

天翼云·企业主机安全

用户使用指南

天翼云科技有限公司





目 录

1 产	品介绍	4
1.1	什么是企业主机安全服务	4
1.2	产品优势	13
1.3	服务版本差异	13
1.4	应用场景	19
1.5	使用约束	20
1.6	HSS 权限管理	24
1.7	与其他云服务的关系	24
1.8	相关概念	25
2 用	户指南	28
2.1	开通主机防护	
2.2	查看主机防护列表	57
2.3	主机风险总览	60
2.4	安全配置	64
2.5	主机管理	71
2.6	风险预防	76
2.7	入侵检测	91
2.8	高级防御	
2.9	安全运营	



2.10	网页防篡改	
2.11	管理防护配额	
2.12	(可选)管理企业项目	192
3 常	见问题	201
3.1	产品咨询	
3.2	开通与配置	
3.3	告警事件处理	
3.4	漏洞管理	
3.5	网页防篡改	
3.6	其他	



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。

1.1.1 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0所示。





企业主机安全服务的组件功能及工作流程说明如下:

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	 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。 集成多种杀毒引擎,深度查杀主机中的恶意程序。
	• 接收您在控制台下友的配直信息和检测任务,开转友给安装在服务器上的 Agent。
	• 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。
Agent	 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。
	 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。
	• 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。
	• 根据操作系统版本选择对应的安装命令/安装包进行安装。
	 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。

1.1.2 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。

功能项	功能描述	检测周期
账号信息 管理	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。 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。 账号的实时信息包括账号的"账号名"、"对应主	实时检测
	机数"以及具体账号对应的"对应服务器"、"管理员权限"、"用户组"、"用户目录"和"用户 启动 Shell"。	
	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"、"管理员权限"、"用户组"、"用户目录"、"用户启动 Shell"和"发生变动时间"。	
开放端口 检测	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。	实时检测
	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。	
进程信息 检测	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。	实时检测
	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。	



功能项	功能描述	检测周期
Web 目 录管理	检测并列出当前系统中 Web 服务使用的目录,帮助 用户进行 Web 资源管理。	实时检测
	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"。	
软件信息 管理	检测并列出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。	每日凌晨自动检 测
	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。	手动检测
	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"。	
	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"。	
	您可以使用手动检测功能检测主机中的软件信息。	
自启动	检测并列出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。	实时检测
	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。	

● 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。

功能项	功能描述	检测周期
软件漏洞	包括 Linux 软件漏洞和 Windows 系统漏洞。	每日凌晨自动检测
检测	通过与漏洞库进行比对,检测出系统和官方软件	



功能项	功能描述	检测周期
	(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。	手动检测
Web- CMS 漏 洞检测	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

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。

功能项	功能描述	检测周期
口令复杂 度策略检 测	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。 您可以使用手动检测功能检测主机中的口令复杂 度策略。	每日凌晨自动检测 手动检测
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,防止账户口令被轻易猜 解。 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"。	每日凌晨自动检测 手动检测
	您可以使用手动检测切能检测王机中使用的弱口 令。	
配置检测	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。 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"。 根据配置检测规则和检测结果详情 您可以处理	每日凌晨自动检测 手动检测
	含有风险的配置项或忽略可信的配置项。	



功能项	功能描述	检测周期
	您可以使用手动检测功能检测主机中的关键配置 信息。	

● 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。

功能项	功能描述	检测周期
账户暴力 破解	检测 SSH、RDP、FTP、SQL Server、MySQL 等 账户遭受的口令破解攻击。	实时检测
	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。	
	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。	
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。	实时检测
	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"。	
	若在非常用登录地登录,则触发安全事件告警。	
	若账户暴力破解成功,登录到云主机,则触发安全 事件告警。	



功能项	功能描述	检测周期
恶意程序 (云查 杀)	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。 HSS 仅支持检测运行中的恶意程序。 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。 说明 恶意程序(云查杀) 仅支持检测运行中的恶意程 序。	实时检测
进程异常 行为	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。 进程异常行为可以监控以下异常行为: 监控进程 CPU 使用异常。 检测进程对恶意 IP 的访问。 检测进程并发连接数异常等。	实时检测
关键文件 变更	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。 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"。	实时检测
网站后门 (Websh ell)	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。 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。	实时检测 手动检测



功能项	功能描述	检测周期
	您可以使用手动检测功能检测主机中的网站后门。	
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: 利用 SUID 程序漏洞进行 root 提权。 利用内核漏洞进行 root 提权。 对文件的提权。	实时检测
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。 支持使用文件特征码检测 Rootkit。 支持对隐藏文件、端口、进程的检测。	每日自动检测



● 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。

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。	



1.2 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。

1.2.1 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。

1.2.2 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。

1.2.3 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。

1.2.4 轻量 Agent

Agent 占用资源极少,不影响主机系统的正常运行。

1.3 服务版本差异

企业主机安全服务有企业版、旗舰版和网页防篡改版供您选择,具体差异请参见 0。详细的功能介绍请参见 1.1.2 功能特性。

1.3.1 版本功能差异说明

版本功能说明

服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 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。	\checkmark	\checkmark	\checkmark
	开放端口	检测当前系统开放的端口,帮	\checkmark	\checkmark	\checkmark



服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 改版
	检测	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。	V	\checkmark	\checkmark
	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。	V	V	\checkmark
	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。	V	\checkmark	\checkmark
	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。	×	V	\checkmark
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。	V	V	\checkmark
	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。	V	V	\checkmark
	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。	V	V	\checkmark
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。	V	V	\checkmark
	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		\checkmark	\checkmark



服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 改版
		用户修改。			
	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。	V	\checkmark	\checkmark
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。	V	\checkmark	\checkmark
	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。 • 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"。 若在非常用登录地登录, 则触发安全事件告警。 • 若账户暴力破解成功,登 录到云主机,则触发安全 事件告警。	√	√	\checkmark
	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。	\checkmark	\checkmark	\checkmark
	进程异常 行为	检测各个主机的进程信息,包 括进程 ID、命令行、进程路		\checkmark	\checkmark



服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 改版
		径、行为等。 对于进程的非法行为、黑客入 侵过程进行告警。 进程异常行为可以监控以下异 常行为: • 监控进程 CPU 使用异常。 • 检测进程对恶意 IP 的访 问。 • 检测进程并发连接数异常			
	关键文件 变更	了。 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。	√	√	\checkmark
	网站后门 (Webshe ll)	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。 • 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"、"最后发现时 间"。您可以根据网站后 门信息忽略可信文件。 • 您可以使用手动检测功能 检测主机中的网站后门。	\checkmark	\checkmark	\checkmark
	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。	×	\checkmark	\checkmark



服务 功能	功能项	功能概述	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。	×	\checkmark	\checkmark
	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。	×	\checkmark	\checkmark
	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。	×	\checkmark	\checkmark
	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。	\checkmark	\checkmark	\checkmark
	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: •利用 SUID 程序漏洞进行 root 提权。 •利用内核漏洞进行 root 提 权。 •对文件的提权。	×	\checkmark	\checkmark
	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。 • 支持使用文件特征码检测 rootkit。 • 支持对隐藏文件、端口、 进程的检测。	×	\checkmark	\checkmark



服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 改版
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。	×	~	\checkmark
	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。	×	\checkmark	\checkmark
	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。	×	~	\checkmark
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。 • 查看策略组列表 • 依据默认策略组和已创建 的策略组添加策略组 • 自定义策略 • 修改和删除策略组 • 针对策略组包含的策略, 进行修改和关闭策略 • 在"主机管理"页面可以 对主机进行批量部署策略	√ (仅 支持业 版策 组)	√	\checkmark
	安全报告	呈现每周或每月的主机安全趋	\checkmark	\checkmark	\checkmark



服务 功能	功能项	功能概述	企业版	旗舰版	网页防篡 改版
		势以及关键安全事件与风险。			
安全 配置	双因子认 证	通过密码+短信/邮件认证的方 式,彻底防范账号暴力破解行 为。	\checkmark	\checkmark	\checkmark
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。	×	×	\checkmark
	网盘文件 防篡改	防止共享文件网盘中的网页文 件被篡改。	×	×	\checkmark
	动态网页 防篡改	防止网站数据库中动态网页内 容被篡改。	×	×	\checkmark

1.4 应用场景

● 等保合规

企业主机安全是等保合规的关键项,企业主机安全服务提供的入侵检测功能,能协助各企业保护企 业云服务器账户、系统的安全。

● 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。支持双因子认证登录,防止用户云服务器上的账 户遭受暴力破解攻击,提高云服务器的安全性。

● 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, 保证业务系统的正常运行使用,有效应对 APT 攻击等高级威胁。

1.5 使用约束

1.5.1 支持的云服务器类型

弹性云服务器 (Elastic Cloud Server, ECS)

1.5.2 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 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 0 和 0 所示。

Linux 系统版本 (X86 计算)

序号	支持的 OS 类型
1	CentOS: 6, 7 and 8 (64 bit)



序号	支持的 OS 类型
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, 16.04, 18.04 and 20.04 (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 and 7.4 (64bit)

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天翼云主机 Windows 系统版本如 0 所示。

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 McAfee 软件、360
2	Windows Server 2019 数据中心版 64 位简体 中文(40GB)	安全卫士、腾讯管家 等第三方安全防护软



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

企业主机安全服务支持的主机 Windows 系统版本如 0 所示。

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 McAfee 软件、360
2	Windows Server 2019 数据中心版 64 位简体 中文(40GB)	安全卫士、腾讯管家 等第三方安全防护软 件. 请先停止第三方
3	Windows Server 2016 标准版 64 位英文 (40GB)	安全防护软件的防护 功能,待 Agent 安装
4	Windows Server 2016 标准版 64 位简体中文	完成后再开启。



序号	支持的 OS 类型	使用限制说明
	(40GB)	
5	Windows Server 2016 数据中心版 64 位英文 (40GB)	
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)	



1.6 HSS 权限管理

系统默认提供两种权限:用户管理权限和资源管理权限。用户管理权限可以管理用户、用户组及用 户组的权限。资源管理权限可以控制用户对云服务资源执行的操作。

1.7 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。

1.7.1 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》。

1.7.2 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》。

1.7.3 企业管理

企业中有多个项目,多个项目的资源需要分开结算,且分属不同人员进行管理。同时项目可以单独 启动或停止,对其他项目没有影响。那么可以针对企业中的每个项目,分别建立企业项目,管理各自的 资源,并且针对不同的企业项目,设置不同的人员进行管理。

关于企业管理的更多信息,请查看《企业管理用户指南》。



1.7.4 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》。

1.7.5 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》。

1.8 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。

包括检测 SSH、RDP、FTP、SQL Server、MySQL 等账户遭受的口令破解攻击。

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 (云査杀)

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。

• 双因子认证

双因子认证是指结合密码以及验证码两种条件对用户登录行为进行认证的方法。

● 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。

● 软件漏洞

包括 Linux 软件漏洞和 Windows 系统漏洞。

● Web-CMS 漏洞

通过 Web 目录和文件, 识别出 Web-CMS 漏洞, 提升 Web 服务安全性。

● 配置检测

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。



● 网站后门 (WebShell)

云服务器上 Web 目录中的文件,判断是否为 WebShell 木马文件,包括常见的 PHP、JSP 等后门文件类型。

● 反弹 Shell

用户的进程行为,进程的非法 Shell 连接操作产生的反弹 Shell 行为。主要指 TCP、UDP、ICMP 等协议。

● 异常 Shell

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。

● 提权操作

当前系统的"进程提权"和"文件提权"操作。

异常提权操作包括:

- 利用 SUID 程序漏洞进行 root 提权。
- 利用内核漏洞进行 root 提权。
- 对文件的提权。

● Rootkit 程序

Rootkit 安装的文件和目录,帮助用户及时发现可疑的 Rootkit 安装,包括文件特征码、隐藏文件、端口、进程。



2 用户指南

2.1 开通主机防护

2.1.1 步骤一: 购买防护配额

通过本节介绍,您将了解如何购买防护配额。购买网页防篡改赠送旗舰版,包含旗舰版所有功能。

● 约束与限制

• 一个配额只能绑定一个主机,且只能绑定 Agent 在线的主机。

● 天翼云主机: HSS 不支持跨区域使用, 主机与 HSS 配额不在同一区域时, 请退订配额, 重新购 买主机所在区域的配额。

● 前提条件

已获取管理控制台的登录帐号与密码。

购买防护配额(天翼云主机)

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在界面右上角,单击"购买主机安全",进入"购买主机安全配额"界面。

在"购买主机安全配额"界面,设置配额的规格。

1. 选择计费类型,选择"包年/包月"。

支持"包年/包月"和"按需"。

🗀 说明

选择"按需"时,不需要购买企业主机安全防护配额,直接在当前页面右下角单击"立即开通",可跳转到云服务器列表页面。



在云服务器列表的"操作列"中,单击"开启防护","计费模式"选择"按需计费","主机安全版本"选择"企业版",开启"企业版"防护。

2. 选择区域。

HSS 不支持跨区域使用,如果您购买了与主机不在同一区域的配额,请退订配额后重新购买主机所 在区域的配额。

3. 选择版本。

支持"企业版"、"旗舰版"和"网页防篡改版"。

● 若您购买的是企业版/旗舰版配额,请在"企业主机安全 > 主机管理 > 云服务器"页面开启防 护。

● 若您购买的网页防篡改版配额,请在"网页防篡改 > 防护列表"页面开启防护。

4. 选择企业项目。

从下拉列表中选择所在的企业项目。

企业项目针对企业用户使用,只有开通了企业项目的客户,或者权限为企业主帐号的客户才可见。 如需使用该功能,请联系您的客户经理申请开通。企业项目是一种云资源管理方式,企业项目管理服务 提供统一的云资源按项目管理,以及项目内的资源管理、成员管理。

🛄 说明

- "default"为默认企业项目,帐号下原有资源和未选择企业项目的资源均在默认企业项目内。
- 只有注册的帐号购买 HSS 时,"企业项目"下拉列表中才可以选择到"default"。
- 5. 选择购买时长。

支持"按月/按年(自动续费)"。

6. 设置防护主机数量。

购买成功后不支持增加配额,如需增加配额,请重新购买。

企业版

企业版

防护主机数量	- 1 +
	您当前有 0台包年/包月主机,已有企业版及旗舰版配额 10个,还需购买 0个;按需主机请根据实际需求决定是否购买;如购买数量超过500个,请分多次购买。
	为防止未防护主机感染勤素、挖矿等病毒后传染给其他主机,导致企业内网整体沦陷,建议您的云上主机全部署主机安全服务。
	的买企业主机安全配额后,请到企业主机安全控制台"主机管理"页面开启防护



须知

为防止未防护主机感染勒索、挖矿等病毒后传染给其他主机,导致企业内网整体沦陷,**您的云上主机** 应该全部署主机安全服务。若您希望只防护部分主机并承担因此带来的整网风险,可以联系您的服务 经理或销售人员进行配置。

● 旗舰版

无数量限制

● 网页防篡改版

无数量限制

在页面右下角, 单击"立即购买", 进入"订单确认"界面。

确认订单无误后, 单击"去支付", 进入"付款"页面, 付款后, 完成购买防护配额的操作。

● 生效条件

付款成功后,您可以在 HSS 管理控制台的"主机管理 > 防护配额"页面查看当前购买的 HSS 版本、配额状态、配额使用状态以及配额绑定的主机。

2.1.2 步骤二:安装 Agent

2.1.2.1 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 2.1.2.2Windows 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。

● 前提条件

● 待安装 Agent 的主机已绑定弹性 IP。

● 待安装 Agent 所在的线上主机需要与网段相通,要求您的服务器安全组出方向的设置允许访问 100.125.0.0/16 网段的 443 端口。

- 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。



- 约束与限制
 - 天翼云主机

主机与 HSS 必须在**同一区域**,并使用配额所在区域的安装命令或安装包为主机安装 Agent,否则会 导致 HSS Agen **安装失败**。若主机与 HSS 配额不在同一区域,请退订重新购买主机所在区域的配额。

● 非天翼云主机

非**天翼云**主机需要能通过**公网 IP** 访问天翼云,才能接入 HSS。安装 Agent 后,在防护列表中,您 可以根据主机的 IP 地址查找该主机。

须知

● 由于主机的性能差异,非天翼云的主机与企业主机安全服务的兼容性可能较差,为使您获得良好的服务体验,建议您使用天翼云主机。

 安装 Agent 时,请暂时清理主机中可能干扰主机安装的应用进程和配置信息(例,McAfee 软件、 360 安全卫士、腾讯管家等第三方安全防护软件),防止 Agent 安装失败。

系统影响

安装 HSS Agent 对主机没有任何影响。HSS 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。未安装 Agent 插件的主机将不受 HSS 保 护,控制台页面也不会显示该主机资产的任何系统漏洞、基线风险、入侵事件和安全报告等数据。

● 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/"

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。安装成功后,Agent 不会立即生效,需要等待 3~5 分钟左右控制台才会刷新。

登录管理控制台。

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。



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。

复制安装 Agent 的命令



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 帐号在主机中安装 Agent。

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。

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

安装成功后, Agent 不会立即生效, 需要等待 3~5 分钟左右控制台才会刷新。

● 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。



登录管理控制台。

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。

下载 Agent 安装包



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。

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。

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 帐号在主机中安装 Agent。

使用 cd 安装包所在目录命令,进入安装包所在目录。

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。



Hostguard is running. Hostguard installed.

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

安装成功后, Agent 不会立即生效, 需要等待 3~5 分钟左右控制台才会刷新。

2.1.2.2 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 2.1.2.1Linux 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。

● 前提条件

● 待安装 Agent 的主机已绑定弹性 IP。

● 待安装 Agent 所在的线上主机需要与网段相通,要求您的服务器安全组出方向的设置允许访问 100.125.0.0/16 网段的 443 端口。

● 已在本地安装远程管理工具(如: "pcAnywhere"、"UltraVNC")。

● 约束与限制

● 天翼云主机

主机与 HSS 必须在**同一区域**,并使用配额所在区域的安装命令或安装包为主机安装 Agent,否则会 导致 HSS Agen **安装失败**。若主机与 HSS 配额不在同一区域,请退订重新购买主机所在区域的配额。

● 非天翼云主机

非**天翼云**主机需要能通过**公网 IP** 访问天翼云,才能接入 HSS。安装 Agent 后,在防护列表中,您 可以根据主机的 IP 地址查找该主机。



须知

- 由于主机的性能差异,非天翼云的主机与企业主机安全服务的兼容性可能较差,为使您获得良好的服务体验,建议您使用天翼云主机。
- 安装 Agent 时,请暂时清理主机中可能干扰主机安装的应用进程和配置信息(例,McAfee 软件、 360 安全卫士、腾讯管家等第三方安全防护软件),防止 Agent 安装失败。

● 系统影响

安装 HSS Agent 对主机没有任何影响。HSS 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。未安装 Agent 插件的主机将不受 HSS 保 护,控制台页面也不会显示该主机资产的任何系统漏洞、基线风险、入侵事件和安全报告等数据。

● 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"

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。 登录管理控制台。

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。 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。

安装 Windows Agent



企业主机安全	安裝与配置 ⑦	购买主机安全	卸载Agent
总武 主机管理	全边项目 default + C		
 风险預防 ・ 入侵检測 			
安全运营 • · 安安地配置 1 网页防镰衣 •	 ● 使用主机完全款素确保: 您你跟我要全些比约考找包里方示的可100.125.00/16网段的444%同口。 ※可能够了解: 下載化量分報的年 		
	安 現方式- ④ 1 下 8-00m1安地(1年)出 1 1 1 2 で 第時間前の近星風気は使 1 1 2 1 1 1 2 1 1 1 2 1 1 1 2 1 1 1 1	支持系统: Windows 2016 Windows 2012 Windows 2008	
	Linux系統 安装方式二 1. 道理整要的回始路時編。 2. 通过に設定離析の早安装体Agent页面、重接下載最新版Agent者就最考醒。 2. 通过に設定離析の同分構要将用別的勾NAba入受信任的Aden。 道都接示: 通过に設定離的同時需要将用別的勾NAba入受信任的Aden。		

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,并使用管理员帐号在主机中安装 Agent。

将 Agent 安装包上传到待安装 Agent 的主机中。

使用管理员权限运行 Agent 安装程序。

安装 Agent 时,在主机类型界面,选择主机类型。

安装完成后,在"Windows 任务管理器"中查看进程"HostGuard.exe"和"HostWatch.exe",如 0 所示。

若进程不存在,则表示 Agent 安装失败,请尝试重新安装 Agent。

查看 Agent 运行状态


₩ 任务管理器 文件(F) 洗项(O) 音看(V)	– 🗆 X		
进程 性能 用户 详细信息 服务			
^ 名称	3% CPU	48% 内存	
应用 (2)			^
> n∰ Task Manager	2.4%	8.5 MB	
> 清 Windows 资源管理器	0%	21.9 MB	
后台进程 (23)			
> 📧 Antimalware Service Executa	0%	96.1 MB	
> 💽 COM Surrogate	0%	3.0 MB	
> 📧 COM Surrogate	0%	1.2 MB	
› 📧 HostGuard.exe (32 位)	0%	3.0 MB	
› 📧 hostwatch.exe (32 位)	0%	1.8 MB	
> 📧 Intel® PROSet Monitoring S	0%	1.5 MB	
> 🐗 Java Service Wrapper Comm	0%	2.0 MB	
🕌 Java(TM) Platform SE binary	0%	24.7 MB	
骨 Microsoft IME	0%	1.1 MB	
Microsoft Malware Protectio	0%	2.1 MB	~
			结束任务(E)

2.1.3 步骤三:设置告警通知

2.1.3.1 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。

若您不设置告警通知,进入主机管理页面,HSS 会自动弹出您未设置告警的提示框。

若您想屏蔽该提示框,您可以单击"快速设置",设置告警通知,或者勾选"不再提醒",并单击"暂不设置",即可屏蔽该提示框。

● 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,建议您先以管理员身份在"消息通知服务"中创建"消息主题"。



🛄 说明

告警通知方式分为"消息中心"和"消息主题"。 消息中心:使用消息中心和其它安全服务共同使用"安全事件通知"的信息接收人。 消息主题:为 HSS 单独创建的主题,设置告警通知接收人。

● 开启企业版/旗舰版的告警通知

登录管理控制台。

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。 选择"告警通知"页签,进入"告警通知"页面,如0所示。

企业主机安全	安装与配置 ⑦						购买主机安全	如觀Agent
总范								
主机管理	企业项目 defau	t · C						
风险预防 🔻								
入價检測 💌			2					
高级防御	安號Agent	安全配置 双因子认证						
安全运营								
网页防幕放	1、告答通知设 2、告答通知有	置仅在当前区域/项目生效,其他区域 可能被当成垃圾信息而拦截,如未收;	(项目的告答通知清切换到对应区域 别告答通知,请确认是否被拦截。	/项目进行设置。 3				
	每日告警通知							
	漏知顶目	遥知内容						
	资产管理	▶ 危险第二						
	混渴管理	【二 点集演用						
	入侵检测	 ✓ 账户破解防护 ✓ 异常shell 	 ✓ 关键文件变更 ✓ 高危命令执行 	 ✓ 悪意編序 ✓ 提収操作 	 ✓ 网站后门 ✓ Rootkit程序 	🔽 反弹shell		
	基线检查		✓ 风险账号	✓ 配置风险				
	账户登录	▶ 异蛇登录						
	实时告警通知							
	遥知顶日	遥知内容						
	入侵检测	 ✓ 账户异常登录 ⑦ ✓ 异常shell 	 ✓ 悲意程序 ✓ 高性命令执行 	 ✓ 关键文件変更 ⑦ ✓ 提収操作 	✓ 网站告门 ✓ Rootkit程序	✓ 反3年shell		
	账户登录	登录成功通知						
	请选择您的主题 下拉框只展示订阅》		即服务主题					
	应用							

企业版/旗舰版

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。

选择通知项

通知项	说明	选择建议
每日告	每日凌晨,企业主机安全服务	• 接收并定期查看每日告警通知中所有
	将主动检测主机系统中的账	的内容,能有效降低主机中未及时处



通知项	说明	选择建议
警通知	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。	理的风险成为主机安全隐患的概率。 • 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"。
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。	 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。 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"。

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》。

单击"应用",完成配置主机安全告警通知的操作。界面弹出"告警通知设置成功"提示信息,则说明告警通知设置成功。

● 告警通知项说明

通知项	通知内容	通知内容说明		
每日告警通知				
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:				



通知项	通知内容	通知内容说明
00 发送给你游	忝加的手机号或者	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。
入侵检测	账户破解防护	检测 SSH、RDP、FTP、SQL Server、MySQL 等账 户遭受的口令破解攻击。
		 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。
		 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。
	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。



通知项	通知内容	通知内容说明
	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	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。 若在非常用登录地登录,则触发安全事件告警。
	1	
事件发生时,	, 及时发送告警通知	和。
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



通知项	通知内容	通知内容说明
		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	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。
		如果您所有主机上的账户都由个别管理员负责管理, 通过该功能可以对系统账户进行严格的监控。
		如果系统账户由多人管理,或者不同主机由不同管理员负责管理,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
		业土机安全服务控制台天闭该古警坝。
		^{说明} 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。

2.1.3.2 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。

● 前提条件

在设置告警通知前,建议您先以管理员身份在"消息通知服务"中创建"消息主题"。



🛄 说明

告警通知方式分为"消息中心"和"消息主题"。 消息中心:使用消息中心和其它安全服务共同使用"安全事件通知"的信息接收人。 消息主题:为 HSS 单独创建的主题,设置告警通知接收人。

● 开启网页防篡改告警通知

登录管理控制台。

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。 进入"告警通知"页面,选择告警通知时间,如0所示。

告警通知设置

企业主机安全		安装与配置 ⑦	
总选			
主机管理		企业项目 default • C	
风脸预防	*		
入侵检测	-	2 2 cy装Agent 活警通知 辺識备份服务器	
高级防御	Ŧ		
安全运营	*		
安装与配置			
网页防算改 防护列表	*	 告警告现设置仅在当新区域项目主效、其他区域项目的告管语句请切换到过应区域项目进行设置、 发送告答是如需要使用自思想和服务。您每个月都可以免要发送一定发量的消息通知。超出免费改量后按使用 告答通如有可能被当成垃圾信息而拦截。如未收到告答通知,请确认是否被注意。 	量收费。
安装与配置		9 毎日告警	
		通知项目	通知时间
		动态网页防篡改	10:00
		实时告警通知	
		通知项目	通知时间
		动态网页防算改	 24小时 08:00 - 20:00
		请选择您的主题 • C 宣誓消息還知服务主题	
		下拉裡只是示订同状态为"已論认"的肖思道知主题。 应用	

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》。



单击"应用",完成配置主机安全告警通知的操作。界面弹出"告警通知设置成功"提示信息,则说明告警通知设置成功。

2.1.4 步骤四:开启主机防护

2.1.4.1 企业版/旗舰版

开启企业主机安全服务时,您需为指定的主机分配一个配额,关闭企业主机安全服务或删除主机后, 该配额可分配给其他的主机使用。

网页防篡改版,请在"网页防篡改 > 防护列表"页面开启防护,具体请参见 2.1.4.2 网页防篡改版。

● 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

登录管理控制台。



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。 在左侧导航栏中,选择"主机管理",进入"云服务器"界面,如0所示。

进入"云服务器"界面

企业主机安全		主机	管理 ⑦ や 使用解剖									购买主机业全	69 8	0.0M	手动检测
8克 主机管理 1		21	2項目 所有项目	* C											
风脸预防															
入侵检测	×														
拖级防御		0	- 服务器组	防护配额											
安全运营	*														
安装与配置			全选 开启助护	外闭防护	部務策略	分配到組					服务器名称	▼ 清输入关键字	Q	電袋搜索 ※	C C
同页防装改			服务器名称/ID	IP地址	操作系统	服务器状态	Agent铁窗	防护状态	检测结果	当前版本	服务器组	策略组	探作		
			ecs-ac87 6f153beb-e8f3-46d9-!	172.16.1.121 (松和)	Unux	运行中	未安装 安装Agent	0 关闭	4. 未检測	无			开启防护	切换版本	更多 •
			b70fb7ba-8a67-45f0-1	172.16.0.8 (毛油)	Linux	這行中	未安装 安装Apent	● 关闭	() 未位別	无			开启防护	切换版本	更多 •

选择所需开启安全防护的主机,单击"开启防护"。

您可以根据自己的实际场景选择"包年/包月"或者"按需计费",开启主机防护。

● 包年/包月

在"开启防护"对话框中,"计费模式"选择"包年/包月",选择"主机安全版本"、分配"防护配额",如0所示。

开启防护				×
需要开启主机安全	全防护的服务器列表	Ē:		
服务器名称	IP地址	操作系统	当前版本	
ecs		Windows	无	
计费模式	● 包年/包月	○ 按需计费		
主机安全版本	◉ 企业版	() 旗舰版		
防护配额	随机选择配额	•	С	
	企业版总配额13	个,已用配额0个,可用配额	13个。	
	_			
		确定取消		

开启包周期主机防护

"防护配额"分配方式:

随机分配:下拉框选择"随机选择配额",系统优先为主机分发服务剩余时间较长的配额。



指定分配:下拉框选择具体配额 ID,您可以为主机分配指定的配额。

批量分配: 批量开启防护时, 系统会随机为批量选择的主机分配防护配额。

● 按需计费

在"开启防护"对话框中,"计费模式"选择"按需计费",选择"主机安全版本",如0所示。

开启防护					×
需要开启主机安	全防护的服务器列	表:			
服务器名称	IP地址		操作系统	当前版本	
ecs-			Windows	无	
计费模式	○ 包年/包月	• 按	需计费		
主机安全版本	◉ 企业版				
		确定	取消		

开启按需计费主机防护

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",则表示企业版/旗舰版防护已开启。

🛄 说明

- 您也可以通过在"主机管理 > 防护配额"页面的"操作"列中,单击"绑定主机",为主机绑定防护配额, HSS 自动为主机开启防护。
- 一个配额只能绑定一个主机, 且只能绑定 Agent 在线的主机。

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 0 所示。

自动执行的安全检测





● 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。

查看详情



企业主机安全		主机管理	主机器理 ① *** (7月18日)							時天主机安全	教師運行の置	手动检测	
8流 主机管理 1		企业项目	RNZH	* C									
风险预防	*												
入療检測													
能感防御		0 380	時間 服务器道	防护配额									
安全运营													
安装与配置			全透 开启防护	关闭防护 部署	\$16 STEE	992			19	\$888 · •	遺稿入关键字	Q 胞尿液素 >	C
用同助复改	*		服务器名称/ID IP地址	操作系统	服务器状态	Agent秋恋	防护状态	检测结果	动服版本	服务課題	菜籍相	腺性	•
			ecs-balyichuan a1983984-3906-4 10.154.13	2.235 🤆 Linux	运行中	案话	😋 开度	😋 无风险	全世版 配額1D: 56069231-65所-4	a:		968839 tolai	KA HA -
			ecs- ab7ee35d-143b-4	Windows	关机	在线	0 光闭	❷ 无风脸	全业板 配創D: 56069231-65fee	d		开展的户口的研	重和斗钟 15百姓和
			ecs-	Linux	会議中	未安績	⊘ 开启	🕑 无风脸	2016			20/8829 1 12884	Sacring

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。

查看检测结果

企业主机安全		云服务器 / ecs-8285-windows	服务器 / ecs-8285-windows									
总题												
主机管理		资产管理 漏洞管理	基线检查入侵检测									
风险预防	*											
入侵检测	*	账号信息 (4) 开放端口	账号信息(4) 开放端口(0/25) 进程信息(61) WEB目录(0) 软件信息(14) 自启动(24)									
高级防御												
安全运营	*	列出当前系统的账号信息,帮助用	列出当約系統的账号信息,韓助用户进行账户安全性管理。									
安装与配置						请输入账号名 Q C						
网页防复改	*	账号名	管理员权限	用户组	用户目录	用户启动Shell						
		Administrator	是	Administrators								
		DefaultAccount	否	System Managed Accounts Group								
		Guest	否	Guests		**						
		iv	是	Administrators,Users								

● 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0所示。

手动配置的检测项





手动配置检测项

功能	检测项
安全配置	• 常用登录地/IP
	● SSH 登录 IP 白名单
	• 开启恶意程序隔离查杀
入侵检测	● 配置告警白名单
	• 配置登录白名单
高级防御	• 程序运行认证
	• 文件完整性管理
	• 勒索病毒防护
安全运营	 自定义策略管理



● 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。

关闭主机防护后, HSS 会自动释放防护配额。您可将空闲的配额分配给其他主机继续使用或退订无 需使用的配额,避免造成配额资源的浪费。

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。

解绑配额

您可以在"主机管理 > 防护配额"页面的"操作"列中,选择"更多 > 解绑配额",解绑配额。解 绑配额后,该配额的使用状态将从"使用中"变更为"空闲", HSS 将自动关闭关联主机的防护。

您可将"空闲"的配额分配给其他主机继续使用或退订无需使用的配额,避免造成配额资源的浪费。

2.1.4.2 网页防篡改版

开启网页防篡改时,您需为指定的主机分配一个配额,关闭企业主机安全服务或删除主机后,该配额可分配给其他的主机使用。

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

网页防篡改原理

防护类型	原理说明
静态网页防	1. 锁定本地文件目录
护	驱动级锁定 Web 文件目录下的文件,禁止攻击者修改,网站管理 员可通过特权进程进行更新网站内容。
	2. 主动备份恢复



防护类型	原理说明
	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。
	3. 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。
动态网页防	1. 基于 RASP 过滤恶意行为
护	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。
	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。

● 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。



● 开启网页防篡改

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"网页防篡改"界面,单击"开启防护"。

使用指南 购买网页防装改 企业主机安全 防护列表 ② 总览 企业项目 所有项目 • C 主机管理 风险预防 入侵检测 已防御篡改攻击 🛛 防护主机数 0 防护目录 0 防篡改配额 1 使用中 0 _{空闲} 1 配额详情 高级防御 安全运营 开启防护 关闭防护 QC 服务器名称 ▼ | 清输入关键字 安装与配置 服务器名称/ID IP地址 操... ⑦ 服务器状态 Agent... ⑦ 防... ⑦ 动态防复改状态 操作 版木 网页防装改 防护列表 1 ecs-f792 8f08434f-59da-4 172.16.1.160 (私 Linux 运行中 在线 关闭 未开启 2 开启防护 防护设置 | 查看报告 安装与配置 servicestage-nod 81e97d86-04d4-4 172.16.0.106 (¾ Linux 0 关闭 运行中 未安装 未开启 开启防护|防护设置|查看报告 ecs-5364w 172.168.101.246 930db6a5-e930-4 172.16.0.96 (私津 Linux 关机 ● 关闭 未开启 开启防护|防护设置|查看报告 未安装 无

进入"网页防篡改"界面

在"开启防护"对话框中,为指定的主机分配"防护配额",单击"确定",开启防护,如0所示。

🗀 说明

若您的主机使用的是 Linux 操作系统,您可以同时开启动态网页防篡改,动态网页防篡改开启后,需重启 Tomcat 才能使其生效。

开启网页防篡改



开启防护										
▲ 开启功能后需要有防护目录才能起到防护作用,请根据需要设置相应的防护 × 目录。动态网页防篡改开启后,还需重启Tomcat才能使其生效。										
需要开启网页防篡改的服务器列表:										
服务器名称		IP地址	操作系统	防护状态						
host-0011		10.168.4.1 (弹性公网 192.1.1.1 (私有)	Linux	关闭						
防护配额	防护配额 随机选择配额 🔹 C									
网 <u>贝防</u> 装改版:	网页防篡改版总配额4个,已用配额2个,可用配额2个。									
开启动态网页防复改										
		确定	取消							

"防护配额"分配方式:

- 随机分配:下拉框选择"随机选择配额",系统优先为主机分发服务剩余时间较长的配额。
- 指定分配:下拉框选择具体配额 ID,您可以为主机分配指定的配额。
- 批量分配:批量开启防护时,系统会随机为批量选择的主机分配配额。

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。

"网页防篡改版"开启后,旗舰版防护会同步开启。

● 选择 "网页防篡改 > 防护列表",目标主机所在行的 "防护状态"为 "开启",且 "版本"为 "网页防篡改版",则表示网页防篡改版已开启。

● 选择"企业主机安全 > 主机管理 > 云服务器",目标主机所在行的"防护状态"为"开启",且 在"操作"列中主机不能"关闭防护"和"切换版本",则表示网页防篡改赠送的旗舰版已开启。



须知

- 您也可以通过在"网页防篡改 > 防护列表 > 配额详情"页面,单击"绑定主机",为主机绑定防护 配额,HSS 自动为主机开启网页防篡改防护。
- 一个配额只能绑定一个主机, 且只能绑定 Agent 在线的主机。
- 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。

关闭网页防篡改后, HSS 会自动释放防护配额。您可将空闲的配额分配给其他主机继续使用, 避免 造成配额资源的浪费。

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。
- 当用户关闭网页防篡改时会同步关闭旗舰版防护。

解绑配额

您可以在"网页防篡改 > 防护列表 > 配额详情"页面的"操作"列中,选择"更多 > 解绑配额", 解绑配额后,该配额的使用状态将从"使用中"变更为"空闲"。HSS 将自动关闭关联主机的网页防篡改 防护。

您可将"空闲"的配额分配给其他主机继续使用,避免造成配额资源的浪费。



2.1.5 (可选) 步骤五: 切换主机安全版本

您可以根据需要将企业主机安全服务的版本切换为"企业版"或者"旗舰版"。

● 注意事项

● 按需变更为包周期。

按需变更为包周期,需要用户购买包周期配额,生成新的订单,用户支付订单后,包周期配额立即 生效。包周期配额生效后,需要用户在云服务器列表页面,勾选目标主机,单击"开启防护",选择包周 期防护配额,直接开启包周期配额防护。

● 包周期变更为按需。

包周期转按需,需要用户在云服务器列表页面,勾选目标主机,单击"开启防护",选择按需防护, 按需的资费模式才会生效。

- 若企业主机安全服务的版本由高版本版切换为低版本后,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"企业版"或者"旗舰版"。

切换版本前准备

● "企业主机安全 > 主机管理"页面"云服务器"中目标主机的"Agent 状态"为"在线",且已开启主机防护。

切换为包周期配额版本时,需重新为主机指定相应的配额,变更版本前请先购买数量充足的配额。

● 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。

切换版本

登录管理控制台。

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。 在左侧导航栏中,选择"主机管理",进入"云服务器"界面,如0所示。

进入"云服务器"界面



企业主机安全	主机管理 ⑦ 🔍 🔍 🕅	191								购买主机业全	告答遵知论量	手动检测
主机管理	企业项目 所有项目	* C										
风脸预防												
入侵位到												
高级訪問 -	2 云服务器 服务器	组防护配额										
安全运营												
安装与配置	全遇 开启助护	关闭防护	部著領略	分配到组					股份器名称	▼ 请输入关键字	Q 電磁機業 🗧	C
阿肉防装改 *	服务器名称/ID	IP地址	操作系统	服务器状态	Agent铁密	防护状态	检测结果	当前版本	服务制度	施路但	操作	
	ecs-ac87 6f153beb-e8f3-46d	9-1 172.16.1.121 (松湖)	Unux	运行中	未安装 安装Agent	◎ 关闭	4 未检測	无			开启防护 切换版本	更多 •
	test-cgs-86206	0-1 172.16.0.8 (私用)	Linux	這行中	未安装	0 %8	9 未检測	无			开启防护 切换版本	更多 •

选择需要切换版本的主机, 单击"切换版本"。

您可以根据自己的实际场景选择"包年/包月"或者"按需计费",为主机切换版本。

● 包年/包月

在"切换版本"对话框中,"计费模式"选择"包年/包月",选择"主机安全版本"、分配"防护配额",如0所示。

切换版本					×		
需要切换版本的朋	段务器列表:						
服务器名称	IP地址		操作系统	当前版本			
ecs-baiyichuan		2.235 (弹性	Linux	企业版			
计费模式	● 包年/包月	() 按	需计费				
主机安全版本	① 企业版	● 旗	舰版				
防护配额	随机选择配额	Į	*	C			
基础版总配额9个,已用配额9个,可用配额9个。							
	配额不足,请	购买配额					

切换为包周期主机安全版本

"防护配额"分配方式:

随机分配:下拉框选择"随机选择配额",系统优先为主机分发服务剩余时间较长的配额。

指定分配:下拉框选择具体配额 ID,您可以为主机分配指定的配额。

批量分配:批量开启防护时,系统会随机为批量选择的主机分配防护配额。



● 按需计费

按需计费暂不支持版本切换,只支持开启企业版主机安全。

单击"确定",切换版本。切换主机安全版本后,请在云服务器列表页面查看主机的"版本/到期时间"。

若目标主机的"版本/到期时间"为切换后的主机安全版本,则表示主机安全版本已切换成功。

● 切换版本后操作

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。

切换版本后,您可将空余的配额分配给其他主机继续使用或退订无需使用的配额,避免造成配额资源的浪费。

2.2 查看主机防护列表

2.2.1 查看企业版/旗舰版防护列表

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在"云服务器"界面,查看服务器的防护状态。

云服务器列表

企业主机安全		主机管理 ⑦ 🔍 🕅	831							l	购买主机业全	告禁遵約公費	手动检测
^{他这} 主机管理		全业项目 所有项目	* C										
风脸预防	•												
入侵位别	*												
高级防御	•	2 云服务器 服务器	组防护配额										
安全运营	-												
安装与配置		全透 开启防护	关闭防护	部署策略	分配到组		8			股房發名称	▼ 请输入关键字	Q 電缆搜索 >	C C
阿茨防要改		服务器名称/ID	IPI的社	操作系统	服务器状态	Agent秘密	防护状态	检测结果	当前版本	服务器组	論感知	授作	
		ecs-ad87 6f153beb-e8f3-46d	9-1 172.16.1.121 (私有)	Linux	运行中	宋安装 安装Agent	0 共同	. 未检測	无			开启防护 切换版本	更多 •
		test-cgs-86206 b70fb7ba-8a67-45	0-1 172.16.0.8 (私用)	Linux	這行中	未安装 安装Agent	0 9:8	() #128	无			开启防护 切换版本	更多 •

🛄 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"、"服务器状态"、"防护计费模式"或者"服务器 计费模式"搜索符合条件的主机。
- 可以单击 [],导出主机列表。

状态说明

参数	说明
Agent 状 态	 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。 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"。
防护状态	 开启: HSS 为该服务器提供全面的主机安全防护。 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。
检测结果	 有风险:主机存在风险。 无风险:主机暂未发现风险。 未检测:主机未开启防护。

2.2.2 查看网页防篡改防护列表

登录管理控制台。

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。 在"网页防篡改 > 防护列表"界面,查看服务器的防护状态。

服务器列表



企业主机安全		防护列表	0									🕞 使用推离	购买用口防装品	2
88		企业项目	形w20日	• C										
工作管理														
入侵吐用	•			Photo ± KD Ma	0			防御分裂	т. 1 с				RADE: WAR	
南级防御 安全运营			Carlanderstern	N39 (12) (10)		1039 WAR		women.cm/		00 0	10 ·		NURCET IN	
安装与配置		开启	968889						0		服务難名称	▼ 请能入兴禄	i∲ Q	С
同页防复改			服务器名称/ID	IP地址	操作系统 🍞	服务器状态	Agent&	\$ 7	Refer D	动态防篡改状态	版本	很作		
MINFER 1			ecs-ac87 6f153beb-e8f3-46d9-90b6-10	172.16.1.121 (松神)	Linux	运行中	末安装		 关闭 	未开启	£	开启防护 防护	AQ最 重要报告	
安铁与配置			test-cgs-86206 b70fb7ba-8a67-45f0-b254-6c	172.16.0.8 (松平)	Linux	运行中	未安装		◎ 关闭	未开启	Æ	开启防护 防护	AR22 查察报告	

状态说明

参数名称	说明
Agent 状态	 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。 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 在该页面查看"离线原因"。
防护状态	 静态网页防篡改的状态。 开启: HSS 为该服务器提供静态网页防篡改防护。 定时关闭: 在"防护设置 > 定时开关设置"可自定义防护时间段,详细操作请参见 2.10.3 定时开启网页防篡改。 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。
动态防篡改状态	 动态网页防篡改的状态。 已开启:在"防护设置 > 动态网页防篡改"可开启动态网页防篡改,详细操作请参见 2.10.4 开启动态网页防篡改。 已开启未生效:动态网页防篡改开启后,请重启 Tomcat 使其生效。 未开启:未开启动态网页防篡改。



2.3 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。

2.3.1 已开启防护的主机风险统计 (最近 24 小时)

主机风险统计 (最近24小时)							
主机资产风险	基线检查	入侵检测	漏洞风险				
0	161 个	483	1 个				
较昨日 → 持平	较昨日 ↑ 26	较昨日 ↑ 482	较昨日 ↑ 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。

2.3.2 主机防护统计 (最近 24 小时)

主机防护状态

主机防护统计 (最近24小时)						
防护/未防护主机	企业版	旗舰版				
0/5	0台	0 台				
全部开启	开启防护	开启防护				

显示用户开启企业版防护、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。

2.3.3 安全风险趋势

安全风险趋势





可显示最近7天、近30天的安全风险趋势。

风险分类	风险事件
资产风险	• 账号信息
	• 开放端口
	• 进程信息
	• Web 目录
	 软件信息
	• 自启动
漏洞风险	• Linux 漏洞
	• Windows 漏洞
	• Web-CMS 漏洞
基线检测	• 口令复杂度策略检测
	• 经典弱口令检测
	• 配置检测
入侵事件	• 账户破解源 IP
	• 异常 Shell
	• 恶意程序

安全风险趋势说明



风险分类	风险事件
	• 高危命令执行
	• 进程异常行为
	• 自启动检测
	• 账户异常登录
	• 提权操作
	• 关键文件变更
	• 高危恶意程序
	• Rootkit 程序
	• 网站后门
	• 风险账户
	• 反弹 Shell

2.3.4 安全运营趋势 (最近7天)



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。

2.3.5 入侵事件统计

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。

如果因为网络原因,没有查询到入侵事件统计结果,可单击 , 重新查询凌晨 12 点统计的数据。

2.3.6 TOP5 风险主机 (最近7天)

TOP5 风险的云服务器 (最近7天)

TOP5风险主机 (最近7天)	С
EPS_Test	I
st st	
HSS-WIN-AutoTest	
HECS_Windows-2012-R2-Datacenter-64bit-	
HSS-TEST	
● 主机资产风险 ● 漏洞风险 ● 入侵检测 ● 基线检查	



基于开启了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。

如果因为网络原因,没有查询到 TOP5 风险主机的统计结果,可单击 [1],重新查询凌晨 12 点统 计的数据。

2.3.7 实时入侵事件

实时入侵事件

实时入侵事件								查看更多 →
告警名称	受影响服务器名称/IP	简述	发生时间 1三	处理时间 ↓=	状态	处理方式	操作	
自启动检测	192.168.1.163	类型:自启动服务,事件类型:新增,名称: S	2021-02-18 14:41:3		未处理		处理	
风险账户	192.168.1.163	账号名:: 用户启动Shell: /bi	2021-02-18 15:28:4		未处理		处理	
账户暴力破解	XXX 	攻击美型:aasdsafda,端囗: 8000,攻击潦IP	2018-11-27 21:53:2	2020-06-26 07:13:	已处理	手动处理	处理	
异地登录	XXX	登录源IP:198.168.23.3,登录用户名:,城	2018-04-10 10:20:0	2020-06-05 11:13:	已处理	忽略	处理	
关键文件变更	XXX	操作:创建,移动到:,是否目录:,文件	2018-08-04 04:06:4	2018-11-27 21:53:	未处理	手动处理	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。

2.4 安全配置

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

登录管理控制台。

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。



2.4.1 配置常用登录地

配置常用登录地后,企业主机安全服务将对非常用地登录主机的行为进行告警。每个主机可被添加 在多个登录地中。

在"常用登录地"页面,单击"添加常用地登录"。

企业主机安全	_	安装与配置 ⑦
总览		
主机管理		企业项目 所有项目 マ C
风险预防	*	
入侵检测	*	2 安装Agent 安全配置 双因子认证 告警通知
高级防御	*	
安全运营	*	
安装与配置 1		
网页防篡改	*	3 常用百茶加 发出日本 学家的时候的 化
		对于来自常用登录地的登录行为,将不会进行异地登录告誓。
		4 添加常用登录地 您还可以添加10个常用登录地。
		常用登录地

添加常用登录地

在弹出的对话框中选择"常用登录地"和"可选云服务器"即可完成配置。

2.4.2 配置常用登录 IP

配置常用登录 IP, 企业主机安全服务将对非常用 IP 登录主机的行为进行告警。

在"常用登录 IP"页面,单击"添加常用登录 IP"。

常用登录 IP



企业主机安全		安装与配置 ②
总览		
主机管理		企业项目 所有项目 ▼ C
风险预防	•	
入侵检测	*	2 安装Agent 安全配置 双因子认证 告警通知
高级防御	*	
安全运营	-	
安装与配置 1	Ŧ	3 常用登录地 常用登录IP SSH登录IP白名单 恶意程序隔离查杀
		对于来自常用登录IP的登录行为,将不会进行异地登录告警。
		◆ 添加常用登录IP 您还可以添加10个常用登录IP。
		常用登录IP

在弹出的对话框中输入"常用登录 IP",在"可选云服务器"列表中选择云服务器。

🗀 说明

"常用登录 IP" 必须填写公网 IP 或者 IP 段。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。

2.4.3 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)和 Centos 8.0及以上版本的主机,SSH 登录 IP 白名单功能对其不 生效。

在 "SSH 登录 IP 白名单"页面, 单击 "添加白名单 IP"。



SSH 登录 IP 白名单

企业主机安全		安装与配置 ⑦
总览		
主机管理		企业项目 所有项目 🔻 C
风险预防	*	
入侵检测	Ŧ	2 安装Agent 安全配置 双因子认证 告答通知
高级防御	*	
安全运营	*	
安装与配置 列页防篡改	•	3 常用登录地 常用登录IP SSH登录IP白名单 恶意程序隔离查杀
		配置了白名单的服务器,只允许白名单内的IP登录到服务器。 启用该功能对请确保将所有需要发起SSH登录的IP地址都加入白名单中。
		④ 添加白名单ⅠP 想还可以添加10个白名单ⅠP。
		白名单IP/IP段 对应服务器数量 (台) 状态 操作

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。

门 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。

2.4.4 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, 更多恶意程序相关内容详情请参见章节中的"入侵检测 > 恶意程序"内容。

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。

恶意程序隔离查杀

企业主机安全		安装与配置 ⑦	购买主机
意思			
主机管理		企业项目 新有项目 * C	
风险预防	Ŧ		
入侵检测	*	安装Agent 🔗 安全配置 双因子认证 告答通知	
高级防御	Ŧ		
安全运营	Ŧ		
安装与配置 1 网页防篡改	Ŧ	3 案用登录地 常用登录P SSH登录P由名単	
		思想程序隔离直关 对印刷出的信门, 木屯, 植士等思考理学, 提供自动现象重杂功能, 单助用户自动印刷处理系统存在的安全风险, 自动现象重要将每可能处学规模, 您可以不在心生式快会全致特心, 入费处验"页面的"已用意文件"页签量看被用意的思考程序, 在 影影型可以比较合动影响学校内不动间面差, 而使希望作。	关闭



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 2.7.2 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。

2.4.5 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

- 已开启"企业版"、"旗舰版"或"网页防篡改版"主机安全防护。
- 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。
- 订阅主题的手机号码或邮箱单次可增加10个,一个主题最多可添加1万个。

操作步骤

在"双因子认证"页面,单击"开启双因子认证"。



双因子认证

安装与配置	3	安装与配置 ②					购买主机安全	御動Agent
总选			2					
主机管理		安装Agent 安全酯	置 / 双因子认证	告譬通知				
风险预防								
入侵检测	Ŧ	4						
高级防御	Ŧ	开启双因子认证 关	制双因子认证 修改	主题		服务器名称	▼ 请输入关键字	QC
安全运营	-	☑ 开启防护服务器名称	操作系统类型	双因子认证状态	验证方式	消息通知服务主题	操作	
安装与配置		3 ecs-hss-002	Linux	◎ 关闭			开启双因子认证 修改主题	
网页防篡改	-							
业主机安全	安装与	RE ()						卸載
业主机安全 ^宽 11 ^倍 理	安装与 _安	配置 ⑦	2 双因子认证	告警通知				卸數
业主机安全 5. 1.管理 全级防 ▼	安装与 安	配置 ⑦	2 双因子认证	告警通知				卸數
业主机安全 き い管理 全预防 ▼ 要位測 ▼	安装与	配置 ⑦ ÆAgent 安全配置	2 双因子认证	告警通知				印動
<u>业主机安全</u> 高 心管理 登別坊 ・ 表社利 ・ 私力例 ・	安装与 安 开	配置 ⑦ 様Agent 安全配置 ③ 歯双因子い近 美術研	2 <u>双因子认证</u> 因子认证 传放王	告替通知		服労務合称	▼ 请输入关键字	河 動 夏 Q
<u> 业</u> 主机安全 志 小管理 全別防 、 大 次 次 の の 、 、 、 、 、 、 、 、	安装与 安:	 配置 ⑦ 英Agent 安全配置 ② 2回双四子以近 关闭双 オ自防炉服务器名称 	2 双因子认证 因子认证 修改主 操作系统类型	告智通知 	检证方式	服务器合称 消息通知服务主	 ▼ 请給入关键字 適給入关键字 	初節 Q
业主初安全 選 引着理 全別防 学院防 、 表 次防御 、 全 ご 、 、 、 、 、 、 、 、 、	安装与 安 一 开 3	 配置 ⑦ 	2 双因子认证 因子认证 修改主 操作系统类型 Linux	告誓通知 	检证方式 	服务器合称 消息避知服务主	 ▼ 请输入关键字 ■ 操作 开启双因子认证 	知恵

在弹出的"开启双因子认证"的对话框中,选择"验证方式"。

● 短信邮件验证

短信邮件验证需要选择消息通知服务主题。

下拉框只展示状态已确认的消息通知服务主题。

如果没有主题,请单击"查看消息通知服务主题"进行创建。

若您的主题里包含多个手机号码/邮箱,在认证过程中,该主题内的手机号码/邮箱都会收到系统发出的验证码短信或邮件。若您只希望有一个手机号码/邮箱收到验证码,请修改对应主题,仅在主题中保 留您希望收到验证码的手机号码/邮箱。

短信邮件验证



开启双因子认证	×					
验证方式 💿 短信邮件验证 🔷 验证码验证						
选择消息通知服务主题						
请选择您的主题 ▼ C 查看消息通知服	段务主题					
温馨提示: 1、下拉框只展示订阅状态为" <mark>已确认</mark> "的消息通知主题。 2、主题添加订阅时,建议使用手机短信方式。 3、开启双因子认证将会修改系统登录文件。						
需要开启双因子认证的云服务器						
弹性服务器名称	双因子认证状态					
host_name_4	关闭					
确定	取消					

验证码验证

验证码验证

开启双因子认证						
验证方式 🔷 短信邮件验证 💿 验证码验证						
直接在登录服务器时输入验证码进行二次验证。 需要开启双因子认证的云服务器						
弹性服务器名称	双因子认证状态					
host_name_4	关闭					
确定	取消					

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。



2.5 主机管理

2.5.1 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。

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 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0所示。

企业主机安全		主机管理 ⑦ 👒 使用描引			狗哭主机安全 告替通知设置 手动检测
总流 主机管理		企业项目 所有项目 * C			
风险预防	*				
入侵检测					
高级防御	*	云服务器 服务器组 防护配额			
安全运营	•	创建服务器组			请输入服务器组名。 Q (
安装与配置					
同而防算改		服务器组	服务器数量	有风险服务器数量	未防护服务器数量 操作
PERMIT		script	0	0	0 編編 题除

进入服务器组页面

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0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。

创建服务器组



创建朋	服务器组			×
* 服务	S器组名称 hss_test			
可选服务	器	λ 关键字 0	已选服务器	
	弹性服务器名称/弹性IP	操作系统	弹性服务器名称/弹性IP	操作系统
	ecs- 10.154.122.235	Linux	ecs-I 10.154.122.235	Linux
	ecs-	Windows		
	ecs-	Linux		
	ecs-	Linux		
	ecs-	Windows		
	ecs-	Windows		
		确定	取消	

设置完成后,单击"确定",完成服务器组的创建。

2.5.2 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。

单击"云服务器",进入云服务器列表界面。

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0所示。

分配到服务器组

云服	云船务器 服务器组 防护配额										
	全选 开启防护 关闭防护	部署策制	8 分配到相					服务器名称	▼ 清埔入关键字	Q 高级搜索 ※	СС
	服务器名称/ID IP地址	操作系统	服务器状态	Agent状态	防护状态	检测结果	当前版本	服务器组	策略组	操作	
	ecs	Linux	运行中	离线	♥ 开启	🕑 无风脸	企业板 配額ID: 56069231-65	ff-4a.		关闭防护 切换版本	更多 ▼
	ecs- ab7ee35d-143b-4	Windows	关机	在线	◎ 关闭	🕑 无风脸	企业版 配额ID: 56069231-65	feeef		开启防护 切换版本	更多 🔻

🗀 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。 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。

2.5.3 相关操作

● 编辑服务器组

- 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。
- 在弹出的对话框中,重新设置分组包含的云服务器。
- 完成修改后,单击"确定",完成服务器组的修改。

● 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。

2.5.4 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

登录管理控制台。

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。



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。

● 创建策略组

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0所示。

企业主机安全	兼略管理 ⑦					
总览						
主机管理	正亚坝目 所有项目 🔻	C				
风险预防 🔻						
入侵检测 🔻	删除					请输入策略组名称
高级防御	策略组名称	ID	描述	支持的版本	关联服务器数	操作
安全运营▲	default_enterprise_policy_group (d07938e2-2953-484f-9f62-beab36	企业版策略组	企业版	0	
策略管理	default_premium_policy_group (59b6e746-5e4c-4e4e-a518-ddfe36	旗舰板策略组	旗舰版	0	复制
安装与配置 网页防复改 ▼	一 平台侧策略组	e2137cef-ac42-47cf-8064-e0a1dd		旗舰版	0	复制 删除

在弹出的对话框中, 输入"策略组名称"和"描述", 如0所示。

门 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。

创建策略组

复制策略组		×
★ 策略组名称		
描述		
	ß	
	确定取消	

单击"确定",将会创建一个新的策略组。

单击已创建的策略组名称,进入策略组的策略页面,如0所示。



策略组策略

策略	管理 / default_enterprise_policy_	group			
					С
	策略名称	状态 🍞	功能类别	支持的操作系统	操作
	弱口令检测	已启用	基线检查	Linux, Windows	关闭
	系统配置检测	未启用	安全加固	Linux	开启
	网站后门检测	已启用	入侵检测	Linux, Windows	关闭
	提权检测	已启用	入侵检测	Linux	关闭
	反弹/异常Shell检测	未启用	入侵检测	Linux	开启
	SSH白名单	未启用	入侵检测	Linux, Windows	开启
	文件完整性管理	已启用	入侵检测	Linux	关闭
	资产管理	未启用	资产管理	Linux, Windows	开启
	高危命令检测	已启用	数据采集	Linux	关闭

单击策略名称,修改具体的策略内容,详细信息请参见 2.9.2 修改策略内容。

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。

部署策略

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。 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0所示。

部署策略

云服务	器 服务器组 防护面	己載页									
	主选 开启防护 关闭防护	部署策略	分配到组					服务器名称	▼ 清编入关键字	Q 高级搜索 >	СС
	服务器名称/ID IP地址	操作系统	服务器状态	Agent状态	防护状态	检测结果	当前版本	服务器组	策略组	操作	
	ecs	Linux	运行中	寬純	♥ 开启	⊘ 无风脸	企业版 配额ID: 56069231-65ft	-4a		关闭防护 切换版本	更多 •
	ecs- ab7ee35d-143b-4	Windows	关机	在线	◎ 关闭	✓ 无风脸	企业版 配額ID: 56069231-65fe	seef		开启防护 切换版本	更多 🗸
	ecs- ab7ee3ff5d-143b-	Linux	创建中	未安装 安装Agent	⊘ 开启	🕗 无风脸	企业版			关闭防护 划换版本	更多 🗸

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。

选择策略组



		×
🛕 您确定要在已	开启旗舰版的服务器上部署策略吗?	
请选择要部署的策略组	default_premium_policy_gr 🔻	
	确定取消	

🛄 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。

2.6风险预防

2.6.1 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。

2.6.1.1 检测周期

账号信息管理、开放端口检测:实时检测。开放端口检测结果每6小时刷新一次统计数据。 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。

2.6.1.2 查看主机中的资产信息

登录管理控制台。

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。



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。

企业主机安全 	资产管理 ⑦
总览	
主机管理	企业项目 所有项目 マ C
风险预防	
资产管理 1	
漏洞管理	账号信息管理 开放端口检测 进程信息管理 Web目录管理 软件信息管理 自启动
基线检查	
入侵检测 🔻	实时账号数据 历史变动记录
高级防御	
安全运营	
安装与配置	账号名
网页防复改	root

资产管理

2.6.1.3 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、管理员权限或用 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。若发现系统中有不必要的多余账号,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。

2.6.1.4 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。



2.6.1.5 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。

2.6.1.6 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。

2.6.1.7 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。

2.6.1.8 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。

2.6.2 漏洞管理

2.6.2.1 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。

2.6.2.2 检测原理

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。
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。

门 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。

2.6.2.3 漏洞库更新周期

HSS 实时获取官方发布的漏洞信息,并更新到漏洞库中。

2.6.2.4 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。

2.6.2.5 前提条件

已开启"企业版"、"旗舰版"或"网页防篡改版"主机防护。

2.6.2.6 Linux 软件漏洞/Windows 系统漏洞

登录管理控制台。

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。

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0所示。

查看 Linux 软件/Windows 系统漏洞检测结果



Linux软件漏洞管理 Windows系统	漏洞管理 Web-CMS	漏洞管理				
服务器统计 (Linux软件漏洞)		TOP5	5服务器(Linux软件源	ā洞)		
10台	■ 未开屆检測 ■ 无紧急漏洞 ■ 有紧急漏洞	1 	ТОР1 Тор2	Тор3	тор4	Top5
忽略 取消忽略				所有修复紧急度	▼ 请输入漏洞名称	
漏洞名称	修复紧急度	未处理服务器(台)	历史受影响服务器(台)	解决方案		操作
CESA-2019:1481 (kernel security	🧜 可延后修复	9	2	修复建议请参见: RHS	A-2017:3081	修复

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。

Linux软件廠詞管理 / CESA-2019:1481 (kernel socurity update)							
漏洞信息影响服务	12 67						
基本信息							
漏洞名称	CESA-2019:1481 (kernel se	curity update)	状态		😚 需尽快修复		
未处理服务器	1		历史受影响服务	譒	2		
解决方案							
undefined 修复建议链接: https://access.	redhat.com/errata/RHSA-2017:3	081					
漏洞CVE						请输入CVE ID	QC
CVE ID	CVSS分值	披露时间		漏洞描述			
CVE-2019-11477	7.8	2019-06-18 00:00:00 GMT+08:	00	Jonathan Looney was subject to an Selective Acknowl denial of service. T 4.14.127, 4.19.52, 3b4929f65b0d824	discovered that the integer overflow in t edgments (SACKs). This has been fixed i 5.1.11, and is fixed 9f19a50245cd88ed	TCP_SKB_CB(skb)->tcp_g the Linux kernel when hand . A remote attacker could us in stable kernel releases 4.4 in commit I1a2f78cff.	so_segs value ling TCP ee this to cause a l.182, 4.9.182,

漏洞信息

查看漏洞影响的服务器,在该页面,您可以对漏洞进行处理。

影响服务器

漏洞信息影响服务器			
忽略 取消忽略	验证	所有状态 🔻 请	前入服务器名称 Q C
受影响服务器名称	状态	软件信息	操作
CentOS7.1	未处理	bash11.1;openssl12.34	忽略 修复 验证
CentOS7.222	已忽略	bash11.1;openssl12.34	取消忽略

- 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。

2.6.2.7 Web-CMS 漏洞

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"Web-CMS漏洞管理"页面,如0所示。

查看 Web-CMS	漏洞检测结果
------------	--------

企业主机安全		漏洞管理 ⑦
总宽		
主机管理		Linux软件漏洞管理 Windows系统漏洞管理 Web-CMS漏洞管理
风险预防	*	
资产管理		服务器统计 (Web-CMS漏洞) TOP5服务器 (Web-CMS漏洞)
漏洞管理		
基线检查		
入侵检测	*	
高级防御	*	100日 100日 100日 100日 100日 100日 100日 100日
安全运营	*	Addax
安装与配置		
阿贝防 最成	Ŧ	
		漏洞名称 修复紧急度 未处理服务器(历史受影响服务器(台) 解决方案

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。

漏洞详细信息



b-CMS漏洞管理 / wordpre	855		
美利信息 影和	自服务譜		
基本信息			
漏洞名称	wordpress	状态	可延后修复
未处理服务器	2	历史受影响服务器	2
解决方案			
目前厂商已没布升级补 undefined	丁以修复漏洞,补丁获取链接:https://wo	rdpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/	
漏洞详情			
被重时间		漏洞描述	
2020/03/30 02:16:07 G	MT+08:00	WordPress 4.9.2及之前版本中存在安全属间。攻击者可遵 (资源消耗) 。	过使用较大的registered js文件列表,创建请求来多次加载文件利用读意深造成拒绝服务
2020/03/30 02:49:07 GI	MT+08:00	WordPress 4.9.2及之前版本中存在安全漏洞。攻击者可通 (资源编书)。	过使用较大的registered js文件列表,创建请求来多次加载文件利用读篇测道成把绝服务

受影响的服务器

漏洞信息	影响服务器				
忽略	取肖忽略			所有状态	▼ 请输入II
폋	影响服务器名称	状态	路径		操作
C	entOS7.1	未处理	bash11.1;openssl12.34		忽略
Ce	entOS7.222	已忽略	bash11.1;openssl12.34		取消忽略

2.6.2.8 导出漏洞报告

在漏洞列表的右上角,单击 [],导出漏洞报告。

须知

• HSS 支持导出 5000 条漏洞数据,超出的部分数据将无法导出。

例如: HSS 检测到两个漏洞 P1 和 P2, P1 漏洞存在于 N 台主机中, P2 漏洞存在于 M 台主机中, 在 导出漏洞报告时,则为 N+M 条漏洞数据。

报告是展示了全部主机的安全情况,因此导出的漏洞报告是全部主机的报告,不支持只导出单台主机报告。

2.6.2.9 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。

2.6.2.10 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。

2.6.2.11 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。

2.6.2.12 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。

2.6.2.13 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。

登录管理控制台。

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。 进入"漏洞管理"页面,单击"修复",进入影响服务器页面,如0所示。

修复漏洞



企业主机安全	3	剥管理 ⑦							
 息克 主机管理 风险预防 1 		3 Linux软件履用管理 Windows系统	充漏洞管理	Web-CMS漏洞管理					
 労产管理 展行管理 基核检查 入侵检影 電磁防衛 安全运費 安装与配置 空装与配置 	*	服务器统计(Linux软件漏洞) 33台	★开启检测 无紧急端间 有紧急端间		TOP5服务器 1 0	(Linux软件漏)	同) TOP1		
P1348/3866		忽略 取消忽略			所有修复紧急	<u>چ</u> •	请输入漏同名称	QĽ	С
		漏洞名称	修复紧急度	未处理服务器(历史受影响服务器((台) 解决方案		操作	
		CESA-2019:1481 (kernel security	🚺 電尽快修复	1		1 Update the a 修复建议请参	iffected kernel packages. 见:CESA-2019:1481	4 惨复	
		CESA-2017:1680 (bind security up	() 可延后修复	1		Update the a 修复建议请参	ffected bind packages. 见: CESA-2017:1680	修复	

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0所示。

一键修复漏洞

漏洞信息 ① 影响服务器							
忽略 取消忽略	3 ──键修复 验证	۶	有状态 ▼	请输入服务器名称	QC		
■ 受影响服务器名称	状态	软件信息		操作			
2 CentOS7.1	未处理	bash11.1;openssl12.34		忽略 修复 验证			
CentOS7.222	已忽略	bash11.1;openssl12.34		取消忽略			
CentOS7.222	验证中	bash11.1;openssl12.34		忽略 修复 验证			

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"。

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"修复完成后需要手动重启,否则 HSS 仍可能为您推送漏洞消息。

Windows 系统漏洞修复重启后, 您还需要在控制台单击已重启, 确认主机已重启。

2.6.2.14 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0。



- 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"修复完成后需要手动重启,否则 HSS 仍可能为您推送漏洞消息。

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。

门 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。

2.6.2.15 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。

2.6.2.16 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。

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	emergesearch 软件名称
SUSE	zypper search -dCmatch-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。

2.6.3 基线检查

2.6.3.1 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。



2.6.3.2 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。

2.6.3.3 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。

2.6.3.4 检查项列表

检查项列表

检查项	说明
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。
口令复杂度策略检 测	检测系统账号的口令复杂度策略。
配置检测	根据 CIS 标准并结合多年最佳安全实践进行检测。 目前支持的配置检测类型有:Tomcat、SSH、Nginx、 Redis、Apache2、MySQL5。

2.6.3.5 操作步骤

登录管理控制台。



在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 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。

基线检查结果

企业主机安全 	基线检查 ⑦
总览	
主机管理	企业项目 所有项目 🔹 С
风险预防 1 🔺	
资产管理 品	<u> </u>
漏洞管理 🛆	口令复杂度策略检测 经典弱口令检测 配置检测
基线检查 2	
入侵检测 🔻	
高级防御	弹性服务器名称 当前设置

2.6.3.6 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。

门 说明

不支持对单个云服务器执行导出。

2.6.3.7 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。

● 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(企业版和旗舰版)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。



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

● 修改 Linux 主机中口令复杂度策略的详细操作请参见 3.3.6 如何在 Linux 主机上安装 PAM 并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 3.3.7 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(企业版和旗舰版)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。

配置检测报告

こ 美天 む

配置检测报告		×
规则描述: /etc/ssh/sshd_config文作 根据:	牛包含sshd的配置内容。	
审计描述: 运行以下命令并验证Uid和 #stat /etc/ssh/sshd_con Access: (0600/-rw	□Gid都是0/root,Access [;] fig ·) Uid: (0/ root) Gid: (0/	不向组或其他组授予权限: root)
修改建议: 运行以下命令设置/etc/ss #chown root:root /etc/s #chmod og-rwx /etc/ss	h/sshd_config的所有权和 ssh/sshd_config h/sshd_config	权限:
检测用例信息:		
检测描述	期望结果	检测结果
确保所有者和组都是r	root:root 0600 or stri	root:root 0644
	确定	

● 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(企业版和旗舰版)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。



2.7 入侵检测

2.7.1 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。

2.7.1.1 告警事件列表说明

告警名称	告警说明	企业 版	旗舰 版	网页防 篡改版
账户暴力 破解	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。 检测 SSH、RDP、FTP、SQL Server、 MySQL 等账户遭受的口令破解攻击。 • 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	V	\checkmark	\checkmark
	攻击默认拦截 24 小时。 • 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。			
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。 • 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	√	√	\checkmark



告警名称	告警说明	企业 版	旗舰 版	网页防 篡改版
	 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"。 若在非常用登录地登录,则触发安全事件告警。 若账户暴力破解成功,登录到云主机,则触发安全事件告警。 			
恶意程序 (云查 杀)	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。 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。 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。 说明 恶意程序(云查杀)检测功能仅支持检测运行中的 恶意程序。	√ (隔 査 杀)	√ (隔离 査 杀)	√ (隔离 査杀)
进程异常 行为	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。 对于进程的非法行为、黑客入侵过程进行告 警。 进程异常行为可以监控以下异常行为: • 监控进程 CPU 使用异常。 • 检测进程对恶意 IP 的访问。 • 检测进程并发连接数异常等。	V	V	\checkmark
关键文件 变更	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。 • 对系统关键文件 (例如: ls、ps、login、	\checkmark	\checkmark	\checkmark



告警名称	告警说明	企业 版	旗舰 版	网页防 篡改版
	 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关键文件变更监控路径。 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"。 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。 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	以 php、jsp 等网页文件形式存在的一种命令 执行环境。 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。 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。 • 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。 • 您可以使用手动检测功能检测主机中的网站 后门。	√	\checkmark	\checkmark
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。	×	\checkmark	\checkmark



告警名称	告警说明	企业 版	旗舰 版	网页防 篡改版
	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。			
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。	×	\checkmark	\checkmark
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。	×	\checkmark	\checkmark
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。	×	\checkmark	~
风险账户	黑客可能通过风险账号入侵主机,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。	\checkmark	V	√
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。	×	\checkmark	\checkmark



告警名称	告警说明	企业 版	旗舰 版	网页防 篡改版
	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: •利用 SUID 程序漏洞进行 root 提权。 •利用内核漏洞进行 root 提权。 •对文件的提权。			
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。 • 使用文件特征码检测 Rootkit。 • 对隐藏文件、端口、进程的检测。	×	\checkmark	V

2.7.1.2 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/lsmod
	/bin/pidof
	/bin/lsof
	/bin/ss
usr	/usr/bin/ls
	/usr/bin/ps
	/usr/sbin/ps



类型	Linux
	/usr/bin/bash
	/usr/bin/netstat
	/usr/sbin/netstat
	/usr/sbin/rsyslogd
	/usr/sbin/ifconfig
	/usr/bin/login
	/usr/bin/find
	/usr/sbin/lsmod
	/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
sbin	/sbin/syslog-ng
	/sbin/rsyslogd
	/sbin/ifconfig
	/sbin/lsmod
	/sbin/pidof



2.7.2 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、已处理告警事件、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"。

2.7.2.1 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。

2.7.2.2 查看告警事件

登录管理控制台。

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。 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0所示。

企业主机安全		事件管理 ⑦					文件隔离箱	购买主机安全
总范主机管理		企业项目 所有项目	* C					
入侵检测	•	安全告警统计						
白名单管理 凸		存在告留的服务器	0	待处理告答事件	0	已处理告警事件		0
高级防御	•	已拦戦」の	0	已隔离文件	0			
安全运营	*							
安装与配置		助护未完全开启,无法拦截所	有威胁,建议您升级企业版或更高牌	反本开通全部防护,保护您的云上资	严。立即升级			۸
阿贝防囊改	Ť	(2) 日开周防护 (2)	暴力表解 〇 所户异常登录	② 未开启防护 (11)	品 恶音程序(云重杀) 品 反導shell 品 风险账户 品 风险账户	 	△ 关键文件变更 △ ⑦ △ 自启动检测	网站后门
		告營事件列表						
		全部 100	点击上方"已拦截10",同	可查看攻击IP是否被拦截,以及可以	解除拦截。 最近24	小时 ▼ 服务器名称 ▼	受影响服务器名称/IP	QC
		账户暴力破解 50	告告名称 受影响服务	器器名称/IP 简述	发生时	问 1Ξ 处理时间 1Ξ	秋志 🍞 处理方式	0 操作
		账户异常登录 10	自启动检测 192.168.1.	#型:自启动服务, 163	事件类型: 新增 2021-0	12-18 14	未处理	处理
		思惑程序 (云重杀) 0	风险账户 192.168.1.	163 账号名:	. 用户启动5 2021-0	12-18 15	未处理	处理

事件管理

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 参见处理告警事件。
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",可查看已拦截的 IP 地址列 表。 已拦截 IP 列表展示"服务器名称"、"攻击源 IP"、"攻击类 型"、"拦截次数"、"开始拦截时间"、"最近拦截时间"、 "拦截时长"和"拦截状态"。 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。 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。
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, 您可以根据自己的需 要进行一键恢复处理, 关于文件隔离箱的详细信息, 请参见 2.7.3 管理文件隔离箱。

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0 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。

告警事件统计数量



告警事件列表									
全部	75			最 点击上方"已拦截IP",可查看	丘24小时 ▼ 攻击IP是否被拦	服务器名	你 ▼ 受影W 解除拦截。	服务器名称/IP	QC
账户暴力破解	0	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
账户异常登录	0	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
恶意程序 (云查杀)	0	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
进程异常行为	0	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
天键文件受更 网站后门	0	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
反弹Shell	0	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
异常Shell	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件夹,	2020-12		未处理		处理
高危命令执行	0	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	75	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件夹,	2020-12		未处理		处理
提权操作	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件夹,	2020-12		未处理		处理
Rootkit程序	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件夹,	2020-12		未处理		处理

单击告警列表中的告警名称,可查看告警的详细信息,如0所示。

告警详细信息

					自启动检	测 处理 ×
全部	75				服务器名称	ecs
1 HP				□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	IP地址	192.168.1.130
账户暴力破解	0	告警名称	受影响服务器名称/IP	简述		
账户异常登录	• 2	自启动检测	ecs- 192.168.1.130	美型:自启动服务,	服务名	S98denyhosts
恶意程序 (云查杀)	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件	路位	/etc/rc.d/rc3.d/S98denyhosts
进程异常行为	0	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件	<u></u> 事件类型	
关键文件变更	0	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件	运行用户	
反弹Shell	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件	文件HASH	e54ac02e06dea5c51a6f922c4c323e337b2bac0ca90c1b9ba79f4fa89b
异常Shell	0	自启动检测	ecs-8285-windows 192.168.1.209	美型:开机启动文件	状态	未处理
高危命令执行	0	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件		
自启动检测	75	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件		
提权操作	0	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件		
Rootkit程序	0	自启动检测	ecs-8285-windows 192.168.1.209	类型:开机启动文件		



2.7.2.3 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。

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在左侧导航栏,单击"入侵检测 > 事件管理",进入事件管理页面。

2业主机安全	획	軒件管理 ⑦										文件隔离箱		购买主机安
10、 主机管理 2162701*		企业项目 所有项目		* C										
- 便检测 - 要件管理	*	安全告警统计												
白名单管理 凸		存在告替的服务器			0	待处理告警	事件		0	已处罚	豊告啓事件			0
级防御	-	已拦截回			0	已隔高文件			0					
全运营														
装与配置		助护未完全开启, 矛	法拦截所有	威胁, 建议您升级企	业版或更高版	本开通全部防持	户,保护您的云上资7	"。立即升级						
贝防装改	•	\bigcirc	☞ 账户暴	力破解	异常登录		\bigcirc	品 恶意程序 品 反弹Shel	(云亶杀) [合 月	品 进 第Shell	提昇常行为 合 高危命令执行 合 高危命令执行	关键文件变更	 品 网 助检測 	站后门
		已开启防护(2)					未开启防护 (11)	品 风险账户	△撮	权操作	合 Rootkit程序			
		告警事件列表												
		全部	100	点击上方"日	已拦截IP*,可	「查看攻击IP是	香被拦截,以及可以!	聯拦截。	最近24月	ধ্য 🔻	服务器名称 ▼	受影响服务者	始称/IP C	C
		账户暴力破解	50	告罄名称	受影响服务	器名称/IP	简述		发生时间	1Ξ	处理时间↓Ξ	秋志 77	处理方式	操作
		账户异常登录	10	自启动检测	192.168.1.1	63	美型:自启动服务,	事件类型:新增	2021-02-	18 14		未处理		处理
				风险账户	102 168 1 1	63	账号名:	,用户启动5	2021-02-	18 15		未处理		处理

事件管理

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0所示, 处理方式如0所示。

门 说明

您也可以单击告警名称所在行的"处理",处理告警。

处理告警事件



告警事件列表											
全部	175	批量处理]		点击上方	最近24小时 "已拦截IP",可查	▼ 月 看攻击IP是否被	服务器名称 [拦截,以及可]]	▼ 受影响服行 以解除拦截。	S器名称/IP	QC
账户暴力破解	143	✓ 告警	名称 2	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
账户异常登录	3	☑ 进程	异常行为	ecs-hss-002 192.168.0.67	哈希值;	4845dbb7c2e3e	2020-08		未处理		处理
恶意程序 (云童杀)	0	☑ 进程;	异常行为	ecs-hss-002 192.168.0.67	哈希值。	4845dbb7c2e3e	2020-08		未处理		处理
进程异常行为	5	☑ 进程	异常行为	ecs-hss-002 192.168.0.67	哈希值。	4845dbb7c2e3e	2020-08		未处理		处理
大键文件变更	0	☑ 进程	异常行为	ecs-hss-002 192.168.0.67	哈希值:	4845dbb7c2e3e	2020-08		未处理		处理
反弹Shell	0	☑ 进程	异常行为	ecs-hss-002 192.168.0.67	哈希值。	4845dbb7c2e3e	2020-08		未处理		处理
异常Shell	2										
高危命令执行	0										
自启动检测	7										
风险账户	14										
提权操作	0										
Rootkit程序	0										

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。

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	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 2.7.3 管理文件隔离箱。
	有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
	说明
	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。



处理方式	处理方式说明		
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。		
加入登录 白名单	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。 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。		
加入告警 白名单	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。 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。 • 反弹 Shell • Webshell 检测 • 进程异常行为检测 • 进程提权 • 文件提权		

告警处理建议

告警名 称	告警参数说明	处理建议
账户暴 力破解	 服务器名称:云服 务器的名称。 IP 地址:受影响服 务器的 IP 地址。 	该告警事件需要您高度重视。 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:
	 攻击源 IP:攻击主机的 IP 地址。 攻击类型:可拦截 	 系统存在弱口令,同时正在遭受暴力破解攻击。 数次口令输错(但未达到封禁源 IP 条件)后



告警名 称	告警参数说明	处理建议
	 的攻击类型,包含 mysql、mssql、 vsftp、filezilla、 serv-u、ssh、 rdp。 尝试破解次数:被 尝试破解的次数。 状态:处理告警事 件的状态,"已处 理"或者"未处 理"。 	成功登录。 建议您立即确认源 IP 是否是已知的合法 IP。 • 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。 • 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。 1. 建议您将该事件标记为"手动处理"。 2. 立即登录系统并修改并设置安全的账户密 码。 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。 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。
账户异 常登录	 服务器名称:云服 务器的名称。 IP 地址:受影响服 务器的 IP 地址。 攻击类型:攻击的 类型,包含 mysql、mssql、 vsftp、filezilla、 serv-u、ssh、 rdp。 端口:被攻击的端 口。 主机:攻击者的 IP 	 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。 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。 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。



告警名 称	告警参数说明	处理建议
	地址。 • 用户名:攻击者的 用户名。 • 状态:处理告警事 件的状态,"已处 理"或者"未处 理"。	
恶意程 序 (云 査杀)	 服务器名称:云服务器的名称。 IP地址:受影响服务器的 IP地址。 恶意程序的 IP地址。 恶程序的路径。 哈希值:哈希值。 文件限。 这行序的启动的时间。 程序启动的时间。 状态,"已处理"。 	 若检测出存在恶意程序,建议您立即对该程序进行确认: 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。 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。 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。 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。 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。
进程异 常行为	 服务器名称:云服 务器的名称。 IP 地址:受影响服 务器的 IP 地址。 疑似恶意程序路 	若检测出进程异常行为,建议您立即对该进程进行确认: • 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。



告警名 称	告警参数说明	处理建议
	 径:疑似恶意程序的路径。 文件权限:文件的权限。 PID:进程ID。 命令行:启动异常进程的命令行。 父进程 PID:父进程的进程ID。 父进程和的花客路径。 行为:该异常进程的行为,例如:高CPU。 连接数: CPU使用频率:CPU的使用频率。 状态:处理告警事件的状态,"已处理"或者"未处理"。 	 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。 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。 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。 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。
关键文件变更	 服务器名称:云服 务器的名称。 IP地址:受影响服 务器的IP地址。 操作:对关键文件 执行的操作。 文件路径:被操作 的关键文件的路 径。 	若检测出关键文件变更,建议您立即对该变更进 行确认: • 若合法,您可以"忽略"该告警。 • 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。



告警名 称	告警参数说明	处理建议
	 移动到:移动到的路径。 是否目录:操作的是否是目录, "true"或者"false"。 状态:处理告警事件的状态,"已处理"或者"未处理"。 	
冈站后	 服务器名称:云服务器的名称。 IP地址:受影响服务器的IP地址。 木马文件路径:木马所在的文件路径。 发现时间:发现的时间。 状态:处理告警事件的状态,"已处理"或者"未处理"。 	若检测出网站后门,建议您立即确认该文件是否 合法。 • 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。 • 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。
反弹/异 常 Shell	 服务器名称:云服 务器的名称。 IP 地址:受影响服 务器的 IP 地址。 文件路径:文件的 路径。 详情:详情。 状态:处理告警事 	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。 • 若合法,您可以"忽略"该事件。 • 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。



告警名 称	告警参数说明	处理建议
	件的状态,"已处 理"或者"未处 理"。	
高危命令执行	 服务器名称:云服务器的名称。 IP地址:受影响服务器的IP地址。 哈希值:哈希值。 PID:进程的ID。 进程路径:进程的路径。 进程和命令:机行该进程和的合令。 父进程PID:父进程的ID。 父进程APID:父进程的ID。 父进程和名:父进程的APID。 父进和命令:执行父进程的命令。 父进和命令:点话的月上。 会话用户名:会话的用户名。 运行用户:运行的用户。 状态:处理告警事件的状态,"已处理"或者"未处理"。 	 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。 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。 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。
自启动 检测	 服务器名称: 云服 务器的名称。 IP 地址: 受影响服 	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。 • 若合法,您可以"忽略"该事件;或者"加入



告警名 称	告警参数说明	处理建议
	 务器的 IP 地址。 服务名:自启动服 务的名称。 路径:自启动服务 的路径。 数型:自启动的类型。 事件类型:事件的类型。 事件类型:事件的类型。 运行用户:运行的用户。 文件 HASH:文件的HASH。 状态:处理告警事件的状态,"已处理"或者"未处理"。 	告警白名单",该告警将不会再次触发。 • 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。
风险账户	 服务器名称: 云服 务器的名称。 IP 地址: 受影响服 务器的 IP 地址。 账号名: 风险账号 的名称。 用户组: 风险账号 所在的用户组。 UID/SID: UID/SID。 用户目录: 用户的 目录。 用户启动 Shell: 田户启动的 	 若检测出风险账号,建议您立即确认该账号是否合法。 若合法,您可以"忽略"该事件。 若不合法,请将该事件标记为"手动处理",建议执行以下操作: 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。 限制账号权限 通过限制关键配置项,限制非管理员的文件访问权限和文件修改权限,防止未授权


告警名 称	告警参数说明	处理建议
	Shell。 • 状态: 处理告警事 件的状态, "已处 理"或者"未处 理"。	的访问权限和使用操作。
提权操作	 服务器名称:云服 务器的名称。 IP地址:受影响服 务器的IP地址。 提权方式:提权的 方式。 提权文件路径:提 权文件的路径。 状态:处理告警事 件的状态,"已处 理"或者"未处 理"。 	若检测出提权操作,建议您立即确认该提权操作 是否合法。 • 若合法,您可以"忽略"该事件。 • 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。
Rootkit 程序	 服务器名称:云服 务器的名称。 IP地址:受影响服 务器的 IP地址。 Rootkit名称: Rootkit 的名称。 子模块名称:子模 块的名称。 特征:Rootkit程 序特征。 状态:处理告警事 件的状态,"已处 理"或者"未处 理"。 	若检测出 Rootkit 程序安装,建议您立即确认该 Rootkit 安装是否合法。 • 若合法,您可以"忽略"该事件。 • 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。



2.7.3 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
- 2.7.3.1 选择隔离查杀

登录管理控制台。

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。 在左侧导航栏,单击"入侵检测 > 事件管理",进入事件管理页面。

事件管理

企业主机安全		事件管理 ⑦	文件詞篇稿
总览 主机管理 风险预防	÷	全起项目 (C)	
入侵检测	•	安全件整统计	
白名单管理 品		存在告留的服务器 0 待处理告留事件	0 已处理告答事件 0
高级防御	*	已搭創19 0 已隔面文件	0
安全运营	*		
安装与配置		助护未完全开启,无法拦截所有威胁,建议您升级企业贩或更高级本开通全部防护,保护	思约云上资产。立即升级 余
阿贝防蓑政	·	◎ 日开創坊户 (2) ● 照户職力収解 ● 照户開発登录 未开指	() 高 思想年年(正型所) () 正程序和行力 () 天規文件交更 ()
		告營事件列表	
		点击上方"已拦截IP",可查看攻击IP是否被拦截 全部 100	. 以及可以编辑任義。
		告密名称 受影响服务器名称/IP 前述	双生时间 1三 处理时间 1三 状态 7 处理方式 操作
		■ 日本の公式 (中国) (日本の) (日本) (日本の) (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本	I田动服务,事件类型:新道 2021-02-18 14 未处理 处理
		思想程序(云重杀) 0 风险策冲 192.168.1.163 账号名	, 用户启动5 2021-02-18 15 ·· 未处理 ·· 处理

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0所示。

隔离查杀



警事件列表								
全部	175	批量处理		最近30天 点击上方"已拦截IP",可查	▼ 服务器名称 着攻击IP是否被拦截,以及可	▼ 受影响!!	服务器名称/IP	QC
账户暴力破解	143	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
账户异常登录	3	进程异常行为	ecs-hss-002 192.168.0.67	哈希值:4845dbb7c2e3e	2020-08	未处理	2	处理
恶意程序 (云查杀)	0							处理
进程异常行为	5	1 处理告警事件				×		24.70
关键文件变更	1	告警名称	状态	IP地址	简述			SCHE
网站后门	0	进程异常行为	未处理	192.168.0.67	哈希值:4845dbb7c2	e3e064d		处理
反弹Shell	0	处理方式	 手动处理 約 程序无法执行"该/写"操作 	39路 加入告答白名单 同时该程序的进程将被立即终端。	 隔离查杀 3 			处理
异常Shell	2			确认取消				
高危命令执行	0							

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。

2.7.3.2 查看文件隔离箱

在"事件管理"页面,单击"文件隔离箱",弹出文件隔离箱页面。

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0所示。

文件隔离箱				
服务器名称	路径	修改时间	操作	
yhfg	/hjfjdsojfa	2018-11-27 21:53:20 GMT+08:00	恢复	
yhfg	/hjfjdsojfa	2018-11-27 21:53:20 GMT+08:00	恢复	
yhfg	/hjfjdsojfa	2018-11-27 21:53:20 GMT+08:00	恢复	

文件隔离箱

2.7.3.3 一键恢复

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。

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。



2.7.4 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。

2.7.4.1 添加告警白名单

添加告警白名单

添加方式	说明
加入告警白 名单	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 2.7.2 查看和处理入侵告警事件。 以下类型的告警事件加入"告警白名单": • 反弹 Shell • Webshell 检测 • 进程异常行为检测 • 进程提权 • 文件提权 • 高危命令 • 恶意程序
导入告警白 名单	在"告警白名单"页面,导入告警白名单列表。

2.7.4.2 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。

登录管理控制台。

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。



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0所示。

告警白名单列表

告警白名单 登录白	名单						
导入 导出全部	影除			全部类型	▼	(a c
告馨类型	SHA256	cmdLine	数据来源		标记时间↓Ξ	操作	
账户暴力破解	47b320e30bd9f4ebc64675	3000XX	文件导入		2018-11-27 21:53:20 GMT+08:00	删除	
异地登录	47b320e30bd9f4ebc64675	30000X	文件导入		2017-12-15 16:33:20 GMT+08:00	删除	
异地登录	47b320e30bd9f4ebc64675	X000X	文件导入		2018-10-24 04:33:20 GMT+08:00	删除	

2.7.4.3 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。

登录管理控制台。

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。

进入"白名单管理"页面,选择"告警白名单",如0所示。

选择告警白名单

企业主机安全		白名单管理 ⑦					购买主机安全
总宽 主机管理		企业项目 所有项目	• C				
风险预防	*						
入侵检测 1		<u> </u>					
事件管理		告警白名单 登录白	名单				
白各单管理 2		4	1				
高级防御	*	导入导出全部	制除			全部类型 ▼ 哈希(SHA25 ▼ 清緬入	关键字搜索 Q C
安全运营	٠	告察类型	SHA256	cmdLine	数据来源	标记时间 ↓Ξ	操作
安装与配置		账户暴力破解	47b320e30bd9f4ebc64675	X0000X	文件导入	2018-11-27 21:53:20 GMT+08:00	删除
网页防复改	-	异地登录	47b320e30bd9f4ebc64675	X0000X	文件导入	2017-12-15 16:33:20 GMT+08:00	删除



- 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。

2.7.4.4 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。

2.7.5 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。

🛄 说明

如果将已经产生告警的目标 IP 通过添加登录告警白名单方式加入白名单,加入白名单之后的检测会对目标 IP 进行 忽略,但已经产生的告警不会自动放行,仍需对告警进行处理,处理详情请参见 2.7.2 查看和处理入侵告警事件。

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 2.7.2 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。

2.7.5.1 添加登录告警白名单

登录管理控制台。



在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"白名单管理"页面,选择"登录白名单",单击"添加",如0所示。

企业主机安全	白名单管理 ⑦	
总览		
主机管理	企业项目 所有项目 🔻	C
风险预防 🔹		
入侵检测 1 · · · · · · · · · · · · · · · · · ·	3 告警白名单 登录白名单	
 □ 白名単管理 2 高级防御 	4 添加 删除	
安全运营 ▼	服务器IP地址	登录IP
安装与配置).207	.66
网页防复改 ▼	207	.66

登录白名单

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0 所示。

门 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。
- "服务器 IP" 和 "登录 IP" 支持最大长度为 128 字节。

添加登录安全白名单



添加登录安	全白名单	×
★ 服务器IP	192.168.1.1	
<u>★ 登</u> 录IP	192.168.1.2	
* 登录用户名	hss-test	
	确认 取消	

单击"确认",完成登录白名单的添加。

2.7.5.2 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。

2.8 高级防御

2.8.1 程序运行认证

2.8.1.1 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

登录管理控制台。

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。 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0所示。

查看白名单策略列表

企业主机安全		程序运行认证 🤏 💈	流程介绍				文件隔离精	购买主机安全
总览 主机管理		企业项目 所有项目	•	C				
风险预防	*							
入侵检测	Ŧ							
高级防御	*	事件管理 生活	效服务器 白名	单策略				
程序运行认证		创建策略					请输入策略名称	QC
XIT76BIED/E		策略名称	已生效服务器	状态	应用数	策略状态	操作	
勤 新新 病 毒防 护 安全运营	Ŧ	policy1	0	⇔ 学习中	可信 1 不可信 2 未知 3		编辑 删除	
安装与配置		policy2	0	🍄 学习完成,策略未生效。			编辑 删除	
网页防篡改	*	policy3	0	✓ 学习完成,策略已生效。			关联生效服务器	编辑 删除

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	策略的生效状态。包含以下状态:				
	• 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				



参数	参数说明
	建的策略状态都为"学习中"。
	• 子习元成,東崎木主奴 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)。 • 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。
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。
操作	 可对该策略执行的操作。支持以下操作: 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。 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。 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。

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0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。

应用程序列表



白名单策略 / policy1		
应用程序 生效服务器		
标记 应用总数 130 可信 30 不可	可信 40 未知 60	C
文件SHA256	信任状态 🍞	操作
string	「成本」	标记
string	可信	标记
string	不可信	标记

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0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。

白名单策略 / policy1			
应用程序 生效服务器			
添加服务器			服务器名称 ▼
服务器名称/IP地址	异常行为数	异常处理模式	操作
string string	0	阻断	删除
string string	0	告答	删除

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。



2.8.1.2 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

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"程序运行认证"页面,选择"白名单策略",单击"创建策略",如0所示。

创建白名单策略

企业主机安全		程序运行认证 👒 🙇	程介绍				文件隔离箱	购买主机安全
总统主机管理		企业项目 所有项目	¥	C				
入侵检测 高级防御	* *	事件管理 生X	服务器 白名	2 单策略				
程序运行认证 文件完整性管理	•	3 创建策略					请输入策略名称	QC
動変病毒防护		策略名称 policy1	已生效服务器	秋志 ① 学习中	应用数 可信 1 不可信 2 未知 3	策略状态	操作	
安装与配置		policy2	0	🍄 学习完成,策略未生效。			编辑 删除	
网页防篡改	*	policy3	0	📀 学习完成,策略已生效。			关联生效服务器	编辑 删除

在创建策略页面中,配置策略"基本信息",如0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。

配置策略信息



策略管理 / 创建策略					
基本信息					
* 策略名称	请输入策略	铬名称			
智能学习天数 🕜	● 7天	() 15天 ()	30天		
添加服务器					
添加服务器					
服务器名称		IP地址		系统	操作
ecs-76ef				Linux	删除
创建并学习取消					

单击"添加服务器",添加智能学习服务器,如0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和 收集"可信"、"不可信"和"未知"的应用进程数据。

添加白名单策略学习服务器



丁选服	發器(12)			已选服务器(1)		
未分	1组 ▼ 请输入服务器名称	QC		请输入服务器名称		Q
	影响服务器名称/IP	系统		服务器名称	系统	操作
~	ecs-	Linux	L	ecs-	Linux	×
	ecs-	Windows				
	ecs	Linux				
	ecs-	Linux	I			
	ecs-	Windows				
	ecs	Windows				

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。

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"。

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。

● 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。

单击"关联生效服务器",为白名单策略添加生效服务器,如0所示。

添加关联生效服务器



事件管理	生效服务器	白名单策略			
创建策略					请输入策略名称 Q C
策略名称	已生效服务器	状态	应用数	策略状态	操作
policy1	0	🔅 学习中	可信 1 不可信 2 未知 3		编辑 删除
policy2	0	🔅 学习完成,策略未生效。			编辑丨删除
policy3	0	🥑 学习完成,策略已生效。			关联生效服务器编辑 删除

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0所示。

名单策略 policy3		异常处理模式	告警	•	
 选服务器(12) 未分组 ▼ 请输入服务器名称 	QC	已选服务	器(1)		
■ 影响服务器名称/IP	系统	服务器名称	F	系统	操作
ecs- 10.154.122.235	Linux	ecs		Linux	×
ecs-	Windows				
ecs-	Linux				
ecs-	Linux				
ecs-	Windows				
ecs	Windows				

配置关联生效服务器

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。

● 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。

2.8.1.3 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

登录管理控制台。

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。 进入"程序运行认证"页面,选择"事件管理",如0所示。

程序运行事件管理页面

124



企业主机安全		程序运行认证 👒 調理介紹	l.					文件隔离箱	
总范									
主机管理		企业项目 所有项目	٣	С					
风险预防	*								
入侵检测	•	2							
高级防御	•	事件管理生效服务	₿ 白谷	单策略					
程序运行认证		处理					最近24小时 ▼ 服务器名称 ▼		
文件完整性管理		程序路径	信任状态	影响服务器名称/IP	命中白名单策略	发生时间 ↓Ξ	前述	秋恋 🏹	操作
初至時極初却	÷	C:\Windows\System	未知	勤素測试中-勿动 192.168.0.250	test	2020-06-17 10:22:4	陰幣償:c5d699fa15205869828b3f4386082696599b59dc6c	() 未处理	处理
安装与配置	÷	C:\Windows\System	未知	勤実測试中-勿动 192.168.0.250	test	2020-06-17 10:22:4	喻希值, PID: 3852, 运行用户:, 文件权限: 20, 进	()未处理	处理
P2200380A		C:\Windows\System	未知	勘素測试中-勿动 192168-0250	test	2020-06-17 10:15:3	哈希值, PID: 1320, 运行用户:, 文件权限: 20, 进	() 未处理	处理

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"。

● 处理程序运行事件

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0所示。

处理应用进程告警事件



企业主机安全		程序运行认证 🤤 流程介绍	1					文件隔离箱	购买主	机安全
主机管理		企业项目 所有项目	٠	C						
风险预防										
入侵检测	Ŧ	2								
高级防御		事件管理 生效服务	請 白名	单策略						
		处理					最近24小时 ▼ 服务最后称 ▼		Q	С
X14962ECE BAE		程序描述	信任状态	影响服务器名称/IP	命中白名单策路	发生时间 ↓Ξ	前述	秋志 🏹	操作	
60%的增加3-2	•	C:\Windows\System_	未知	動変測试中-勿动 192.168.0.250	test	2020-06-17 10:22:4	始裕룹;c5d699fa15205869828b3f4386082696599b59dc6c	() 未处理 3	处理	
安装与配置	÷	C:\Windows\System_	未知	勤實測试中-勿动 192.168.0.250	test	2020-06-17 10:22:4	始將蠻, PID: 3852, 运行用户:, 文件权限: 20, 进	() 未处理	处理	
		C:\Windows\System	来归	勘索测试中-勿助 192.168.0.250	test	2020-06-17 10:15:3	始帝遭, PID: 1320, 运行用户:, 文件权限: 20, 进	() 來处理	处理	

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0所示。

处理事件			×
事件类型	命中白名单策略	发生时间	状态
application_whit	test	2020-06-17 10:2	1 未处理
处理方式 💿 可信 🤇) 不可信) 未知	「隔离查杀) 取消	肖隔离查杀
	确定	取消	

处理进程告警事件

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



处理方 式	处理方式说明
	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 2.7.3 管理文件隔离箱。 说明 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。 说明 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。

单击"确定",完成进程告警事件处理。

2.8.2 文件完整性管理

2.8.2.1 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

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。

进入"文件完整性管理"页面,单击 ,开启文件完整性管理,如0所示。

开启文件完整性管理

企业主机安全		文件完整性管理
总览		
主机管理		企业项目 所有项目 ▼ C
风险预防	•	
入侵检测	•	
高级防御	•	
程序运行认证		服务器总数(台)
文件完整性管理		文件数:
勒索病毒防护		

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。

● 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。

登录管理控制台。



在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 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。

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0所示。

默认策略组

删除						请输入策略组名称
	策略组名称	ID	描述	支持的版本	关联服务器数	操作
	default_enterprise_policy_group (d07938e2-2953-484f-9f62-beab36	企业版策略组	企业版	0	
	default_premium_policy_group (59b6e746-5e4c-4e4e-a518-ddfe36	旗舰版策略组	旗舰版	0	复制
	平台侧策略组	e2137cef-ac42-47cf-8064-e0a1dd		旗舰版	0	复制 删除
	-default的策略组	44c2ecce-57ee-40f0-aa00-578331		旗舰版	0	复制制除
	DescriptionDescriptionDescriptio	fa225cc7-a6de-4850-9f73-f34e632	DescriptionDescriptionDescriptio	旗舰版	0	复制 删除

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0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。

策略管理 / default_premium_policy_grou	文件完整性管理
	基本信息
策略名称	策略启用状态 已启用
弱口令检测	功能类别 入侵检测
系统配置检测	
网站后门检测	策略ID 7be64100-d964-4637-abad-15ee9dd67012
提权检测	策略内容
反弹/异常Shell检测	全量检测时间间隔(秒): 3600
SSH白名单	文件状态检测时间间隔(秒): 20
文件完整性管理	检测休息时间 (章秒): 50
资产管理	监控文件: /bin/ls
高危命令检测	/usr/bin//s /bin/ps /usr/bin/ps /bin/bash
	/usr/bin/bash
	确定 取消

进入文件完整性管理策略

添加完成后, 单击"确定", 完成管理文件的添加。



● 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。

2.8.2.2 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

登录管理控制台。

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。 进入"文件完整性管理"页面,查看变更概况,如0所示。

查看变更概况

企业主机安全 文件完整性管理 总院 • C 企业项目 所有项目 主机管理 风险预防 入侵检测 60 变更统计 变更类型 高级防御 总变更数 (个) 20个 新增 50 40个 10个 删除 程序运行认证 修改 文件数: 注册表: 30 文件完整性管理 勒索病毒防护

企业主机病	全		文件完整性管理							
总宽										
主机管理			1	变更统计	变更类型	ĥ				
风险预防		Ŧ	服务器总数(台)	总变更数 (个)	⁵ 0↑	2个	3 ↑			
入侵检测		-		文件数:5 注册	表: 0	- 11/2	MUNA-			
高级防御										
程序运行	认证									
文件完整	性管理		云服务器 变更文件							
勒索病毒	防护									
安全运营		Ŧ					清輸入服务器	洛称	Q 高级搜索 ※	С
安装与配置			服务器名称	变更总数	变更文件		变更注册表	最	后变更时间	
网页防篡改		•	ecs-hss-002	4	4		0	20	20-09-07 10:26:35 GMT+08	8:00

变更概况

送别 · · · · · · · · · · · · · · · · · · ·	
--	--



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	 • 变更总数(个):所有管理的变更的总的数量。 • 文件数:所有管理的文件变更的数量。 • 注册表:所有管理的注册表变更的数量。
变更类别	 修改:所有管理的文件和注册表修改的数量 新增:所有管理的文件和注册表新增的数量。 删除:所有管理的文件和注册表删除的数量。

● 查看单个云服务器变更文件

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0所示。

云服务器列表页面

云服务器	变更文件			
			Ĩ	青輸入服务器名称 Q 高级搜索 ≫ C
服务器名称	变更总数	变更文件	变更注册表	最后变更时间 1三
server1	1	1	1	2020-04-26 11:14:22 GMT+08:00
server2	2	2	2	2020-02-17 00:34:22 GMT+08:00
server3	3	3	3	2020-02-28 14:21:02 GMT+08:00
server4	4	4	4	2020-03-11 04:07:42 GMT+08:00

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0所示。

门 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。

服务器变更详情



文化	非完整性管理 / server1						
	变更总数108 🕴 变更5	文件50 变更注册:	表20	4	名称	▼ 请输入名称	Q 高级搜索 ≫ C
	文件	路径	变更内容	变更类型	3	医更类别	变更时间
	file_name	file_path	将SHA256"before_change"改为"afte	注册表	C	新増	2020-04-26 11:24:41 GMT+08:00
	file_name	file_path	将SHA256"before_change"改为"afte	文件		修改	2020-04-26 11:24:41 GMT+08:00
	file_name	file_path	将SHA256"before_change"政为"afte	注册表	(新増	2020-04-26 11:24:41 GMT+08:00

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。

● 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0所示。

云服务器	变更文件					
					名称 ▼ 请输入名称	Q 高级搜索 ≫ C
名称	路径	变更内容	服务器名称	变更类型	变更类别	最后变更时间↓Ξ
test	test		host-001	文件	修改	2020-04-26 11:14:22 GMT+08
test1	test		host-002	文件	新增	2020-02-17 00:34:22 GMT+08
test2	/test		host-003	注册表	删除	2020-02-28 14:21:02 GMT+08

变更文件列表

🛄 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。



2.8.3 勒索病毒防护

2.8.3.1 防勒索病毒概述

服务器感染勒索病毒越来越普遍,一旦服务器遭受勒索病毒攻击,关键文件会被加密,无法正常使用,企业业务将受到严重影响。HSS 针对勒索病毒提供了防勒索解决方案。

● 功能介绍

创建勒索病毒防护策略后, HSS 通过机器学习引擎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。同时, 学习服务器上的可信进程修改文件的行为。防护策略学习完成后, 自动应 用于关联服务器, 在防护阶段对非可信程序的操作进行告警。

● Windows 防护勒索

创建 Windows 防护策略完成后,智能学习策略通过机器学习引擎学习关联服务器上的可信进程修改文件的行为,对非可信进程修改文件的行为进行告警。

2.8.3.2 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。

- 前提条件
 - 已开启"旗舰版"或"网页防篡改版"主机安全防护。
 - Linux 主机的 "Agent 状态"为 "在线"。
- 创建 Linux 防护策略

登录管理控制台。

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。 进入"勒索病毒防护"页面,单击"创建策略",创建 Linux 防护策略,如0所示。

Linux 防护策略管理页面



企业主机安全		勒察病毒防护 🍞 🕅	着南 💘 流程介绍										购买主	机安全
息览		为了得到更好的勤素#	毒防护,建议到云备6	服务开启	云备份。									>
主机管理														
风险预防	٠	企业项目 所有项目	¥	С										
入侵检测	*		•											
高级防御 1	*	事件管理 策	管理											
程序运行认证		4												
文件完整性管理		Linux防护 W	indows防护											
勤素病毒助护 2	Ţ	5 创建策略										请输入策略名称	Q	С
X±liom		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	诱饵防护状态	操作	
安装与配置		test111		0		1		6	c:\Program Files (x86)	ini;db;log;txt	告答		编辑	Billio
网页防复改	*	string?		0		0		0	c\Program Files (x86)	inidblogtyt	881WF		648	-

配置 Linux 防护策略基本信息,如0所示。

基本信息	
* 策略名称	请输入策略名称
诱饵防护	 开启 关闭
智能学习天数 ?	● 7天 ○ 15天 ○ 30天
防护状态	告警・
* 监控文件路径	/home;/root;/opt 多个文件路径请用分号隔开。
★ 扩展名	例: log; js 多个扩展名请用分号隔开。

配置 Linux 防护策略

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。
诱饵防护	开启诱饵防护后, HSS 将会在关联服务器中预置诱饵文件, 帮助您实 时诱捕新型未知的勒索病毒。
智能学习天 数	请根据您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"。



参数	参数说明
	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。
监控文件路 径	监控的文件的路径,多个文件以分号分隔。监控填写的路径下的文件 操作。
	例: /opt;/opt/sap 说明 若是防护所有路径,可设置为"",但建议配置关键文件的具体路径即可。
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。 例:sql;txt;sh

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0所示。

添加 Linux 关联服务器

可选服	送务器(12)		已选服务器(1)		
未分	1 ■ 请输入服务器名称	QC	请输入服务器名称		Q
	影响服务器名称/IP	系统	服务器名称	系统	操作
~	ecs	Linux	ecs-	Linux	×
	ecs-	Windows			
	ecs-	Linux			
	ecs-	Linux			
	ecs-	Windows			
	ecs	Windows			

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。

完成关联服务器添加后,单击"创建并学习",完成 Linux 防护策略的创建。

Linux 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0所示。

Linux 防护策略列表

事件管理	策略管理								
Linux防护	Windows防护	1							
创建策略								请输入策略名称	QC
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	诱饵防护状态	操作
test111	0		1	6	c:\Program Files (x86)	ini;db;log;txt	告蓉		编辑 删除
string2	0		0	0	c:\Program Files (x86)	ini;db;log;txt	阻断		编辑 删除

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	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。
诱饵防护状 态	 开启:诱饵防护为开启状态,HSS 在关联服务器中预置诱饵文件,发现未知勒索病毒加密诱饵文件的行为,立即告警。 关闭:诱饵防护为关闭状态。



● 创建 Windows 防护策略

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"勒索病毒防护"页面,单击"创建策略",创建 Windows 防护策略,如0所示。

Windows 防护策略管理页面

企业主机安全		勒索病毒防护 🖻 使用	· 寮病毒防护 ₽ 使用指用 № 流星介绍								购买主	机安全	
总武		为了得到更好的勘索	D 为7得到更好处到室病毒防护、建议到正确份服务开启正备份。 ×										
土の店理 风险预防 入侵松測	•	企业项目 所有项目	Ŧ	С	Linux防护	a Wind	owsß	方护					
高級防御 1	*	事件管理 第	3 略管理										
文件完整性管理		Linux防护 4	/indows防护										
<u>勤素病毒防护</u> 2 安全运营		5 创建策略									请输入策略名称	Q] C
安装与配置		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	诱饵防护状态	操作	
网页防算改	.	test111		0	1		6	c:\Program Files (x86)	ini;db;log;txt	告營		编辑	删除
Concernance.		string2		0	0		0	c:\Program Files (x86)	ini;db;log;txt	阻断	-	编辑	删除

配置勒索病毒防护策略基本信息,如0所示。

配置 Windows 防护策略

基本信息	
* 策略名称	请输入策略名称
智能学习天数 ?	● 7天 ○ 15天 ○ 30天
防护状态	告警 ▼
监控文件路径	例: x:\xxx\xxx 多个文件路径请用分号隔开。
★ 扩展名	例: log; js 多个扩展名请用分号隔开。

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。
监控文件路径	监控的文件的路径,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。

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0所示。

添加 Windows 关联服务器

添加关联服务器				×
可选服务器(12)		已选服务器(1)		
未分组 ▼ 请输入服务器名称	QC	请输入服务器名称		Q
■ 影响服务器名称/IP	系统	服务器名称	系统	操作
ecs-l	Windows	ecs-	Windows	×
ecs-	Windows			
ecs 	Linux			
ecs-	Linux			
ecs-	Windows			
ecs-	Windows			
	确认	取消		



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。

完成关联服务器添加后,单击"创建并学习",完成 Windows 防护策略的创建。

Windows 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0所示。

Windows 防护策略管理列表

事件管理	策略管理									
Linux防护	Windows防护									
创建策略								请输入策略名称	C	C
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	
test111	c)	1		6	c:\Program Files (x86)\Ho	ini;db;log;txt	告警	编辑	删除
string2	C)	0		0	c:\Program Files (x86)\Ho	ini;db;log;txt	阻断	编辑	删除

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	监控的文件的路径,多个文件以分号分隔。监控该路径下的文件操作。 如果监控文件路径为"",表示 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。



参数	参数说明
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。

2.8.3.3 管理防护策略

防护策略创建完成后,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。

如果您需要修改已创建策略的基本信息或者关联服务器,您可以通过策略管理页面,执行相关操作。

● 前提条件

"服务器状态"为"运行中",已安装 HSS 的 Agent,且"Agent 状态"为"在线"。

● 查看防护策略列表

登录管理控制台。

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。 进入"勒索病毒防护"页面,单击"策略管理",进入防护策略管理列表页面,如0所示。

策略管理列表

企业主机安全		勒索病毒防护										
200 200		为了得到更好的勘案病義	\$\$\$}护,建议到云备份服务;	干启云备份。								×
主机管理												
风险预防	*	企业项目所有项目	• C									
入侵检测	*											
高级防御 1	*	事件管理 策略	管理									
程序运行认证												
文件完整性管理		Linux防护 Win	dows防护									
勤素病毒防护		创建策略								请输入策略名称	Q	С
交主地員		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	诱饵防护状态	操作	
安装与配置							al Designer Files (c.D.C.)	to table la solution			-	INCO.
网页防复改	-	testiti	L.		1	6	C:\Program Files (X86)	ini,uo,iog;txt			2482	NEAGE 1
		string2	C		0	0	c:\Program Files (x86)	ini;db;log;txt	阻断		编辑	删除

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。



参数	参数说明
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"。
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	监控的文件的路径,多个文件以分号分隔。监控该路径下的 文件操作。 如果监控文件路径为"",表示 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。

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0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。

第)略管理 / test111								
	基本信息 🖉								
	策略名称	test111		监控文件路径	c\Program Files	(x86)\HostGuard\;C:\ProgramData			
	智能学习天数	7天		扩展名	ini;db;log;txt				
	防护状态	告警		更新时间	2020-06-07 11:4	16:39 GMT+08:00			
	进程文件	已关联服务器							
	标记	进程总数 100 可信进程 20	不可信进程	80					
	进程文	大件	进程签名的	发布者		进程HASH	信任状态	· 7	操作
	string	1	string1		string1		可信		标记
	string	2	string2			string2	不可信		标记
	string	2	string2			string2	可信		标记

防护策略详情



单击"已关联服务器",查看关联服务器,如0所示。

查看关联服务器

进程文件 已关联服务器				
添加服务器 重新学习 删除			服务器名称 🔻	輸入服务器名称
服务器名称	IP地址	系统	策略状态	操作
host_name1	host_ip1	windows	② 学习中	重新学习 删除
host_name2	host_ip2	Linux	② 学习中	重新学习 删除
host_name3	host_ip3	Linux	❷ 学习完成,策略已生效	重新学习 删除

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	 策略的生效状态。包含以下状态: 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"。 一类习完成, 等败口生效
	• 学习完成,束略已至效 该策略已完成智能学习,并且已应用到关联服务器中。
操作	可对该策略执行的操作。支持以下操作: 重新学习 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。 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。



参数	参数说明
	 - 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
	 删除 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。

● 编辑防护策略

编辑防护策略后,防护策略需要重新开始学习。

若编辑防护策略前已开启诱饵防护,编辑防护策略时关闭诱饵防护,预置的诱饵文件会被删除。 HSS 将无法及时隔离查杀新型未知的勒索病毒,请谨慎操作。

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"勒索病毒防护"页面,单击"策略管理",进入防护策略管理列表页面,如0所示。

企业主机安全		勒索病毒防护	家病毒防护											
5 5		为了得到更好的勘索病書	① 为了得到便好的激励病毒的护, 建议到云香台服务开展云香台。 ×											
主机管理														
风险预防	٣	企业项目 所有项目	v	С										
入侵检测	*													
南级防御 1	•	事件管理 策略	官理											
程序运行认证 文件完整性管理		Linux防护 Win	dows防护											
勤素病毒防护 2	Ŧ	创建策略										请输入策略名称	Q	С
		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	诱饵防护状态	操作	
XXTRE		test111		0		1		6	c:\Program Files (x86)	ini;db;log;txt	苦警		编辑	删除
网页防要改	*	string2		0		0		0	c:\Program Files (x86)	ini;db;log;txt	阻断		编辑	删除

策略管理列表

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。

编辑策略		×
★ 策略名称	test111	
诱饵防护	○ 开启 ● 关闭	
智能学习天数	● 7天 ○ 15天 ○ 30天	
防护状态	告警 ▼	
★ 监控文件路径	c:\Program Files (x86)\HostGuard\;C:\ProgramData 多个文件路径请用分号隔开。	
★ 扩展名	ini;db;log;txt 多个扩展名请用分号隔开。	
	确认 取消	

编辑策略

单击"确认",完成策略编辑。

● 管理策略中的关联服务器

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。

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"勒索病毒防护"页面,单击"策略管理",进入防护策略管理列表页面,如0所示。

策略管理列表


企业主机安全		勒索病毒防护											购灭主	机安全
总质		 为了得到更好的勘: 	奏病毒防护,建议到云备()服务开)	启云备份。									×
主机管理														
风险预防	Ŧ	企业项目 所有项目	*	С										
入侵检测	Ŧ		3											
高级防御 1	*	事件管理	策略管理											
程序运行认证														
文件完整性管理		Linux防护	Windows防护											
新素病毒防护 2		创建策略										请输入策略名称	Q	С
文王运言	*	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	诱饵防护状态	操作	
文表与取直		test111		0		1		6	c:\Program Files (x86)	ini;db;log;txt	告警		编辑	删除
网贝防暴改	Ŧ	string2		0		0		0	c:\Program Files (x86)	ini;db;log;txt	阻断		编辑	删除

单击已创建策略的策略名称,进入详情页面,如0所示。

	0											
事件管理 策	管理											
2 Linux防护 W	indows防护											
创建策略										请输入策略名称	Q	C
策略名称	已生效服务器		学习中服务器	R	可信进程数		监控文件路径	扩展名	防护状态	诱饵防护状态	操作	
3 test111		0	1			6	c:\Program Files (x86)	ini;db;log;txt	告警		编辑	删除
string2		0	C)		0	c:\Program Files (x86)	ini;db;log;txt	阻断		编辑	删除

进入策略详情页面

选择"关联服务器",单击"添加服务器",添加关联的服务器,如0所示。

添加关联的服务器

进程文件 已关联服务器				
添加服务器重新学习	删除		服务器名称 🔻 请	输入服务器名称 Q C
服务器名称	IP地址	系统	策略状态	操作
host_name1	host_ip1	windows	🔅 学习中	重新学习 删除

在弹出的添加服务器窗口中,选择关联的服务器,如0所示。

添加 Windows 关联服务器



选服务器(12)		已选择	段务器(1)		
未分组 🔻 请输入服	资器 名称	Q C 講	俞入服务器名称		Q
■ 影响服务器名称/IP	系统	服务器	絡称	系统	操作
ecs-	Windows	ecs-		Windows	×
ecs-	Windows				
ecs	Linux				
ecs.	Linux				
ecs-	Windows				
ecs-	Windows				

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。

● 删除防护策略

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 进入"勒索病毒防护"页面,单击"策略管理",进入防护策略管理列表页面,如0所示。

策略管理列表

企业主机安全	勒索病毒防护	
1016	分了得到更好的和素质毒物的,建议到云新份服务开启云新份。	×
主机管理		
风险预防	企业项目 所有项目 ▼ C	
入侵检测	0	
高级防御 1 🔺		
程序运行认证		
文件完整性管理	Linux防护 Windows防护	
和实际电防护 2	())	
受全运营 ▼	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 透细防护状态 操作	
安装与配置	test111 0 1 6 c1/Program Files (x86) ini;db;log;b.t 音音 编編 世经	
PSI-CROBERK V	string2 0 0 0 c-brogram Files (v56) init/thightyt 2015 556 Hills	

146



单击"删除", 弹出删除策略窗口。

单击"确定",完成策略删除。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。

2.8.3.4 处理防护告警事件

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。

在事件管理列表中,处理防护告警事件时,若标记为"不可信",您需要对不可信进程进行手动排查 和处理,避免不可信进程对您的主机造成危害。

🛄 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。

● 查看防护告警事件列表

登录管理控制台。

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。 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0所示。

勒索病毒防护列表

企业主机安全		勒索病毒防护	期茶病毒防护								诠
总览		1 为了得到更好的勘测	_{乾病毒助护,建议到云备}	份服务开启云言	HB.						×
主机管理											
风险预防	Ŧ	企业项目 所有项目		С							
入侵检测	*										
高级防御 1	*	3 事件管理 常	1.86957田								
程序运行认证		Series and Series									
文件完整性管理		处理					最近24小时	▼ 服务器名称	▼ 请输入服务器名称	QC	
勤素病毒防护 2		文件路径	影响服务器名称/IP	进程路径	进程HASH	进程签名的发行者	命中策略	发生时间 ↓Ξ	状态 🔽	操作	
安全运营	*	file_path1	host_name1 host_ip1	path1	hash1	signer1	policy_name1	2020-05-21 11:29:08	1 未处理	处理	
网页防复改	*	file_path2	host_name2 host_lp2	path2	hash2	signer2	policy_name2	2020-05-21 11:30:14	() 未处理	处理	
		file_path3	host_name3 host_lp3	path3	hash3	signer3	policy_name3	2020-05-21 11:30:25	⊘ 已处理	处理	

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。
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"。

● 处理防护告警事件

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0所示。

处理勒索病毒防护告警事件

企业主机安全		朝紫病毒防护 85	医主机安全
武总		⑦ 为了得到便行的政策病毒物的,建议到近年份期的开启云音份。	×
主机管理			
风险预防	٠	企业项目 所有项目 V C	
入侵检测	*		
	*	● 事件管理 策能管理	
文件完整性管理		赴渡 最近24小61 ▼ 服务器名称 ▼ 溶総入服务器名称 Q	C
勤素病毒助护 2		文件器径 影响服务器名称/IP 进程路径 进程HASH 进程签名的发行者 命中撤销 发生时间 (三 秋态 \7 操作	
安全运营	Ŧ	- file_path1 host_name1 path1 hash1 signer1 policy_name1 2020-05-2111/29.08 🚷 来85連 📢 応要]

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0所示。

处理勒索病毒防护事件



🛕 你确定要对以	下进程文件进行标记处理吗	ዓ?
文件路径	进程路径	影响服务器名称/IP
file_path1	path1	host_name1 host_ip1
信任状态	可信 不可信 确认	取消

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。

单击"确定",完成勒索病毒防护告警事件标记处理。

2.9 安全运营

2.9.1 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。

2.9.1.1 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。

2.9.1.2 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)	V	~
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)	V	~
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	×	\checkmark	\checkmark
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	×	\checkmark	\checkmark
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	×	V	\checkmark
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: •利用 SUID 程序漏洞进行 root 提权。	Linux	×	V	\checkmark



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
	 利用内核漏洞进行 root 提权。 权文件的提权。 				
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	×	\checkmark	\checkmark
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	×	\checkmark	\checkmark

2.9.1.3 进入策略管理

登录管理控制台。

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。

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。

2.9.1.4 查看策略组列表

在"策略管理"界面,查看显示的策略组。如0所示,字段说明如0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 C, 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。

策略组列表



企业主机安全		策略管理 ⑦						
总览 主机管理		企业项目所有项目	Ŧ	С				
风脸预防	٣							
入侵检测	٠	删除						请输入策略组名称
高级防御	٣	策略组名称		ID	描述	支持的版本	关联服务器数	操作
安全运营	*	default_enterprise	_policy_group (d07938e2-2953-484f-9f62-beab36	企业版策略组	企业版	0	
策略管理		default_premium_	policy_group (59b6e746-5e4c-4e4e-a518-ddfe36	旗舰版策略组	旗舰版	0	复制
女表句能量		平台侧策略组		e2137cef-ac42-47cf-8064-e0a1dd		旗舰版	0	复制 删除

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。

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0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。

策略组详情



策略管	理 / default_enterprise_po	olicy_group			
					C
鍧	策略名称	状态 🍞	功能类别	支持的操作系统	操作
100	易口令检测	已启用	基线检查	Linux, Windows	关闭
NR	系统配置检测	未启用	安全加固	Linux	开启
×	网站后门检测	已启用	入侵检测	Linux, Windows	关闭
执	是权检测	已启用	入侵检测	Linux	关闭
Б	2弹/异常Shell检测	未启用	入侵检测	Linux	开启
s	SH白名单	未启用	入侵检测	Linux, Windows	开启
3	文件完整性管理	已启用	入侵检测	Linux	关闭
X43	8产管理	未启用	资产管理	Linux, Windows	开启
Ĩ	高危命令检测	已启用	数据采集	Linux	关闭

单击策略名称,可以查看策略的详情,以弱口令为例,如0所示。

🛄 说明

若需要修改策略,请参见 2.9.2 修改策略内容。

策略详情



策略管理 / default_premium_policy_group	弱口令检测
	基本信息
策略名称	策略启用状态 已启用
弱口令检测	功能类别 基线检查
系统配置检测	策略ID aa1f2fdf-867a-4551-8974-0a02828cb829
网站后门检测	笙政 九 ∽
提权检测	ни Поланка П
反弹/异常Shell检测	使用關口令字典
SSH白名单	弱口令字典更新URL
文件完整性管理	弱口令字典SHA256
资产管理	检测日
高危命令检测	自定义弱口令
	mysql晹口令检测:
	稍 定 取消

● 创建策略组

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0所示。

复制策略组

企业主机安全	策略管理 ②					
总览						
主机管理	企业项目 所有项目 🔻	С				
风险预防 🔻						
入侵检测 🔻	删除					请输入策略组名称
高级防御 🔻	策略组名称	ID	描述	支持的版本	关联服务器数	操作
安全运营 🔺	default_enterprise_policy_group (d07938e2-2953-484f-9f62-beab36	企业版策略组	企业贩	0	
策略管理	default_premium_policy_group (59b6e746-5e4c-4e4e-a518-ddfe36	旗舰板策略组	旗舰版	0	复制
安装与配盒 四面防算改 🔻	- 平台侧策略组	e2137cef-ac42-47cf-8064-e0a1dd		旗舰版	0	复制 删除

在弹出的对话框中, 输入"策略组名称"和"描述", 如0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。

创建策略组

复制策略组		×
★ 策略组名称		
描述	Æ	
	确定取消	

单击"确定",将会创建一个新的策略组。

单击已创建的策略组名称,进入策略组的策略页面,如0所示。

策略组策略

策略	管理 / default_enterprise_policy_	group				
					(>
	策略名称	状态 🍞	功能类别	支持的操作系统	操作	
	弱口令检测	已启用	基线检查	Linux, Windows	关闭	
	系统配置检测	未启用	安全加固	Linux	开启	
	网站后门检测	已启用	入侵检测	Linux, Windows	关闭	
	提权检测	已启用	入侵检测	Linux	关闭	
	反弹/异常Shell检测	未启用	入侵检测	Linux	开启	
	SSH白名单	未启用	入侵检测	Linux, Windows	开启	
	文件完整性管理	已启用	入侵检测	Linux	关闭	
	资产管理	未启用	资产管理	Linux, Windows	开启	
	高危命令检测	已启用	数据采集	Linux	关闭	

单击策略名称,修改具体的策略内容,详细信息请参见 2.9.2 修改策略内容。

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。

2.9.1.5 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"。 选中需要删除的一个或多个策略组,单击"删除",如0所示。

删除策略组列表

删除						请输入策略组名称
	策略组名称	ID	描述	支持的版本	关联服务器数	操作
	default_enterprise_policy_group (d07938e2-2953-484f-9f62-beab36	企业版策略组	企业版	0	
	default_premium_policy_group (59b6e746-5e4c-4e4e-a518-ddfe36	旗舰版策略组	旗舰版	0	复制
	平台侧策略组	e2137cef-ac42-47cf-8064-e0a1dd		旗舰版	0	复制 删除
	-default的策略组	44c2ecce-57ee-40f0-aa00-578331		旗舰版	0	复制 删除

门 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。

在弹出对话框中,单击"确定",完成策略组的删除。

2.9.2 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。

2.9.2.1 进入策略管理

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 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。

2.9.2.2 资产管理

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。

单击"资产管理", 弹出资产管理界面。

在弹出的资产管理界面中,修改"策略内容",如0所示,参数说明如0所示。

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 Asset					
策略ID 7b3887ba-f	8b0-40ae-b942-95f57b43bc	05			
策略内容					
账号与软件信自答理					
	00.01				
检测时间	00:01				
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:	/usr/local,/usr/bin,/u windows主机不用添加	usr/sbin,/usr/lib			
主要应用/组件:	软件名	软件主程序	执行命令	操作	
	openssl	openssl	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): 30 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					
确定 取消					

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	 软件名称中不能包含空格旦内容长度不得超过 5000 字符,多 个软件名称用逗号分隔。 如果不配置,则获取所有已安装软件信息。 	
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	• 软件名:软件名称。	



参数	说明
	• 软件主程序: 软件的主程序。
	• 执行命令:执行的命令。
	 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。
获取 UDP 端口	获取 UDP 端口信息,检测 WEB 的目录。
	• 〇 : 开启。
	• 〇〇 : 关闭。
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"。

单击"确定",完成修改。

2.9.2.3 系统配置检测

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。

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。

在"系统配置检测"界面,修改"修改策略内容",如0所示,参数说明如0所示。

系统配置检测



系统配置检测						
基本信息	基本信息					
策略启用状态	已启用					
功能类别	Conf					
策略ID	f2691980-2a5a-46c2-8bba-fb397e718da3					
策略内容						
检测时间 检测日	00:10 図:10 周一 周二 周二 周二 周二 周二 周二 周二 月二 周二 月二 </th <th>B</th>	B				
启用	操作系统	名称				
	Linux	ssh				
	Linux	nginx				
	Linux	tomcat				
	Linux	apache2				
	Linux	redis				
	Linux	mysql5				
	Linux	mongodb				
	Linux	vsftp				
	Linux	centos7				
	确定取消]				

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。	

勾选需要检测的操作系统。

单击"确定",完成修改。



2.9.2.4 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。

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。

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。

在弹出的"策略内容"界面中,修改"策略内容",如0所示,参数说明如0所示。

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 aa1f2fdf-867a-4551-8974-0a02828cb829
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
自定义弱口令
mysql弱口令检测:
确定 取消

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。 • ・ : 开启。 • : 关闭。
弱口令字典更 新 URL	弱口令字典更新的网页地址。



参数	说明
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。

单击"确定",完成修改。

2.9.2.5 高危命令检测

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。

单击"高危命令检测", 弹出高危命令检测界面。

在弹出的高危命令检测界面中,修改"策略内容",如0所示,参数说明如0所示。

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:		
	_	
进程统计信息上据问题(分轴)。	600	
CITAGE DECTORISING AND		
独立进程最大cpu使用率 (%) :	10	
独立进程最大内存使用 (MB) :	300	
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):	4	
梢间口芯馍式:		
此生讲程网络连接信目,		
WARENT-SAMITA (Disk		
	_	
记录日志:		
日志记录路径:	/usr/local/hostguard/log/hc	
日志记录最大文件大小 (MB) :	10	
	strace	
高危命令:	wget	
	zypper	
	yum rz	
	e e e e e e e e e e e e e e e e e e e	
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
	添加	
	湘定	

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。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
使用消息通道去重 上报	 是否开启使用消息通道去重上报。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・



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。 <l< td=""></l<>
收集进程网络连接 信息	 是否开启收集进程网络连接信息。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
记录日志	是否开启记录日志。 • ①: 开启。 • ①: 关闭。
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"。 • 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。 • 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



参数	说明
	继续写入".log"文件。
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)	 进程全路径或程序名:进程的完整路径或者程序的名称。 命令行正则表达式:命令行的正则表达式。 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。

单击"确定",完成修改。

2.9.2.6 提权检测

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。

单击"提权检测", 弹出提权检测界面。

在弹出的"提权检测"策略内容中,修改"策略内容",如 2.9.2.7 所示,参数说明如 0 所示。



2.9.2.7 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	a0657c06-883e-4891-b328-b392b91d9ea0
策略内容	
忽略的进程	i文件路径:
检测时间间	隔(秒): 50
	确定取消

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"。

单击"确定",完成修改。



2.9.2.8 异常/反弹 Shell 检测

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。

单击"异常/反弹 Shell 检测",弹出异常/反弹 Shell 检测界面。

在弹出的异常/反弹 Shell 检测界面中, 修改"策略内容", 如 0 所示, 参数说明如 0 所示。

反弾/异常Shell检测 基本信息 策略启用状态 未启用 功能类别 入侵检测 策略D ea8f5881-bf60-4b3a-aef3-71df6afd81b3 策略内容 反弹shell忽略的进程文件路径: 反弹shell泪描周期(秒): 30 异常shell检测: ④ 进程打开文件上限: 4000

异常/反弹 shell 检测

反弹/异常 shell 检测策略内容参数说明

取消

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。 • ①: 开启。 • ①: 关闭。
进程打开文件上限	进程打开文件的上限数,可配置范围为"10- 300000"。

单击"确定",完成修改。

2.9.2.9 文件完整性管理

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。

单击"文件完整性管理",弹出关键文件完整性管理界面。

在弹出的文件完整性管理界面中,修改"策略内容",如0所示,参数说明如0所示。 文件完整性管理



文件完整性管理	
基本信息	
策略启用状态 已启用	
功能类别 入侵检测	
策略ID 7be64100-d964-4637	-abad-15ee9dd67012
策略内容	
全量检测时间间隔(秒):	3600
文件状态检测时间间隔(秒):	20
检测休息时间 (毫秒) :	50
监控文件:	/bin/ls /usr/bin/ls /bin/ps /usr/bin/ps /usr/bin/bash /usr/bin/bash
	确定取消

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"。
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/ls"后,等待"50"毫秒 再检测"/usr/bin/ls"。



参数	说明
监控文件	需要检测的文件。
	说明
	• 策略默认添加的文件是非常关键的文件,请谨慎删除!
	 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。

单击"确定",完成修改。

2.9.2.10 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。

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。

单击"网站后门检测",弹出网站后门检测界面。

在弹出的网站后门检测界面中,修改"策略内容",如0所示,参数说明如0所示。

网站后门检	2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	148cf0ff-fb46-4c41-aeb5-62e580b629fa
策略内容	
自动识别We	eb目录:
手动添加We	eb目录:
检查文件后线	缀: jsp.jspx.jspf,php,php5,p
监测文件修	at:
	職定取消

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。

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	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。 • ①: 开启。 • ①: 关闭。
手动添加 Web 目录	手动添加需要检测的 Web 目录。 • 文件路径以"/"开头,不能以"/"结尾。 • 结尾必须有端口号。 • 多个路径通过回车换行分隔且名称中不能包含空格。
检查文件后缀	检查文件的后缀,可以检测"jsp"、"jspx"、"jspf"、 "php"、"php5"和"php4"。
监测文件修改	是否开启监测文件修改功能。

单击"确定",完成修改。

2.10 网页防篡改

2.10.1 添加防护目录

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。

2.10.1.1 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。
- 设置本地备份路径时,请设置合法的备份目录,若设置的备份目录不存在,则防篡改不生效。
- 本地备份路径与添加的防护目录不能重叠,否则会导致本地备份失败。



● 备份目录所在磁盘需要有足够的磁盘空间,若备份目录所在磁盘空间不足,会导致防篡改失败。

2.10.1.2 保护指定目录

登录管理控制台。

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。 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。

在"网页防篡改"界面

企业主机安全		防护列表 ②								购买网页防装改
总范 主机管理		企业项目 所有项目	• C							
风险预防	*									
入侵检测	٠	新增动态网页防要改功能,可:	点击"防护设置"开启,欢迎隽	動調试用体验。						×
高级防御	Ť									
安全运营 安装与配置	Ť	已防御篡改攻击 0	防护主机数 🔾	防护	中目录 🛛	防篡改	記额 1 使师	∃中 0	空闲 1	配额详情
网页防装改	•	开启防护 关闭防护					服务者	洺称	▼ 请输入关键字	QC
防护列表		服务器名称/ID IP地址	操作 7	服务器状态	Agent铁态 🏹	防护 7	动态防篡改状态	版本	操作	
安装与配置		servicestage-nodel 81e97d86-04d4-42	.106 (私有 Linux	运行中	在线	◎ 关闭	未开启	无	开启防护 防护	设置 查看报告

"防护模式"选择"保护指定目录",如0所示。

保护指定目录

防护目录设置	定时开关设置 动态	网页防篡改					
防护模式 💿 保护排	首定目录						
添加防护目录	关闭远端备份最多可	可添加50个防护目录。 (远端	<mark>备份服务器</mark> : dfefef)				
防护目录	排除子目录	排除文件类型	本地备份路径	防护状态	操作		
C:\中文	a	js,html		✓ 开启	暂停防护	编辑	删除
\Home\2	b	js,html		◎ 关闭	恢复防护	编辑	删除

添加防护目录,您最多可在主机中添加50个防护目录。

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0。

添加防护目录



添加防护目录	×
* 防护目录:	例:/xxx/xxx 提示:请勿对操作系统目录进行防护, 例如:不对/bin进行防护。
排除子目录:	例:/xxx/xxx 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:	例: log; js 多个文件 类 型请用分号隔开。
★ 本地备份路径:	例:/xxx/xxx 本地备份路径与添加的防护目录不能重叠,否则将导致本地备份失 败!
	确定取消

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。
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	开启网页防篡改防护后,防护目录	本地备份路径与添加的防护目录



参数	说明	限制
路径	下的文件会自动备份到设置的本地备份路径中。	不能重叠。
	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。	

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。

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 2.10.2 添加远端备份服务器。

1. 单击"启动远端备份"。

开启远端备份

	防护目录设置	定时开关设置	动态网页防篡改				
1							
	防护模式 💿 保护	消定目录					
				HARTING R. dfafafi			
	添加防护日求	后动远病备份	板3を円1000月つい1700374日.米。(23	23两曲1万加295名音: Uielei)			
	防护目录	排除子目录	排除文件类型	本地备份路径	防护状态	操作	
	C:\中文	а	js,html		✓ 开启	暂停防护 编辑	删除
			4.2				

2. 通过下拉框选择备份服务器。

启动远端备份



启动远端备份	}
远端备份服务器:	ecs-hss001(192.168.0.2 🔻
新建/修改远端备份	服务器,立即设置
	确定取消

3. 单击"确定",启动远端备份。

2.10.1.3 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。

2.10.2 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。

2.10.2.1 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。

2.10.2.2 设置远端备份服务器

登录管理控制台。

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。

在"远端备份服务器"页面,单击"添加远端备份服务器"。

远端备份服务器

企业主机安全		安装与配置 ②				购买网页防载	卸書	能Agent
总览								
主机管理		企业项目 所有项目	• C					
风险预防	*		2					
入侵检测	*	安装Agent 告警通知	远端备份服务器					
高级防御	*							
安全运营	*							
安装与配置								
网页防篡改	*	备份服务器用于防护目录设置中的")	远涛备份"功能,此功能为可选配置。					
防护列表		3 添加远端备份服务器						С
		服务器名称	地址	端口	备份路径	状态	操作	
		host-001	192.1.1.1	876	/xxxx/xxxx	启动中	编辑 删除	

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0。

添加远端备份服务器



添加远端	备份服务器
服务器名称	egthhyhyj1 💌
地址 ②	1.2.3.5
端口	48486 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	例:/xxx/xxx 提醒:备份路径与本机添加的防护目录不能重叠,否则将导致远端备份失 败。
	确定取消

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	 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。 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"。 备份后路径为"/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f"和"/hss01"。 若设置为远端备份服务器的主机开启了"网页放篡改"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。



单击"确定",完成添加备份服务器的操作。

2.10.2.3 启动远端备份

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。

在"网页防篡改"界面

企业主机安全		防护列表	0										购买网页阶	篡改
总宽 主机管理		企业项目	所有项目	Ŧ	С									
风脸预防	Ŧ													
入侵检测	Ŧ	() 新	增动态网页防装改现	如此,可点击"防护设	置"开启,欢迎免	费试用体验。								×
高级防御	Ŧ													
安全运营	•	B	防御篡改攻击 🛛	防护当	日本	防护	_{唱录} 0	防篡改	配额 1	使用中	0	空闲 1	配额详情	
网页防装改	•	开启财	加 关闭助	护						服务器名标	10	▼ │ 请输入关键字	Q	С
助护列表			服务器名称/ID	IP地址	操作 7	服务器状态	Agent铁态 🏹	防护 7	动态防篡改获	恣	版本	操作		
安装与配置			servicestage-nodel 81e97d86-04d4-42	.106(私者	Linux	运行中	在线	◎ 关闭	未开启		无	开启防护 防护	2011 查看报告	

"防护模式"选择"保护指定目录",单击"启动远端备份",如0所示。

开启远端备份

防护目录设置 定时开关设置 动态网页防篡改										
防护模式 💿 保护描定目录										
添加防护目录	启动远端备份最多	可添加50个防护目录。 (远端	省份服务器 : dfefef)							
防护目录	排除子目录	排除文件类型	本地备份路径	防护状态	操作					
C:\中文	a	js,html		✓ 开启	暂停防护 编辑 删除					

在"远端备份服务器"下拉框中,选择远端备份服务器。

启动远端备份



单击"确定",启动远端备份。

2.10.2.4 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。

2.10.3 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

登录管理控制台。

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。

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。

在"网页防篡改"界面



企业主机安全		防护列表 ⑦
总道		
主机管理		
风脸预防	*	
入侵检测	*	● 新運动志同页防要改功能,可点击"防护设置"开启, 这论免费说用体验。
高级防御	*	
安全运营	*	已防御算改攻曲 0 防护主机数 0 防护目录 0 防算改配额 1 使用中 0 空闲 1 配额洋情
安装与配置		
网页防接改	*	开启防护 关闭防护 关闭防护 · 南部人关键字 Q C
防护列表		服务器名称AD IP地址 操作7 服务器状态 Agent状态 又 助护 又 动态防管改状态 版本 操作
安装与配置		Servicestage-nodel 105 (Linux 造行中 전域

在"定时开关设置"页面,开启定时开关。

防护目录设置	定时开关设置 动态网页防篡改
定时开关	定时开关能够定时关闭静态网页防篡改功能,适用于定时更新发布网页的场景。

定时开关

在弹出的对话框中, 单击"确定"。

设置"关闭防护时间段"和"定时关闭防护频率"。

设置定时防护参数

防护目录设置 定时开关设置	动态网页防篡改							
	闭轴太网面防算动顶能 活田干宁时再新安左网面的							
添加关闭时间段 忽还可以添加1个时	间段	3-%3 Jett 6						
关闭防护时间段	关闭时间段描述	操作						
07:00-09:00	morning workddd	修改删除						
11:00-11:20	morning workdd	修改删除						
选择自动关闭防护频率周期								
周一 🔽 周二 🔽 周三 🔽 周四	🛛 周五 🗌 周六 🔽 周日 🏻 确定							


2.10.3.1 关闭防护时段设置规则

- 每个时间段最小关闭时间 >= 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 >= 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

2.10.4 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。

2.10.4.1 前提条件

主机为 Linux 操作系统。

2.10.4.2 操作步骤

登录管理控制台。

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。

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。

在"网页防篡改"界面

企业主机安全		防护列表 ⑦ 网络网络马马马马马马马马马马马马马马马马马马马马马马马马马马马马马马马马马	
0.7			
主机管理		企业项目 所由项目 • C	
风险预防	Ŧ		
入侵检测	Ŧ		×
高级防御	Ŧ		
安全运营	Ŧ	已防崩署改攻击 0 防护主机数 0 防护目录 0 防算改配额 1 使用中 0 空间 1 配额半情	
安装与配置			
网页防装改	•	开始的炉 美洲防炉 · · · · · · · · · · · · · · · · · · ·	С
防护列表		■ 医外部系统/10 即地址 提作_ 了 图频器状态 Agent(系) 了 防护_ 了 动态的复数系态 版本 提作	
安装与配置		servicetage-model	

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。 动态网页防篡改



防护目录设置	目时开关设置	动态网页防篡改	
动态网页防篡改提供tomc	at应用运行时自我保护	户, 能够检测针对数据库	等动态数据的篡改行为。
动态网页防篡改	注: 开启动态网页随	5.篡改功能后要重启Tom	icat才能生效。

动态网页防篡改开启后,还需重启 Tomcat 才能使其生效。

当您关闭动态网页防篡改,再重新开启后,仍需要重启 Tomcat 才能使其生效。

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。

2.10.4.3 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"。

2.10.4.4 操作步骤

登录管理控制台。

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。 在"网页防篡改 > 防护列表"页面,单击"查看报告"。

查看防护记录

企业主机安全		护列表 ⑦						
总克 主机管理		2 · BRAN BRAN						
风险预防								
入侵检测	-	新聞的志思同時實改功能,可但主作物均衡而且, 双股先最成用体验。	×					
高级防御	Ŧ							
安全运营	-	已防御業双攻击 0 防护主机政 0 防护目录 0 防業双配版 1 使用中 0 空闲 1 配肥料料	青					
安装与配置								
网页防赛改	•	开始的护 美洲的护	С					
防护列表		■ 服务器名称/10 P地址 操作 ▽ 服务器状态 Agent状态 ▽ 防P ▽ 动态防装改状态 版本 操作						
安装与配置		servicestage-nodel 106 (Kit Linux 遠行中 在城 O 短时地市 日开島未生效 同页防御政策 外間から 防中企業 音音振音	F					

在防护记录界面,查看防护记录详情。



静态网页防篡改防护记录

静态网页防算改 动态网页防算改	
已防御篡改攻击: 12	
如需进行本地测试等工作时可设置特权进行名单。立即设置	2021-04-18 15:44:46 - 2021-04-25 16:49:12 X 曲 查询
检测时间 1日	防护文件
1970-01-18 15:36:42 GMT+08:00	d: omcatweb.xml

动态网页防篡改防护记录

网页防篡改 / ecs-76ef					
静态网页防篡改	动态网页防篡改				
已发现篡改攻击:	0				
			2020-11-27 17:34:0	5 - 2020-12-04 18:00:15	× 🗎 童询
告誓时间	威胁类型	告警级别	攻击源IP	攻击URL	攻击结果

2.11 管理防护配额

2.11.1 查看配额

您可以在防护配额页面查看配额的使用情况、配额的状态,及时为即将到期的配额进行续费,或对 没有使用额配额执行退订操作。

配额列表仅显示在所选区域购买的配额,若未找到您的配额,请切换到正确的区域后再进行查找。

2.11.1.1 企业版/旗舰版配额

登录管理控制台。

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。 在"主机管理"页面,选择"防护配额"页签,进入防护配额列表页面。

查看主机安全防护配额



企业主机安全		主机管理 ⑦			购买主机安全 告誓還	和设置 手助检测
总览 主机管理		企业项目 所有项目	• C			
风险预防	-					
入侵检测 高级防御	* *	云服务器 服务器组 防	护配额			
安全运营	*					
安装与配置		旗舰版		企业版		
网页防装改	*	配额使用	配额状态	配额使用	配额状态	
		4个 三 2月 (4	(0) (0) (1) (1) (2) (3) (4) (3) (4) (5) (5) (5) (5) (6) (7) (7) (7) (7) (7) (7) (7) (7	51	● 思闹(5) 5个	正常 (4) 已过期 (0) 已活动能 (1)
		批量解绑	所有版本 ▼ 所有配続状态 ▼	所有使用状态 🔻	配額D ▼ 请输入关键字	QCC
		配额类型/版本	配額D	配線状态	使用状态 操作	
		■ 主机安全防护 第90所	246b971a-1036-40f4-92c4-b0eb3241e895	■正常	空闲 绑定主机	、 续费 更多 ▼

在防护配额页面,查看主机安全防护配额,以及使用该配额的服务器名称。

参数说明

参数名称	说明
配额类型/ 版本	配额的版本类型。
配额 ID	配额的 ID。
配额状态	 正常:您购买的服务配额未到期,且能正常使用。 已过期:您购买的服务配额已到期,在此期间您仍然可以正常使用 配额。 已冻结:冻结期间,HSS将不再防护您的主机;冻结期满,该配 额将被彻底删除。
使用状态	 使用中:该配额已被使用,下方显示"使用该配额的服务器名称"。 空闲:该配额未被使用。

🗀 说明

• 绑定主机

您也可以通过在"主机管理 > 防护配额"页面的"操作"列中,单击"绑定主机",为主机绑定防护配额, HSS 自动为主机开启防护。



一个配额只能绑定一个主机,且只能绑定 agent 在线的主机。

• 续费

您可以在需要续费的资源所在行的操作列,单击"续费",为购买的企业主机安全续费。

退订

您可以在需要退订的资源所在行的操作列,单击"退订",退订不需要使用的配额。

• 解绑配额

您也可以在"主机管理 > 防护配额"页面的"操作"列中,选择"更多 > 解绑配额",解绑配额后, HSS 将自动关闭关联主机的防护,该配额的使用状态变更为"空闲"状态。

2.11.1.2 网页防篡改配额

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在左侧导航树中,选择"网页防篡改",进入网页防篡改的防护列表界面。

企业主机安全		防护列表 ⑦)									购买网页防管。	敳
息 范 主机管理		企业项目	所有项目	v	С								
风脸预防	*												
入侵检测	•			Reto-H	-10.85	Photo		The second	anas 1	使用由 0		和如此	
高级防御	*	□ #0 (#		NO 19-11	EN BOX	NO3-	-ж V	的复数	HCARL	1967 1 944	20/5	以 (1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(
安全运营	Ť	开启助护	关闭助	÷					[服务器名称	▼ │ 语输入关键	φ Q	С
同页防复改		B\$	§器名称/ID	IP地址	操作 7	服务器状态	Agent状态 🍞	防护 7	动态防篡改机	ō 版本	操作		
防护列表		sen 81e	vicestage-nodel 197d86-04d4-42	172.16.0.106 (私有	Linux	运行中	未安装	◎ 关闭	未开启	无	开启防护	• 防护设置 查看报告	
安装与配置			-5364w	172.168.101.246 (Linux	关机	未安装	◎ 关闭	未开启	无	开启防护	1 防护设置 查看报告	

查看企业主机安全"网页防篡改版"防护配额

单击"配额详情",进入网页防篡改防护配额详细信息页面。

配额详情

配额使用		配额状态			
17	使用中 (0) 至7月 (1)	(1↑	正常 (1) 日过期 (0) 日示结 (0)	
批風解绑	所有配銀伏态。	所有使用状态	▼ 配額ID	▼ 请输入关键字	QC
配额类型/版本	配額ID	配额状态	使用状态	操作	
网页防篡改版	20bd4630-b55b-42c6-a448-3f0db6d43349	■正常	💮 空闲	绑定主机 续费 更多 ▼	



在网页防篡改防护配额页面,查看防护配额详细信息。

参数说明

参数名称	说明
配额状态	 正常:您购买的服务配额未到期,且能正常使用。 已过期:您购买的服务配额已到期,在此期间您仍然可以正常使用配额。 已冻结:冻结期间,HSS将不再防护您的主机;冻结期满,该配额将被彻底删除。
使用状态	 使用中:该配额已被使用,下方显示使用该配额的服务器 名称。 空闲:该配额未被使用。

🗀 说明

• 绑定主机

您也可以通过在"网页防篡改 > 防护列表 > 配额详情"页面的"操作"列中,单击"绑定主机",为主机绑定防护配额,HSS 自动为主机开启防护。

一个配额只能绑定一个主机,且只能绑定 Agent 在线的主机。

• 续费

您可以在需要续费的网页防篡改配额所在行的操作列,单击"续费",为购买的网页防篡改续费。

退订

您可以在需要退订的网页防篡改配额所在行的操作列,单击"退订",退订购买的网页防篡改。

• 解绑配额

您也可以在"网页防篡改 > 防护列表 > 配额详情"页面的"操作"列中,选择"更多 > 解绑配额",解绑配额后, HSS 将自动关闭关联主机的防护,该配额的使用状态变更为"空闲"状态。

2.11.2 绑定主机

一个配额只绑定一个主机, 且只能绑定 agent 在线的主机。

2.11.2.1 前提条件

- 已获取管理控制台的登录账号与密码。
- 主机已安装 agent。



● 购买的防护配额的"配额状态"为"正常","使用状态"为"空闲"。

2.11.2.2 绑定主机配额

登录管理控制台。

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。 在"主机管理"页面,选择"防护配额"页签,进入防护配额列表页面。

企业主机安全		主机管理 ②			购买主机安全	告替通知设置 手动检测
总览 主机管理		企业项目 所有项目 v	C			
风险预防	*					
入侵检测 高级防御	•	云服务器 服务器组 防护者	2.10			
安全运营						
安装与配置		旗舰版		企业版		
网页防装改	•	配额使用	配额状态	配额使用	配額状态	2
		4个 ● 愛用 (4)	4↑ ■ 記題(0) ■ 記題(2)	57	使用中 (0) 空闲 (5)	正年(4) 日辺第(0) 日初第(1)
		批量解绑	所有版本 ▼ 所有配额状态 ▼	所有使用状态 🔻	■記載ID ▼ 请输入关	ep Q L C
		配膜类型/版本	配額D	配線状态	使用状态	探作
		主机安全防护 推职版	246b971a-1036-40f4-92c4-b0eb3241e895	■正常	😁 空闲	御定主机 续奏 更多 ▼

查看主机安全防护配额

在防护配额列表页面,单击"绑定主机",为空闲配额绑定主机。

🛄 说明

您也可以在"网页防篡改 > 防护列表 > 配额详情"页面的"操作"列中,单击"绑定主机",为主机绑定网页防篡 改防护配额,HSS 自动为主机开启网页防篡改防护。

绑定主机

批量解绑	所有版本 ▼ 所有配额状态	▼ 所有使用状态	: ▼ 配额ID	▼ 请输入关键字
配额类型/版本	配额ID	配额状态	使用状态	操作
□ 主机安全防护 旗舰版	246b971a-1036-40f4-92c4-b0eb3241e895	■正常	 空闲 	绑定主机 续费 更多 ▼
主机安全防护 旗舰版	b94c9c64-2254-4d86-845d-72069af23e7f	■正常		绑定主机 续费 更多 ▼

在弹出的绑定主机窗口中,选择一个待绑定的主机。

选择绑定的主机



绑定主机			×
配额版本 旗舰版 到期时间	配额ID 246	b971a-1036-40f4-92c4	I-b0eb3241e895
注: 一个配额只能绑定一个主机, 且只能	绑定agent在线的主机。如未找到可选服务器,请查	语agent状态。	
可选服务器 (共1个) 🕜		已选服务器 (共1	个)
■ 服务器名称	服务器ID	服务器名称	服务器ID
ecs-bahuan	a1983984-390b-48c6-ab6d-f5cc71cd026b	ecs-bahuan	a1983984-390b-48c6-ab6d-f5
	确认取消		

单击"确定",完成主机的绑定,HSS 自动为主机开启防护。

2.11.3 升级配额版本

若您当前的防护配额的版本无法满足您的业务需求,您可以根据需要将企业主机安全服务的版本升级为"旗舰版"。

若您有网页防篡改版的业务需求,您需要参照购买防护配额重新购买。

2.11.3.1 前提条件

- 已获取管理控制台的登录账号 (拥有 HSS Administrator 与 BSS Administrator 权限) 与密码。
- 已购买"企业版"防护配额。
- 待升级的防护配额的"配额状态"为"正常","使用状态"为"空闲"。
- 多个防护配额同时升级时,请确保待升级的防护配额为相同的版本。
- 2.11.3.2 升级版本

登录管理控制台。

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。



在左侧导航栏中,选择"主机管理 > 防护配额",在需要升级配额的"操作"列,单击"更多 > 升级规格",如0所示。。

升级规格

批量解绑	企业版 🔻 所有配额状态	▼ 所有使用状态	▼ 配额ID	▼ │ 请输入关键字
配额类型/版本	配额ID	配额状态	使用状态	操作
主机安全防护 企业版	09fbbc16-3755-4421-b5b6-99b47dec6d8e	■正常	 空闲 	绑定主机│续费 更多▼
主机安全防护 企业版	4aed4abf-cb8e-4aeb-812c-79091582571d	■正常	 空闲 	返り 绑定主机 頻 解绑配額
□ 主机安全防护 企业版	6f2bde9e-6d69-49be-a2d1-b0a369d5a306	■正常	 空闲 	#定主机 续费 更多 ▼

在"主机安全配额升级规格"页面,设置升级后的规格。

1. 选择升级后的规格

支持升级为"旗舰版"。

- 2. 需要升级规格的主机安全配额
- 请确认需要升级规格的防护配额的"当前区域"、"当前计费模式"、"当前规格"和"升级后规格"
 无误。
- 处理无法进行升级操作的防护配额后,才能提交升级规格任务。
- 若主机安全配额处于"已过期"或者"已冻结"状态,无法进行升级操作。

请先进行移除或者续订。

■ 若主机安全配额处于"使用中"状态,无法进行升级操作。

在不影响业务场景的情况下,您可以选择"允许升级时了关闭防护",或者移除。

🛄 说明

升级规格时关闭防护可能会造成当前云服务器业务中断,请谨慎操作。

在页面右下角, 单击"立即购买", 进入"详情"界面。

确认订单无误后,请阅读并勾选"我已阅读并同意《企业主机安全免责声明》"。

单击"去支付",进入"付款"页面,付款后,完成主机安全配额的升级规格操作。

2.11.4 解绑配额

● 解绑配额后, HSS 会关闭主机防护, 无法检测主机存在的潜在风险, 请谨慎操作。



您可将解绑后的空闲配额分配给其他主机继续使用或退订无需使用的配额,避免造成配额资源的浪费。

2.11.4.1 解绑机制

- 在防护配额页面,通过手动解绑配额的方式,解除绑定的配额。
- Agent 离线 30 天后,自动解绑配额。

2.11.4.2 前提条件

- 已获取管理控制台的登录账号与密码。
- 主机已绑定配额。
- 2.11.4.3 解绑基础版/企业版/旗舰版配额

登录管理控制台。

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。 在"主机管理"页面,选择"防护配额"页签,进入防护配额列表页面。

查看主机安全防护配额

	主机管理 ②			购买主机安全 告誓	通知设置 手动检测
总览 主机管理	企业项目 所有项目 🔻	C			
风险预防 ▼ 入侵检測 ▼ 高级防御 ▼ 由会注意 ▼	云服务器 服务器组 防护者	۶.			
 × maxim 安装与配置 网页防要故 	旗舰版 配称使用	配额状态	企业版 配额使用	配额状态	
	4个 単現中(0) 空雨(4)	4个 単正第 (2) 単过期 (0) 目示系統 (2)	57	使用中 (0) 空间 (5)	正葉 (4) 已过期 (0) 已流統 (1)
	批量新加 配線类型/版本	「所有版本 × 」 所有配数状态 × 配額D	所有使用状态 ▼ 配線状态	配款D ▼ 语输入关键字 使用状态 操作	QCC

在防护配额列表页面,选择"更多",单击"解绑配额",解除绑定的配额,如0所示。 解绑配额



批量角	释绑		所有版本 🔻	所有配额状态	▼ 所有使用状	ক ▼	配额ID ▼
	配额类型/版本	配额ID		配额状态	使用状态	操作	
	主机安全防护 旗舰版	9e3c883f-bf25-4322-a206-c62ea8	327510	■正常	● 使用中 ecs-54f8	绑定主机	续费更多▼
	主机安全防护 企业版	9e3c883f-bf25-4322-a206-c62ea8	327590	■正常	⊖ 使用中 ecs-54f8c	绑定主机	121) 解绑配额 升级规格
					_ _		

门 说明

您也可以勾选待解绑配额,单击"批量解绑",批量解绑配额。解绑配额后,HSS将无法检测您主机存在的潜在风险,请谨慎操作。

在弹出的解绑配额对话框中, 单击"确定", 解除绑定。

2.11.4.4 解绑网页防篡改配额

登录管理控制台。

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。 在左侧导航树中,选择"网页防篡改",进入网页防篡改的防护列表界面。

查看企业主机安全"网页防篡改版"防护配额

企业主机安全	防	护列表 ⑦										购买网页防营	良政
总宽													
主机管理		企业项目 所有项目	*	C									
风脸预防													
入侵检测	-	0		•		0		4		_	1		
高级防御	-	已防御篡改攻击 🕖	防护主	:机数 🕖	防护	■目录 🕖	防篡改	記額	使用中	0	空闲	配额详情	
安全运营													
安装与配置		开启助护 关闭防	ث						服务器名称		▼ 语输入关键字	Q	С
网页防装改		服务器名称/ID	IP地址	操作 🍞	服务器状态	Agent状态 🍞	防护 🍞	动态防篡改状	ō	版本	操作		
防护列表		servicestage-nodel 81e97d86-04d4-42	172.16.0.106 (私有	Linux	运行中	未安装	◎ 关闭	未开启		无	开启防护丨防护	设置 查看报告	
安装与配置		ecs-5364w 930db6a5-e930-44	172.168.101.246 (172.16.0.96 (私有)	Linux	关机	未安装	● 关闭	未开启		无	开启防护 防护	设置 查看报告	

单击"配额详情",进入网页防篡改防护配额详细信息页面。

配额详情



配额使用		配额状态			
17	使用中(0) 空闲(1)	(1↑	正常 (1) 已过期 (0) 日示绪 (0)	
批量解绑	所有配额状态	, 所有使用状态	▼ 配额ID	▼ │ 请输入关键字	QC
配额类型/版本	配額ID	配額状态	使用状态	操作	
网页防篡改版	20bd4630-b55b-42c6-a448-3f0db6d43349	■正常	😶 空闲	绑定主机 续费 更多 ▼	

在防护配额列表页面,选择"更多",单击"解绑配额",解除绑定的配额,如0所示。

解绑网页防篡改配额

批量創	解绑		所有版本	•	所有配额状态	•	所有使用状态	2 *	配着	顷ID	•
	配额类型/版本	配额ID			配额状态	使用状	态	操作			
	网页防篡改版	9e3c883f-bf25-4322-a206-c62ea83	327510		■正常	● 使 ecs-54	用中 f8	绑定主机	续费	更多 •	-
									戶	御配额	
									升	级规格]

🛄 说明

您也可以勾选待解绑配额,单击"批量解绑",批量解绑配额。解绑配额后,HSS将无法检测您主机存在的潜在风险, 请谨慎操作。

在弹出的解绑配额对话框中,单击"确定",解除绑定。

2.12 (可选) 管理企业项目

2.12.1 管理项目和企业

企业项目仅针对企业用户使用,只有开通了企业项目的客户,或者权限为企业主帐号的客户才可见。 如需使用该功能,请联系您的客户经理申请开通。企业项目是一种云资源管理方式,企业项目管理服务 提供统一的云资源按项目管理,以及项目内的资源管理、成员管理。

2.12.1.1 创建项目并授权

● 创建项目

进入管理控制台页面,单击右上方的用户名,在下拉列表中选择"统一身份认证",进入统一身份认 证服务页面。选择左侧导航中的"项目",单击"创建项目",选择区域并输入项目名称。



授权

通过为用户组授予权限(包括资源集和操作集),实现项目和用户组的关联。将用户加入到用户组, 使用户具有用户组中的权限,从而精确地控制用户所能访问的项目,以及所能操作的资源。具体步骤如 下:

在"用户组"页面,选择目标用户组,单击操作列的"权限配置",进入"用户组权限"区域。在新 创建的项目所在行,单击"设置策略",给对应项目选择需要的云资源权限集。

在"用户"页面,选择目标用户,单击操作列的"修改",进入修改用户页面。在"所属用户组"区域为用户添加用户组,完成授权过程。

2.12.1.2 创建企业项目并授权

● 创建企业项目

进入管理控制台页面,单击右上方的"企业",进入企业管理页面。选择左侧导航中的"企业项目管理",单击"创建",输入名称。

门 说明

开通了企业项目的客户,或者权限为企业主帐号的客户才可以看到控制台页面上方的"企业"入口。如需使用该功能,请联系技术支持申请开通。

● 授权

通过为企业项目添加用户组,并设置策略,实现企业项目和用户组的关联。将用户加入到用户组, 使用户具有用户组中的权限,从而精确地控制用户所能访问的项目,以及所能操作的资源。具体步骤如 下:

在新创建的企业项目所在行,单击操作列的"更多 > 查看用户组",进入"用户组"区域。单击 "添加用户组",在左侧选择目标用户组,移入右侧区域。继续下一步设置策略,选择需要的云资源权限 集。

进入"人员管理 > 用户管理"页面,选择目标用户,单击操作列的"加入到用户组",在左侧区域选择已设置策略的用户组,移入右侧区域,完成授权过程。

● 关联资源与企业项目

企业项目可以将云资源按企业项目统一管理。

- 购买企业主机安全时选择企业项目
- 在购买页面,"企业项目"下拉列表中选择目标企业项目,实现资源与企业项目关联。

- 资源迁入



- 对于帐号下的存量弹性云服务器/裸金属服务器, 您可以在"企业项目管理"页面将资源迁入目标企业项目。

- "default"为默认企业项目,帐号下原有资源和未选择企业项目的资源均在默认企业项目内。

更多信息。

- 管理所有项目

如果您已开通企业项目,您可以在"所有项目"中,对您拥有的所有主机进行批量安全配置,可避 免您到每个企业项目中对主机进行重复配置。

● 绑定主机配额

在"所有项目"中,任意一个企业项目中的配额绑定给任意一个企业项目中的主机,实现配额共享 使用,但计费仍归属于配额所在企业项目。

● 批量安全配置

对所有主机进行安全配置,包含告警白名单、登录白名单、恶意程序自动隔离查杀和告警通知等。

● 部署策略组

"所有项目"中的策略组,可以部署给您所在的任意企业项目中的任意一台开启旗舰版防护的主机。 "所有项目"中的策略组独立于其他每一个企业项目的策略组,与其他企业项目的策略组互不干扰。

● 订阅所有项目安全报告

"所有项目"的安全报告独立于其他每一个企业项目的安全报告,订阅设置与报告内容互不干扰。

在"所有项目"中进行批量配置后,若对其中某一个企业项目中的安全配置有差异化需求,您可以 到具体的企业项目中进行单独配置。在某个企业项目中的差异化配置是独立的,对其他企业项目不产生 影响。

2.12.1.3 绑定主机配额

如下,以在"所有项目"中为任意一个企业项目的主机绑定"主机安全旗舰版配额"为例说明。 登录管理控制台。

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。

选择"主机管理 > 所有项目 > 防护配额",进入"防护配额"页面,在防护配额页面,您可以查看 到所有项目的防护配额,如0所示。

防护配额页面

194



企业主机安全	主机管理 ⑦				购买主机安全告	警通知设置 手动检测
規定	2 企业项目 所有项目	- C				
主机管理						
风险预防						
入侵检测 🔻	_	3				
高级防御	云服务器 服务器组 防	户配额				
安全运营 ▼						
安装与配置	旗舰版		企业版			
同市防管政						
132473464	自己被对此开始	BCRMAAS	AC48XU2/HJ		BCBRHA.SS	
容器安全 。						
志勢感知 ピ		正第 (8)				正常 (1)
弹性云服务器 d ^o	11↑ ■ 空词(7)	4) 日11个 日志編(3)	3↑	使用中(0) ■空闲(3)	3↑	■ 已过期(0) ■ 已添結(2)
	批量续费	所有版本 ▼ 所有配额状态 ▼	所有使用状态 ▼	配额ID	▼ 请输入关键字	QCC
	配额类型/版本	配板ID	配额状态	使用状态	倒计时	操作
	□ 主机安全防护 旗舰版	f4b66b91-c29a-488d-919b-27b24dd98885	■正常	● 使用中 ce2	28天后到期 	鄉定主机 续费 《
	□ 主机安全防护 旗舰版	a4a3544c-7cfd-469f-b75a-fe9a2b88aa5b	■正常	😌 使用中	28天后到期 	绑定主机 续费

在配额列表中,选择"使用状态"为"空闲"的配额,单击"绑定主机",为主机绑定配额。

为主机绑定配额

批量续费	所有版本	所有配额状态	▼ 空闲	▼ 配額ID ▼	i 请输入关键字 Q C C
配额类型/版本	配额ID	配额状态	使用状态	倒计时	操作
主机安全防护 旗舰版	fb58f180-ae52-40b4-a001	■正常	💮 空闲	28天后到期 	绑定主机 续费 更多 ▼
主机安全防护 旗舰版	21a87b02-42b9-4445-80df	■正常	😶 空闲	28天后到期 	绑定主机 续费 更多 ▼
主机安全防护 旗舰版	9e3c883f-bf25-4322-a206	■正常	😐 空闲		绑定主机 续费 更多 ▼

在弹出的配额详情对话框中,选择待绑定配额的主机。

绑定配额



额版本	5. 旗舰版	配额ID fb581	180-ae52-40b4-a001-86	i62cfd15534
期时间	128天后到期			
	▶配額只能绑定一个主机, Ⅰ ■哭(共7小)の	且只能绑定agent在线的主机。如未找到可选服务器,请查	看agent状态。 日选肥冬哭 (共1个)	
	服务器名称	服务器ID	服务器名称	服务器ID
	HSS xd	bfe999fd-0c33-4f43-baae-90cd9608e552	win-406713	57fe4ef7-255b-487b-bc92-96
		7e998f85-6099-4723-8f27-042cac507420		
	测试多项目test	51c69cf3-dee9-43b9-8e9a-4d81ebe0fe9e		
	ce1	84dfe8e9-5fdb-4181-8e94-490e2f4d1164		
~	win-406713	57fe4ef7-255b-487b-bc92-96e2e7f2ad96		
	ce2	b45149e3-ea55-4004-81a6-ff2b9fd0c1fd		
	测证	8bf4a400-6f3b-47c9-9d82-982ace4091ea		

单击"确定",完成配额绑定。绑定配额后,您可以在云服务器列表中,查看到该主机已开启防护。

2.12.1.4 批量安全配置

"所有项目"仅作为用户对每一个企业项目进行批量配置使用,不作为实际生效的配置,实际生效的 配置仍以各自所属企业项目中显示的配置为准。

须知

在"所有项目"中可以进行批量配置操作的包含:告警白名单、登录白名单、恶意程序自动隔离查杀和告警通知。

如下以"配置告警白名单"为例说明,"企业项目一"中无告警白名单,"企业项目二"中无告警白 名单。

选择"入侵检测 > 事件管理",进入事件管理页面。

事件管理页面



企业主机安全	事件管理 ⑦				文件隔离箱	购买主机安全
急览	2 企业项目 所有项目	• C				
风於称訪						
入侵检测 ▲	安全告警统计					
事件管理 1	存在告誓的服务器	5	待处理告警事件	13 日处理的	吉警事件	2
白名単管理 高级防御 ▼	已拦截IP	0	已隔离文件	1		
安全运营 🔻						
安装与配置						~
网页防篡改 🔻	◎ 账户暴力	「解●● 账户异常登录●●	◎ 恶意程序 (云查杀)	关键文件变更 网站。	新门 🥝 反理 Shell 🔮 异常 Shell	
容器安全 6	已开启防护 (13) 🔮 高危命令社	い行 🔮 自启动检測 🥹	风险账户 🥑 提权操作 🔮 Rootkit的	呈序		
志勢感知						
弹性云服务器 6	告警事件列表					
				Bichadat - R	佐藤かみ - 10月1日日本1月から10月	
	全部 15		点击	上方"已拦截IP",可查看攻击IP是否被打	Hand Hand Hand Hand Hand Hand Hand Hand	
	账户暴力破解 0	告警名称 受影响服务	奇纖名称/IP 简述	发生时间 处理时	町 状态 ♡ 处理方式	操作
	账户异常登录 0	进程异常行为 zhangxiao 192.168.0.	dong 15,192.168.1.163 哈岩值:4845dbb7c2e	3e064d 2020/09/08	未处理	处理
	恶意程序 (云童杀) 3	Ce1 风险账户 192.168.0.	206 账号名:aa,用户启动	Shell: / 2020/09/08	未处理	处理

在"企业项目"下拉列表中,选择"所有项目"。

在告警事件列表中,以"恶意程序(云查杀)"为例,将"恶意程序(云查杀)"加入告警白名单,如0所示。

hп	λ	生	敬	白	攵	畄
лн	/ \		言	ш	п	Ŧ

告警事件列表					
全部	15	批量处理 最近24小时 ▼ 服务器名件 点击上方"已扫翻P*,可查看攻击P星石被拦截、以	你 ▼ 受影 1及可以解除拦截。	周服务器名称/I₽	QC
账户暴力破解	0	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 ⑦	处理方式	操作
账户异常登录	0	惑意程序(未处理	2	处理
恶意程序 (云查杀)	3		×		处理
进程异常行为	3	处理告警事件			
关键文件变更	0	告警名称 状态 IP地址 前述		加入告留	处埋
网站后门	0		0010d1		
反3单Shell	0	シリンボーン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シ	安全不会再		
异常Shell	0	对版制作进行音智。			
高危命令执行	0	abù, 80%			

选择"白名单管理 > 所有项目 > 告警白名单",进入告警白名单页面。

告警白名单页面



企业主机安全	白名单管理 ⑦	购买主机安全
总览 主机管理	企业项目 所有项目 ▼ C	
风险预防 入侵检测 事件管理	 ▼ ● ●	
 白名单管理 高級防御 安全运营 	今入 専业全部 割除 ・ 合物完成 SHA256 cmdUne 数据来源	金部提証 ◆ 総特(SHA25. ▼) 街前人关键字推奏 Q C K応討問 接作 Propring 16-27-20 CUL 0000 開始
安装与配置 网页防复改		2020/09/05 23:42:29 GMT-08:00

在"企业项目"下拉列表中,分别选择"企业项目一"和"企业项目二",查看"恶意程序(云查 杀)"均已分别添加到"企业项目一"和"企业项目二"下的告警白名单中。

企业项目一告警白名单

企业项目	• C								
告警白名单 登录白	名单								
导入导出全部	册你会			全部类型	•	哈希(SHA25 ▼ 请编入关	建字搜索	Q	С
告警类型	SHA256	cmdLine	数据来源		标	记时间	操作		
恶意程序 (云童杀)	08a7baa28dd268f8a12bc1f6fd9586		手动标记		20	20/09/08 16:37:00 GMT+08:00	删除		
自启动检测	e3b0c44298fc1c149afbf4c8996fb92		手动标记		20	20/09/05 23:42:29 GMT+08:00	删除		

若 "企业项目二" 中需要 HSS 对添加的 "恶意程序 (云查杀)" 事件进行告警, 您可以在 "企业项目二" 中将添加的告警白名单删除。

"企业项目二"中的告警白名单删除后,对企业项目一中的已添加的告警白名单不产生影响。

2.12.1.5 部署策略组

"所有项目"中的策略组,可以部署给您所在的任意企业项目中的任意一台开启旗舰版防护的主机。

以"在"所有项目"中创建策略组"hss_test",将创建的策略组部署给任意一台开启旗舰版防护的 主机"为例说明。

选择"安全运营 > 策略管理 > 所有项目",单击"复制",在所有项目中,创建策略组。

复制默认策略组



企业主机安全		策略管理 ⑦						购买主机安全
总流		2 企业项目 所有项目	• C					
主机管理								
风险预防	Ŧ							
入侵检测	*	删除					请输入策略组名称	QC
高级防御	*	策略组名称	ID	描述	支持的版本	关联服务器数	操作	
安全运营		default_enterprise_policy_gro	65aa77a0-ca81-4b5b-abd9-5	企业版策略组	企业版	0		
安全报告		default_premium_policy_gro	da09f1c4-6c0f-465f-8f7a-65	33	旗舰版	6	3 無制	
策略管理 1								
安装与配置								
网页防篡改	*							

在弹出的窗口中,输入策略组名称,例如"hss_test",如0所示。

复制策略组		×
* 策略组名称	hss_test	
描述	A	
	确定取消	

配置策略组

单击"确定",完成策略组的创建。

您可以根据您的需要单击策略组的名称,配置策略组。

选择"主机管理 > 所有项目",选择任意一台开启旗舰版防护的主机,单击"部署策略",为主机部 署创建的"hss_test"策略组。

部署自定义策略



企业主机安全		主机管理 ③ 與哭主視念金 手动金属 手动金属 <th< th=""><th>1</th></th<>	1
总统 主机管理		全业项目 所有项目 C	
风脸预防	*		
入侵检测	•		
高级防御	*		
安全运营	*		
安装与配置		✓ 服务器名歌/」 IP地址 操作系统 服务器状态 Agent状态 防护状态 检测结果 版本质测时间 服务器组 頻繁组 操作	
网页防篡改 	°	H55	
态势感知	ø	2011年1月1日 - 2015年1日 - 2015日 - 20150	
弹性云服务器	e		

在弹出的窗口中,选择策略组,如0所示。

选择待部署的策略组

			×
🛕 您确定要在已	开启旗舰版	的服务器上部署策略吗	?
请选择要部署的策略组	hss_test	•	
	确定	取消	

单击"确定",完成策略组的部署。



3 常见问题

3.1 产品咨询

3.1.1 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。

3.1.1.1 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0所示。

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:

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	• 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。		
	• 集成多种杀毒引擎,深度查杀主机中的恶意程序。		
	• 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。		
	 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。 		
Agent	• 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 。		
	 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) 		



组件	说明		
	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。		
	• 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。 		
	• 根据操作系统版本选择对应的安装命令/安装包进行安装。		
	 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。 		

3.1.2 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。

3.1.2.1 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。

3.1.2.2 Linux Agent 相关进程

Agent 进程运行账号:root。

Agent 包含以下进程:

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/host guard



Agent 进程名称	进程功能	进程所在路径
upgrade	该进程用于 Agent 版本的 升级。	/usr/local/hostguard/bin/upgr ade

3.1.2.3 Windows Agent 相关进程

Agent 进程运行账号: system。

Agent 包含以下进程:

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.e xe
HostWatch.exe	该进程用于 Agent 进程的 守护和监控。	C:\Program Files (x86)\HostGuard\HostWatch.e xe
upgrade.exe	该进程用于 Agent 升级。	C:\Program Files (x86)\HostGuard\upgrade.exe

3.2 开通与配置

3.2.1 如何安装 Agent?

- Linux 客户端,请参见 2.1.2.1 Linux 版本。
- Windows 客户端,请参见 2.1.2.2Windows 版本。

3.2.2 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;

3.2.3 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 0 所示。

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

3.2.4 如何筛选未安装 Agent 的主机?

登录管理控制台。

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。

在主机管理页面,筛选未安装 Agent 的云服务器,如 0 所示。

筛选未安装 Agent 的主机



企业主机安全	主机管理()										告答通知设置	手动检测
总流 主机管理 1	2 云服务器	服务	叢虹 防护	配額									
风险预防 * 入侵检测 *	二 全	开启防护	A 关闭防	护	略 分配子	相			183	·蜀名称 🔻	请输入关键字(3	Ľ C
 高级防御 安全运营 	服务器名	称		Q	服务器ID		Q	IP地址		Q	5	臺灣	重要
安装与配置	摄作系统	全部		•	Agent状态 策略组	全部 全部	*	防护状服务器	は 全部 地	•			
	版本选择	全部		¥	4 服务器状态	未安装 在线			πıν				
		务器名称/ID	IP地址	操作系统	服务器状态	篇线 AgenuAge	NO37-4/084	检测结果	版本	服务器组	策略组	操作	
	b i	s-hss ad4f2c-75f9-4	192.168.0.234 (Linux	运行中	在线	🕑 开启	有风险	<u>据税</u> 板 (网页防额改赠送) test1	default_wtp	关闭防护 切换版:	5 更多 ▼
	□ ec 23	s-hss-win 62e3c2-54e1-	192.168.0.114 (Windows	运行中	在线	🕑 开启	有风险	旗舰板 (包年/包月)		default_pre	关闭防护 切换版:	↓ 更多 ▼

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"。

3.2.5 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,可能是 Agent 与服务器间通信异常。请参见本文进行排查。

- 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。

3.2.5.1 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 3~5 分钟左右控制台才会刷新。

3.2.5.2 处理方法

排查网络故障。

待网络恢复正常后:

206



- 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。

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。

重启 Windows Agent

🔤 任务管理器 💶						
文件(F) 选项(O) 查看(V)						
进程 性能 应用历史记	晟 启动	动用户	详细信息	服务	2	
名称		PID	描述			
🔍 HaccService		4980	HaccSer	vice		
Generation Head Head Head Head Head Head Head Head		主机保护	者客户前	耑服务		
🔍 hidserv		2000	Human	Interfac	e Device Serv	
🔍 hns			主机网络	服务		
🕼 HostGuard 🛛 🗿		4856	HostGua	ard		
🔍 HostWatch	开始(S	5)		h		
🔍 H HDP Tra	停止(T)	_	DP Tr	aceLogC	
🔍 HvHost	重新启	动(R)	4	傍		
iaStorAfsService	打开服	冬(1)		ptane	(TM) Memory	
icssvc 🔍	左任 埋	(い)	v) O)		点服务	
iDeskService	11.5818 ## A IN¥	(SR)(U) (細(左自(D))		rice		
igfxCUIService2	HUITSF -			.D Gra	phics Control	
🔍 IKEEXT	4972	IKE and	AuthIP	IPsec Keying		
C. InstallService		Microso	ft Store	安装服务		

● 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。若无回显信息,请 3.2.7 如何卸载 Agent?,重新 3.2.1 如何安装 Agent?。

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 3.2.7 如何卸载 Agent?,再重新 3.2.1 如何安装 Agent?。

ullet

3.2.6 安装 HSS Agent 有什么影响?

安装 HSS Agent 不影响在线业务,也不会影响服务器的运行状态。

企业主机安全服务 (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。

更多有关 HSS Agent 的信息,请参见 3.1.2 什么是 HSS 的 Agent?。

3.2.7 如何卸载 Agent?

3.2.7.1 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。

3.2.7.2 前提条件

- 已获取管理控制台的登录帐号与密码。
- 云服务器的 "Agent 状态"为 "在线"。

3.2.7.3 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。

登录管理控制台。

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。 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"。



在弹出的"卸载 Agent"界面中,如 0 所示,选择需要卸载 Agent 的云服务器。

卸载	čAgent						×
警告: 离线地	卸载Agent后主机安全服务将无法 状态下的服务器无法从控制台自动能	<mark>去为该服务器提供</mark> 卸戴Agent,您可	<mark>任何防护。</mark> 以手动执行卸载:	如何手动卸载	Ager	nt?	
请选	择需要卸载Agent的服务						
可选朋	送券器 (共1个) ⑦	服务器名称	▼ │ 请输)	、关键字 (ג	已选服务器 (共1个)	
	弹性服务器名称/IP	操作系统	防护状态	当前版本		弹性服务器名称/IP 操作系统	
C	ecs-hss-001 .6.211 (弹性公网) 192.168.0.170 (私有)	Linux	关闭	无		ecs-hss-001 .6.211 (弹性公网) Linux 192.168.0.170 (私有)	
			-	TRAN	,		
			确定	取消	1		

卸载 Agent

单击"确定"。

云服务列表"Agent 状态"显示为"离线", 卸载 Agent 成功。

3.2.7.4 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

a. 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。 b. 在任意目录执行以下命令,卸载 Agent。

i. 针对 ".rpm"格式的安装包,执行命令: rpm -e --nodeps hostguard
ii. 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

- c. 登录需要卸载主机安全服务 Agent 的云服务器。
- d. 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"。

3.3 告警事件处理

3.3.1 HSS 如何拦截账户暴力破解?

3.3.1.1 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 0 所示。

新增规则

Chain INPUT (policy ACCEPT)			
target prot opt source	destination		
TN HTDS MYSOLD BTP DROP ton	0000/0	0 0 0 0/0	ton dat:3306
TN HTDS MYSOLD DENV DROP top	0 0 0 0/0	0.0.0.0/0	tcn dnt+3306
	0.0.0.0/0	0.0.0.0/0	tep upt.3300
Chain EOPWARD (nalicy ACCEPT)			
threat protocol	dectination		
target procopt source	destination		
Chain OUTPUT (policy ACCEPT)			
chain ourfor (policy Accert)	4+		
target prot opt source	destination		
	(2) (2)		
Chain IN_HIDS_MYSQLD_BIP_DROP	(1 references)		
target prot opt source	destination		
Chain IN_HIDS_MYSQLD_DENY_DROP	<pre>> (1 references)</pre>		
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。

3.3.1.2 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)和 Centos 8.0及以上版本的主机,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。

3.3.1.3 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。

3.3.1.4 查看账户破解检测结果

登录管理控制台。

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。

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0所示。

账户破解防护



企业主机安全	事件管理 ①	文件隔离箱
总选主机管理	安全告誓统计	
风脸预防	存在告留的服务器 2 传处理告留事件 3 已处理告留事件	0
入侵检测 •	日活動P 1 日間第2/年 0	
白名单管理	防护已完全开启 防护已完全开启	*
 高級防御 マ 安全运营 マ 安装与配置 	● 院中県大陸部 ● 院中県本登表 ● 医登録本(法量本) ● 逆程用和行方 ● 关键文件变更 ● 网站后门 ● 同葉Shell ● 用菜Shell ● 日井田訪知 (13) ● 回意动地海 ● 建校連件 ● Rootkit留來 ●	高危命令执行
网页防复改 · ·	告警事件列表	
	金部 2 3 武法処理 武法(24)対 ・ 服务器名称 ◆ 受到地區防器名称//P 点击上方 "已迁載(P",可量署改法員,以及可以編除注載。	QC
	死-最力或解 2 告警名称 受影响服务器名称/IP 筒述 没生时间 处理时间 状态 ♡ 处理方式 当	操作
	既户募業登录 0	比理
	専髪輝穿 (云意外) 0	达理
	进程异常行为 0	

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。

3.3.1.5 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
 3.3.3 如何手动解除误拦截 IP? 。

须知

若您手动解除被拦截的可信 IP,仅可以解除本次 HSS 对该 IP 的拦截。若再次发生多次密码输错,该 IP 会再次被 HSS 拦截。



3.3.2 如何解决部分 Linux 系统的账户破解防护功能未生效的问题?

3.3.2.1 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。

3.3.2.2 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.

3.3.2.3 存在问题的镜像版本

- 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)

3.3.3 如何手动解除误拦截 IP?

在 30 秒内,账户暴力破解次数达到 5 次及以上,或者 3600 秒内,账户暴力破解次数达到 15 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。若已拦截 IP 为合法 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),您可以参照本章节手动解除拦截 IP。

手动解除被拦截的可信 IP,仅可以解除本次 HSS 对该 IP 的拦截。若再次发生多次密码输错,该 IP 仍会被 HSS 拦截。

门 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。
- 当 HSS 检测到拦截 IP 超过默认拦截时间后, 主机不再被暴力破解攻击, 将会自动解除拦截。

3.3.3.1 手动解除拦截 IP

登录管理控制台。



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。 在左侧导航树中,选择"入侵检测 > 事件管理"。 在安全告警统计区域中,单击"已拦截 IP"。 在弹出的"已拦截 IP"页面,勾选误禁 IP 后,单击列表上方的"解除拦截",解除拦截 IP。

3.3.4 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。

3.3.4.1 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帐号, 会被系统判定为弱密码。

3.3.4.2 排查弱口令

登录管理控制台。

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。

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。

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。

3.3.4.3 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	以 Windows 10 为例说明。 1. 登录 Windows 主机系统。 2. 单击左下角的 , 然后单击 ②, 弹出 "Windows 设置"窗	无
	3. 在"Windows 设置"窗口中, 单	



系统名称	修改登录口令	说明
	击"帐户"。 4. 在左侧导航栏中,单击登录选项。 5. 在"登录选项"页面,请根据页面 提示信息修改服务器密码。	
Linux 系统	登录 Linux 服务器,执行以下命令, 修改用户登录口令。 passswd [<user>]</user>	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。 说明 "user"为登录用户名。
MySQL 数 据库	 登录 MySQL 数据库。 执行以下命令,查看数据库用户密码。 SELECT user, host, authentication_string Fromuser; 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。 SELECT user, host password Fromuser; 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。 SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码'); 执行以下命令,刷新修改的密码信息。 	无
	flush privileges;	
Redis 数据	1.	• 若已存在登录口令,则将



系统名称	修改登录口令	说明
库	2. 执行以下命令,修改弱口令。	其修改为复杂口令。
	requirepass <password>;</password>	• 若不存在登录口令,则添加为新口令。 说明 "password"为登录口令。
Tomcat	 打开 Tomcat 根目录下的配置文件 "conf/tomcat-user.xml"。 修改 user 节点的 password 属性 值为复杂口令。 	无

3.3.5 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
- c. 密码不为用户名或用户名的倒序。
- 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/帐号使用不同的密码。
- 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。

3.3.6 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略?

3.3.6.1 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。

3.3.6.2 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



🛄 说明

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

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
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"。

b. vi /etc/pam.d/common-password

c. 找到文件中的以下内容:

password requisite pam_cracklib.so retry=3 minlen=8 difok=3



d. 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0所示。

e. 示例:

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

3.3.7 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:

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0所示。

输入命令



程序(1)
🔁 secpol.msc
▶ 查看更多结果
secpol.msc 注销

选择"账户策略 > 密码策略"后执行以下操作,如0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。

本地安全策略配置项

220



🖥 本地安全策略		
文件 (2) 操作 (A) 查看 (Y) 帮助 (H)		
🗢 🔿 🖄 📰 💥 🗟 🔽 🖬		
 ■ 安全设置 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	 ● 金码必须符合复杂性要求 ● 密码长便用期限 ● 密码最长使用期限 ● 密码最长使用期限 ● 密码最大使用期限 ● 强制密码历史 ● 用可还原的加密未储存密码 	安全设置 已启用 0 个字符 0 天 42 天 0 个记住的密码 已禁用
J		J

运行 gpupdate 命令刷新策略,刷新成功后,如0所示,以上设置被应用与系统中。

执行结果





3.4 漏洞管理

3.4.1 如何处理漏洞?

3.4.1.1 处理方法和步骤

查看漏洞检测结果。

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手动重启。
- Linux 系统 Kernel 类的漏洞修复完成后需要手动重启。

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 3.6.4 如何立即执行手动检测?。

3.4.2 漏洞修复后,为什么仍然提示漏洞存在?

在企业主机安全控制台上使用漏洞管理功能修复系统软件漏洞时,如果提示漏洞修复失败,请参见 以下可能原因:

门 说明

建议您参考章节对您服务器上的漏洞进行修复。

3.4.2.1 Windows 系统服务器

● **补丁安装包**下载**不成功**

您的服务器可能无访问公网权限,请在能访问 Internet 后,重新执行漏洞修复操作。

● **补丁安装包不**匹配

请进一步确认补丁安装包的详细信息,如果补丁确实与您的服务器系统不匹配,建议您在"漏洞管理"界面中**忽略**该漏洞。

● **另一个补丁**正在**安装**

由于服务器不能同时运行两个补丁安装程序,建议您等当前补丁安装完成后尝试重新执行漏洞修复 操作。

● 检查其他设置



- 服务器开启了系统自动更新补丁功能。在确认服务器已更新该漏洞后,建议您在漏洞管理界面
 中忽略该漏洞。
- 服务器安装了更新的补丁将旧补丁覆盖(如,2016及以上系统,最新的月度补丁会覆盖以前的 所有补丁)。在确认无误后,建议您在漏洞管理界面中忽略该漏洞。
- 其他安全软件对补丁安装进行了拦截(如 "360 安全卫士服务器版"),您可以先暂停使用安全 软件,待漏洞修复后,在开启安全软件。

须知

微软已于 2020 年 1 月 14 日停止对 Windows Server 2008 R2 系统的更新和维护,如果需要继续使用该系统,则需要购买相应的 ESU (扩展安全更新) 密钥并进行激活或更换 Windows 操作系统版本。

3.4.2.2 Linux 系统服务器

● 无 yum 源配置

您的服务器可能未配置 yum 源,请根据您的 Linux 系统选择 yum 源进行配置。配置完成后,重新 执行漏洞修复操作。

● yum 源没有相应软件的最新升级包

切换到有相应软件包的 yum 源, 配置完成后, 重新执行漏洞修复操作。

● **内网环境连接不上**公网

在线修复漏洞时,需要连接 Internet,通过外部 yum 源提供漏洞修复服务。如果服务器无法访问 Internet,或者外部 yum 源提供的服务不稳定时,可以使用天翼云提供的进行漏洞修复。

内核老版本存留

由于内核升级比较特殊,一般都会有老版本存留的问题。您可通过执行 3.4.2.3 查看当前使用的内核版本是否已符合漏洞要求的版本。确认无误后,对于该漏洞告警,您可以在企业主机安全管理控制台的 "漏洞管理 > Linux 软件漏洞管理"页面进行**忽略**。同时,不建议您删除老版本内核。

3.4.2.3 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



操作系统	修复命令
Debian/Ubuntu	dpkg -l grep 软件名称
Gentoo	emergesearch 软件名称
SUSE	zypper search -dCmatch-words 软件名称

3.4.2.4 后续操作

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 3.6.4 如何立即执行手动检测?。

🗀 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。
- Windows 系统漏洞和 Linux 系统 Kernel 类的漏洞修复完成后需要手动重启主机,否则 HSS 仍可能为您推送漏洞消息。

3.4.3 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。

3.4.4 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手动重启主机。
- Linux 系统 Kernel 类的漏洞修复完成后需要手动重启主机,其它类型漏洞修复完成后不重启也能生效。

3.5 网页防篡改

3.5.1 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。

3.5.2 如何修改防护目录?

登录管理控制台。



在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在左侧导航栏中,选择"网页防篡改",进入"网页防篡改"界面。

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。

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。

企业主机安全		> 同页防银衣 / ecs-hss001					
总筑		② ③ □ □ □ □ □ □ □ □ □ □ □ □ □					
主机管理							
风险预防	*						
入侵检测	*		803.004 Grant Contraction Contraction Contraction				
高级防御	*						
安全运营	Ŧ	添加防护目录 启动	添加加於自要 启动运转备份 最多可添加50个物护目录。默认进行本地备份,请供描思的需求选择是否启动运转备份。				
安装与配置		防护目录	排除子目录	排除文件类型	本地备份路径	防护状态	操作 4
网页防复改		/hss/test			/backup	♥ 开启	暂停防护 编辑 删除
防护列表 1							
安装与配置							

防护设置

在"编辑防护目录"弹框中进行修改,单击"确定"完成修改。

编辑防护目录



编辑防护目录	×	
★ 防护目录:	/root/123 提示:请勿对操作系统目录进行防护, 例如:不对/bin进行防护。	
排除子目录:	例:/xxx/xxx 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:	例: log; js 多个文件 类 型请用分号隔开。	
★ 本地备份路径:	/root/wtp 提醒:本地备份路径与添加的防护目录不能重叠,否则将导致本地备 份失败!	
	明元	

3.5.3 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。
- 仅 Windows 系统支持特权进程。

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。

3.5.4 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放篡改。

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。

3.6 其他

3.6.1 如何使用 Windows 远程桌面连接工具连接主机?

3.6.1.1 操作步骤

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。

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0所示。

远程桌面连接



😼 远程桌面连接	
远程桌面 连接	
常规 显示 本地资源 稱	序 体验 高级
武法 武法	•
	3键 00):
本地设备和资源 选择您要在远程会 ✓ 打印机 (T) 详细信息 (M)	活中使用的设备和资源。 ☑ 剪贴板 (L)
 → 法项(0) 	

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0所示。

设置常规信息



😼 远程桌面	连接 🛛 🗖 🗖 🗾
N	远程桌面 连接
常规 昻	示 本地资源 程序 体验 高级
一登录设置	
	输入远程计算机的名称。
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	计算机 (C): ▼
	用户名: Administrator
	当您连接时将向您询问凭据。
	□ 允许我保存凭据 ⑧
注接设置	将当前连接设置保存到 RDP 文件或打开一个已保存的连接。 保存(S) 另存为(V) 打开(C)
🗻 选项 @	

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。

# 3.6.2 如何查看 HSS 的日志文件?

# 3.6.2.1 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/	• daemon.log:记录守护进程运
Windows	C:\Program Files (x86)\HostGuard\log\	行时相关日志。 • hostguard.log:记录监控进程 运行时相关日志。
		<ul> <li>hostguard_procmon.log: 记 录进程创建的信息。</li> </ul>



操作系统	日志所在路径	日志文件
		<ul> <li>urlconfig.log:只在安装时, 记录识别 region 信息。</li> </ul>
		• upgrade.log:记录升级时相关 日志。
		<ul> <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
hostguard.lo g	10M	保留 5 个最新的 "hostguard.log"日志文件。	不卸载 HSS Agent,会一 直保留日志信
hostguard_p rocmon.log	20M	保留 2 个最新的 "hostguard_procmon.log" 日志 文件。	息。
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_r sync.log	不限制	保留1个 "hostguard_rsync.log" 日志文件。	



# 3.6.3 如何开启登录失败日志开关?

# 3.6.3.1 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:

使用 root 权限登录主机。

查询 log_warnings 值, 命令如下:

## show global variables like 'log_warnings'

修改 log_warnings 值, 命令如下。

## set global log_warnings=2

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

# 3.6.3.2 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。

开户日志开关的操作步骤如下:

打开 filezilla 软件。

选择 "Edit > Settings > Logging" , 勾选 "Enable logging to file", 如 0 所示。

filezilla 配置



ZFileZilla Server (127.0.	0.1)		
File Server Edit ?			
] 🗲 🔒 🐘 🚨 📽 🕴 /c.	/ C:\ 🎛 🕶		
(000004)2018/9/10 20:08:45 - 6	not logged in) (127.0.0.1)>	· USER test	
(000004)2018/9/10 20:08:45 - 6	not logged in) (127.0.0.1)>	331 Password required for test	
(000004)2018/9/10 20:08:47 -	VileZille Server Ontion	e	X
(000004)2018/9/10 20:08:47 -		-	
(000004)2018/9/10 20:09:15 -	General settings	Logging	FileZilla Server
(000004)2018/9/10 20:09:15 -	- Welcome message	Enable logging to file	
(000004)2018/9/10 20:09:15 -	- IP bindings		
(000005)2018/9/10 20:09:17 -	- IP Filter	Limit log file size to 100 KB	
(000005)2018/9/10 20:09:17 -	Passive mode settings	Loofile tupo	
(000005)2018/9/10 20:09:17 -	- Security settings	Course type.	
(000005)2018/9/10 20:09:17 -	Miscellaneous	• Log all to Filezilla Server.log	
(000005)2018/9/10 20:09:19 -	Admin Interface settings	C Use a different logfile each day (example: fzs-2003-02-10.log)	
(000005)2018/9/10 20:09:19 -	Logging	Delete old logfiles after 14 days	
(000005)2018/9/10 20:09:21 -	Speed Limits	All log files will be saved in the "Logs" subfolder in the EileZilla Server folder.	
(000005)2018/9/10 20:09:21 -	Filetransfer compression		
(000005)2018/9/10 20:10:17 -	Autobas		
Retwiner settings along w	Autobari		
Done vetviewing settings			
Sending settings please wait			
Done sending settings.			
Warning: FTP over TLS is not			
Retrieving settings, please w			
Done retrieving settings			
Sending settings, please wait	1		
Done sending settings.			
Warning: FTP over TLS is not	ОК		
Retrieving settings, please w			
Done retrieving settings	Cancel		
ID 🛆 Account			

## 3.6.3.3 vsftp

本节指导用户开启 vsftp 的登录失败日志开关。

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

重启 vsftp 服务。设置成功后,登录时,会返回如 0 所示的日志记录。

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]	<pre>[ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
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]	<pre>[ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Aug	29	14:55:26	2018	[pid 1]	<pre>[ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
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]	<pre>[ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"</pre>
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]	<pre>[ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"</pre>
Wed	Sep	5	14:00:08	2018	[pid 1]	<pre>[ftp test] FAIL LOGIN: Client "::ffff:10.130.153.31"</pre>

# 3.6.4 如何立即执行手动检测?

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。



#### 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。

### 3.6.4.1 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"。

3.6.4.2 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。

## 3.6.4.3 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。

### 3.6.4.4 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。

登录管理控制台。

在页面左上角选择"区域",单击 三,选择"安全 > 企业主机安全",进入企业主机安全页面。 在"主机管理"页面的右上角,单击"手动检测",执行手动检测,如0所示。

一键执行手动检测

企业主机安全	主机管理 ① 告密透知设置 ⑧ 手动检测	-
<ul> <li>总流</li> <li>1</li> <li>1<td>2 元服売舗 服売編組 助計配額     章語    介配時間    「</td><td></td></li></ul>	2 元服売舗 服売編組 助計配額     章語    介配時間    「	
高级防御	服务器名	
安全运营 ▼ 安装与配置	ecs-hss-002 10.6.211 Linux 進行中 在线 🔮 开館 🔮 視聴 (周気防算装護 default_w 光动防护 ) 切動版本   更多 🗸	
网页防篡改 🔻	ecs-10ec 4195 29fb5a80+ef6-192.168.10.19 Linux 运行中 未安装 ◎ 关闭 ③ 未检测 无 开型助护 切损版本   更多 ▼	
	excs-1991	

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。



手动检测

手动检测					
<ol> <li>手动检测功能支持对Ager</li> <li>手动检测功能对用户选择</li> <li>、 待检测完成后,可在企业:</li> </ol>	nt状态为在线并 的服务器执行以 主机安全服务控	且开启了企业 、下检测项目: 制台查看各风	版或旗舰版防护的服务 软件信息检测、漏洞相 ,险项统计,或者指定到	子器执行检测。 佥测、网站后门检测、口令风 查看单个服务器的安全详情。	险检测、配置检测。
青选择需要执行手动检测的 企业版 旗舰版	服务器				
可选服务器 🔤 全选 (共1个)	服务器	名称 🔻	请输入关键字 Q	已选服务器	
✓ 弹性服务器名称/弹性IP	操作系统	防护状态	当前版本	弹性服务器名称/弹性IP	操作系统
ecs-hss-002	Linux	开启	旗舰版 (网页防篡改赠送)	ecs-hss-002 .6.211	Linux
			确定取消		

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。

## 3.6.4.5 单点执行手动检测

登录管理控制台。

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。

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。

### 查看详情



企业主机安全	主机管理 ①         音音题和设置         手动性
^{总选}   主机管理 1	2 云服分器 服务器组 防护配額
风险预防	,
入侵检测	★ 全語 开朗前护 关闭前护 影響無幅 分配到组 服务器名称 ▼   南柏入关键字 Q 高级建赛 ※ □ C
高级防御	服务器名 IP地址 操作系统 服务器状态 Agent状态 防护状态 检测结果 版本 服务器组 集略组 操作
安全运营 ▼ 安装与配置	・ ecx-hos-002
网页防要改	Comparison     Comparison
	ecs-1991         3.207         Linux         运行中         未安義         ● 未检测         无          开启助中         財動版本         更多、

#### ● 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。

资产管理 漏洞管理 基线检查 入侵检测	
账号信息(22) 开放端口(0/13) 进程信息(24) WEB目录(1) 软件	<u>信息(390)</u> 自启动(3)
列出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。	
手动检测 手动检测状态: 检测完成 2020-09-08 14:08:56 GMT+08:00	
	海输入软件名称 Q C
软件名称	软件版本号
acl	2.2.51-12.el7.x86_64
aic94xx-firmware	30-6.el7.noarch
alsa-firmware	1.0.28-2.el7.noarch

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。

● 系统软件漏洞检测



(加产管理 通過管理 基线检查 入侵检测							
Linux软件描写(117) Web-CMS箴言()							
通过与漏洞库进行比对,检测出系统和软件(例如:SSH	, OpenSSL, Apach	ne、Mysql等)存在的	5漏洞,帮助	用户识别出存在	的风险。		
手动检测 ⑦ 手动检测状态: 检测完成2020-0	09-08 14:08:56 GMT	1+08:00					
忽略 取消忽略 一键修复 验试	E		所有状态	5. 🔻	所有修复紧急	<b>岐度 ▼</b> 漏洞名称 ▼ 清	输入关键字 Q C
漏洞名称	修复紧急度	状态		软件信息		解决方案	操作
CESA-2019:1481 (kernel security u	● 需尽快修复	未处理		python-perf:	3.10.0-693	Update the affected kernel packag 修复建议清参见:CESA-2019:1481	忽略丨修复丨验证
CESA-2017:1680 (bind security up	● 可延后修复	未处理		bind-libs-lite:	9.9.4-50.el	Update the affected bind packages. 修复建议请参见:CESA-2017:1680	忽略 修复 验证

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。

#### Web-CMS 漏洞检测

资产管理 漏洞管理 基线检查	入侵检测						
Linux软件题词 (117) Web-CMS题词 (0)							
還过对Web目录和文件进行检测,识别出Web-CMS	通过对Web目录和文件进行检测,识别出Web-CMS篇词,提升Web服务安全性。						
手动检测 手动检测状态: 检测完成2020-09	9-08 03:08:13 GMT+08:0	D					
忽略 取消忽略		未处	理 *	所有修复紧急度	漏洞名称 🔹	请输入关键字 Q	С
漏洞名称	修复紧急度	伏态	路径	解决方案		操作	

#### ● 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。

### 弱口令风险检测

资产管理 漏洞管理 基线检查 入侵检测						
口令风险(1) 配置风险(35)						
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	全性检测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。				
手动检测 手动检测状态: 检测完成 2020-09-08 00:39:29 (	GMT+08:00					
存在調口令的账号 口令复杂旋策略						
		C				
		C				
账号名	账号类型	弱口令使用时长 (天)				
test	系统账号	10				

● 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。

资产管理 漏洞管理 基线检查 入侵检测							
日令和陰(1) 配置和陰(35)							
对常见的Tomcat配置、SSH登录配置、Nginx配置进行检	对常见的Tomcat配置。SSH登录配置。Nginx配置进行检查,帮助用户识别不安全的配置项。						
手动检测 手动检测状态: 检测完成 2020-09-07	7 22:37:07 GMT+08:00						
			所有配置检测种类 ▼ C				
配置检测种类	风险项	已通过检查项	描述				
V SSH	12	3	本策略通过检查SSH服务中基本的安全配置项,				
✓ Tomcat-1	23	11	Tomcat安全配置规范主要从版本部署、基本配				

配置检测

当"手动检测状态"为"检测完成"时,单击 C,查看最新检测结果。

# 3.6.5 HSS 支持告警日志转存 OBS 吗?

HSS 暂不支持告警日志转存 OBS 桶,日志文件存在服务文件夹中,详细的存储路径及日志保留期, 请查看 3.6.2 如何查看 HSS 的日志文件?