

企业主机安全

# 用户指南

文档版本 01  
发布日期 2022-07-28



版权所有 © 华为技术有限公司 2022。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 目录

<b>1 产品介绍</b>	<b>1</b>
1.1 什么是企业主机安全服务	1
1.2 功能特性	2
1.3 产品优势	8
1.4 服务版本差异	8
1.5 应用场景	14
1.6 使用约束	14
1.7 HSS 权限管理	16
1.8 与其他云服务的关系	17
1.9 相关概念	18
<b>2 开通主机防护</b>	<b>20</b>
2.1 安装 Agent	20
2.1.1 Linux 版本	20
2.1.2 Windows 版本	23
2.2 设置告警通知	25
2.2.1 基础版/企业版/旗舰版	25
2.2.2 网页防篡改改版	30
2.3 开启主机防护	31
2.3.1 基础版/企业版/旗舰版	31
2.3.2 网页防篡改改版	36
<b>3 查看主机防护列表</b>	<b>40</b>
<b>4 主机风险总览</b>	<b>43</b>
<b>5 安全配置</b>	<b>48</b>
<b>6 主机管理</b>	<b>52</b>
6.1 创建服务器组	52
6.2 部署策略	54
<b>7 风险预防</b>	<b>58</b>
7.1 资产管理	58
7.2 漏洞管理	60
7.2.1 查看漏洞详情	60
7.2.2 漏洞修复与验证	64

7.3 基线检查.....	67
7.3.1 查看基线检查详情.....	67
7.3.2 基线检查风险项修复建议.....	69
<b>8 入侵检测.....</b>	<b>71</b>
8.1 告警事件概述.....	71
8.2 查看和处理入侵告警事件.....	76
8.3 管理文件隔离箱.....	84
8.4 配置告警白名单.....	86
8.5 配置登录白名单.....	88
<b>9 高级防御.....</b>	<b>91</b>
9.1 程序运行认证.....	91
9.1.1 查看白名单策略列表.....	91
9.1.2 应用白名单策略.....	94
9.1.3 查看和处理程序运行事件.....	98
9.2 文件完整性管理.....	101
9.2.1 添加管理文件.....	101
9.2.2 查看变更统计.....	103
9.3 勒索病毒防护.....	105
9.3.1 查看防护策略列表.....	106
9.3.2 创建防护策略.....	109
9.3.3 查看和处理防护事件.....	114
<b>10 安全运营.....</b>	<b>117</b>
10.1 查看和创建策略组.....	117
10.2 修改策略内容.....	123
<b>11 网页防篡改.....</b>	<b>136</b>
11.1 添加防护目录/文件系统.....	136
11.2 添加远端备份服务器.....	142
11.3 添加特权进程修改防护文件.....	145
11.4 定时开启网页防篡改.....	147
11.5 开启动态网页防篡改.....	148
11.6 查看网页防篡改报告.....	149
<b>12 权限管理.....</b>	<b>151</b>
12.1 HSS 自定义策略.....	151
12.2 HSS 授权项说明.....	152
<b>13 常见问题.....</b>	<b>156</b>
13.1 产品咨询.....	156
13.1.1 什么是企业主机安全? .....	156
13.1.2 什么是 HSS 的 Agent? .....	158
13.2 开通与配置.....	159
13.2.1 Agent 是否和其他安全软件有冲突? .....	159

13.2.2 如何安装 Agent? .....	159
13.2.3 Agent 的默认安装路径是什么? .....	160
13.2.4 如何筛选未安装 Agent 的主机? .....	160
13.2.5 Agent 状态异常应如何处理? .....	160
13.2.6 如何卸载 Agent? .....	162
13.3 告警事件处理.....	164
13.3.1 账户暴力破解问题.....	164
13.3.1.1 如何拦截账户暴力破解? .....	164
13.3.1.2 如何预防账户暴力破解攻击? .....	166
13.3.1.3 如何解决部分 Linux 系统的账户破解防护功能未生效的问题? .....	167
13.3.2 弱口令和风险账号问题.....	167
13.3.2.1 出现弱口令告警, 怎么办? .....	167
13.3.2.2 如何设置安全的口令? .....	169
13.3.3 配置风险问题.....	170
13.3.3.1 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略? .....	170
13.3.3.2 如何在 Windows 主机上设置口令复杂度策略? .....	172
13.4 漏洞管理.....	175
13.4.1 如何处理漏洞? .....	175
13.4.2 按照提示修补了漏洞为什么警告还在? .....	175
13.4.3 为什么漏洞修复未生效? .....	175
13.4.4 漏洞管理显示的主机不存在? .....	176
13.4.5 漏洞修复完毕后是否需要重启主机? .....	176
13.5 网页防篡改.....	176
13.5.1 为什么要添加防护目录? .....	176
13.5.2 如何修改防护目录? .....	176
13.5.3 开启网页防篡改后, 如何修改文件? .....	177
13.5.4 开启动态网页防篡改后, 状态是“已开启未生效”, 怎么办? .....	178
13.6 其他.....	178
13.6.1 如何使用 Windows 远程桌面连接工具连接主机? .....	178
13.6.2 如何查看 HSS 的日志文件? .....	180
13.6.3 如何开启登录失败日志开关? .....	181
13.6.4 如何立即执行检测? .....	183
<b>A 修订记录.....</b>	<b>188</b>

# 1 产品介绍

## 1.1 什么是企业主机安全服务

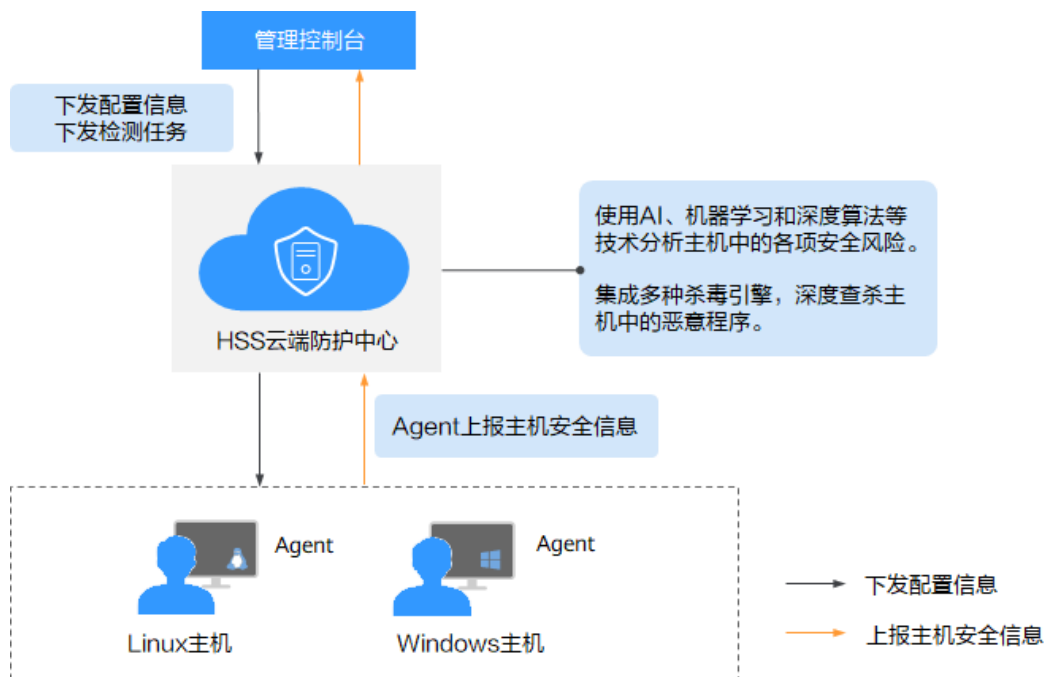
企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

### 工作原理

在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

企业主机安全服务的工作原理如图1-1所示。

图 1-1 工作原理



企业主机安全服务的组件功能及工作流程说明如下：

表 1-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	<ul style="list-style-type: none"><li>使用AI、机器学习和深度算法等技术分析主机中的各项安全风险。</li><li>集成多种杀毒引擎，深度查杀主机中的恶意程序。</li><li>接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。</li><li>接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面。</li></ul>
Agent	<ul style="list-style-type: none"><li>Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：443。</li><li>每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。</li><li>根据您配置的安全策略，阻止攻击者对主机的攻击行为。</li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。</li><li>根据操作系统版本选择对应的安装命令/安装包进行安装。</li><li>网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。</li></ul>

## 1.2 功能特性

企业主机安全服务主要包含资产管理、漏洞管理、入侵检测、基线检查和网页防篡改功能。

### 资产管理

资产管理功能可深度扫描出主机中的账号、端口、进程、Web目录、软件信息和自启动任务，在“资产管理”界面，您可以统一管理主机中的信息资产。

表 1-2 资产管理

功能项	功能描述	检测周期
账号信息管理	<p>检测主机系统中的账号，列出当前系统的账号信息，帮助用户进行账户安全性管理。</p> <p>根据账号的实时信息和历史变动，您可以快速排查主机中的可疑账号。</p> <ul style="list-style-type: none"> <li>账号的实时信息包括账号的“账号名”、“对应主机数”以及具体账号对应的“对应服务器”、“权限”、“用户组”、“用户目录”和“用户启动Shell”。</li> <li>账号的历史变动信息包括“变动状态”、“弹性服务器名称”、“账号名”、“权限”、“用户组”、“用户目录”、“用户启动Shell”和“发生变动时间”。</li> </ul>	实时检测
开放端口检测	<p>检测主机系统中的端口，列出当前系统开放的端口列表，帮助用户识别出其中的危险端口和未知端口。</p> <p>根据端口的“端口类型”、“对应主机数”、“危险程度”、“状态”、“端口描述”以及具体端口对应的“对应服务器”、“绑定IP”、“状态”、“对应进程的PID”、“程序文件”，您能够快速排查主机中含有风险的端口。</p>	实时检测
进程信息检测	<p>检测主机系统中运行的进程，对运行中的进程进行收集及呈现，便于自主清点合法进程发现异常进程。</p> <p>根据主机中“进程名”、“对应主机数”、“进程总数”、“文件名称总数”以及具体进程对应的“对应服务器”、“进程路径”、“文件权限”、“运行用户”、“PID”以及“进程启动时间”，您能够快速排查主机中的异常进程。</p>	实时检测
Web目录管理	<p>检测并列当前系统中Web服务使用的目录，帮助用户进行Web资源管理。</p> <p>在“Web目录管理”界面，您可以统一查看Web目录对应的“文件路径”、“应用类型”、“本地端口”、“URL”、“进程编号（PID）”和“程序文件”。</p>	实时检测



功能项	功能描述	检测周期
软件信息管理	<p>检测并列出现当前系统安装的软件信息，帮助用户清点软件资产，识别不安全的软件版本。</p> <p>根据软件的实时信息和历史变动，您能够快速排查主机中含有风险的软件。</p> <ul style="list-style-type: none"> <li>软件的实时信息包括“软件名称”、“对应主机数”以及具体软件对应的安装该软件的“对应服务器”和“软件版本号”。</li> <li>软件变动的历史记录包括软件的“变动状态”、“服务器名称”、“软件名称”、“软件版本号”和“发生变动时间”。</li> <li>您可以使用手动检测功能检测主机中的软件信息。</li> </ul>	<ul style="list-style-type: none"> <li>每日凌晨自动检测</li> <li>手动检测</li> </ul>
自启动	<p>检测并列出现当前所有主机系统中自启动服务、定时任务、预加载动态库、Run注册表键或者开机启动文件夹的汇总信息。</p> <p>帮助用户通过自启动变更情况，及时发现异常自启动项，快速定位木马程序的问题。</p>	实时检测

## 漏洞管理

漏洞管理功能将检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，帮助用户识别潜在风险。

表 1-3 漏洞管理

功能项	功能描述	检测周期
软件漏洞检测	<p>包括Linux软件漏洞和Windows系统漏洞。</p> <p>通过与漏洞库进行比对，检测出系统和官方软件（非绿色版、非自行编译安装版；例如：SSH、OpenSSL、Apache、Mysql等）存在的漏洞，帮助用户识别出存在的风险。</p>	<ul style="list-style-type: none"> <li>每日凌晨自动检测</li> <li>手动检测</li> </ul>
Web-CMS漏洞检测	<p>通过对Web目录和文件进行检测，识别出Web-CMS漏洞，提升Web服务安全性。</p>	

## 基线检查

基线检查功能可扫描出主机系统和关键软件含有风险的配置信息。

表 1-4 基线检查

功能项	功能描述	检测周期
口令复杂度策略检测	<ul style="list-style-type: none"> <li>检测系统中的口令复杂度策略，并给出修改建议，帮助用户提升口令安全性。</li> <li>您可以使用手动检测功能检测主机中的口令复杂度策略。</li> </ul>	<ul style="list-style-type: none"> <li>每日凌晨自动检测</li> <li>手动检测</li> </ul>
经典弱口令检测	<ul style="list-style-type: none"> <li>检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改，防止账户口令被轻易猜解。</li> <li>在经典弱口令检测界面，您可查看使用弱口令的“账号名”、“账号类型”以及“弱口令使用时长”。</li> <li>您可以使用手动检测功能检测主机中使用的弱口令。</li> </ul>	<ul style="list-style-type: none"> <li>每日凌晨自动检测</li> <li>手动检测</li> </ul>
配置检测	<p>检测常见的Tomcat配置、Nginx配置、SSH登录配置，帮助用户识别不安全的配置项。</p> <p>在配置检测界面，您可以查看主机中不同配置检测种类的“描述”、存在威胁的“检测规则”、“威胁等级”和“状态”。</p> <ul style="list-style-type: none"> <li>根据配置检测规则和检测结果详情，您可以处理含有风险的配置项或忽略可信的配置项。</li> <li>您可以使用手动检测功能检测主机中的关键配置信息。</li> </ul>	<ul style="list-style-type: none"> <li>每日凌晨自动检测</li> <li>手动检测</li> </ul>

## 入侵检测

入侵检测功能可识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。

表 1-5 入侵检测

功能项	功能描述	检测周期
账户暴力破解	<p>检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击。</p> <ul style="list-style-type: none"> <li>如果30秒内，账户暴力破解次数达到5次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因账户破解被入侵。SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。</li> <li>根据账户暴力破解告警详情，如“攻击源IP”、“攻击类型”和“拦截次数”，您能够快速识别出该源IP是否为可信IP，如果为可信IP，您可以通过手动解除拦截的方式，解除拦截的可信IP。</li> </ul>	实时检测

功能项	功能描述	检测周期
账户异常登录	<p>检测“异地登录”和“账户暴力破解成功”等异常登录。</p> <ul style="list-style-type: none"> <li>检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。异地登录检测信息包括“登录源IP”、“登录时间”，攻击者尝试登录主机时使用的“用户名”和“云服务器名称”。</li> <li>若在非常用登录地登录，则触发安全事件告警。</li> <li>若账户暴力破解成功，登录到云主机，则触发安全事件告警。</li> </ul>	实时检测
恶意程序（云查杀）	<p>通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。</p> <p>根据恶意程序的相关信息，您可以“隔离查杀”已识别的恶意程序和可疑的恶意程序，“取消隔离”或“忽略”可信的程序。</p>	实时检测
进程异常行为	<p>通过对运行进程的管控，全局检测各个主机的运行信息，保障云主机的安全性。您可以建立自己的进程白名单，对于进程的非法行为、黑客入侵过程进行告警。</p> <p>进程异常行为可以监控以下异常行为：</p> <ul style="list-style-type: none"> <li>监控进程CPU使用异常。</li> <li>检测进程对恶意IP的访问。</li> <li>检测进程并发连接数异常等。</li> </ul>	实时检测
关键文件变更	<ul style="list-style-type: none"> <li>对系统关键文件（例如：ls、ps、login、top等）进行监控，一旦文件被修改就进行告警，提醒用户关键文件存在被篡改的可能。</li> <li>关键文件变更信息包括“被更改的关键文件路径”、“文件最后修改时间”以及配置文件所在的“服务器名称”。</li> </ul>	实时检测
网站后门（Webshell）	<p>检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。</p> <ul style="list-style-type: none"> <li>网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略可信文件。</li> <li>您可以使用手动检测功能检测主机中的网站后门。</li> </ul>	<ul style="list-style-type: none"> <li>实时检测</li> <li>手动检测</li> </ul>

功能项	功能描述	检测周期
反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。	实时检测
异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。	实时检测
高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	实时检测
自启动检测	检测并列举当前系统中的自启动服务、定时任务、预加载动态库、Run注册表键和开机启动文件夹，帮助用户及时发现非法自启动。	实时检测
风险账户	检测主机系统中的账号，列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。 在风险账号告警详情界面，您可以查看“账号名”、“用户组”、“UID/SID”、“用户目录”以及“用户启用Shell”等信息。	实时检测
提权操作	检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： <ul style="list-style-type: none"> <li>● 利用SUID程序漏洞进行root提权。</li> <li>● 利用内核漏洞进行root提权。</li> <li>● 对文件的提权。</li> </ul>	实时检测

## 高级防御

功能项	功能描述	检测周期
程序运行认证	支持将重点防御的主机加入到白名单策略中，通过检测白名单中指定的应用程序区分“可信”、“不可信”和“未知”，防止未经白名单授权的程序运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。	实时检测
文件完整性管理	检查Linux系统、应用程序软件和其他组件的文件，帮助用户及时发现发生了可能遭受攻击的更改。	实时检测
勒索病毒防护	通过对主机运行状态的自动学习和管理端智能分析，完成可信程序的判定，在防护阶段对非可信程序的操作进行告警。	实时检测

## 网页防篡改

网页防篡改功能可实时发现并拦截篡改指定目录下文件的行为，并快速获取备份的合法文件恢复被篡改的文件，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。

表 1-6 网页防篡改

功能项	功能描述	检测周期
静态网页防篡改	防止网站服务器中的静态网页文件被篡改。	实时检测
网盘文件防篡改	防止共享文件网盘中的网页文件被篡改。	
动态网页防篡改	防止网站数据库中动态网页内容被篡改。	

## 1.3 产品优势

企业主机安全服务是一个用于全面保障主机整体安全的服务，能帮助您高效管理主机的安全状态，并构建服务器安全体系，降低当前服务器面临的主要安全风险。

### 集中管理

实现检测和防护的一体化管控，降低管理的难度和复杂度。

您可以在安全控制台上统一查看同一区域内主机中各项风险的来源，根据各项风险的处理建议处理主机中的各项风险；利用多样化检索、批量处理等功能，快速分析同一区域内所有主机的风险。

### 精准防御

拥有先进的检测技术和丰富的检测库，提供精准防御。

### 全面防护

提供事前预防、事中防御、事后检测的全面防护，全面降低入侵风险。

### 轻量 Agent

Agent占用资源极少，不影响主机系统的正常运行。

## 1.4 服务版本差异

企业主机安全服务有基础版、企业版、旗舰版和网页防篡改版供您选择，具体差异请参见表1-7。详细的功能介绍请参见[功能特性](#)。

表 1-7 版本功能说明

服务功能	功能项	功能概述	基础版	企业版	旗舰版	网页防篡改改版
资产管理	账号信息管理	检测当前系统的账号信息，帮助用户进行账户安全性管理。	×	√	√	√
	开放端口检测	检测当前系统开放的端口，帮助用户识别出其中的危险端口和未知端口。	×	√	√	√
	进程信息管理	监测运行中的进程并进行收集及呈现，便于用户自主清点合法进程，发现异常进程。	×	√	√	√
	Web目录管理	统计当前系统中Web服务使用的目录，帮助用户进行Web资源管理。	×	√	√	√
	软件信息管理	监测并记录当前系统安装的软件信息，帮助用户清点软件资产，识别不安全的软件版本。	×	√	√	√
	自启动	对系统中的自启动项进行检测，及时统计自启动项的变更情况。	×	×	√	√
漏洞管理	Windows漏洞管理	通过与漏洞库进行比对，检测并管理Windows系统和软件存在的漏洞，对当前系统中存在的紧急漏洞进行提醒。	×	√	√	√
	Linux漏洞管理	通过与漏洞库进行比对，检测并管理Linux系统和软件存在的漏洞，对当前系统中存在的紧急漏洞进行提醒。	×	√	√	√
	Web-CMS漏洞管理	通过对Web目录和文件进行检测，识别出Web-CMS漏洞，提升Web服务安全性。	×	√	√	√
基线检查	口令复杂度策略检测	检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性。	√	√	√	√
	经典弱口令检测	检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改。	√	√	√	√

服务功能	功能项	功能概述	基础版	企业版	旗舰版	网页防篡改改版
	配置检测	对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项。	×	√	√	√
入侵检测	账户暴力破解	检测账户遭受的口令破解攻击，封锁攻击源，防止云主机因账户破解被入侵。	√	√	√	√
	账户异常登录	<p>检测“异地登录”和“账户暴力破解成功”等异常登录。</p> <ul style="list-style-type: none"> <li>检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。异地登录检测信息包括“登录源IP”、“登录时间”，攻击者尝试登录主机时使用的“用户名”和“云服务器名称”。</li> <li>若在非常用登录地登录，则触发安全事件告警。</li> <li>若账户暴力破解成功，登录到云主机，则触发安全事件告警。</li> </ul>	√	√	√	√
	恶意程序（云查杀）	对运行中的程序进行检测，识别出其中的后门、木马、挖矿软件、蠕虫和病毒等恶意程序。	×	√	√	√

服务功能	功能项	功能概述	基础版	企业版	旗舰版	网页防篡改改版
	进程异常行为	<p>检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。</p> <p>对于进程的非法行为、黑客入侵过程进行告警。</p> <p>进程异常行为可以监控以下异常行为：</p> <ul style="list-style-type: none"> <li>• 监控进程CPU使用异常。</li> <li>• 检测进程对恶意IP的访问。</li> <li>• 检测进程并发连接数异常等。</li> </ul>	×	√	√	√
	关键文件变更	<p>对于系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。</p>	×	√	√	√
	网站后门 (Webs hell)	<p>检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。</p> <ul style="list-style-type: none"> <li>• 网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略可信文件。</li> <li>• 您可以使用手动检测功能检测主机中的网站后门。</li> </ul>	×	√	√	√
	反弹Shell	<p>实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。</p> <p>支持对TCP、UDP、ICMP等协议的检测。</p>	×	×	√	√
	异常Shell	<p>检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。</p>	×	×	√	√



服务功能	功能项	功能概述	基础版	企业版	旗舰版	网页防篡改改版
	高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	×	×	√	√
	自启动检测	检测并列举当前系统中的自启动服务、定时任务、预加载动态库、Run注册表键和开机启动文件夹，帮助用户及时发现非法自启动。	×	×	√	√
	风险账户	检测主机系统中的账号，列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。	×	√	√	√
	提权操作	检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： <ul style="list-style-type: none"> <li>● 利用SUID程序漏洞进行root提权。</li> <li>● 利用内核漏洞进行root提权。</li> <li>● 对文件的提权。</li> </ul>	×	×	√	√
	Rootkit程序	检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。 <ul style="list-style-type: none"> <li>● 支持使用文件特征码检测rootkit。</li> <li>● 支持对隐藏文件、端口、进程的检测。</li> </ul>	×	×	√	√
高级防御	程序运行认证	支持将重点防御的主机加入到白名单策略中，通过检测白名单中指定的应用程序区分“可信”、“不可信”和“未知”，防止未经白名单授权的程序运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。	×	×	√	√

服务功能	功能项	功能概述	基础版	企业版	旗舰版	网页防篡改版
	文件完整性管理	检查Linux系统、应用程序软件和其他组件的文件，帮助用户及时发现发生了可能遭受攻击的更改。	×	×	√	√
	勒索病毒防护	通过对主机运行状态的自动学习和管理端智能分析，完成可信程序的判定，在防护阶段对非可信程序的操作进行告警。	×	×	√	√
安全运营	策略管理	支持自定义检测策略配置与下发，能够为每组或每台主机灵活配置检测规则，便于精细化安全运营。 <ul style="list-style-type: none"> <li>查看策略组列表</li> <li>依据默认策略组和已创建的策略组添加策略组</li> <li>自定义策略</li> <li>修改和删除策略组</li> <li>针对策略组包含的策略，进行修改和关闭策略</li> <li>在“主机管理”页面可以对主机进行批量部署策略</li> </ul>	×	√ (仅支持默认企业版策略组)	√	√
	安全报告	呈现每周或每月的主机安全趋势以及关键安全事件与风险。	×	√	√	√
网页防篡改	静态网页防篡改	防止网站服务器中的静态网页文件被篡改。	×	×	×	√
	网盘文件防篡改	防止共享文件网盘中的网页文件被篡改。	×	×	×	√
	动态网页防篡改	防止网站数据库中动态网页内容被篡改。	×	×	×	√

## 1.5 应用场景

### 统一安全管理

企业主机安全服务提供统一的主机安全管理能力，帮助用户更方便地管理云服务器的安全配置和安全事件，降低安全风险和管理成本。

### 安全风险评估

对主机系统进行安全评估，将系统存在的各种风险（账户、端口、软件漏洞、弱口令等）进行展示，提示用户及时加固，消除安全隐患。

### 账户安全保护

提供覆盖事前、事中和事后的账户安全保护功能。

### 主动安全防御

通过清点主机安全资产，管理主机漏洞与不安全配置，预防安全风险；通过网络、应用、文件主动防护引擎主动防御安全风险。

### 黑客入侵检测

提供主机全攻击路径检测能力，能够实时、准确地感知黑客入侵事件，并提供入侵事件的响应手段，对业务系统“零”影响，有效应对APT攻击等高级威胁。

## 1.6 使用约束

### 支持的云服务器类型

弹性云服务器（Elastic Cloud Server, ECS）

### 支持的操作系统

企业主机安全服务的Agent可运行在CentOS、EulerOS等Linux系统以及Windows 2008、Windows 2012、Windows 2016等Windows系统的主机上。

---

#### 须知

已停止服务的Linux系统版本或者Windows系统版本，与Agent可能存在兼容性问题，建议重装或者升级为Agent支持的操作系统版本，以便获得企业主机安全更好的服务体验。

- 企业主机安全服务支持的主机Linux系统版本如[表1-8](#)和[表1-9](#)所示。

表 1-8 Linux 系统版本（X86 计算）

序号	支持的OS类型
1	CentOS: 6, 7 and 8 (64 bit)
2	Debian: 7, 8, 9 and 10 (32/64 bit)
3	EulerOS: 2.2, 2.3 and 2.5 (64 bit)
4	Fedora: 24, 25 and 30 (64 bit)
5	OpenSUSE: 13.2, 15.0 and 42.2 (64bit)
6	Ubuntu: 14.04, 16.0 and 18.04 (32/64 bit)
7	SUSE: 11 and 12 (64 bit) and SAP HANA
8	Gentoo: 13.0 and 17.0 (64 bit)
9	Oracle Linux: 6.9, 7.4 (64bit)

表 1-9 Linux 系统版本（鲲鹏计算）

序号	支持的OS类型
1	CentOS: 7.4, 7.5, 7.6, 8.0 64bit with ARM(40GB)
2	EulerOS: 2.8 64bit with ARM(40GB)
3	Fedora: 29 64bit with ARM(40GB)
4	OpenSUSE: 15.0 64bit with ARM(40GB)
5	Ubuntu: 18.04 64bit with ARM(40GB)

- 企业主机安全服务支持的主机Windows系统版本如表1-10所示。

表 1-10 Windows 系统版本

序号	支持的OS类型	使用限制说明
1	Windows Server 2019 数据中心版 64位英文 (40GB)	若服务器安装了三方安全防护软件，请先停止第三方安全防护软件的防护功能，待Agent安装完成后再开启。
2	Windows Server 2019 数据中心版 64位简体中文 (40GB)	
3	Windows Server 2016 标准版 64位英文 (40GB)	
4	Windows Server 2016 标准版 64位简体中文 (40GB)	
5	Windows Server 2016 数据中心版 64位英文 (40GB)	

序号	支持的OS类型	使用限制说明
6	Windows Server 2016 数据中心版 64位简体中文(40GB)	
7	Windows Server 2012 R2 标准版 64位英文(40GB)	
8	Windows Server 2012 R2 标准版 64位简体中文(40GB)	
9	Windows Server 2012 R2 数据中心版 64位英文(40GB)	
10	Windows Server 2012 R2 数据中心版 64位简体中文(40GB)	
11	Windows Server 2008 R2 标准版 64位英文(40GB)	
12	Windows Server 2008 R2 标准版 64位简体中文(40GB)	
13	Windows Server 2008 R2 数据中心版 64位简体中文(40GB)	
14	Windows Server 2008 R2 企业版 64位英文(40GB)	
15	Windows Server 2008 R2 企业版 64位简体中文(40GB)	
16	Windows Server 2008 R2 Web版 64位简体中文(40GB)	

## 1.7 HSS 权限管理

如果您需要对HSS资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务资源的访问。

通过IAM，您可以在帐号中给员工创建IAM用户，并授权控制他们对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有HSS的使用权限，但是不希望他们拥有删除HSS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用HSS服务，但是不允许删除HSS的权限，控制他们对HSS资源的使用范围。

如果帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用HSS的其它功能。

## HSS 权限

默认情况下，系统管理员创建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

HSS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效，如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问HSS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对HSS服务，系统管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如表1-11所示，包括了HSS的所有系统权限。

表 1-11 HSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
HSS Administrator	企业主机安全服务（HSS）管理员，拥有该服务下的所有权限。	系统角色	● 依赖Tenant Guest角色。 Tenant Guest：全局级角色，在全局项目中勾选。
HSS FullAccess	企业主机安全服务所有权限。	系统策略	
HSS ReadOnlyAccess	企业主机安全服务的只读访问权限。	系统策略	无

## 1.8 与其他云服务的关系

使用企业主机安全服务，您将可以同时使用消息通知服务接收告警通知信息，使用统一身份认证服务管理用户权限，利用云审计服务审计用户行为。

### 弹性云服务器

企业主机安全服务的Agent软件可安装在ECS服务器上。

- 关于弹性云服务器的详细内容，请参见《弹性云服务器用户指南》。

## 消息通知服务

消息通知服务（Simple Message Notification，简称SMN），是一个可拓展的高性能消息处理服务。

- 开启告警通知前，您需先配置“消息通知服务”。
- 开启消息通知服务后，当您的主机遭受攻击或被检测出有高危风险时，您将接收到企业主机安全服务发送的各项风险告警通知。
- 在“告警通知”界面，您可以根据运维计划选择“每日告警通知”和“实时告警通知”。

关于SMN的详细内容，请参见《消息通知服务用户指南》。

## 统一身份认证服务

统一身份认证服务（Identity and Access Management，简称IAM），是一个免费的身份管理服务。通过IAM服务，您可以根据用户的身份，对用户的权限进行精细化隔离和控制。IAM是权限管理的基础服务，无需付费即可使用。

关于IAM的详细内容，请参见《统一身份认证服务用户指南》。

## 云审计服务

云审计服务（Cloud Trace Service，CTS），是一个专业的日志审计服务。云审计服务能够记录主机中用户对企业主机安全服务的操作，方便您对主机执行安全分析、合规审计、资源跟踪和问题定位等审计工作。云审计服务是管理日志的基础服务，无需付费即可使用。

关于CTS的详细内容，请参见《云审计服务用户指南》。

# 1.9 相关概念

## 账户破解

账户破解指入侵者对系统密码进行猜解或暴力破解的行为。

## 弱口令

弱口令指密码强度低，容易被攻击者破解的口令。

## 恶意程序

恶意程序指带有攻击或非法远程控制意图的程序，例如：后门、特洛伊木马、蠕虫、病毒等。

恶意程序通过把代码在不被察觉的情况下嵌到另一段程序中，从而达到破坏被感染服务器数据、运行具有入侵性或破坏性的程序、破坏被感染服务器数据的安全性和完整性的目的。按传播方式，恶意程序可以分为：病毒、木马、蠕虫等。

恶意程序包括已被识别的恶意程序和可疑的恶意程序。

## 勒索病毒

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。

一旦遭受勒索病毒攻击，将会使绝大多数的关键文件被加密。被加密的关键文件均无法通过技术手段解密，用户将无法读取原本正常的文件，仅能通过向黑客缴纳高昂的赎金，换取对应的解密私钥才能将被加密的文件无损的还原。黑客通常要求通过数字货币支付赎金，一般无法溯源。

如果关键文件被加密，企业业务将受到严重影响；黑客索要高额赎金，也会带来直接的经济损失，因此，勒索病毒的入侵危害巨大。

## 网页防篡改

网页防篡改为用户的文件提供保护功能，避免指定目录中的网页、电子文档、图片等类型的文件被黑客、病毒等非法篡改和破坏。

## 项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。项目可以是一个部门或者一个项目组。

一个帐户中可以创建多个项目。



# 2 开通主机防护

## 2.1 安装 Agent

### 2.1.1 Linux 版本

安装Agent后，您才能开启企业主机安全服务。通过本节介绍，您将了解如何在Linux操作系统的主机中安装Agent。Windows操作系统的Agent安装请参见[Windows版本](#)。

#### 说明

网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

#### 默认安装路径

在Linux操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装在以下路径中：

“/usr/local/hostguard/”


#### 前提条件

- 待安装Agent的主机已绑定弹性IP。
- 已在本地安装远程管理工具（如：“Xftp”、“SecureFX”、“WinSCP”）。
- 请关闭Selinux防火墙，防止Agent安装失败，安装成功后再打开。

#### 使用安装命令安装

登录待安装Agent的云主机，使用安装命令在线安装Agent。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏中，选择“安装与配置”，进入“安装Agent”界面，复制安装Agent的命令。

图 2-1 复制安装 Agent 的命令



**步骤4** 远程登录待安装Agent的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
- 若您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：“Xftp”、“SecureFX”、“WinSCP”）登录主机，并使用root账号在主机中安装Agent。

**步骤5** 粘贴复制的安装命令，并按“Enter”，在主机中安装Agent。

若界面回显信息与如下信息类似，则表示Agent安装成功。

```
Preparing... ##### [100%]
1:hostguard ##### [100%]
Hostguard is running.
Hostguard installed.
```

**步骤6** 使用service hostguard status命令，查看Agent的运行状态。

若界面回显如下信息，则表示Agent服务运行正常。

```
Hostguard is running
```

----结束

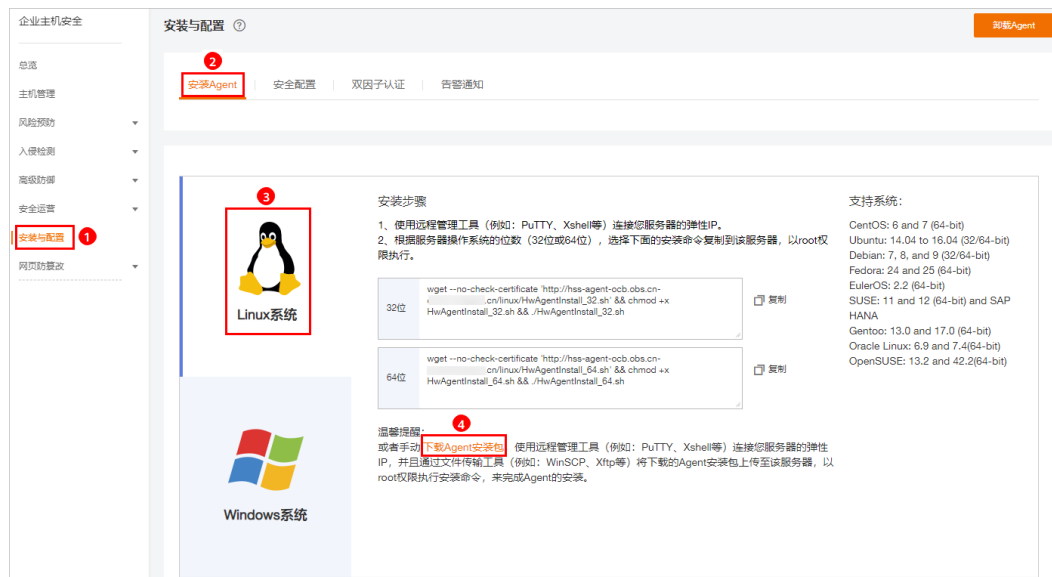
## 使用安装包安装

下载企业主机安全服务的Agent软件，上传至待安装Agent的云主机后，在云主机中使用安装命令安装Agent。

**步骤1** 登录管理控制台。

**步骤2** 在左侧导航栏中，选择“安装与配置”，进入“安装Agent”界面，下载Agent安装包。

图 2-2 下载 Agent 安装包



**步骤3** 在弹出的对话框中，根据待安装Agent的云服务器操作系统版本，下载所需安装的Agent。

**步骤4** 使用文件传输工具（例如：“Xftp”、“SecureFX”、“WinSCP”），将下载的Agent安装包上传至云主机。

**步骤5** 远程登录待安装Agent的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
- 若您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：“Xftp”、“SecureFX”、“WinSCP”）登录主机，并使用root账号在主机中安装Agent。

**步骤6** 使用cd 安装包所在目录命令，进入安装包所在目录。

**步骤7** 使用如下命令，在云主机中安装Agent。

- 安装“.rpm”格式的安装包，请执行命令：**rpm -ivh 安装包名称**。

#### 📖 说明

强制安装请执行命令：**rpm -ivh --force 安装包名称**

- 安装“.deb”格式的安装包，请执行命令：**dpkg -i 安装包名称**。

若界面回显信息与如下信息类似，则表示Agent安装成功。

```
Preparing... ##### [100%]
1:hostguard ##### [100%]
Hostguard is running.
Hostguard installed.
```

**步骤8** 使用**service hostguard status**命令，查看Agent的运行状态。

若界面回显如下信息，则表示Agent服务运行正常。

```
Hostguard is running
```

----结束

## 2.1.2 Windows 版本

在主机中安装Agent后，您才能开启企业主机安全服务。通过本节介绍，您将了解如何在Windows操作系统的主机中安装Agent。Linux操作系统的Agent安装请参见[Linux版本](#)。

### 说明

网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

### 默认安装路径

在Windows操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装在以下路径中：

“C:\Program Files (x86)\HostGuard”

### 前提条件


- 待安装Agent的主机已绑定弹性IP。
- 已在本地安装远程管理工具（如：“pcAnywhere”、“UltraVNC”）。

### 操作步骤

有两种安装方式，以下步骤演示方式一。

- 方式一：下载企业主机安全服务的Agent，上传至待安装Agent的云主机后，在云主机中安装Agent。
- 方式二：登录待安装Agent的云主机，在云主机中登录管理控制台，下载并安装Agent。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏中，选择“安装与配置”，进入“安装Agent”界面，获取下载Agent安装脚本的链接，下载Agent安装包。

图 2-3 安装 Windows Agent



**步骤4** 远程登录待安装Agent的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
- 若您的主机已经绑定了弹性IP，您也可以使用Windows系统的“远程桌面连接”工具，或第三方远程管理工具（例如：“pcAnywhere”、“UltraVNC”）登录主机，并使用系统管理员账号在主机中安装Agent。

**步骤5** 将Agent安装包上传到待安装Agent的主机中。

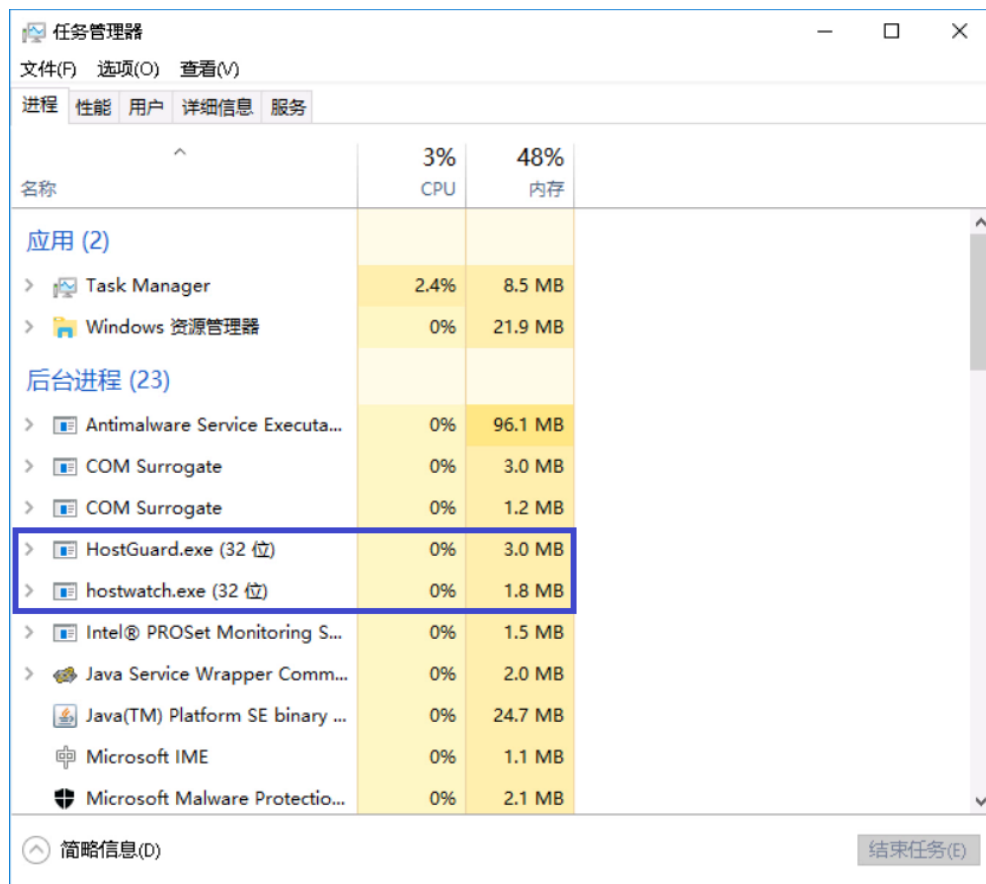
**步骤6** 使用系统管理员权限运行Agent安装程序。

安装Agent时，在主机类型界面，选择主机类型。

**步骤7** 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”，如图2-4所示。

若进程不存在，则表示Agent安装失败，请尝试重新安装Agent。

图 2-4 查看 Agent 运行状态



----结束

## 2.2 设置告警通知

### 2.2.1 基础版/企业版/旗舰版

开启告警通知功能后，您能接收到企业主机安全服务发送的告警通知，及时了解主机/网页内的安全风险。否则，无论是否有风险，您都只能登录管理控制台自行查看，无法收到报警信息。


- 告警通知设置仅在当前区域生效，若需要接收其他区域的告警通知，请切换到对应区域后进行设置。
- 告警通知信息可能会被误拦截，若您未收到相关告警信息，请在信息拦截中查看。

#### 前提条件

在设置告警通知前，建议您先以系统管理员身份在“消息通知服务”中创建“消息主题”。

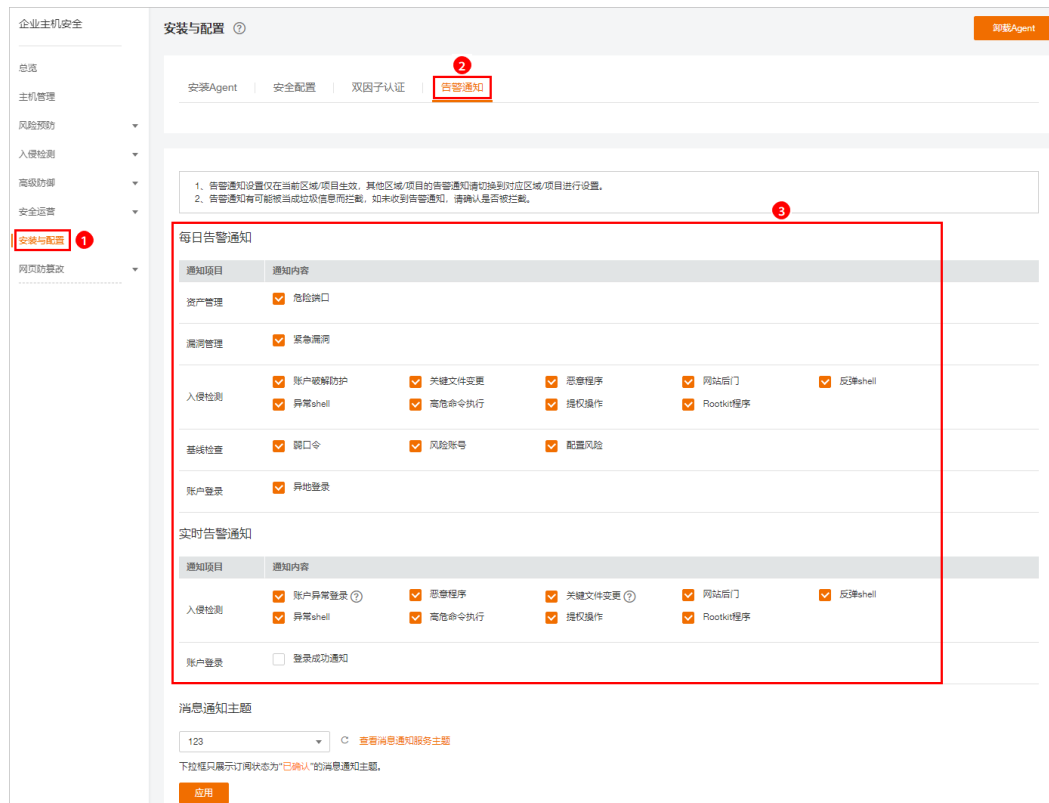
#### 开启基础版/企业版/旗舰版的告警通知

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 选择“安装与配置 > 告警通知”，进入“告警通知”页面，如图2-5所示。

图 2-5 基础版/企业版/旗舰版



**步骤4** 根据需要勾选“每日告警通知”和“实时告警通知”中的通知项。关于告警通知项详细说明，请参见[告警通知项说明](#)。

表 2-1 选择通知项

通知项	说明	选择建议
每日告警通知	每日凌晨，企业主机安全服务将主动检测主机系统中的账号、Web目录、漏洞、恶意程序及关键配置等，汇总各项检测结果后，将检测结果发送给您在“消息通知服务主题”中添加的订阅终端。	<ul style="list-style-type: none"> <li>接收并定期查看每日告警通知中所有的内容，能有效降低主机中未及时处理的风险成为主机安全隐患的概率。</li> <li>由于每日告警中通知项的内容较多，如果您使用的“消息通知服务”，接收告警通知，建议您选择“订阅终端”配置为“邮箱”的“消息通知服务主题”。</li> </ul>

通知项	说明	选择建议
实时告警通知	当攻击者入侵主机时，企业主机安全服务将按照“消息通知服务主题”为您告警。	<ul style="list-style-type: none"> <li>建议您接收实时告警通知中所有的内容并及时查看。企业安全服务实时监测主机中的安全情况，能监测到攻击者入侵主机的行为，接收实时告警通知能快速处理攻击者入侵主机的行为。</li> <li>由于实时告警中通知项的内容紧急度较高，如果您使用的“消息通知服务”，接收告警通知，建议您选择“订阅终端”配置为“短信”的“消息通知服务主题”。</li> </ul>

**步骤5** 选择消息通知主题。

您可以选择使用已有的主题，或者单击“查看消息通知服务主题”创建新的主题。

- 每个主题可以添加多个订阅，在选择主题前，请确保您在该主题中添加的订阅的状态为“已确认”，否则将不能收到告警通知。
- 主题订阅确认的信息可能被当成垃圾短信拦截，如未收到，请查看是否设置了垃圾短信拦截。
- 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

**步骤6** 单击“应用”，完成配置主机安全告警通知的操作。

----结束

## 告警通知项说明

通知项	通知内容	通知内容说明
<b>每日告警通知</b>		
每日凌晨检测主机中的风险，汇总并统计检测结果后，将检测结果于每日上午10:00发送给你添加的手机号或者邮箱。		
资产管理	危险端口	检测开放了的危险端口或者不必要的端口，通知用户及时排查这些端口是否用于正常业务。
漏洞管理	紧急漏洞	检测系统中的紧急漏洞，通知用户尽快修复，防止攻击者利用该漏洞会对主机造成较大的破坏。



通知项	通知内容	通知内容说明
入侵检测	账户破解防护	<p>检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击。</p> <ul style="list-style-type: none"> <li>如果30秒内，账户暴力破解次数达到5次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因账户破解被入侵。SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。</li> <li>根据账户暴力破解告警详情，如“攻击源IP”、“攻击类型”和“拦截次数”，您能够快速识别出该源IP是否为可信IP，如果为可信IP，您可以通过手动解除拦截的方式，解除拦截的可信IP。</li> </ul>
	关键文件变更	对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。
	恶意程序	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。
	网站后门	检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。
	高危命令执行	HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	提权操作	HSS检测当前系统的“进程提权”和“文件提权”操作。
	Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。
基线检查	弱口令	检测MySQL、FTP及系统账号的弱口令。
	风险账号	检测系统中的可疑账号、主机中无用的账号，防止未授权的访问权限和使用操作。
	配置风险	检测系统中的关键应用，如果采用不安全配置，有可能被黑客利用作为入侵主机系统的手段。
账户登录	异地登录	<p>检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施。</p> <p>若在非常用登录地登录，则触发安全事件告警。</p>

通知项	通知内容	通知内容说明
<b>实时告警通知</b> 事件发生时，及时发送告警通知。		
入侵检测	账户异常登录	检测“异地登录”和“账户暴力破解成功”等异常登录。若发生异常登录，则说明您的主机可能被黑客入侵成功。
	恶意程序	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。
	关键文件变更	对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。
	网站后门	检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。
	高危命令执行	HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	提权操作	HSS检测当前系统的“进程提权”和“文件提权”操作。
	Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。
账户登录	登录成功通知	<p>如果在“实时告警通知”项目中勾选了“登录成功通知”选项，则任何账户登录成功的事件都会向您实时发送告警信息。</p> <p>如果您所有主机上的账户都由个别系统管理员负责管理，通过该功能可以对系统账户进行严格的监控。</p> <p>如果系统账户由多人管理，或者不同主机由不同系统管理员负责管理，那么运维人员可能会因为频繁收到不相关的告警而对运维工作造成困扰，此时建议您登录企业主机安全服务控制台关闭该告警项。</p> <p><b>说明</b> 登录成功并不代表发生了攻击，需要您确认登录IP是否是已知的合法IP。</p>

## 2.2.2 网页防篡改版

开启告警通知功能后，您能接收到企业主机安全服务发送的告警通知，及时了解主机/网页内的安全风险。否则，无论是否有风险，您都只能登录管理控制台自行查看，无法收到报警信息。


- 告警通知设置仅在当前区域生效，若需要接收其他区域的告警通知，请切换到对应区域后进行设置。
- 告警通知信息可能会被误拦截，若您未收到相关告警信息，请在信息拦截中查看。

### 前提条件

在设置告警通知前，建议您先以系统管理员身份在“消息通知服务”中创建“消息主题”。

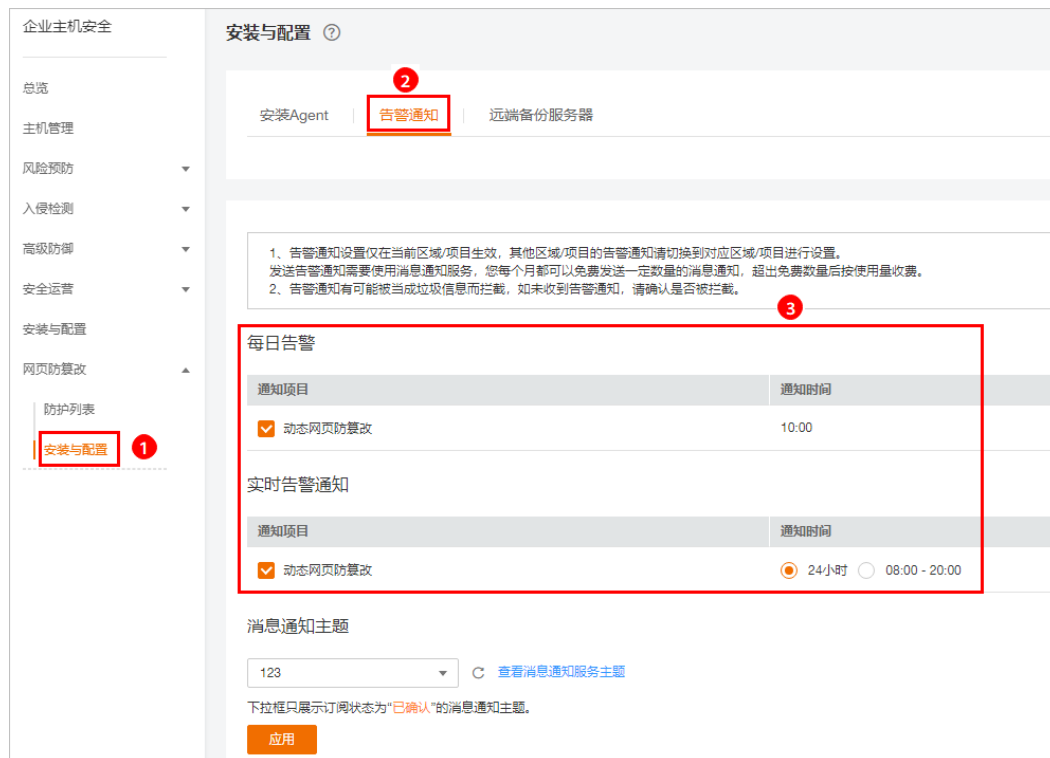
### 开启网页防篡改告警通知

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 选择“安装与配置 > 告警通知”，进入“告警通知”页面，选择告警通知时间，如图 2-6 所示。

图 2-6 告警通知设置



**步骤4** 选择消息通知主题。

您可以选择使用已有的主题，或者单击“查看消息通知服务主题”创建新的主题。

- 每个主题可以添加多个订阅，在选择主题前，请确保您在该主题中添加的订阅的状态为“已确认”，否则将不能收到告警通知。
- 主题订阅确认的信息可能被当成垃圾短信拦截，如未收到，请查看是否设置了垃圾短信拦截。
- 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

**步骤5** 单击“应用”，完成配置主机安全告警通知的操作。

----结束

## 2.3 开启主机防护

### 2.3.1 基础版/企业版/旗舰版

#### 检测周期

主机防护每日凌晨会进行全量检测。

若您在检测周期前开启防护，您需要等到次日凌晨检测后才能查看检测结果，或者立即执行手动检测。

#### 前提条件


- “企业主机安全 > 主机管理”页面“云服务器”中“Agent状态”为“在线”。
- 已开启告警通知。
- 为达到更好的防护效果，建议在开启防护前进行[安全配置](#)。

#### 约束条件

- Linux操作系统  
使用鲲鹏计算EulerOS（EulerOS with ARM）的主机，在遭受SSH账户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警。
- Windows操作系统
  - 开启主机防护时，需要授权开启Windows防火墙，且使用企业主机安全服务期间请勿关闭Windows防火墙。若关闭Windows防火墙，HSS无法拦截账户暴力破解的攻击源IP。
  - 通过手动开启Windows防火墙，也可能导致HSS不能拦截账户暴力破解的攻击源IP。

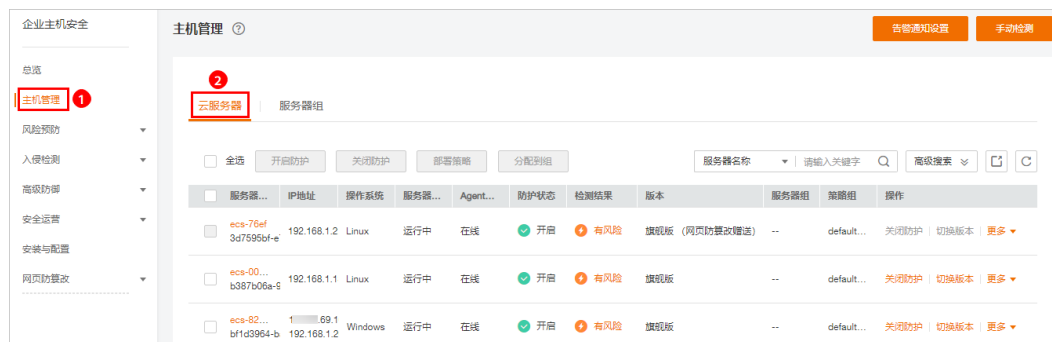
#### 开启防护

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏中，选择“主机管理”，进入“云服务器”界面，如[图2-7](#)所示。

图 2-7 进入“云服务器”界面



**步骤4** 选择所需开启安全防护的主机，单击“开启防护”。

在“开启防护”对话框中，选择“主机安全版本”，如图2-8所示。

图 2-8 开启主机防护



**步骤5** 单击“确定”，开启防护。开启企业主机安全防护后，请在控制台上查看企业主机安全服务的开启状态。

若目标主机的“防护状态”为“开启”，则表示基础版/企业版/旗舰版防护已开启。

开启主机防护后，HSS将根据您的服务版本，自动对您的主机执行服务版本对应的安全检测，如图2-9所示。

版本之间的差异请参见[服务版本差异](#)。

图 2-9 自动执行的安全检测



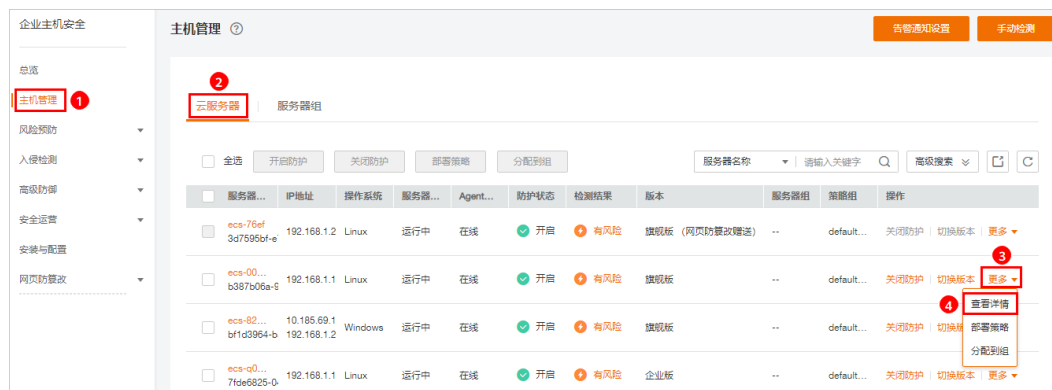
----结束

### 查看检测详情

开启防护后，企业主机安全服务将立即对主机执行全面的检测，检测时间可能较长，请您耐心等待。

在防护列表的“操作”列中单击“查看详情”，统一查看指定主机的检测结果。

图 2-10 查看详情



在详情界面，能快速查看主机中已被检测出的各项信息和风险。

图 2-11 查看检测结果



## 切换版本

您可根据需要将企业主机安全服务的版本从切换为“基础版”、“企业版”或者“旗舰版”。

### 须知

- 若企业主机安全服务的版本由高版本切换为低版本后，主机遭受攻击的可能性将升高。
- 仅支持将主机安全防护的版本切换为“基础版”、“企业版”或者“旗舰版”。

#### 变更前准备

- 切换为低版本前，请对主机执行相应的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。

#### 切换后操作

- 切换为低版本后，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。

- 切换为高版本后，请及时对主机执行安全检测、处理主机中的安全隐患并配置必要的功能。

## 后续操作

如果您需要检测更多的项目，请根据服务各版本支持的功能手动配置检测项，如图 2-12 所示。

版本之间的差异请参见[服务版本差异](#)。

图 2-12 手动配置的检测项



表 2-2 手动配置检测项

功能	检测项	相关链接
安全配置	<ul style="list-style-type: none"> <li>• 常用登录地/IP</li> <li>• SSH登录IP白名单</li> <li>• 开启恶意程序隔离查杀</li> </ul>	<a href="#">安全配置</a>
入侵检测	<ul style="list-style-type: none"> <li>• 配置告警白名单</li> <li>• 配置登录白名单</li> </ul>	<a href="#">入侵检测</a>



功能	检测项	相关链接
高级防御	<ul style="list-style-type: none"> <li>程序运行认证</li> <li>文件完整性管理</li> <li>勒索病毒防护</li> </ul>	<a href="#">高级防御</a>
安全运营	<ul style="list-style-type: none"> <li>自定义策略管理</li> </ul>	<a href="#">安全运营</a>

## 相关操作

### 关闭主机防护

您可以在“主机管理 > 云服务器”列表的“操作”列中单击“关闭防护”，关闭对指定主机的安全防护。

#### 须知

- 关闭主机防护前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。
- 关闭主机防护后，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。

## 2.3.2 网页防篡改改版

开启网页防篡改防护时会同步开启主机安全的旗舰版防护。

### 网页防篡改原理

表 2-3 网页防篡改原理

防护类型	原理说明
静态网页防护	<ol style="list-style-type: none"> <li>锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站负责人可通过特权进程进行更新网站内容。</li> <li>主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。</li> <li>远端备份恢复 若本地主机上的文件目录和备份目录失效，还可通过远端备份服务恢复被篡改的网页。</li> </ol>

防护类型	原理说明
动态网页防护	<ol style="list-style-type: none"><li>1. 基于RASP过滤恶意行为 采用RASP检测应用程序行为，有效阻断攻击者通过应用程序篡改网页内容的行为。</li><li>2. 网盘文件访问控制 精细化定义网盘文件中的文件访问权限，包括新增，修改，查询等，确保防篡改同时不影响网站内容发布。</li></ol>

## 约束条件

操作系统类型为Windows的主机在开启防护时，需开启Windows防火墙，使用企业主机安全服务期间请勿关闭Windows防火墙。

## 前提条件

- 在“网页防篡改 > 防护列表”页面中“Agent状态”为“在线”、“防护状态”为“关闭”。
- 在“企业主机安全 > 主机管理”页面“云服务器”列表中“Agent状态”为“在线”、“防护状态”为“关闭”。


## 设置防护目录

网页防篡改功能需要有防护目录才能起到防护作用，网页防篡改提供以下目录防护模式：

- 保护指定目录  
您最多可在主机中添加50个防护目录，详细操作请参见[保护指定目录](#)。  
为实时记录主机中的运行情况，请排除防护目录下Log类型的文件，您可以为日志文件添加等级较高的读写权限，防止攻击者恶意查看或篡改日志文件。
- 保护网络文件系统  
您最多可以添加5个文件系统，详细操作请参见[保护网络文件系统](#)。  
请确保添加的文件系统不是操作系统所在的系统分区。

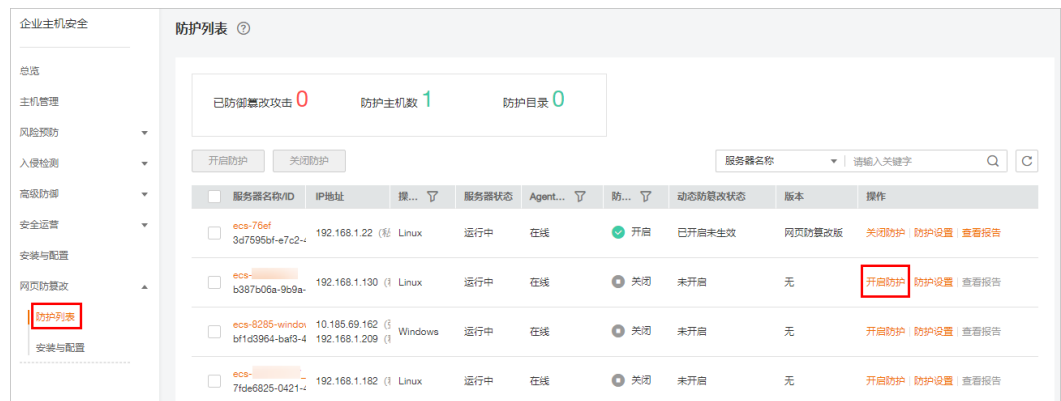
## 开启网页防篡改

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“网页防篡改”界面，单击“开启防护”。

图 2-13 进入“网页防篡改”界面



步骤4 在“开启防护”对话框中，单击“确定”，开启防护，如图2-14所示。

图 2-14 开启网页防篡改



步骤5 开启“网页防篡改”防护服务后，请在控制台上查看企业主机安全服务的开启状态。

----结束

### 须知

- 开启网页防篡改后如果需要更新网站请先临时关闭网页防篡改，完成更新后再开启。否则会造成网站更新失败。
- 关闭网页防篡改期间，您的网站不受保护，更新网页后，请及时开启网页防篡改。

## 相关操作

### 关闭网页防篡改

您可以在“网页防篡改 > 防护列表”列表的“操作”列中，单击“关闭防护”，关闭对指定主机的网页防篡改防护。

---


#### 须知

- 关闭网页防篡改防护服务前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。
  - 关闭网页防篡改防护服务后，网页应用被篡改的可能性将大大提高，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。
  - 执行关闭网页防篡改操作后，防护目录下的文件将不再受“网页防篡改”功能的防护，建议您提前处理防护目录下的文档，再对文档执行暂停防护、编辑或删除的相关操作。
  - 执行关闭网页防篡改操作后，若您的文档不慎被删除，请在主机本地备份或远端主机的备份路径中查找。
-

# 3 查看主机防护列表

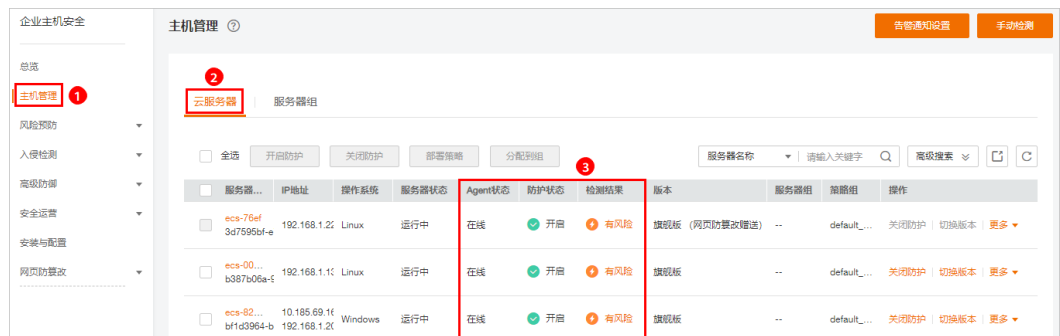
## 查看基础版/企业版/旗舰版防护列表

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“云服务器”界面，查看服务器的防护状态。

图 3-1 云服务器列表



### 说明


- 可以通过输入“服务器名称”、“公网IP地址”或者“私有IP地址”的方式，搜索符合条件的主机。
- 可以单击“高级搜索”，输入“服务器名称”、“服务器ID”、“IP地址”，选择“操作系统”、“Agent状态”、“防护状态”、“检查结果”、“策略组”、“服务器组”、“版本选择”或者“服务器状态”搜索符合条件的主机。
- 可以单击 ，导出主机列表。


表 3-1 状态说明

参数	说明
Agent状态	<ul style="list-style-type: none"> <li>未安装：未安装Agent，或Agent已安装但未成功启动。单击“安装Agent”，您可以根据弹出框给出的安装提示，进行Agent的安装。</li> <li>在线：Agent运行正常。</li> <li>离线：Agent与HSS服务器通信异常，HSS无法提供安全防护功能。单击“离线”，您可以查看Agent不在线的主机列表，并查看“离线原因”。</li> </ul>
防护状态	<ul style="list-style-type: none"> <li>开启：HSS为该服务器提供全面的主机安全防护。</li> <li>关闭：单击“关闭防护”可以暂停HSS对服务器的防护，降低该服务器的资源消耗。</li> </ul>
检测结果	<ul style="list-style-type: none"> <li>有风险：主机存在风险。</li> <li>无风险：主机暂未发现风险。</li> <li>未检测：主机未开启防护。</li> </ul>

----结束

## 查看网页防篡改防护列表

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

步骤3 在“网页防篡改 > 防护列表”界面，查看服务器的防护状态。

图 3-2 服务器列表

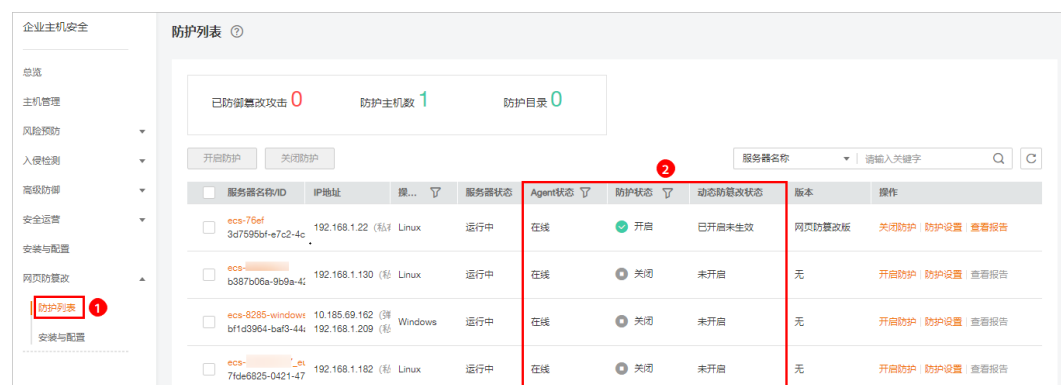


表 3-2 状态说明

参数名称	说明
Agent状态	<ul style="list-style-type: none"><li>未安装：未安装Agent，或Agent已安装但未成功启动。单击“未安装”，您可以根据弹出框给出的安装提示，进行Agent的安装。</li><li>在线：Agent运行正常。</li><li>离线：Agent与HSS服务器通信异常，HSS无法提供安全防护功能。单击“离线”，您可以查看Agent不在线的主机列表，并在该页面查看“离线原因”。</li></ul>
防护状态	<p>静态网页防篡改的状态。</p> <ul style="list-style-type: none"><li>开启：HSS为该服务器提供静态网页防篡改防护。</li><li>定时关闭：在“防护设置 &gt; 定时开关设置”可自定义防护时间段，详细操作请参见<a href="#">定时开关设置</a>。</li><li>关闭：单击“关闭防护”可以暂停静态网页防篡改防护，降低该服务器的资源消耗。</li></ul>
动态防篡改状态	<p>动态网页防篡改的状态。</p> <ul style="list-style-type: none"><li>已开启：在“防护设置 &gt; 动态网页防篡改”可开启动态网页防篡改，详细操作请参见<a href="#">开启动态网页防篡改</a>。</li><li>已开启未生效：动态网页防篡改开启后，请重启Tomcat使其生效。</li><li>未开启：未开启动态网页防篡改。</li></ul>

----结束

# 4 主机风险总览

企业主机安全在控制台提供总览页面，包括云主机的防护状态、当前开启防护的云主机最近24小时的风险统计、最近一周风险趋势和最近一周TOP5风险的云服务器，帮助您实时了解云主机的安全状态和存在的安全风险。

## 已开启防护的主机风险统计（最近 24 小时）

图 4-1 已开启防护的主机风险统计（最近 24 小时）



显示最近24小时，企业主机安全服务为开启防护的云服务器发现的各类风险的个数。

## 主机防护统计（最近 24 小时）

图 4-2 主机防护状态

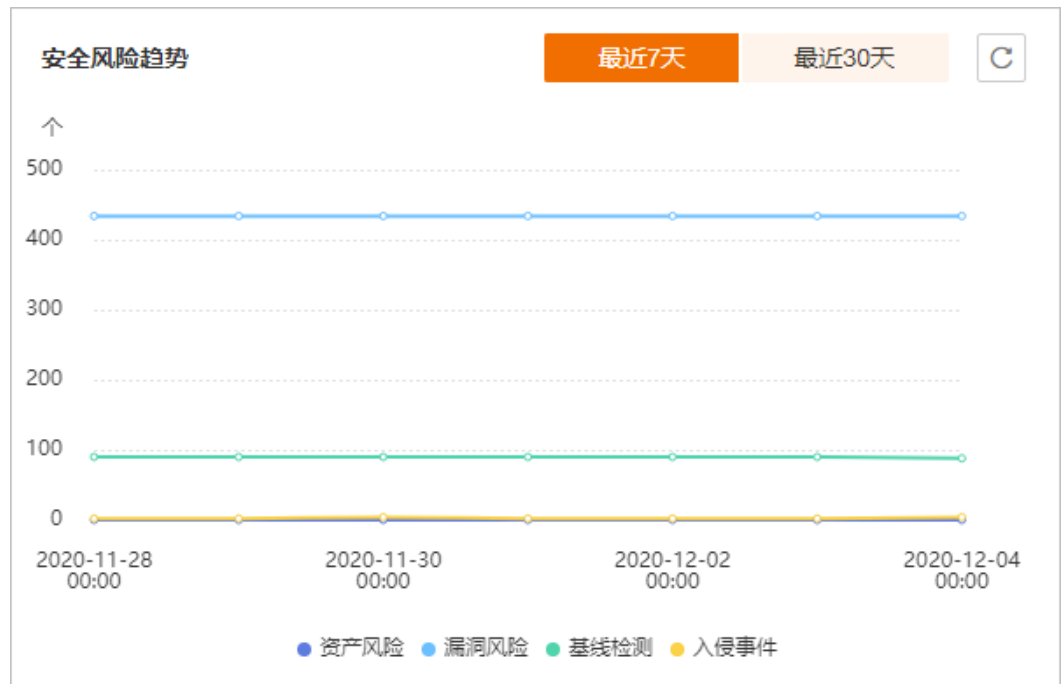


显示用户开启基础版防护、企业版防护、旗舰版防护和未开启防护的服务器的数量。单击“全部开启”，可跳转到云服务器列表，对未开启防护的服务器开启防护。



## 安全风险趋势

图 4-3 安全风险趋势



可显示最近7天、近30天的安全风险趋势。

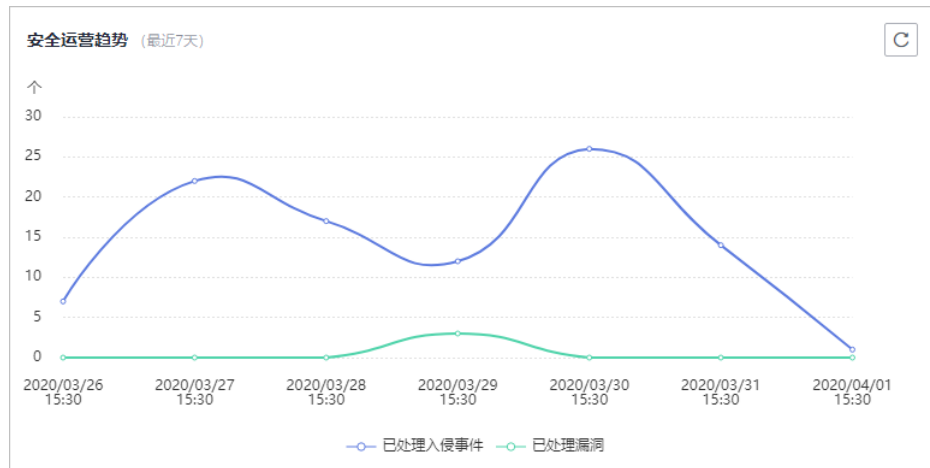
表 4-1 安全风险趋势说明

风险分类	风险事件
资产风险	<ul style="list-style-type: none"><li>• 账号信息</li><li>• 开放端口</li><li>• 进程信息</li><li>• Web目录</li><li>• 软件信息</li><li>• 自启动</li></ul>
漏洞风险	<ul style="list-style-type: none"><li>• Linux漏洞</li><li>• Windows漏洞</li><li>• Web-CMS漏洞</li></ul>
基线检测	<ul style="list-style-type: none"><li>• 口令复杂度策略检测</li><li>• 经典弱口令检测</li><li>• 配置检测</li></ul>

风险分类	风险事件
入侵事件	<ul style="list-style-type: none"><li>• 账户破解源IP</li><li>• 异常Shell</li><li>• 恶意程序</li><li>• 高危命令执行</li><li>• 进程异常行为</li><li>• 自启动检测</li><li>• 账户异常登录</li><li>• 提权操作</li><li>• 关键文件变更</li><li>• 高危恶意程序</li><li>• Rootkit程序</li><li>• 网站后门</li><li>• 风险账户</li><li>• 反弹Shell</li></ul>

### 安全运营趋势（最近 7 天）

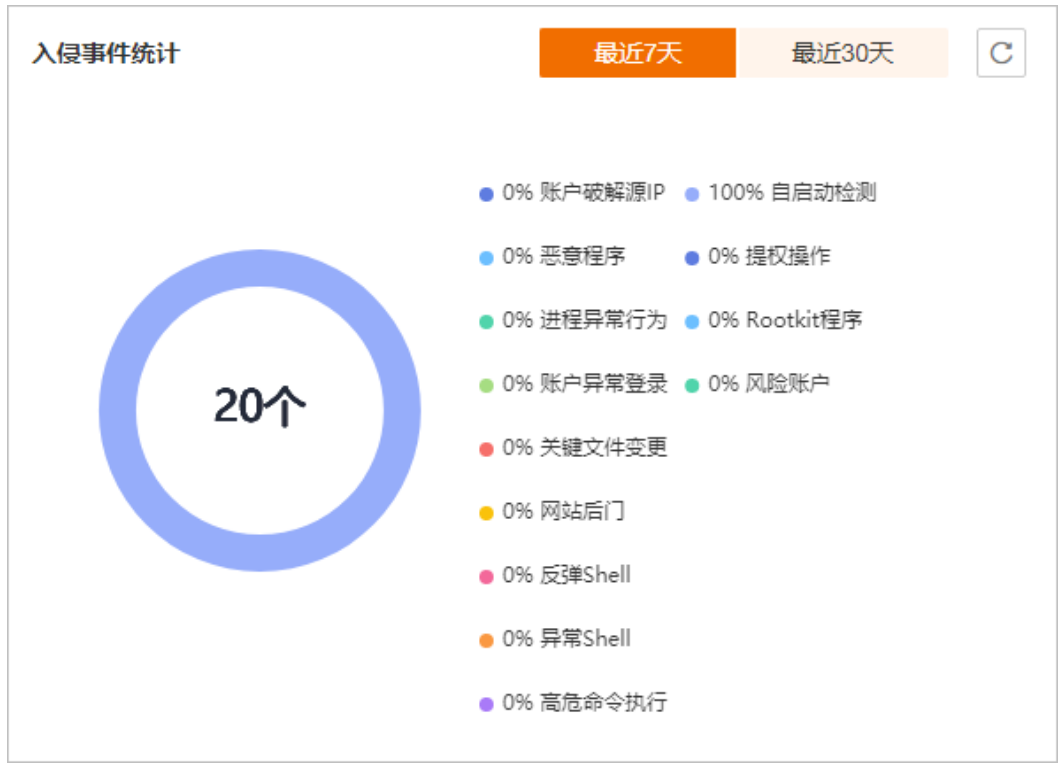
图 4-4 安全运营趋势



显示最近7天的已处理入侵事件和已处理漏洞。

## 入侵事件统计

图 4-5 入侵事件统计

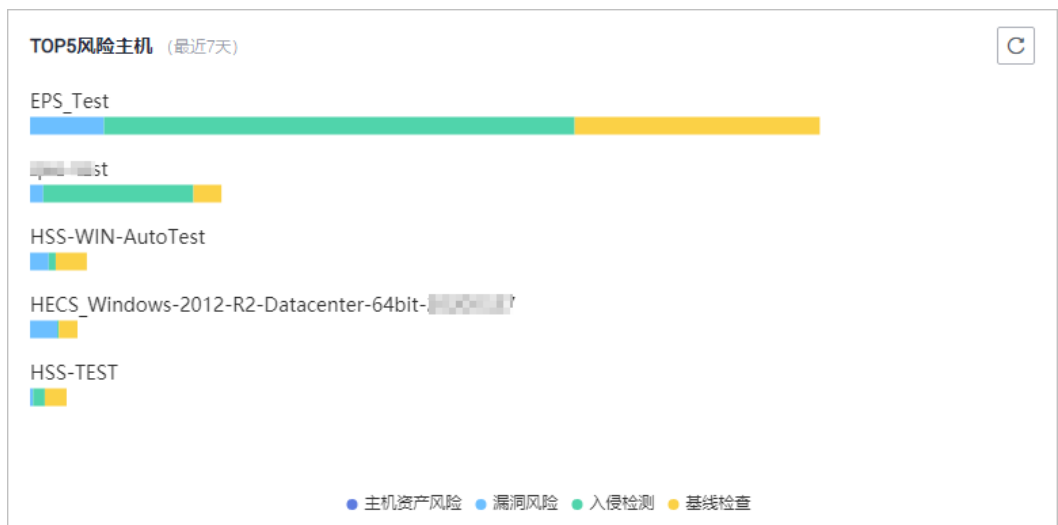


显示最近7天或者最近30天的入侵事件总个数，以及各类入侵事件分类占比。

每日凌晨12点，定时统计并更新用户的所有主机发生的入侵事件个数及各类入侵事件百分比。

## TOP5 风险主机（最近 7 天）

图 4-6 TOP5 风险的云服务器（最近 7 天）



基于开启了基础版、企业版或者旗舰版防护功能的云服务器，最近一周企业主机安全服务对其检测出的风险项TOP5的云服务器及各风险项的数量。

每日凌晨12点，定时统计用户的每个主机最近7天发生的风险个数，并展示TOP5风险的主机及各风险的数量。

## 实时入侵事件

图 4-7 实时入侵事件

实时入侵事件 <span style="float: right;">查看更多 &gt;</span>							
告警名称	受影响服务器名称/IP	简述	发生时间	处理时间	状态	处理方式	操作
风险账户	68.1.95	账号名: [redacted], 用户启动Shell: /bin/...	2020/05/11 09:2...	--	未处理	--	处理
Rootkit程序	68.1.95	Rootkit名称-SHV4 Rootkit, 特征: Found direct...	2020/05/11 09:2...	--	未处理	--	处理
Rootkit程序	68.1.95	Rootkit名称-SHV6, 特征: Found directory:/fi...	2020/05/11 09:2...	--	未处理	--	处理
异常自启动	68.1.247	类型: 自启动服务, 事件类型: 新增, 服务名: S12...	2020/05/11 09:2...	--	未处理	--	处理
异常自启动	68.1.247	类型: 自启动服务, 事件类型: 新增, 服务名: S20...	2020/05/11 09:2...	--	未处理	--	处理


展示最近24小时内发生的最近的5条“未处理”的入侵事件，包含入侵事件的“告警名称”、“受影响服务器名称/IP”、“简述”、“发生时间”和“状态”。

- 单击告警名称，可查看告警详细信息。
- 单击告警所在行的“操作列”中的“处理”，可处理该告警。处理该告警后，该告警将从该列表中消失，列表重新显示最近7天内发生的最近5条“未处理”的入侵事件。
- 单击“查看更多”，可进入“事件管理”页面，处理相关告警事件。

# 5 安全配置

开启防护后，您可以根据需要进行安全配置。包括配置SSH登录IP白名单，开启恶意程序自动隔离查杀功能。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

----结束

## 配置 SSH 登录 IP 白名单

SSH登录IP白名单功能是防护账户爆破的一个重要方式，主要是限制需要通过SSH登录的服务器。

配置了白名单的服务器，只允许白名单内的IP通过SSH登录到服务器，拒绝白名单以外的IP：

- 启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中，否则您将无法SSH远程登录您的服务器。  
若您的业务需要访问主机，但不需要SSH登录，则可以不用添加到白名单。
- IP加入白名单后，账户破解防护功能将不再对来自白名单中的IP登录行为进行拦截，该IP对您加入白名单的服务器登录访问将不受任何限制，请谨慎操作。

### 说明

使用鲲鹏计算EulerOS（EulerOS with ARM）的主机，SSH登录IP白名单功能对其不生效。

**步骤1** 在“SSH登录IP白名单”页面，单击“添加白名单IP”。

图 5-1 SSH 登录 IP 白名单



**步骤2** 在“添加SSH登录IP白名单”对话框中输入“白名单IP”，在“可选云服务器”列表中选择云服务器。

**说明**

“白名单IP”必须填写公网IP或者IP段（支持IPv6、IPv4地址）。如果设置的非公网IP地址，您将无法SSH远程登录您的服务器。

----结束

## 开启恶意程序隔离查杀

开启恶意程序隔离查杀后，HSS对识别出的后门、木马、蠕虫等恶意程序，提供自动隔离查杀功能，帮助用户自动识别处理系统存在的安全风险。

在“恶意程序隔离查杀”界面，选择“开启”，开启恶意程序隔离查杀功能，HSS将自动隔离查杀恶意程序。

图 5-2 恶意程序隔离查杀



自动隔离查杀有可能发生误报。您可以在企业主机安全控制台“入侵检测”页面中，选择“事件管理”页签，查看被隔离的恶意程序。在此您可以对指定的恶意程序执行取消隔离、忽略等操作，详情请参见[查看和处理入侵告警事件](#)。

### 须知

- 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若隔离查杀有误报，您可以执行取消隔离/忽略操作。
- 在“恶意程序隔离查杀”界面，如果不开启“恶意程序隔离查杀”功能，当HSS检测到恶意程序时，将会触发告警。  
您可以在“入侵检测”的“事件管理”中，查看“恶意程序（云查杀）”中的告警信息，并对恶意程序进行隔离查杀。

## 开启双因子认证

- 双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次认证，极大地增强云服务器账户安全性。
- 开启双因子认证功能后，登录云服务器时，主机安全服务将根据绑定的“消息通知服务主题”验证登录者的身份信息。

### 前提条件

- 用户已创建“协议”为“短信”或“邮箱”的消息主题。
- 主机已开启防护。
- Linux主机使用“密码”登录方式。
- 开启双因子认证需要关闭Selinux防火墙。
- 在Windows主机上，双因子认证功能可能会和“网防G01”软件、服务器版360安全卫士存在冲突，建议停止“网防G01”软件和服务器版360安全卫士。

### 约束与限制

- 开启双因子认证后，不能通过已安装图形化界面的Linux系统登录主机。

### 操作步骤

**步骤1** 在“双因子认证”页面，单击“开启双因子认证”。

图 5-3 双因子认证



**步骤2** 在弹出的“开启双因子认证”的对话框中，选择“验证方式”。

- **验证码验证**

在“开启双因子认证”页面选择“验证码验证”，单击“确认”，开启验证码验证。

图 5-4 验证码验证



**步骤3** 单击“确定”，完成开启双因子认证的操作。开启双因子认证功能后，需要等大约5分钟才生效。

#### 须知

在开启双因子认证功能的Windows主机上远程登录其他Windows主机时，需要在开启双因子主机上手动添加凭证，否则会导致远程登录其他Windows主机失败。

添加凭证：打开路径“开始菜单 > 控制面板 > 用户账户 > 凭据管理器 > 添加Windows凭据”，添加您需要访问的远程主机的用户名和密码。

----结束




# 6 主机管理

## 6.1 创建服务器组

用户可以创建服务器组，并将主机分配到服务器组，将主机进行分类管理。用户可以根据创建的服务器组，查看该服务器组内的服务器数量、有风险服务器的数量、以及未防护的服务器数量。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航树中，选择“主机管理”，在“服务器组”界面，单击“创建服务器组”，如图6-1所示。

图 6-1 进入服务器组页面

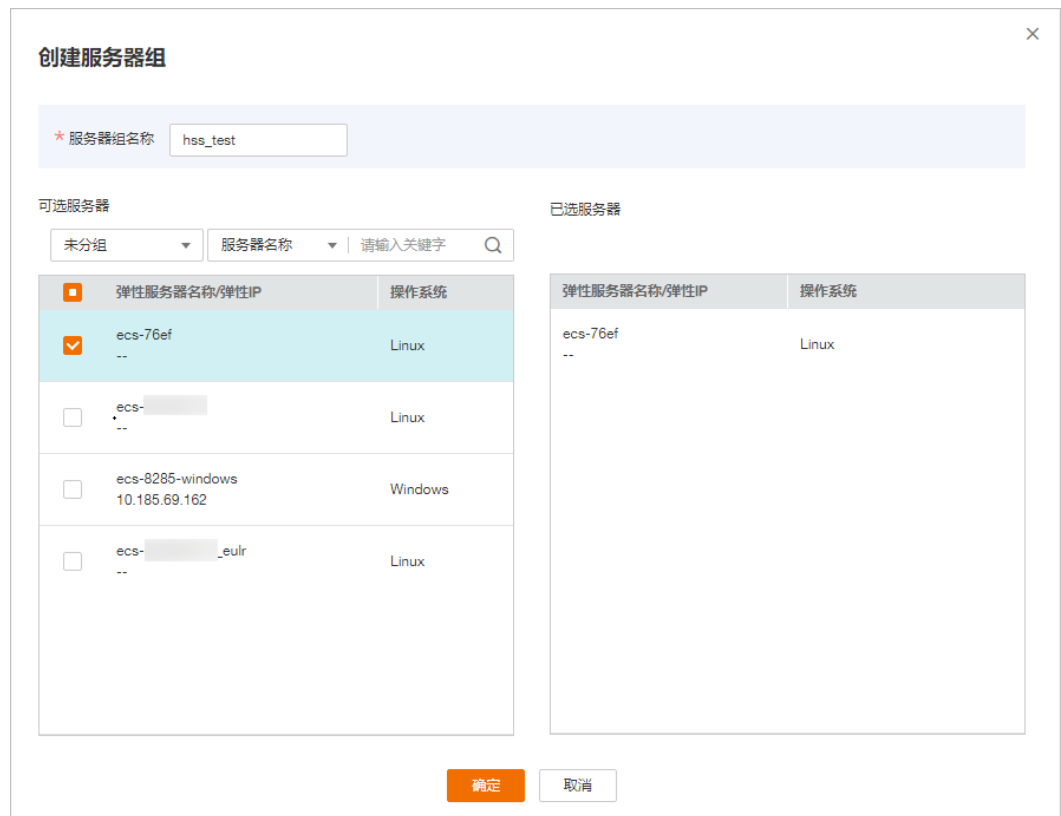


**步骤4** 在弹出的“创建服务器组”对话框中，输入“服务器组名称”，并设置服务器组中包含的云服务器，如图6-2所示。

### 说明

- 服务器组名称不能重复，如果尝试填写的服务器组名称重复，操作将会失败。
- “服务器组名称”不能包含空格，只能包含字母、数字、下划线、中划线、点、星号(\*)、加号(+); 且内容长度不能超过64个字符。

图 6-2 创建服务器组



步骤5 设置完成后，单击“确定”，完成服务器组的创建。

----结束

## 分配服务器到组

若服务器没有被分配到服务器组，您可以将服务器分配到已创建的服务器组。

步骤1 单击“云服务器”，进入云服务器列表界面。

步骤2 选中需要分配到服务器组的一台或多台云服务器，单击“分配到组”，将云服务器分配到服务器组，如图6-3所示。

图 6-3 分配到服务器组



### 📖 说明

您也可以在云服务器所在行的操作列，单击“更多”，然后单击“分配到组”，分配云服务器到服务器组。

**步骤3** 在弹出的对话框中，选择服务器组后，单击“确定”，完成分配云服务器到服务器组的操作。

### 📖 说明

一个云服务器只能分配到一个服务器组。

----结束

## 相关操作

### 编辑服务器组

**步骤1** 在待修改的服务器组所在行的操作列，单击“编辑”，修改服务器组。

**步骤2** 在弹出的对话框中，重新设置分组包含的云服务器。

**步骤3** 完成修改后，单击“确定”，完成服务器组的修改。

----结束

### 查看服务器组

在服务器组列表中，单击服务组的名称，可以查看服务器组中主机的状态、Agent状态、防护状态、检测结果等信息。

### 删除服务器组

在需要删除的服务器组所在行的“操作”列，单击“删除”，删除单个服务器组。

服务器组被删除后，隶属于该服务器组的所有云服务器将被划分到“未分组”中。

## 6.2 部署策略

用户可以通过新建策略组并将策略组快速分发给目标云服务器，云服务器上的Agent将会根据策略组中配置的策略开启相应的检测功能，实现安全检测。


### 操作须知

- 开启企业版防护时，默认绑定“默认企业版策略组”（包含“弱口令检测”和“网站后门检测”策略），应用于全部的云服务器，不需要单独部署策略
- 开启旗舰版/网页防篡改版防护时，默认绑定了“默认旗舰版策略组”。

用户也可以通过复制“默认旗舰版策略组”的方式，创建自定义策略组，将“默认旗舰版策略组”替换为用户的自定义策略组，更加灵活的应用于不同的云服务器或者云服务器组。

### 进入策略管理

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，选择“安全运营”，单击“策略管理”，进入“策略管理”界面。

----结束

## 创建策略组

**步骤1** 选择“default\_premium\_policy\_group（默认旗舰版策略组）”策略组，在该策略组所在行的操作列中，单击“复制”，如图6-4所示。

图 6-4 复制策略组



**步骤2** 在弹出的对话框中，输入“策略组名称”和“描述”，如图6-5所示。

### 说明

- 策略组的名称不能重复，如果尝试通过复制来创建一个同名的策略组，将会失败。
- “策略组名称”和“描述”只能包含中文、字母、数字、下划线、中划线、空格，并且首尾不能为空格。

图 6-5 创建策略组



**步骤3** 单击“确定”，将会创建一个新的策略组。

**步骤4** 单击已创建的策略组名称，进入策略组的策略页面，如图6-6所示。

图 6-6 策略组策略

策略名称	状态	功能类别	支持的操作系统	操作
资产管理	已启用	资产管理	Linux, Windows	关闭
系统配置检测	已启用	基线检查	Linux, Windows	关闭
弱口令检测	已启用	基线检查	Linux, Windows	关闭
高危命令检测	已启用	数据收集	Linux	关闭
提权检测	已启用	入侵检测	Linux	关闭
反弹/异常Shell检测	已启用	入侵检测	Linux	关闭
文件完整性管理	已启用	入侵检测	Linux	关闭
网站后门检测	已启用	入侵检测	Linux, Windows	关闭

**步骤5** 单击策略名称，修改具体的策略内容，详细信息请参见[修改策略内容](#)。

**步骤6** 策略内容修改完成后，单击策略所在行的“开启”或者“关闭”，开启或者关闭对应的策略。

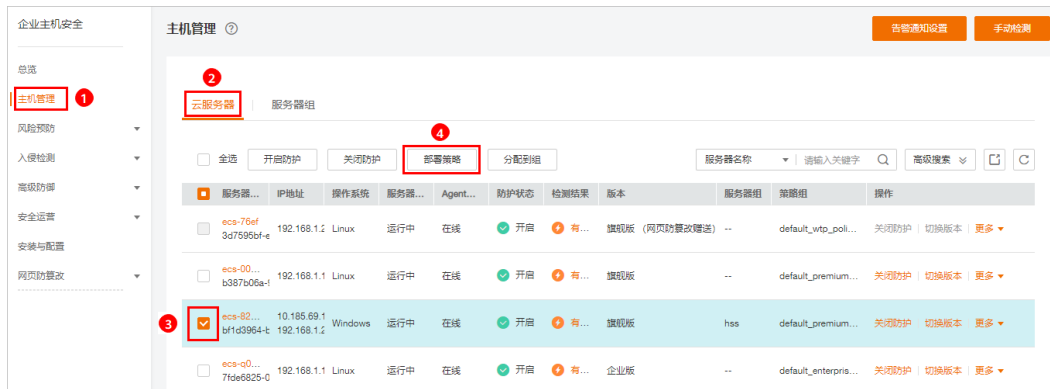
----结束

## 部署策略

**步骤1** 在左侧导航栏，选择“主机管理”，单击“云服务器”，进入云服务器列表界面。

**步骤2** 选中需要进行策略部署的一台或多台云服务器，单击“部署策略”，如[图6-7](#)所示。

图 6-7 部署策略



**步骤3** 在弹出的对话框中，选择策略组后，单击“确定”，完成部署策略操作。

图 6-8 选择策略组



#### 📖 说明

- 若当前云服务器已部署策略，再次部署策略时，会替换原有的策略组。
- 在1分钟内，策略组将被部署到所选主机上，对应的安全功能将会被启用。
- 对当前处于离线状态的主机，策略部署不会立即生效，需要等主机再次上线后，部署才会生效。
- 策略部署完成后，您可以通过开启或者关闭策略组中的策略的方式，或者修改策略组中策略内容的方式修改策略组。
- 已经部署的策略组不能删除。

---结束

# 7 风险预防

## 7.1 资产管理

HSS提供资产管理功能，主动检测主机中的开放端口、系统运行中的进程、主机中的Web目录和自启动项，并对账号信息和软件信息的变动情况进行记录。

通过资产管理，您能集中清点主机中的各项资产信息，及时发现主机中含有风险的各项资产。

资产管理仅提供风险检测功能，若发现有可疑资产信息，请手动处理。


### 检测周期

账号信息管理、开放端口检测：实时检测。

进程信息管理、Web目录管理、软件信息管理、自启动：**每日凌晨**自动进行一次检测。

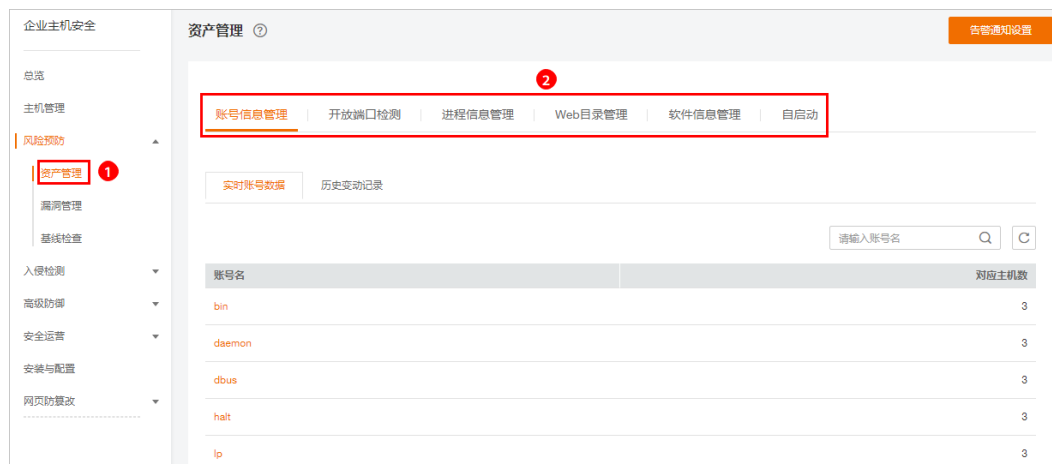
### 查看主机中的资产信息

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“资产管理”页面，选择不同页签，查看HSS检测到的您服务器上的所有资产。

图 7-1 资产管理



---结束

## 账号信息管理

历史变动状态说明：

- 变动状态：新建（新建了账号）、删除（删除了账号）、修改（修改了账号名、权限或用户组等信息）。
- 发生变动时间：由于为周期收集，变动记录的时间是获取到改动的时间，非真实发生的时间。

根据实时账号数据和历史变动记录，您可以统一管理所有主机中的账号信息。若发现系统中有多余的账号，或者发现有超级权限的账号（拥有root权限），需要排查这些账号是否是正常业务使用，如果不是则建议删除多余账号或者修改账号的权限，避免账号被黑客利用。

## 开放端口检测

根据开放端口检测结果中的详细信息，您可以统一管理所有主机中的开放端口。

- 手动关闭风险端口  
如果检测到开放了危险端口或者开放了不必要的端口，需要排查这些端口是否是正常业务使用，如果不是正常业务端口，建议关闭端口。对于危险端口建议进一步检查程序文件，如果存在风险建议删除或者隔离源文件。  
建议您及时优先处理危险程度为“危险”的端口，根据业务实际情况处理危险程度为“未知”的端口。
- 忽略风险：如果检测出的危险端口是业务正在使用的正常端口，您可以忽略该条告警。忽略之后将不再作为危险项进行记录，也不再发送告警。

## 进程信息管理

根据进程检测结果中的详细信息，您可以快速查看主机中可疑的应用进程，并及时终止可疑的应用进程。

进程信息管理检测的机制是30天检测不到进程后，自动清除进程信息管理列表中的进程信息。



## Web 目录管理

HSS能够检测出主机中存在的Web目录，您可以根据检测结果及时发现主机中可能含有风险的Web目录，及时删除可疑的Web目录并终止可疑的进程。

## 软件信息管理

历史变动状态说明：

- 变动状态：新增（新增的软件）、删除（删除的软件）。
- 发生变动时间：由于为周期收集，变动记录的时间是获取到改动的时间，非真实发生的时间。

根据实时软件数据和历史变动记录，您可以统一管理所有主机中的软件信息。若发现主机中的软件版本过低或存在可疑的软件，您可以及时升级低版本的软件或删除可疑和无需使用的软件。

## 自启动

大多数木马通常通过创建自启动服务、定时任务、预加载动态库、Run注册表键或者开启启动文件夹的方式入侵主机，自启动管理会收集所有云主机自启动的汇总信息，包含自启动的名称、类型和覆盖主机数。您可以根据统计并展示的自启动信息，快速发现主机中可疑的自启动。

您可以查看自启动项对应的服务器名称、路径、文件HASH和最后修改时间，及时发现并清除木马程序问题。

## 7.2 漏洞管理

### 7.2.1 查看漏洞详情

HSS提供漏洞管理功能，检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞。

在“漏洞管理”界面，您可以查看漏洞的信息和状态，根据“修复紧急度”排查主机中的漏洞。

“TOP5服务器”柱状图中，仅展示“修复紧急度”为“需尽快修复”的漏洞。

## 检测原理

表 7-1 漏洞检测原理

漏洞分类	原理说明
Linux软件漏洞	通过与漏洞库进行比对，检测出系统和软件（例如：SSH、OpenSSL、Apache、Mysql等）是否存在的漏洞，将结果上报至管理控制台，并为您提供漏洞告警。
Windows系统漏洞	通过订阅微软官方更新，判断服务器上的补丁是否已经更新，并推送微软官方补丁，将结果上报至管理控制台，并为您提供漏洞告警。

漏洞分类	原理说明
Web-CMS漏洞	通过对Web目录和文件进行检测，识别出Web-CMS漏洞，将结果上报至管理控制台，并为您提供漏洞告警。

### 说明


漏洞管理显示24小时内检测到的结果。若检测到主机存在漏洞后，您修改了主机的名称，检测结果会显示原主机名称。

## 检测周期

企业主机安全服务**每日凌晨**将自动进行一次全面的检测。

## Linux 软件漏洞/Windows 系统漏洞

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

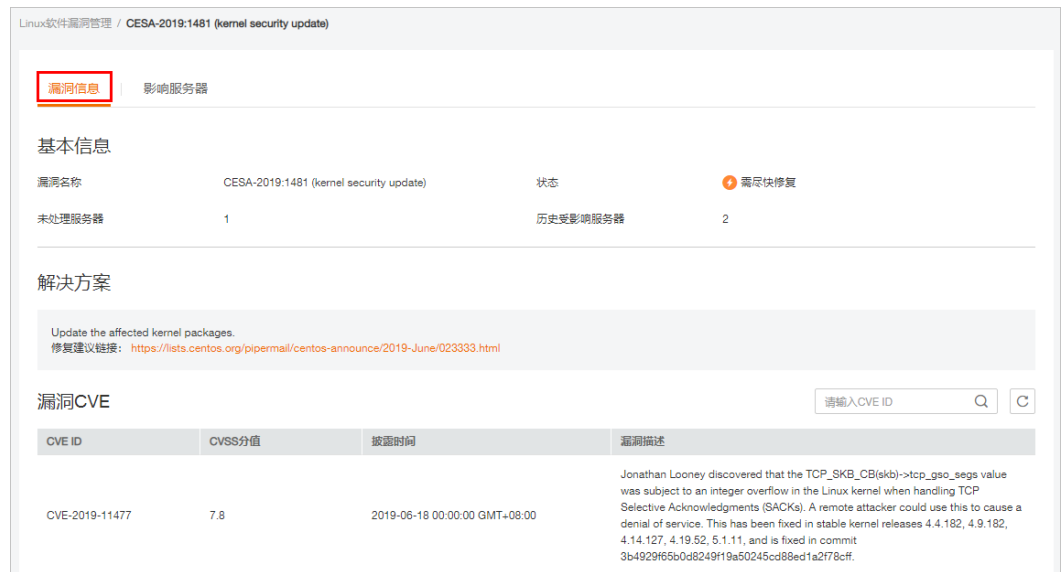
**步骤3** 选择“Linux软件漏洞管理”或“Windows系统漏洞管理”页签，进入相应漏洞管理页面，如图7-2所示。

图 7-2 查看 Linux 软件/Windows 系统漏洞检测结果



**步骤4** 单击“漏洞名称”，查看漏洞信息，包括漏洞基本信息、解决方案、CVE漏洞描述。

图 7-3 漏洞信息




**步骤5** 查看漏洞影响的服务器，在该页面，您可以对漏洞进行处理。

- 单击“修复”，您可一键修复该漏洞。
- 单击“忽略”，您可忽略该漏洞，HSS将不再上报并告警此服务器上的这个漏洞。
- 修复漏洞后，您可以单击“验证”，一键验证该漏洞是否已修复成功。  
若您未进行手动验证，主机防护每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看修复结果。  
若提示修复失败，可以单击“查看原因”了解具体原因并处理。

----结束

## Web-CMS 漏洞

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“Web-CMS漏洞管理”页面，如图7-4所示。

图 7-4 查看 Web-CMS 漏洞检测结果



**步骤4** 单击“漏洞名称”查看漏洞详情和受影响的服务器。

- Web-CMS漏洞不支持一键修复功能，请根据界面提供的修复建议进行手动修复。
- 漏洞修复后，请手动执行漏洞检测查看漏洞修复结果。若您未进行手动验证，主机防护每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看修复结果。
- 单击“忽略”，您可忽略该漏洞，HSS将不再上报并告警此服务器上的这个漏洞。

图 7-5 漏洞详细信息



图 7-6 受影响的服务器



---结束

## 导出漏洞报告

在漏洞列表的右上角，单击 ，导出漏洞报告。

### 7.2.2 漏洞修复与验证

- Linux软件漏洞和Windows系统漏洞：  
您可以使用“一键修复”功能进行修复，也可以根据界面提供的修复建议进行手动修复。  
修复完成后，可通过“验证”功能，快速验证漏洞是否修复成功。

#### 须知

Windows漏洞修复需要公网访问权限。

- Web-CMS漏洞：  
请根据界面提供的修复建议进行手动修复。

## 操作风险

- 执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云服务器备份（CSBS）为ECS创建备份。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。
- 在线修复主机漏洞时，需要连接Internet，通过外部镜像源提供漏洞修复服务。

## 修复紧急度

- 需尽快修复：您必须立即修复的漏洞，攻击者利用该类型的漏洞会对主机造成较大的破坏。
- 可延后修复：您需要修复的漏洞，为提高您主机的安全能力，建议您修复该类型的漏洞。
- 暂可不修复：该类型的漏洞对主机安全的威胁较小，您可以选择修复或忽略。


## 漏洞显示时长

- 漏洞状态为“修复失败”或者“未处理”的漏洞会一直显示在漏洞列表中。
- 漏洞状态为“修复成功”的漏洞，修复成功后，30天后才不会在漏洞列表中显示。

## 控制台一键修复漏洞

仅Linux软件漏洞和Windows系统漏洞支持控制台一键漏洞修复。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“漏洞管理”页面，单击“修复”，进入影响服务器页面，如图7-7所示。

图 7-7 修复漏洞



**步骤4** 在影响服务器页面，勾选影响的服务器，单击“一键修复”，修复漏洞，如图7-8所示。

图 7-8 一键修复漏洞



**步骤5** 在弹出的一键修复漏洞窗口中，勾选“我确定知晓如未进行创建备份，可能存在修复失败导致业务中断的风险，同时无法进行回滚”。

**步骤6** 单击“确定”，进行一键修复漏洞，修复状态处于“修复中”。

漏洞修复完成后，若修复成功，修复状态将变更为“修复成功”。若修复失败，修复状态将变更为“修复失败”。

### 说明

“Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要重启，否则HSS仍可能为你推送漏洞消息。

----结束

## 手动修复系统软件漏洞

根据漏洞列表右侧“解决方案”列中的修复建议修复主机中已经被识别出的漏洞，漏洞修复命令可参见表7-2。

- 不同的漏洞请根据修复建议依次进行修复。

- 若同一主机上的多个软件包存在同一漏洞，您只需修复一次即可。

#### 📖 说明

“Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要重启，否则HSS仍可能为你推送漏洞消息。

表 7-2 漏洞修复命令

操作系统	修复命令
CentOS/Fedora /Euler/ Redhat/Oracle	yum update 软件名称
Debian/Ubuntu	apt-get update && apt-get install 软件名称 -- only-upgrade
Gentoo、SUSE	请参见漏洞修复建议。

漏洞修复有可能影响业务的稳定性，为了防止在修复漏洞过程影响当前业务，建议参考以下两种方案，选择其中一种执行漏洞修复：

#### 方案一：创建新的虚拟机执行漏洞修复

1. 为需要修复漏洞的ECS主机创建镜像。
2. 使用该镜像创建新的ECS主机。
3. 在新启动的主机上执行漏洞修复并验证修复结果。
4. 确认修复完成之后将业务切换到新主机。
5. 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。

#### 方案二：在当前主机执行修复

1. 为需要修复漏洞的ECS主机创建备份。
2. 在当前主机上直接进行漏洞修复。
3. 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态。

#### 📖 说明

- 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。如果漏洞修复不成功可以随时释放以节省开销。
- 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。

## 漏洞忽略

某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某些漏洞无害，可以忽略该漏洞，无需修复。

忽略后，企业主机安全服务将不会对该漏洞告警。

## 修复验证

漏洞修复后，建议您立即进行验证。

### 手动验证

- 通过漏洞详情页面的“验证”，进行一键验证。
- 执行以下命令查看软件升级结果，确保软件已升级为最新版本。

表 7-3 验证修复命令

操作系统	修复命令
CentOS/Fedora /Euler/ Redhat/Oracle	rpm -qa   grep 软件名称
Debian/Ubuntu	dpkg -l   grep 软件名称
Gentoo	emerge --search 软件名称
SUSE	zypper search -dC --match-words 软件名称

- 手动执行漏洞检测查看漏洞修复结果。

### 自动验证

若您未进行手动验证，主机防护每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看修复效果。

## 7.3 基线检查

### 7.3.1 查看基线检查详情

HSS提供基线检查功能，主动检测主机中的口令复杂度策略，关键软件中含有风险的配置信息，并针对所发现的风险为您提供**修复建议**，帮助您正确地处理服务器内的各种风险配置信息。

### 检测周期

- 企业主机安全服务**每日凌晨**将自动进行一次全面的检查。
- 在“主机管理”页面右上角，单击“手动检测”，立即对选择执行手动检测的主机执行一键手动检测。

检测项目包含**软件信息**、**Linux软件漏洞**、**Windows系统漏洞**、**Web-CMS漏洞**、**网站后门检测**、**口令风险**和**配置风险**。

各检测项目并行检测，检测时长为30分钟内。

- 在“主机管理”页面，单击“检测结果”中的“有风险”或者“无风险”，进入单主机检测结果页面。

单击“基线检查”，在“口令风险”和“配置风险”页面，分别单击“手动检测”，立即对该主机执行“口令风险”和“配置风险”检测，检测时长为30分钟内。



## 告警策略

通过检测您服务器上的口令、账号、软件配置信息，如果发现您的服务器存在弱口令、配置风险，HSS将会触发告警信息。

### 📖 说明

您可在“企业主机安全 > 安装与配置”页面开启相应告警通知。详细操作请参见[基础版/企业版/旗舰版](#)。


## 检查项列表

表 7-4 检查项列表

检查项	说明
口令复杂度策略检测	检测系统账号的口令复杂度策略。
经典弱口令检测	通过与弱口令库对比，检测账号口令是否属于常用的弱口令。支持MySQL、FTP及系统账号的弱口令检测。
配置检测	目前支持的配置检测类型有： Tomcat、SSH、Nginx、Redis、Apache2、MySQL5、MongoDB、Windows、vsftp、CentOS。

## 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。


**步骤3** 进入“基线检查”页面，选择不同页签，查看HSS检测到的您服务器上存在的配置风险。

图 7-9 基线检查结果



----结束

## 导出配置检测报告

在配置检测页面，列表右上角单击，可将所有云服务器的配置检测风险列表下载到本地。

### 说明

不支持对单个云服务器执行导出。

## 7.3.2 基线检查风险项修复建议

当基线检查功能检测到并提示您服务器上存在的风险项时，请参考如下风险项修复建议为您的服务器进行安全加固。

### 增强口令复杂度策略

- 如需监测Linux主机中的口令复杂度策略，请先在主机中安装PAM（Pluggable Authentication Modules），详细操作请参见[如何为Linux主机安装PAM?](#)
- 修改Linux主机中口令复杂度策略的详细操作请参见[如何在Linux主机上设置口令复杂度策略?](#)
- 修改Windows主机中口令复杂度策略的详细操作请参见[如何在Windows主机上设置口令复杂度策略?](#)

**验证：**完成口令复杂度策略修改后，建议您立即执行手动检测，查看修复结果。如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

### 存在弱口令

- 为保障您的主机安全，请您及时修改登录主机系统时使用弱口令的账号，如SSH账号。
- 为保障您主机内部数据信息的安全，请您及时修改使用弱口令的软件账号，如MySQL账号和FTP账号等。

**验证：**完成弱口令修复后，建议您立即执行手动检测，查看弱口令修复结果。如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

## 存在配置风险

系统中的关键应用如果采用不安全配置，有可能被黑客利用作为入侵主机系统的手段。例如：SSH采用了不安全的加密算法；Tomcat服务采用root权限启动。

HSS可以检测系统中关键软件的配置风险并给出详细的加固方法。查看风险项的具体内容和建议的操作步骤如下：

- 修改有风险的配置项  
您可以根据“审计描述”验证检测结果，根据“修改建议”处理主机中的异常信息。  
建议您及时优先修复“威胁等级”为“高危”的关键配置，根据业务实际情况修复威胁等级为“中危”或“低危”的关键配置。

图 7-10 配置检测报告



- 忽略可信任的配置项  
选中单个存在风险的检测规则，单击操作列的“忽略”进行单个忽略。也可以选中多个检测规则，单击列表左上角的“忽略”批量进行忽略。  
对于已经忽略的检测规则，可以单击操作列的“取消忽略”，单个进行取消忽略，也可以批量选中想要取消忽略的规则撤销忽略。

验证：完成配置项的修复后，建议您立即执行手动检测，查看配置项修复结果。如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

# 8 入侵检测

## 8.1 告警事件概述

企业主机安全支持账户暴力破解、进程异常行为、网站后门、异常登录、恶意进程等13大类入侵检测能力，用户可通过事件管理全面了解告警事件类型，帮助用户及时发现资产中的安全威胁、实时掌握资产的安全状态。

### 告警事件列表说明

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改改版
账户暴力破解	<p>黑客通过账户暴力破解成功登录主机后，便可获得主机的控制权限，进而窃取用户数据、勒索加密、植入挖矿程序，DDoS木马攻击等恶意操作，严重危害主机的安全。</p> <p>检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击。</p> <ul style="list-style-type: none"><li>如果30秒内，账户暴力破解次数达到5次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因账户破解被入侵。SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。</li><li>根据账户暴力破解告警详情，如“攻击源IP”、“攻击类型”和“拦截次数”，您能够快速识别出该源IP是否为可信IP，如果为可信IP，您可以通过手动解除拦截的方式，解除拦截的可信IP。</li></ul>	√	√	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
账户异常登录	<p>检测“异地登录”和“账户暴力破解成功”等异常登录。若发生异常登录，则说明您的主机可能被黑客入侵成功。</p> <ul style="list-style-type: none"> <li>检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。异地登录检测信息包括被拦截的“登录源IP”、“登录时间”，攻击者尝试登录主机时使用的“用户名”和“云服务器名称”。</li> <li>若在非常用登录地登录，则触发安全事件告警。</li> <li>若账户暴力破解成功，登录到云主机，则触发安全事件告警。</li> </ul>	√	√	√	√
恶意程序（云查杀）	<p>恶意程序可能是黑客入侵成功之后植入的木马、后门等，用于窃取数据或攫取不当利益。</p> <p>例如：黑客入侵之后植入木马，将受害主机作为挖矿、DDoS肉鸡使用，这类程序会大量占用主机的CPU资源或者网络资源，破坏用户业务的稳定性。</p> <p>通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。</p>	×	√ (隔离查杀)	√ (隔离查杀)	√ (隔离查杀)
进程异常行为	<p>检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。</p> <p>对于进程的非法行为、黑客入侵过程进行告警。</p> <p>进程异常行为可以监控以下异常行为：</p> <ul style="list-style-type: none"> <li>监控进程CPU使用异常。</li> <li>检测进程对恶意IP的访问。</li> <li>检测进程并发连接数异常等。</li> </ul>	×	√	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
关键文件变更	<p>篡改系统关键文件，通常是黑客入侵成功后进行身份隐藏或者发起下一步攻击的准备工作。</p> <ul style="list-style-type: none"> <li>对系统关键文件（例如：ls、ps、login、top等）进行监控，一旦文件被修改就进行告警，提醒用户关键文件存在被篡改的可能。监控的关键文件的路径请参见<a href="#">关键文件变更监控路径</a>。</li> <li>关键文件变更信息包括“被更改的关键文件路径”、“文件最后修改时间”以及配置文件所在的“服务器名称”。</li> <li>添加关键文件指纹库，收集关键文件信息，便于清点合法文件信息，检测异常文件。</li> </ul> <p>对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。</p>	×	√	√	√
网站后门	<p>以php、jsp等网页文件形式存在的一种命令执行环境。</p> <p>黑客在入侵了一个网站后，通常会将后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后使用浏览器来访问php或者jsp后门，得到一个命令执行环境，以达到控制网站服务器的目的。</p> <p>检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。</p> <ul style="list-style-type: none"> <li>网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略被查杀的可信文件。</li> <li>您可以使用手动检测功能检测主机中的网站后门。</li> </ul>	×	√	√	√
反弹Shell	<p>实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。</p> <p>支持对TCP、UDP、ICMP等协议的检测。</p> <p>您可以在“策略管理”的“反弹/异常Shell检测”中配置反弹Shell检测，HSS会实时检测执行的可疑指令，主机被远程控制执行任意命令等。</p>	×	×	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。 您可以在“策略管理”的“反弹/异常Shell检测”中配置异常Shell检测，HSS会实时检测执行的可疑指令，主机被远程控制执行任意命令等。	×	×	√	√
高危命令执行	您可以在“策略管理”的“高危命令检测”中预置高危命令。 HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	×	×	√	√
自启动检测	大多数木马通常通过创建自启动服务、定时任务、预加载动态库等方式入侵主机，自启动检测会收集所有云主机自启动的信息，帮助您快速发现主机中可疑的自启动，并清除木马程序问题。 HSS检测并列举当前系统中的自启动服务、定时任务、预加载动态库、Run注册表键和开机启动文件夹，帮助用户及时发现非法自启动。	×	×	√	√
风险账户	黑客可能通过风险账户入侵主机，以达到控制主机的目的，需要您及时排查系统中的账户。 HSS检查系统中存在的可疑隐藏账号、克隆账号；若存在可疑账号、克隆账号等，则触发告警。	×	√	√	√
提权操作	当黑客成功入侵主机后，会尝试利用漏洞进行root提权或者文件提权，从而达到非法创建和修改系统账号的权限或者篡改文件的目的。 HSS检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： <ul style="list-style-type: none"> <li>● 利用SUID程序漏洞进行root提权。</li> <li>● 利用内核漏洞进行root提权。</li> <li>● 对文件的提权。</li> </ul>	×	×	√	√
Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。 <ul style="list-style-type: none"> <li>● 使用文件特征码检测Rootkit。</li> <li>● 对隐藏文件、端口、进程的检测。</li> </ul>	×	×	√	√

## 关键文件变更监控路径

类型	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/netstat /bin/login /bin/find /bin/lsmmod /bin/pidof /bin/lsof /bin/ss
usr	/usr/bin/ls /usr/bin/ps /usr/sbin/ps /usr/bin/bash /usr/bin/netstat /usr/sbin/netstat /usr/sbin/rsyslogd /usr/sbin/ifconfig /usr/bin/login /usr/bin/find /usr/sbin/lsmmod /usr/sbin/pidof /usr/bin/lsof /usr/sbin/lsof /usr/sbin/tcpd /usr/bin/passwd /usr/bin/top /usr/bin/du /usr/bin/chfn /usr/bin/chsh /usr/bin/killall /usr/bin/ss /usr/sbin/ss /usr/bin/ssh /usr/bin/scp



类型	Linux
sbin	/sbin/syslog-ng /sbin/rsyslogd /sbin/ifconfig /sbin/lsmmod /sbin/pidof

## 8.2 查看和处理入侵告警事件

企业主机安全可对您已开启的告警防御能力提供总览数据，帮助您快速了解安全告警概况包括存在告警的服务器、待处理告警事件、未处理告警事件、已拦截IP和已隔离文件。

事件管理列表仅保留近30天内发生的告警事件，您可以根据自己的业务需求，自行判断并处理告警，快速清除资产中的安全威胁。


告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

### 约束与限制

- 若不需要检测高危命令执行、提权操作、反弹Shell、异常Shell或者网站后门，您可以通过“策略管理”页面手动关闭指定策略的检测。关闭检测后，HSS不对策略组关联的服务器进行检测。
- 其他检测项不允许手动关闭检测。

### 查看告警事件

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏中，单击“入侵检测 > 事件管理”，进入“事件管理”页面，如[图8-1](#)所示。

图 8-1 事件管理

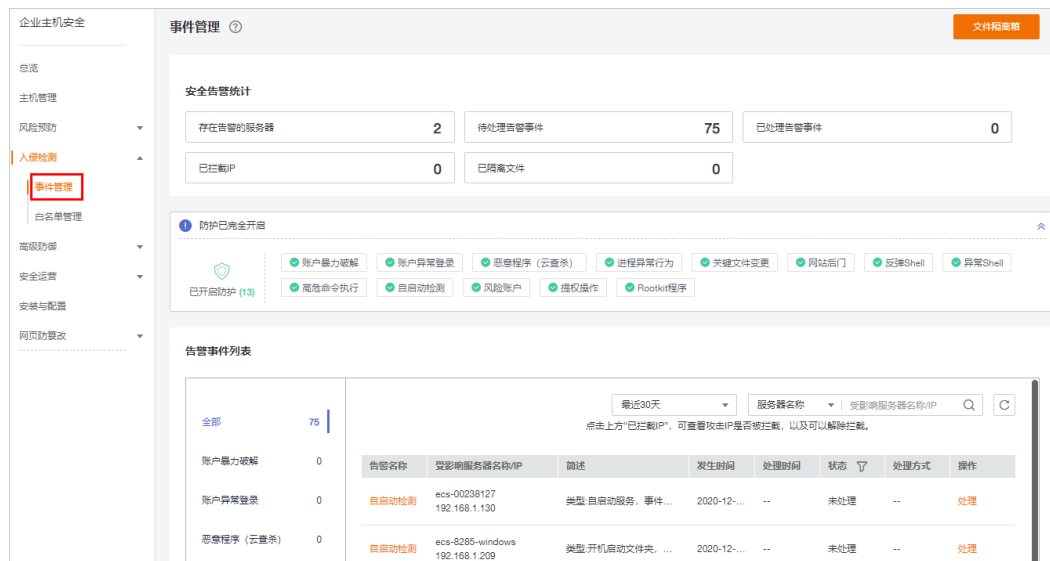


表 8-1 安全告警事件列表说明

告警事件状态	告警事件状态说明
存在告警的服务器	展示存在告警的服务器数量。
待处理告警事件	展示您资产中所有待处理告警的数量。 安全告警处理页面默认展示所有待处理告警信息，更多详细内容请参见 <a href="#">处理告警事件</a> 。
已处理告警事件	展示您资产中所有已处理的告警事件数量。
已拦截IP	展示已拦截的IP。单击已拦截IP的数量，可查看已拦截的IP地址列表。 如果您发现有合法IP被误封禁（比如运维人员因为记错密码，多次输错密码导致被封禁），可以手工解除拦截。如果发现某个主机被频繁攻击，需要引起重视，建议及时修补漏洞，处理风险项。 <b>须知</b> 解除被拦截的IP后，主机将不会再拦截该IP地址对主机执行的操作。
已隔离文件	企业主机安全可对检测到的威胁文件进行隔离处理，被成功隔离的文件会添加到“事件管理”的“文件隔离箱”中。 被成功隔离的文件一直保留在文件隔离箱中，您可以根据需要进行一键恢复处理，关于文件隔离箱的详细信息，请参见 <a href="#">管理文件隔离箱</a> 。

**步骤4** 单击告警事件列表中的告警事件，可查看告警事件对应的受影响的服务器、发生时间等信息，如图8-2所示。

- 全部：展示发生的总的告警数。
- 告警事件：展示各告警事件发生的告警数。

图 8-2 告警事件统计数量

告警名称	受影响服务器名称/IP	简述	发生时间	处理时间	状态	处理方式	操作
自启动检测	ecs-192.168.1.130	类型:自启动服务, 事件...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...	2020-12-...	--	未处理	--	处理

步骤5 单击告警列表中的告警名称，可查看告警的详细信息，如图8-3所示。

图 8-3 告警详细信息

告警名称	受影响服务器名称/IP	简述
自启动检测	ecs-192.168.1.130	类型:自启动服务, 事件...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...
自启动检测	ecs-8285-windows-192.168.1.209	类型:开机启动文件夹, ...

自启动检测	
服务器名称	ecs-192.168.1.130
IP地址	192.168.1.130
服务名	S98denyhosts
路径	/etc/rc.d/rc3.d/S98denyhosts
类型	自启动服务
事件类型	删除
运行用户	--
文件HASH	e54ac02e06dea5c51a6f922c4c323e337b2bac0ca90c1b9ba79f4fa89b
状态	未处理

---结束


## 处理告警事件

当发生安全告警事件后，为了保障您的云服务器安全，可以根据以下方式处理安全告警事件。

### 说明

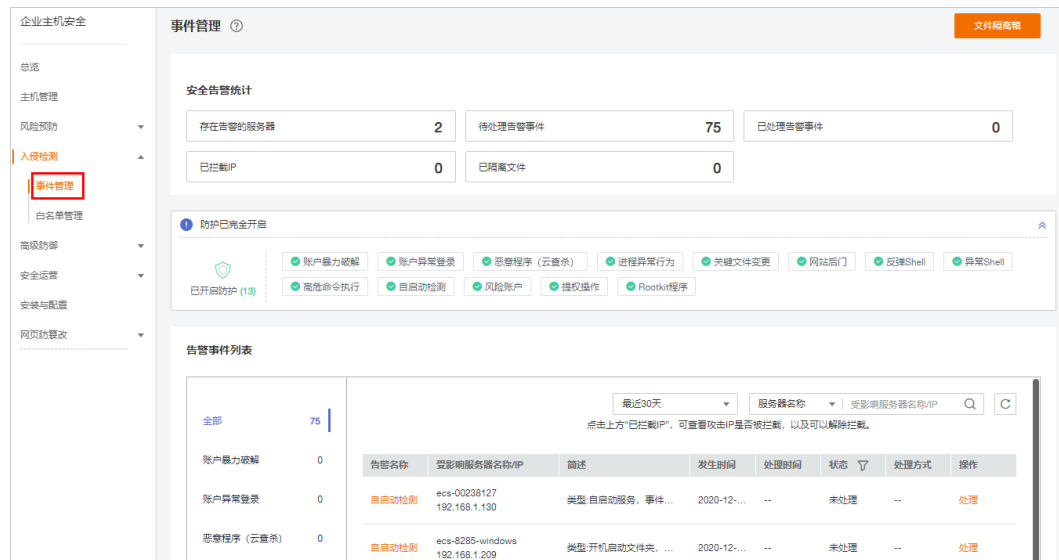
由于网络攻击手段、病毒样本在不断演变，实际的业务环境也有不同差异，因此，无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，单击“入侵检测 > 事件管理”，进入事件管理页面。

图 8-4 事件管理



**步骤4** 单击告警列表中的告警事件，勾选待处理的告警事件，单击“批量处理”，处理告警事件，如图8-5所示，处理方式如表8-2所示。

### 说明

您也可以单击告警名称所在行的“处理”，处理告警。

图 8-5 处理告警事件



告警事件展示在“事件管理”页面中，事件管理列表仅展示最近30天的告警事件。

您需要根据自己的业务需求，自行判断并处理告警。告警事件处理完成后，告警事件将从“未处理”状态变更为“已处理”。HSS将不再对已处理的事件进行统计，并且不在“总览”页展示。

表 8-2 处理告警事件

处理方式	处理方式说明
忽略	仅忽略本次告警。若再次出现相同的告警信息，HSS会再次告警。
隔离查杀	<p>选择隔离查杀后，该程序无法执行“读/写”操作，同时该程序的进程将被立即终止。HSS将程序或者进程的源文件加入文件隔离箱，被隔离的文件不会对主机造成威胁。</p> <p>您可以单击“文件隔离箱”，查看已隔离的文件，详细信息请参见<a href="#">管理文件隔离箱</a>。</p> <p>有以下两类告警事件支持线上隔离查杀。</p> <ul style="list-style-type: none"> <li>● 恶意程序（云查杀）</li> <li>● 进程异常行为</li> </ul> <p><b>说明</b> 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若隔离查杀有误报，您可以执行取消隔离/忽略操作。</p>
手动处理	选择手动处理。您可以根据自己的需要为该事件添加“备注”信息，方便您记录手动处理该告警事件的详细信息。

处理方式	处理方式说明
加入登录白名单	<p>如果确认“账号暴力破解”和“账户异常登录”类型的告警事件是误报，且不希望HSS再上报该告警，您可以将本次登录告警事件加入登录白名单。</p> <p>HSS不会对登录白名单内的登录事件上报告警。加入登录白名单后，若再次出现该登录事件，则HSS不会告警。</p>
加入告警白名单	<p>如果确认以下类型的告警事件是误报，且不希望HSS再上报该告警，您可以将本次告警事件加入告警白名单。</p> <p>HSS不会对告警白名单内的告警事件上报告警。加入告警白名单后，若再次出现该告警事件，则HSS不会告警。</p> <ul style="list-style-type: none"> <li>● 反弹Shell</li> <li>● Webshell检测</li> <li>● 进程异常行为检测</li> <li>● 进程提权</li> <li>● 文件提权</li> <li>● 高危命令</li> <li>● 恶意程序</li> </ul>

----结束

## 告警处理建议

告警名称	处理建议
账户暴力破解	<p><b>该告警事件需要您高度重视。</b></p> <p>若接收到账户暴力破解告警通知，说明您的主机可能存在被暴力破解风险，包括但不限于以下这些情况：</p> <ul style="list-style-type: none"> <li>● 系统存在弱口令，同时正在遭受暴力破解攻击。</li> <li>● 数次口令输错（但未达到封禁源IP条件）后成功登录。</li> </ul> <p>建议您立即确认源IP是否是已知的合法IP。</p> <ul style="list-style-type: none"> <li>● 若源IP合法。 您可以“忽略”该次告警并手工解除IP封禁。或者“加入告警白名单”，该告警将不会再次触发。</li> <li>● 若源IP不合法，是未知IP，那么您的主机系统可能已经被黑客入侵成功。 <ol style="list-style-type: none"> <li>1. 建议您将该事件标记为“手动处理”。</li> <li>2. 立即登录系统并修改并设置安全的账户密码。</li> <li>3. 通过账号信息管理和风险账户排查所有系统账户，对可疑账户进行处理，防止攻击者创建新的账户或者更改账户权限。</li> <li>4. 通过恶意程序（云查杀）排查系统是否被植入了恶意程序。针对恶意程序，请登录云主机，尽快结束其进程，阻止恶意程序运行。</li> </ol> </li> </ul>

告警名称	处理建议
账户异常登录	<p>若检测出账户异常登录，建议您立即确认该源IP是否是已知的合法IP。</p> <ul style="list-style-type: none"> <li>若源IP合法，您可以“忽略”该事件。如果该登录地是合法的常用登录地，您可以将该地区加入“常用登录地”列表。</li> <li>若该源IP不合法，是未知IP，那么您的主机系统已经被入侵成功，需要您高度重视。建议您将该事件标记为“手动处理”，并立即登录系统并修改账户密码，同时全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>
恶意程序（云查杀）	<p>若检测出存在恶意程序，建议您立即对该程序进行确认：</p> <ul style="list-style-type: none"> <li>若该程序属于正常业务，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。</li> <li>若是未知程序或者经确认是恶意程序，建议立即执行进程查杀并隔离程序源文件。 <ul style="list-style-type: none"> <li>您可以对已检测出的恶意程序或疑似恶意程序，执行一键“隔离查杀”。或者将该事件标记为“手动处理”，立即登录系统终止该进程并全面排查系统风险，避免系统遭受进一步破坏。</li> <li>HSS提供恶意程序自动隔离查杀功能，可对目前部分主流勒索病毒、DDOS木马等进行主动防护和主动隔离。建议您启用该功能，加固主机安全防线。</li> </ul> </li> <li>若事后确认该程序是无害程序或者查杀该程序影响了业务，可以“取消隔离查杀”，或者从“文件隔离箱”中还原程序源文件。</li> </ul>
进程异常行为	<p>若检测出进程异常行为，建议您立即对该进程进行确认：</p> <ul style="list-style-type: none"> <li>若该进程属于正常业务，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。</li> <li>若是未知进程或者经确认是恶意程序，建议立即执行进程查杀并隔离程序源文件。 <ul style="list-style-type: none"> <li>您可以对已检测出的恶意程序或疑似恶意程序，执行一键“隔离查杀”。或者将该事件标记为“手动处理”，立即登录系统终止该进程并全面排查系统风险，避免系统遭受进一步破坏。</li> <li>HSS提供恶意程序自动隔离查杀功能，可对目前部分主流勒索病毒、DDOS木马等进行主动防护和主动隔离。建议您启用该功能，加固主机安全防线。</li> </ul> </li> <li>若事后确认该程序是无害程序或者查杀该程序影响了业务，可以“取消隔离查杀”，或者从“文件隔离箱”中还原程序源文件。</li> </ul>
关键文件变更	<p>若检测出关键文件变更，建议您立即对该变更进行确认：</p> <ul style="list-style-type: none"> <li>若合法，您可以“忽略”该告警。</li> <li>若不合法，关键文件被异常的读取、写入、删除等，确认非用户主动行为。建议您将该事件标记为“手动处理”，立即将该文件替换为操作系统的标准版本。并修改账户密码，同时全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>

告警名称	处理建议
网站后门	<p>若检测出网站后门，建议您立即确认该文件是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该告警；或者“加入告警白名单”，该告警将不会再次触发。</li> <li>● 若不合法，建议您将该事件标记为“手动处理”，并对该文件立即执行隔离。</li> </ul>
反弹/异常Shell	<p>若检测出反弹/异常Shell，建议您立即确认该反弹/异常Shell是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该事件。</li> <li>● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统阻断非法连接或者命令执行，并全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>
高危命令执行	<p>若检测出高危命令执行，建议您立即确认该高危命令执行是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。</li> <li>● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统排查该命令所执行的操作，并全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>
自启动检测	<p>若检测出新增自启动项，需要用户自行判断该自启动是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。</li> <li>● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统删除非法自启动项目，并全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>
风险账户	<p>若检测出风险账号，建议您立即确认该账号是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该事件。</li> <li>● 若不合法，请将该事件标记为“手动处理”，建议执行以下操作： <ul style="list-style-type: none"> <li>- 删除可疑账号 删除主机中无用的系统登录账号，如SSH账号。 删除主机中MySQL、FTP使用的无用的账号。</li> <li>- 限制账号权限 通过限制关键配置项，限制非系统管理员的文件访问权限和文件修改权限，防止未授权的访问权限和使用操作。</li> </ul> </li> </ul>
提权操作	<p>若检测出提权操作，建议您立即确认该提权操作是否合法。</p> <ul style="list-style-type: none"> <li>● 若合法，您可以“忽略”该事件。</li> <li>● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统阻止非法创建和修改系统账号或者篡改文件的行为，并全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>



告警名称	处理建议
Rootkit程序	<p>若检测出Rootkit程序安装，建议您立即确认该Rootkit安装是否合法。</p> <ul style="list-style-type: none"> <li>若合法，您可以“忽略”该事件。</li> <li>若不合法，请将该事件标记为“手动处理”，建议您立即登录系统终止该Rootkit安装行为，并全面排查系统风险，避免系统遭受进一步破坏。</li> </ul>

## 8.3 管理文件隔离箱


企业主机安全可对检测到的威胁文件进行隔离处理，被成功隔离的文件会添加到“事件管理”的“文件隔离箱”中，无法对主机造成威胁。被成功隔离的文件一直保留在文件隔离箱中，您也可以根据自己的需要进行一键恢复。

对以下两类告警事件支持线上隔离查杀：

- 恶意程序（云查杀）
- 进程异常行为

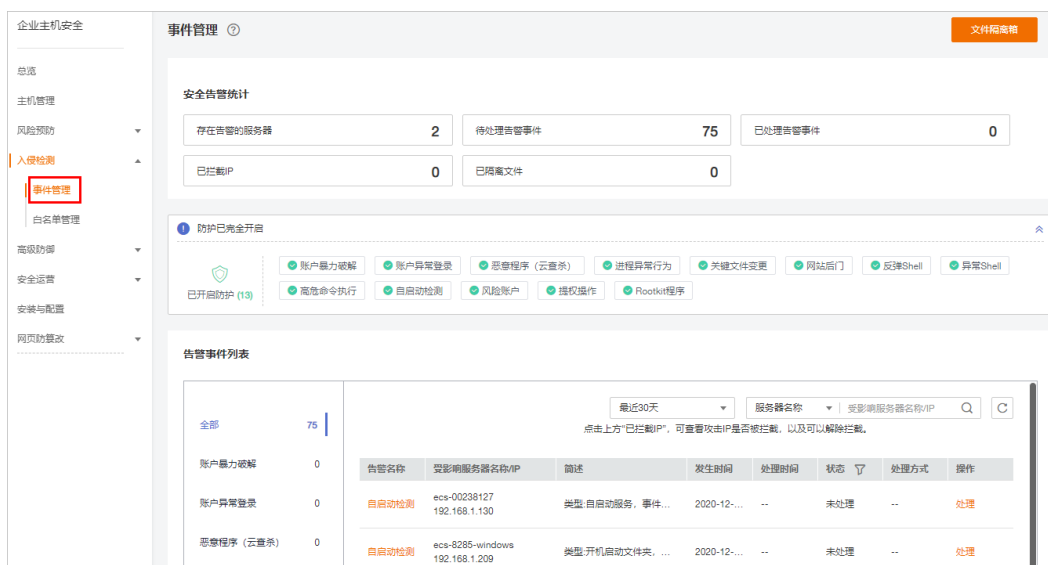
### 选择隔离查杀

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，单击“入侵检测 > 事件管理”，进入事件管理页面。

图 8-6 事件管理



**步骤4** 单击存在威胁的“恶意程序（云查杀）”或者“进程异常行为”，选择“隔离查杀”，以“进程异常行为”告警事件为例，如图8-7所示。

图 8-7 隔离查杀



**步骤5** 单击“确认”，对进程异常行为告警事件进行隔离查杀。被成功隔离的文件会添加到“事件管理”的“文件隔离箱”中，无法对主机造成威胁。

----结束

## 查看文件隔离箱

**步骤1** 在“事件管理”页面，单击“文件隔离箱”，弹出文件隔离箱页面。

**步骤2** 在文件隔离箱列表中，您可以查看被隔离的文件服务器名称、路径和修改时间，如图 8-8所示。

图 8-8 文件隔离箱



----结束

## 一键恢复

**步骤1** 单击文件隔离箱列表中操作列的“恢复”，可以指定被隔离的文件从隔离箱中移除。

**步骤2** 单击“确认”，恢复的文件将重新回到告警事件列表中。

### 说明

执行恢复操作会将隔离文件查杀恢复，请谨慎操作。

----结束

## 8.4 配置告警白名单

白名单管理提供告警白名单的展示与批量导入/导出功能，用户可以通过导入/导出告警白名单避免大量告警误报的发生，提升安全事件告警质量。

告警白名单用于忽略告警，把当前告警事件加入告警白名单后，当再次发生相同的告警时不再进行告警。

在“事件管理”页面处理告警事件时，如果告警为误报，您可以将告警加入告警白名单。告警加入白名单后，后续企业主机安全不会再对该事件进行告警，“总览”页面也不会对该告警事件统计数据。

### 添加告警白名单


表 8-3 添加告警白名单

添加方式	说明
加入告警白名单	<p>处理告警事件时，将告警事件加入到告警白名单，详细信息请参见<a href="#">查看和处理入侵告警事件</a>。</p> <p>以下类型的告警事件加入“告警白名单”：</p> <ul style="list-style-type: none"> <li>● 反弹Shell</li> <li>● Webshell检测</li> <li>● 进程异常行为检测</li> <li>● 进程提权</li> <li>● 文件提权</li> <li>● 高危命令</li> <li>● 恶意程序</li> </ul>
导入告警白名单	在“告警白名单”页面，导入告警白名单列表。

### 查看告警白名单

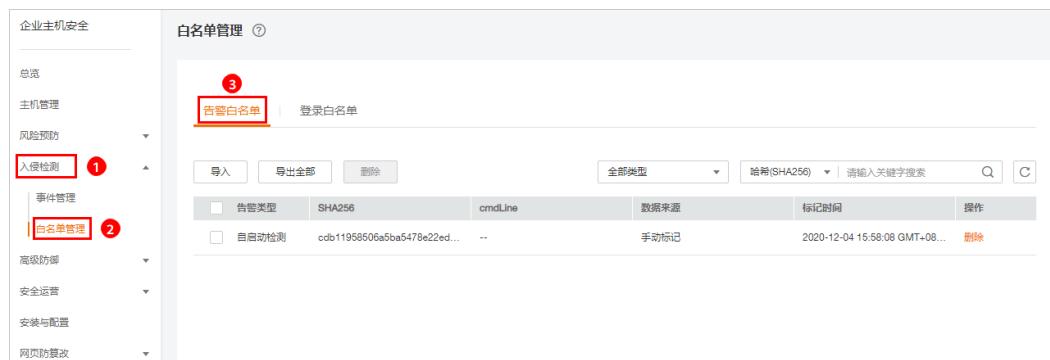
加入告警白名单后，您可以查看已添加的告警白名单，操作步骤如下所示。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“白名单管理”页面，单击“告警白名单”，查看已添加的告警白名单列表，如图8-9所示。

图 8-9 告警白名单列表



----结束

## 导入/导出告警白名单

导入和导出告警白名单功能用来备份和恢复告警白名单。

### 须知

- 导出为“.csv”格式的告警白名单。
- 如果需要手动修改导出的“.csv”表格，请按照格式要求修改（不能使用excel打开修改，否则，会导致导入失败）。


#### 格式要求：

告警类型,SHA256,cmdLine,数据来源,标记时间

```
"webshell","66baecfe7208c00e139b898509626ee4d2ea81382ef15a4283b95d50f669b121","--","文件导入",
"2020/02/28 07:32:44 GMT+08:00"
```

- 告警白名单支持增量导入，相同的记录多次导入不会增加。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“白名单管理”页面，选择“告警白名单”，如图8-10所示。

图 8-10 选择告警白名单



- 单击“全部导出”，将当前告警白名单列表导出，导出为“.csv”格式表格。
- 单击“导入”，选择已导出的告警白名单表，将表中记录的内容重新导入告警白名单。

在弹出的对话框中，单击“上传文件”，选择待上传的文件，导入告警白名单。导入成功后，告警白名单展示在告警白名单列表中。

#### 📖 说明

- 文件格式仅限csv、txt、UTF-8编码。
- 文件大小不超过5MB。
- 文件名格式为：1-64位字符，只能包含字母、数字、下划线、中划线或者点。

----结束

## 相关操作

### 删除告警白名单

若您需要删除已添加的告警白名单，您可以进入告警白名单列表，选择待删除的告警白名单，单击“删除”，删除告警白名单。

#### 📖 说明

删除告警白名单后，若发生再次发生该告警事件，将触发告警，删除操作执行后无法恢复，请谨慎操作。

## 8.5 配置登录白名单

登录白名单用于忽略指定IP登录指定主机发生的“账户暴力破解”的登录告警事件。


在登录白名单页面，您可以添加指定“登录IP”和“登录用户名”登录到指定“服务器IP”的登录白名单。添加登录白名单后，HSS将不会对该登录白名单内的合法登录事件上报登录告警。

您可以通过以下两种方式添加登录白名单：

- 处理告警事件时，将“账户暴力破解”和“账户异常登录”类型的告警事件加入到登录白名单，详细信息请参见[查看和处理入侵告警事件](#)。
- 在“登录白名单”页面，添加登录白名单。

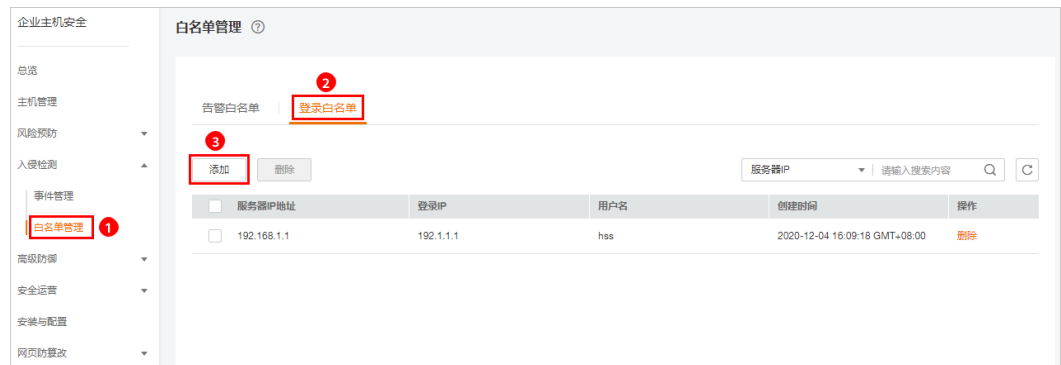
### 添加登录告警白名单

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“白名单管理”页面，选择“登录白名单”，单击“添加”，如[图8-11](#)所示。

图 8-11 登录白名单



**步骤4** 在“添加登录安全白名单”对话框中，输入“服务器IP”、“登录IP”和“登录用户名”，如图8-12所示。

#### 说明

- “服务器IP”和“登录IP”支持IPv4地址。
- “服务器IP”和“登录IP”支持单个IP、IP范围、IP掩码，以英文逗号分隔，例如：192.168.1.1、192.168.2.1-192.168.6.1、192.168.7.0/24。

图 8-12 添加登录安全白名单



**步骤5** 单击“确认”，完成登录白名单的添加。

----结束

## 其他操作

### 删除登录白名单

若需要删除已添加的登录白名单，勾选待删除的登录白名单，单击“删除”，或者在待删除服务器IP地址所在行，单击“删除”，删除登录白名单。

 **说明**

执行删除操作后无法恢复，请谨慎操作。

# 9 高级防御

## 9.1 程序运行认证

### 9.1.1 查看白名单策略列表

企业主机安全支持程序运行认证功能，可有效防止您云主机上有未经过认证或授权的程序运行，为您提供可信的资产运行环境。

#### 背景信息

程序运行认证功能支持将重点防御的主机加入到白名单策略中，通过检测白名单中指定的应用程序区分“可信”、“不可信”和“未知”，防止未经白名单授权的程序运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。


在创建白名单策略之后，您可以通过在需要重点防御的主机中应用该白名单策略，企业主机安全将检测服务器中是否存在可疑或恶意进程，并对不在白名单中的进程进行告警提示或者隔离。

#### 📖 说明

- 非白名单中的应用程序启动时，会触发告警。
- 非白名单内的应用程序启动，可能是新启动的正常程序，或是被入侵后植入的恶意程序。
  - 若提示告警的应用程序为正常程序、常用程序或者您安装的第三方案程序，建议您将该应用程序加入白名单。已加入白名单的应用程序再次启动时，将不再触发告警。
  - 若该进程为恶意程序，建议您及时清理该进程，并查看计划任务等配置文件是否被篡改。

### 查看白名单策略列表

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。





**步骤3** 进入“程序运行认证”页面，选择“白名单策略”页签，查看白名单策略列表，如图9-1所示。

图 9-1 查看白名单策略列表



表 9-1 策略列表说明

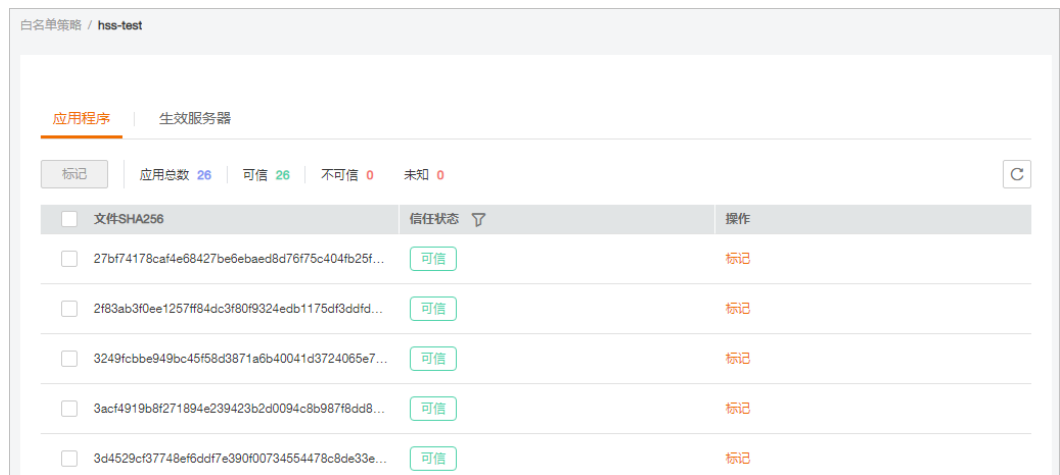
参数	参数说明
策略名称	创建的白名单策略的策略名称。
已生效服务器	应用白名单策略生效的服务器数量。
状态	<p>策略的生效状态。包含以下状态：</p> <ul style="list-style-type: none"> <li>● 学习中 智能学习进行中。 策略创建完成后，自动对学习的服务器执行智能学习。新创建的策略状态都为“学习中”。</li> <li>● 学习完成，策略未生效 该策略已完成智能学习，需确认并启用策略。  智能学习完成后，您还需单击该策略状态下的 ，启用该策略。启用策略后，策略才能生效，HSS会自动识别您服务器中进程的风险类型（可信、不可信和未知）。</li> <li>● 学习完成，策略已生效 该策略已完成智能学习，并且已应用到关联生效服务器中。</li> </ul>
应用数	HSS自动识别学习服务器中应用进程的风险数量，包含“可信”、“不可信”和“未知”应用进程的数量。
策略状态	策略的状态，白名单策略处于“学习完成，策略未生效”，可单击  ，开启白名单策略。开启白名单策略后，策略才生效。

参数	参数说明
操作	<p>可对该策略执行的操作。支持以下操作：</p> <ul style="list-style-type: none"> <li>● 关联生效服务器：单击“关联生效服务器”，打开“关联生效服务器”页面，可增加或删除应用该白名单策略的服务器。</li> <li>● 编辑：单击“编辑”打开编辑策略白名单页面，对该策略进行修改。可修改该策略的“智能学习天数”和执行智能学习的服务器。</li> <li>● 删除：删除白名单策略。 策略删除后，对应的生效服务器的进程将不再受到该白名单策略的保护。</li> </ul>

**步骤4** 单击策略名称，进入白名单策略详情页面，查看关联服务器的“应用程序”，如**图9-2**所示。

您可以查看应用总数、可信应用数、不可信应用数和未知应用数。您可以自行识别并判断应用程序是否可信，并为应用程序标记“可信”、“不可信”或者“未知”，为应用程序创建应用白名单。

**图 9-2** 应用程序列表



**步骤5** 单击“生效服务器”页签，查看应用该白名单策略的生效服务器，如**图9-3**所示。

您可以查看生效服务器的“服务器名称/IP地址”、“白名单策略”、“异常行为数”和“异常处理模式”。

- 异常行为数：异常行为包括非白名单策略中的进程启动行为和白名单内的“不可信”或者“未知”进程的启动行为。
- 异常处理模式：当HSS检测发现异常行为时，触发告警。

图 9-3 查看生效服务器



### 说明

你可以根据需要删除生效服务器，删除生效服务器后，生效服务器的进程将不再受到该白名单策略的保护。

----结束

## 9.1.2 应用白名单策略


白名单策略通过机器学习引擎实现自动化和收集正常的进程行为数据，您可以将重点防御的主机中应用该白名单策略。HSS将检测该主机中是否存在可疑或恶意进程，并对不在白名单策略中的进程进行告警提示或者隔离。

### 前提条件

- 已开启旗舰版防护。
- 添加为智能学习的服务器处于“运行中”、Agent为“在线”状态，且已开启旗舰版防护。
- 一个服务器只能应用一个白名单策略。

### 创建白名单策略

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“程序运行认证”页面，选择“白名单策略”，单击“创建策略”，如图9-4所示。

图 9-4 创建白名单策略



**步骤4** 在创建策略页面中，配置策略“基本信息”，如图9-5所示。

- 策略名称：设置白名单策略的名称。
- 智能学习天数：请根据您的业务的场景选择智能学习的天数，您可以选择“7天”、“15天”或者“30天”。

如果选择的智能学习天数小于实际业务场景操作的天数，会导致智能学习失败。

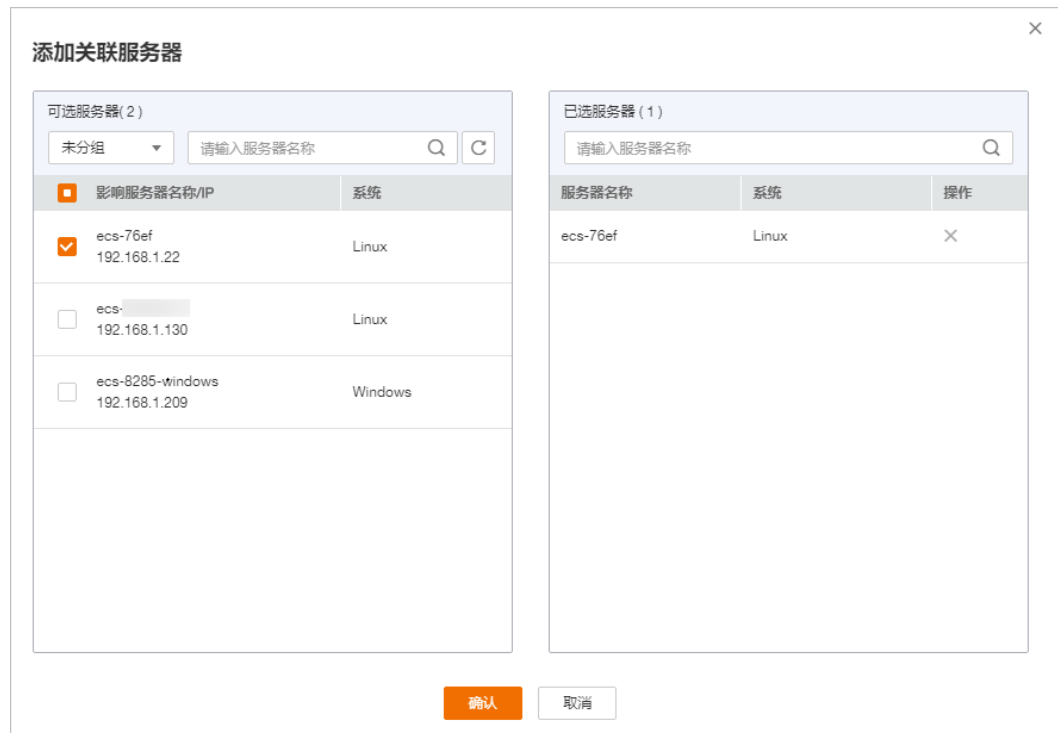
**图 9-5** 配置策略信息

**步骤5** 单击“添加服务器”，添加智能学习服务器，如图9-6所示。

### 须知

- 添加为智能学习的服务器，服务器处于“运行中”、Agent为“在线”状态，且需要开启旗舰版防护。
- 添加学习服务器时，可以添加一个或者多个服务器，HSS将对一个或多个服务器进行自动化聚类 and 收集“可信”、“不可信”和“未知”的应用进程数据。

图 9-6 添加白名单策略学习服务器




**步骤6** 单击“确认”，完成白名单策略学习服务器的添加。

- 在学习服务器列表中，您可以查看学习服务器的“服务名称”、“IP地址”和“系统”。
- 您可以根据需要新增或者删除添加的学习服务器。

**步骤7** 单击“创建并学习”，完成白名单策略的创建。

创建的白名单策略展示在白名单策略列表中，您可以查看策略的“策略名称”、“已生效服务器”、策略学习的“状态”、“应用数”和“策略状态”。

**步骤8** 白名单策略学习完成后，处于“学习完成，策略未生效”。单击 ，开启白名单策略。

开启白名单策略后，白名单策略状态为“学习完成，策略已生效”，说明白名单策略创建成功。

----结束

## 添加生效服务器

白名单策略创建完成后，需要将重点防御的主机添加到白名单策略中，HSS将根据白名单策略检测该主机中是否存在可疑或恶意进程。

白名单策略状态处于“学习完成，策略已生效”，才能成功添加生效服务器。

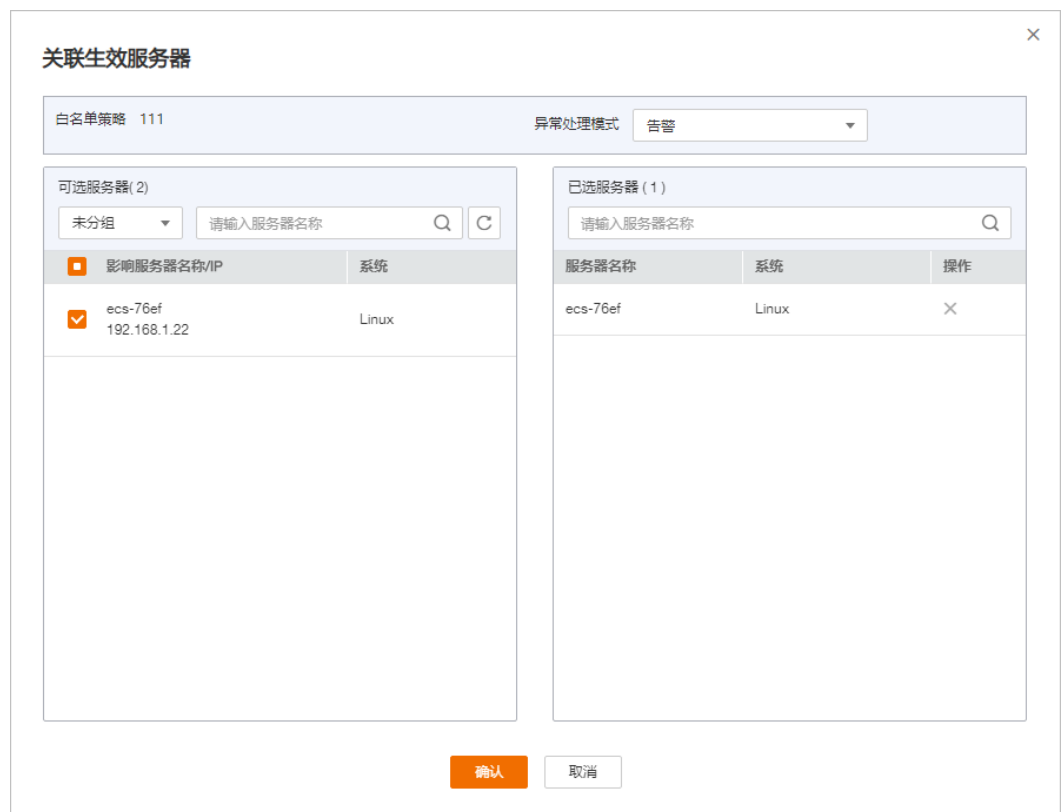
**步骤1** 单击“关联生效服务器”，为白名单策略添加生效服务器，如图9-7所示。

图 9-7 添加关联生效服务器



**步骤2** 在弹出的“关联生效服务器”窗口中，在“异常处理方式”下拉列表中选择“告警”，并在可选服务器列表中，选择生效服务器，如图9-8所示。

图 9-8 配置关联生效服务器



**步骤3** 配置完成后，单击“确认”，完成关联生效服务器的添加。

生效服务器添加完成后，在白名单策略列表中，可以查看该白名单策略已生效服务器的数量。

----结束

## 相关操作

### 管理生效服务器

- 您也可以选择“生效服务器”页签，单击“添加服务器”，为白名单策略添加生效服务器。

您可以查看生效服务器的“服务器名称/IP地址”、“白名单策略”、“异常行为数”和“异常处理模式”。

- 若不需要检测添加的生效服务器，可以在该生效服务器所在行的“操作”列，单击“删除”，删除生效服务器。删除后，该服务器的进程将不再受该白名单策略的保护。

#### 编辑白名单策略

单击“编辑”，打开编辑策略白名单页面，对该策略进行修改。可修改该策略的“智能学习天数”和执行智能学习的服务器。

修改“智能学习天数”或者智能学习的服务器，学习完成前不再受策略保护，请谨慎操作。

#### 删除白名单策略

单击“删除”，删除白名单策略，白名单策略删除后，对应的生效服务器的进程将不再受到该白名单策略的保护。

### 9.1.3 查看和处理程序运行事件

服务器应用白名单策略后，HSS将检测该服务器中进程的风险类型，包括“可信”、“不可信”和“未知”，帮助您有效识别服务器中的风险，并对不在白名单策略中的进程进行告警提示或者隔离。

你可以对进程告警事件进行“可信”、“不可信”和“未知”标记。

若您判断进程为恶意程序，可以手动执行“隔离查杀”。程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若对恶意进程执行误杀，您可以执行取消隔离查杀操作。


事件管理列表展示生效服务器命中白名单策略的“不可信”、“未知”和不在白名单策略中的进程。

#### 📖 说明

建议您对“不可信”、“未知”和不在白名单策略中的进程进行重点排查和处理。

### 查看程序运行事件

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“程序运行认证”页面，选择“事件管理”，如[图9-9](#)所示。

图 9-9 程序运行事件管理页面

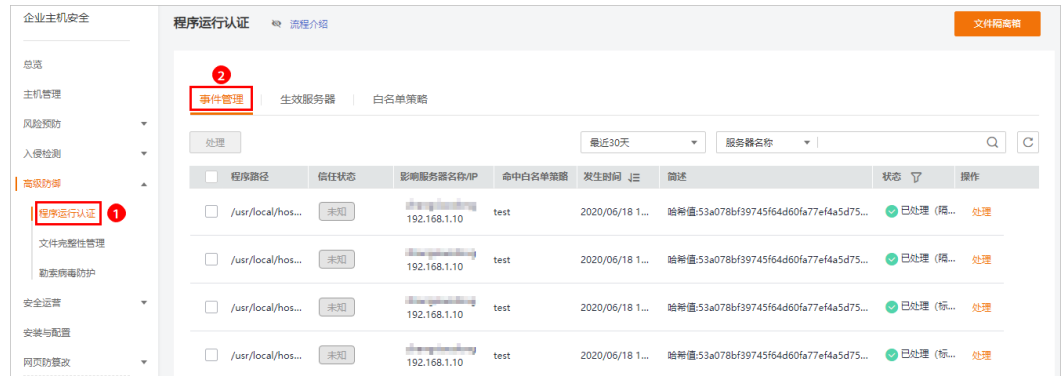


表 9-2 程序运行事件管理

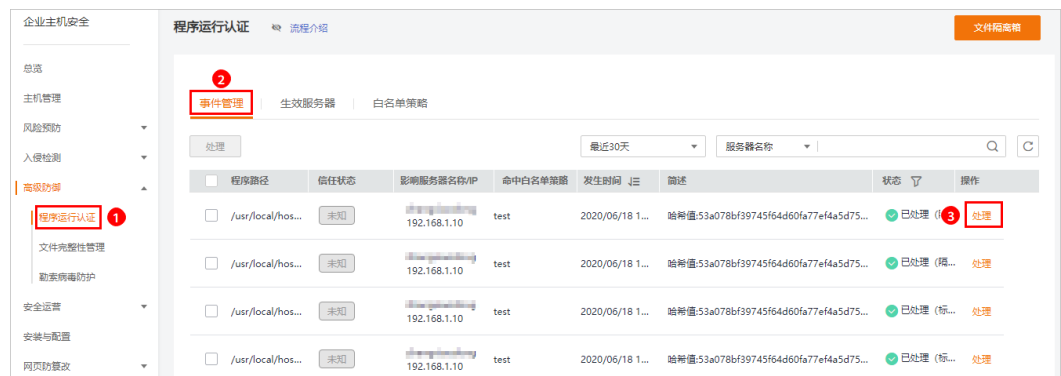
参数	参数说明
程序路径	运行程序的路径。
信任状态	运行程序的可信状态，包括：可信、不可信和未知。
影响服务器名称/IP	影响的服务器的名称和IP地址。
命中白名单策略	告警命中的白名单策略。
发生时间	触发告警的时间。
简述	告警事件的简要描述信息。
状态	程序运行事件的处理状态，包括“已处理”和“未处理”。

----结束

## 处理程序运行事件

**步骤1** 在事件管理列表的操作列中，单击“处理”，处理进程告警事件，如图9-10所示。

图 9-10 处理应用进程告警事件





**步骤2** 在弹出的处理事件窗口中，选择处理方式，处理进程告警事件，如图9-11所示。

**图 9-11** 处理进程告警事件



**表 9-3** 处理告警事件

处理方式	处理方式说明
可信	标记进程为“可信”状态，标记为“可信”的进程，该进程启动后将不会触发告警。
不可信	标记进程为“不可信”状态，标记为“不可信”的进程，该进程启动后将触发告警。
未知	标记进程为“未知”状态，标记为“未知”的进程，该进程启动后将触发告警。
隔离查杀	选择隔离查杀后，该程序无法执行“读/写”操作，同时该程序的进程将被立即终止。HSS将程序或者进程的源文件加入文件隔离箱，被隔离的文件不会对主机造成威胁。 您可以单击“文件隔离箱”，查看已隔离的文件，详细信息请参见 <a href="#">管理文件隔离箱</a> 。 <b>说明</b> 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若对进程进行误杀，您可以对隔离查杀文件执行恢复操作。
取消隔离查杀	若对进程进行误杀，您可以该进程进行取消隔离查杀。 <b>说明</b> 请确认取消隔离查杀的进程不是恶意程序，执行取消隔离查杀后，将对隔离查杀的文件进行恢复，请谨慎操作。

**步骤3** 单击“确定”，完成进程告警事件处理。

----**结束**

## 9.2 文件完整性管理

### 9.2.1 添加管理文件

文件完整性管理可以检查操作系统、应用程序软件和其他组件的文件，确定它们是否发生了可能遭受攻击的更改，同时，能够帮助用户通过PCI-DSS等安全认证。

文件完整性管理功能是使用对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态，利用这种对比来确定文件是否发生了有效或可疑的修改。

文件完整性管理会验证Linux文件的完整性，并管理针对文件执行的活动，包括：

- 文件的创建与删除。
- 文件的修改（文件大小、访问控制列表和内容哈希的更改）。

后续将支持注册表变更统计，敬请期待。


#### 须知

选择需要管理的文件时，需要考虑对系统和应用程序至关重要的文件，选择不会在计划外发生更改的文件。

如果选择应用程序或操作系统经常更改的文件（例如：日志文件和文本文件）会造成很多的干扰，使攻击识别变得非常困难。

### 开启文件完整性管理

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“文件完整性管理”页面，单击 ，开启文件完整性管理，如图9-12所示。

图 9-12 开启文件完整性管理



**步骤4** 开启文件完整性管理后，可查看服务器总的台数、变更统计、变更类别、变更风险、云服务器列表和变更文件列表。

----结束


## 添加管理文件

若需要添加管理文件，请满足以下条件：

- 主机已部署策略。
- 已部署策略的“文件完整性管理”策略开关“已开启”。

添加管理文件的操作步骤，如下所示。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，选择“安全运营”，单击“策略管理”，进入“策略管理”界面。

**步骤4** 在策略管理页面，单击主机应用的策略组的名称，进入策略列表页面，以默认“旗舰版策略组”为例，如**图9-13**所示。

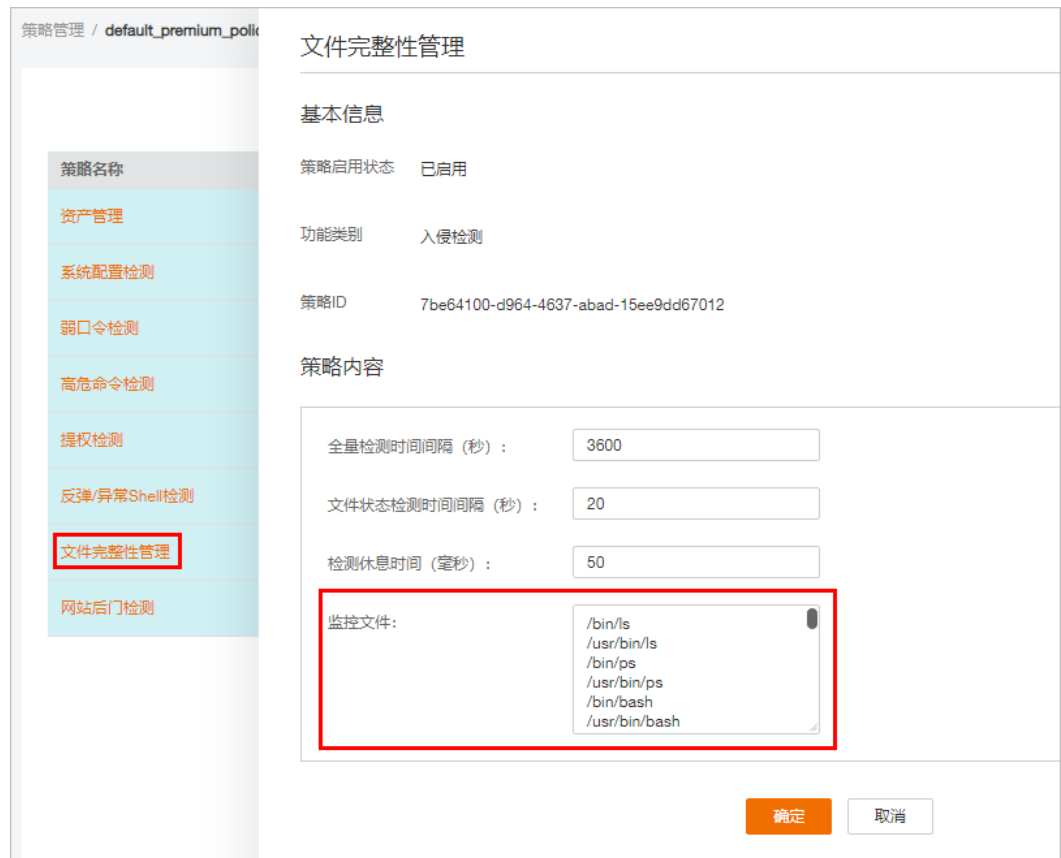
**图 9-13** 默认策略组



**步骤5** 单击“文件完整性管理”，弹出文件完整性管理策略的页面，添加需要管理的文件，如**图9-14**所示。

关于配置“文件完整性管理”策略，详细操作请参见[文件完整性管理](#)。

图 9-14 进入文件完整性管理策略




**步骤6** 添加完成后，单击“确定”，完成管理文件的添加。

----结束

## 相关操作

### 关闭文件完整性管理


若您不需要使用文件完整性管理功能，可单击 ，关闭文件完整性管理。关闭后，企业主机安全将不再管理添加监控的文件，您也无法查看文件完整性管理页面的数据。

## 9.2.2 查看变更统计

文件完整性管理为您提供变更统计、变更类别、单个服务器文件和注册表的变更数量、以及文件和注册表的变更详情。让您实时了解监控文件的变更情况，及时发现恶意变更。

### 查看变更概况

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“文件完整性管理”页面，查看变更概况，如图9-15所示。

**图 9-15** 查看变更概况



**表 9-4** 变更概况

类别	说明
服务器总数 (台)	所有管理的服务器的总台数。
变更统计	<ul style="list-style-type: none"> <li>变更总数(个)：所有管理的变更的总的数量。</li> <li>文件数：所有管理的文件变更的数量。</li> <li>注册表：所有管理的注册表变更的数量。</li> </ul>
变更类别	<ul style="list-style-type: none"> <li>修改：所有管理的文件和注册表修改的数量</li> <li>新增：所有管理的文件和注册表新增的数量。</li> <li>删除：所有管理的文件和注册表删除的数量。</li> </ul>

----结束

## 查看单个云服务器变更文件

**步骤1** 在云服务器列表中，查看服务器对应的文件和注册表变更总数、变更文件、变更注册表和最后变更时间，如图9-16所示。

**图 9-16** 云服务器列表页面



**步骤2** 单击服务器名称，你可以在列表上方查看该服务器的变更统计总数，包括变更总数、变更文件数量、变更注册表数量，如图9-17所示。

### 📖 说明

可以通过单击“高级搜索”，输入“服务器名称”，选择“变更时间”搜索符合条件的服务器。

图 9-17 服务器变更详情

文件	路径	变更内容	变更类型	变更类别	变更时间
ss	/usr/sbin/ss	--	文件	删除	2020-09-07 10:26:35 GMT...
ss	/usr/sbin/ss	--	文件	新增	2020-09-07 10:15:05 GMT...
ss	/usr/sbin/ss	--	文件	删除	2020-09-07 09:37:36 GMT...
ss	/usr/sbin/ss	--	文件	新增	2020-09-03 20:42:06 GMT...

**步骤3** 在该服务器的文件列表中，您可以查看该服务器文件和注册表的变更详情。

包含“文件名称”、“路径”、“变更内容”、“变更类型”、“变更类别”和“变更时间”。

**说明**

- 可以通过在列表上方输入文件名称或者文件路径，搜索符合条件的文件。
- 可以通过单击“高级搜索”，输入“文件名称”、“文件路径”，选择“变更时间”、“变更类型”、“变更类别”或者“信任状态”搜索符合条件的文件。

----结束

## 查看全量变更文件

在变更文件列表中，查看所有主机的变更文件，包含文件变更的文件名称、路径、变更内容、服务器名称、变更类型、变更类别和变更时间，如图9-18所示。

图 9-18 变更文件列表

名称	路径	变更内容	服务器名称	变更类型	变更类别	变更时间
ss	/usr/sbin/ss	--	ecs-hss-002	文件	删除	2020-09-07 10:26:35 ...
ss	/usr/sbin/ss	--	ecs-hss-002	文件	新增	2020-09-07 10:15:05 ...
ss	/usr/sbin/ss	--	ecs-hss-002	文件	删除	2020-09-07 09:37:36 ...
ss	/usr/sbin/ss	--	ecs-hss-002	文件	新增	2020-09-03 20:42:06 ...

**说明**

- 可以通过在列表上方输入文件名称或者文件路径，搜索符合条件的文件。
- 可以通过单击“高级搜索”，输入“文件名称”、“文件路径”，选择“变更时间”、“变更类型”、“变更类别”或者“信任状态”搜索符合条件的文件。

## 9.3 勒索病毒防护

### 9.3.1 查看防护策略列表

企业主机安全支持勒索病毒防护功能，可有效监控您云主机上存储的重要文件，防止未经过认证或授权的进程文件对监控文件的加密或修改操作，保障您的主机不被勒索病毒侵害。

您可以通过创建勒索病毒防护策略，并为策略配置防护状态、监控的文件路径与关联服务器。策略通过机器学习引擎学习服务器上的进程修改文件的行为。策略学习完成后，自动应用于关联服务器。


策略通过对服务器运行状态的自动学习和管理端智能分析，完成可信程序的判定，在防护阶段对非可信程序的操作进行告警。

#### 前提条件

- 仅支持防护Windows操作系统。
- “服务器状态”为“运行中”，已安装HSS的Agent，且“Agent状态”为“在线”。

#### 查看策略管理列表

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“勒索病毒防护”页面，单击“策略管理”，进入勒索病毒防护策略管理列表页面，如图9-19所示。

图 9-19 策略管理列表

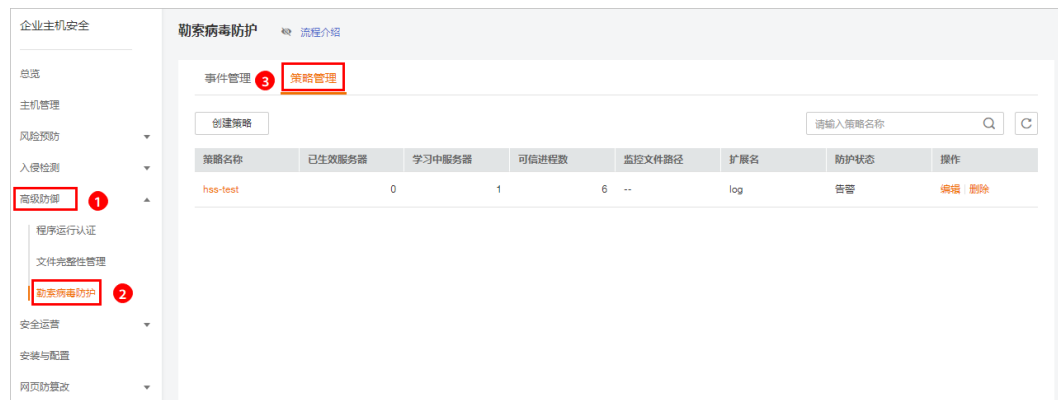


表 9-5 防护策略列表说明

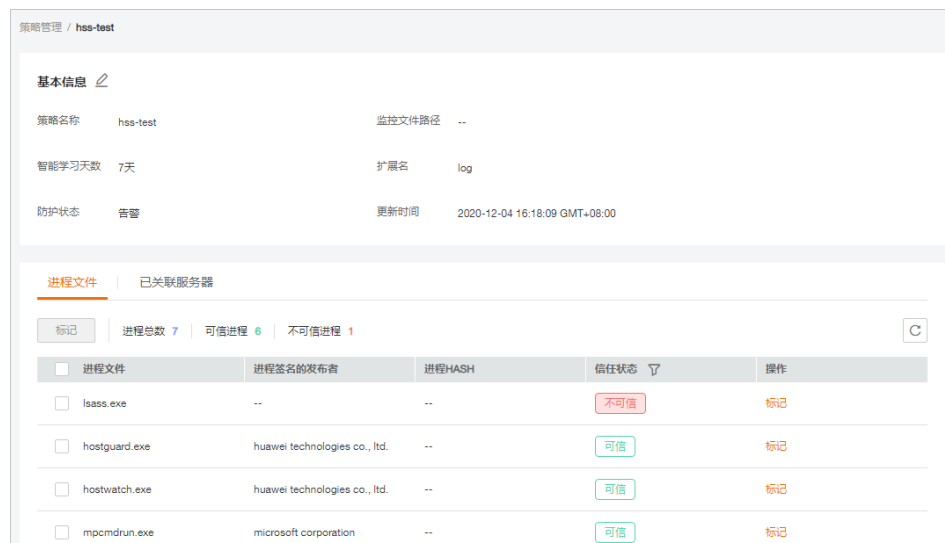
参数	参数说明
策略名称	创建的防护策略的策略名称。
已生效服务器	应用防护策略生效的服务器数量。
学习中服务器	智能学习进行中，自动对关联服务器执行智能学习。新创建的策略状态都为“学习中”。

参数	参数说明
可信进程数	HSS自动识别关联服务器中的可信进程的数量。
监控文件路径	监控的文件的的路径，多个文件以分号分隔。监控填写的路径下的文件操作。 如果不填写监控文件路径，HSS会监控主机上所有的文件路径。
扩展名	检测监控路径下包含文件扩展名的所有文件。
防护状态	检测到进程文件对监控路径文件扩展名的文件的不可信操作，触发进行告警。

**步骤4** 单击策略名称，进入策略详细信息页面，您可以查看策略的“基本信息”和“进程文件”信息，如图9-20所示。

- 您可以查看策略的名称、智能学习天数、防护状态、监控文件路径、扩展名和更新时间。
- 您也可以查看进程文件的“进程总数”、“可信进程”和“不可信进程”，以及“进程文件”、“进程签名的发布者”、“进程HASH”和“信任状态”。
- 您也可以根据进程文件的实际情况为进程文件标记“可信”和“不可信”状态。标记为不可信状态的进程启动时，根据策略防护状态，进行告警。

图 9-20 防护策略详情



**步骤5** 单击“已关联服务器”，查看关联服务器，如图9-21所示。



图 9-21 查看关联服务器



表 9-6 已关联服务器列表

参数	参数说明
服务器名称	服务器的名称。
IP地址	服务器的IP地址。
系统	服务器的操作系统，仅支持防护Windows操作系统。
策略状态	<p>策略的生效状态。包含以下状态：</p> <ul style="list-style-type: none"> <li>● 学习中 智能学习进行中。 策略创建完成后，自动对关联服务器执行智能学习。新创建的策略状态都为“学习中”。</li> <li>● 学习完成，策略已生效 该策略已完成智能学习，并且已应用到关联服务器中。</li> </ul>

参数	参数说明
操作	<p>可对该策略执行的操作。支持以下操作：</p> <ul style="list-style-type: none"> <li>● 重新学习                             <ul style="list-style-type: none"> <li>- 若软件出现重大改版，需要对关联服务器进行重新学习。请单击“重新学习”，重新对关联服务器进行智能学习。</li> <li>- 若设置的智能学习天数不够，不能完成机器的智能学习，或者策略学习的时间已超过设置的“智能学习天数”，仍然处于“学习中”状态。请根据业务场景重新设置“智能学习天数”后，单击“重新学习”，重新对关联服务器进行智能学习。</li> <li>- 若学习过程中，服务器处于“关机”或者“故障”状态、Agent处于“离线”状态、或者服务器关闭旗舰版防护，学习将会已中断，但策略仍然处于“学习中”，单击“重新学习”，无法对Agent下发任务。请检查并恢复以上场景，满足服务器“运行中”、Agent“在线”和开启旗舰版防护后，单击“重新学习”，重新对关联服务器进行学习。</li> </ul> </li> <li>● 删除                             <p>删除关联服务器，关联服务器删除后，关联服务器的文件将不再受到该策略的保护。</p> </li> </ul>

----结束


## 9.3.2 创建防护策略

为了防止您的主机被勒索病毒侵害，请创建防护策略，将重点防御的文件添加到防护策略的监控路径中，并启动机器学习。

机器学习会自动聚类并收集该策略下的所有服务器的正常进程行为数据。该策略下的不可信进程行为和非该策略下的进程行为对监控文件路径下的文件执行文件操作，HSS会根据策略设置的防护状态，触发告警。

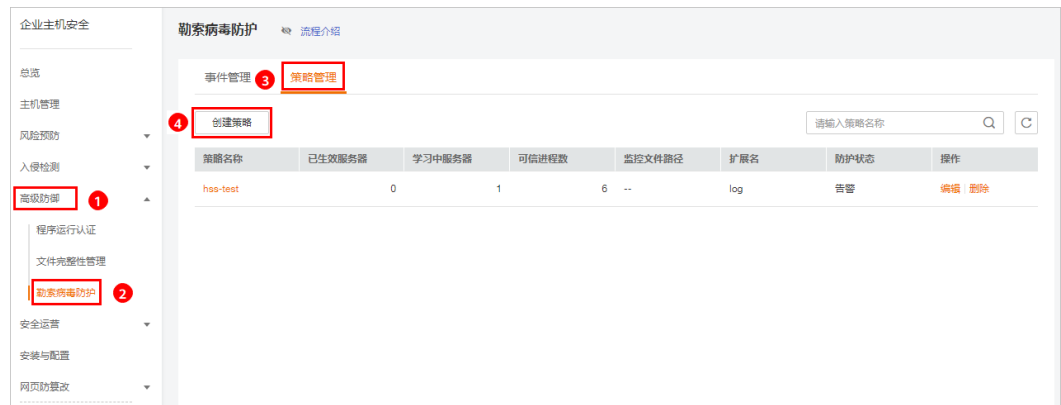
### 创建防护策略

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“勒索病毒防护”页面，单击“创建策略”，创建勒索病毒防护策略。

图 9-22 策略管理页面



步骤4 配置勒索病毒防护策略基本信息，如图9-23所示。

图 9-23 配置勒索病毒防护策略

### 基本信息

**\* 策略名称**

智能学习天数 ?  7天  15天  30天

防护状态

监控文件路径   
多个文件路径请用分号隔开。

**\* 扩展名**   
多个扩展名请用分号隔开。

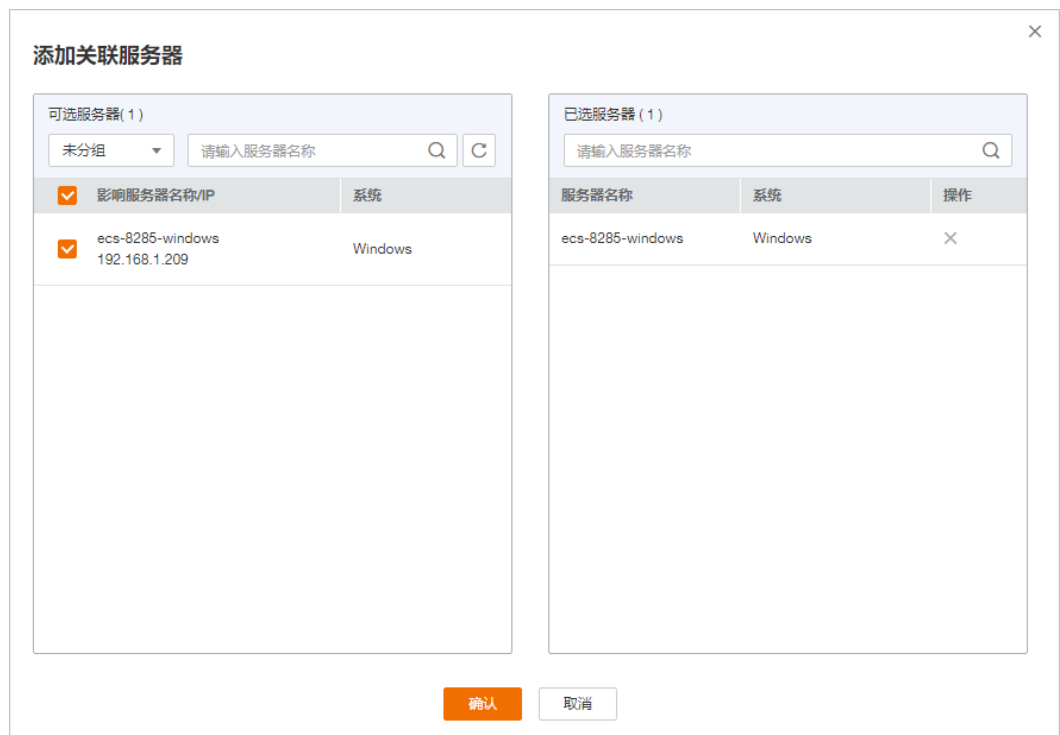
表 9-7 策略基本信息说明

参数	参数说明
策略名称	创建的勒索病毒防护策略的策略名称。
智能学习天数	请根据您的业务的场景选择智能学习的天数，您可以选择“7天”、“15天”或者“30天”。 智能学习功能是通过机器学习引擎学习服务器上的进程修改文件的行为。
防护状态	告警：当检测到对设置的监控路径文件的不可信操作时，触发告警。

参数	参数说明
监控文件路径	监控的文件的的路径，多个文件以分号分隔。监控填写的路径下的文件操作。 如果不填写监控文件路径，HSS会监控主机上所有的文件路径。
扩展名	检测监控路径下包含文件扩展名的所有文件，多个扩展名以分号分隔。

**步骤5** 单击“添加服务器”，在弹出的“添加关联服务器”的窗口中，选择关联服务器，如图9-24所示。

图 9-24 添加关联服务器



**步骤6** 添加完成关联服务器后，单击“确认”，完成关联服务器的添加。

#### 说明

- 您可以查看添加的关联服务器的“服务器名称”、“IP地址”和“系统”。
- 您也可以根据需要在关联服务器的“操作”列，单击“删除”，删除不需要的关联服务器。

**步骤7** 完成关联服务器添加后，单击“创建并学习”，完成勒索病毒防护策略的创建。

勒索病毒防护策略创建完成后，该策略的详情将会自动展示在策略管理列表中，如图9-25所示。

图 9-25 勒索病毒防护策略管理列表

策略名称	已生效服务器	学习中服务器	可信进程数	监控文件路径	扩展名	防护状态	操作
hss-test	0	1	6	--	log	告警	编辑   删除

表 9-8 策略管理列表说明

参数	参数说明
策略名称	创建的智能学习策略的策略名称。
已生效服务器	应用该智能学习策略的服务器数量。
学习中服务器	学习该策略的服务器数量。
可信进程数	智能学习策略生效后，HSS会自动识别您服务器中进程的可信进程，并统计可信进程的数量。
监控文件路径	监控的文件的的路径，多个文件以分号分隔。监控填写的路径下的文件操作。 如果不填写监控文件路径，HSS会监控主机上所有的文件路径。
扩展名	检测监控路径下包含文件扩展名的所有文件，多个扩展名以分号分隔。
防护状态	使用该策略的服务器的防护状态。 告警：当检测到对设置的监控路径文件的不可信操作时，触发告警。

---结束

## 添加关联服务器

若在创建智能学习策略时添加的关联服务器无法满足您的要求，您可以在“已关联服务器”页签下，为该智能学习策略添加或者删除关联服务器。

**步骤1** 单击已创建策略的策略名称，进入详情页面，如图9-26所示。

图 9-26 进入策略详情页面

策略名称	已生效服务器	学习中服务器	可信进程数	监控文件路径	扩展名	防护状态	操作
hss-test	0	1	6	--	log	告警	编辑   删除

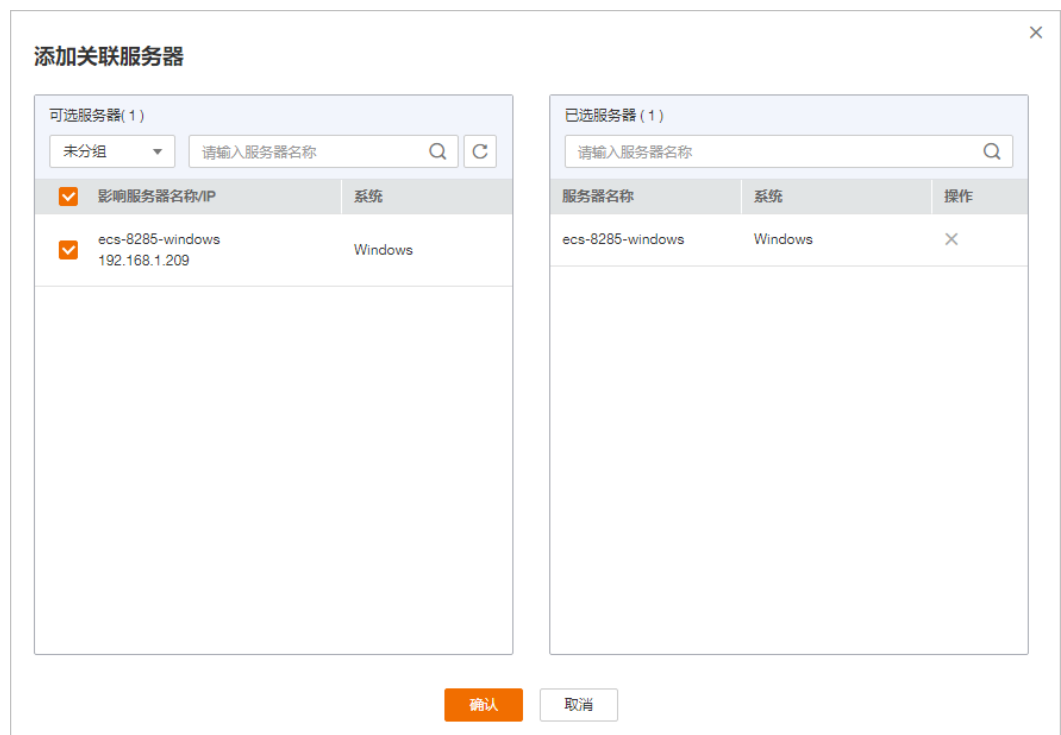
**步骤2** 选择“关联服务器”，单击“添加服务器”，添加关联的服务器，如图9-27所示。

图 9-27 添加关联的服务器



步骤3 在弹出的添加服务器窗口中，选择关联的服务器，如图9-28所示。

图 9-28 添加关联服务器



步骤4 单击“确认”，完成关联服务器添加。

关联服务器添加完成后，您可以查看关联服务器的服务器名称、IP地址、系统和策略状态，策略默认状态处于“学习中”。

学习完成后，策略状态处于“学习完成，策略已生效”。勒索病毒防护策略自动应用于该策略下的所有服务器。

----结束

## 相关操作

### 编辑策略

单击“编辑”打开“编辑策略”页面，对该策略进行修改。可修改该策略的策略名称、智能学习天数、防护状态、监控文件路径和扩展名。

### 删除策略

单击“删除”，删除策略，策略删除后，对应的关联服务器进程将不再受到该策略的保护。

## 9.3.3 查看和处理防护事件

服务器应用勒索病毒防护策略后，HSS将检测该服务器中进程文件对监控路径下文件的操作风险，包括“可信”和“不可信”，帮助您有效识别服务器中的风险操作，并对不在策略中的进程文件对监控路径下的文件操作进行告警提示。


事件管理列表展示关联服务器命中策略的“不可信”和不在勒索病毒防护策略中的进程对监控文件路径下文件的操作。

### 说明

建议您对“不可信”和不在策略中的进程对监控路径下文件的操作进行重点排查和处理。

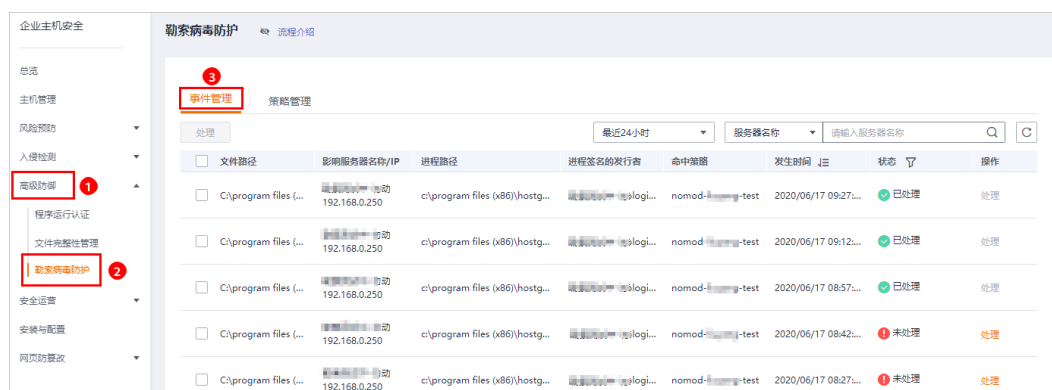
## 查看勒索病毒防护事件列表

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 进入“勒索病毒防护”页面，选择“事件管理”页签，查看勒索病毒防护事件列表，如图9-29所示。

图 9-29 勒索病毒防护列表



文件路径	影响服务器名称/IP	进程路径	进程签名的发行者	命中策略	发生时间	状态	操作
C:\program files (...)	192.168.0.250	c:\program files (x86)\hostg...	...	nomod-...-test	2020/06/17 09:27...	已处理	处理
C:\program files (...)	192.168.0.250	c:\program files (x86)\hostg...	...	nomod-...-test	2020/06/17 09:12...	已处理	处理
C:\program files (...)	192.168.0.250	c:\program files (x86)\hostg...	...	nomod-...-test	2020/06/17 08:57...	已处理	处理
C:\program files (...)	192.168.0.250	c:\program files (x86)\hostg...	...	nomod-...-test	2020/06/17 08:42...	未处理	处理
C:\program files (...)	192.168.0.250	c:\program files (x86)\hostg...	...	nomod-...-test	2020/06/17 08:27...	未处理	处理

表 9-9 勒索病毒防护列表说明

参数	参数说明
文件路径	进程操作的文件的路径。

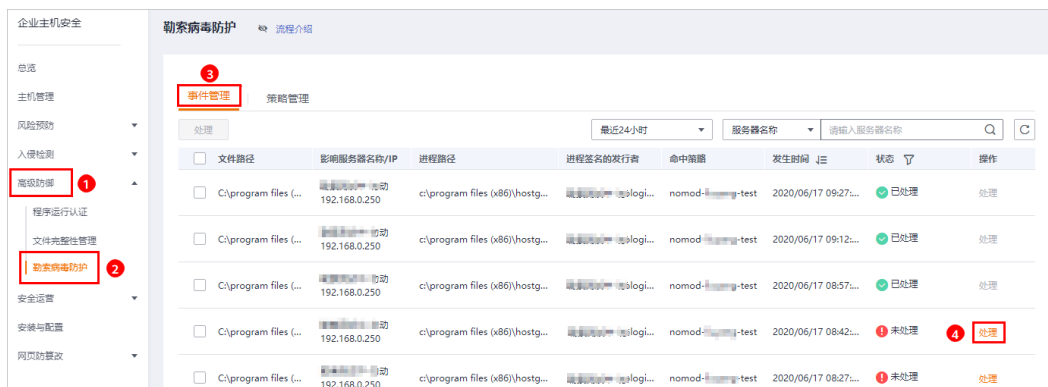
参数	参数说明
影响服务器名称/IP	文件操作的服务器的名称/IP。
进程路径	操作监控路径下文件的进程。
进程签名的发行者	进程签名的发行者。
命中策略	告警命中的勒索病毒防御策略。
发生时间	触发告警的时间。
状态	该操作事件的处理状态，包含“已处理”和“未处理”。

----结束

## 处理勒索病毒防护事件

**步骤1** 在“事件管理”列表的“操作”列中，单击“处理”，处理勒索病毒防护告警事件，如图9-30所示。

图 9-30 处理勒索病毒防护告警事件



**步骤2** 在弹出的处理事件窗口中，选择信任状态“可信”或者“不可信”，处理进程文件操作告警事件，如图9-31所示。

图 9-31 处理勒索病毒防护事件





表 9-10 处理告警事件

处理方式	处理方式说明
可信	标记进程文件为“可信”状态，标记为“可信”的进程文件操作，该进程文件再次对监控路径下的文件进行操作时，将不会触发告警。
不可信	标记进程文件为“不可信”状态，标记为“不可信”的进程文件操作，该进程文件再次对监控路径下的文件进行操作时，将会触发告警。

**步骤3** 单击“确定”，完成勒索病毒防护告警事件处理。

----结束

# 10 安全运营

## 10.1 查看和创建策略组

企业主机安全旗舰版提供灵活的策略管理能力，用户可以根据需要自定义安全检测规则，并可以为不同的主机组或主机应用不同的策略，以满足不同应用场景的主机安全需求。

### 操作须知

- 开启企业版防护时，默认绑定“默认企业版策略组”（包含“弱口令检测”和“网站后门检测”策略），应用于全部的云服务器，不需要单独部署策略
- 开启旗舰版/网页防篡改版防护时，默认绑定了“默认旗舰版策略组”。  
用户也可以通过复制“默认旗舰版策略组”的方式，创建自定义策略组，将“默认旗舰版策略组”替换为用户的自定义策略组，更加灵活的应用于不同的云服务器或者云服务器组。


### 策略列表

策略名称	策略说明	支持的操作系统	企业版	旗舰版	网页防篡改版
弱口令检测	检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改。	Linux, Windows	√ (只支持自定义弱口令)	√	√
网站后门检测	检测云服务器上Web目录中的文件，判断是否为WebShell木马文件。	Linux, Windows	√ (只支持配置检测路径)	√	√

策略名称	策略说明	支持的操作系统	企业版	旗舰版	网页防篡改版
资产管理	检测系统中的软件信息，包含软件名称、软件路径、主要应用等，帮助用户识别异常资产。	Linux, Windows	×	√	√
系统配置检测	对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项。	Linux, Windows	×	√	√
高危命令检测	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	Linux	×	√	√
提权检测	检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： <ul style="list-style-type: none"> <li>● 利用SUID程序漏洞进行root提权。</li> <li>● 利用内核漏洞进行root提权。</li> <li>● 对文件的提权。</li> </ul>	Linux	×	√	√
异常/反弹Shell检测	检测系统中异常/反弹Shell的获取行为，包括对shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。	Linux	×	√	√
文件完整性管理	检测操作系统、应用程序软件和其他组件的文件，确定文件是否发生了可能遭受攻击的更改。	Linux	×	√	√

## 进入策略管理

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，选择“安全运营”，单击“策略管理”，进入“策略管理”界面。

----结束

## 查看策略组列表

**步骤1** 在“策略管理”界面，查看显示的策略组。如图10-1所示，字段说明如表10-1所示。

### 说明


- default\_enterprise\_policy\_group（默认企业版策略组）：企业版系统预置策略，仅可被查看，不可被复制和删除。
- default\_premium\_policy\_group（默认旗舰版策略组）：旗舰版系统预置策略，可通过复制该策略组来创建新的策略组。
- 可在列表右上角单击 ，手动刷新当前列表。
- 可单击关联服务器数的数量，查看策略组关联的服务器。

图 10-1 策略组列表

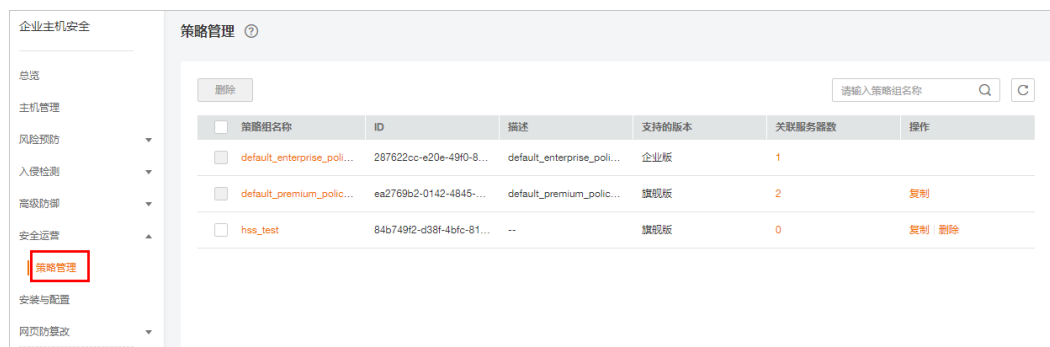


表 10-1 策略组列表字段说明

字段	说明
策略组名称	策略组的名称。
ID	策略组的ID号，对策略组的唯一标识。
描述	对策略组的描述。
支持的版本	策略组支持的企业主机安全的版本。

**步骤2** 单击策略组名称，进入查看策略组详情界面，可以查看该策略组的策略列表，包括策略名称、状态、功能类别和支持的操作系统，如图10-2所示。

### 说明

- “默认企业版策略组”和“默认旗舰版策略组”中的所有策略默认为“已启用”状态。
- 若您不需要执行其中一项策略的检测，您可以在策略所在行的“操作”列，单击“关闭”，关闭该策略项的检测。请根据您的需要“开启”或者“关闭”策略的检测。

图 10-2 策略组详情

策略管理 / default\_premium\_policy\_group

策略名称	状态 <input type="text" value=""/>	功能类别	支持的操作系统	操作
资产管理	已启用	资产管理	Linux, Windows	关闭
系统配置检测	已启用	基线检查	Linux, Windows	关闭
弱口令检测	已启用	基线检查	Linux, Windows	关闭
高危命令检测	已启用	数据采集	Linux	关闭
提权检测	已启用	入侵检测	Linux	关闭
反弹/异常Shell检测	已启用	入侵检测	Linux	关闭
文件完整性管理	已启用	入侵检测	Linux	关闭
网站后门检测	已启用	入侵检测	Linux, Windows	关闭

**步骤3** 单击策略名称，可以查看策略的详情，以弱口令为例，如图10-3所示。

**说明**

若需要修改策略，请参见[修改策略内容](#)。

图 10-3 策略详情



----结束

## 创建策略组

**步骤1** 选择“default\_premium\_policy\_group（默认旗舰版策略组）”策略组，在该策略组所在行的操作列中，单击“复制”，如图10-4所示。

图 10-4 复制策略组



**步骤2** 在弹出的对话框中，输入“策略组名称”和“描述”，如图10-5所示。

### 说明

- 策略组的名称不能重复，如果尝试通过复制来创建一个同名的策略组，将会失败。
- “策略组名称”和“描述”只能包含中文、字母、数字、下划线、中划线、空格，并且首尾不能为空格。

图 10-5 创建策略组



步骤3 单击“确定”，将会创建一个新的策略组。

步骤4 单击已创建的策略组名称，进入策略组的策略页面，如图10-6所示。

图 10-6 策略组策略



策略名称	状态	功能类别	支持的操作系统	操作
资产管理	已启用	资产管理	Linux, Windows	关闭
系统配置检测	已启用	基线检查	Linux, Windows	关闭
弱口令检测	已启用	基线检查	Linux, Windows	关闭
高危命令检测	已启用	数据收集	Linux	关闭
提权检测	已启用	入侵检测	Linux	关闭
反弹/异常Shell检测	已启用	入侵检测	Linux	关闭
文件完整性管理	已启用	入侵检测	Linux	关闭
网站后门检测	已启用	入侵检测	Linux, Windows	关闭

步骤5 单击策略名称，修改具体的策略内容，详细信息请参见[修改策略内容](#)。

步骤6 策略内容修改完成后，单击策略所在行的“开启”或者“关闭”，开启或者关闭对应的策略。

----结束

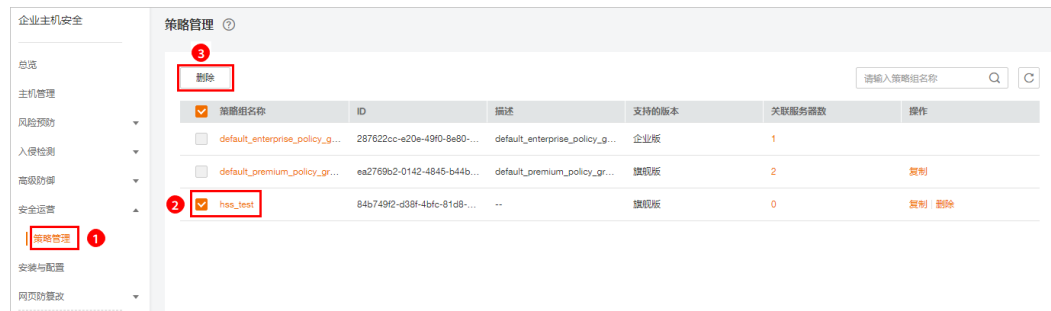
## 相关操作

### 删除策略组

若被删除的策略组已经部署给了主机，在策略组被删除后，这些主机的策略组信息将被设置为“无”。

**步骤1** 选中需要删除的一个或多个策略组，单击“删除”，如图10-7所示。

图 10-7 删除策略组列表



### 说明

用户也可以在需要删除的策略组所在行的“操作”列中，单击“删除”，删除单个策略组。

**步骤2** 在弹出对话框中，单击“确定”，完成策略组的删除。

----结束

## 10.2 修改策略内容


当您创建策略组后，需要修改策略内容时，可按照本文档的指导完成策略内容的修改。

### 须知

策略内容的修改，只在当前所修改的策略组生效。

### 进入策略管理

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏，选择“安全运营”，单击“策略管理”，进入“策略管理”界面。

----结束

### 资产管理

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 单击“资产管理”，弹出资产管理界面。



**步骤3** 在弹出的资产管理界面中，修改“策略内容”，如图10-8所示，参数说明如表10-2所示。

**图 10-8** 资产管理策略

**资产管理**

---

**基本信息**

策略启用状态: 已启用

功能类别: 资产管理

策略ID: c700396e-75fb-494d-9062-fcc524a6380d

**策略内容**

**账号与软件信息管理**

检测时间:

检测日:  周一  周二  周三  周四  周五  周六  周日

需要获取信息的软件名称:   
如果不配置，则获取所有已安装软件信息

软件搜索路径:   
windows主机不用添加

主要应用/组件:	软件名	软件主程序	执行命令	操作
	<input type="text" value="openssl"/>	<input type="text" value="openssl"/>	<input type="text" value="version"/>	删除

添加



**开放端口检测**

获取UDP端口:

检测端口信息的时间间隔 (秒):   
可以打开程序运行认证策略以获得更全面的相关进程数据

**表 10-2** 资产管理策略内容参数说明

参数	说明
检测时间	检测的时间，可具体到每一天的每一分钟。
检测日	检测日期，勾选周一到周日的任意日期。
需要获取信息的软件名称	<ul style="list-style-type: none"> <li>• 软件名称中不能包含空格且内容长度不得超过5000字符，多个软件名称用逗号分隔。</li> <li>• 如果不配置，则获取所有已安装软件信息。</li> </ul>

参数	说明
软件搜索路径	软件搜索的路径。Windows主机不需要添加。
主要应用/组件	<ul style="list-style-type: none"> <li>● 软件名：软件名称。</li> <li>● 软件主程序：软件的主程序。</li> <li>● 执行命令：执行的命令。</li> <li>● 操作：单击“添加”可以将软件添加到此列表；单击“删除”可以将软件从该列表移除。</li> </ul>
获取UDP端口	获取UDP端口信息，检测WEB的目录。 <ul style="list-style-type: none"> <li>● ：开启。</li> <li>● ：关闭。</li> </ul>
检测端口信息的时间间隔（秒）	进程文件检测端口信息的时间间隔，可配置范围为“30秒~86400秒”。

**步骤4** 单击“确定”，完成修改。

---结束

## 系统配置检测

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 在策略组列表中，单击“系统配置检测”，弹出系统配置检测界面。

**步骤3** 在“系统配置检测”界面，修改“修改策略内容”，如[图10-9](#)所示，参数说明如[表10-3](#)所示。

图 10-9 系统配置检测

### 系统配置检测

---

**基本信息**

策略启用状态 已启用

功能类别 基线检查

策略ID 4bf02dc2-a60b-4498-a2f8-7bfd2a3ae932

**策略内容**

检测时间

检测日  周一  周二  周三  周四  周五  周六  周日

启用	操作系统	名称
<input checked="" type="checkbox"/>	Linux	ssh
<input checked="" type="checkbox"/>	Linux	nginx
<input checked="" type="checkbox"/>	Linux	tomcat
<input checked="" type="checkbox"/>	Linux	apache2
<input checked="" type="checkbox"/>	Linux	redis
<input checked="" type="checkbox"/>	Linux	mysql5
<input checked="" type="checkbox"/>	Linux	mongodb
<input checked="" type="checkbox"/>	Linux	centos7
<input checked="" type="checkbox"/>	Linux	vsftp

表 10-3 系统配置检测策略内容参数说明

参数	说明
检测时间	配置系统检测的时间，可具体到每一天的每一分钟。
检测日	系统配置检测日期，勾选周一到周日的检测系统配置的时间。

**步骤4** 勾选需要检测的操作系统。

**步骤5** 单击“确定”，完成修改。

----结束

## 弱口令检测

弱口令/密码不归属于某一类漏洞，但其带来的安全隐患却不亚于任何一类漏洞。数据、程序都储存在系统中，若密码被破解，系统中的数据和程序将毫无安全可言。

企业主机安全服务会对使用经典弱口令的用户账号告警，主动检测出主机中使用经典弱口令的账号。您也可以将疑似被泄露的口令添加在自定义弱口令列表中，防止主机中的账户使用该弱口令，给主机带来危险。

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 在策略组列表中，单击“弱口令检测”，弹出弱口令检测“策略内容”界面。

**步骤3** 在弹出的“策略内容”界面中，修改“策略内容”，如图10-10所示，参数说明如表10-4所示。

图 10-10 弱口令检测

弱口令检测

基本信息

策略启用状态 已启用

功能类别 基线检查

策略ID 7c3d20b3-539c-4f0b-9af0-7e4fd1d7b2aa

策略内容

使用弱口令字典

弱口令字典更新URL

弱口令字典SHA256



检测日  周一  周二  周三  周四  周五  周六  周日

自定义弱口令

mysql弱口令检测:

确定 取消

表 10-4 弱口令检测策略内容参数说明

参数	说明
使用弱口令字典	选择是否开启使用弱口令字典。 <ul style="list-style-type: none"> <li> : 开启。</li> <li> : 关闭。</li> </ul>
弱口令字典更新URL	弱口令字典更新的网页地址。
弱口令字典SHA256	弱口令字典的SHA256值。
检测日	弱口令检测日期。勾选周一到周日检测弱口令的时间。
自定义弱口令	您可以将疑似被泄露的口令添加在自定义弱口令文本框中，防止主机中的账户使用该弱口令，给主机带来危险。
mysql弱口令检测	对登录mysql的口令进行弱口令检测，您可以选择开启或者关闭mysql弱口令检测。

**步骤4** 单击“确定”，完成修改。

----结束

## 高危命令检测

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 单击“高危命令检测”，弹出高危命令检测界面。

**步骤3** 在弹出的高危命令检测界面中，修改“策略内容”，如[图10-11](#)所示，参数说明如[表10-5](#)所示。

图 10-11 高危命令检测内容

策略内容

上报或记录进程消亡消息:

使用消息通道去重上报:

进程统计信息上报间隔(分钟):

独立进程最大cpu使用率(%) :

独立进程最大内存使用(MB) :

独立进程数据接收方IP和端口:

独立进程数据发送限速(KB/S) :

精简日志模式:

收集进程网络连接信息:

记录日志:

日志记录路径:

日志记录最大文件大小(MB) :







高危命令:

白名单(不记录/不上报):

进程全路径或程序名	命令行正则表达式	操作
<span style="color: red;">添加</span>		

表 10-5 高危命令检测策略内容参数说明

参数	说明
上报或记录进程消亡消息	是否开启上报或记录进程消亡消息。 • <input checked="" type="checkbox"/> : 开启。 • <input type="checkbox"/> : 关闭。
使用消息通道去重上报	是否开启使用消息通道去重上报。 • <input checked="" type="checkbox"/> : 开启。 • <input type="checkbox"/> : 关闭。

参数	说明
进程统计信息上报间隔（分钟）	开启消息通道去重上报后有效。 配置进程统计信息上报间隔，配置为有效数字。
独立进程最大CPU使用率（%）	开启消息通道去重上报后有效。 配置独立进程最大CPU使用率，可配置范围为“5~99”。
独立进程最大内存使用（MB）	开启消息通道去重上报后有效。 配置独立进程最大内存使用，可配置范围为“50~1024”。
独立进程数据接收方IP和端口	开启消息通道去重上报后有效。 配置独立进程数据接收方IP和端口。
独立进程数据发送限速（KB/S）	开启消息通道去重上报后有效。 独立进程数据发送限速，可配置范围为“1~100”。
精简日志模式	是否开启使用精简日志模式。 <ul style="list-style-type: none"> <li>● ：开启。</li> <li>● ：关闭。</li> </ul>
收集进程网络连接信息	是否开启收集进程网络连接信息。 <ul style="list-style-type: none"> <li>● ：开启。</li> <li>● ：关闭。</li> </ul>
记录日志	是否开启记录日志。 <ul style="list-style-type: none"> <li>● ：开启。</li> <li>● ：关闭。</li> </ul>
日志记录路径	日志记录的路径。
日志记录最大文件大小（MB）	日志记录最大文件的大小，可配置范围“10~1024”。 <ul style="list-style-type: none"> <li>● 若日志超过配置的最大文件大小，系统会自动将“.log”文件重命名为“.log.0”，并新建“.log”日志文件，将日志继续写入“.log”文件。</li> <li>● 最多存在2个日志文件，若日志再次超过配置的最大文件大小，系统会删除“.log.0”的日志文件，将“.log”日志文件重命名为“.log.0”，并新建“.log”日志文件，将日志继续写入“.log”文件。</li> </ul>
高危命令	设置高危命令，一行一个高危命令。
白名单（不记录/不上报）	<ul style="list-style-type: none"> <li>● 进程全路径或程序名：进程的完整路径或者程序的名称。</li> <li>● 命令行正则表达式：命令行的正则表达式。</li> <li>● 操作：单击“添加”可以将进程或者程序添加到此列表；单击“删除”可以将进程或者程序从该列表移除。</li> </ul>

**步骤4** 单击“确定”，完成修改。

----结束

## 提权检测

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 单击“提权检测”，弹出提权检测界面。

**步骤3** 在弹出的“提权检测”策略内容中，修改“策略内容”，如**图10-12**所示，参数说明如**表10-6**所示。

**图 10-12** 提权检测

提权检测

基本信息

策略启用状态 已启用

功能类别 入侵检测

策略ID 0a589014-e4e0-40b5-99c3-2f8a1ba1712a

策略内容

忽略的进程文件路径：  
/usr/lib64/hal/hald-runner  
/usr/sbin/hald  
/opt/nfast/sbin/privconn  
/usr/sbin/dhclient

检测时间间隔（秒）： 20

确定 取消

**表 10-6** 提权检测策略内容参数说明

参数	说明
忽略的进程文件路径	忽略的进程文件的路径。
检测时间间隔（秒）	进程文件检测时间间隔，可配置范围为“5~3600”。

**步骤4** 单击“确定”，完成修改。

----结束





## 异常/反弹 Shell 检测

- 步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。
- 步骤2** 单击“异常/反弹Shell检测”，弹出异常/反弹Shell检测界面。
- 步骤3** 在弹出的异常/反弹Shell检测界面中，修改“策略内容”，如图10-13所示，参数说明如表10-7所示。

图 10-13 异常/反弹 shell 检测

表 10-7 反弹/异常 shell 检测策略内容参数说明

参数	说明
反弹shell忽略的进程文件路径	反弹shell忽略的进程文件的路径。
反弹shell扫描周期（秒）	反弹shell扫描的周期，可配置范围为“30-86400”。
异常shell检测	选择是否开启异常shell检测，建议开启。 <ul style="list-style-type: none"> <li>：开启。</li> <li>：关闭。</li> </ul>
进程打开文件上限	进程打开文件的上限值，可配置范围为“10-300000”。

**步骤4** 单击“确定”，完成修改。

----结束

## 文件完整性管理

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 单击“文件完整性管理”，弹出关键文件完整性管理界面。

**步骤3** 在弹出的文件完整性管理界面中，修改“策略内容”，如图10-14所示，参数说明如表10-8所示。

图 10-14 文件完整性管理

表 10-8 文件完整性管理策略内容参数说明

参数	说明
全量检测时间间隔 (秒)	检测配置的所有文件的时间间隔，可配置范围为“3600-100000”。 例如：配置为“3600”，就是间隔一个小时检测一次所有文件。
文件状态检测时间间隔 (秒)	文件状态检测周期。可配置范围为“10-600”。

参数	说明
检测休息时间（毫秒）	检测配置的单个文件的时间间隔，可配置范围为“0-1000”。 例如：配置为“50”，检测“/bin/lis”后，等待“50”毫秒再检测“/usr/bin/lis”。
监控文件	需要检测的文件。 <b>说明</b> <ul style="list-style-type: none"> <li>策略默认添加的文件是非常关键的文件，请谨慎删除！</li> <li>若删除默认添加的文件，HSS将不会再对该文件发生的变更进行统计。</li> </ul>

**步骤4** 单击“确定”，完成修改。

----结束

## 网站后门检测

网站后门检测功能只有在设置Web路径之后才会生效。

**步骤1** 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

**步骤2** 单击“网站后门检测”，弹出网站后门检测界面。



**步骤3** 在弹出的网站后门检测界面中，修改“策略内容”，如**图10-15**所示，参数说明如**表10-9**所示。

**图 10-15** 网站后门检测

 说明

为防止Web目录中的软件影响企业主机安全服务Agent的正常运行，请勿将Web目录配置在“/usr/local”的路径下。

**表 10-9** 网站后门检测策略内容参数说明

参数	说明
自动识别Web目录	<p>请根据需要开启或关闭自动识别Web路径，若缺少目录请进行手动添加。</p> <ul style="list-style-type: none"> <li> : 开启。</li> <li> : 关闭。</li> </ul>
手动添加Web目录	<p>手动添加需要检测的Web目录。</p> <ul style="list-style-type: none"> <li>文件路径以“/”开头，不能以“/”结尾。</li> <li>结尾必须有端口号。</li> <li>多个路径通过回车换行分隔且名称中不能包含空格。</li> </ul>
检查文件后缀	<p>检查文件的后缀，可以检测“jsp”、“jspx”、“jspxf”、“php”、“php5”和“php4”。</p>
监测文件修改	<p>是否开启监测文件修改功能。</p>

**步骤4** 单击“确定”，完成修改。

----结束

# 11 网页防篡改

## 11.1 添加防护目录/文件系统

网页防篡改可实时监控网站目录，并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。


网页防篡改可以[保护指定目录](#)，也可以[保护网络文件系统](#)。

### 约束与限制

网页防篡改仅防护“防护目录”下的文件，不防护文件中链接指向的文件。

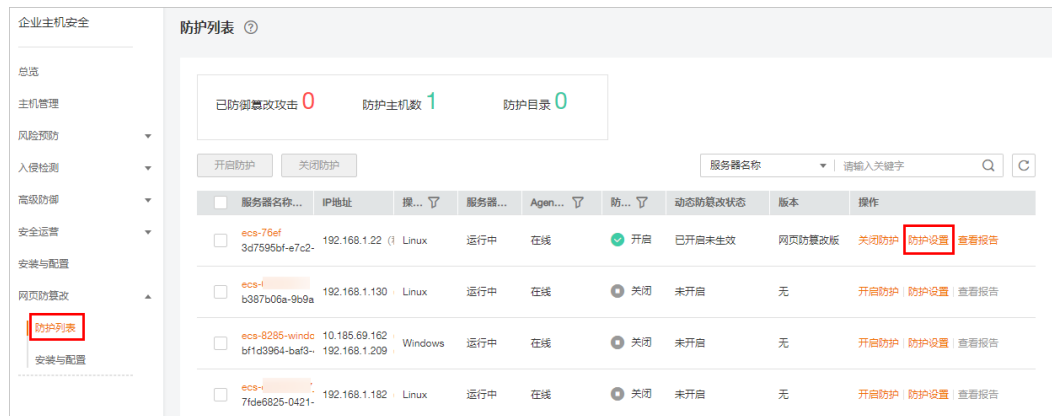
### 保护指定目录

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。

图 11-1 在“网页防篡改”界面



步骤4 “防护模式”选择“保护指定目录”，如图11-2所示。

图 11-2 保护指定目录



步骤5 添加防护目录，您最多可在主机中添加50个防护目录。

1. 单击“添加防护目录”，在弹出的“添加防护目录”对话框中添加防护目录，有关防护规则的详细内容请参见表11-1。

图 11-3 添加防护目录



表 11-1 防护规则

参数	说明	限制
防护目录	防护目录下的文件和文件夹为只读。	请勿对操作系统目录进行防护。

参数	说明	限制
排除子目录	排除防护目录下不需要防护的子目录，例如临时文件目录。 多个子目录请用英文分号隔开。	排除子目录为防护目录中的相对目录。
排除文件类型	排除防护目录下不需要防护的文件类型，例如Log类型的文件。 多个文件类型请用英文分号隔开。  为实时记录主机中的运行情况，请排除防护目录下Log类型的文件，您可以为日志文件添加等级较高的读写权限，防止攻击者恶意查看或篡改日志文件。	-
本地备份路径	开启网页防篡改防护后，防护目录下的文件会自动备份到设置的本地备份路径中。  防护目录下文件大小不同，备份时间也不同，一般约10分钟备份完成。备份完成后，立即生效。 被排除的子目录和文件类型不会备份。  若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。	本地备份路径与添加的防护目录不能重叠。

2. 添加完成后，单击“确定”，完成添加防护目录的操作。

若您需要修改防护目录中的文件，请先暂停对防护目录的防护后再修改文件，以避免误报。文件修改完成后请及时恢复防护功能。

#### 步骤6 启用远端备份。

HSS默认会将防护目录下的文件备份在“添加防护目录”时添加的本地备份路径下（被排除的子目录和文件类型不会备份），为防止备份在本地的文件被攻击者破坏，请您启用远端备份功能。

有关添加远端备份服务器的详细操作，请参见[添加远端备份服务器](#)。

1. 单击“启动远端备份”。

图 11-4 开启远端备份



2. 通过下拉框选择备份服务器。

图 11-5 启动远端备份



3. 单击“确定”，启动远端备份。


----结束

## 保护网络文件系统

### 说明

仅Linux操作系统支持防护网络文件系统。

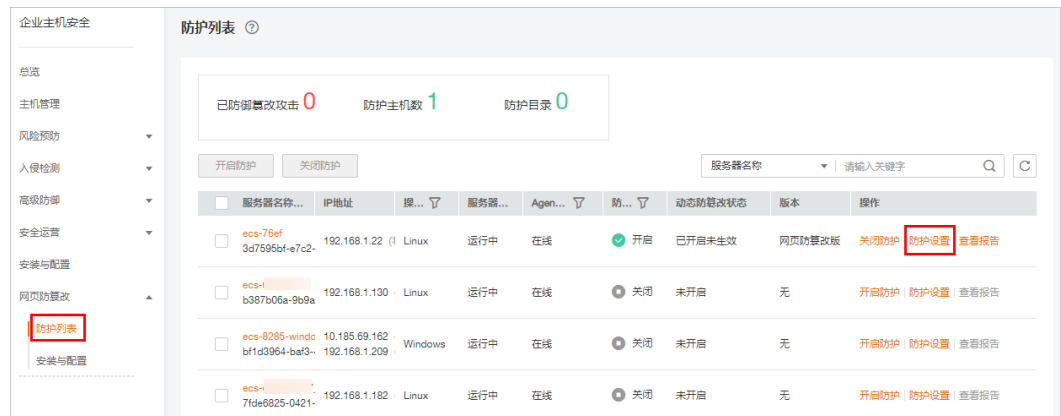
**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。



图 11-6 在“网页防篡改”界面



步骤4 “防护模式”选择“保护网络文件系统”，如图11-7所示。

图 11-7 保护网络文件系统



步骤5 单击“添加文件系统”，在弹出的“添加防护目录”对话框中添加防护目录，有关防护规则的详细内容请参见表11-2。

图 11-8 添加文件系统

✕

## 添加防护目录

**\* 防护目录:**

请输入需要保护的文件系统名称  
提示: 请勿对操作系统盘进行防护

**排除子目录:**

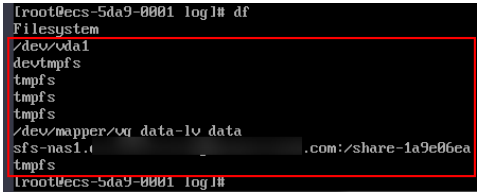
排除子目录为相对路径, 通常为防护目录下的子目录, 多个子目录请用分号隔开。

**排除文件类型:**

多个文件类型请用分号隔开。

确定
取消

表 11-2 防护规则

参数	说明	限制
文件系统	<p>防护文件系统下的文件和文件目录为只读。</p> <p><b>说明</b> 执行df命令, 查看所有文件系统。如下图所示, “Filesystem” 列为文件系统名称。</p> <p><b>图 11-9 文件系统</b></p>  <pre style="font-family: monospace; font-size: small; border: 1px solid black; padding: 5px;"> root@ecs-5da9-0001 log]# df Filesystem /dev/vda1 devtmpfs tmpfs tmpfs tmpfs /dev/mapper/vg_data-lv_data sfs-nas1.0 .com:/share-1a9e06ea tmpfs root@ecs-5da9-0001 log]#                     </pre>	请勿对操作系统盘进行防护。
排除子目录	<p>您可以排除文件系统中不需要防护的子目录, 例如临时文件目录。</p> <p>多个子目录请用英文分号隔开。</p>	该目录为文件系统中的相对目录。
排除文件类型	<p>您可以排除文件系统中不需要防护的文件类型, 例如Log类型的文件。</p> <p>多个文件类型请用英文分号隔开。</p>	-

### 须知

若您需要修改防护目录中的文件，您可以[设置特权进程](#)。特权进程可以访问被防护的目录，请确保特权进程安全可靠。

**步骤6** 添加完成后，单击“确定”，完成添加文件系统的操作。

---结束

## 相关操作

- 暂停防护：暂停“网页防篡改”服务对某一目录的防护，在暂停防护后，请您及时恢复防护，避免该目录下的文档被篡改。
- 编辑防护目录：根据需要修改已添加的防护目录。
- 删除防护目录：为方便管理，您可以删除已无需防护的目录。

### 须知

- 执行暂停防护、编辑或删除防护目录后，防护目录下的文件将不再受“网页防篡改”功能的防护，建议您提前处理防护目录下的文档，再对文档执行暂停防护、编辑或删除的相关操作。
- 执行暂停防护、编辑或删除防护目录后，若您的文档不慎被删除，请在主机本地备份或远端主机的备份路径中查找。

## 11.2 添加远端备份服务器

HSS默认会将防护目录下的文件备份在“添加防护目录”时添加的本地备份路径下（被排除的子目录和文件类型不会备份），为防止备份在本地的文件被攻击者破坏，请您启用远端备份功能。

若本地主机上的文件目录和备份目录失效，用户可通过远端备份服务恢复被篡改的网页。

## 前提条件

设置为远端备份服务器的主机，需要满足以下条件：


“Linux操作系统”的主机、“服务器状态”为“运行中”，已安装HSS的Agent且“Agent状态”为“在线”。

### 须知

- Linux备份服务器与主机间网络可通时即可使用远程备份功能，但为保证备份功能的正常工作，建议您将同一内网中的主机设置为备份服务器。
- 建议尽量选择不容易被攻击的内网服务器作为远端备份服务器。

## 设置远端备份服务器

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“远端备份服务器”页面，单击“添加远端备份服务器”。

图 11-10 远端备份服务器



**步骤4** 在弹出的对话框中，添加远端备份服务器，相关参数说明请参见表11-3。

图 11-11 添加远端备份服务器



表 11-3 添加远端备份服务器参数说明

参数名称	说明
地址	该地址为主机的私网地址。
端口	请确保设置的端口未被安全组、防火墙等拦截，并且未被占用。
备份路径	<p>将需要备份的防护目录下的内容备份在该远端备份服务器的目录下。</p> <ul style="list-style-type: none"> <li>若多个主机的防护目录同时备份在同一远端备份服务器时，备份路径下生成以“Agentid”为目录的文件夹，存放各主机的防护文件，以便用户手动恢复被篡改的网页。 例如：两台主机的防护目录分别为“/hss01”和“hss02”，主机Agentid分别为“f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“f2ddbabc-6cdc-43af-abcd-e4e6f086626f”，设置远端备份路径为“/hss01”。</li> <li>备份后路径为“/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f”。</li> <li>若设置为远端备份服务器的主机开启了“网页防篡改”防护，那么该备份路径与自身的“防护目录”不能重叠，否则会导致远端备份失败。</li> </ul>

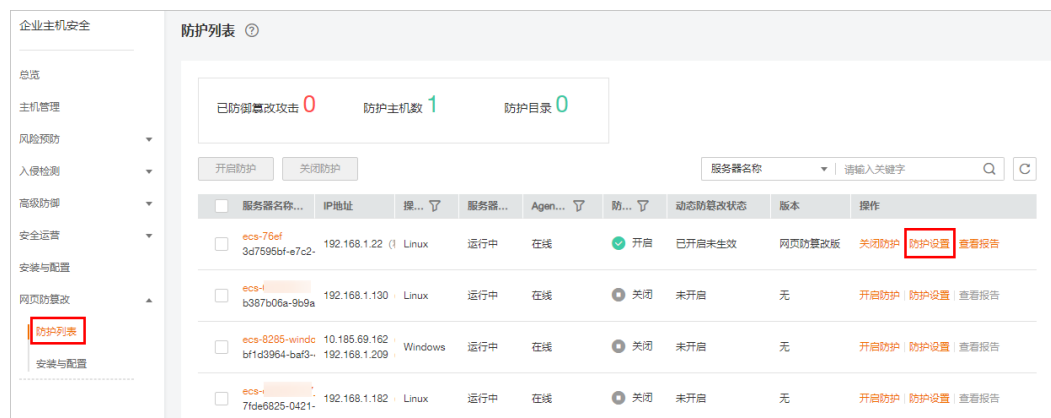
步骤5 单击“确定”，完成添加备份服务器的操作。

----结束

## 启动远端备份

步骤1 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。

图 11-12 在“网页防篡改”界面



步骤2 “防护模式”选择“保护指定目录”，单击“启动远端备份”，如图11-13所示。

图 11-13 开启远端备份



**步骤3** 在“远端备份服务器”下拉框中，选择远端备份服务器。

图 11-14 启动远端备份



**步骤4** 单击“确定”，启动远端备份。

----结束

## 相关操作

### 关闭远端备份

关闭远端备份后，HSS将不再备份您防护目录下的文件；若您本地主机上的文件目录和备份目录被攻击者破坏或者失效，您将无法从远端备份服务器恢复被篡改的网页，请谨慎操作。

## 11.3 添加特权进程修改防护文件

开启网页防篡改防护后，防护目录中的内容是只读状态，如果您需要修改防护目录中的文件或更新网站，可以添加特权进程。

通过这个特权进程去修改防护目录里的文件或者更新网站，修改才会生效。若没有添加特权进程，网页防篡改仅防护原来的文件或者网站，即使修改了内容，文件或者网站也会恢复到原来的状态，修改不会生效。

特权进程可以访问被防护的目录，请确保特权进程安全可靠。


每个主机中最多可以添加10个特权进程的路径。

## 前提条件

- 在“网页防篡改 > 防护列表”页面中“Agent状态”为“在线”、“防护状态”为“开启”。
- 针对Linux系统服务器特权进程，请在“防护目录设置”页签下将“防护模式”设置为“保护网络文件系统”，“特权进程设置”才会生效。

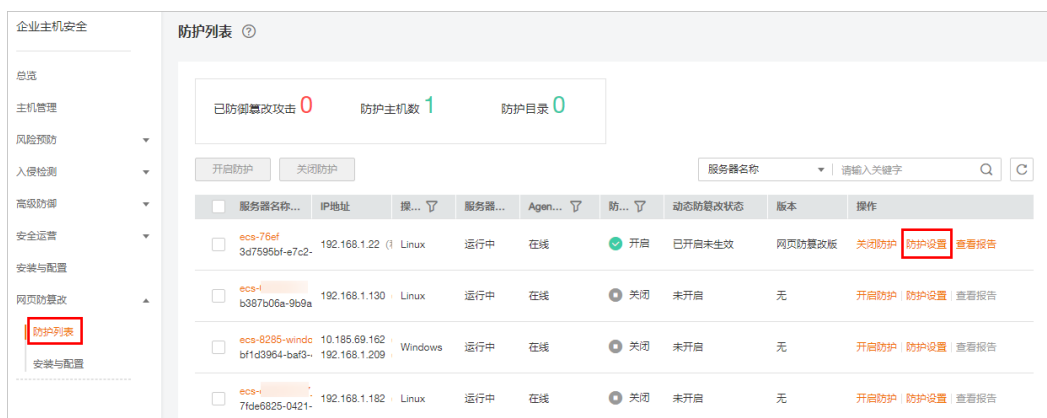
## 添加特权进程

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。

图 11-15 在“网页防篡改”界面



**步骤4** 在“特权进程设置”页面，单击“添加特权进程”。

图 11-16 添加特权进程



**步骤5** 在弹出的“添加特权进程”对话框中，添加特权进程文件所在的路径。

特权进程文件所在的路径需包含进程的名称和格式，如“C:/Path/Software.type”，若进程无格式，请确保进程名称的唯一性。

**步骤6** 特权进程添加完成后，单击“确定”，完成添加特权进程的操作。

---结束

## 相关操作

### 修改或删除已添加的特权进程

在特权进程列表右侧的操作列表中，您可以根据需要修改已添加的特权进程，为方便管理，您也可以删除已无需使用的特权进程。

#### 说明

- 执行编辑或删除操作后，特权进程将不能修改防护目录下的文件，为不影响业务应用的正常运行，请您谨慎处理。
- 无用的进程可能会因为进程自身的漏洞被攻击者利用，请及时删除无需使用的特权进程。

## 11.4 定时开启网页防篡改


网页防篡改提供的定时开关功能，能够定时开启/关闭静态网页防篡改功能，您可以使用此功能定时更新需要发布的网页。

#### 说明

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

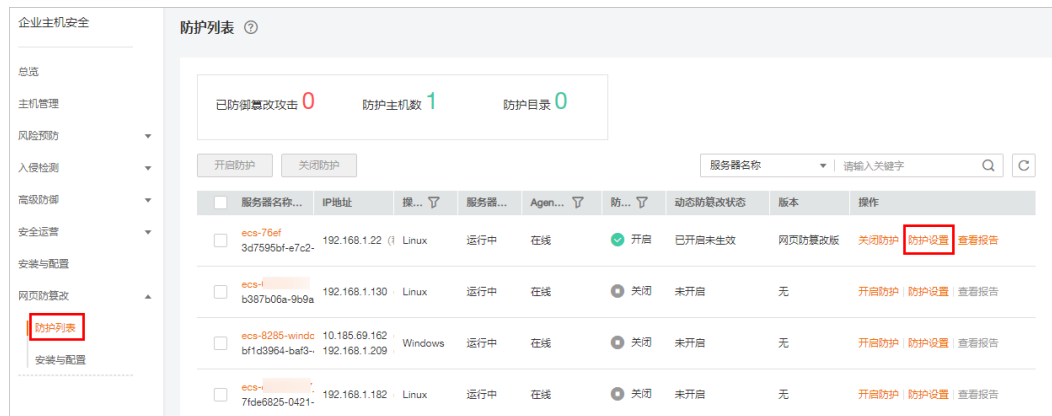
### 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。

图 11-17 在“网页防篡改”界面



**步骤4** 在“定时开关设置”页面，开启定时开关。

图 11-18 定时开关





**步骤5** 在弹出的对话框中，单击“确定”。

**步骤6** 设置“关闭防护时间段”和“定时关闭防护频率”。

图 11-19 设置定时防护参数



----结束

## 关闭防护时段设置规则

- 每个时间段最小关闭时间  $\geq$  5分钟
- 每个时间段最长关闭时间  $<$  24小时
- 时间段之间不允许重叠且两段时间间隔必须  $\geq$  5分钟（时间00:00和23:59特例除外）
- 不允许单个时间段跨天配置
- 时间段以主机时间为准

## 11.5 开启动态网页防篡改


动态网页防篡改提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为，若您在开启防护时未开启动态网页防篡改，您可以在此处开启。

### 前提条件

主机为Linux操作系统。

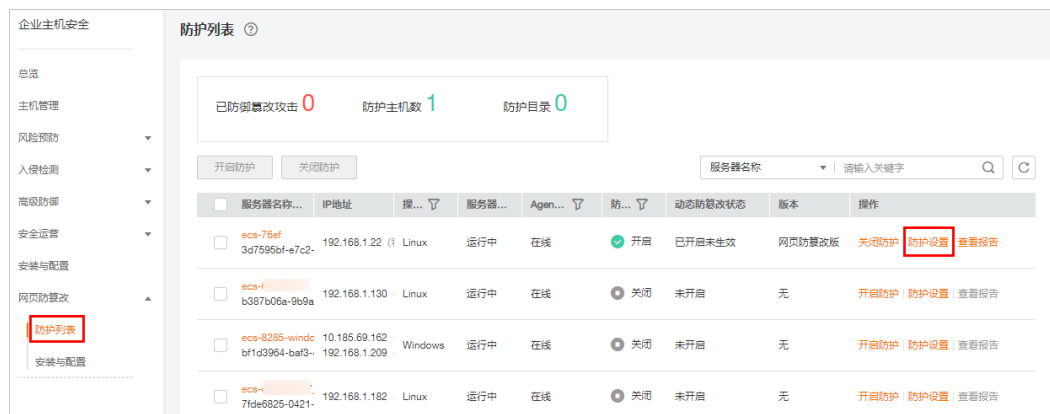
### 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“防护设置”，进入“防护设置”页面。

图 11-20 在“网页防篡改”界面



**步骤4** 在“动态网页防篡改”页面，打开动态网页防篡改开关，即可开启动态网页防篡改功能。

图 11-21 动态网页防篡改



**步骤5** 动态网页防篡改开启后，还需重启Tomcat才能使其生效。

----结束

## 11.6 查看网页防篡改报告


开启网页防篡改防护后，企业主机安全服务将立即对您添加的防护目录执行全面的安全检测。您可以查看主机被非法篡改的详细记录。

### 前提条件

- 已获取管理控制台的登录账号与密码。
- 云服务器的“Agent状态”为“在线”且“防护状态”为“开启”。

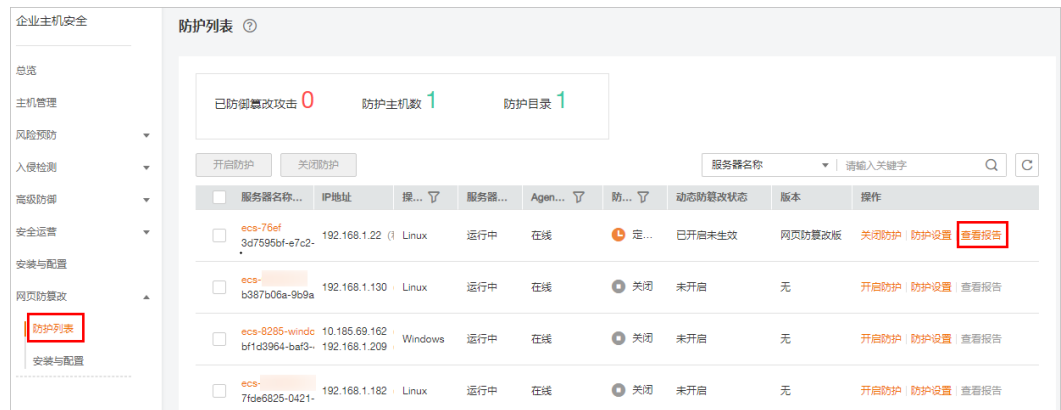
### 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“网页防篡改 > 防护列表”页面，单击“查看报告”。

图 11-22 查看防护记录



步骤4 在防护记录界面，查看防护记录详情。

图 11-23 静态网页防篡改防护记录

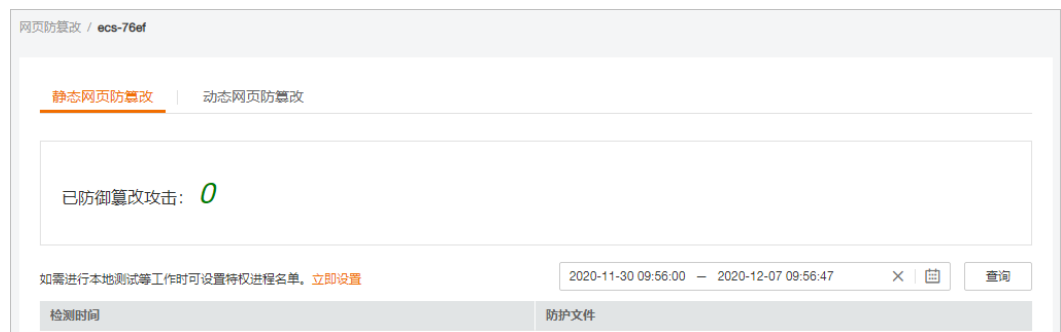


图 11-24 动态网页防篡改防护记录



---结束

# 12 权限管理

## 12.1 HSS 自定义策略

如果系统预置的HSS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见[HSS授权项说明](#)。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

### HSS 自定义策略样例

- 示例1：授权用户查询主机防护列表

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:list"
      ]
    }
  ]
}
```

- 示例2：拒绝用户卸载Agent

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予“HSS Administrator”的系统策略，但不希望用户拥有“HSS Administrator”中定义的卸载Agent的权限（hss:agent:uninstall），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后将“HSS Administrator”和拒绝策略授予用户，根据Deny优先原则用户可以对HSS执行除了卸载Agent的所有操作。以下策略样例表示：拒绝用户卸载Agent。

```
{
  "Version": "1.1",
  "Statement": [
    {

```

```
        "Effect": "Deny",
        "Action": [
            "hss:agent:uninstall"
        ]
    },
]
```

- 多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
      ]
    }
  ]
}
```

## 12.2 HSS 授权项说明

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

### 支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，系统管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。

企业主机安全服务（HSS）支持的自定义策略授权项如下所示：

## 授权列表

权限	授权项	依赖的授权项
查询主机安全防护列表	hss:hosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
云服务器开启或关闭防护	hss:hosts:switchVersion	-
手动检测	hss:hosts:manualDetect	-
手动检测返回检测状态	hss:manualDetectStatus:get	-
查询弱口令检测报告	hss:weakPwds:list	-
查询账户破解防护报告	hss:accountCracks:list	-
账户破解防护解除拦截IP	hss:accountCracks:unblock	-
查询恶意程序检测报告	hss:maliciousPrograms:list	-
查询异地登录检测报告	hss:abnorLogins:list	-
查询关键文件变更报告	hss:keyfiles:list	-
查询开放端口信息列表	hss:ports:list	-
查询漏洞列表	hss:vuls:list	-
批量操作漏洞	hss:vuls:operate	-
查询账号信息列表	hss:accounts:list	-
查询软件信息列表	hss:softwares:list	-
查询Web路径列表	hss:webdirs:list	-
查询进程信息列表	hss:processes:list	-
查询配置检测报告	hss:configDetects:list	-
查询网站后门检测报告	hss:webshells:list	-
查询风险账号检测报告	hss:riskyAccounts:list	-
云服务器风险统计	hss:riskyDashboard:get	-
查询口令复杂度策略检测报告	hss:complexityPolicies:list	-
批量操作恶意程序	hss:maliciousPrograms:operate	-
批量操作开放端口	hss:ports:operate	-
操作配置检测风险	hss:configDetects:operate	-

权限	授权项	依赖的授权项
批量操作网站后门	hss:webshells:operate	-
设置常用登录地	hss:commonLocations:set	-
查询常用登录地	hss:commonLocations:list	-
设置常用登录IP	hss:commonIPs:set	-
查询常用登录IP	hss:commonIPs:list	-
设置登录IP白名单	hss:whitelips:set	-
查询登录IP白名单	hss:whitelips:list	-
设置自定义弱口令	hss:weakPwds:set	-
查询自定义弱口令	hss:weakPwds:get	-
设置Web路径	hss:webDirs:set	-
查询Web路径	hss:webDirs:get	-
查询双因子认证服务器列表	hss:twofactorAuth:list	-
设置双因子认证	hss:twofactorAuth:set	-
开启或关闭恶意程序自动隔离查杀	hss:automaticKillMp:set	-
查询恶意程序自动隔离查杀	hss:automaticKillMp:get	-
查询Agent下载地址	hss:installAgent:get	-
卸载Agent	hss:agent:uninstall	-
查询主机安全告警	hss:alertConfig:get	-
设置主机安全告警	hss:alertConfig:set	-
查询网页防篡改防护列表	hss:wtpHosts:list	vpc:ports:get vpc:publicIps:list ecs:cloudServers:list
开启或关闭网页防篡改	hss:wtpProtect:switch	-
设置备份服务器	hss:wtpBackup:set	-
查询备份服务器	hss:wtpBackup:get	-
设置防护目录	hss:wtpDirectorys:set	-
查询防护目录列表	hss:wtpDirectorys:list	-
查询网页防篡改防护记录	hss:wtpReports:list	-

权限	授权项	依赖的授权项
设置特权进程	hss:wtpPrivilegedProcess:set	-
查询特权进程列表	hss:wtpPrivilegedProcesses:list	-
设置防护模式	hss:wtpProtectMode:set	-
查询防护模式	hss:wtpProtectMode:get	-
设置防护文件系统	hss:wtpFilesystems:set	-
查询防护文件系统列表	hss:wtpFilesystems:list	-
设置定时关闭防护	hss:wtpScheduledProtections:set	-
查询定时关闭防护设置	hss:wtpScheduledProtections:get	-
设置网页防篡改告警	hss:wtpAlertConfig:set	-
查询网页防篡改告警	hss:wtpAlertConfig:get	-
查询网页防篡改统计信息	hss:wtpDashboard:get	-
查询策略组信息	hss:policy:get	-
设置策略组信息	hss:policy:set	-
查询程序运行认证	hss:ars:get	-
设置程序运行认证	hss:ars:set	-
查询入侵检测事件列表	hss:event:get	-
入侵检测事件操作	hss:event:set	-
查询服务器分组信息	hss:hostGroup:get	-
设置服务器组	hss:hostGroup:set	-
文件完整性管理	hss:keyfiles:set	-
查询关键文件变更报告	hss:keyfiles:list	-
查询自启动列表	hss:launch:list	-



# 13 常见问题

## 13.1 产品咨询

### 13.1.1 什么是企业主机安全？

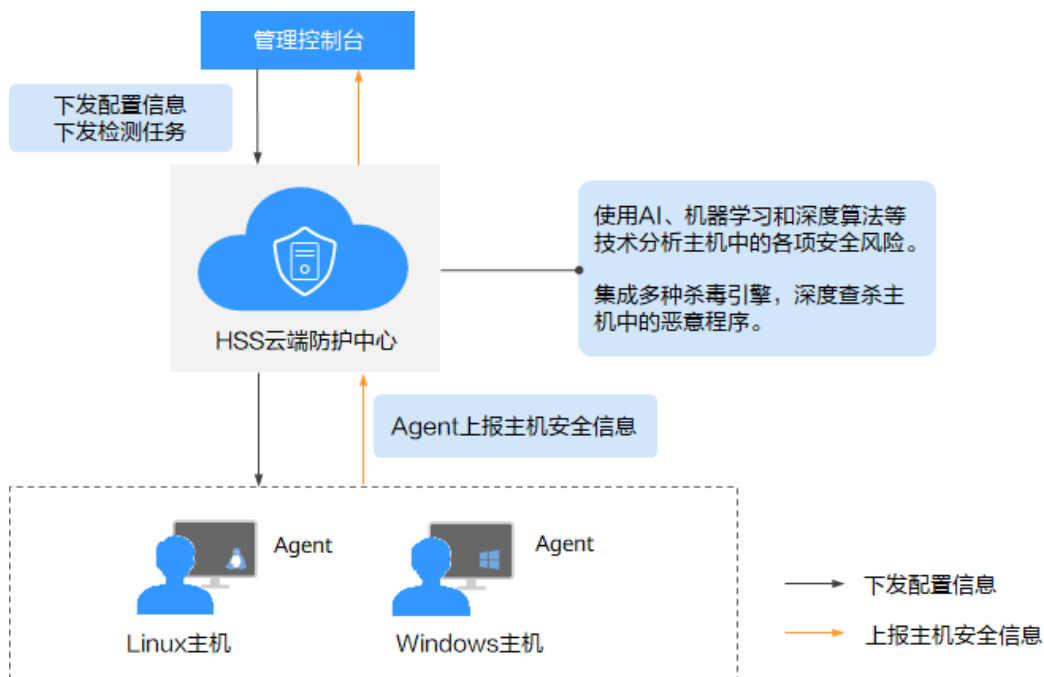
企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

#### 工作原理

在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

企业主机安全服务的工作原理如[图13-1](#)所示。

图 13-1 工作原理



企业主机安全服务的组件功能及工作流程说明如下：

表 13-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	<ul style="list-style-type: none"> <li>使用AI、机器学习和深度算法等技术分析主机中的各项安全风险。</li> <li>集成多种杀毒引擎，深度查杀主机中的恶意程序。</li> <li>接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。</li> <li>接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面。</li> </ul>

组件	说明
Agent	<ul style="list-style-type: none"> <li>Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：443。</li> <li>每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。</li> <li>根据您配置的安全策略，阻止攻击者对主机的攻击行为。</li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。</li> <li>根据操作系统版本选择对应的安装命令/安装包进行安装。</li> <li>网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。</li> </ul>

### 13.1.2 什么是 HSS 的 Agent?

Agent是企业主机安全服务（Host Security Service, HSS）提供的Agent，用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。

#### Agent 的作用

- 每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息上报给云端防护中心。
- 根据您配置的安全策略，阻止攻击者对主机的攻击行为。

#### 说明

- 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。
- 网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

#### Linux Agent 相关进程

Agent进程运行账号：root。

Agent包含以下进程：

表 13-2 Linux Agent 包含以下进程

Agent进程名称	进程功能	进程所在路径
hostguard	该进程用于系统的各项安全检测与防护、Agent进程的守护和监控。	/usr/local/hostguard/bin/hostguard
upgrade	该进程用于Agent版本的升级。	/usr/local/hostguard/bin/upgrade

## Windows Agent 相关进程

Agent进程运行账号：system。

Agent包含以下进程：

表 13-3 Windows Agent 包含以下进程

Agent进程名称	进程功能	进程所在路径
HostGuard.exe	该进程用于系统的各项安全检测与防护。	C:\Program Files (x86)\HostGuard\HostGuard.exe
HostWatch.exe	该进程用于Agent进程的守护和监控。	C:\Program Files (x86)\HostGuard\HostWatch.exe
upgrade.exe	该进程用于Agent升级。	C:\Program Files (x86)\HostGuard\upgrade.exe

## 13.2 开通与配置

### 13.2.1 Agent 是否和其他安全软件有冲突？

Agent可能会和DenyHosts这款软件产生冲突。

- 冲突表现：若登录主机的IP地址被识别为攻击IP，但是无法被“解封”。
- 冲突原因：企业主机安全服务和DenyHosts会同时封禁可能为攻击IP的登录IP地址，企业主机安全服务无法解封DenyHosts中封禁的IP地址。
- 处理方法：建议停止DenyHosts。

1. 以root用户登录ECS。
2. 执行以下命令，检查是否安装了DenyHosts。

```
ps -ef | grep denyhosts.py
```

若界面回显类似以下信息，则说明安装了DenyHosts。

```
[root@hss-test ~]# ps -ef | grep denyhosts.py
root      64498      1   0 17:48 ?        00:00:00 python denyhosts.py --daemon
```

3. 执行以下命令，停止DenyHosts。  
**kill -9 'cat /var/lock/denyhosts'**
4. 执行以下命令，取消DenyHosts的自启动。  
**chkconfig --del denyhosts;**

### 13.2.2 如何安装 Agent？

- Linux客户端，请参见[安装Linux版本Agent](#)。
- Windows客户端，请参见[安装Windows版本Agent](#)。

### 13.2.3 Agent 的默认安装路径是什么？


在Linux/Windows操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装在以下路径中，如表13-4所示。

表 13-4 Agent 的默认安装路径

操作系统	默认安装路径
Linux	/usr/local/hostguard/
Windows	C:\Program Files (x86)\HostGuard

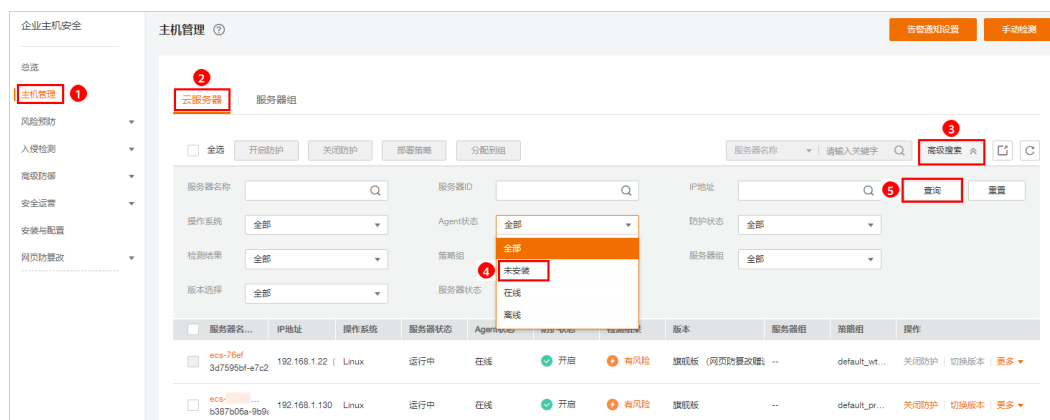
### 13.2.4 如何筛选未安装 Agent 的主机？

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在主机管理页面，筛选未安装Agent的云服务器，如图13-2所示。

图 13-2 筛选未安装 Agent 的主机



Agent状态，如下所示：

- 未安装：未安装Agent，或Agent已安装但未成功启动。
- 在线：Agent运行正常。
- 离线：Agent与HSS服务器通信异常，HSS无法提供安全防护功能。  
单击“离线”，您可以查看Agent不在线的主机列表，并查看“离线原因”。

----结束

### 13.2.5 Agent 状态异常应如何处理？

Agent状态主要分为以下三种，若Agent的运行状态为“未安装”或者“离线”时，表示Agent与服务器间通信异常。

- 未安装：主机从未安装Agent，或Agent已安装但未成功启动。
- 离线：Agent与服务器通信异常，主机中的Agent已被删除，或主机离线。
- 在线：主机内的Agent运行正常。

## 可能的原因

- 网络故障。  
主机中的Agent和云端防护中心出现异常，如网卡故障、IP地址异变及带宽较低
- Agent进程异常。
- 安装Agent后，不会立即生效，需要等待2分钟左右控制台才会刷新。

## 处理方法

### 步骤1 排查网络故障。

待网络恢复正常后：

- 若Agent状态为“在线”，则故障清除。
- 若Agent状态仍为“未安装”或者“离线”，请执行**步骤2**。

### 步骤2 若长时间Agent状态仍为“未安装”或者“离线”，可能是Agent进程异常，需要登录主机，重启Agent进程。

- Windows操作系统  
以管理员**administrator**权限登录主机，完成重启Agent。

图 13-3 重启 Windows Agent



- Linux操作系统  
请以root用户在命令行终端执行以下命令，完成重启Agent。

#### service hostguard restart

若回显以下信息，则表示重启成功。

```
root@HSS-Ubuntu32:~#service hostguard restart
Stopping Hostguard...
Hostguard stopped
Hostguard restarting...
Hostguard is running
```

重启进程后等待约2分钟：

- 若Agent状态为“在线”，则故障清除。
- 若Agent状态仍为“未安装”或者“离线”，请卸载Agent，再重新安装Agent。

---结束

## 13.2.6 如何卸载 Agent?

### 操作场景

- Agent包选择错误，需要卸载Agent后重新安装。
- 安装命令复制错误（如在32位的主机中安装64位的Agent），需要卸载Agent后重新安装。

### 前提条件

- 已获取管理控制台的登录账号与密码。
- 云服务器的“Agent状态”为“在线”。


### 控制台一键卸载 Agent

用户可以通过企业主机安全控制台直接卸载Agent，方便用户操作。

#### 说明

卸载Agent后主机安全服务将无法为该服务器提供任何防护。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航中选择“安装与配置”，进入“安装与配置”界面，单击右上角“卸载Agent”。

**步骤4** 在弹出的“卸载Agent”界面中，如图13-4所示，选择需要卸载Agent的云服务器。

图 13-4 卸载 Agent



步骤5 单击“确定”。

云服务列表“Agent状态”显示为“离线”，卸载Agent成功。

----结束

## 主机本地卸载

用户在不需要使用企业主机安全服务或需要重新安装Agent时，可从本地卸载版本Agent。

### 说明

卸载Agent后主机安全服务将无法为该服务器提供任何防护。

#### ● 卸载Linux版本Agent

- 登录需要卸载企业主机安全服务Agent的云服务器，并执行`su - root`命令切换到root用户。
- 在任意目录执行以下命令，卸载Agent。
  - 针对“.rpm”格式的安装包，执行命令：`rpm -e --nodeps hostguard`
  - 针对“.deb”格式的安装包，执行命令：`dpkg -P hostguard`

若界面回显如下信息，则表示卸载完成。

```
Stopping Hostguard...  
Hostguard stopped  
Hostguard uninstalled.
```

#### ● 卸载Windows版本Agent

- 登录需要卸载主机安全服务Agent的云服务器。
- 在“控制面板 > 程序和功能”中选中“HostGuard”，然后单击“卸载”。



### 说明

- 用户也可以进入安装目录，双击“unins000.exe”，启动卸载程序。
  - 若安装Agent时创建了开始菜单下存放Agent快捷方式的文件夹，用户还可以在“开始 > HostGuard”中选择“卸载HostGuard”进行卸载。
- a. 在“HostGuard卸载”提示框中，单击“是”，开始卸载。
  - b. 卸载完成后单击“确定”。

## 13.3 告警事件处理

### 13.3.1 账户暴力破解问题

#### 13.3.1.1 如何拦截账户暴力破解？

##### 拦截范围

HSS可拦截的攻击类型包括：mysql、mssql、vsftp、filezilla、serv-u、ssh、rdp。

若您的服务器上安装了mysql或者vsftp，开启主机安全防护之后，Agent会在iptables里面新增一些规则，用于mysql/vsftp爆破防护。当检测到爆破行为后会将爆破IP加入到阻断列表里面，新增的规则如图13-5所示。

图 13-5 新增规则

```
root@ub32:~# ss04-mysql@/usr/local/hostguard/ logs iptables -nL
Chain INPUT (policy ACCEPT)
target prot opt source destination
IN_HIDS_MYSQLD_BIP_DROP tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain IN_HIDS_MYSQLD_BIP_DROP (1 references)
target prot opt source destination

Chain IN_HIDS_MYSQLD_DENY_DROP (1 references)
target prot opt source destination
```

#### 须知

不建议删除已添加的iptables规则，若删除iptables规则，HSS将无法防护mysql/vsftp被暴力破解。

### 账户破解拦截原理

暴力破解是一种常见的入侵攻击行为，通过暴力破解或猜解主机密码，从而获得主机的控制权限，会严重危害主机的安全。

通过暴力破解检测算法和全网IP黑名单，若发现暴力破解主机的行为，HSS会对发起攻击的源IP进行拦截，SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。

若被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截。同时HSS支持双因子认证功能，双重认证用户身份，有效阻止攻击者对主机账号的破解行为。

### 说明


使用鲲鹏计算EulerOS（EulerOS with ARM）的主机，在遭受SSH账户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警；SSH登录IP白名单功能也对其不生效。

## 告警策略

- 如果黑客暴力破解密码成功，且成功登录您的服务器，会立即发送实时告警通知用户。
- 如果检测到暴力破解攻击并且评估认为账户存在被破解的风险，会立即发送实时告警通知用户。
- 如果该次暴力破解没有成功，主机上也没有已知风险项（不存在弱口令），评估认为账户没有被破解的风险时，不会发送实时告警。企业主机安全服务会在每天发送一次的每日告警信息中通告当日攻击事件数量。您也可以登录企业主机安全控制台入侵检测页面实时查看拦截信息。

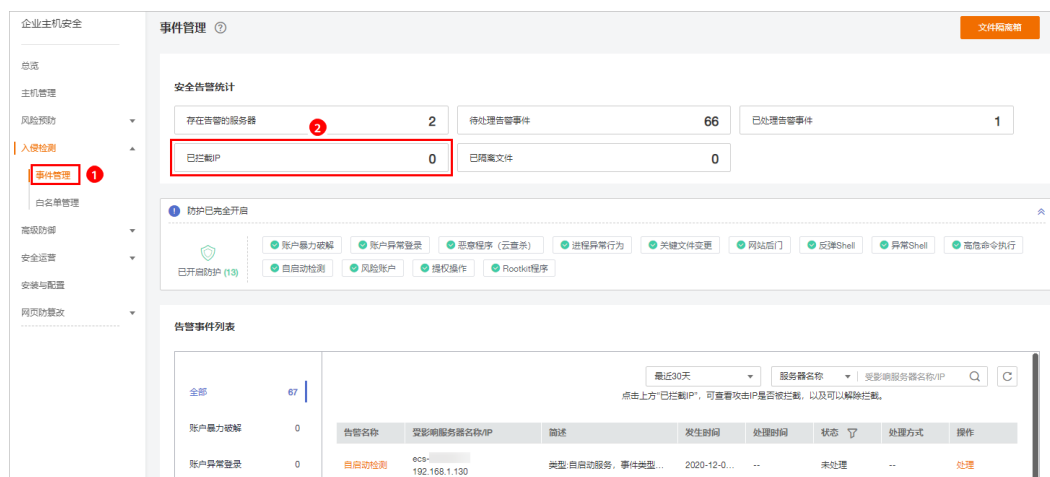
## 查看账户破解检测结果

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“账户暴力破解”页面，查看已防护的服务器上的暴力破解拦截记录，如图13-6所示。

图 13-6 账户破解防护



步骤4 单击“已拦截IP”，可查看已拦截的攻击源IP、攻击类型、拦截次数、开始拦截时间和最近拦截时间，以及拦截状态。

- 已拦截：表示该暴力破解行为已被HSS成功拦截。
- 已解除：表示您已解除对该暴力破解行为的拦截。

### 📖 说明

SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。若被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截。

----结束

## 处理拦截 IP

- 如果发现某个主机被频繁攻击，需要引起重视，建议及时修补漏洞，处理风险项。
- 如果发现有合法IP被误封禁（比如运维人员因为记错密码，多次输错密码导致被封禁），可以手工解除拦截。

### 须知

解除被拦截的IP后，主机将不会再拦截该IP地址对主机执行的操作。

### 13.3.1.2 如何预防账户暴力破解攻击？

#### 账户破解风险

一旦主机账户被破解，入侵者就拥有了对主机的操作权限，主机上的数据将面临被窃取或被篡改的风险，企业的业务会中断，造成重大损失。

#### 如何预防

- 设置安全强度高的口令
- 配置SSH登录白名单  
SSH登录白名单功能是防护账户破解的一个重要方式，配置后，只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。
- 开启双因子认证  
双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次身份认证。  
在“双因子认证”页面，勾选需要开启双因子的主机，单击“开启双因子认证”，开启双因子认证。
- 修改默认端口号  
将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。
- 设置安全组规则，限制攻击源IP访问您的服务端口

### 📖 说明

建议设置对外开放的远程管理端口（如SSH、远程桌面登录），只允许固定的来源IP进行连接。

帐户破解防护可实时检测攻击者对主机中账户的暴力破解攻击，拦截攻击源IP。您可以通过来限制攻击源IP访问您的服务端口。

如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。以仅允许特定IP地址（例如，192.168.20.2）通过SSH协议访问Linux操作系统的弹性云服务器的22端口为例，安全组规则如下所示：

表 13-5 仅允许特性 IP 地址远程连接云服务器

方向	协议应用	端口	源地址
入方向	SSH ( 22 )	22	例如：192.168.20.2/32

### 13.3.1.3 如何解决部分 Linux 系统的账户破解防护功能未生效的问题？

#### 故障原因

主机系统中SSHD服务没有依赖libwrap.so。

#### 说明

libwrap是一个免费的软件程序库，实现了通用的TCP Wrapper功能。任何包含了libwrap.so的daemon程序可以使用/etc/hosts.allow和/etc/hosts.deny文件中的规则对主机进行简单的访问控制。

#### 解决方法

登录云服务器安装企业主机安全Agent，然后执行下面的命令：

```
sh /usr/local/hostguard/conf/config_ssh_xinetd.sh。
```

#### 存在问题的镜像版本

- SUSE的镜像存在该问题的版本如下：
  - SUSE Enterprise 12 SP2 64bit ( 40GB )
  - SUSE Enterprise 12 SP2 64bit for SAP ( 100GB )
  - SAP HANA express edition Server only
  - SAP HANA express edition XS Advanced Application
- Gentoo的镜像存在该问题的版本如下：
  - Gentoo Linux 17.0 64bit ( 40GB )
  - Gentoo Linux 13.0 64bit ( 40GB )
- OpenSUSE的镜像存在该问题的版本如下：
  - OpenSUSE 42.2 64bit ( 40GB )
  - OpenSUSE 13.2 64bit ( 40GB )

## 13.3.2 弱口令和风险账号问题

### 13.3.2.1 出现弱口令告警，怎么办？

若您收到弱口令告警，则说明您的主机存在被入侵的风险。数据、程序都存储在系统中，若密码被破解，系统中的数据和程序将毫无安全可言，请及时修改弱口令。


#### 出现弱口令告警的原因

- 设置的自动生成密码的方式过于简单，与弱口令检测的密码库相重合。

- 将同一密码用于多个子账号，会被系统判定为弱密码。

## 排查弱口令

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 选择“风险预防 > 基线检查”，单击“经典弱口令检测”，查看存在的弱口令。



图 13-7 经典弱口令



**步骤4** 根据经典弱口令列表中的“弹性云服务器名称”、“账号名”、“账号类型”和“弱口令使用时长”，登录待修改弱口令的主机，修改弱口令。

----结束

## 修改常见的服务器弱口令

系统名称	修改登录口令	说明
Windows系统	<p>以Windows 10为例说明。</p> <ol style="list-style-type: none"> <li>1. 登录Windows主机系统。</li> <li>2. 单击左下角的 ，然后单击 ，弹出“Windows设置”窗口。</li> <li>3. 在“Windows设置”窗口中，单击“帐户”。</li> <li>4. 在左侧导航栏中，单击登录选项。</li> <li>5. 在“登录选项”页面，请根据页面提示信息修改服务器密码。</li> </ol>	无

系统名称	修改登录口令	说明
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 <b>passwd [&lt;user&gt;]</b>	<user>为登录用户名。 若不输入登录用户名，则修改的是当前用户的口令。 命令执行完成后，请根据提示输入新的口令。
MySQL数据库	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 <b>SELECT user, host, authentication_string From user;</b> 部分MySQL数据库版本可能不支持以上查询命令。 若执行以上命令没有获取到用户密码信息，请执行命令。 <b>SELECT user, host password From user;</b> 3. 执行以下命令，根据查询结果及弱密码告警信息，修改具体用户的密码。 <b>SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');</b> 4. 执行以下命令，刷新修改的密码信息。 <b>flush privileges;</b>	无
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 <b>requirepass &lt;password&gt;;</b>	password为登录口令。 若已存在登录口令，则将其修改为复杂口令； 若不存在登录口令，则添加为新口令。
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

### 13.3.2.2 如何设置安全的口令？

请按如下建议设置口令：

- 使用复杂度高的密码。  
建议密码复杂度至少满足如下要求：
  - a. 密码长度至少8个字符。
  - b. 包含如下至少三种组合：

- i. 大写字母 (A~Z)
  - ii. 小写字母 (a~z)
  - iii. 数字 (0~9)
  - iv. 特殊字符 ( `~!@#\$%^&\*()-\_+=\|[{]};:"',<>/?和空格 )
- c. 密码不为用户名或用户名的倒序。  
例如：adminstrator/administrator、test/test、oracle/oracle、mysql/mysql等。
- 不使用有一定特征和规律容易被破解的常用弱口令。
    - 生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份
    - 数字或字母连排或混排，常用彩虹表中的密码、滚键盘密码。
    - 短语密码
    - 公司名称、admin、root等常用词汇
  - 不使用空密码或系统的缺省密码。
  - 不要重复使用最近5次（含5次）内已使用的密码。
  - 不同网站/账号使用不同的密码。
  - 根据不同应用设置不同的帐号密码，不建议多个应用使用同一套账户/密码。
  - 定期修改密码，建议至少每90天更改一次密码。
  - 帐号管理人员初次发放或者初始化密码给用户时，如果知道密码内容，建议强制用户首次使用修改密码，若不能强制用户修改密码，则为密码设置过期的期限（用户必须及时修改密码，否则密码应被强制失效）。
  - 建议为所有账户配置设置连续认证失败次数超过5次（不含5次），锁定账号策略和30分钟自动解除锁定策略。
  - 建议对所有账户设置不活动时间超过10分钟自动退出或锁定策略。
  - 新建系统中的帐号缺省密码在首次使用前，建议强制用户更改。
  - 建议开启账户登录记录日志功能，登录日志最少保存180天，登录日志中不能保存用户的密码。

### 13.3.3 配置风险问题

#### 13.3.3.1 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略？

##### 安装 PAM

如果当前系统中未安装PAM（Pluggable Authentication Modules），就无法为系统提供口令复杂度策略检测功能。

若云服务器的操作系统为Debian或Ubuntu，请以系统管理员用户在命令行终端执行命令**apt-get install libpam-cracklib**进行安装。

##### 说明

CentOS、Fedora、EulerOS系统默认安装了PAM并默认启动。

## 设置口令复杂度策略

为了确保系统的安全性，建议设置的口令复杂度策略为：口令最小长度不小于8，至少包含大写字母、小写字母、数字和特殊字符中的三种。

### 说明

以下配置为基础的安全要求，如需其他更多的安全配置，请执行以下命令获取Linux帮助信息。

- 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统  
`man pam_pwquality`
- 其他Linux系统  
`man pam_cracklib`
- CentOS、Fedora、EulerOS操作系统
  - a. 执行以下命令，编辑文件“/etc/pam.d/system-auth”。  
`vi /etc/pam.d/system-auth`
  - b. 找到文件中的以下内容。
    - 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统：  
password requisite pam\_pwquality.so try\_first\_pass retry=3 type=
    - 其他CentOS、Fedora、EulerOS系统：  
password requisite pam\_cracklib.so try\_first\_pass retry=3 type=
  - c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表13-6所示。

示例：

```
password requisite pam_cracklib.so try_first_pass retry=3 minlen=9
dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=
```

### 说明

“dcredit”、“ucredit”、“lcredit”、“ocredit”中至少有三个需要配置为负数。

表 13-6 参数说明

参数	说明	示例
minlen	口令最小长度配置项。 PAM默认使用了“credits”，因此最小口令长度需要加1，若需要设置最小口令长度为8，则minlen的值应该设置为9。	minlen=9
dcredit	口令数字要求的配置项。 值为负数N时表示至少有N个数字，值为正数时对数字个数没有限制。	dcredit=-1



参数	说明	示例
ucredit	口令大写字母要求的配置项。 值为负数N时表示至少有N个大写字母，值为正数时对大写字母个数没有限制。	ucredit=-1
lcredit	口令小写字母要求的配置项。 值为负数N时表示至少有N个小写字母，值为正数时对小写字母个数没有限制。	lcredit=-1
ocredit	特殊字符要求的配置项。 值为负数N时表示至少有N个特殊字符，值为正数时对特殊字符个数没有限制。	ocredit=-1

- Debian、Ubuntu操作系统
  - a. 执行以下命令，编辑文件“/etc/pam.d/common-password”。  
**vi /etc/pam.d/common-password**
  - b. 找到文件中的以下内容：  
password requisite pam\_cracklib.so retry=3 minlen=8 difok=3
  - c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表13-6所示。  
示例：  
password requisite pam\_cracklib.so retry=3 minlen=9 dcredit=-1  
ucredit=-1 lcredit=-1 ocredit=-1 difok=3

### 13.3.3.2 如何在 Windows 主机上设置口令复杂度策略？

为了确保系统的安全性，建议设置的口令复杂度策略为：口令最小长度不小于8位，至少包含大写字母、小写字母、数字和特殊字符中的三种。

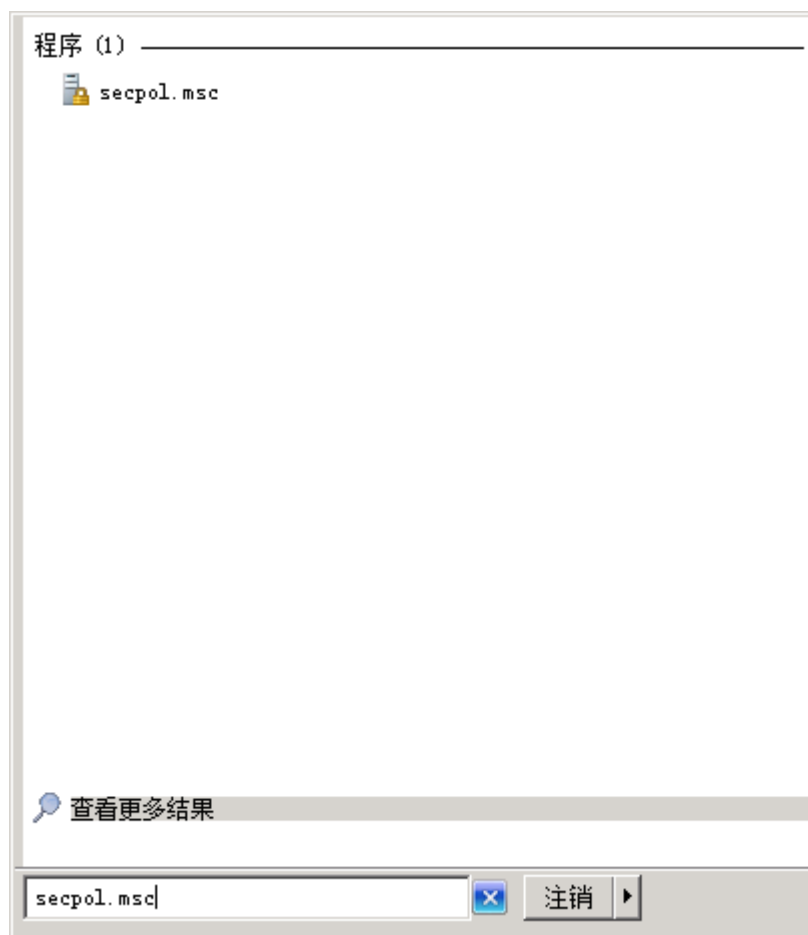
设置本地安全策略中的账户策略步骤如下：

- 步骤1** 以管理员账户Administrator登录。单击“开始 > 控制面板 > 系统和安全 > 管理工具”，进入管理工具文件夹，双击“本地安全策略”，打开“本地安全策略”控制面板。

#### 说明

也可直接在开始菜单栏输入命令secpol.msc直接进入本地安全策略控制面板，如图13-8所示。

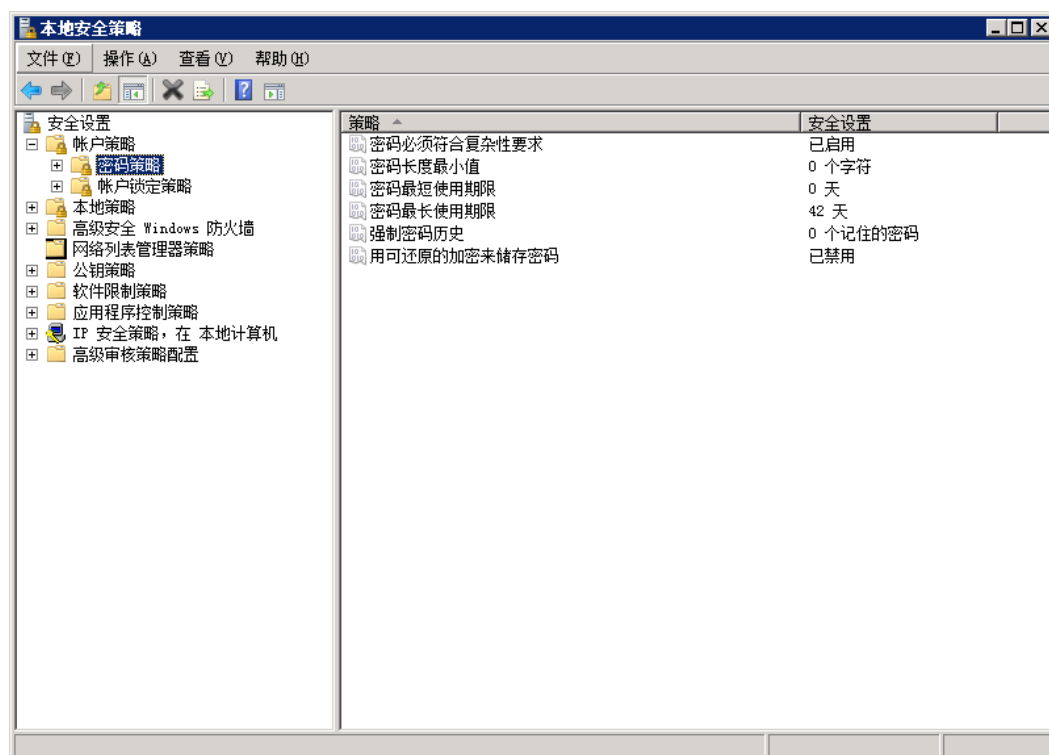
图 13-8 输入命令



**步骤2** 选择“账户策略 > 密码策略”后执行以下操作，如图13-9所示。

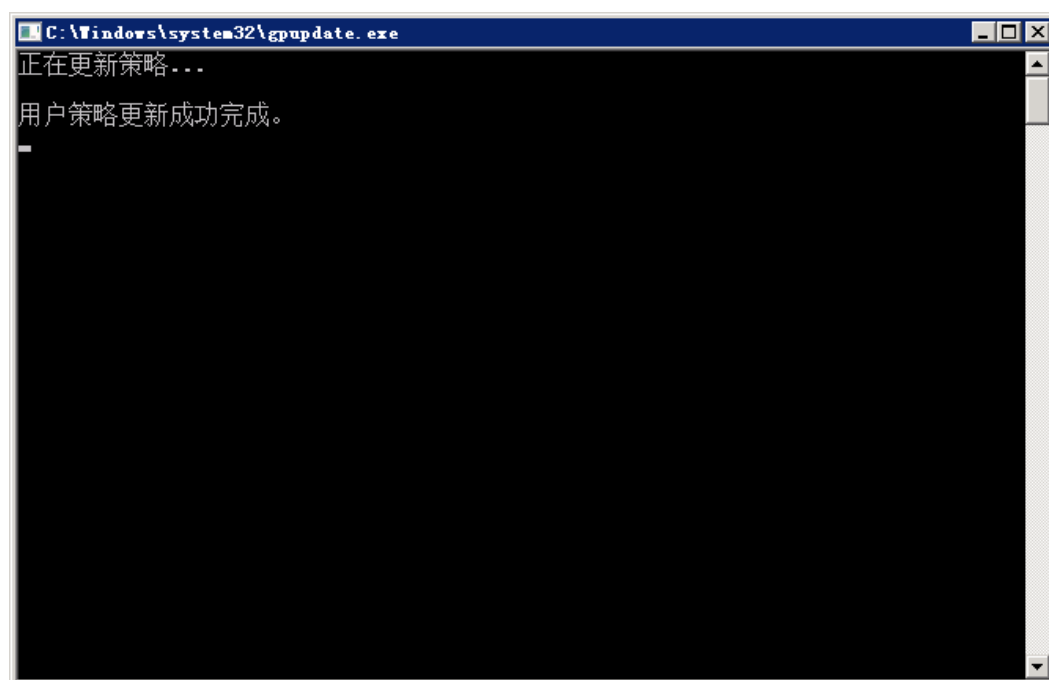
- 双击“密码必须符合复杂性要求”，勾选“已启用”选项，单击“确定”，启用“密码必须符合复杂性要求”策略。
- 双击“密码长度最小值”，填入长度（建议大于等于8），单击“确定”，设置“密码长度最小值”策略。

图 13-9 本地安全策略配置项



**步骤3** 运行gpupdate命令刷新策略，刷新成功后，如图13-10所示，以上设置被应用与系统中。

图 13-10 执行结果



----结束

## 13.4 漏洞管理

### 13.4.1 如何处理漏洞？

#### 处理方法和步骤

**步骤1** 查看漏洞检测结果。

**步骤2** 按照漏洞检测结果给出的漏洞修复紧急度和解决方案逐个进行修复漏洞。

- windows系统漏洞修复完成后需要重启。
- Linux系统Kernel类的漏洞修复完成后需要重启。

**步骤3** 企业主机安全服务每日凌晨将全面检测Linux主机和Windows主机，以及主机Web-CMS的漏洞，漏洞修复完成后建议立即执行一次检测，核实修复结果，请参见[手动执行软件漏洞检测](#)。

---结束

### 13.4.2 按照提示修补了漏洞为什么警告还在？

#### 解决方法

- 漏洞修复完成后，建议您查看软件升级结果，确保软件已升级为最新版本。
- 漏洞修复后，建议立即执行一次检测，核实修复效果，详情请参见[手动执行软件漏洞检测](#)。

#### 📖 说明

若未进行手动验证，主机防护每日凌晨进行全量检测，修复后需要等到次日凌晨检测后才能查看检测结果。

### 13.4.3 为什么漏洞修复未生效？

若您未进行手动验证，主机防护每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看检测结果。

可以执行以下步骤立刻查看修复结果：

**步骤1** 漏洞修复完成后，建议您查看软件升级结果，确保软件已升级为最新版本，详细的操作命令请参见[表13-7](#)。

表 13-7 验证修复命令

操作系统	修复命令
CentOS/Fedora /Euler/ Redhat/Oracle	rpm -qa   grep 软件名称
Debian/Ubuntu	dpkg -l   grep 软件名称
Gentoo	emerge --search 软件名称

操作系统	修复命令
SUSE	zypper search -dC --match-words 软件名称

步骤2 [手动执行软件漏洞检测](#)查看漏洞修复结果。

----结束

## 13.4.4 漏洞管理显示的主机不存在？

漏洞管理显示24小时内检测到的结果。若检测到主机存在漏洞后，您修改了主机的名称，检测结果会显示原主机名称。

## 13.4.5 漏洞修复完毕后是否需要重启主机？

- Windows系统漏洞修复完成后需要重启。
- Linux系统Kernel类的漏洞修复完成后需要重启。


# 13.5 网页防篡改

## 13.5.1 为什么要添加防护目录？

网页防篡改是对目录中的文件进行防篡改防护，所以，开启网页防篡改后，需要添加防护目录才能起到防护作用。

## 13.5.2 如何修改防护目录？

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航栏中，选择“网页防篡改”，进入“网页防篡改”界面。

步骤4 选择所需开启“网页防篡改”防护的主机，在主机列表右侧的“操作”列中，单击“防护设置”，进入防护设置页面。

步骤5 选择所需修改的防护目录，在防护目录列表右侧操作列中，单击“编辑”修改。

### 说明

- 若您需要修改防护目录中的文件，请先暂停对防护目录的防护，再修改文件，以避免误报。
- 文件修改完成后请及时恢复防护功能。

图 13-11 防护设置



步骤6 在“编辑防护目录”弹框中进行修改，单击“确定”完成修改。

图 13-12 编辑防护目录



----结束

### 13.5.3 开启网页防篡改后，如何修改文件？

开启防护后，防护目录中的内容是只读，如果您需要修改文件或更新网站：

#### 指定特权进程

特权进程有权修改文件。

- 特权进程可以访问被防护的目录，请确保特权进程安全可靠。
- Linux系统服务器特权进程，仅在“防护目录设置”的“防护模式”为“保护网络文件系统”时生效。

## 临时关闭网页防篡改

请先临时关闭网页防篡改，完成修改或更新后再开启。

关闭网页防篡改期间，文件存在被篡改的风险，更新网页后，请及时开启网页防篡改。

## 设置定时开关

定时开关可以定时关闭**静态网页防篡改**，您可以使用此功能定时更新需要发布的网页。

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

### 13.5.4 开启动态网页防篡改后，状态是“已开启未生效”，怎么办？

动态网页防篡改提供tomcat应用运行时的自我保护。

开启动态网页防篡改需要满足以下条件：

- 仅针对Tomcat应用。
- 主机是Linux操作系统。
- 开启动态网页防篡改后，请等待大约20分钟后检查“tomcat/bin”目录下是否已生成“setenv.sh”文件，若已生成该文件，则重启Tomcat即可成功开启动态网页防篡改。

如果您开启网页防篡改后，状态是“已开启未生效”：

- 请检查您的“tomcat/bin”目录下的“setenv.sh”文件是否生成。
- 若“setenv.sh”文件已生成，请检查Tomcat是否重启。

## 13.6 其他

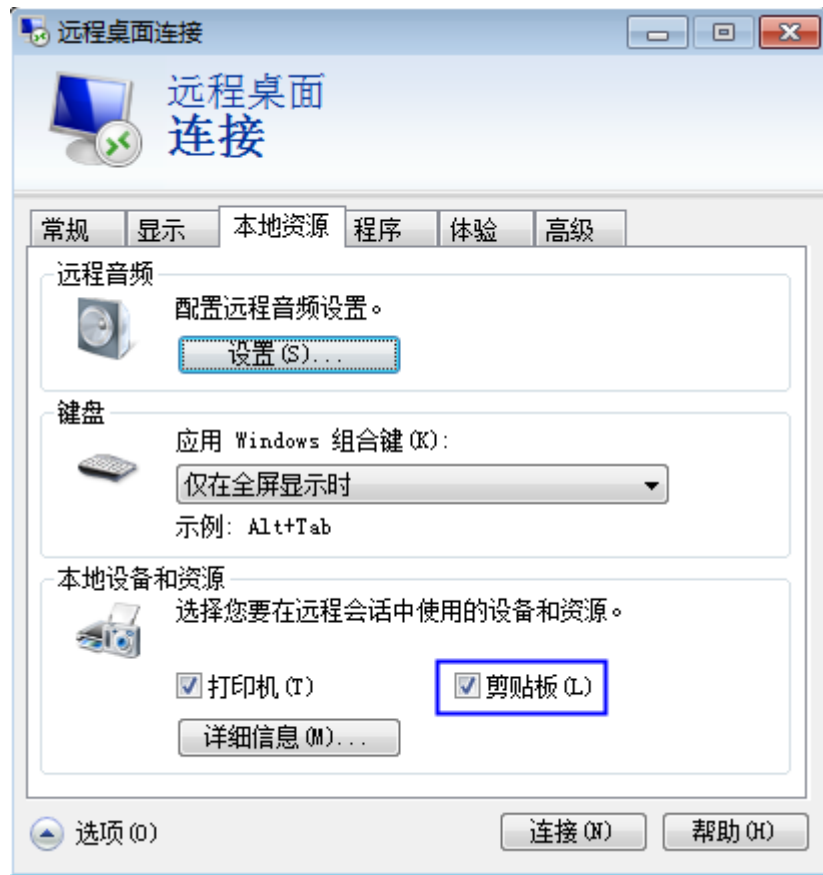
### 13.6.1 如何使用 Windows 远程桌面连接工具连接主机？

#### 操作步骤

**步骤1** 在本地主机上选择“开始 > 运行”，输入命令**mstsc**，打开Windows“远程桌面连接”工具。

**步骤2** 单击“选项”，选择“本地资源”页签，在“本地设备和资源”区域中，勾选“剪贴板”，如图13-13所示。

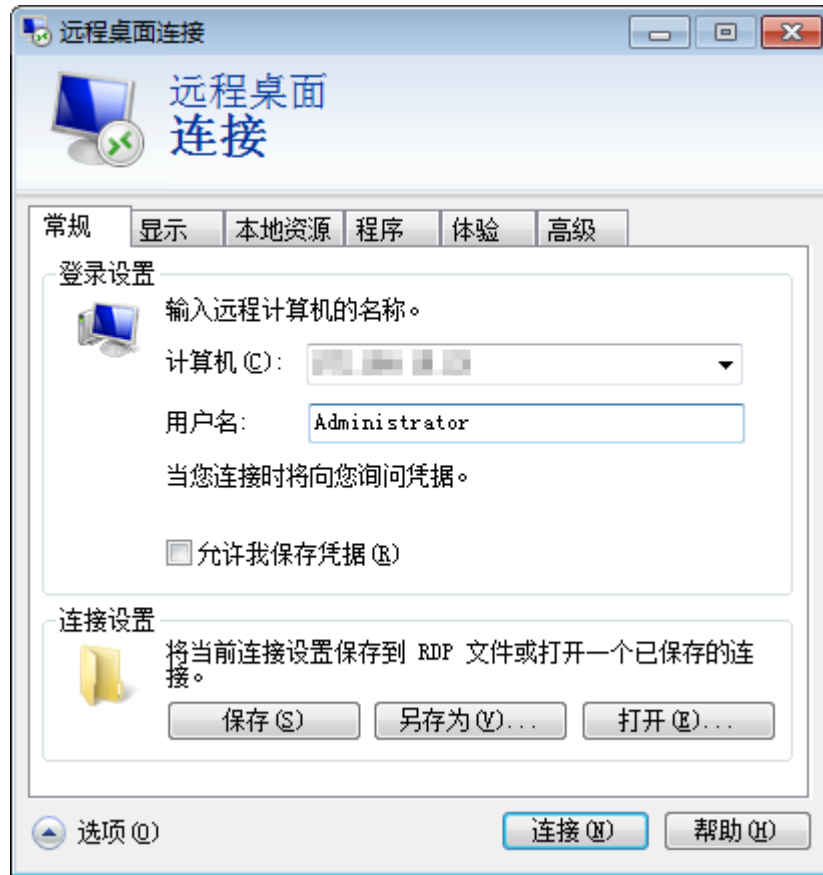
图 13-13 远程桌面连接



**步骤3** 选择“常规”页签，在“计算机”中输入云服务器的弹性IP，在“用户名”中输入“Administrator”，单击“连接”，如图13-14所示。



图 13-14 设置常规信息



**步骤4** 在弹出的对话框中，输入主机的用户密码，单击“确定”，连接至主机。

----结束

## 13.6.2 如何查看 HSS 的日志文件？

### 日志路径

您需要根据主机的操作系统，查看日志文件。

操作系统	日志所在路径	日志文件
Linux	/usr/local/hostguard/log/	<ul style="list-style-type: none"><li>• daemon.log: 记录守护进程运行时相关日志。</li><li>• hostguard.log: 记录监控进程运行时相关日志。</li><li>• hostguard_procmon.log: 记录进程创建的信息。</li><li>• urlconfig.log: 只在安装时，记录识别region信息。</li><li>• upgrade.log: 记录升级时相关日志。</li></ul>

操作系统	日志所在路径	日志文件
Windows	C:\Program Files (x86)\HostGuard\log\	<ul style="list-style-type: none"> <li>hostguard_rsync.log: 记录网页防篡改备份服务器的运行日志。</li> </ul>

## 日志保留周期

日志文件	文件大小限制	路径下保留的文件	保留周期
daemon.log	10M	保留5个最新的“daemon.log”日志文件。	不超过文件大小限制，只要不卸载HSS Agent，会一直保留日志信息。
hostguard.log	10M	保留5个最新的“hostguard.log”日志文件。	
hostguard_procmon.log	20M	保留2个最新的“hostguard_procmon.log”日志文件。	
urlconfig.log	不限制	保留1个“urlconfig.log”日志文件。	
upgrade.log	不限制	保留1个“upgrade.log”日志文件。	
hostguard_rsync.log	不限制	保留1个“hostguard_rsync.log”日志文件。	

### 13.6.3 如何开启登录失败日志开关?

#### MySQL

在账户破解防护功能中，Windows和Linux系统都支持MySQL软件的5.6和5.7版本，开启登录失败日志开关的具体的操作步骤如下：

**步骤1** 使用root权限登录主机。

**步骤2** 查询log\_warnings值，命令如下：

```
show global variables like 'log_warnings'
```

**步骤3** 修改log\_warnings值，命令如下。

```
set global log_warnings=2
```

**步骤4** 修改配置文件。

- Windows系统，修改配置文件my.ini，在[mysqld]中增加log\_warnings=2。
- Linux系统中，修改配置文件my.conf，在[mysqld]中增加log\_warnings=2。

----结束

## Filezilla

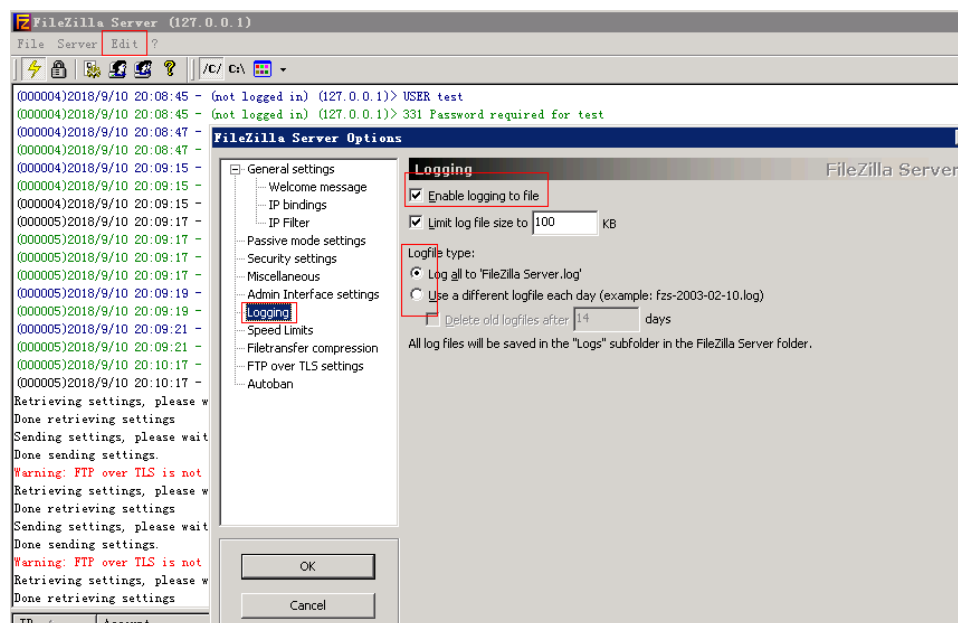
在账户破解防护功能中，仅Windows系统支持filezilla软件的0.9.60版本。filezilla默认不开启日志，需要在设置中开启日志开关。

开启日志开关的操作步骤如下：

**步骤1** 打开filezilla软件。

**步骤2** 选择“Edit > Settings > Logging”，勾选“Enable logging to file”，如图13-15所示。

图 13-15 filezilla 配置



---结束

## vsftp

本节指导用户开启vsftp的登录失败日志开关。

**步骤1** 修改配置文件（比如：/etc/vsftpd.conf），设置以下两项：

**vsftpd\_log\_file=log/file/path**

**dual\_log\_enable=YES**

**步骤2** 重启vsftp服务。设置成功后，登录时，会返回如图13-16所示的日志记录。

图 13-16 日志记录

```
Wed Aug 29 14:53:05 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:53:11 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:14 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:18 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"  
Wed Aug 29 14:55:26 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 11:50:16 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Sep 5 11:50:23 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 13:59:53 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"  
Wed Sep 5 13:59:59 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"  
Wed Sep 5 14:00:08 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
```

----结束

## 13.6.4 如何立即执行检测？

企业主机安全服务将实时检测主机中的风险和异常操作，在每日凌晨将对主机执行全面扫描，此外，您也可以使用手动检测功能全面检测主机中关键的配置信息。

手动检测功能仅支持检测主机中的软件、漏洞、网站后门、含有风险的口令和关键配置信息。

### 须知

手动检测完成后，需至少间隔三分钟，才能再次对同一个项目执行手动检测。

## 前提条件

服务器的“Agent状态”为“在线”、“防护状态”为“开启”、“版本”为“企业版”或者“旗舰版”。

## 检测项目

软件信息、Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、网站后门检测、口令风险和配置风险。


## 检测时长

- 检测单个检测项目（例如：口令风险）的检测时长为30分钟内。
- 一键手动检测，检测多个检测项目时，各个检测项目并行检测，检测时长为30分钟内。

## 一键手动检测

一键执行手动检测能同时检测主机中的软件信息、漏洞、网站后门、关键配置信息、较弱的口令复杂度策略、使用弱口令的用户账号。检测完成后，可在企业主机安全服务控制台查看各项风险统计或指定查看单个服务器的安全详情。

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在“主机管理”页面的右上角，单击“手动检测”，执行手动检测，如图13-17所示。

图 13-17 一键执行手动检测



**步骤4** 在弹出的“手动检测”对话框中，选择所需检测的主机，单击“确定”，完成一键手动检测的操作。

图 13-18 手动检测




**步骤5** 在安全控制台“企业主机安全”菜单或主机列表“操作”列的“查看详情”中查看各项手动检测结果并对检测结果执行相应的操作。

----结束

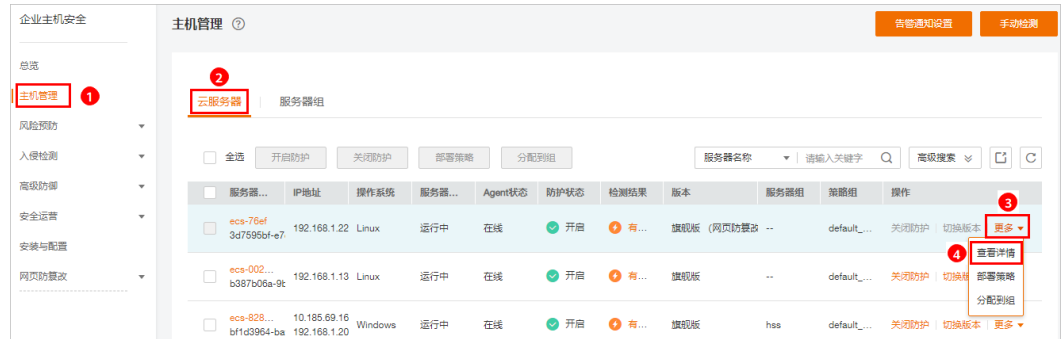
## 单点执行手动检测

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角选择“区域”，单击 ，选择“安全 > 企业主机安全”，进入企业主机安全页面。

**步骤3** 在左侧导航栏中，选择“主机管理”，在云服务器列表的“操作”列中，单击“查看详情”，进入指定主机的详情页面。

图 13-19 查看详情



- **手动收集软件信息**

选择“资产管理”页签，在页面下侧“软件信息”中，手动检测主机中的软件信息。

图 13-20 收集软件信息



- **手动执行漏洞检测**

选择“漏洞管理”页签，在“Linux软件漏洞管理”和“Web-CMS漏洞管理”中，手动检测主机中的软件漏洞和Web-CMS漏洞。

**说明**

- 软件漏洞检测和软件信息管理任意一个手动检测都会触发收集服务器上的软件信息。
- 选择“漏洞管理”页签，选择系统软件漏洞，单击“手动检测”，系统将立即执行一次系统软件漏洞检测。

图 13-21 系统软件漏洞检测



- 选择“漏洞管理”页签，选择Web-CMS漏洞，单击“手动检测”，系统将立即执行一次Web-CMS漏洞检测。

图 13-22 Web-CMS 漏洞检测



● 手动执行口令风险检测

选择“基线检查”页签，在“口令风险”中，手动检测主机中较弱的口令复杂度策略、弱口令以及风险配置项。

图 13-23 弱口令检测




● 手动执行配置检测

选择“基线检查”页签，在“配置检测”中，手动检测主机中不安全的配置项。

图 13-24 配置检测



步骤4 当“手动检测状态”为“检测完成”时，单击，查看最新检测结果。

----结束



# A 修订记录

发布日期	修改说明
2022-08-30	第二次正式发布。 优化资料描述。
2022-05-30	第一次正式发布。