, please use command: sdaalog;
(2)If apache defense module is failed to use, you can try to restart Apache service.
1.5 install completely!
```

如需安装apache防护模块且程序未自动识别到apache服务路径，请手动填写，或直接回车略过。注：如需安装Web服务器防护模块，请预先安装Apache服务器（目前支持Apache2.2及以下版本）

```
[root@KsyunAgent_linux64]# ./install.py
1.1 Start install KsyunAgent..
1.2 Install common file
1.3 Start the application
1.4 Install apache plugin

step 0/0, start install Apache Defense Module..
step 0.1, input apache configuration file's path: [enter "CTRL+c" to exit]
The path must be a configuration file.
For example: /usr/local/apache/conf/httpd.conf
Please input the absolute path:
```

为支持数据库弱口令扫描，需修改Mysql配置文件（如：/etc/my.cnf），添加红框中标注的配置

```
[mysql]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

[client]
socket=/var/lib/mysql/mysql.sock
```

卸载Linux版客户端

进入安装程序解压目录，如：/home/test/KsyunAgent_linux64.tar.gz

执行 ./uninstall.py 即可

```
[root@KsyunAgent_linux64]# python uninstall.py
Start uninstall..
uninstall apache plugin..

remove load information in apache.. [ok]
remove file of Apache Defense Module.. [ok]
restart apache server.. [ok]
uninstall apache defense module succeed..
stop the application..
uninstall file..
uninstall completely!
```

安装Windows版客户端

下载方法一：在Windows安装区域点击链接，下载服务器管家安装包

下载方法二：32位及64位系统服务器均可通过浏览器访问地址 http://www.ksyun.com/sec-st/KsyunAgent_1.0.12845_Installer.exe

将客户端程序复制到服务器，以管理员权限安装客户端程序



点击“下一步”，选择安装路径，继续点击“下一步”，直到安装完成。若已安装过KsyunAgent，选择“是”进行覆盖安装。注：如需安装Web服务器防护模块，请预先安装IIS服务器。（目前支持IIS6.0模式，如安装IIS版本大于6.0[如IIS 7.0, IIS 7.5]，请在安装过程中勾选兼容IIS 6.0模式）



卸载Windows版客户端

进入安装目录，如：C:\Program Files(x86)\KsyunAgent

双击uninst.exe，弹出对话框，点击“是(Y)”即可完成卸载。备注：卸载过程中可能弹出对话框，点击 yes / retry 即可继续完成卸载



防护数据

在服务器列表页选择某个服务器，点击后面的“查看服务器安全数据”



点击左侧的二级菜单，查看各个防护项的历史数据

二级菜单包括登录权限、后门程序、系统补丁、暴力破解、网站安全五个部分，每个部分具体对应的防护功能，详见服务器安全[产品描述](#)

时间	攻击IP	被攻击端口
2017-02-24 15:31:05	192.168.1.1	22
2017-02-24 15:31:05	192.168.1.1	22
2017-02-24 14:51:05	11.11.11.2	22
2017-02-24 14:41:05	20.20.20.4	22
2017-02-24 14:21:05	21.21.21.5	22
2017-02-24 14:21:05	21.21.21.5	22

功能设置

在服务器列表页选择某个服务器，点击后面的“查看服务器安全数据”

服务器名称	IP地址	客户端状态	安全情况	操作
<input type="checkbox"/> sec_test	10.0.0.22(内) 120.92.128.186(外)	在线	✓ 服务器今日暂无安全威胁	查看服务器安全数据

点击左侧二级菜单的“设置”，进入设置页面，用户可以选择开关各个防护项

登录权限
系统弱口令 <input checked="" type="checkbox"/> 数据库弱口令 <input checked="" type="checkbox"/> 数据库权限 <input checked="" type="checkbox"/> 异地登录 <input checked="" type="checkbox"/> 配置
后门程序
系统webshell <input checked="" type="checkbox"/> 病毒 <input checked="" type="checkbox"/>
系统补丁
系统补丁 <input checked="" type="checkbox"/>
暴力破解 <small>(开启FTP暴力破解功能将占用服务器一定资源)</small>
远程桌面暴力破解 <input checked="" type="checkbox"/> 间隔时间: <input type="text" value="600"/> 秒 尝试登录次数: <input type="text" value="5"/> 次 FTP暴力破解 <input checked="" type="checkbox"/> 间隔时间: <input type="text" value="600"/> 秒 尝试登录次数: <input type="text" value="5"/> 次 端口: <input type="text" value="21,22"/>
网站安全
应用漏洞 <input checked="" type="checkbox"/> webshell上传 <input checked="" type="checkbox"/> CC攻击 <input checked="" type="checkbox"/>

注意：

- FTP暴力破解功能默认关闭，若开启此功能，将占用服务器一定资源
- 暴力破解检测的间隔时间默认12秒，尝试登陆次数默认10次，若12秒内10次登陆失败，则发出告警通知，用户可自主修改此项防护设置
- 异地登录功能需要用户设置常用登录地，最多可设置10个市级登录地

设置常用登录地

城市：

国家	省/直辖市/地区	<input checked="" type="checkbox"/> 市级
中国	<input checked="" type="checkbox"/> 北京市	<input checked="" type="checkbox"/> 北京市
	<input type="checkbox"/> 天津市	
	<input type="checkbox"/> 上海市	
	<input type="checkbox"/> 重庆市	
	<input type="checkbox"/> 香港	
	<input type="checkbox"/> 澳门	

城市：(最多可选10个城市)，已选 4 个

云安全 > 服务器安全 > WAF_Qiuyanjie 上海3区(VPC) 上海3区(Basic)

登录权限

系统弱口令 数据库弱口令 数据库权限

异地登录 北京市 天津市 上海市 重庆市