# 天翼云·服务器安全卫士
# 用户使用指南

中国电信股份有限公司云计算分公司

# 1 产品介绍

## 1.1. 产品定义

服务器安全卫士通过在服务器安装轻量级 agent 进行监测和防护,与防护中心的规则进行联动,实时感知和防御入侵事件，对高危事件可以对客户通过邮件进行告警。功能涵盖：异常登录，资产清点，漏洞扫描、文件一致性检测、文件防篡改、基线检查。

## 1.2. 功能特性

1、Agent 集中管理一键安装,自动激活。

2、文件防篡改检测提早发现潜在威胁。

3、对云主机进行实时监测实时进行安全事件上报。

4、Agent 资源占用极低 cpu 使用率不到 1%。

## 1.3. 名词解释

【Agent】：指服务器安全监测与防护代理软件，运行在客户服务器操作系统，该安全代理具备严格的权限和运行负载控制，保护服务器的同时对业务运行不产生影响。

## 1.4. 产品功能

| 功能 | 描述 | 规则说明 |
| --- | --- | --- |
| 概览 | 1、统计帐号下的服务器数量及防护状态、风险状态、待处理告警信息、最近 7/30 天已处理告警信息、服务器端口、进程、软件、账号资产清点及排名。 | 实时统计最新数据。 |
| 服务器 | 1、展示账号下服务器列表信息,可对服务器进行安装、卸载 agent;对服务器进行开启防护、关闭防护操作。可查看单台服务器的详细信息,包括基本信息、资产清点、异常登录、漏洞扫 | agent 状态判断：控制台会每隔 2 分钟调一次服务端接口获取 agent 状态。如果 Agent 没 |

| | | |
|---|---|---|
| | 描、文件一致性检测。 | 有按时上报在线信息，服务器端则在 4 分钟后判定该服务器不在线，且在管理控制台中此 agent 状态显示为离线。<br><br>Agent 自动卸载：agent 在线的情况下，点击卸载后 3 分 30 秒后，agent 状态变为离线。 |
| 资产清点 | 支持对服务器监听端口的清点，可查看监听端口最新数据；支持对服务器运行进程的清点，可查看运行进程最新数据；支持对服务器账号的清点，可查看账号最新数据和变动数据；支持对服务器安装软件的清点，可查看软件最新数据和变动数据。 | 每 12 小时收集一次。 |
| 漏洞扫描 | Linux 软件漏洞：对标 CVE 官方漏洞库，提供系统软件漏洞的自动检测，并提供修复方案。系统软件漏洞功能可检测出服务器上的 Vim、Bind、及 OpenSSL 等软件漏洞。支持将漏洞加入白名单进行管理。 | 每 24 小时自动检测一次。 |
| 入侵检测 | 异常登录告警类型支持异地登录、爆破登录、非法 IP 登录、非法账号登录、非法时间登录；可对登录安全进行自定义设置，包括对合法登录地、合法 IP、合法登陆时间和合法账号账号进行设置；系统对可疑入侵行为进行拦截，并记录拦截结果。 | 实时检测，只会对第一次异常登录行为进行告警。异地登录只对公网 IP 进行告警。 |
| 文件一致性检测 | 支持对用户重点关注的文件一致性进行检测，可查看检测结果列表，可配置检测规则，并将规则下发到服务器。 | 实时检测。每台服务器最多可添加 10 个防护目录，Linux 系统单个防护目录大小不超过 5G；单个防护目录下的文件夹个数不超过 3000 个；防护目录文件夹层级不超过 20 个；单文件大小不超过 3MB。<br><br>目前不支持 Windows |

| | | |
|---|---|---|
| | | 版 |
| 网页防篡改 | 可添加、修改、删除防篡改规则，规则中可设置防篡改目录，排除子目录，排除文件等，支持将防篡改规则下发至服务器。 | 实时检测。每台服务器最多可添加 10 个防护目录，Linux 系统单个防护目录大小不超过 5G；单个防护目录下的文件夹个数不超过 3000 个；防护目录文件夹层级不超过 20 个；单文件大小不超过 3MB。<br>目前不支持 Windows 版 |
| 基线检查 | 支持创建基线策略，支持将检查项加入白名单。 | 关闭防护后，将同步删除策略中的服务器信息。目前不支持 windows 版. |
| 设置 | 支持对异常登录、漏洞扫描配置告警，告警方式可选择支持邮件方式。 | 异常登录告警实时发送，只会对第一次异常登录行为进行告警，漏洞报告按周发送。 |

# 2 快速入门

## 2.1. 开通方式

服务器安全卫士（基础版）属于免费服务，用户可通过天翼云控制台开通使用。

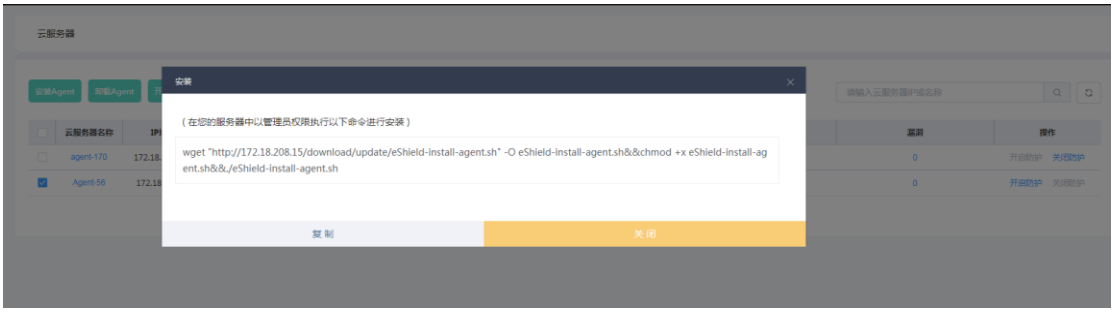
## 2.2. Agent 说明

服务器安全卫士管理控制台会每隔 2 分钟调一次服务端接口获取 agent 状态。

如果 Agent 没有按时上报在线信息，服务器端则在 4 分钟后判定该服务器不在线，且在管理控制台中此 agent 状态显示为离线。

## 2.3. 安装 Agent

**说明：** Agent 插件已集成于天翼云默认公共镜像中。您也可参考为您的天翼云服务器手动安装 Agent 进行防护。（如果您登录服务器安全管理控制台 - 服务器列表页面，查看您所有服务器的 Agent 在线状态。若您的服务器 Agent 显示离线状态，请勾选服务器后，点击安装 Agent 按钮，在弹出框内查看安装指导。）




Agent 手动安装脚本会自动根据您的云服务器的操作系统版本安装相对应的 Agent 版本，并在成功安装后一分钟在云服务器列表中显示为在线状态。


## 2.4. 开启/关闭防护

Agent 在安装后显示为在线状态，此时选中需要开启保护的服务器，单击开启防护按钮， 可开启防护，如不需防护，点击关闭防护按钮，可关闭防护。

在开启防护后，如 agent 在线，则防护状态为“防护中”如 agent 不在线，防护状态为“暂停防护”，在关闭防护成功后，防护状态为“未开启”。

## 2.5. Agent 离线排查

如果您的 Agent 处于离线状态，请按照以下步骤进行排查：

1、登录您的服务器查看 Agent 相关进程是否正常运行。

如果 Agent 相关进程无法运行，建议重启您的服务器，或者参考 **安装 Agent** 重新装 Agent。

在您的云服务器上查看相关进程是否正常。

```
/var/ctcss/bin/ctcss-agentd
/var/ctcss/bin/eShield-modulesd
```

2、如果首次安装 Agent 的服务器在安装完成后显示状态为离线，请尝试参考以下方式重新启动 Agent：

**Linux 系统**：执行/var/ctcss/bin/ctcss-control restart 命令

3、检查您的服务器网络连接是否正常。

**服务器有公网 IP （如经典网络、EIP、云外机器）**

**Linux：** 执行 ping www.ctyun.cn -s 1000 命令。

**服务器无公网 IP （如金融云、VPC 专有网络）**

**Linux：** 执行 ping www.ctyun.cn -s 1000 命令。

4、检查您的服务器 CPU、内存是否长期维持较高占用率（如 95%、100%），此情况可能导致 Agent 进程无法正常工作。

## 2.6. 卸载 Agent

您可以通过以下方式在天翼云服务器安全卫士管理控制台中自动卸载 Agent：

**注意：** 通过该种方式卸载指定 Agent，请务必确保当前机器 Agent 处于在线状态，否则无法接收到卸载指令。如果卸载后重新安装 Agent，请手工进行安装，忽略期间的报错，（ Agent 会在重新安装后 10 分钟在线）

1、登录天翼云服务器安全管理平台，点击云服务器列表

2、点击卸载 Agent

# 3 购买

## 3.1. 价格

服务器安全卫士（基础版）免费。

## 3.2. 购买

支持线上开通和线下开通两种方式。线上通过控制台进行在线开通，线下通过客户经理完成开通。

## 3.3. 规格变更

服务器安全卫士（基础版）目前不支持规格变更。

## 3.4. 续订

服务器安全卫士（基础版）目前不支持续订。

## 3.5. 退订

服务器安全卫士（基础版）目前不支持退订。如不需要安全服务，将已开启的服务器设置为关闭防护状态即可。

# 4 操作指南

## 4.1. 开通服务

用户在控制台点击“服务器安全卫士（基础版）”，阅读并同意服务协议后，直接开通服务。

**前提条件：**已获取管理控制台的登录账号与密码。

**操作步骤：**

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

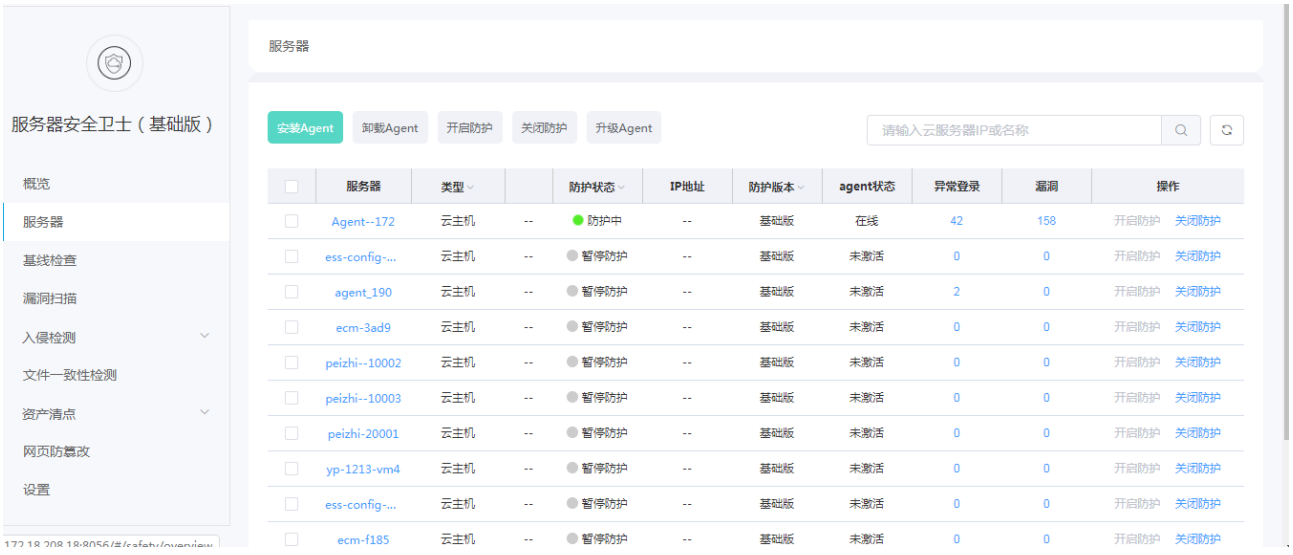
2 在页面右上方选择“地域”后，点击安全>服务器安全位置菜单。

## 4.2. 安装 agent

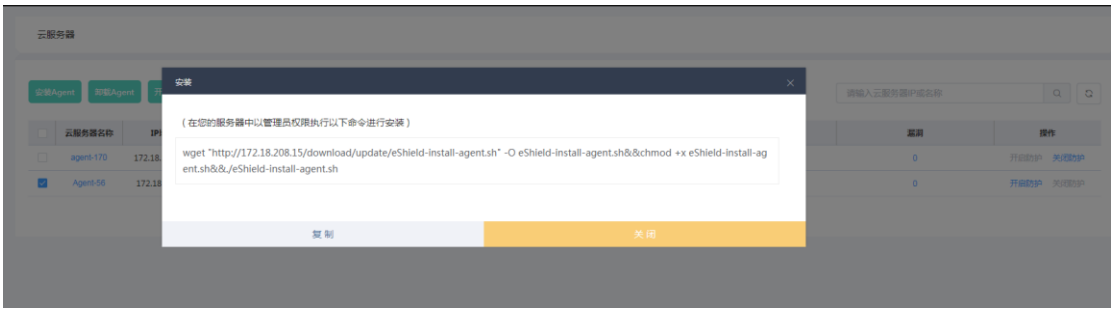
安装 agent 后，您才能对服务器开启安全防护。目前支持 Linux 系统安装 agent。

**操作步骤：**

1 在服务器列表页面，选中服务器，点击安装 agent 按钮。




2 弹出安装提示，按照提示进行安装。



# 4.3. 开启/关闭安全防护

开启防护时，选中一台服务器，点击开启防护按钮，系统对服务器开启实时防护。

关闭防护时，选中要关闭的服务器，点击关闭防护按钮，系统对服务器关闭防护。

**前提条件：**

1 服务器 agent 在线。

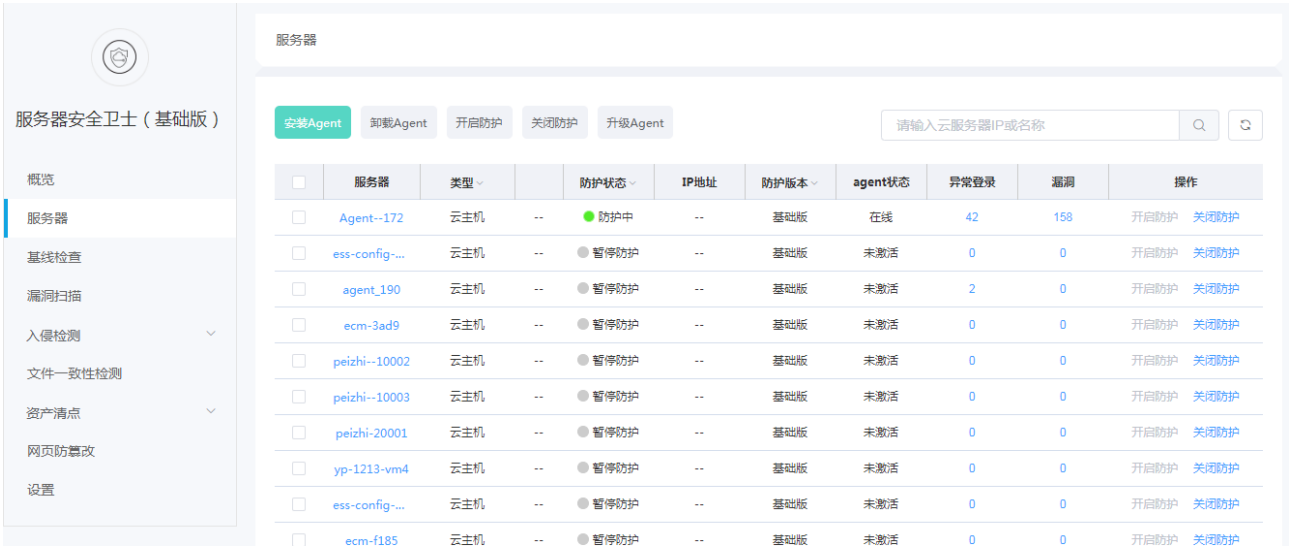
**操作步骤：**

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

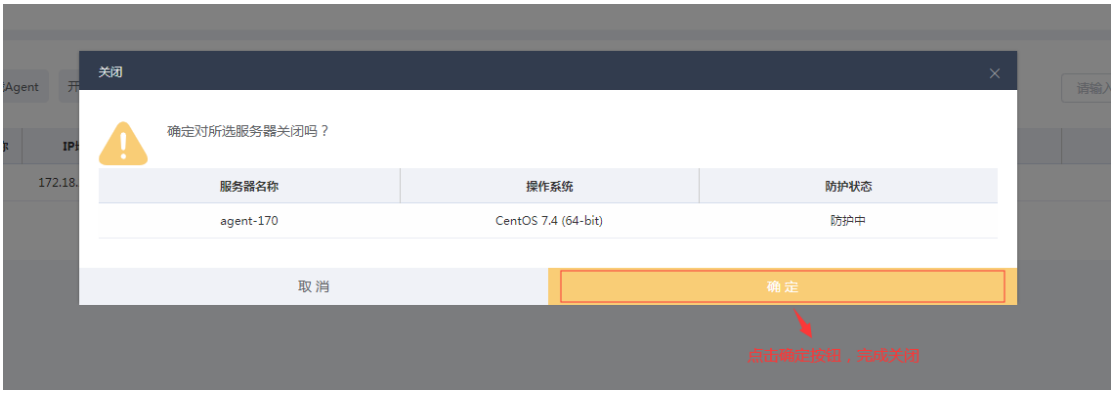
3 在左侧导航中点击“服务器”菜单。

4 在服务器列表中选中要开启的服务器，点击开启防护按钮。




5 开启防护完成后，在服务器列表查看防护状态，正常显示为“防护中”。


如需关闭防护，可在服务器列表中选中服务器，点击关闭防护按钮，弹出框内点击确定按钮，会关闭防护。



**提示：**

1 关闭防护前，请对服务器执行全面检测，处理已知风险并记录操作信息，避免运维失误，使您的服务器遭受攻击。

2 关闭安全服务后，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。

3 关闭安全服务后，您可将空余的配额分配给其他服务器继续使用，避免造成配额资源的浪费。

## 4.4. 服务器安全概览

服务器安全卫士-概览页面，包括云服务器的数量、防护状态、服务器风险统计、服务器待处理告警、服务器安近 7 天/30 天安全运营数据，服务器端口、账号、进程、软件总体数据及各项排名数据。

**操作步骤：**

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“概览”菜单，查看概览信息。

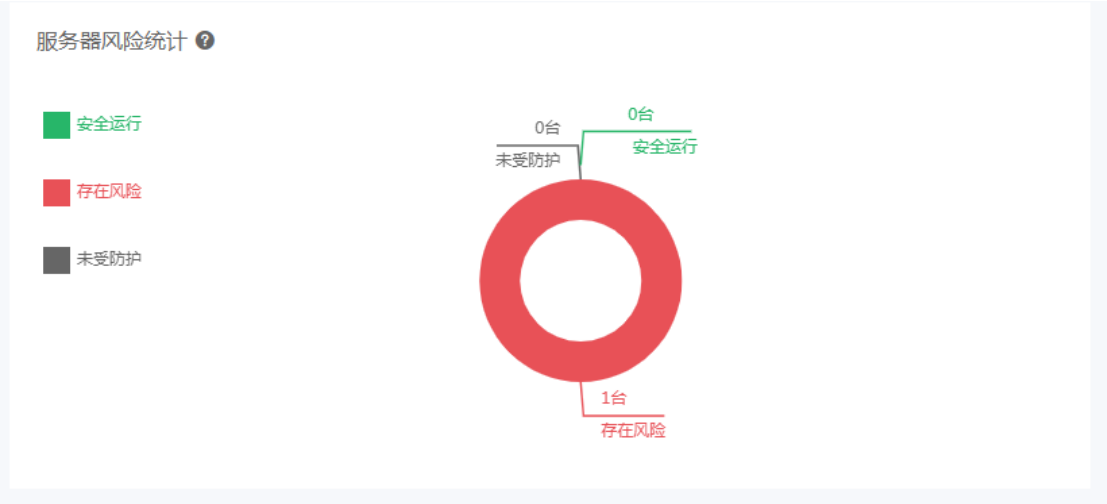
a 服务器数量统计：


服务器数量：账户下的服务器总台数。

防护数量：防护状态为“防护中”和“暂停防护中”的服务器总台数。

未开启：防护状态为“未开启”的服务器总台数。

b 服务器风险统计：




存在风险：在“防护中”和“暂停防护中的”服务器中，有异常登录或漏洞扫描未处理的服务器数量。

安全运行：在“防护中”和“暂停防护中的”服务器中，无异常登录或漏洞扫描未处理的服务器数量。

未受防护：防护状态为“未开启”的服务器数量。

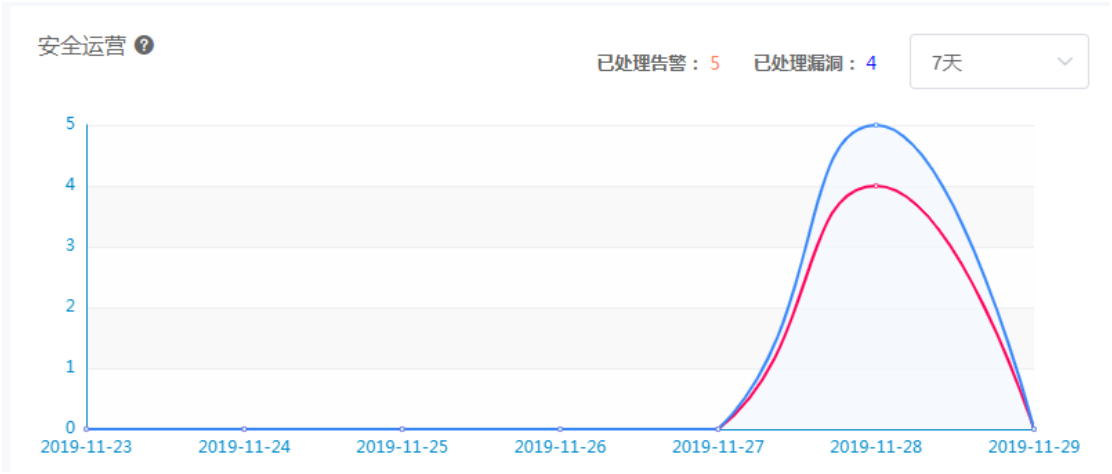
c 待处理信息：


异常登录：异常登录中未处理告警的数量，点击可跳转至异常登录页面查看详细信息。

系统漏洞：漏洞管理中未处理告警的数量，点击可跳转至漏洞管理页面查看详细信息。

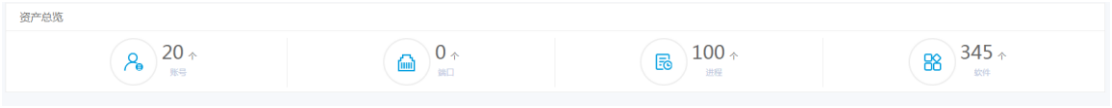
文件一致性：文件一致性检测中未处理的数量，点击可跳转至漏洞管理页面查看详细信息。

d 安全运行状况：



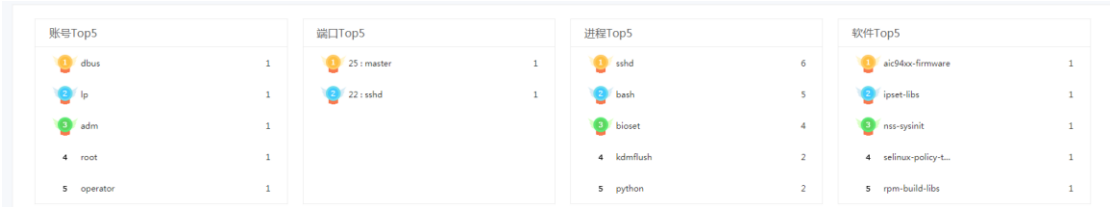

显示已处理的异常登录和漏洞数据，支持按 7 天和 30 天查看。

e 资产清点数据：




显示本地域内的服务器中账号、端口、进程、软件数量的总和。点击可跳转至对应页面查看详细信息。

f 资产清点数据排名：




显示账号、端口、进程、软件各项前五名及对应数据。

## 4.5. 服务器列表

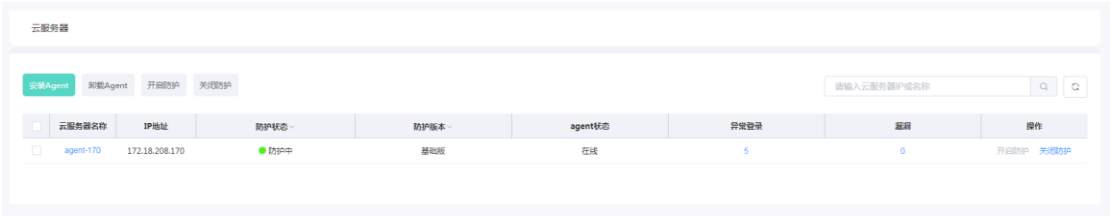
服务器列表包括服务器基本信息和安全防护信息，可通过列表页查看服务器名称、IP、防护状态，agent 在线状态等信息。

**操作步骤：**

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“服务器”菜单，查看服务器信息。




| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 云服务器 | 云服务器的名称。 | 点击服务器名称，跳转至服务器相信信息页面。 |
| IP 地址 | 云服务器对应的 IP 地址。 | |
| 防护状态 | 云服务器防护状态，包括“防护中”、“暂停防护中”、“未开启”<br>支持按防护状态筛选服务器。 | 防护中:表示已开启防护，且 agent 在线。<br>暂停防护中:已开启防护，agent 离线。<br>未开启：为开启服务器安全防护。 |
| 防护版本 | 服务器分配的配额版本。 | 当前只有基础版。 |
| Agent 状态 | 服务器安装的 Agent 的状态，包括在线，离线。<br>支持按防护状态筛选服务器。 | |

| | | |
|---|---|---|
| 异常登录 | 服务器未处理的异常登录告警信息条数。 | 点击可跳转至服务器详情页面中的异常登录模块 |
| 漏洞 | 服务器未处理的漏洞信息条数。 | 点击可跳转至服务器详情页面中的漏洞管理模块 |
| 操作 | 开启、关闭按钮，可对主机开启、关闭防护。 | 对于“防护中”和“暂停防护中”状态的服务器，可点击关闭按钮。<br>对于未开启状态的服务器，可点击开启按钮。 |

4 在列表信息中点击服务器名称，进入服务器详细信息页面。服务器详细新包括端口、进程、软件、账号及异常登录告警信息、漏洞告警信息、文件一致性检测信息。并对告警信息进行处理。


a 服务器基本信息：点击服务器详细，页面上方默认显示基本信息

| **参数名称** | **说明** | **备注** |
|---|---|---|

| | | |
|---|---|---|
| 服务器名称 | 云服务器的名称 | |
| ID | 服务器 ID | |
| 所在区域 | 服务器所在的资源区域 | |
| 公网 IP | 服务器绑定的公网 IP 地址 | |
| 内网 IP | 服务器的内网 IP 地址 | |
| 操作平台 | 服务器所安装的操作系统名称 | |
| 防护状态 | 云服务器防护状态，包括“防护中”、“暂停防护中”、“未开启” | 防护中:表示已开启防护，且 agent 在线。<br>暂停防护：已开启防护，agent 离线。<br>未开启：为开启服务器安全防护。 |

b 资产清点：点击资产清点按钮，显示资产清点信息，包括端口、进程、账号、软件 4 类信息。


c 异常登录：点击异常登录按钮，显示异常登录信息。异常登录包括异地登录、爆破登录、登录日志 3 类信息。

d 文件一致性检测：点击文件一致性检测按钮，显示文件一致性检测信息

e 漏洞扫描：点击漏洞扫描按钮，显示漏洞扫描信息。

# 4.6. 资产清点

查看服务器的资产信息，资产信息包括端口、进程、账号、软件 4 类信息。

前提条件：服务器已开启安全防护。

## 4.6.1 端口信息

定期收集服务器的对外端口监听信息，便于快读定位可疑监听行为。可查看单个端口的所有服务器信息，也可查看一台服务器的所有端口信息。

数据收集周期：每 12 小时

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“资产清点”菜单，在二级菜单中选择“端口”进入端口列表信息页面。


| 参数名称 | 说明 | 备注 |
| --- | --- | --- |

| | | |
|---|---|---|
| 端口号 | 端口名称 | |
| 进程名 | 端口对应的进程名称 | |
| 网络协议 | 端口对应的网络协议 | |
| 主机数 | 端口对应的服务器数量 | |

4 在端口列表页面点击主机统计数量，可查看端口对应的服务器信息。


5 点击导出按钮，将端口数据以 Excel 格式导出至指定目录下。

## 4.6.2 进程信息

定期收集服务器的进程信息，便于进程清点和查看。可查看单个端口的所有服务器信息，也可查看一台服务器的所有端口信息。

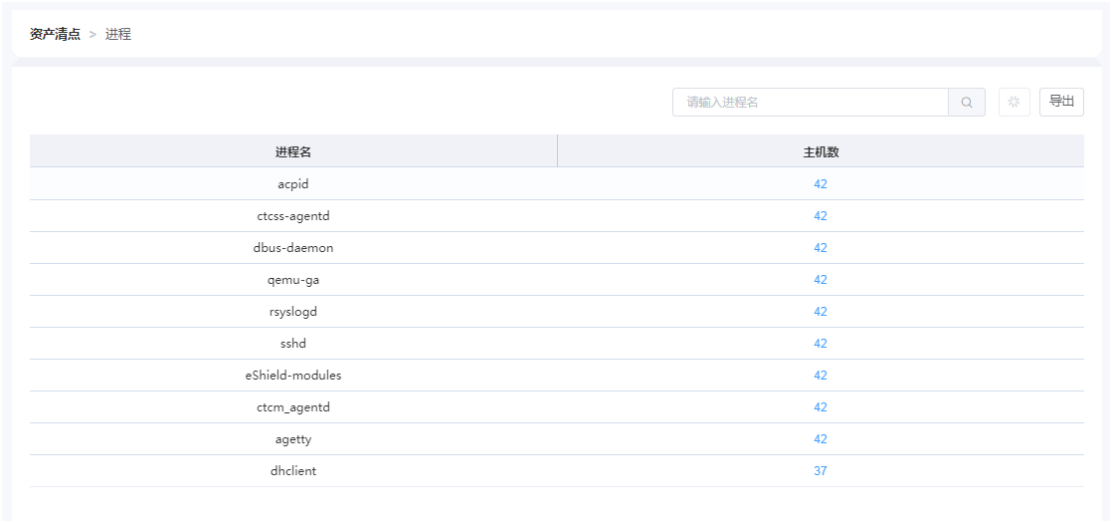
数据收集周期：每 12 小时。

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

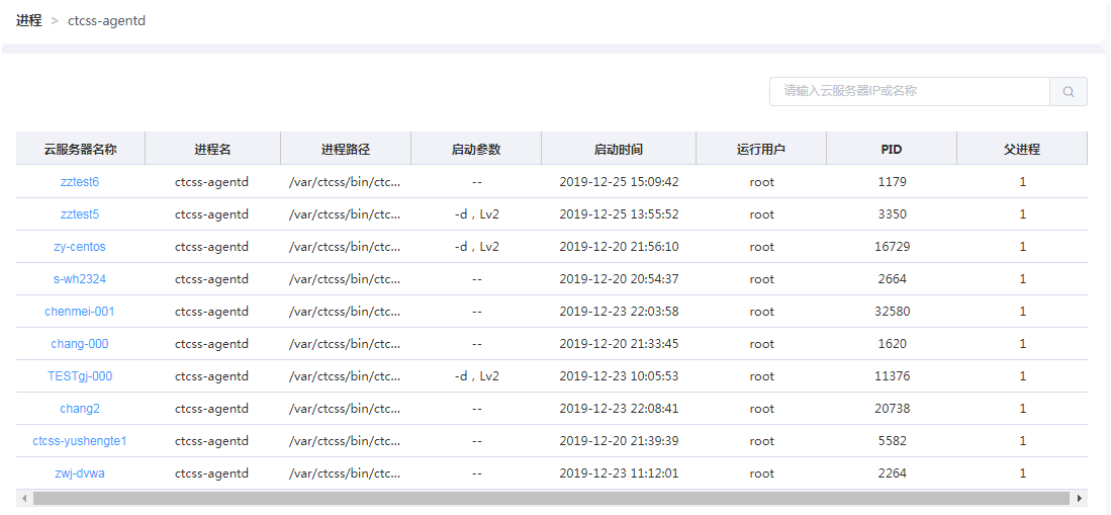
2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“资产清点”菜单，在二级菜单中选择“进程”进入账号列表信息页面。




| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 进程名 | 进程名称 | |
| 主机数 | 进程对应的服务器数量 | |

4 在进程列表页面点击主机统计数量，可查看进程对应的服务器信息。




5 点击导出按钮，将进程数据以 Excel 格式导出至指定目录下。

## 4.6.3 软件信息

定期收集服务器的软件信息，并对变动情况进行记录，便于软件清点和查看。可查看单个软件的所有服务器信息，也可查看一台服务器的所有软件信息。

数据收集周期：每 12 小时。

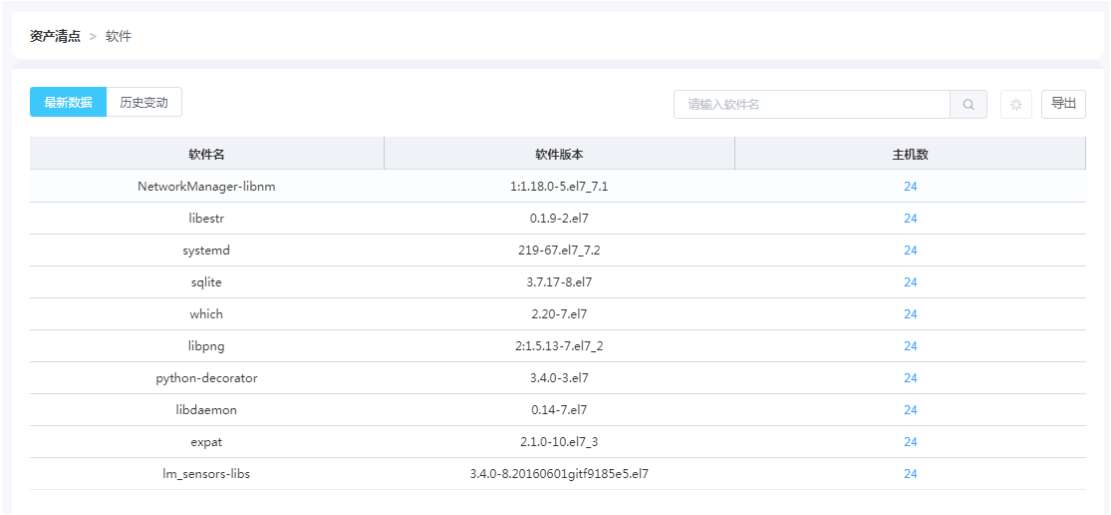
操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

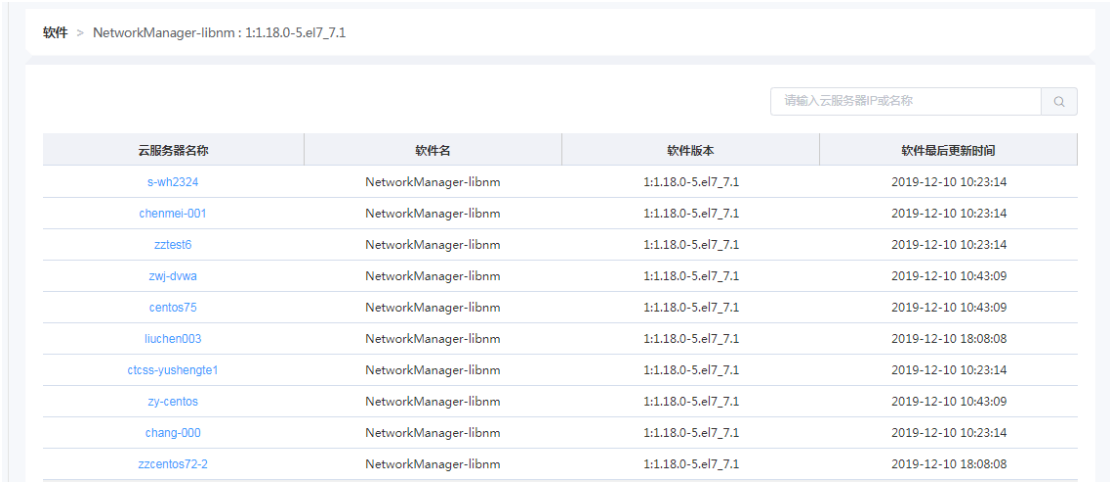
3 在左侧菜单中点击“资产清点”菜单，在二级菜单中选择“软件”进入账号列表信息页面。

4 在软件列表页面点击最新数据，可查看软件最新信息。




| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 软件名称 | 服务器装载的软件名称 | |
| 软件版本 | 软件对应的软件版本 | |
| 主机数 | 软件对应的主机数 | |

5. 点击主机数，可查看软件对应的服务器详细信息。




6 点击导出按钮，将软件数据以 Excel 格式导出至指定目录下。

7 在软件列表页面点击“历史变动”按钮，查看软件历史信息。


| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 云服务器 | 云服务器名称 | |
| 软件名称 | 软件名称 | |
| 软件版本 | 软件对应的软件版本 | |
| 变动状态 | 新增、修改 | |

| | | |
|---|---|---|
| 上报时间 | 变动上报时间 | |

## 4.6.4 账号信息

定期收集服务器的账号信息，并对变动情况进行记录，便于账号清点和查看。可查看单个账号的所有服务器信息，也可查看一台服务器的所有账号信息。

数据收集周期：每 12 小时。

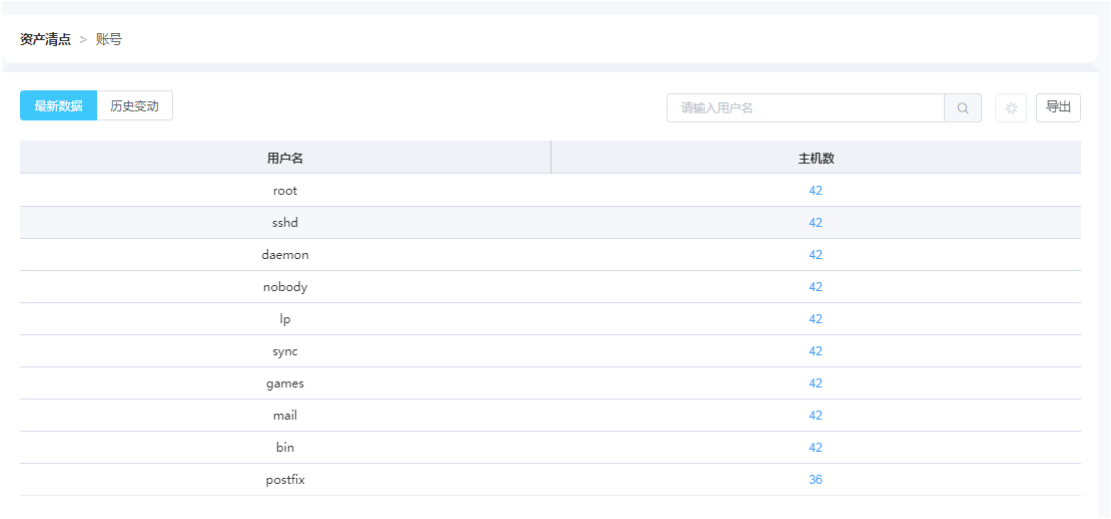
操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

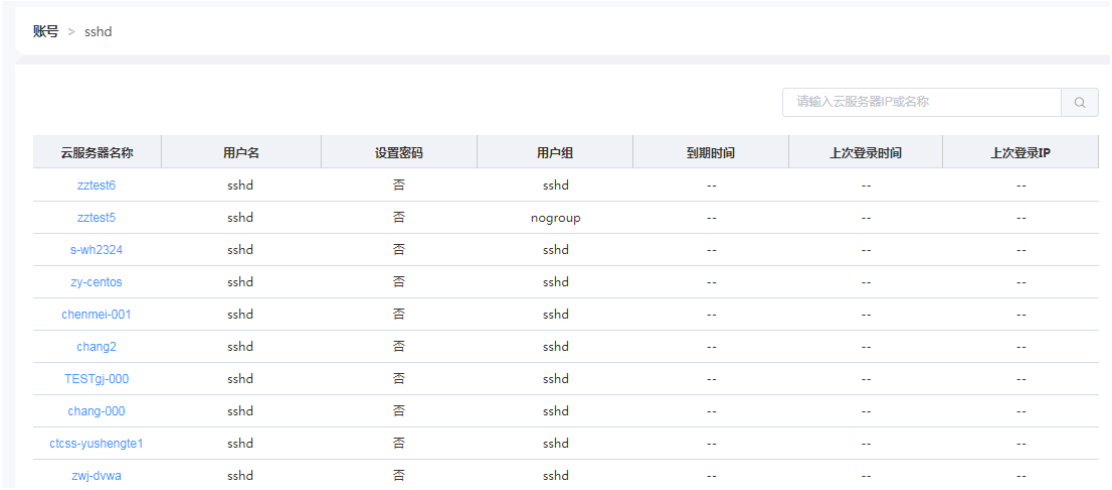
3 在左侧菜单中点击“资产清点”菜单，在二级菜单中选择“账号”进入账号列表信息页面。

4 在账号列表页面点击最新数据，可查看账号最新信息。



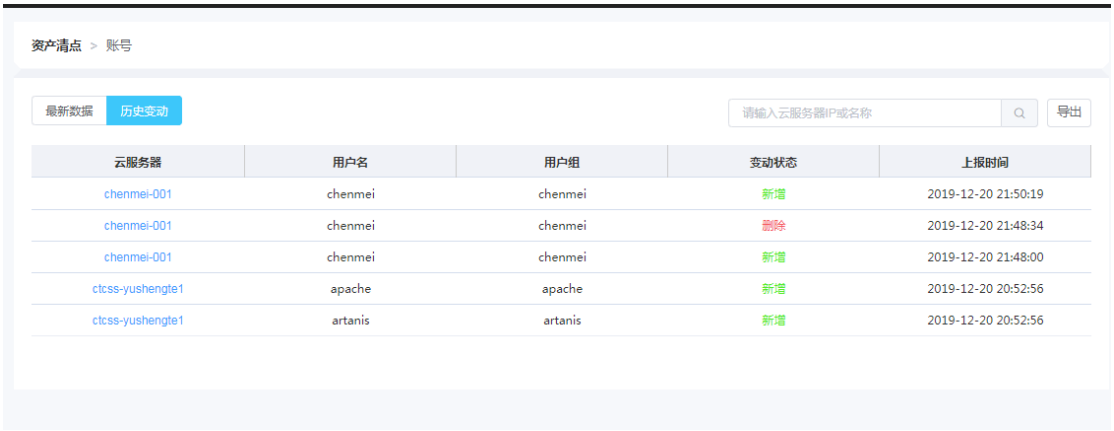

| 参数名称 | 说明 | 备注 |
|---|---|---|
| 用户名 | 用户名信息。 | |
| 主机数 | 软件对应的主机数。 | |

5. 点击主机数，查看用户名对应的服务器信息。




6 点击导出按钮，将账号数据以 Excel 格式导出至指定目录下。

7 在账号列表页面点击“历史变动”按钮，查看账号历史信息。




| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 云服务器 | 云服务器名称 | |
| 用户名 | 用户名信息 | |
| 用户组 | 用户名所处的用户组 | |
| 变动状态 | 新增、修改 | |

| | | |
|---|---|---|
| 上报时间 | 变动上报时间 | |

## 4.7. 漏洞管理

服务器安全卫士订阅 CVE 官方漏洞源，通过收集和识别服务器上的软件版本信息，进行软件漏洞检测。可查看漏洞详细信息，提供漏洞修复建议。如检测出无需修复的漏洞，可将漏洞加入白名单，系统再次检测出该漏洞时会自动忽略，也可将白名单中的漏洞进行移除，恢复检测提示。

检测周期：每天进行一次检测。

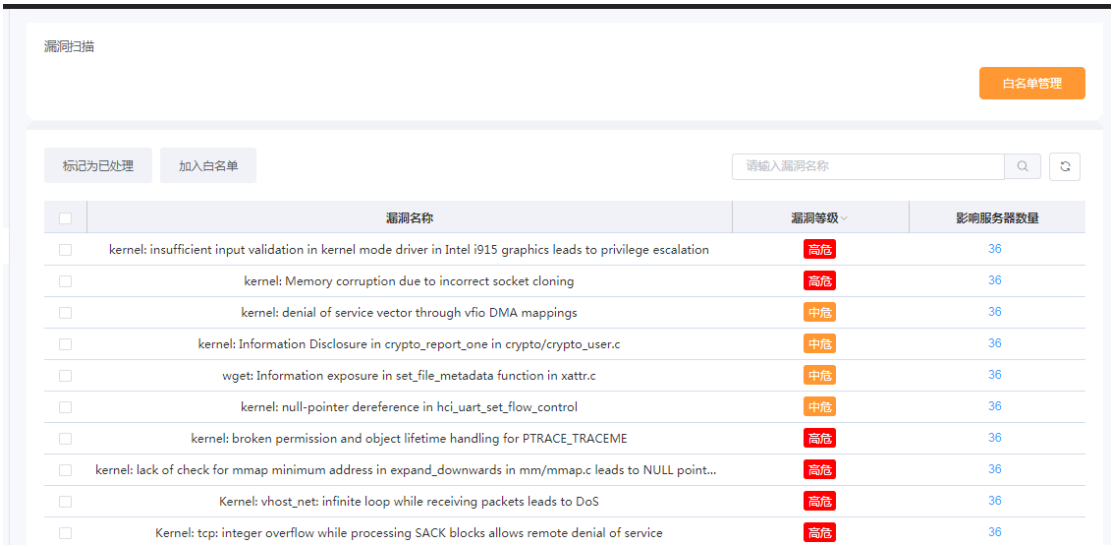
**漏洞信息查看：**

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

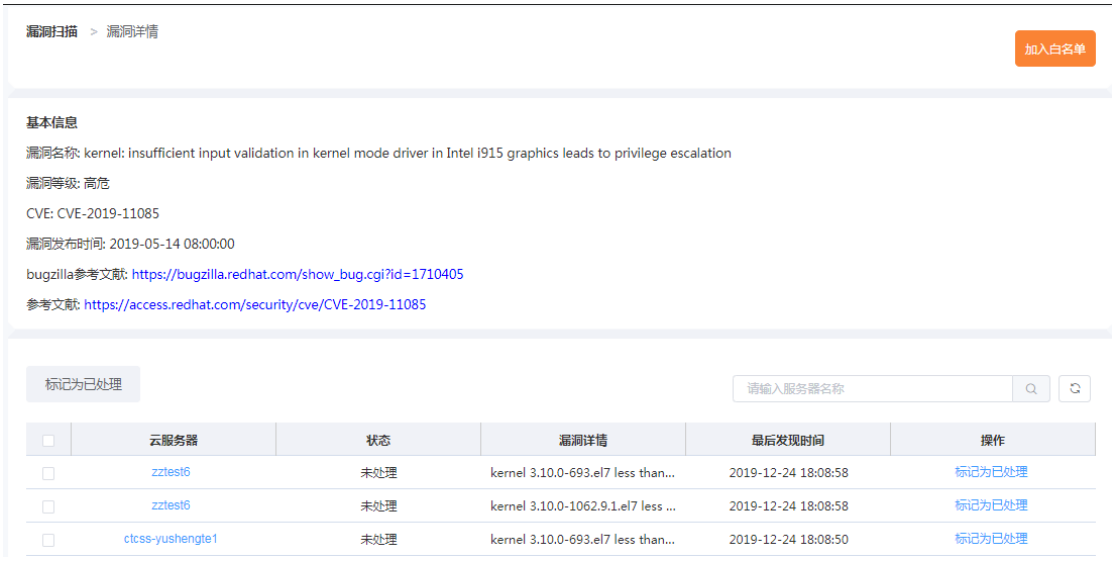
2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“漏洞管理”菜单，进入漏洞管理列表页面。可勾选漏洞，点击“标记为已处理”，将漏洞标记为已处理状态；勾选漏洞名称，点击“加入白名单”按钮，将漏洞加入白名单，后续不再列表中显示此漏洞。




| 参数名称 | 说明 | 备注 |
| --- | --- | --- |
| 漏洞名称 | 漏洞的名称 | |
| 漏洞等级 | 高级、中级、低级 | |
| 未处理资产 | 有该漏洞且未进行处理的服务器数量 | |
| 最后发现时间 | 最近一次检测时间 | |

4 点击漏洞列表中的未处理资产数字，进入漏洞详细信息页面。




**白名单管理：**

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

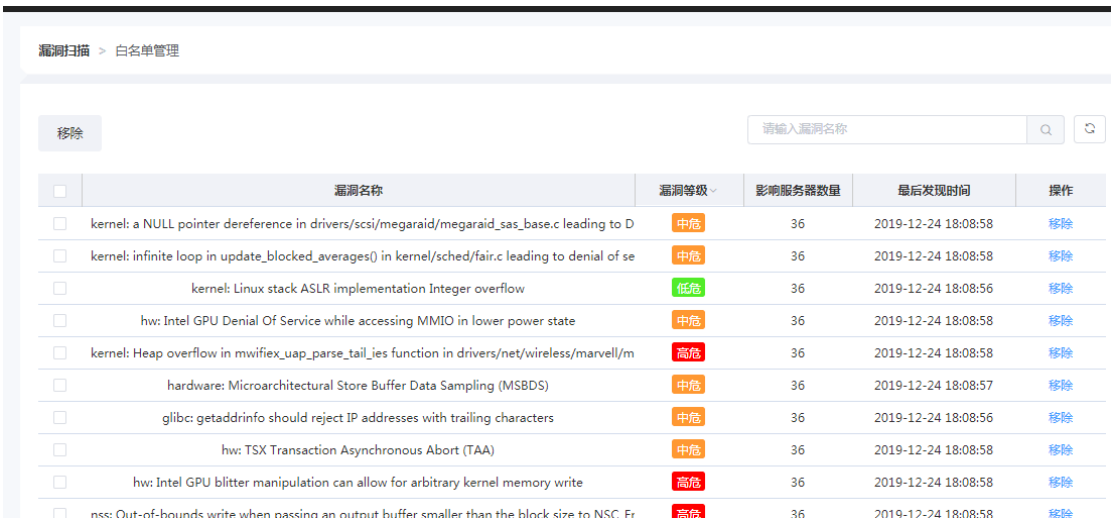
2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“漏洞管理”菜单，进入漏洞管理列表页面。

4 在漏洞列表信息中勾选漏洞，点击加入白名单，在弹出提示框中点击确认按钮，完成操作。

5 在漏洞列表页面右上方，点击白名单管理，查看白名单列表信息。

6 在白名单列表信息页面，点击移除按钮，将漏洞移除白名单。




## 4.8. 异常登录

异常登录检测服务器登录行为，对于异常的登录行为进行告警。告警类型分为两大类：异常登录告警和爆破登录告警，异常登录告警包括在非常用登录地登录、非常用登录时间登录、非常用登录 IP 登录、非常用登录账号登录的信息，爆破告警指通过暴力破解方式进登录的告警。

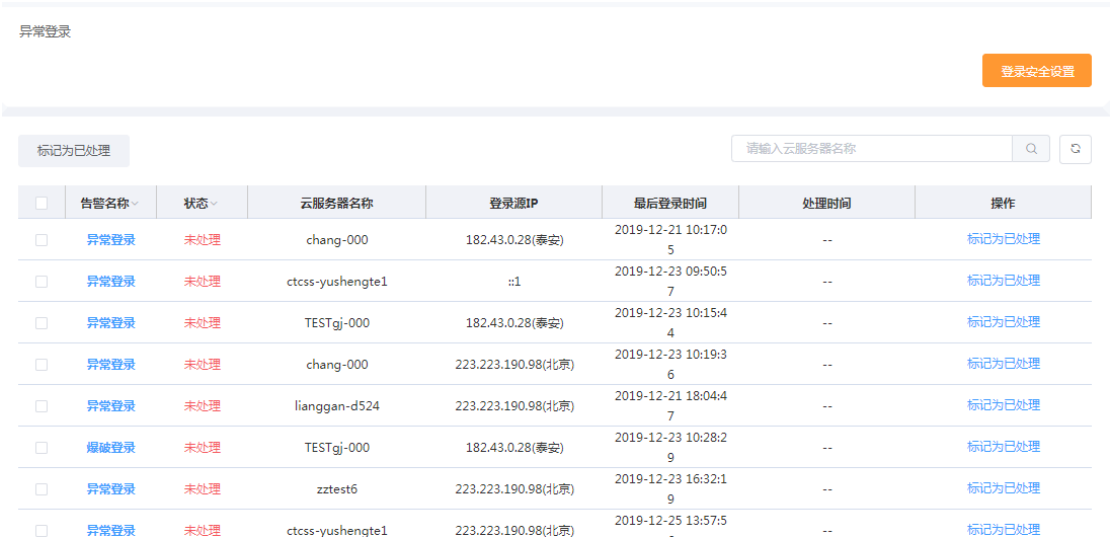
告警策略：只会对第一得登录行为进行告警。异地登录只对公网 IP 进行告警。

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“入侵检测”菜单，在二级菜单中选择“异常登录”进入异常登录列表信息页面。勾选告警名称，点击“标记为已处理”按钮，将告警标记为已处理状态。




4 点击告警名称，进入告警详细信息页面，查看告警详细信息。点击“导出”按钮，将告警信息以 Excel 格式导出至指定目录。


5 点击“登录安全设置”按钮，对安全登录进行条件设置，包括常用地、常用 IP、常用时间、常用账号设置，设置完成后，在非设置条件范围内的登录一律认为是异常登录。

# 4.9. 入侵防御记录

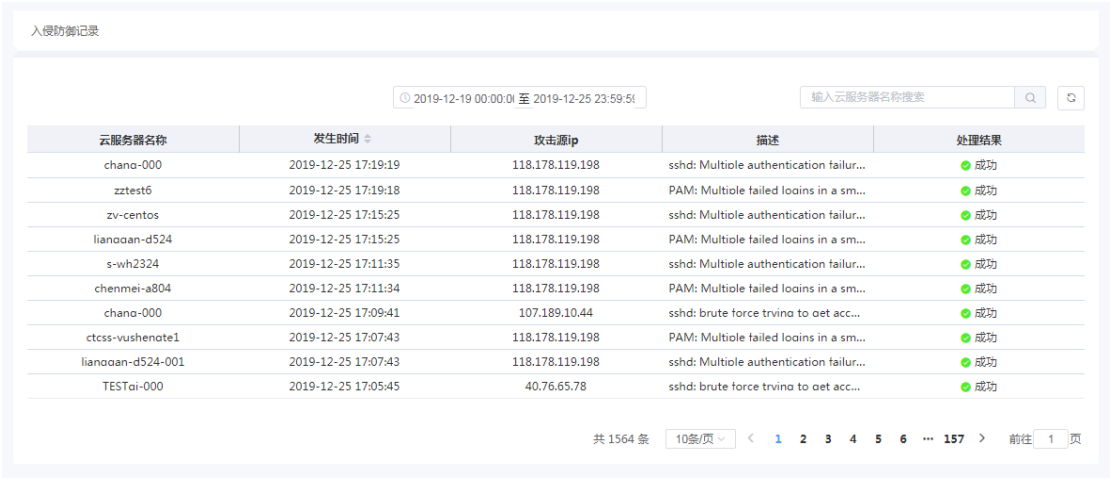
对于入侵的行为，系统记录并展示拦截入侵的行为数据。

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“文件一致性检测”菜单，进入检测列表页面，勾选服务器，点击“标记为已处理”将检测结果标记为已处理状态。




# 4.10. 文件一致性检测

对服务器中文件一致性进行检测，对于出现修改的文件进行提示，可查看新增、修改、删除的文件内容。用户可设置检测目录。支持按全部事件和分类事件两种查看方式。

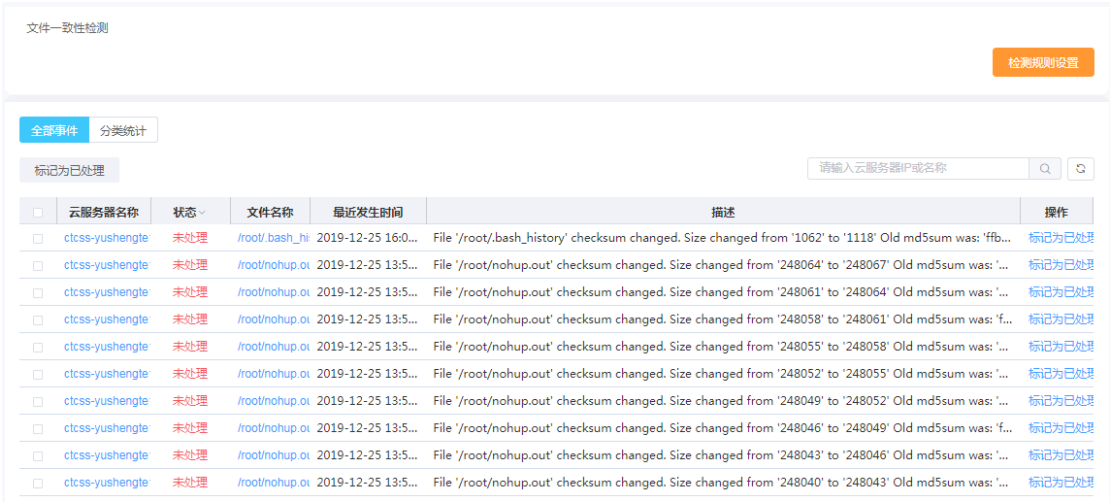
检测周期：每天检测。同一个文件 12 小时内最多纪录 3 次变动数据。

操作步骤：

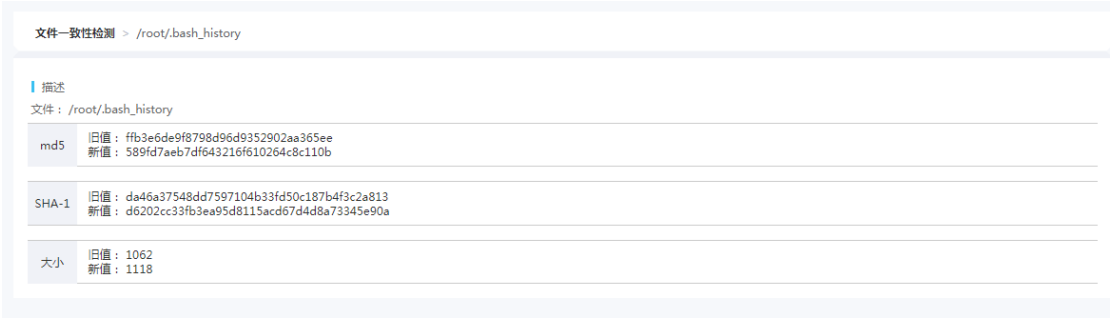
1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“文件一致性检测”菜单，进入检测列表页面，勾选服务器，点击“标记为已处理”将检测结果标记为已处理状态。




4 点击详情按钮，查看检测详情信息。




5 点击“检测规则”设置按钮，对检测目录及规则进行设置，可添加、修改、删除检测规则，并对规则设置对应的生效服务器。



## 4.11. 网页防篡改

网页防篡改可发现并阻止篡改指定目录下文件的行为，快速回复被篡改的文件，保护主机安全。用户可指定防护目录。

检测周期：实时监控。

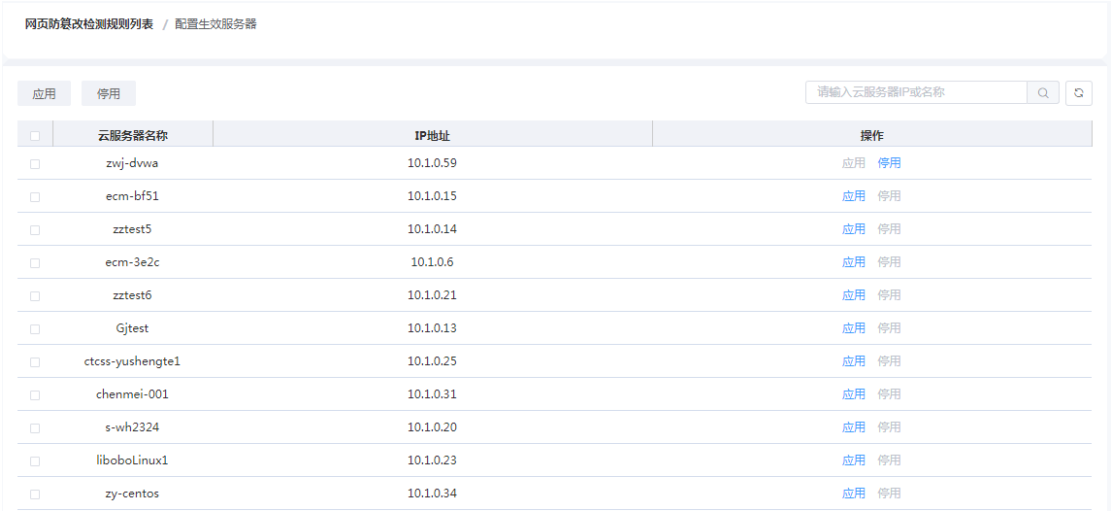
操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“网页防篡改”菜单，进入列表页面。

4 在页面中点击“检测目录设置”设置防护目录。


## 4.12. 基线检查

对系统基线进行全面检查，支持定时、手动检查方式，可配置基线策略，查看基线检查详细信息，对基线进行白名单设置。

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

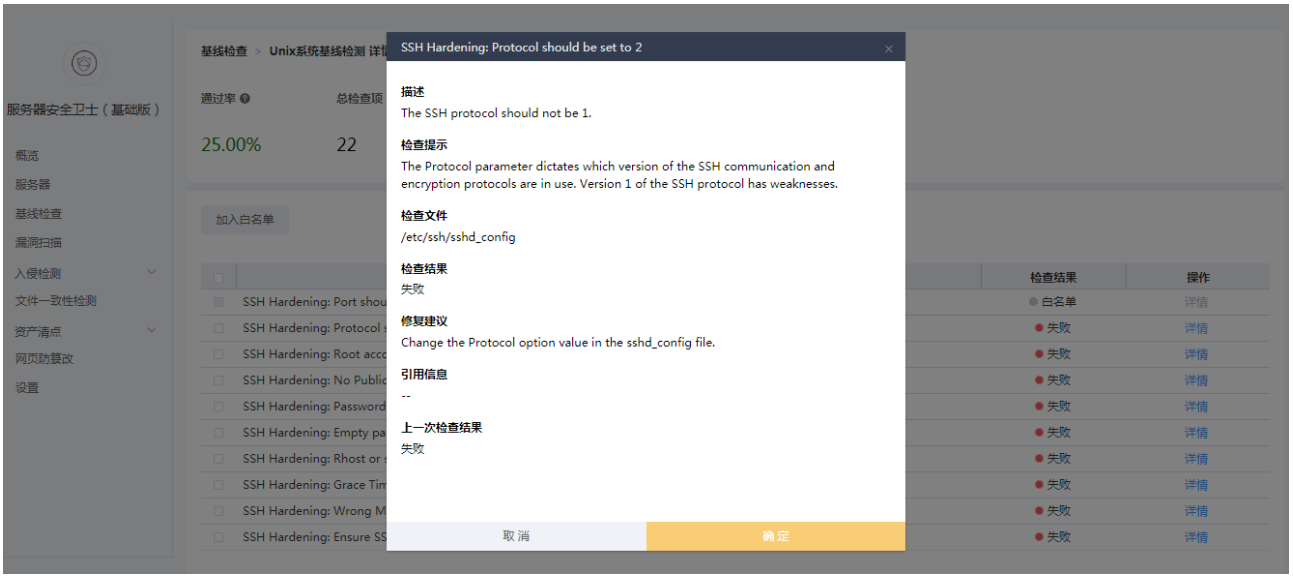
3 在左侧菜单中点击“基线检查”菜单，进入列表页面，。


**4 创建基线策略，点击新建策略按钮，可新建基线策略，输入策略名称，选择检查频率、选择检查时间、基线名称、服务器信息。可在基线检查功能首页右上角的策略管理中，管理已创建的策略，支持新建、修改、删除策略信息。**

**5 查看基线检查信息，在列表中点击基线名称，可查看当前策略下的基线详细信息**

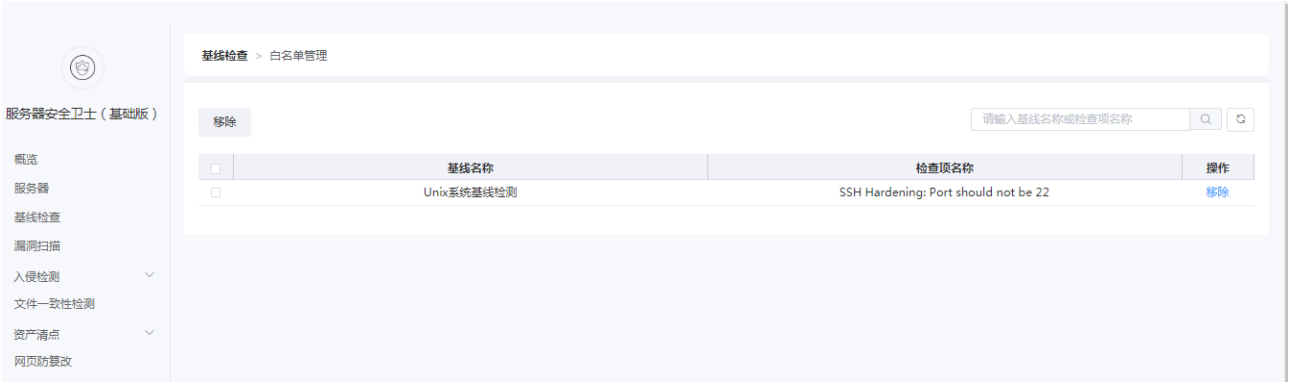

**6 在基线详情页面点击服务器列表中的详情按钮，可查看选中服务器的详细检查信息**


**7 在服务器详情信息页面，基线检查项列表中，点击详情按钮，可查看基线每一项的检查结果及详细信息。**




**7 在基线检查项列中，可将基线检查项加入白名单，选中项目，点击加入白名单按钮，将该检查项加入白名单中。**


**8 在基线检查功能首页，点击白名单管理，可管理白名单中的基线检查项信息，可将检查项信息移除白名单。**




# 4.13. 设置

通过设置通知信息，通知设置功能中，可调整服务器安全卫士向用户发送告警通知和漏洞报告的方式。告警通知默认以邮件方式实时发送至用户邮箱，漏洞扫描报告默认以邮件的方式按周发送至邮箱。设置功能中，可开启/关闭默认防护功能，可开启/关闭 Agent 自动升级功能。

操作步骤：

1 登录管理控制台，点击页面右上方“控制中心”，进入控制中心页面。

2 在页面右上方选择“地域”后，点击安全>服务器安全卫士菜单。

3 在左侧菜单中点击“设置”菜单，进入列表页面，可勾选通知方式，目前支持邮件方式发送。


4 点击设置功能，对默认防护、Agent 自动升级进行开启/关闭操作。

默认防护：默认处于开启状态。关闭默认防护后，新创建的主机处于关闭防护状态，需要手动开启。

Agent 自动升级：默认处于开启状态。关闭 Agent 自动升级后，如 Agent 版本更新后，需要手动进行升级操作。


设置
通知设置
设置
设置项目
规则
操作
默认防护
新创建的服务器自动开启防护状态。
Agent升级
当服务器中的Agent版本需要升级时，自动完成升级。

# 5 常见问题

## 5.1. agent 代理程序是否安全？

agent 和 server 之间有唯一认证，通过特定的加密算法的密钥来进行通信，使用安全的金钥来把守防止数据被破解，同时加密之后不会露出蛛丝马迹。

## 5.2. 安装 agent 程序是否会使云主机变慢？

安装 agent 程序对云主机的影响极小，一般情况下只会占用不到 1%的 CPU 和 10M 的内存，几乎不会影响云主机的正常运行。

## 5.3. 安装 agent 程序是否会占用云主机本地存储空间？

agent 本身很轻量级,只会占用 3M 左右的空间,如果用户在配置完整性检测时添加了 report_changes（文件改变内容）的检测配置的会，会在本地对监控的文件做一个备份存储。(后期重新生成完整性基线功能可以清除掉本地备份文件）

## 5.4. agent 安装支持哪些操作系统？

CENTOS, UBUNTU, RHEL, 。

## 5.5. 发现云主被非法入侵后应该如何操作？

及时更改云主机密码，对爆破登录的事件进行追溯取证。

## 5.6. 告警邮件是否有条数限制？

漏洞扫描告警按周发送，异常登录告警实时发送，单台云主机一天最多发送一条，一个账号一天最多发送 5 条。

## 5.7. “防护中”“暂停防护”“未开启”这些状态的区别是什么？

防护中指为服务器分配了防护配额，且服务器 agent 在线；“暂停防护”指为服务器分配了配额，但

是服务器 agent 未在线，无法进行安全防护；未开启指没有为服务器分配配额的状态。

## 5.8. 如何减少云主机被爆破登录的风险？

在给云服务器设置密码的时候避免弱密码，在公网上布置的机器要特别注意，如果暴力破解的事件很多，需要引起用户重视，关注攻击的源和 ip 地址。