

TopAV服务端安装教程

天融信防病毒管理平台安装说明

最低系统要求

- 操作系统: Centos7.2.1511+(内核3.10.0-327+)
- 内存: 16G
- cpu: 8核
- 硬盘: 500G

建议测试环境配置

- 操作系统: Centos7.2.1511+(4.4.78-1.el7.elrepo.x86_64+)
- 内存: 32G
- cpu: 16核
- 硬盘: SSD 1T

安装分区要求

- 单独划分 `/topsec` 分区: 安装系统时选择手动分区, 进入后自动点击自动创建, 将 `/home` 修改为 `/topsec` 即可

依赖环境

- Centos7.2.1511+(内核3.10.0-327+)
- docker 1.12.5+
- docker-compose 1.13.0+

依赖安装

外出安装:

- 将网盘文件 `Docker.tar.gz` 上传到服务器后 `tar -zxvf Docker.tar.gz` 进行解压
- 进入到docker目录,执行 `yum -y install *.rpm` 进行安装
- 进入到 `docker-compose` 目录,执行 `yum -y install *.rpm` 进行安装
- 关闭防火墙和selinux, 执行 `service firewalld stop && chkconfig firewalld off && setenforce 0 && sed -i 's/SELINUX=enforcing/SELINUX=disabled/`

公司内安装:

- 关闭防火墙和selinux, 执行 `service firewalld stop && chkconfig firewalld off && setenforce 0 && sed -i 's/SELINUX=enforcing/SELINUX=disabled/`
- `yum install docker python-pip -y && chkconfig docker on && pip install docker-compose`

安装

- 执行 `systemctl enable docker && systemctl start docker` (设置docker开机自动启动, 并立即启动docker)
- 上传网盘文件 `Server` 文件夹下的所有文件至服务器后执行 `tar -zxvf topav-1.13.3.tar.gz` 解压docker镜像;解压完成后执行 `docker load -i topav-1.13.3.tar` 加载docker镜像
- 执行 `tar -zxvf topav-1.13.3-compose.tar.gz` 解压compose文件, 解压后进入到 `topav-master...` 执行 `make install`
- 执行 `topav up` 启动服务

注意:

* 安装说明中的版本可能不是最新版, 最新版的安装包找公司获取, 文档中的安装包名称和最新版不同时自行理解对应

注: 如果是现场环境,需启动 `node-monitor` (系统挂后自动重启功能),先执行 `systemctl enable node-monitor` 以使其开机自启动

注: 启动 `node-monitor` 后, 不用再执行 `topav up` 命令, 平台会自己启动, 如果一分钟内没有启动, 请编辑 `/etc/sudoers`, 将 `Defaults requiretty` 所在行注释掉, 然后执行 `service node-monitor restart`。

使用

注: 如果是测试环境请先手动执行 `service node-monitor stop` 命令,停止对docker集群的监控

- `topav up` # 创建集群并启动
- `topav down` # 停止集群并删除(一般情况下不建议使用该项)
- `topav start` # 启动集群
- `topav restart` # 重启集群
- `topav stop` # 停止集群
- `topav ps` # 查看集群状态

平台开放服务地址

注: 以设备IP192.168.1.100为例

- 平台管理界面: `https://192.168.1.100`
- 客户端下载界面: `http://192.168.1.100`
- 上报接口服务: `https://192.168.1.100:8090`

其它说明

license使用方法

软件版: 登陆系统在 **系统管理 - 系统信息** 里点击 **生成license请求文件**, 点击 **生成文件**。将生成的文件发送给license制造者, 制造license。拿到license后, 在相同页面点击 **上传License文件**。

硬件版: 插上Ukey, 虚拟机挂载ukey。(usb驱动优先选1.1, 经测试1.1比较稳定)

上传客户端\升级包\离线安装包

- 授权完成后即可进行客户端上传操作, 客户端文件为网盘文件中的 `WindowsClient` 所有文件
- 录系统管理中心, 进入到 **终端中心 > 终端升级**; 点击 **上传升级包** 选择 `topsec_ESendpoint_20180323.zip` 上传, 上传完成后点击 **启用**

升级包管理

刷新

上传升级包

删除

启用

同步

配置

平台类型	升级包版本	架构	大小	上传时间
windows	2018-03-18 16:14:20		20.12MB	2018-03-23 15:54:29
windows	2018-03-26 15:05:57		20.14MB	2018-03-27 17:37:16

<

总条数为 2 条(显示 1 到 2)

每页显示10条记录

安装包管理

刷新

上传安装包

删除

启用

平台类型	安装包版本	架构	大小	上传时间
windows	1.0.1.10		1.61MB	2018-03-23 15:54:39
windows	1.0.1.9		1.61MB	2018-03-27 17:37:16

<

总条数为 2 条(显示 1 到 2)

每页显示10条记录

离线包管理

刷新

上传安装包

删除

安装包版本	大小	上传时间
offline	15.09MB	2018-03-27 17:37:16

<

总条数为 1 条(显示 1 到 1)

每页显示10条记录

- 点击 **上传安装包** 选择 `installer_1.0.1.10.exe`, 上传完成后点击 **启用**
- **离线包管理** 上传点击 **上传安装包** 选择 `offline_installer_offline.exe` 上传并启用

客户端安装

- 登录服务端, 进入到 **终端中心 > 终端管理**; 添加右键ALL选择添加部门分组信息

天融信终端威胁防御系统

终端中心策略中心统计报表系统管理

> 终端中心 >> 终端管理 | 终端任务 | 终端升级 |

导入导出

按部门显示

All

新建

删除

重命名

责任人IP地址MAC地址终端类型

刷新修改修改部门删除修改策略任务下发标签操作

责任人	所在部门	终端IP
数据为空		
<		
总条数为 0 条(显示 0 到 0)		每页显示 25 条

- 在客户PC的浏览器中登录 <http://服务端地址> 下载客户端，选择部门信息进行安装