企业主机安全

用户指南（巴黎区域）

文档版本 01

发布日期 2023-11-30

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品介绍

1.1 什么是企业主机安全

企业主机安全（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

HSS不受地理位置影响，为主机、容器等提供统一的可视化和控制能力。

HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

主机安全

主机安全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。

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。

主机安全的组件功能及工作流程说明如下：

表 1-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。

组件	说明
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：10180。 ● 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。 ● 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、容器安全与主机安全共用同一个Agent，您只需在同一主机安装一次。

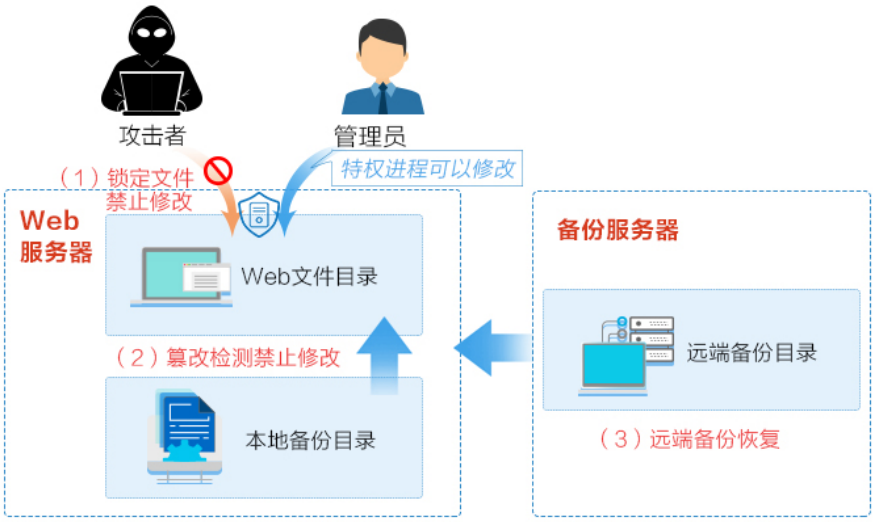
容器安全

容器安全是HSS为容器提供的一种防护能力，通过部署在容器宿主机中的Agent，能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时容器安全提供容器进程白名单、文件只读保护和容器逃逸检测功能，可以有效防止容器运行时安全风险事件的发生。

网页防篡改

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，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。

图 1-1 网页防篡改原理



1.2 产品优势

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

集中管理

实现检测和防护的一体化管控，降低管理的难度和复杂度。

- 将Agent安装在ECS服务器中，您可以集中管理同一区域内多样化部署的主机。
- 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。

全面防护

提供事前预防、事中防御、事后检测的全面防护，全面降低入侵风险。

轻量 Agent

Agent占用资源极少，不影响主机系统的正常运行。

网页防篡改

- 使用第三代网页防篡改技术，内核级事件触发技术，锁定用户目录下的文件后，有效阻止非法篡改行为。
- 篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当企业主机安全检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。

1.3 应用场景

主机安全

- 统一安全管理

  企业主机安全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。

- 主动安全防御

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

- 黑客入侵检测

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

容器安全

- 容器镜像安全

  即使在Docker Hub下载的官方镜像中也常常包含了漏洞，而研发人员在使用大量开源框架时更加剧了镜像漏洞问题的出现。

  容器镜像安全对镜像进行安全扫描，将镜像中存在的各种风险（镜像漏洞、账号、恶意文件等）进行展示，提示用户及时修改，消除安全隐患。

- 容器运行时安全

  通常容器的行为是固定不变的，容器安全服务帮助企业制定容器行为的白名单，确保容器以最小权限运行，有效阻止容器安全风险事件的发生。

1.4 版本功能特性

企业主机安全有企业版、旗舰版、网页防篡改版和容器安全供您选择，包含了资产管理、漏洞管理、基线检查、入侵检测、勒索防护、网页防篡改、容器镜像安全等功能，具体功能详情及版本差异详情请参见**版本功能差异说明**。

功能特性说明

企业主机安全包含了资产管理、基线检查、勒索防护、入侵检测等功能特性，每一个功能都从不同维度提升主机的安全性，全方位保证主机的安全可靠，不同版本支持的功能详情请参见**版本功能差异说明**。

表 1-2 企业主机安全功能特性说明

功能名称	功能描述
资产管理	提供资产概览、资产指纹管理、主机管理、容器管理功能，支持查看资产运行状态、资产指纹和资产分类情况，同时可按照主机、容器的维度查看或管理目标服务器，实现主机全量资产的统一可视管理。
漏洞管理	提供检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞、应用漏洞，帮助用户识别潜在风险。
基线检查	扫描主机系统和关键软件含有风险的配置、弱口令、口令复杂度策略。 支持的检测基线包含安全实践和等保合规基线，且可自定义选择检测的子基线项。 支持对检测风险的修复和验证。
容器镜像安全	扫描镜像仓库与正在运行的容器镜像，发现镜像中的漏洞、恶意文件等并给出修复建议，帮助用户得到一个安全的镜像。
应用防护	为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。 当前只支持操作系统为Linux的服务器，且仅支持Java应用接入。
网页防篡改	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。
勒索病毒防护	支持已知勒索病毒检测能力，支持自定义勒索备份恢复策略。
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。
容器防火墙	对容器集群内部和外部的网络流量进行控制和拦截，防止恶意访问和攻击。
主机入侵检测	识别并阻止入侵主机的行为，实时检测主机的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。
容器入侵检测	实时监控容器节点运行状态，发现挖矿、勒索等恶意程序，发现违反容器安全策略的进程运行和文件修改，以及容器逃逸等行为并给出解决方案。
白名单管理	可以通过加入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。将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。
策略管理	提供灵活的策略管理能力，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/容器应用不同的策略，以满足不同应用场景的主机/容器安全需求。
历史处置记录	提供漏洞的历史处置记录，方便您查看处理时间和处理人等信息。
安全报告	提供每周或每月的主机安全趋势以及关键安全事件与风险。

功能名称	功能描述
安全配置	提供配置常用登录地、常用登录IP、SSH登录IP白名单、恶意程序自动隔离查杀功能，满足不同应用场景的主机/容器安全需求。

版本推荐说明

- 若您使用的主机涉及重要资产或者高风险情况，建议开启**旗舰版或者网页防篡改版**，例如：对外暴露EIP、保存有关键资产、存在数据库等。
- 有网站或者关键系统防篡改需求，以及有应用安全防护需求的主机，主要部署在网站或者应用的主机上，**推荐使用网页防篡改版**。
- 有镜像安全、容器运行时安全需求，以及需要满足容器化部署业务的用户，**推荐使用容器安全**。

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，**建议您的云上主机全部署企业主机安全**。

版本功能差异说明

表 1-3 版本功能差异说明

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
资产概览		所有主机的资产状态、清点情况统计。	√	√	√	√	Linux、Windows	实时检测
主机管理		所有主机资产管理，包含主机的防护状态、配额绑定、策略分配等。	√	√	√	√	Linux、Windows **注**：批量安装Agent仅支持Linux	-
容器管理		容器节点管理，容器镜像管理。	×	×	×	√	Linux	-

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
资产指纹	账号	检测当前系统的账号信息，帮助用户进行账户安全性管理。	×	√	√	√	√	Linux、Windows 实时检测
	开放端口	检测当前系统开放的端口，帮助用户识别出其中的危险端口和未知端口。	×	√	√	√	√	Linux、Windows 实时检测
	进程	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。	×	√	√	√	√	Linux、Windows 实时检测
	软件	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。	×	√	√	√	√	Linux、Windows 每日凌晨自动检测
	自启动项	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。	×	√	√	√	√	Linux、Windows 实时检测
	Web应用	Web应用主要统计、展示推送发布web内容的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
	Web服务	统计、展示对外提供web内容访问的软件详细信息，您可查看所有软件的版本、路径、配置文件、关联进程等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
	Web框架	统计、展示Web内容对外呈现时所使用框架的详细信息，您可查看所有框架的版本、路径、关联进程等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	Web站点	统计、展示存放Web内容的目录及对外提供访问的站点信息，您可以查看所有目录及权限、以及和站点所关联访问路径、对外端口、关键进程等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
	中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
	数据库	统计、展示提供数据存储的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息；	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
	内核模块	统计、展示运行在内核层的全量程序模块文件，您可查看所有模块所关联的服务器、版本号、模块描述、驱动文件路径、文件权限、文件哈希等信息。	×	√	√	√	√	Linux 1次/周（每周一凌晨05:00）
漏洞管理	Linux漏洞检测	通过与漏洞库进行比对，检测Linux操作系统官方维护的软件（非绿色版、非自行编译安装版；例如：kernel、openssl、vim、glibc等）存在的漏洞。	√	√	√	√	Linux	• 每日凌晨自动检测 • 手动检测
	Windows漏洞检测	通过同步微软官方的补丁公告，检测Windows操作系统存在的漏洞。	√	√	√	√	Windows	• 每日凌晨自动检测 • 手动检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	Web-CMS漏洞检测	通过对Web目录和文件进行检测，识别Web-CMS漏洞，提升Web服务安全性。	√	√	√	√	Linux、Windows	• 每日凌晨自动检测 • 手动检测
	应用漏洞检测	检测开源的jar包、elf文件等的漏洞，比如log4j、spring-core的漏洞。	√	√	√	√	Linux	• 1次/周（每周一凌晨05:00） • 手动检测
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。	√	√	√	√	Linux	• 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。	√	√	√	√	Linux	• 每日凌晨自动检测 • 手动检测
	配置检查	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	• 每日凌晨自动检测 • 手动检测
容器镜像安全	容器镜像漏洞	通过与漏洞库进行比对，检测并管理本地镜像和私有镜像仓库存在的漏洞，对当前镜像中存在的紧急漏洞进行提醒。	×	×	×	√	Linux	• 每日凌晨自动检测 • 手动检测
	镜像基线检查	提供18类容器基线配置检查，帮助用户识别不安全的配置。	×	×	×	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
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。	×	×	√	×	Linux、Windows	实时检测
	动态网页防篡改	防止网站数据库中动态网页内容被篡改。	×	×	√	×	Linux	实时检测
勒索病毒防护	勒索病毒防护	帮助用户识别检测已知勒索病毒攻击，通过勒索备份恢复业务。	×	√	√	√	Linux、Windows	实时检测
文件完整性管理	文件完整性检测	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。	×	√	√	√	Linux	实时检测
容器防火墙	容器防火墙	对容器集群内部和外部的网络流量进行控制和拦截，防止恶意访问和攻击。	×	×	×	√	Linux	实时检测
主机入侵检测	未分类恶意软件	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。	√	√	√	√	Linux、Windows	实时检测
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。	√	√	√	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。	×	√	√	√	Linux、Windows	实时检测
	Webshell	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。 ● 您可以使用手动检测功能检测主机中的网站后门。	√	√	√	√	Linux、Windows	实时检测
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	√	√	√	√	Linux	实时检测
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	√	√	√	√	Linux	实时检测
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	√	√	√	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。	√	√	√	√	Linux	实时检测
	文件提权	检测当前系统对文件的提权。	√	√	√	√	Linux	实时检测
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。	√	√	√	√	Linux	实时检测
	关键文件变更	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。	√	√	√	√	Linux、Windows	实时检测
	文件/目录变更	对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。	√	√	√	√	Linux、Windows	实时检测
	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。	√	√	√	√	Linux、Windows	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	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。	√	√	√	√	Linux、Windows	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、复制、硬链接、访问权限变化。	√	√	√	√	Linux	实时检测
	Crontab可疑任务	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。 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。	√	√	√	√	Linux、Windows	实时检测
	系统安全防护被禁用	检测勒索软件加密前准备动作：通过注册表关闭 Windows Defender 实时保护功能，一旦发现立即上报告警。	√	√	√	√	Windows	实时检测
	备份删除	检测勒索软件加密前准备动作：删除备份格式文件或Backup文件夹下的文件，一旦发现立即上报告警。	√	√	√	√	Windows	实时检测
	异常注册表操作	检测通过注册表关闭系统防火墙、勒索病毒Stop修改注册表并写入特定字符串等操作，一旦发现立即上报告警。	√	√	√	√	Windows	实时检测
	系统日志删除	检测到通过命令或工具清除系统日志的操作时进行告警。	√	√	√	×	Windows	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	可疑命令执行	• 检测通过命令或工具创建、删除计划任务或自启动任务。 • 检测远程执行命令的可疑行为。	√	√	√	√	Linux、Windows	实时检测
	暴力破解	检测“尝试暴力破解”和“暴力破解成功”等暴力破解。 • 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。 • 若账户暴力破解成功，登录到云主机，则触发安全事件告警。	√	√	√	√	Linux、Windows	实时检测
	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）。 若在非常用登录地登录，则触发安全事件告警。	√	√	√	√	Linux、Windows	实时检测
	非法系统账号	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。	√	√	√	√	Linux、Windows	实时检测
	用户账号添加	检测使用命令创建隐藏账户，一旦创建成功后用户交互界面和命令查询均不可见。	√	√	√	√	Windows	实时检测
	用户密码窃取	检测主机中的系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。	√	√	√	√	Windows	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	可疑的下载请求	检测到利用系统工具下载程序的可疑HTTP请求时进行告警。	√	√	√	×	Windows	实时检测
	可疑的HTTP请求	检测到利用系统工具或进程执行远程托管脚本的可疑HTTP请求时进行告警。	√	√	√	×	Windows	实时检测
	端口扫描	检测用户指定的端口存在被扫描或者嗅探的行为，一旦发现进行告警上报。	×	√	√	√	Linux	实时检测
容器入侵检测	未分类恶意软件	对容器中运行的程序进行检测，识别出其中的后门、木马、挖矿软件、蠕虫和病毒等恶意程序。	×	×	×	√	Linux	实时检测
	勒索软件	检测容器场景下勒索软件，并进行告警上报。	×	×	×	√	Linux	实时检测
	Webshell	检测容器中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。	×	×	×	√	Linux	实时检测
	漏洞逃逸攻击	监控到容器内进程行为符合已知漏洞的行为特征时，触发逃逸漏洞攻击告警。	×	×	×	√	Linux	实时检测
	文件逃逸攻击	监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，仍然会触发告警。	×	×	×	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。支持对TCP、UDP、ICMP等协议的检测。	×	×	×	√	Linux	实时检测
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。	×	×	×	√	Linux	实时检测
	容器进程异常	● 容器恶意程序 监控容器内启动的容器进程的行为特征和进程文件指纹，如果特征与已定义的恶意程序吻合则触发容器恶意程序告警。 ● 容器异常进程 对于已关联的容器镜像启动的容器，只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。	×	×	×	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	容器异常启动	监控新启动的容器，对容器启动配置选项进行检测，当发现容器权限过高存在风险时触发告警。 支持以下容器环境检测： ● 禁止启动特权容器(privileged:true) ● 需要限制容器能力集（capabilities:[xxx]） ● 建议启用seccomp（seccomp=unconfined） ● 限制容器获取新的权限(no-new-privileges:false) ● 危险目录映射(mounts:[...])	×	×	×	√	Linux	实时检测
	高危命令执行	实时检测容器场景系统中执行的高危命令，当发生高危命令执行时触发告警。	×	×	×	√	Linux	实时检测
	高危系统调用	Linux系统调用是用户进程进入内核执行任务的请求通道，容器安全监控容器进程，如果发现进程使用了危险系统调用，触发高危系统调用告警。	×	×	×	√	Linux	实时检测
	敏感文件访问	监控容器内已配置文件保护策略的容器镜像文件状态。如果发生文件修改事件则触发文件异常告警。	×	×	×	√	Linux	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	容器镜像阻断	在Docker环境中容器启动前，告警并阻断镜像异常行为策略中指定的不安全容器镜像运行。	×	×	×	√	Linux	实时检测
	暴力破解	检测容器场景下“尝试暴力破解”和“暴力破解成功”等暴破异常行为，发现暴破行为时触发告警。 支持检测容器场景下SSH、Web和Enumdb暴破行为。 **说明** 目前暂仅支持Docker容器运行时的暴力破解检测告警。	×	×	×	√	Linux	实时检测
	非法系统用户账户	检测容器场景系统中的账号，列出当前系统中的可疑账号信息并告警上报，帮助用户及时发现非法账号。	×	×	×	√	Linux	实时检测
白名单管理	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。	√	√	√	√	Linux、Windows	实时检测
	登录白名单	对部分告警可加入告警白名单。	√	√	√	√	Linux、Windows	实时检测
	系统用户白名单	对于主机中新添加的root用户组权限用户（非root用户）可添加到系统用户白名单，避免HSS进行风险账号告警。	√	√	√	√	Linux、Windows	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
策略管理	查看和修改策略	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	√（仅支持默认企业版策略组）	√	√	√	Linux、Windows	实时检测
历史处置记录	历史处置记录	提供漏洞、安全告警事件的历史处置记录，方便您查看相关处理时间和处理人等信息。	√	√	√	√	Linux、Windows	-
安全报告	主机安全报告	呈现每周或每月的主机安全趋势以及关键安全事件与风险。	√	√	√	√	Linux、Windows	-
安全配置	Agent管理	可查看所有服务器的Agent状态，可进行升级、卸载、安装等操作。	√	√	√	√	Linux、Windows	实时检测
	常用登录地	配置常用登录地后，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。	√	√	√	√	Linux、Windows	实时检测
	常用登录IP	配置常用登录IP，服务将对非常用IP登录主机的行为进行告警。	√	√	√	√	Linux、Windows	实时检测

服务功能	功能项	功能概述	企业版	旗舰版	网页防篡改版	容器安全	支持的操作系统	检测周期
	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。	√	√	√	√	Linux	实时检测
	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。	√	√	√	√	Linux、Windows	实时检测
	插件管理	对插件进行安装、卸载、升级及统一管理。	×	×	×	√	Linux	-

1.5 HSS 权限管理

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

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

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

HSS 权限

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

HSS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生

效，如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问HSS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

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

如表1-4所示，包括了HSS的所有系统权限。

表 1-4 HSS 系统权限

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

1.6 约束与限制

HSS 支持的操作系统

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。

- Agent支持的主机操作系统。

操作系统类型	系统架构	支持的操作系统版本
Linux	X86	• CentOS 7.4、7.5、7.6、7.7、7.8、7.9、8.0、8.1、8.2、9（64位） • Debian 9、10、11.0.0、11.1.0（64位） • EulerOS 2.2、2.3、2.5、2.7、2.9（64位） • Fedora 28（64位） • OpenSUSE: 15.3 (64-bit) • Ubuntu 16、18、20.03、20.04、22.04（64位） • RedHat 7.4、7.6、8.0、8.7（64位） • OpenEuler 20.03 LTS、22.03 SP3 LTS、22.03（64位） • AlmaLinux 9.0（64位） • RockyLinux 8.4、8.5、9.0（64位）
	ARM	• CentOS 7.4、7.5、7.6、7.7、7.8、7.9、8.0、8.1、8.2、9（64位） • EulerOS 2.8、2.9（64位） • Fedora 29（64位） • OpenSUSE: 15 64bit with ARM(40GB) • Ubuntu 18（64位） • kylin V7、V10（64位） • NeoKylin: V10 (aarch64-bit)
Windows	X86	• Windows Server 2016 • Windows Server 2012 • Windows Server 2008 **说明** 若服务器安装了第三方安全防护软件，请先停止第三方安全防护软件的防护功能，待Agent安装完成后再开启。

1.7 计费说明

本小节主要介绍企业主机安全的计费说明，包括计费项、计费模式等。

计费项

HSS根据您的HSS服务版本和申请时长计费。

表 1-5 计费项信息

计费项目	计费说明
服务版本（必选）	按申请的服务版本（企业版、旗舰版、网页防篡改版或者容器安全版）计费。

计费模式

HSS提供按需计费模式。

表 1-6 HSS 各服务版本计费模式

服务版本	支持的计费模式	说明
企业版	按需计费	按需计费模式，即按实际使用的时长收费，以小时为单位，每小时整点结算，不设最低消费标准。
旗舰版		
网页防篡改版		
容器安全版		

1.8 HSS 与其他云服务的关系

弹性云服务器

企业主机安全的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》。

云容器引擎

云容器引擎（Cloud Container Engine，CCE）基于云服务器快速构建高可靠的容器集群，将节点纳管到集群，企业主机安全通过在集群所在节点上部署Hostguard-agent，为集群中所可用有节点上的容器应用提供防护。

说明

云容器引擎提供高可靠、高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。更多信息请参见《云容器引擎用户指南》。

容器镜像服务

容器镜像服务（Software Repository for Container，SWR）是一种支持容器镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务，更多信息请参见《容器镜像服务用户指南》。企业主机安全通过扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题。

1.9 基本概念

账户破解

账户破解指入侵者对系统密码进行猜解或暴力破解的行为。

弱口令

弱口令指密码强度低，容易被攻击者破解的口令。

恶意程序

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

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

恶意程序包括已被识别的恶意程序和可疑的恶意程序。

勒索病毒

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

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

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

网页防篡改

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

集群

集群是同一个子网中一个或多个弹性云服务器（又称：节点）通过相关技术组合而成的计算机群体，为容器运行提供计算资源池。

节点

在容器中，每一个节点对应一台弹性云服务器（Elastic Cloud Server，ECS），容器运行在节点上。

镜像

镜像（Image）是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数。镜像不包含任何动态数据，其内容在构建之后也不会被改变。

容器

容器（Container）是镜像的实例，容器可以被创建、启动、停止、删除、暂停等。

安全策略

安全策略是指容器运行时需要遵循的安全规则，如果容器违反了安全策略，容器安全服务控制台的“运行时安全”页面会显示容器异常。

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。

一个账户中可以创建多个项目。

防护配额

目标主机开启检测防护需要绑定的对象，即防护配额。

在企业主机安全申请的不同版本的数量在控制台中是以防护配额的描述呈现。

示例：

- 申请了1个企业版，即企业版可用防护配额数量为1个，只能绑定任意1台主机；
- 申请了10个旗舰版，即旗舰版可用防护配额数量为10个，可分配至10台不同主机进行分别绑定；

2 开通 HSS

2.1 安装 Agent

2.1.1 安装 Linux 版本 Agent

安装Agent后，您才能正常开启云服务器的负载保护。

本节指导您如何在Linux操作系统的主机中安装Agent。

说明

CentOS 6.x版本由于Linux官网已停止更新维护，企业主机安全也不再支持CentOS 6.x及以下的系统版本，谢谢您的理解！

默认安装路径

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

“/usr/local/hostguard/”

前提条件

- 安装其他云主机时，待安装Agent的主机操作系统为Linux，且网络环境能正常访问公网。
- 请关闭Selinux防火墙，防止Agent安装失败，安装成功后再打开。

安装须知

- Agent支持的操作系统请参见**支持的操作系统**。
- 您的云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 如果您的服务器已安装第三方安全软件，可能会导致企业主机安全Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。
- 安装Agent的磁盘剩余可用容量须大于300M，否则可能导致Agent安装失败。

- 安装成功后，需要等待5~10分钟左右才会刷新Agent状态。请前往“资产管理>主机管理>云服务器”界面查看。

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。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

步骤4 选择“Agent管理 > Agent不在线(X)”页签，在目标服务器的“操作”列，单击“安装Agent”。

步骤5 在弹窗中，根据该服务器的系统架构和操作系统，单击“复制”安装Agent的命令。

步骤6 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、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。

步骤7 粘贴复制的安装命令，以root权限执行，在主机中安装Agent。

若界面回显信息与如下信息类似，则表示Agent安装成功。

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

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

若界面回显如下信息，则表示Agent服务运行正常。

```
Hostguard is running
```

----结束

2.1.2 安装 Windows 版本 Agent

在主机中安装Agent后，您才能开启企业主机安全。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**安装Linux版本Agent**。

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\HostGuard”

提示说明

Windows主机中若将Agent卸载后重装，重装过程中界面提示“Installation failed”，实际Agent已成功安装，不影响正常使用。

前提条件

- 待安装Agent的主机操作系统为Windows。
- 已在本地安装远程管理工具（如：“pcAnywhere”、“UltraVNC”）。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面，选择“Agent管理 > Agent不在线(X)”。

步骤4 在需要安装Agent的“操作”列，单击“安装Agent”，获取下载Agent安装脚本的链接。

步骤5 远程登录待安装Agent的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。
- 若您的主机已经绑定了弹性IP，您也可以使用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。

步骤6 在待安装Agent的主机中，通过IE浏览器访问**步骤4**中获取的链接，下载Agent安装脚本。

步骤7 下载完成后，请使用管理员权限运行Agent安装脚本。

步骤8 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”。

若进程不存在，则表示Agent安装失败，请尝试重新安装Agent。

----结束

2.2 开启防护

2.2.1 开启企业版/旗舰版防护

开启主机安全防护时，您需为指定的主机分配一个配额，关闭主机安全防护或删除主机后，该配额可分配给其他的主机使用。

若您申请的是网页防篡改版，请在“主动防御 > 网页防篡改 > 防护配置”页面开启防护。

说明

申请“网页防篡改版”后，您也可以使用“旗舰版”中的所有功能，但是您需要通过“主动防御 > 网页防篡改 > 防护配置”页面开启防护，当开启网页防篡改防护时会自动开启旗舰版防护。

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 > 资产管理 > 主机管理”页面“云服务器”中“Agent状态”为“在线”。
- 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期间请勿关闭Windows防火墙。若关闭Windows防火墙，HSS无法拦截账户暴力破解的攻击源IP。
  - 通过手动开启Windows防火墙，也可能导致HSS不能拦截账户暴力破解的攻击源IP。

开启防护

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“资产管理 > 主机管理 > 云服务器”，进入“云服务器”界面。

步骤4 选择所需开启安全防护的主机，单击“操作”列“开启防护”。

在“开启防护”对话框中，选择“主机安全版本”。

步骤5 单击“确认”，开启防护。开启主机安全防护后，请在控制台上查看企业主机安全的开启状态。

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

说明

- 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将根据您开启的服务版本，自动对您的主机执行服务版本对应的安全检测。

----结束

查看检测详情

开启防护后，企业主机安全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。

在防护列表的左侧，单击“有风险”，您可以选择查看有风险的服务器，查看服务器的详细检测结果。

单击服务器名称，进入详情界面，能快速查看主机中已被检测出的各项信息和风险。

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。

表 2-1 手动配置检测项

功能	检测项	相关链接
安装与配置	• 常用登录地/IP • SSH登录IP白名单 • 开启恶意程序隔离查杀	常用安全配置
入侵检测	• 配置告警白名单 • 配置登录白名单	入侵检测
主动防御	• 应用防护 • 勒索病毒防护 • 文件完整性管理	主动防御
安全运营	• 策略管理	安全运营
安全报告	• 订阅安全报告	

相关操作

关闭主机防护

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

须知

- 关闭主机防护前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免未处理已知风险就关闭防护，从而造成被攻击的情况。
- 关闭主机防护后，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。

2.2.2 开启网页防篡改版防护

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

表 2-2 网页防篡改原理

防护类型	原理说明
静态网页防护	1. 锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站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 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。
动态网页防护	提供Tomcat应用运行时自我保护，防护原理如下： 1. 基于RASP过滤恶意行为 采用自研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。

前提条件

- 在“主动防御 > 网页防篡改 > 防护配置”页面中“防护状态”为“未防护”。
- 在“资产管理 > 主机管理”页面“云服务器”列表中“Agent状态”为“在线”、“防护状态”为“未防护”。

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

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面，单击“添加防护服务器”。

步骤4 在“添加防护服务器”页面，选择“可添加服务器”页签，勾选需要开启防护的服务器，选择目标配额，可默认随机选择，单击“添加并开启防护”。

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

“网页防篡改版”开启后，旗舰版防护会同步开启。

- 选择“主动防御 > 网页防篡改”，目标服务器所在行的“防护状态”为“防护中”，则表示网页防篡改版已开启。
- 选择“资产管理 > 主机管理 > 云服务器”，目标服务器所在行的“防护状态”为“防护中”，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。

----结束

须知

- 您也可以通过在“资产管理 > 主机管理 > 防护配额”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“主动防御 > 网页防篡改 > 防护配置”列表的“操作”列中，单击“关闭防护”，关闭对指定主机的网页防篡改防护。

须知

- 关闭网页防篡改防护服务前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。
- 关闭网页防篡改防护服务后，网页应用被篡改的可能性将大大提高，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。
- 执行关闭网页防篡改操作后，防护目录下的文件将不再受“网页防篡改”功能的防护，建议您提前处理防护目录下的文档，再对文档执行暂停防护、编辑或删除的相关操作。
- 执行关闭网页防篡改操作后，若您的文档不慎被删除，请在主机本地备份或远端主机的备份路径中查找。
- 当用户关闭网页防篡改时会同步关闭旗舰版防护。

2.2.3 开启容器版防护

开启容器节点防护时，您需为指定的节点（主机）分配一个配额，关闭容器安全防护或删除节点（主机）后，该配额可分配给其他的节点（主机）使用。

检测周期

企业主机安全每日凌晨进行全量检测。

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看到检测结果。

前提条件

- “企业主机安全 > 资产管理 > 容器管理”页面“容器节点管理”中“Agent状态”为“在线”。
- 已在云容器引擎成功创建节点。
- 节点的“防护状态”为“未防护”。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 在“节点列表”中单击目标服务器“操作”列的“开启防护”，为需要开启防护的节点开启防护。

步骤5 在弹出的提示框中，确认服务器信息。

步骤6 单击“确定”，开启节点防护，目标服务器“容器防护状态”变更为“防护中”，说明该节点已开启防护。

说明

一个容器安全配额防护一个集群节点。

----结束

相关操作

关闭节点防护

您可以在“资产管理 > 容器管理 > 容器节点管理 > 节点列表”的“操作”列，单击“关闭防护”，关闭对指定容器集群节点的安全防护。

关闭节点防护后，HSS会自动释放防护配额。您可将空闲的配额分配给其他节点继续使用，避免造成配额资源的浪费。

须知

- 关闭节点防护前，请对容器执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的容器遭受攻击。
- 关闭节点防护后，请及时清理容器中的重要数据、关停容器中的重要业务并断开容器与外部网络的连接，避免因容器遭受攻击而承担不必要的损失。

2.3 开启告警通知

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

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

开启告警通知

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置”，选择“告警配置”页签，进入“告警配置”页面，配置参数说明请参见**表2-3**。

表 2-3 告警配置参数

通知项	说明	选择建议
每日告警通知	每日凌晨，企业主机安全将主动检测主机系统中的账号、Web目录、漏洞、恶意程序及关键配置等，汇总各项检测结果后，将检测结果发送给您在“消息通知服务主题”中添加的订阅终端。 单击“查看每日告警默认通知事件”可查看通知项。	• 接收并定期查看每日告警通知中所有的内容，能有效降低主机中未及时处理的风险成为主机安全隐患的概率。 • 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，企业主机安全将按照选定的“消息通知服务主题”为您告警。 单击“查看实时告警默认通知事件”可查看通知项。	• 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”。
告警等级	自定义勾选通知的告警等级。	选择全部。
屏蔽事件	选择无需发送告警通知的事件。 展开选框可自定义选择不发送告警的事件类型。	根据**告警通知项说明**的内容说明判断需要屏蔽的事件。

步骤4 设置事件告警的通知方式。

- **消息主题**

  单击下拉列表选择已创建的主题，或者单击“查看消息通知服务主题”创建新的主题。

  您可以根据运维计划和告警通知类型，创建多个“消息通知主题”，以接收不同类型的告警通知。更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤5 单击“应用”，完成配置主机安全告警通知的操作。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。

----结束

告警通知项说明

- **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10：00发送给您添加的手机号或者邮箱。

表 2-4 每日告警通知

通知项	通知内容	通知内容说明
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。
	未安装Agent	检测当前账号未安装企业主机安全Agent的服务器数量，通知用户及时对这些服务器安装Agent进行防护。
漏洞管理	需紧急修复漏洞	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。
基线检查	配置检查	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。
	经典弱口令	检测MySQL、FTP及系统账号的弱口令。
入侵检测	未分类恶意软件	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。
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。
	Webshell	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。 ● 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。
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。

通知项	通知内容	通知内容说明
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	文件提权	检测当前系统对文件的提权。
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。
	关键文件变更	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。
	文件/目录变更	对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。
	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。
	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。
	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、复制、硬链接、访问权限变化。
	Crontab可疑任务	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。 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。
	容器镜像阻断	在Docker环境中容器启动前，对镜像异常行为策略中指定的不安全容器镜像进行告警并阻断。
	暴力破解	检测“尝试暴力破解”和“暴力破解成功”等暴力破解。 ● 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。 ● 若账户暴力破解成功，登录到云主机，则触发安全事件告警。
	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）。 若在非常用登录地登录，则触发安全事件告警。

通知项	通知内容	通知内容说明
	非法系统账号	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。
	漏洞逃逸攻击	监控到容器内进程行为符合已知漏洞的行为特征时（例如：“脏牛”、“bruteforce”、“runc”、“shocker”等），触发逃逸漏洞攻击告警。
	文件逃逸攻击	监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，仍然会触发告警。
	容器进程异常	容器业务通常比较单一。如果用户能够确定容器内只会运行某些特定进程，可以在控制台配置安全策略设置进程白名单并将策略关联容器镜像。 对于已关联的容器镜像启动的容器，只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。
	容器异常启动	对容器启动时使用不合规的参数进行检测告警。 容器启动时可以带有很多参数，对容器进行权限设置。如果没有正确设置，可能会导致权限过大，给攻击者留下可以利用的方式。
	高危系统调用	Linux系统调用是用户进程进入内核执行任务的请求通道。监控容器进程，如果发现进程使用了危险系统调用（例如：“open_by_handle_at”、“ptrace”、“setns”、“reboot”等），触发高危系统调用告警。
	敏感文件访问	检测重要文件的提权或持久化等访问行为，对访问行为进行告警。
	Windows网页防篡改	防止网站Windows服务器中的静态网页文件被篡改。
	Linux网页防篡改	防止网站Linux服务器中的静态网页文件被篡改。
	动态网页防篡改	防止网站Windows和Linux服务器中的动态网页文件被篡改。
	应用防护	为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。 当前只支持操作系统为Linux的服务器，且仅支持Java应用接入。
	病毒查杀	针对检测到的病毒文件进行告警。

- **实时告警通知**
  事件发生时，及时发送告警通知。

  表 2-5 实时告警通知

通知项	通知内容	通知内容说明
入侵检测	未分类恶意软件	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。
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。
	Webshell	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。 ● 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。
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	文件提权	检测当前系统对文件的提权。
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。
	关键文件变更	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。
	文件/目录变更	对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。

通知项	通知内容	通知内容说明
	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。
	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。
	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、复制、硬链接、访问权限变化。
	Crontab可疑任务	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。 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。
	容器镜像阻断	在Docker环境中容器启动前，对镜像异常行为策略中指定的不安全容器镜像进行告警并阻断。
	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）。 若在非常用登录地登录，则触发安全事件告警。
	非法系统账号	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。
	漏洞逃逸攻击	监控到容器内进程行为符合已知漏洞的行为特征时（例如：“脏牛”、“bruteforce”、“runc”、“shocker”等），触发逃逸漏洞攻击告警。
	文件逃逸攻击	监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，仍然会触发告警。
	容器进程异常	容器业务通常比较单一。如果用户能够确定容器内只会运行某些特定进程，可以在控制台配置安全策略设置进程白名单并将策略关联容器镜像。 对于已关联的容器镜像启动的容器，只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。

通知项	通知内容	通知内容说明
	容器异常启动	对容器启动时使用不合规的参数进行检测告警。 容器启动时可以带有很多参数，对容器进行权限设置。如果没有正确设置，可能会导致权限过大，给攻击者留下可以利用的方式。
	高危系统调用	Linux系统调用是用户进程进入内核执行任务的请求通道。监控容器进程，如果发现进程使用了危险系统调用（例如：“open_by_handle_at”、“ptrace”、“setns”、“reboot”等），触发高危系统调用告警。
	敏感文件访问	检测重要文件的提权或持久化等访问行为，对访问行为进行告警。
	Windows网页防篡改	防止网站Windows服务器中的静态网页文件被篡改。
	Linux网页防篡改	防止网站Linux服务器中的静态网页文件被篡改。
	动态网页防篡改	防止网站Windows和Linux服务器中的动态网页文件被篡改。
	应用防护	为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。 当前只支持操作系统为Linux的服务器，且仅支持Java应用接入。
	暴力破解	检测“尝试暴力破解”和“暴力破解成功”等暴力破解。 ● 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。 ● 若账户暴力破解成功，登录到云主机，则触发安全事件告警。
	自动化阻断	对恶意程序自动隔离查杀、勒索病毒自动阻断、网页防篡改自动阻断成功的事件进行通知。
账户登录	登录成功	对登录成功的账户进行通知。

2.4 常用安全配置

开启防护后，您可配置常用登录地、常用登录IP、SSH登录IP白名单，以及开启恶意程序自动隔离查杀，进一步提升云服务器的安全。

步骤1 登录管理控制台。

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

----结束

配置常用登录地

配置常用登录地后，企业主机安全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。

步骤1 选择“安装与配置 > 安全配置 > 常用登录地”，单击“添加常用地登录”。

步骤2 在弹出的对话框中依次选择地理位置、国家名称、城市名称，选择后勾选需要生效登录地信息的云服务器，可勾选多个服务器，确认无误单击“确认”，添加操作完成。

步骤3 返回“安装与配置 > 安全配置 > 常用登录地”页面查看是否已新增，出现新增表示添加成功。

----结束

配置常用登录 IP

配置常用登录IP，企业主机安全将对非常用IP登录主机的行为进行告警。

步骤1 选择“安装与配置 > 安全配置 > 常用登录IP”，单击“添加常用登录IP”。

步骤2 在弹出的对话框中输入“常用登录IP”，勾选需要生效的云服务器，可勾选多个服务器，确认无误单击“确认”，添加操作完成。

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。
- 单次只能添加一个IP，若需添加多个IP，需重复操作添加动作，直至全部IP添加完成，且最多可添加20个登录IP。

步骤3 返回“安装与配置 > 安全配置 > 常用登录IP”页面查看是否已新增，出现新增表示添加成功。

----结束

配置 SSH 登录 IP 白名单

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

说明

- 单一账号最多可添加10个SSH登录IP白名单。
- 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。

步骤1 选择“安装与配置 > 安全配置 > SSH登录IP白名单”，单击“添加白名单IP”。

步骤2 在弹出的对话框中输入“白名单IP”，勾选需要生效的云服务器，可勾选多个服务器，确认无误单击“确认”，添加操作完成。

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。
- 单次只能添加一个IP，若需添加多个IP，需重复操作添加动作，直至全部IP添加完成。

步骤3 返回“安装与配置 > 安全配置 > 常用登录IP”页面查看是否已新增，出现新增表示添加成功。

----结束

开启恶意程序隔离查杀

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

步骤1 选择“安装与配置 > 安全配置 > 恶意程序隔离查杀”，单击“恶意程序隔离查杀”的开关，开启“恶意程序隔离查杀”。

说明

开启后将应用至企业主机安全全局服务器，但部分检测能力受主机安全配额版本的限制无法运行，若需正常使用，建议您开启企业版及以上版本更好的体验隔离查杀功能。

步骤2 在弹出的对话框中单击“确认”，开启“恶意程序隔离查杀”。

自动隔离查杀有可能发生误报。您可以在企业主机安全控制台“入侵检测”页面中，选择“事件管理”页签，查看被隔离的恶意程序。在此您可以对指定的恶意程序执行取消隔离、忽略等操作。

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“安全告警事件”中，查看“恶意程序”中的告警信息，并对恶意程序进行隔离查杀。

----结束

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，企业主机安全将根据绑定的“消息通知服务主题”验证登录者的身份信息。

前提条件

- 用户已创建“协议”为“短信”或“邮箱”的消息主题。
- 主机已开启防护。
- 开启双因子认证需要关闭Selinux防火墙。

约束与限制

开启双因子认证后，仅以下登录方式支持双因子认证：

- Linux：使用SSH密码方式登录云服务器，且OpenSSH版本小于8。
- Windows：使用RDP文件登录Windows云服务器。

操作步骤

步骤1 在“双因子认证”页面，可勾选多个目标服务器后单击上方“开启双因子认证”，也可单击目标服务器操作列“开启双因子认证”。

步骤2 在弹出的“开启双因子认证”的对话框中，选择“验证方式”。

- **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。具体操作请参见《消息通知服务》中“创建主题”章节。
  - 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。

- **验证码验证**

  选择验证码验证，仅通过实时收到的验证进行验证。

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

须知

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

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

----结束

3 主机安全总览

3.1 风险统计

企业主机安全在控制台提供总览页面，实时展示了您所有资产的风险指数、风险趋势、TOP5事件类型以及您开通的主机安全和容器安全服务数量，帮助您实时了解主机和容器的安全状态和存在的安全风险。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“总览”，进入总览页查看相关信息。

----结束

风险指数（最近 24 小时）

显示最近24小时，企业主机安全开启防护的主机/容器资产存在的安全风险。

单击“立即处理”，在右侧展开安全风险处理面板，您可根据该面板的提示，参考对应的帮助文档或直接对风险进行处理。安全风险处理包含所有需要您尽快处理的安全风险和威胁，分为以下类别：

- 入侵风险
- 漏洞风险
- 基线风险

单击“重新体检”，您可立即对您的资产进行安全检测。

防护统计（最近 24 小时）

显示用户开启主机防护、容器防护和未开启防护的主机/节点的数量。

单击“开启防护”，可跳转到云服务器列表/容器节点列表，对未开启防护的服务器开启防护。

风险预防（最近 24 小时）

风险预防显示“主机资产风险”、“主机漏洞风险”、“主机基线风险”和“容器风险”个数以及与较昨日风险的对比。

风险趋势

风险趋势区域展示“最近24小时”“、最近3天”、“最近7天”、“最近30天”的风险趋势图。

表 3-1 风险趋势说明

风险分类	风险事件
主机资产风险	• 账号信息 • 开放端口 • 进程信息 • 软件信息 • 自启动项 • Web应用 • Web服务 • Web框架 • Web站点 • 中间件 • 数据库 • 内核模块
主机漏洞风险	• Linux漏洞 • Windows漏洞 • Web-CMS漏洞 • 应用漏洞
主机基线风险	• 口令复杂度策略检测 • 经典弱口令检测 • 配置检测
容器风险	• 本地镜像漏洞 • 私有镜像仓库漏洞 • 镜像恶意文件 • 镜像基线检查

入侵检测（最近 24 小时）

显示主机安全和容器安全入侵总个数，以及入侵威胁等级。

每日凌晨12点，定时统计并更新用户的所有主机/容器发生的入侵事件个数及入侵威胁等级个数。

TOP5 事件类型

基于开启了基础版、企业版、旗舰版防或容器安全护功能的云服务器，展示“最近24小时”、“最近3天”、“最近7天”、“最近30天”企业主机安全对其检测出的入侵检测TOP5的事件类型及各事件的数量。

如果因为网络原因，没有查询到TOP5事件类型的统计结果，可单击  ，重新查询凌晨12点统计的数据。

实时安全告警

查看主机安全和容器安全的实时告警详情。

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“威胁等级”、“告警名称”、“发生时间”、“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24小时内发生的最近5条“未处理”的入侵事件。
- 单击“查看更多”，可进入“安全告警事件”页面，处理相关告警事件。

4 资产管理

4.1 资产概览

展示您所使用全量资产的状态和清点情况。包括Agent状态、防护状态、配额情况以及账号、端口、进程、软件、自启动项的清点情况。

约束限制

未开启防护不支持查看资产概览。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“资产管理 > 资产概览”，进入资产概览总览页，查看资产状态和资产清点情况。

----结束

4.2 主机指纹

4.2.1 查看主机资产指纹

HSS提供主机资产指纹采集功能，支持采集主机中的端口、进程、Web应用、Web服务、Web框架和自启动项等资产信息。通过主机资产指纹功能，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。

前提条件

服务器已开启HSS企业版、旗舰版、网页防篡改版或容器版防护。

查看所有主机资产信息

步骤1 登录管理控制台。

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

步骤3 选择“资产管理 > 主机指纹”，进入“主机指纹”页面，查看所有主机资产。

表 4-1 主机资产指纹特性

功能项	功能描述	支持的操作系统	检测周期
账号	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“账号名称”、“服务器数”以及具体账号对应的“服务器名称/IP”、“登录权限”、“ROOT权限”、“用户组”、“用户目录”、“用户启动Shell”和“最近扫描时间”。 ● 账号的历史变动记录包括“服务器名称/IP”、“变动状态”、“登录权限”、“ROOT权限”、“用户组”、“用户目录”、“用户启动Shell”和“最近扫描时间”。	Linux、Windows	实时检测
开放端口	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。 根据“本地端口”、“协议类型”以及具体端口对应的“服务器名称/IP”、“状态”、“进程PID”、“程序文件”，您能够快速排查主机中含有风险的端口。 ● 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。	Linux、Windows	实时检测

功能项	功能描述	支持的操作系统	检测周期
进程	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。 根据主机中“进程路径”以及具体进程对应的“服务器名称/IP”、“启动参数”、“启动时间”、“运行用户”、“文件权限”、“进程PID”以及“文件HASH”，您能够快速排查主机中的异常进程。 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。	Linux、Windows	实时检测
软件	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。 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。 ● 软件的实时信息包括“软件名称”、“服务器数”以及具体软件对应的安装该软件的“服务器名称/IP”和“版本”、“软件更新时间”和“最近扫描时间”。 ● 软件的历史变动记录包括软件的“服务器名称/IP”、“变动状态”、“版本”、“软件更新时间”和“最近扫描时间”。	Linux、Windows	每日自动检测
自启动项	检测并列出当前所有主机系统中的自启动项，帮助用户及时发现异常自启动项，快速定位木马程序的问题。 ● 自启动项的实时信息包括“名称”、“类型”（自启动服务、开机启动文件夹、预加载动态库、Run注册表键或者定时任务）、“服务器数”以及类型对应的“服务器名称/IP”、“路径”、“文件HASH”、“运行用户”、以及“最近扫描时间”。 ● 自启动项的历史变动记录包括“服务器名称/IP”、“变动状态”、“路径”、“文件HASH”、“运行用户”和“最近扫描时间”。	Linux、Windows	实时检测
Web站点	统计、展示存放Web内容的目录及对外提供访问的站点信息，您可以查看所有目录及权限、以及和站点所关联访问路径、对外端口、证书信息（后续提供）、关键进程等信息。	Linux	1次/周（每周一凌晨06:00）
Web框架	统计、展示Web内容对外呈现时所使用框架的详细信息，您可查看所有框架的版本、路径、关联进程等信息。	Linux	1次/周（每周一凌晨06:00）

功能项	功能描述	支持的操作系统	检测周期
中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。	Linux、Windows	1次/周（每周一凌晨06:00）
内核模块	统计、展示运行在内核层的全量程序模块文件，您可查看所有模块所关联的服务器、版本号、模块描述、驱动文件路径、文件权限、文件哈希等信息。	Linux	1次/周（每周一凌晨06:00）
Web服务	统计、展示对外提供web内容访问的软件详细信息，您可查看所有软件的版本、路径、配置文件、关联进程等信息。	Linux	1次/周（每周一凌晨06:00）
Web应用	Web应用主要统计、展示推送发布web内容的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息。	Linux、Windows（仅支持Tomcat）	1次/周（每周一凌晨06:00）
数据库	统计、展示提供数据存储的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息；	Linux、Windows（仅支持mysql）	1次/周（每周一凌晨06:00）

----结束

查看单服务器的主机资产信息

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 单击目标服务器名称 ，进入目标服务器的详情页面，选择“资产指纹 > 主机资产”页签。

步骤5 单击指纹列表的目标指纹类型，查看对应资产信息。

----结束

4.3 容器指纹

4.3.1 查看容器资产指纹

HSS提供容器资产指纹采集功能，支持采集容器的账号、端口、进程、集群、服务和工作负载等资产信息。通过容器资产指纹功能，您能集中清点容器中的各项资产信息，及时发现容器中含有风险的各项资产。本章节介绍如何查看采集到容器资产信息。

约束限制

- 仅HSS容器版支持容器指纹功能
- 仅支持Linux系统。

查看所有容器的资产指纹数据

步骤1 登录管理控制台。

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

步骤3 选择“资产管理 > 容器指纹 > 资产指纹”，进入“资产指纹”页面，查看所有容器指纹数据。

表 4-2 容器资产指纹特性

功能项	功能描述	检测周期
账号	检测容器系统中的账号，列出当前系统的账号信息，帮助用户进行账户安全性管理。 账号的实时信息包括账号的“账号名称”、“服务器数”以及具体账号对应的“服务器名称/IP”、“登录权限”、“ROOT权限”、“用户组”、“用户目录”、“用户启动Shell”、“容器名称”、“容器ID”和“最近扫描时间”。	实时检测

功能项	功能描述	检测周期
开放端口	检测容器系统中的端口，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。 根据“本地端口”、“协议类型”以及具体端口对应的“服务器名称/IP”、“状态”、“进程PID”、“程序文件”，您能够快速排查容器中含有风险的端口。 ● 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。	实时检测
进程	检测容器系统中运行的进程，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。 根据容器中“进程路径”以及具体进程对应的“服务器名称/IP”、“启动参数”、“启动时间”、“运行用户”、“文件权限”、“进程PID”以及“文件HASH”，您能够快速排查容器中的异常进程。 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。	实时检测
软件	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。 根据软件的实时信息和历史变动，您能够快速排查容器中含有风险的软件。 ● 软件的实时信息包括“软件名称”、“服务器数”以及具体软件对应的安装该软件的“服务器名称/IP”和“版本”、“软件更新时间”和“最近扫描时间”。 ● 软件的历史变动记录包括软件的“服务器名称/IP”、“变动状态”、“版本”、“软件更新时间”和“最近扫描时间”。	每日自动检测

功能项	功能描述	检测周期
自启动项	检测并列出当前所有容器中的自启动项，帮助用户及时发现异常自启动项，快速定位木马程序的问题。 自启动项的实时信息包括“名称”、“类型”（自启动服务、开机启动文件夹、预加载动态库、Run注册表键或者定时任务）、“服务器数”以及类型对应的“服务器名称/IP”、“路径”、“文件HASH”、“运行用户”、“容器名称”、“容器ID”以及“最近扫描时间”。	实时检测
Web站点	统计、展示存放Web内容的目录及对外提供访问的站点信息，您可以查看所有目录及权限、以及和站点所关联访问路径、对外端口、证书信息（后续提供）、关键进程等信息。	1次/周（每周一凌晨06：00）
Web框架	统计、展示Web内容对外呈现时所使用框架的详细信息，您可查看所有框架的版本、路径、关联进程等信息。	1次/周（每周一凌晨06：00）
中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。	1次/周（每周一凌晨06：00）
Web服务	统计、展示对外提供web内容访问的软件详细信息，您可查看所有软件的版本、路径、配置文件、关联进程等信息。	1次/周（每周一凌晨06：00）
Web应用	统计、展示推送发布web内容的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息。	1次/周（每周一凌晨06：00）
数据库	统计、展示提供数据存储的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息；	1次/周（每周一凌晨06：00）

----结束

查看单容器的资产指纹数据

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 单击目标服务器名称，进入目标服务器的详情页面，选择“资产指纹 > 容器资产”页签。

步骤5 单击“指纹列表”的目标指纹类型，查看对应资产信息，资产指纹类型特性如**表 容器资产指纹特性**所示。

----结束

查看集群

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

步骤5 “最近同步时间”更新为最新同步任务完成时间，表示手动同步集群、服务、工作负载和容器实时数据成功。

步骤6 在“集群列表”页面，查看集群相关信息。

集群列表页面展示了集群的名称、类型、可用节点、版本、创建时间和状态信息。

- 搜索目标集群

  您可以在集群列表上方的搜索框中输入集群名称、状态等信息，单击，查找目标集群。

- 查看目标集群详细信息

  a. 单击目标集群名称，跳转到CCE控制台。

  b. 在CCE控制台，单击目标集群名称，进入集群详细信息页面，查看集群基本信息、网络信息和链接信息。

----结束

查看服务

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

步骤5 “最近同步时间”更新为最新同步任务完成时间，表示手动同步集群、服务、工作负载和容器实时数据成功。

步骤6 选择“服务 > 服务”，进入服务页面，查看服务相关信息。

服务页面展示了服务的名称、端点名称、访问方式、服务IP、命名空间、所属集群和创建时间信息。

- 搜索目标服务

  您可以在端点列表上方的搜索框中输入服务名称、访问方式等信息，单击，查找目标服务。

- 查看目标服务详细信息

  单击目标服务名称，进入服务的详情页面，可以查看目标服务的选择器、标签和端口等信息。

----结束

查看工作负载

步骤1 登录管理控制台。

步骤2 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤3 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

步骤4 “最近同步时间”更新为最新同步任务完成时间，表示手动同步集群、服务、工作负载和容器实时数据成功。

步骤5 选择“工作负载”，进入工作负载页面。

步骤6 选择不同的工作负载，查看相关工作负载的信息。

可查看无状态负载、有状态负载、守护进程集、普通任务、定时任务和容器组信息。各类工作负载列表展示的信息项请参见**表 工作负载信息项**。

您可以在各类工作负载列表上方的搜索框中输入工作负载名称、所属集群等信息，单击 ，查找目标工作负载。

表 4-3 工作负载信息项

工作负载类型	信息项
无状态负载	• 工作负载名称 • 状态 • 实例个数 • 命名空间 • 创建时间 • 镜像名称 • 所属集群
有状态负载	• 工作负载名称 • 状态 • 实例个数 • 命名空间 • 创建时间 • 镜像名称 • 所属集群

工作负载类型	信息项
守护进程集	• 工作负载名称 • 状态 • 实例个数 • 命名空间 • 创建时间 • 镜像名称 • 所属集群
普通任务	• 工作负载名称 • 状态 • 实例个数 • 命名空间 • 执行时间 • 镜像名称 • 所属集群
定时任务	• 工作负载名称 • 状态 • 任务触发 • 正在运行任务数 • 命名空间 • 最近调度时间 • 创建时间 • 镜像名称 • 所属集群
容器组	• 名称 • 命名空间 • 所属集群 • 节点 • 节点IP • POD IP • 状态 • 创建时间

----结束

查看容器实例

步骤1 登录管理控制台。

步骤2 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤3 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

步骤4 “最近同步时间”更新为最新同步任务完成时间，表示手动同步集群、服务、工作负载和容器实时数据成功。

步骤5 选择“容器实例”，进入容器实例页面，查看容器实例相关信息。

容器实例页面展示了容器的名称、状态、所属POD、所属集群、创建时间、镜像名称。

- 搜索目标容器

  您可以在容器列表上方的搜索框中输入容器名称、状态等信息，单击，查找目标容器。

- 查看目标容器详细信息

  单击目标容器名称，进入容器的详情页面，可以查看目标容器的进程、端口和数据挂载等信息。

----结束

4.4 主机管理

4.4.1 查看主机防护状态

主机管理的云服务器列表中仅显示以下主机的防护状态：在所选区域使用的主机。

查看主机防护状态

步骤1 登录管理控制台。

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

步骤3 在左侧导航树，选择“资产管理 > 主机管理”，在“云服务器”界面，查看服务器的防护状态，状态说明如**表 防护状态说明**所示。

- 在服务器防护列表上方，输入服务器名称、服务器ID或IP地址等，并单击搜索，可搜索查看目标服务器防护状态。
- 在服务器防护列表左侧通过选择服务器防护版本、资产重要性分类，可查看各类别服务器防护状态。

表 4-4 防护状态说明

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。

参数	说明
防护状态	• 防护中：HSS为该服务器提供全面的主机安全防护。 • 未防护：目标完全未开启主机安全防护。单击“操作”列“开启防护”可以开启HSS对服务器的防护，提升服务器的安全性。 • 防护中断：主机关机、Agent通信异常或Agent被卸载导致主机防护中断。
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。

----结束

查看网页防篡改防护状态

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在“主动防御 > 网页防篡改 > 防护配置”界面，查看服务器的防护状态。

防护列表上方，输入服务器名称、服务器ID或IP地址等，并单击搜索，可搜索查看目标服务器防护状态。

表 4-5 状态说明

参数名称	说明
防护状态	防护中：HSS为该服务器提供静态网页防篡改防护。
动态防篡改状态	动态网页防篡改的状态。
静态防篡改攻击	检测静态网页文件被攻击、被篡改的行为次数。
动态防篡改攻击	检测web应用的漏洞利用、注入攻击等行为次数。

----结束

主机列表导出

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 选择“资产管理 > 主机管理”，选择“云服务器”界面。

步骤3 在云服务器列表右上角单击，导出云服务器列表详情。

说明

当前云服务器详情导出单次最大支持1000台服务器。

----结束

4.4.2 开启防护

4.4.2.1 企业版/旗舰版

您可以为已的服务器开启企业版/旗舰版安全防护，开启后按照已申请版本所提供的能力对服务器进行安全防护。

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

已申请的服务器已正常安装Agent且“Agent状态”为“在线”、“防护状态”为“未防护”。

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。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 根据实际情况操作开启单服务器防护或通过勾选批量开启防护。

- **单服务器开启防护**

  在目标服务器“操作”列单击“开启防护”，在弹窗中确认服务器信息。

表 4-6 开启防护参数配置说明

参数名称	参数说明	取值样例
版本选择	提供企业版、旗舰版选择。 – 企业版：满足**等保认证**的需求，支持资产指纹管理、漏洞管理、恶意程序检测、Webshell检测、进程异常行为检测等能力。 – 旗舰版：满足**等保认证**的需求，支持应用防护、勒索防护、高危命令检测、提权检测、异常shell检测等能力。	企业版

- **批量开启防护**

  勾选多台目标服务器前的选框，单击上方“开启防护”，在弹窗中确认服务器信息。

表 4-7 开启防护参数配置说明

参数名称	参数说明	取值样例
版本选择	提供企业版、旗舰版选择。 – 企业版：满足**等保认证**的需求，支持资产指纹管理、漏洞管理、恶意程序检测、Webshell检测、进程异常行为检测等能力。 – 旗舰版：满足**等保认证**的需求，支持应用防护、勒索防护、高危命令检测、提权检测、异常shell检测等能力。	企业版

步骤5 确认信息无误，单击确认，开启防护，查看目标服务器的“防护状态”为“防护中”表示防护已开启。

----结束

4.4.2.2 网页防篡改版

您可以为已申请的服务器开启网页防篡改版安全防护，开启后按照网页防篡改版所提供的能力对服务器进行安全防护。

网页防篡改原理

表 4-8 网页防篡改原理

防护类型	原理说明
静态网页防护	1. 锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站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 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。
动态网页防护	为Tomcat提供动态网页防护。 1. 基于RASP过滤恶意行为 采用自研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。

前提条件

- 在“资产管理 > 主机管理”页面“云服务器”列表中目标服务器“Agent状态”为“在线”、“防护状态”为“未防护”。

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。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面，选择“防护配置”页签，进入“防护配置”页面。

步骤4 单击“添加防护服务器”，在弹窗勾选需要开启防护的服务器。

说明

选择的服务器数量应等于或少于可用配额数量。

步骤5 单击“添加并开启防护”，在“主动防御 > 网页防篡改 > 防护配置”查看目标服务器的“防护状态”为“防护中”表示已开启防护。

须知

- 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，操作详情请参见**添加防护目录**。
- 仅Linux服务器支持动态网页防篡改，且开启后，还需重启Tomcat才能使其生效。
- 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“主动防御 > 网页防篡改”，目标服务器所在行的“防护状态”为“防护中”，则表示网页防篡改版已开启。
  - 选择“资产管理 > 主机管理 > 云服务器”，目标服务器所在行的“版本选择”为“网页防篡改版”，则表示网页防篡改赠送的旗舰版已开启。

----结束

4.4.3 关闭防护

4.4.3.1 关闭企业版/旗舰版防护

您可以根据需求来关闭服务器的防护，关闭后可释放配额，可供其他服务器防护使用。

操作须知

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

关闭防护

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 根据实际情况操作关闭单服务器防护或通过勾选批量关闭防护。

- **单服务器关闭防护**
  a. 在目标服务器“操作”列单击“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。
  c. 关闭后在“云服务器”页面查看目标服务器的“防护状态”为“未防护”，关闭成功。

注意

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

- **批量关闭防护**
  a. 勾选多台目标服务器前的选框，单击上方“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，所有目标服务器防护关闭。
  c. 关闭后在“云服务器”页面查看目标服务器的“防护状态”为“未防护”，关闭成功。

注意

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

----结束

4.4.3.2 关闭网页防篡改版防护

您可以为已开启防护的服务器关闭网页防篡改版安全防护，关闭后可释放配额，可供其他服务器防护使用。

操作须知

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面，选择“防护配置”页签，进入“防护配置”页面。

步骤4 单击目标服务器“操作”列的“关闭防护”。

步骤5 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。

步骤6 关闭后在“资产管理 > 主机管理 > 云服务器”页面查看目标服务器的“防护状态”为“未防护”，关闭成功。

⚠ 注意

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

----结束

4.4.4 切换主机防护配额版本

您可以根据需要将服务器绑定的防护配额版本切换为基础版、专业版、企业版或旗舰版。

防护配额切换说明

服务器支持切换绑定的防护配额版本为企业版、旗舰版。

如需使用“网页防篡改版”或“容器版”，请先申请“网页防篡改版”或“容器安全”的配额，再开启网页防篡改版或容器版防护。

前提条件

- 待切换防护配额的服务器防护状态为“防护中”。
- 切换为低版本防护配额前，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。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“资产管理 > 主机管理 > 云服务器”，进入“云服务器”界面。

步骤4 选择需要切换版本的主机，单击“操作”列“切换版本”。

须知

- 若企业主机安全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，如需使用“网页防篡改版”，请先申请“网页防篡改版”的配额，再开启网页防篡改防护。

步骤5 单击“确定”切换版本。

切换企业主机安全版本后，请在云服务器列表页面查看目标服务器的版本。若目标服务器的“版本”为切换后的企业主机安全版本，则表示企业主机安全版本已切换成功。

----结束

后续操作

- 切换版本后，您可将空余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。
- 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。

4.4.5 部署策略

您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“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”或者“网页防篡改赠送旗舰版”后，开启旗舰版/网页防篡改版防护时，默认绑定了“旗舰版策略组”。

  用户也可以通过复制“旗舰版策略组”的方式，创建自定义策略组，将“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。

创建策略组

步骤1 登录管理控制台。

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

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

步骤4 复制策略组。

- 复制linux策略组：选择“tenant_linux_premium_default_policy_group”策略组，在该策略组所在行的“操作”列中，单击“复制”。
- 复制windows策略组：选择“tenant_windows_premium_default_policy_group”策略组，在该策略组所在行的“操作”列中，单击“复制”。

步骤5 在弹出的对话框中，输入“策略组名称”和“描述”。

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。

步骤6 单击“确认”，将会创建一个新的策略组。

步骤7 单击已创建的策略组名称，进入策略组的策略页面。

步骤8 单击“策略名称”，修改具体的策略内容，详细信息请参见**编辑策略内容**。

步骤9 策略内容修改完成后，单击策略所在行的“开启”或者“关闭”并单击右上角刷新，开启或者关闭对应的策略才会生效。

----结束

部署策略

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航栏，选择“资产管理 > 主机管理”，单击“云服务器”，进入云服务器列表界面。

步骤3 选中需要进行策略部署的一台或多台云服务器，单击“更多 > 部署策略”。

步骤4 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。

说明

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

----结束

4.4.6 管理服务器组

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。

创建服务器组

创建服务器组后，可将服务器按照一定类别分配到组进行统一管理。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 主机管理”，在“云服务器”界面，选择“服务器组”，单击“创建服务器组”。

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

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。

步骤5 设置完成后，单击“确认”，完成服务器组的创建。

----结束

分配服务器到组

若服务器没有被分配到服务器组，您可以将服务器分配到已创建的服务器组。

步骤1 单击“云服务器”，进入云服务器列表界面。

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

说明

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

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

说明

一个云服务器只能分配到一个服务器组。

----结束

相关操作

编辑服务器组

步骤1 选择“主机管理 > 云服务器”下的“服务器组”页签。

步骤2 在待修改的服务器组所在行的“操作”列，单击“编辑”，修改服务器组。

步骤3 在弹出的对话框中，可重新修改“服务器组名称”和设置分组包含的云服务器。

步骤4 完成修改后，单击“确认”，完成服务器组的修改。

----结束

删除服务器组

步骤1 选择“主机管理 > 云服务器”下的“服务器组”页签。

步骤2 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。

说明

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。

----结束

4.4.7 管理服务器重要性

HSS默认所有服务器为一般资产，您可以为服务器关联匹配的资产重要等级，关联后，您可通过资产重要等级对服务器进行分类管理。

资产重要等级分类如下：

- 重要资产：一般绑定运行业务或数据均为企业核心资产的服务器。

- 一般资产：一般绑定无重要业务运行、无核心资产的服务器。
- 测试资产：用于绑定用来测试业务或数据的服务器。

查看资产重要等级

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 在页签页面内下方查看“资产重要性”，单击“重要资产”、“一般资产”、“测试资产”，可按照类别查看服务器。

----结束

关联资产重要等级

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤3 关联资产重要性。

- 单服务器关联
  - 方式一：通过勾选服务器关联
    i. 勾选目标服务器前的选框，单击上方的“关联资产重要性”。
    ii. 在弹窗中“资产重要性”项选择对应的资产重要等级。
    iii. 确认无误，单击“确认”，完成关联。
  - 方式二：通过“操作”列选项关联
    i. 在目标服务器的“操作”列选择“更多 > 关联资产重要性”。
    ii. 在弹窗中“资产重要性”项选择对应的资产重要等级。
    iii. 确认无误，单击“确认”，完成关联。
- 批量关联
  a. 勾选多个目标服务器前的选框，单击上方的“关联资产重要性”。
  b. 在弹窗中“资产重要性”项选择对应的资产重要等级。
  c. 确认无误，单击“确认”，完成批量关联。

----结束

4.4.8 批量服务器一键安装 Agent（服务器账号、密码相同）

指导您完成服务器Agent的批量安装操作，创建批量安装后系统将自动执行Agent安装操作，安装后才可以对目标服务器开启防护。

前提条件

- 待安装Agent的服务器所属VPC内已有一台Agent在线的服务器。
- 待安装Agent的服务器需要支持ssh登录。
- 已获取待安装Agent的服务器正确的登录账号、端口、密码。
- 待安装Agent的服务器“状态”为“运行中”。

约束限制

- 目前仅支持Linux系统的服务器进行批量安装Agent。
- 单次最多可为50台服务器批量安装Agent。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面，选择“云服务器”页签，进入云服务器页面。

步骤4 单机上方“批量安装Agent”，在弹窗中勾选需要批量安装的服务器。

须知

- 批量安装的主机“服务器状态”必须为“运行中”。
- 批量安装Agent的服务器所属VPC内至少有一台服务器已安装Agent，若均未安装需先在VPC内至少安装一台，否则将安装失败。
- 单次勾选的所有服务器的root密码和端口都必须保持一致，若存在密码或端口其中任意一项不一致，需将按照密码和端口一致的服务器进行分批次安装，否则将安装失败。
- 批量安装单次最多50台服务器。

步骤5 确认无误，单击“下一步”，输入“服务器root密码”和“服务器登录端口”。

说明

系统默认系统端口为22，若需查询Linux SSH端口，远程登录目标服务器后，在Linux服务器中执行以下命令即可查询。

```
cat /etc/ssh/sshd_config | grep Port
```

步骤6 单击“确认”，服务器将自动执行Agent安装。

说明

自动安装程序为依次安装，您可在“资产管理 > 主机管理 > 云服务器”查看安装情况，若目标服务器“Agent状态”变更为“在线”，表示您已经可以对该服务器开启防护。

----结束

4.5 容器管理

4.5.1 查看容器节点防护列表

节点列表展示了云容器引擎服务（CCE）中集群节点的防护状态、节点状态和Agent状态，帮助您实时了解节点的安全状态。

约束限制

- 仅支持Linux系统。
- 未开启企业版、旗舰版、网页防篡改版、容器版防护不支持容器相关操作。

查看容器节点防护列表

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，单击“容器节点管理”。

步骤4 选择“节点列表”页签，查看节点防护状态。节点列表参数说明如表4-9所示。

说明

HSS容器节点列表只能查看已安装Agent的服务器，未安装Agent的服务器需要在“主机管理 > 云服务器”中查看。

表 4-9 节点防护状态参数说明

参数名称	说明
服务器名称	目标服务器名称。
容器防护状态	节点的防护状态，包括： • 未防护 • 防护中
服务器状态	• 运行中 • 不可用 • 正常
Agent状态	可通过选择状态来筛选想要查找的主机。 • 在线 • 离线 • 未安装

----结束

4.5.2 开启容器安全防护

您可以为已申请的服务器开启容器版安全防护，开启后按照容器版所提供的能力对服务器进行安全防护。

开启容器节点防护时，您需为指定的节点（主机）分配一个配额，关闭容器安全防护或删除节点（主机）后，该配额可分配给其他的节点（主机）使用。

检测周期

企业主机安全每日04：10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04：10检测后才能看到检测结果。

前提条件

- “资产管理 > 容器管理”页面“容器节点管理”中目标服务器“Agent状态”为“在线”。
- 已在云容器引擎成功创建节点。
- 节点的“容器防护状态”为“未防护”。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 根据需求可选择批量开启防护和单服务器开启防护。

- **单服务器开启防护**
  a. 在“节点列表”中目标服务器的“操作”列单击“开启防护”，为需要开启防护的节点开启防护。
  b. 在弹窗中确认信息。

  说明

  一个容器安全配额防护一个集群节点。

  c. 确认选择信息无误，单击确认，返回页面查看“容器防护状态”为“防护中”表示容器版安全防护已开启。
- **批量开启防护**
  a. 在“节点列表”中勾选多个目标服务器前的选框，单击上方“开启防护”。
  b. 在弹窗中确认信息。

  说明

  一个容器安全配额防护一个集群节点。

  c. 确认选择信息无误，单击确认，返回页面查看“容器防护状态”为“防护中”表示容器版安全防护已开启。

----结束

4.5.3 关闭容器版防护

您可以为已开启容器版防护的服务器关闭安全防护，关闭后可释放配额，可供其他服务器防护使用。

操作须知

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 根据需求可选择批量关闭防护和单服务器关闭防护。

- **单服务器关闭防护**
  a. 在“节点列表”中目标服务器的“操作”列单击“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。
  c. 关闭后在“资产管理 > 容器管理 > 节点列表”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

  注意

  关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

- **批量关闭防护**
  a. 在“节点列表”中勾选多个目标服务器前的选框，单击上方“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。
  c. 关闭后在“资产管理 > 容器管理 > 节点列表”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

  注意

  关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

----结束

4.5.4 容器镜像

4.5.4.1 SWR 私有镜像管理

私有镜像仓库中的镜像来源于容器镜像服务(SWR)的自有镜像，企业主机安全支持对这些共享镜像手动执行漏洞、恶意文件、软件信息、文件信息、基线检查、敏感信息的扫描并提供扫描报告。

约束限制

- 仅HSS容器版支持该功能。
- 仅支持对Linux镜像执行安全扫描。

查看私有镜像

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，进入容器管理界面，选择“容器镜像 > SWR私有镜像”页签。

步骤4 单击“从SWR更新自有镜像”，可以同步SWR所有自有镜像。

----结束

4.5.5 查看容器信息

您可以在容器管理页面查看容器信息，了解容器状态、所属集群以及安全风险情况等。本章节介绍如何查看容器信息。

约束限制

- 仅HSS容器版支持该功能。
- 仅支持Docker引擎的本地镜像上报到企业主机安全控制台。
- 仅支持对Linux镜像执行安全扫描。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“资产管理 > 容器管理”，进入“容器管理”页面。

步骤4 选择“容器”，进入容器页签。

步骤5 查看容器信息和安全状态。

您可以在容器列表查看容器名称、状态、是否有安全风险，重启次数、所属POD、所属集群等相关信息。

- 查看容器详细信息。

  单击目标容器名称，进入容器详情页面查看容器镜像、进程、端口、数据挂载等相关信息。

- 查看容器安全风险分布。

  鼠标滑动至有风险的目标容器所在行的安全风险列，查看容器存在低危、中危、高危、致命风险的数量。

----结束

5 风险预防

5.1 漏洞管理

5.1.1 漏洞管理概述

漏洞管理功能支持扫描Linux漏洞、Windows漏洞、Web-CMS漏洞和应用漏洞，并提供相关漏洞的修复建议和一键修复功能（Linux漏洞、Windows漏洞），帮助您及时了解和修复主机漏洞。本章节为您介绍漏洞扫描原理和HSS各版本支持扫描和修复的漏洞类型。

漏洞检测分为自动检测和手动检测，自动检测按照系统预设时间在每日凌晨自动执行，若需要查看目标服务器的漏洞情况或查看服务器当前漏洞情况可选择手动检测。

漏洞扫描原理

各类型漏洞的扫描原理如**表 漏洞扫描原理**所示。

表 5-1 漏洞扫描原理

漏洞分类	原理说明
Linux漏洞	通过与漏洞库进行比对，检测Linux操作系统官方维护的软件（非绿色版、非自行编译安装版；例如：kernel、openssl、vim、glibc等）是否存在的漏洞，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
Windows漏洞	通过同步微软官方的补丁公告，判断服务器上的补丁是否已经更新，并推送微软官方补丁，将存在风险的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，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
应用漏洞	通过检测服务器上运行的软件及依赖包发现是否存在漏洞，将存在风险的漏洞上报至控制台，并为您提供漏洞告警。

约束限制

- 基础版支持自动扫描和查看Linux系统漏洞、Windows系统漏洞，不支持切换主机视图和漏洞处理相关操作。
- 目标服务器“服务器状态”为“运行中”，“Agent状态”为“在线”，“防护状态”为“防护中”，否则无法进行漏洞扫描。
- 漏洞扫描和修复支持的操作系统**表 漏洞扫描和修复支持的操作系统**所示。

表 5-2 漏洞扫描和修复支持的操作系统

操作系统类型	支持的操作系统版本
Windows	• Windows Server 2019 数据中心版 64位英文(40GB) • Windows Server 2019 数据中心版 64位简体中文(40GB) • Windows Server 2016 标准版 64位英文(40GB) • Windows Server 2016 标准版 64位简体中文(40GB) • Windows Server 2016 数据中心版 64位英文(40GB) • Windows Server 2016 数据中心版 64位简体中文(40GB) • Windows Server 2012 R2 标准版 64位英文(40GB) • Windows Server 2012 R2 标准版 64位简体中文(40GB) • Windows Server 2012 R2 数据中心版 64位英文(40GB) • Windows Server 2012 R2 数据中心版 64位简体中文(40GB)
Linux	• EulerOS 2.2、2.3、2.5、2.8、2.9（64位） • CentOS 7.4、7.5、7.6、7.7、7.8、7.9（64位） • Ubuntu16.04、18.04、20.04（64位） • Debian 9、10、11（64位） • kylin V10（64位）

支持扫描和修复的漏洞类型

HSS各版本支持扫描和修复的漏洞类型请参见**表 HSS各版本支持扫描和修复的漏洞类型**。

表中的标识含义如下：

- √表示支持
- ×表示不支持

表 5-3 HSS 各版本支持扫描和修复的漏洞类型

漏洞类型	功能	基础版	企业版	旗舰版	网页防篡改版	容器版
Linux系统漏洞	自动扫描漏洞（默认每周一次）	√	√	√	√	√
	手动扫描漏洞	×	√	√	√	√
	漏洞一键修复	×	√（不支持全量修复，批量单次最多50条）	√	√	√
Windows系统漏洞	自动扫描漏洞（默认每周一次）	√	√	√	√	×
	手动扫描漏洞	×	√	√	√	×
	漏洞一键修复	×	√（不支持全量修复，批量单次最多50条）	√	√	×
Web-CMS漏洞	自动扫描漏洞（默认每周一次）	×	√	√	√	√
	手动扫描漏洞	×	√	√	√	√
	漏洞一键修复	×	×	×	×	×
应用漏洞	自动扫描漏洞（默认每周一次）	×	√	√	√	√
	手动扫描漏洞	×	√	√	√	√
	漏洞一键修复	×	×	×	×	×

说明

- HSS支持扫描Web-CMS漏洞、应用漏洞，不支持修复。您可以参考漏洞详情页面提示的修复建议，登录到您的服务器手动修复漏洞。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“风险预防 > 漏洞管理”，进入漏洞管理页查看漏洞概览。

----结束

5.1.2 漏洞扫描（手动）

如果您需要查看服务器实时的漏洞情况，您可以进行手动漏洞检测。

定期扫描资产漏洞，有利于减低资产损害风险。本章节为您介绍如何扫描漏洞。

手动扫描漏洞

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 单击漏洞管理界面右上角“手动扫描”。

步骤5 在漏洞扫描对话框中，选择扫描的漏洞类型和范围。相关参数说明请参见**表 手动扫描漏洞参数说明**。

表 5-4 手动扫描漏洞参数说明

参数	参数说明
漏洞类型	选择扫描的漏洞类型。目前支持扫描的漏洞类型如下： ● Linux系统漏洞 ● Windows系统漏洞 ● Web-CMS软件漏洞 ● 应用漏洞
扫描范围	选择扫描哪些服务器。 ● 全部服务器 ● 指定服务器 您可以选择服务器组或通过服务器名称、ID、公网IP、私网IP搜索目标服务器。 **说明** 以下服务器不能被选中执行漏洞扫描： ● 非“运行中”状态的服务器。 ● Agent状态为“离线”的服务器。

步骤6 单击“确定”。

步骤7 单击漏洞管理界面右上角的“任务管理”，选择“扫描任务”页签，可以查看漏洞扫描任务的执行状态和扫描情况。

单击扫描情况列红色图形旁的数字，可以查看扫描失败的服务器信息。

说明

您也可以在“资产管理 > 主机管理 > 云服务器”页面，为单台服务器手动扫描漏洞，具体操作如下：

1. 单击服务器名称。
2. 选择“漏洞管理”页签。
3. 选择需要扫描的漏洞类型页签，单击“手动扫描”。

----结束

自动扫描漏洞

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，单击“漏洞策略配置”，设置自动扫描漏洞的周期和范围。

- 扫描周期
  - 扫描时间段：默认00:00:00 - 07:00:00，不支持修改。
  - 扫描周期：选择每天、每三天或每周。
- 扫描范围
  - 选择扫描服务器：单击“管理”，在管理服务器页面，选择需要扫描的服务器。

    说明

    以下服务器不能被选中执行漏洞扫描：

    - 使用企业主机安全“基础版”的服务器。
    - 非“运行中”状态的服务器。
    - Agent状态为“离线”的服务器。

步骤5 单击漏洞管理界面右上角的“任务管理”，选择“扫描任务”页签，可以查看漏洞扫描任务的执行状态和扫描情况。

单击扫描情况列红色图形旁的数字，可以查看扫描失败的服务器信息。

----结束

5.1.3 查看漏洞详情

漏洞扫描完成后，您可以在漏洞管理页面查看资产中存在的漏洞。

约束限制

- 未开启防护的服务器不支持该功能。
- 目标服务器“服务器状态”为“运行中”，“Agent状态”为“在线”，“防护状态”为“防护中”。

查看漏洞详情（漏洞视图）

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面查看漏洞相关信息。

- 查看漏洞扫描结果概览

  在漏洞管理界面上方的漏洞数据统计区域，查看漏洞扫描结果汇总，相关参数说明请参见**表 漏洞扫描概览参数说明**。

  表 5-5 漏洞扫描概览参数说明

参数	说明
需紧急修复漏洞	单击“需紧急修复漏洞”区域的数字，您可以在需紧急修复漏洞页面查看各类需紧急修复的漏洞。
未完成修复的漏洞	单击“未完成修复的漏洞”区域的数字，您可以在未完成修复的漏洞页面查看各类需尚未修复的漏洞。
存在漏洞的服务器	单击“存在漏洞的服务器”区域的数字，您可以在漏洞管理界面下方查看存在漏洞的服务器。
今日处理漏洞	单击“今日处理漏洞”区域的数字，您可以在今日处理漏洞页面中查看今日已处理的各类型漏洞。
累计处理漏洞	单击“累计处理漏洞”区域的数字，您可以在累计处理漏洞页面中查看各类型累计已处理的漏洞。此项数据只统计一年内的累计处理数量，超过一年将重新开始统计。
已支持漏洞	展示HSS已支持检测漏洞个数。
累计执行漏洞扫描	展示漏洞扫描次数。 单击“手动扫描”，可以手动扫描服务器存在的漏洞。

- 查看漏洞影响的资产重要性

  在“影响主机（台）”列查看漏洞影响到的服务器的重要性。

  - ：表示重要资产
  - ：表示一般资产
  - ：表示测试资产

- 查看漏洞详情

  单击目标漏洞名称，进入漏洞详情页面，您可以查看该漏洞的修复建议、漏洞CVE详情、受影响服务器、历史处置记录等信息。

- 查看待处理或已处理漏洞

  在漏洞列表上方，漏洞处理状态选框中选择“待处理”或“已处理”，筛选待处理或已处理的漏洞。

- 导出漏洞列表

  单击漏洞列表上方的“导出”，一键导出漏洞数据，您可以在本地查看漏洞信息。

  说明

  单次最多支持导出30000条漏洞数据。

----结束

查看漏洞详情（主机视图）

说明

基础版不支持该操作。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面右上方，选择“主机视图”，查看漏洞相关信息。

- 查看漏洞扫描结果概览

  在漏洞管理界面上方的漏洞数据统计区域，查看漏洞扫描结果汇总，相关参数说明请参见**表 漏洞扫描概览参数说明**。

表 5-6 漏洞扫描概览参数说明

参数	说明
需紧急修复漏洞	单击“需紧急修复漏洞”区域的数字，您可以在需紧急修复漏洞页面查看各类需紧急修复的漏洞。
未完成修复的漏洞	单击“未完成修复的漏洞”区域的数字，您可以在未完成修复的漏洞页面查看各类需尚未修复的漏洞。
存在漏洞的服务器	展示当前存在漏洞的服务器数量。
今日处理漏洞	单击“今日处理漏洞”区域的数字，您可以在今日处理漏洞页面中查看今日已处理的各类型漏洞。
累计处理漏洞	单击“累计处理漏洞”区域的数字，您可以在累计处理漏洞页面中查看各类型累计已处理的漏洞。
已支持漏洞	展示HSS已支持检测漏洞个数。

参数	说明
执行漏洞扫描	展示漏洞扫描次数。 单击“手动扫描”，可以手动扫描服务器存在的漏洞。

- 查看主机详情和主机存在的漏洞
  a. 单击目标服务器名称，进入主机详情页面，您可以查看该主机的详细信息和存在的各类漏洞。
  b. 单击目标漏洞名称，进入漏洞详情页面，您可以查看该漏洞的漏洞CVE详情、受影响服务器、历史处置记录等信息。
- 查看待处理或已处理漏洞
  在漏洞列表上方，漏洞处理状态选框中选择“待处理”或“已处理”，筛选查看待处理或已处理的漏洞。
- 导出存在漏洞的主机列表
  单击漏洞列表上方的“导出”，一键导出漏洞数据，您可以在本地查看漏洞信息。

  说明

  单次最多支持导出30000条漏洞数据。

----结束

5.1.4 导出漏洞列表

您可以参考本章节导出漏洞列表到本地。

前提条件

- 服务器已开启HSS专业版及以上版本防护。
- 目标服务器“服务器状态”为“运行中”，“Agent状态”为“在线”，“防护状态”为“防护中”。

5.1.5 处理漏洞

当HSS扫描到服务器存在漏洞时，您需要及时根据漏洞的危害程度结合实际业务情况处理漏洞，避免漏洞被入侵者利用入侵您的服务器。

漏洞支持以下三种处理方式：

- **修复漏洞**
  如果漏洞对您的业务可能产生危害，建议您尽快修复漏洞。对于Linux漏洞、Windows漏洞，您可以在企业主机安全控制台一键自动修复漏洞，对于Web-CMS漏洞、应用漏洞，暂不支持自动修复，您可以参考漏洞详情界面提供的修复建议手动修复漏洞。
- **忽略漏洞**
  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。如果评估后确认某漏洞暂时无害，可以忽略该漏洞。下一次漏洞扫描任务执行后，HSS仍然会向您告警该漏洞。

- **添加漏洞白名单**

  如果确认漏洞不会对您的业务造成任何影响，无需修复，您可以将漏洞添加至白名单。漏洞加入白名单后，针对漏洞列表已经展示的漏洞信息会系统处理为“忽略”，不再为您上报告警，在下一次漏洞扫描任务执行时系统不会再扫描和呈现该漏洞信息。

约束限制

- CentOS 6和CentOS 8官方已停止维护，HSS使用Redhat的补丁公告替代扫描，因此这两个操作系统的漏洞无法修复，建议您切换其他操作系统。
- Ubuntu 18.04及以下版本目前已不支持免费补丁更新，需要申请配置Ubuntu Pro后才能安装升级包，未配置Ubuntu Pro会导致漏洞修复失败。
- CCE 、MRS、BMS的主机不能修复内核漏洞，贸然修复可能导致功能不可用。
- 处理漏洞时需保证目标服务器的“服务器状态”为“运行中”、“Agent状态”为“在线”、“防护状态”为“防护中”。

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，建议您通过云备份（CBR）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。

漏洞修复优先级

HSS的漏洞扫描系统将漏洞修复优先级分为紧急、高、中、低四个等级，您可以参考修复优先级优先修复对您的服务器影响较大的漏洞。

- 紧急：您必须立即修复的漏洞，攻击者利用该漏洞会对主机造成较大的破坏。
- 高：您需要尽快修复的漏洞，攻击者利用该漏洞会对主机造成损害。
- 中：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。
- 低：该类型的漏洞对主机安全的威胁较小，您可以选择修复或忽略。

漏洞显示时长

扫描到的漏洞，无论您是否处理过，都将在漏洞列表展示7天。

自动修复漏洞（漏洞视图）

仅Linux系统漏洞和Windows系统漏洞支持控制台一键自动修复漏洞。

说明

单次最多可修复1000个服务器漏洞，如果您有超过1000的漏洞需要修复，请分批修复。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 修复Linux漏洞和Windows漏洞

- 修复单个漏洞。

  在目标漏洞所在行的“操作”列，单击“修复”。
- 修复多个漏洞。

  勾选当前页面所有目标漏洞，单击漏洞列表左上角的“批量修复”，批量修复漏洞。

  如果需要修复所有Linux或Windows漏洞，您可以勾选批量修复对话框中的“选中全部Linux/Windows漏洞”。

  说明

  拥有至少一个旗舰版防护配额的主机时，支持选中全部Linux或Windows漏洞操作。
- 修复受漏洞影响的单台或多台服务器。

  a. 单击漏洞名称，进入漏洞详情页面。

  b. 选择“受影响服务器”页签，在目标服务器所在行的“操作”列，单击“修复”。

  您也可以勾选所有目标服务器，单击服务器列表上方的“批量修复”，批量为服务器修复漏洞。

步骤5 在修复对话框中勾选知晓风险后，单击“自动修复”。

步骤6 单击漏洞名称，进入漏洞详情页面。

步骤7 选择“历史处置记录”页签，您可以查看目标漏洞“状态”列的修复状态。漏洞修复状态含义请参见**表 漏洞修复状态说明**。

表 5-7 漏洞修复状态说明

状态	说明
未处理	表示漏洞未进行修复。
已忽略	漏洞对您的业务不会产生影响，您已经对漏洞进行了忽略处理。
验证中	表示HSS正在验证已修复的漏洞是否修复成功。
修复中	表示HSS正在为您修复漏洞。
修复成功	表示漏洞已经被成功修复。
修复成功待重启	表示漏洞已经修复成功，需要您尽快重启服务器。
修复失败	表示漏洞修复失败，可能因为漏洞已不存在或漏洞已经被更改。
请重启主机再次修复	仅Windows主机存在的漏洞会显示此状态。 表示Windows主机长时间未修复漏洞，导致最新的补丁无法成功安装，需要先安装之前的旧补丁后重启主机，再安装最新的补丁。

----结束

自动修复漏洞（主机视图）

仅Linux系统漏洞和Windows系统漏洞支持控制台一键自动修复漏洞。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 修复Linux漏洞和Windows漏洞。

- 修复服务器存在的所有Linux或Windows漏洞
  a. 在目标漏洞服务器所在行的“操作”列，单击“修复”。
     您也可以选中多台服务器，并在列表上方单击“批量修复”；如果需要修复所有主机漏洞，您可以勾选批量修复对话框中的“选中全部主机”。

     说明

     拥有至少一个旗舰版防护配额的主机时，支持选中全部主机操作。

  b. 在修复对话框中，勾选需要修复漏洞的类型并勾选知晓风险后，单击“确认”。
     仅Linux系统漏洞、Windows系统漏洞支持一键自动修复，Web-CMS漏洞、应用漏洞需要您登录服务器手动修复。
  c. 单击服务器名称，进入服务器详情页面，查看所有漏洞修复状态。漏洞修复状态含义请参见**表 漏洞修复状态说明**。
- 修复单台服务器存在的一个或多个漏洞
  a. 单击目标漏洞服务器名称，进入服务器详情页面。
  b. 在目标漏洞所在行的“操作”列，单击“修复”。
     您也可以勾选所有目标漏洞，单击漏洞列表上方的“批量修复”，批量修复漏洞。
  c. 勾选知晓风险后，单击“自动修复”。
  d. 在目标漏洞行的状态列，查看漏洞的修复状态。漏洞修复状态含义请参见**表 漏洞修复状态说明**。

表 5-8 漏洞修复状态说明

状态	说明
未处理	表示漏洞未进行修复。
已忽略	漏洞对您的业务不会产生影响，您已经对漏洞进行了忽略处理。
验证中	表示HSS正在验证已修复的漏洞是否修复成功。
修复中	表示HSS正在为您修复漏洞。
修复成功	表示漏洞已经被成功修复。
修复成功待重启	表示漏洞已经修复成功，需要您尽快重启服务器。

状态	说明
修复失败	表示漏洞修复失败，可能因为漏洞已不存在或漏洞已经被更改。
请重启主机再次修复	仅Windows主机存在的漏洞会显示此状态。 表示Windows主机长时间未修复漏洞，导致最新的补丁无法成功安装，需要先安装之前的旧补丁后重启主机，再安装最新的补丁。

----结束

手动修复漏洞

对于Web-CMS漏洞和应用漏洞，HSS不支持一键自动修复，您可以参考漏洞详情页面的修复建议，登录服务器手动修复。

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服务器，否则HSS仍可能为您推送漏洞消息。
- 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。

查看漏洞修复建议

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 单击目标漏洞名称，进入漏洞详情页面，查看修复建议。

----结束

参考漏洞修复方案进行漏洞修复

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
  a. 为需要修复漏洞的ECS主机创建镜像。
  b. 使用该镜像创建新的ECS主机。
  c. 在新启动的主机上执行漏洞修复并验证修复结果。
  d. 确认修复完成之后将业务切换到新主机。
  e. 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
  a. 为需要修复漏洞的ECS主机创建备份。

b. 在当前主机上直接进行漏洞修复。

c. 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态。

说明

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

忽略漏洞

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，企业主机安全将不会对该漏洞告警。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在目标漏洞所在行的“操作”列，单击“忽略”。

步骤5 在弹出的对话框中，单击“确认”。

----结束

漏洞添加白名单

如果您评估某些漏洞对您的业务不会产生影响，并且不想在漏洞列表中看到该漏洞，您可以将该漏洞加入白名单，加入白名单后，针对漏洞列表已经展示的漏洞信息会处理为忽略，不再为您上报告警，在下一次漏洞扫描任务执行时不再扫描该漏洞和呈现该漏洞信息。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

- 将漏洞影响的所有服务器加入白名单

  HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。

  a. 在目标漏洞所在行的“操作”列，选择“更多 > 加入白名单”。

  您也可以都选多个目标漏洞，单击漏洞列表上方的“加入白名单”。

  b. 在弹出的对话框中，单击“确认”。

- 将漏洞影响的单个或多个服务器加入白名单。

  HSS为这些服务器扫描漏洞时，不再关注漏洞。

  a. 单击目标漏洞的名称，进入漏洞详情页面。

b. 选择“受影响服务器”页签。
c. 在目标服务器所在行的“操作”列，选择“更多 > 加入白名单”。
   您也可以勾选多个服务器，单击服务器列表上方的“加入白名单”。
d. 在弹出的对话框中，单击“确认”。

- 通过白名单规则将漏洞加入白名单。
  a. 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。
  b. 在漏洞白名单配置区域，单击“新增规则”。
  c. 根据界面提示配置白名单规则，相关参数说明请参见**表 漏洞白名单规则参数说明**。

表 5-9 漏洞白名单规则参数说明

参数	说明
类型选择	选择添加白名单的漏洞类型： ■ Linux系统漏洞 ■ Windows系统漏洞 ■ Web-CMS软件漏洞 ■ 应用漏洞
漏洞选择	选择为哪个漏洞添加白名单。支持选择单个或多个漏洞。
规则范围	选择将漏洞影响的哪些服务器添加到白名单。 ■ 全部服务器 HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。 ■ 指定服务器 选择单个或多个目标服务器，HSS为这些服务器扫描漏洞时，不再关注漏洞。 您可以通过服务器名称、ID、公网IP、私网IP搜索目标服务器。
备注（可选）	填写您需要备注的信息。

d. 单击“确认”。

----结束

修复验证

漏洞修复后，建议您立即进行验证。

手动验证

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

表 5-10 验证修复命令

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

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。

5.1.6 管理漏洞白名单

如果您评估某些漏洞对您的业务不会产生影响，并且不想在漏洞列表中看到该漏洞，您可以将该漏洞加入白名单，加入白名单后，针对漏洞列表已经展示的漏洞信息会处理为忽略，不再为您上报告警，在下一次漏洞扫描任务执行时不再扫描该漏洞和呈现该漏洞信息。

本章节为您介绍漏洞如何加入白名单，以及如何修改和删除漏洞白名单。

漏洞添加白名单

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

- 将漏洞影响的所有服务器加入白名单

  HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。

  a. 在目标漏洞所在行的“操作”列，选择“更多 > 加入白名单”。

  您也可以都选多个目标漏洞，单击漏洞列表上方的“加入白名单”。

  b. 在弹出的对话框中，单击“确认”。

- 将漏洞影响的单个或多个服务器加入白名单。

  HSS为这些服务器扫描漏洞时，不再关注漏洞。

  a. 单击目标漏洞的名称，进入漏洞详情页面。

  b. 选择“受影响服务器”页签。

  c. 在目标服务器所在行的“操作”列，选择“更多 > 加入白名单”。

  您也可以勾选多个服务器，单击服务器列表上方的“加入白名单”。

  d. 在弹出的对话框中，单击“确认”。

- 通过白名单规则将漏洞加入白名单。

  a. 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。

  b. 在漏洞白名单配置区域，单击“新增规则”。

c. 根据界面提示配置白名单规则，相关参数说明请参见**表 漏洞白名单规则参数说明**。

表 5-11 漏洞白名单规则参数说明

参数	说明
类型选择	选择添加白名单的漏洞类型： ■ Linux系统漏洞 ■ Windows系统漏洞 ■ Web-CMS软件漏洞 ■ 应用漏洞
漏洞选择	选择为哪个漏洞添加白名单。支持选择单个或多个漏洞。
规则范围	选择将漏洞影响的哪些服务器添加到白名单。 ■ 全部服务器 HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。 ■ 指定服务器 选择单个或多个目标服务器，HSS为这些服务器扫描漏洞时，不再关注漏洞。 您可以通过服务器名称、ID、公网IP、私网IP搜索目标服务器。
备注（可选）	填写您需要备注的信息。

d. 单击“确认”。

----结束

编辑漏洞白名单

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。

步骤5 在目标漏洞白名单规则所在行的“操作”列，单击“编辑”。

步骤6 在编辑界面，完成信息修改后，单击“确认”。

----结束

删除漏洞白名单

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。

步骤5 在目标漏洞白名单规则所在行的“操作”列，单击“删除”。

步骤6 在弹窗中确认信息后，单击“确认”。

----结束

5.1.7 查看漏洞历史处置记录

对于已经处理过的漏洞，您可以参考本章节查看漏洞历史处置记录（处理人、处理时间）。

查看单个漏洞的历史处置记录

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入“漏洞管理”页面。

步骤4 在已处理漏洞列表中，单击漏洞名称，进入漏洞详情页面。

步骤5 选择“历史处置记录”页签，查看单个漏洞的历史处置记录。

----结束

查看所有漏洞的历史处置记录

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“安全运营 > 历史处置记录”，进入“历史处置记录”页面。

步骤4 选择“漏洞管理”页签，查看所有漏洞的历史处置记录。

- 查看指定属性的漏洞处置记录
  在漏洞处置记录列表上方搜索框中，输入漏洞类型、漏洞名称、服务器IP等并单击，可查看指定属性的漏洞处置记录。

----结束

5.2 基线检查

5.2.1 查看基线检查概览

HSS提供基线检查功能，包括检测复杂策略、弱口令及配置详情，包括对主机配置基线通过率、主机配置风险TOP5、主机弱口令检测、主机弱口令风险TOP5的统计。主动检测主机中的口令复杂度策略，关键软件中含有风险的配置信息，并针对所发现的风险为您提供**修复建议**，帮助您正确地处理服务器内的各种风险配置信息。

检查方式

- 自动检查

  企业主机安全默认**每日凌晨01：00**左右将自动进行一次全面的检查。若您需自定义基线自动检测周期及时间，您可开启旗舰版、网页防篡改版、容器版满足需求，自定义基线自动检测周期操作详情请参见**配置检测**。

- 手动检查

  如果您需要查看指定服务器的基线风险，您可以为这些服务器**创建基线检查策略**，然后在“基线检查”页面右上角，选择目标基线检查策略，单击“手动检测”。在手动基线检测完成后，查看指定服务器的基线风险。

检查详情

检查项名称	检查详情说明
口令复杂度策略检测	检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性。
经典弱口令检测	检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改。
配置检查	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。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 在“基线检查”页面，查看检测数据的统计，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，参数说明如**表5-12**所示。

如果您想查看不同基线检查策略下服务器的检查数据统计，您可以通过切换“基线检查策略”进行查看。

表 5-12 基线检查概览

参数名称	参数说明
基线检查策略	选择要查看的基线策略检测的结果，所有可选择的基线检查策略均为已添加的基线检查策略，可进行自定义创建、编辑、删除。
检测主机数	已检测的主机总数。
检测基线数	检测主机时执行的基线数。
主机配置检查项	已检查主机配置项的总数。
主机配置基线通过率	按照基线检测主机配置通过的配置项占总检测项的占比，同时按照不同风险等级分别统计未通过的配置项总数。
主机配置风险TOP5	按照主机的维度统计存在配置风险的主机。 优先按照高危且风险总数最多的前5台主机进行排序，若不存在高危，则依次为中危、低危。
主机弱口令检测统计	统计检测弱口令的主机总数，以及有弱口令、未开启检测、无弱口令检测的主机数。
主机弱口令风险TOP5	按照主机的维度统计存在弱口令风险最多的前5台主机。
配置检查	对所有存在配置风险的主机进行等级告警及风险信息统计。
口令复杂度策略检测	对所有主机存在弱口令复杂度不满足基线标准的进行统计。
经典弱口令检测	按照主机的维度对存在弱口令的主机及涉及的账号进行统计。

----结束

手动执行基线检查

须知

- 手动检测只针对目标基线策略所关联的服务器。若使用默认策略，请先**关联服务器**后再执行手动检测。
- 执行手动检测前，请先确认在“基线检查策略”选框是否可以选择到目标策略，若需新建策略，详情请参见**新建基线检查策略**。

步骤1 在“风险预防 > 基线检查”概览页选择目标“基线检查策略”。

步骤2 单击页面右上角“手动检测”，执行检测。

步骤3 查看“基线检查策略”下方“最近检测时间”为当前检测时间时，表示检测完成。

说明

- 执行手动检测后，按钮状态变为检测中，若检测时间超过30分钟，按钮会自动释放为可单击状态，此时仍需等待“最近检测时间”显示为当前检测时间才表示检测完成。
- 检测结束后可参照**查看基线检查详情**查看对应检查项结果及修改建议。

----结束

导出基线检查报告

根据需要可通过筛选导出基线检测报告。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 在“基线检查”页面，查看检测数据的统计，选择不同页签，可查看HSS检测到的风险告警。

说明

当前仅支持“配置检查”和“经典弱口令检测”的报告导出。

步骤5 选择“配置检查”或“经典弱口令检测”页签，在列表右上角单击，对筛选的风险告警进行下载。

说明

- 在“配置检查”页签可单击“风险等级”和“标准类型”对告警信息进行筛选。
- 在“经典弱口令检测”页签可通过筛选服务器名称、IP地址、账号名称进行筛选下载。
- “配置检查”和“经典弱口令检测”的风险检测报告单次下载最大数量为5000条。

----结束

5.2.2 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。

前提条件

配置检查只有开启了防护且防护配额在企业版及以上的主机数据才会显示在列表中。

检查项列表

表 5-13 检查项列表

检查项	说明
配置检查	目前支持的检测标准及类型如下： ● Linux系统： – 云安全实践：Apache2、Docker、MongoDB、Redis、MySQL5、Nginx、Tomcat、SSH、vsftp、CentOS7、EulerOS、EulerOS_ext、Kubernetes-Node、Kubernetes-Master。 – 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS6、CentOS7、CentOS8、Debian9、Debian10、Debian11、Redhat6、Redhat7、Redhat8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma。 ● Windows系统： – 云安全实践：MongoDB、Apache2、MySQL、Nginx、Redis、Tomcat、Windows_2008、Windows_2012、Windows_2016、Windows_2019。
口令复杂度策略检测	检测系统账号的口令复杂度策略。
经典弱口令检测	通过与弱口令库对比，检测账号口令是否属于常用的弱口令。 支持MySQL、FTP及系统账号的弱口令检测。

查看配置检查

查看配置检查的风险统计及对应的处理建议。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 选择“配置检查”页签，查看所有服务器的配置检查风险项，参数说明如表5-14所示。

如果您需要查看指定基线检查策略下服务器的配置检查结果统计，您可以在基线检查策略栏选择目标基线检查策略后查看。

表 5-14 配置检查参数说明

参数名称	参数说明
风险等级	按照基线标准匹配检测结果划分的等级。 • 高危 • 低危 • 中危 • 无风险
基线名称	检测执行的基线的名称。
标准类型	检测执行的基线所属策略的标准类型。 • 云安全实践 • 等保合规
检查项	累计检查的配置项总数。
风险项	检查项中存在风险的配置项总数。
影响服务器数	目标风险基线所影响的服务器总数。
最新检测时间	最近一次检测的时间。
描述	目标风险基线的描述说明。

步骤5 单击列表中目标基线名称，查看目标基线描述、受影响服务器以及所有检查项详情。

步骤6 单击目标检查项“操作”列的“检测详情”，查看检查项描述、审计描述和修改建议。

您需要确认检查的风险项是否是致命或需要修改的风险。

如果是，可根据修改建议对目标检查项进行修改。如果不是，可在配置检查项列表页面单击目标检查项“操作”列的“忽略”操作进行忽略。

----结束

查看口令复杂度策略检测

查看口令复杂度策略检测的风险统计及对应的处理建议。

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤3 选择“口令复杂度策略检测”页签，查看口令复杂度策略检测的风险统计项及修改建议，参数说明如表5-15所示。

表 5-15 口令复杂度策略检测参数说明

参数名称	参数说明
服务器名称/IP地址	被检测的服务器名称及IP地址。
口令长度	目标服务器的口令长度是否符合标准。 • 符合 • 不符合
大写字母	目标服务器的口令大写字母是否符合标准。 • 符合 • 不符合
小写字母	目标服务器的口令小写字母是否符合标准。 • 符合 • 不符合
数字	目标服务器的口令数字是否符合标准。 • 符合 • 不符合
特殊字符	目标服务器的口令特殊字符是否符合标准。 • 符合 • 不符合
建议	对目标服务器发现的口令风险的修改建议。

----结束

查看经典弱口令检测

查看经典弱口令检测的风险统计及对应的处理建议。

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤3 选择“经典弱口令检测”页签，查看服务器中存在风险的弱口令账号的统计，参数说明如表5-16所示。

表 5-16 经典弱口令检测参数说明

参数名称	参数说明
服务器名称/IP地址	被检测的服务器名称及IP地址。
账号名称	目标服务器中被检测出是弱口令的账号。
账号类型	账号的类型。

参数名称	参数说明
弱口令使用时长（单位：天）	目标弱口令使用的时间周期。

说明

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

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

- 口令设置建议：设置长度超过8个字符且均包含大写字母、小写字母、数字和特殊字符。

----结束

导出基线检查报告

在基线检查页面，可对配置检查和经典弱口令检查详情进行导出，列表右上角单击  ，可将所有云服务器的配置检测风险列表下载到本地。

说明

- 不支持对单个云服务器执行导出。
- 单次最大导出告警数为5000条。

5.2.3 基线检查风险项修复及验证

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。

弱口令修复

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

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

单服务器风险修复及验证

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。

步骤1 在HSS控制台选择“资产管理 > 主机管理 > 云服务器”，进入服务器页面。

步骤2 搜索目标服务器，单击目标服务器名称进入服务器详情页面。

步骤3 选择“基线检查 > 配置检查”页签，单击风险项前的展开按钮，查看所有检查项。

步骤4 处理风险项。

- 忽略风险

  在目标检查项“操作”列单击“忽略”，忽略单条风险检查项。

  勾选多个目标检查项前的选框，单击上方出现的“忽略”按钮，进行批量忽略处理。

- 修复风险

  a. 单击目标风险项“操作”列的“检查详情”，查看检查项详情。

  b. 查看“审计描述”、“修改建议”等信息，根据“修改建议”修复主机中的异常信息。

  说明

  - 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。

----结束

全量服务器风险修复及验证

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。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 选择“配置检查”页签，查看所有服务器的配置检查风险项，参数说明如表5-17所示。

如果您需要查看指定基线检查策略下服务器的配置检查结果统计，您可以在基线检查策略栏选择目标基线检查策略后查看。

表 5-17 配置检查参数说明

参数名称	参数说明
风险等级	按照基线标准匹配检测结果划分的等级。 • 高危 • 低危 • 中危 • 无风险
基线名称	检测执行的基线的名称。

参数名称	参数说明
标准类型	检测执行的基线所属策略的标准类型。 ● 云安全实践 ● 等保合规
检查项	累计检查的配置项总数。
风险项	检查项中存在风险的配置项总数。
影响服务器数	目标风险基线所影响的服务器总数。
最新检测时间	最近一次检测的时间。
描述	目标风险基线的描述说明。

步骤5 单击列表中目标基线名称，查看目标基线描述、受影响服务器以及所有检查项详情。

步骤6 处理风险项。

- 忽略风险

  在目标检查项“操作”列单击“忽略”，忽略单条风险检查项。

  勾选多个目标检查项前的选框，单击上方出现的“忽略”按钮，进行批量忽略处理。

- 修复风险

  a. 单击目标风险项“操作”列的“检查详情”，查看检查项详情。

  b. 查看“审计描述”、“修改建议”等信息，根据“修改建议”或“检测用例信息”的“期望结果”修复主机中的异常信息。

  说明

  ■ 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。

  c. 单击“受影响服务器”，查看该检查项影响的服务器。

  单击“验证”，可更新受影响的服务器列表。

----结束

5.2.4 基线检查策略管理

您可通过新建、编辑、删除来管理手动检测时的基线检查策略，同时可对基线策略的检查项进行自定义编辑，根据需要创建不同的基线检查策略。

约束限制

- 在“风险预防 > 基线检查 > 策略管理”中的策略仅限于基线检查的“手动检测”时使用。若需对基线检查的基础策略进行编辑，操作详情请参见**编辑策略内容**章节中的“配置检测”和“弱口令检测”。
- 未开启防护的服务器不支持基线相关操作。

新建基线检查策略

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 单击页面右上角“策略管理”，进入策略列表页面。

步骤5 单击“新建策略”，填写配置策略信息，参数说明如表5-18所示。

鼠标滑动至基线名称右侧，单击“规则详情”，可以查看每个检查基线的详细信息。

说明

“操作系统”选择“Linux系统”时，所有“检测基线”项下的子基线支持自定义勾选检测规则检查项，Windows暂不支持。

表 5-18 新建基线策略信息

参数名称	参数说明	取值样例
策略名称	自定义策略名称。	linux_web1_security_policy
操作系统	选择基线检测的目标系统。 ● Linux ● Windows	Linux
检测基线	自定义勾选支持的检测标准及类型，详情如下： ● Linux系统： – 云安全实践：Apache2、Docker、MongoDB、Redis、MySQL5、Nginx、Tomcat、SSH、vsftp、CentOS7、EulerOS、EulerOS_ext、Kubernetes-Node、Kubernetes-Master。 – 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS6、CentOS7、CentOS8、Debian9、Debian10、Debian11、Redhat6、Redhat7、Redhat8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma。 ● Windows系统： – 云安全实践：MongoDB、Apache2、MySQL、Nginx、Redis、Tomcat、Windows_2008、Windows_2012、Windows_2016、Windows_2019。	云安全实践：全选 等保合规：全选

步骤6 确认填写信息无误，单击“下一步”，根据服务器名称、服务器ID、弹性公网IP地址或私有IP地址选择需要应用关联的服务器。

步骤7 确认无误，单击“确认”，在策略管理页面新增1条基线策略，新建完成。

----结束

编辑基线检查策略

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤3 单击页面右上角“策略管理”，进入策略列表页面。

步骤4 单击目标策略“操作”列的“编辑”，进入策略详情页面，可对策略名称、检测基线项进行修改。

步骤5 确认修改无误，单击“下一步”，编辑需要应用的服务器。

步骤6 确认无误，单击“确认”，编辑完成，可在“策略管理”页面查看目标策略编辑后的信息。

----结束

删除基线检查策略

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤3 单击页面右上角“策略管理”，进入策略列表页面。

步骤4 单击目标策略“操作”列的“删除”，在弹窗确认删除的信息无误，单击“确认”，完成删除。

----结束

5.3 容器镜像安全

5.3.1 镜像漏洞

本章节指导用户查看私有镜像上存在的漏洞，并判断是否需要“忽略”漏洞。

前提条件

已开启容器节点防护。

检测方式

用户开启容器节点防护后，容器安全服务**自动执行**对Linux镜像的安全扫描。

约束限制

仅支持查看Linux镜像存在的漏洞。

查看私有镜像仓库漏洞

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航树中，选择“风险预防 > 容器镜像安全”，选择“容器镜像漏洞 > 私有镜像仓库漏洞”页签，查看私有镜像窗口漏洞。

说明

单击风险镜像名称，可查看该风险镜像的漏洞概况，包括漏洞名称、修复紧急度、受影响镜像个数、漏洞描述等信息。

表 5-19 参数说明

参数名称	说明	操作
漏洞名称	-	• 单击 ，查看漏洞详情，包括漏洞ID、漏洞分值、漏洞披露时间和漏洞描述。 • 单击漏洞名称，查看该漏洞的基本信息以及受该漏洞影响的镜像列表，具体请参见步骤**步骤3**。
修复紧急度	提示您是否需要立刻处理该漏洞。	-
受影响镜像数（个）	显示受该漏洞影响的镜像个数。	-
解决方案	针对该漏洞给出的解决方案。	单击“解决方案”列的链接，查看修复意见。

步骤3 单击漏洞名称，查看该漏洞的基本信息及受该漏洞影响的镜像列表。

----结束

5.3.2 镜像恶意文件

容器安全服务能自动检测私有镜像仓库恶意文件，为您展示资产中存在的安全威胁，大幅降低您使用镜像的安全风险。

检测周期

容器安全服务**每日凌晨**自动执行一次全面的检测。

前提条件

已开启容器节点防护。

约束限制

仅支持检测Linux镜像存在的恶意文件。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

步骤4 选择“镜像恶意文件”页签，查看私有镜像中恶意文件详情，并根据检测结果删除恶意文件，重新制作镜像。

- 恶意文件类型如：Trojan、Worm、Virus病毒和Adware垃圾软件等类型。
- 在“镜像版本”列，单击某个镜像版本号，可查看该镜像版本的漏洞报告详情。

----结束

5.3.3 镜像基线检查

基线检查功能自动检测您私有镜像仓库中存在的配置风险，针对所发现的问题为您提供加固建议，帮助您正确地处理镜像内的各种风险配置信息，降低入侵风险并满足安全合规要求。

检测周期

企业主机安全每天04：10自动进行一次全面的检查。

前提条件

已开启容器节点防护。

约束限制

仅支持检测Linux镜像存在的配置风险。

检测项

- 确保系统中不存在账号名或UID相同的账号
- UID为0的非root账号检查
- 代码中的口令检查
- 确保系统中不存在相同密码哈希值的账号
- 禁止使用弱密码哈希算法
- 确保账户密码不为空
- 确保系统中不存在相同组名或GID
- 确保没有非特权账号加入特权组
- 确保/etc/passwd中不存在旧的"+"条目
- 确保/etc/shadow中不存在旧的"+"条目
- 确保/etc/group中不存在旧的"+"条目
- 确保/etc/passwd中的所有组都存在于/etc/group中
- 确保配置了密码有效期

- 确保所有用户的密码更改日期都是过去日期
- 禁用建立host信任
- 禁止建立预置的root级别的信任关系
- 确保root账户的默认组为GID 0
- 确保shadow组为空

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

步骤4 选择“镜像基线检查”页签，查看镜像中存在的配置风险。

步骤5 单击检测项前的，查看该检测项的详情、存在的问题及加固建议，并根据加固建议修复有风险的配置信息。

----结束

6 主动防御

6.1 网页防篡改

6.1.1 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。

前提条件

已开启企业主机安全版本为网页防篡改版。

约束与限制

- 仅开启网页防篡改版防护后才支持防篡改相关操作。
- 防护目录，存在以下约束：
  - Linux系统：
    - 每台服务器最多可添加50个防护目录。
    - 每个被防护的目录的完整路径长度不得超过256个字符。
    - 每个被防护的目录文件夹层级不超过100。
    - 所有被防护的目录下的文件夹个数不超过900000。
  - Windows系统：
    - 每台服务器最多可添加50个防护目录。
    - 每个被防护的目录的完整路径长度不得超过256个字符。
- 本地备份路径，存在以下约束：
  - 本地备份功能仅支持Linux系统。
  - 本地备份路径须为合法路径，如果该路径不存在，会导致防篡改不生效。

- 本地备份路径与添加的防篡改目录不能重叠。
- 本地备份路径所属磁盘剩余可用容量大于所有被防护目录的大小。

添加防护目录

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤4 单击“防护目录设置”下的“设置”，进入防护目录设置页面。

步骤5 添加防护目录，您最多可在主机中添加50个防护目录。

1. 单击“添加防护目录”，在弹出的“添加防护目录”对话框中添加防护目录，有关防护规则的详细内容请参见**表6-1**。

表 6-1 防护规则

参数	说明	限制
防护目录	防护目录下的文件和文件夹为只读。	请勿对操作系统目录进行防护。
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，最多可添加10个子目录。	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。	-

参数	说明	限制
本地备份路径	- 仅支持Linux系统。 - 开启网页防篡改防护后，防护目录下的文件会自动备份到设置的本地备份路径中。 - 防护目录下文件大小不同，备份时间也不同，一般约10分钟备份完成。备份完成后，立即生效。 - 被排除的子目录和文件类型不会备份。 - 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。	本地备份路径与添加的防护目录不能重叠。
排除文件路径列表	- 排除防护目录下不需要防护的路径。 - 多个路径请用英文分号隔开，最多可添加50个路径，路径最长字符限制为256。 - 单个路径不能以空格开始，不能以/结束。	排除文件路径为防护目录的相对文件路径。

2. 添加完成后，单击“确认”，完成添加防护目录的操作。

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

步骤6 启用远端备份。

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

有关添加远端备份服务器的详细操作，请参见**配置远端备份**。

1. 在“防护目录设置”页单击“启动远端备份”。
2. 通过下拉框选择备份服务器。
3. 单击“确认”，启动远端备份。

----结束

相关操作

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

须知

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

6.1.2 配置远端备份

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。

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。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

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。

添加远端备份服务器

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤4 单击“防护目录设置”下的“设置”，进入防护目录设置页面。

步骤5 单击“管理远端备份服务器”，在弹出的对话框中，“添加远端备份服务器”，填写备份服务器信息，相关参数说明请参见**表6-2**。

表 6-2 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/f2ddbabc-6cdc-43af-abcd-e4e6f086626f”。 ● 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。

步骤6 单击“确认”，完成添加备份服务器的操作。

----结束

启动远端备份

步骤1 登录管理控制台。

步骤2 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤3 单击“防护目录设置”下的“设置”，进入防护目录设置页面。

步骤4 单击“启动远端备份”，在弹出的对话框中，选择远端备份服务器。

步骤5 单击“确认”，启动远端备份。

----结束

相关操作

关闭远端备份

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

6.1.3 添加特权进程

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

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

特权进程可以访问被防护的目录，请确保特权进程安全可靠。

约束限制

- 仅开启网页防篡改版防护后才支持防篡改相关操作。
- 仅X86架构且系统内核为4.18版本的操作系统支持该功能。
- Agent需要升级至3.2.4及以上版本特权进程才能生效。
- 每台服务器最多可添加10个特权进程。
- 仅支持Linux系统。

前提条件

在“主动防御 > 网页防篡改 > 防护配置”页面中“防护状态”为“防护中”。

添加特权进程

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤4 单击“特权进程设置”下的“设置”，进入特权进程“设置”页面。

步骤5 在“特权进程设置”页面，单击“添加特权进程”。

步骤6 在弹出的“添加特权进程”对话框中，添加特权进程文件所在的路径。

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

步骤7 特权进程添加完成后，单击“确定”，完成添加特权进程的操作。

----结束

相关操作

修改或删除已添加的特权进程

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

说明

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

6.1.4 定时开启/关闭静态网页防篡改

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。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

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

操作步骤

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤4 在“防护设置”页面，单击“定时开关设置”下的“设置”。

步骤5 进入定时开关设置页面，设置关闭防护时间段和自动关闭防护频率周期。

1. 单击“添加关闭时间段”，在弹窗中填写新增的关闭时间段信息。

   说明

   时间段规则：
   - 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. 确认无误单击“确认”，添加关闭时间段成功。
3. 勾选自动关闭防护的频率周期，勾选后在目标勾选的当日执行关闭防护。

   示例：勾选值为周一、周四、周六，则服务器在这些时间的关闭防护时间段自动关闭防篡改功能，关闭时间结束服务器自动启动静态网页防篡改。
4. 确认无误，单击“确认”，完成关闭防护频率周期设置。

步骤6 返回“防护设置”页面，在“定时开关设置”栏，单击开启定时开关，开启静态网页防篡改的定时开启和关闭策略。

----结束

6.1.5 开启动态网页防篡改

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

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

前提条件

主机为Linux操作系统。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“防护设置”，进入“防护设置”页面。

步骤4 进入“防护设置”页面，在“动态网页防篡改”栏，单击开启动态网页防篡改。

步骤5 在弹出的开启动态网页防篡改页面中，设置“Tomcat bin目录”。

开启动态网页防篡改需先设置Tomcat bin目录，系统会将setenv.sh脚本预置在bin目录中，用于设置防篡改程序的启动参数。开启动态网页防篡改之后需要重启Tomcat才能生效。

步骤6 单击“确认”，开启动态网页防篡改。

----结束

6.1.6 查看网页防篡改报告

开启网页防篡改防护后，企业主机安全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。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

前提条件

云服务器的“Agent状态”为“在线”且“防护状态”为“开启”。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护配置”页面，单击目标服务器“操作”列的“查看报告”。

步骤4 在查看报告界面，查看防护记录详情。

----结束

6.1.7 查看网页防篡改防护事件

开启静态网页防篡改防护后，企业主机安全将立即对您添加的防护目录执行全面的安全检测。您可以查看所有主机防护文件被非法篡改的记录。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

前提条件

- 云服务器的“Agent状态”为“在线”且“防护状态”为“开启”。
- 已开启网页防篡改。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在“主动防御 > 网页防篡改 > 防护事件”页面，查看主机防护文件被篡改记录。

----结束

6.2 勒索病毒防护

6.2.1 开启勒索病毒防护

勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机业务中断、数据泄露或丢失，主机所有者即使支付赎金也可能难以挽回所有损失，因此勒索病毒是当今网络安全面临的最大挑战之一。企业主机安全支持静态、动态勒索病毒防护，定期备份主机数据，可以帮助您抵御勒索病毒，降低业务损失风险。

前提条件

- 已开启企业主机安全版本为旗舰版、网页防篡改版或容器安全版。

约束限制

- 仅旗舰版、网页防篡改版、容器版支持勒索病毒防护功能。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 勒索病毒防护 > 防护服务器 ”，单击“为服务器开启防护”。

步骤4 在弹出的对话框中选择需要防护的目标系统并配置防护策略。

- 服务器操作系统：选择需要防护的服务器系统。
- 勒索防护：开启或关闭勒索防护。
  - 开启：
  - 关闭：
- 防护策略：选择已有策略或新建防护策略。
  - 选择已有策略：选择已有的防护策略，参数说明请参见**表 选择已有策略参数说明**。

    表 6-3 选择已有策略参数说明

参数名称	参数说明
选择防护策略	选择已有的防护策略。
防护动作	当前选择的防护策略支持的勒索病毒事件处理方式。 ■ 告警并自动隔离 ■ 告警
诱饵防护	开启诱饵防护后，系统会在防护目录和关键目录（不包括排除目录）中部署诱饵文件。诱饵文件会占用小部分服务器资源，不会影响您的服务器正常运行。 在开启服务器的勒索病毒防护时，诱饵防护状态为默认开启。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。

  - 新建防护策略：在当前页面新建一条防护策略，参数说明请参见**表 新建防护策略参数说明**。

表 6-4 防护策略参数说明

参数名称	参数说明	取值样例
防护策略名称	设置防护策略的名称。	test
防护动作	发现勒索病毒事件后的处理方式。 ■ 告警并自动隔离 ■ 告警	告警并自动隔离
诱饵防护	开启诱饵防护后，系统会在防护目录和关键目录（不包括排除目录）中部署诱饵文件。诱饵文件会占用小部分服务器资源，不会影响您的服务器正常运行。 在开启服务器的勒索病毒防护时，诱饵防护状态为默认开启。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	被防护的目录（不包括子目录）。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc/lesuo Windows：C:\Test
排除目录（选填）	不进行部署诱饵文件的目录。 多个目录请用英文分号隔开，最多支持填写20个排除目录。	Linux：/test Windows：C:\ProData
防护文件类型	被防护的服务器文件类型或格式，自定义勾选即可。 涵盖数据库、容器、代码、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选

步骤5 配置完成，单击“下一步”，进入服务器选择页面，通过分组筛选或服务器名称搜索目标服务器，勾选目标服务器。

步骤6 确认无误，单击“确认”，开启服务器勒索防护。

步骤7 左侧导航树选择“主动防御 > 勒索病毒防护 ”，选择“防护服务器”页签，查看已开启勒索防护的服务器。

----结束

6.2.2 查看勒索病毒防护

开启勒索病毒防护功能后，当服务器发生勒索攻击防护事件时，防护事件会被记录并展示在勒索病毒防护事件列表中供您查看分析，您可以结合自身业务情况处理防护事件。

前提条件

已开启企业主机安全版本为旗舰版、网页防篡改版或容器安全版。

约束限制

- 开启勒索病毒防护后需要及时处置勒索病毒告警、修复系统及中间件漏洞。

勒索病毒防护概览

步骤1 登录管理控制台。

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

步骤3 在导航树选择“主动防御 > 勒索病毒防护”，查看勒索防护详情。

表 6-5 勒索病毒概览参数

参数名称		参数说明	取值样例
时间范围		选择目标时间周期查看勒索病毒防护的检测情况和统计数据。 取值范围：“最近24小时”、“最近3天”、“最近7天”、“最近30天”。	“最近30天”
防护统计	已防护服务器	已开启勒索病毒防护的服务器总数。	-
	防护事件	所选时间范围内勒索病毒防护检测发现的事件总数。	-
防护服务器	服务器名称/ID	服务器的名称和ID，单击服务器名称可查看服务的详情。	-
	IP地址	防护服务器的弹性公网IP和私有IP。	-
	操作系统	服务器所属的操作系统。	Linux
	服务器状态	服务器当前状态。 ● 运行中 ● 关机	-

参数名称		参数说明	取值样例
	勒索防护状态	目标服务器的勒索防护状态。 ● 开启中：目标服务器正在开启勒索防护。 ● 已开启：目标服务器已开启勒索防护。 ● 关闭中：目标服务器勒索防护正在关闭。 ● 未开启：目标服务器未开启勒索防护，单击“立即开启”可开启勒索防护。	已开启
	防护策略	该服务器使用的防护策略名称。	-
	防护事件	所选时间范围内已检测防护到的事件数量。	-
防护策略	防护策略名称	防护策略的名称。	-
	防护动作	策略的防护机制。 ● 告警：发现病毒，仅产生告警事件。 ● 告警并自动隔离：发现病毒，产生告警事件的同时系统自动隔离发现的病毒。	告警并自动隔离
	诱饵防护	在服务器中存放无效数据的文件和目录，作为预防被攻击后访问的目录和文件。 在开启服务器的勒索病毒防护时，诱饵防护会默认开启。 开启诱饵防护后，系统会在防护目录和关键目录（不包括排除目录）中部署诱饵文件。诱饵文件会占用小部分服务器资源，不会影响您服务器的正常运行。	开启
	操作系统	目标策略绑定服务器的操作系统。	Windows
	关联服务器数	目标防护策略被关联的服务器数量。	-

----结束

6.2.3 防护策略管理

须知

目前勒索病毒防护策略的新建必须通过开启防护的流程才能创建。

约束限制

仅旗舰版、网页防篡改版、容器版支持勒索病毒防护功能。

新建防护策略

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 勒索病毒防护 > 防护服务器 ”，单击“为服务器开启防护”。

步骤4 在弹出的对话框选择Linux或Windows系统，开启勒索防护，“防护策略”选择“新建防护策略”，参数说明如表6-6所示。

以下以linux为示例。

表 6-6 防护策略参数说明

参数名称	参数说明	取值样例
防护策略名称	设置防护策略的名称。	test
防护动作	发现勒索病毒事件后的处理方式。 • 告警并自动隔离 • 告警	告警并自动隔离
诱饵防护	开启诱饵防护后，系统会在防护目录和关键目录（不包括排除目录）中部署诱饵文件。诱饵文件会占用小部分服务器资源，不会影响您的服务器正常运行。 在开启服务器的勒索病毒防护时，诱饵防护状态为默认开启。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	被防护的目录（不包括子目录）。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc/lesuo Windows：C:\Test

参数名称	参数说明	取值样例
排除目录（选填）	不进行部署诱饵文件的目录。 多个目录请用英文分号隔开，最多支持填写20个排除目录。	Linux：/test Windows：C:\ProData
防护文件类型	被防护的服务器文件类型或格式，自定义勾选即可。 涵盖数据库、容器、代码、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选

步骤5 配置完成，单击“下一步”，进入服务器选择页面，通过分组筛选或服务器名称搜索目标服务器，勾选目标服务器。

步骤6 确认无误，单击“确认”，开启服务器勒索防护，同时防护策略创建成功。

步骤7 左侧导航树选择“主动防御 > 勒索病毒防护 ”，选择“防护策略”页签，查看已创建的防护策略。

----结束

修改防护策略

步骤1 登录管理控制台，进入企业主机安全界面。

步骤2 选择“主动防御 > 勒索病毒防护 > 防护策略 ”。

步骤3 单击目标防护策略操作列的“编辑”，弹出防护策略编辑页面，对策略信息和关联服务器进行编辑，参数说明如**表 防护策略参数说明**所示。

以下以Linux为例。您也可以在“防护服务器”页面，单击服务器关联的防护策略名称，编辑防护策略。

表 6-7 防护策略参数说明

参数名称	参数说明	取值样例
防护策略名称	设置防护策略的名称。	test
防护动作	发现勒索病毒事件后的处理方式。 • 告警并自动隔离 • 告警	告警并自动隔离

参数名称	参数说明	取值样例
诱饵防护	开启诱饵防护后，系统会在防护目录和关键目录（不包括排除目录）中部署诱饵文件。诱饵文件会占用小部分服务器资源，不会影响您的服务器正常运行。 在开启服务器的勒索病毒防护时，诱饵防护状态为默认开启。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	被防护的目录（不包括子目录）。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc/lesuo Windows：C:\Test
排除目录（选填）	不进行部署诱饵文件的目录。 多个目录请用英文分号隔开，最多支持填写20个排除目录。	Linux：/test Windows：C:\ProData
防护文件类型	被防护的服务器文件类型或格式，自定义勾选即可。 涵盖数据库、容器、代码、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选

步骤4 确认信息无误，单击“确认”，完成防护策略修改。

----结束

删除防护策略

步骤1 登录管理控制台，进入企业主机安全界面。

步骤2 选择“主动防御 > 勒索病毒防护 > 防护策略 ”。

步骤3 单击目标策略“操作”列的“删除”。

步骤4 在弹窗确认正在删除的策略信息，确认无误，单击“确认”，完成删除。

----结束

6.2.4 关闭勒索病毒防护

操作场景

如果您不需要再为服务器进行勒索病毒防护，您可以关闭勒索病毒防护。关闭防护后，您的服务器将会面临被勒索病毒入侵的风险，请谨慎操作！

关闭勒索病毒防护

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 勒索病毒防护 > 防护服务器 ”。

步骤4 单击目标服务器“操作”列的“更多 > 关闭防护”。

步骤5 确认关闭信息无误，单击“确认”，完成关闭。

----结束

6.3 文件完整性管理

通过本章节操作可指导您查看云服务器文件变更总览和变更详情，包括变更的服务器、类型、路径、内容等信息。

6.3.1 查看文件完整性管理

检查Linux系统、应用程序软件和其他组件的文件，帮助您及时发现发生可能遭受攻击的更改。

约束限制

仅旗舰版、网页防篡改版、容器版支持文件完整性相关操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 文件完整性管理”，进入文件管理界面，选择“云服务器”和“变更文件”页签可查看对应的变更详情。

----结束

6.3.2 查看云服务器变更详情

约束限制

仅旗舰版、网页防篡改版、容器版支持文件完整性相关操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“主动防御 > 文件完整性管理”，进入文件管理界面。

步骤4 选择“云服务器”和“变更文件”页签可查看对应的变更详情。

步骤5 单击服务器名称进入服务器变更详情页。

表 6-8 变更参数说明

参数名称	参数说明	取值样例
文件	发现变更的文件名称。	du
路径	发现变更文件所在的路径。	-
变更内容	变更的情况描述。 鼠标放置变更内容可查看详情。	将SHA2560ba0c4b5e48e55a6改为4f6079f5b37d1513
变更类型	变更的文件类型。 • 文件	文件
变更类别	变更文件的类别。 • 新增 • 修改 • 删除	修改
变更时间	目标文件最后一次发生变更的时间。	-

----结束

6.3.3 查看历史变更文件

约束限制

仅旗舰版、网页防篡改版、容器版支持文件完整性相关操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 左侧选择“主动防御 > 文件完整性管理 > 变更文件”，进入变更文件页面，查看所有文件变更记录，企业项目可默认，参数可参见**查看云服务器变更详情**章节中的**表6-8**。

----结束

6.4 容器防火墙

6.4.1 容器防火墙概述

容器防火墙是一种为容器环境提供的防火墙服务，支持对容器集群内部与外部的网络流量进行控制和拦截，防止恶意访问和攻击。

版本限制

仅HSS容器版支持该功能。

容器防火墙原理

容器防火墙通过为容器中的Pod、服务器设置网络流量访问策略，限制源容器访问目的容器的范围或目的容器访问源容器的范围，从而达到防止来自内部和外部恶意访问或攻击的目的。

防护集群类型

用户在云容器引擎（Cloud Container Engine，简称CCE）服务中申请的集群，简称CCE集群。

相关操作

- 创建防御策略（容器隧道网络模型集群）
- 创建防御策略（VPC网络模型集群）

6.4.2 创建防御策略（容器隧道网络模型集群）

容器隧道网络模型的集群支持通过设置网络策略的方式限制访问Pod的流量。当未配置网络策略时，默认所有进出命名空间中的Pod的流量都被允许。

约束与限制

- 仅容器隧道网络模型的集群支持网络策略。网络策略分为以下规则
  - 入方向规则：所有CCE集群版本均支持。
  - 出方向规则：CCE集群版本大于或等于1.23时支持。
- 不支持对IPv6地址网络隔离。

通过 YAML 创建网络策略

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 单击容器隧道网络模型的集群所在行操作列的“策略管理”，进入策略管理页面。

步骤5 单击策略列表上方“YAML创建”。

步骤6 在YAML创建界面输入或单击“导入”数据。

以下为一个YAML创建的网络策略示例：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:                    #规则对具有role=db标签的Pod生效
    matchLabels:
      role: db
  policyTypes:
    - Ingress
    - Egress
  ingress:                        #表示入规则
    - from:
        - namespaceSelector:      #只允许具有project=myproject的命名空间访问
            matchLabels:
              project: myproject
        - podSelector:            #只允许具有role=frontend标签的Pod访问
            matchLabels:
              role: frontend
      ports                       #只允许使用TCP协议访问6379端口
        - protocol: TCP
          port: 6379
  egress:                         #表示出规则
    - to:
        - ipBlock:                #只允许访问目的对象的10.0.0.0/24网段。
            cidr: 10.0.0.0/24
      ports:                      #只允许使用TCP协议访问目的对象的6379端口
        - protocol: TCP
          port: 6379
```

步骤7 输入完成后，单击“确认”。

----结束

通过可视化界面创建网络策略

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 单击容器隧道网络模型的集群所在行操作列的“策略管理”，进入策略管理页面。

步骤5 单击网络策略列表上方“创建网络策略”。

- 策略名称：自定义输入网络策略名称。
- 命名空间：选择网络策略所在命名空间。
- 选择器：输入标签键和标签值选择要关联的Pod，然后单击“确认添加”。您也可以单击“引用负载标签”直接引用已有负载的标签。不选择时，默认关联命名空间下的全部Pod。
- 入方向规则：单击添加规则，添加入方向规则，参数说明请参见**表 添加入方向规则**。

表 6-9 添加入方向规则

参数	参数说明
协议端口	填写需要关联的Pod的入方向协议类型和端口，目前支持TCP和UDP协议。不填写表示全部放通。
源对象命名空间	选择允许哪个命名空间的对象访问。不填写表示和当前策略属于同一命名空间。
源对象Pod标签	允许带有这个标签的Pod访问，不填写表示允许命名空间下全部Pod访问。

- 出方向规则：单击添加规则，添加出方向规则，参数说明请参见**表 添加出方向规则**。

表 6-10 添加出方向规则

参数	参数说明
协议端口	填写目的对象的端口和协议。不填写表示不限制。
目标网段	允许将流量转发至指定的一个网段内（可指定多个例外网段）。 指定网段和例外网段用竖线（|）分隔，多个例外网段用逗号（,）分隔。 例如：172.17.0.0/16|172.17.1.0/24,172.17.2.0/24 表示允许访问 172.17.0.0/16 网段，其中 172.17.1.0/24 和 172.17.2.0/24 两个网段例外。
目的对象命名空间	目的对象所在的命名空间，不填写表示和当前策略属于同一命名空间。
目的对象Pod标签	允许访问带有这个标签的Pod，不填写表示允许访问命名空间下全部Pod。

步骤6 设置完成后，单击“确定”。

----结束

相关操作

同步CCE网络策略

支持同步在CCE中创建的网络策略至HSS。

步骤1 单击网络策略列表上方“手动同步”。

步骤2 “最近同步时间”更新为最新同步任务完成时间，表示同步完成。

----结束

6.4.3 创建防御策略（VPC 网络模型集群）

VPC网络模型的集群支持通过配置安全组规则的方式限制访问容器所属服务器的流量。当未配置安全组规则时，默认所有进出容器所属服务器的流量都被允许。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 在目标VPC网络模型的集群所在行的“操作”列，单击“策略管理”，进入策略管理页面。

步骤5 在目标节点所在行的“操作”列，单击“配置策略”。

步骤6 在弹出的对话框中单击“确认”，跳转到ECS服务器详情页面。

步骤7 选择“安全组”页签，查看安全组规则。

步骤8 单击安全组ID，系统自动跳转到安全组页面。

步骤9 根据界面提示设置入方向规则和出方向规则。

详细操作请参见《虚拟私有云用户指南》中“添加安全组规则”章节。

----结束

6.4.4 管理防御策略（容器隧道网络模型集群）

容器隧道网络模型的集群防御策略创建完成后，您可以参考本章节修改防御策略或删除不需要的防御策略。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 在目标容器隧道网络模型的集群所在行的“操作”列，单击“策略管理”，进入策略管理页面。

步骤5 单击网络策略列表上方“手动同步”。

步骤6 “最近同步时间”更新为最新同步任务完成时间，表示同步完成。

步骤7 定位目标网络策略，选择执行管理操作。

- 修改网络策略
  - 在目标策略所在行的“操作”列，单击“编辑YAML”，进入YAML界面，修改YAML信息后，单击“确认”。

  - 在目标策略所在行的“操作”列，单击“更新”，进入更新网络策略界面，修改网络策略信息后，单击“确认”。
- 删除网络策略
  - 在目标策略所在行的“操作”列，单击“删除”，在弹出的确认信息框中，单击“确认”。
  - 勾选所有需要删除的网络策略，单击网络策略列表上方的“批量删除”，在弹出的确认信息框中，单击“确认”。

----结束

6.4.5 管理防御策略（VPC 网络模型集群）

VPC网络模型的集群防御策略创建完成后，您可以参考本章节修改防御策略或删除不需要的防御策略。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 在目标VPC网络模型的集群所在行的“操作”列，单击“策略管理”，进入策略管理页面。

步骤5 单击节点列表上方的“手动同步”，同步节点信息。

步骤6 “最近同步时间”更新为最新同步任务完成时间，表示同步完成。

步骤7 在目标节点所在行的“操作”列，单击“配置策略”。

步骤8 在弹出的对话框中单击“确认”，跳转到ECS服务器详情页面。

步骤9 选择“安全组”页签，查看安全组规则。

步骤10 单击安全组ID，系统自动跳转到安全组页面。

----结束

7 入侵检测

7.1 安全告警事件

7.1.1 主机安全告警

7.1.1.1 主机安全告警事件概述

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。

约束限制

未开启防护不支持告警事件相关操作。

主机告警事件支持情况说明

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
恶意软件	未分类恶意软件	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，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。	×	√	√	√	Linux、Windows	√	√
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。	×	√	√	√	Linux	√	×
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。	×	×	√	√	Linux、Windows	√	√（部分支持）
	Webshell	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。 您可以在“策略管理”的“Webshell检测”中配置Webshell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。 该告警需要您在策略管理中添加防护目录，添加详情请参见**Webshell检测**。	×	√	√	√	Linux、Windows	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
漏洞利用	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	Linux	√	×
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	Linux	√	×
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	Linux	√	×
系统异常行为	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。 您可以在“策略管理”的“恶意文件检测”策略中配置反弹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。	×	√	√	√	Linux	√	×
	文件提权	检测当前系统对文件的提权行为并进行告警。	×	√	√	√	Linux	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
	进程提权	检测以下进程提权操作并进行告警： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。	×	√	√	√	Linux	√	×
	关键文件变更	实时监控系统关键文件（例如：ls、ps、login、top等），对修改文件内容的操作进行告警，提醒用户关键文件可能被篡改。监控的关键文件的路径请参见**关键文件变更监控路径**。 对于关键文件变更，HSS只检测文件内容是否被修改，不关注是人为还是进程进行的修改。	×	√	√	√	Linux	√	×
	文件/目录变更	实时监控系统文件/目录，对创建、删除、移动、修改属性或修改内容的操作进行告警，提醒用户文件/目录可能被篡改。	×	√	√	√	Linux、Windows	√	×
	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。	×	√	√	√	Linux、Windows	√	×（部分支持）
	高危命令执行	您可以在“策略管理 > 实时进程”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。	×	√	√	√	Linux、Windows	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
	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、复制、硬链接、访问权限变化。 您可以在“策略管理”的“恶意文件检测”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。	×	√	√	√	Linux	√	×
	Crontab可疑任务	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。 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。	×	×	√	√	Linux、Windows	√	×
	系统安全防护被禁用	检测勒索软件加密前准备动作：通过注册表关闭 Windows Defender 实时保护功能，一旦发现立即上报告警。	×	√	√	√	Windows	√	×
	备份删除	检测勒索软件加密前准备动作：删除备份格式文件或Backup文件夹下的文件，一旦发现立即上报告警。	×	√	√	√	Windows	√	×
	异常注册表操作	检测通过注册表关闭系统防火墙、勒索病毒Stop修改注册表并写入特定字符串等操作，一旦发现立即上报告警。	×	√	√	√	Windows	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
	系统日志删除	检测到通过命令或工具清除系统日志的操作时进行告警。	×	√	√	√	Windows	√	×
	可疑命令执行	● 检测通过命令或工具创建、删除计划任务或自启动任务。 ● 检测远程执行命令的可疑行为。	×	√	√	√	Windows	√	×
用户异常行为	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（连续输入错误密码）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。	√	√	√	√	Linux、Windows	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
	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。	√	√	√	√	Linux、Windows	√	×
	非法系统账号	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。	×	√	√	√	Linux、Windows	√	×
	用户密码窃取	检测主机中的系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。	×	√	√	√	Windows	√	×
网络异常访问	可疑的下载请求	检测到利用系统工具下载程序的可疑HTTP请求时进行告警。	×	√	√	√	Windows	√	×

事件类型	告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	隔离查杀
	可疑的HTTP请求	检测到利用系统工具或进程执行远程托管脚本的可疑HTTP请求时进行告警。	×	√	√	√	Windows	√	×
资源侦查	端口扫描	检测用户指定的端口存在被扫描或者嗅探的行为，一旦发现进行告警上报。	×	×	√	√	Linux	×	×

关键文件变更监控路径

类型	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

7.1.1.2 查看主机告警事件

您可自定义查询30天内发生的告警事件，您可以根据自己的业务需求，自行判断并处理告警，快速清除资产中的安全威胁。

告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

约束与限制

- 若不需要检测高危命令执行、提权操作、反弹Shell、异常Shell或者Webshell，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。
- 未开启防护的服务器不支持告警事件相关操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，单击“入侵检测 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

表 7-1 安全告警统计说明

参数名称		告警事件状态说明
时间范围		支持选择固定周期，支持自定义查询告警的时间范围，自定义只能选择30天范围内的查询。 固定周期可选择如下： ● 最近24小时 ● 最近3天 ● 最近7天 ● 最近30天
主机安全告警	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。
	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。

参数名称		告警事件状态说明
	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”、“登录类型”、“拦截状态”、“拦截次数”、“开始拦截时间”、“最近拦截时间”。 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。 • 每种软件最多拦截10000个ip。 如果您的linux主机不支持ipset，mysql和vsftp最多拦截50个ip。 如果您的linux主机既不支持ipset不支持hosts.deny，ssh最多拦截50个ip。
	已隔离文件	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“主机安全告警”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**管理文件隔离箱**。
容器安全告警	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。
	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。
	威胁等级	将被告警按照不同等级进行统计。 • 致命 • 高危 • 中危 • 低危
	TOP5事件类型	展示数量最多的前五种告警类型及数量。

步骤4 单击事件类型中的告警事件，可查看告警事件对应的受影响的服务器、发生时间等信息。

- 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。

步骤5 单击事件类型的告警名称，可查看告警的详细信息。

----结束

7.1.1.3 处理主机告警事件

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

告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

约束与限制

- 若不需要检测高危命令执行、提权操作、反弹Shell、异常Shell或者Webshell，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。
- 未开启防护的服务器不支持告警事件相关操作。

操作步骤

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

说明

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

步骤1 登录管理控制台。

步骤2 在页面左上角单击三，选择“区域”，选择“安全 > 企业主机安全”，进入“企业主机安全”页面。

步骤3 在左侧导航栏中，单击“入侵检测 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

表 7-2 安全告警统计说明

参数名称		告警事件状态说明
时间范围		支持选择固定周期，支持自定义查询告警的时间范围，自定义只能选择30天范围内的查询。 固定周期可选择如下： • 最近24小时 • 最近3天 • 最近7天 • 最近30天
主机安全告警	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。

参数名称		告警事件状态说明
	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”、“登录类型”、“拦截状态”、“拦截次数”、“开始拦截时间”、“最近拦截时间”。 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。 • 每种软件最多拦截10000个ip。 如果您的linux主机不支持ipset，mysql和vsftp最多拦截50个ip。 如果您的linux主机既不支持ipset不支持hosts.deny，ssh最多拦截50个ip。
	已隔离文件	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“主机安全告警”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**管理文件隔离箱**。
容器安全告警	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。
	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。
	威胁等级	将被告警按照不同等级进行统计。 • 致命 • 高危 • 中危 • 低危
	TOP5事件类型	展示数量最多的前五种告警类型及数量。

步骤4 处理告警事件。

说明

告警事件展示在“主机安全告警”页面中，事件列表仅展示最近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。

- 处理全量告警
  a. 通过“事件类型”选中需要全量处理的告警项，单击“事件列表”下方的“全量处理”。

     说明

     全量处理前务必选择至最小的告警事件类别，否则“全量处理”按钮无法单击。

  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成全量告警处理，处理方式详情如**表7-3**所示。

     说明

     批量处理后的告警无法进行二次批量处理，若需二次处理告警事件，只能逐条处理。

- 批量处理告警
  a. 任意选中“事件类型”，在事件列表勾选多个目标告警，单击“事件列表”下方的“批量处理”。
  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成勾选告警处理，处理方式详情如**表7-3**所示。
- 处理单个告警
  a. 选中目标“事件类型”，单击目标告警事件“操作”类的“处理”。
  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成单个告警处理，处理方式详情如**表7-3**所示。

表 7-3 告警事件处理方式说明

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**管理文件隔离箱**。 对应告警事件支持隔离查杀的情况详情请参见**主机安全告警事件概述**。 **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。
手动处理	选择手动处理。您可以根据自己的需要为该事件添加“备注”信息，方便您记录手动处理该告警事件的详细信息。

处理方式	处理方式说明
加入登录白名单	如果确认“暴力破解”和“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。 有以下告警事件支持加入登录白名单。 ● 暴力破解 ● 异常登录
加入告警白名单	如果确认告警事件是误报，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。 对应告警事件支持隔离查杀的情况详情请参见**主机安全告警事件概述**。

----结束

7.1.1.4 导出主机告警事件

本章节为您介绍如何将主机安全告警事件导出到本地进行查看。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“入侵检测 > 安全告警事件”，进入“安全告警事件”页面。

步骤4 选择“主机告警事件”页签。

步骤5 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

----结束

7.1.1.5 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“主机安全告警”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。

对应告警事件支持隔离查杀的情况详情请参见**主机安全告警事件概述**。

约束限制

未开启防护不支持告警事件相关操作。

隔离查杀操作

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，单击“入侵检测 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

表 7-4 安全告警统计说明

参数名称		告警事件状态说明
时间范围		支持选择固定周期，支持自定义查询告警的时间范围，自定义只能选择30天范围内的查询。 固定周期可选择如下： ● 最近24小时 ● 最近3天 ● 最近7天 ● 最近30天
主机安全告警	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。
	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”、“登录类型”、“拦截状态”、“拦截次数”、“开始拦截时间”、“最近拦截时间”。 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。 ● 每种软件最多拦截10000个ip。 如果您的linux主机不支持ipset，mysql和vsftp最多拦截50个ip。 如果您的linux主机既不支持ipset不支持hosts.deny，ssh最多拦截50个ip。

参数名称		告警事件状态说明
	已隔离文件	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“主机安全告警”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**管理文件隔离箱**。
容器安全告警	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。
	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。
	威胁等级	将被告警按照不同等级进行统计。 • 致命 • 高危 • 中危 • 低危
	TOP5事件类型	展示数量最多的前五种告警类型及数量。

步骤4 单击支持隔离查杀的告警事件“操作”列的“处理”，选择“隔离查杀”。

说明

对应告警事件支持隔离查杀的情况详情请参见**主机安全告警事件概述**。

步骤5 单击“确认”，对目标告警事件进行隔离查杀。

被成功隔离的文件会添加到“主机安全告警”的“文件隔离箱”中，无法对主机造成威胁。

----结束

查看文件隔离箱

步骤1 在“主机安全告警”页面的“安全告警统计”中，单击“已隔离文件”下方的“查看详情”，进入“文件隔离箱”页面。

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

----结束

一键恢复

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

步骤2 单击“确认”，恢复的文件将重新回到告警事件列表中。

说明

执行恢复操作会将隔离文件查杀恢复，请谨慎操作。

----结束

7.1.2 容器安全告警

7.1.2.1 容器安全告警事件概述

开启节点防护后，部署在每个容器宿主机上的Agent会对容器运行状态进行实时监控，支持逃逸检测、高危系统调用、异常进程检测、文件异常检测、容器环境等检测。用户可通过容器安全告警全面了解告警事件类型，及时发现资产中的安全威胁、实时掌握资产的安全状态。

约束限制

- 仅HSS容器版支持容器安全告警功能。
- 仅支持对Docker容器进行入侵检测告警。

告警事件列表说明

事件类型	告警名称	原理说明
恶意软件	未分类恶意软件	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出容器中未知的恶意程序和病毒变种。
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。
	Webshell	检测容器中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。
漏洞利用	漏洞逃逸攻击	HSS监控到容器内进程行为符合已知漏洞的行为特征时（例如：“脏牛”、“bruteforce”、“runc”、“shocker”等），触发逃逸漏洞攻击告警
	文件逃逸攻击	HSS监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，HSS仍然会触发告警。

事件类型	告警名称	原理说明
系统异常行为	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。 您可以在“策略管理”的“恶意文件检测”策略中配置反弹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。
	进程提权	当黑客成功入侵容器后，会尝试利用漏洞进行root提权或者文件提权，从而达到非法创建和修改系统账号的权限或者篡改文件的目的。 HSS支持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。
	高危系统调用	Linux系统调用是用户进程进入内核执行任务的请求通道。CGS监控容器进程，如果发现进程使用了危险系统调用（例如：“open_by_handle_at”、“ptrace”、“setns”、“reboot”等），触发高危系统调用告警。
	高危命令执行	实时检测容器系统中执行的高危命令，当发生高危命令执行时触发告警。
	容器进程异常	● 容器恶意程序 HSS监控容器内启动的容器进程的行为特征和进程文件指纹，如果特征与已定义的恶意程序吻合则触发容器恶意程序告警。 ● 容器异常进程 容器业务通常比较单一。如果用户能够确定容器内只会运行某些特定进程，可以在“策略管理”设置“容器进程白名单”并将策略关联容器镜像。 对于已关联的容器镜像启动的容器，HSS只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。
	敏感文件访问	HSS监控容器内已配置文件保护策略的容器镜像文件状态。如果发生文件修改事件则触发文件异常告警。

事件类型	告警名称	原理说明
	容器异常启动	HSS监控新启动的容器，对容器启动配置选项进行检测，当发现容器权限过高存在风险时触发告警。容器环境检测触发的告警只是提醒容器启动风险，并不是发生实际攻击。如果黑客利用容器配置风险执行了真实攻击，仍然会触发HSS容器安全的其他检测告警。 HSS支持以下容器环境检测： ● 禁止启动特权容器(privileged:true) 特权容器是指容器以最大权限启动，类似于操作系统的root权限，拥有最大能力。docker run启动容器时携带“ –privileged=true”参数，或者kubernates POD配置中容器的“securityContext”配置了“privileged:true”，此时容器会以特权容器方式启动。 告警名称为“容器安全选项”，告警内容中提示“privileged:true”，表示该容器以特权容器模式启动。 ● 需要限制容器能力集（capabilities:[xxx]） Linux系统将系统权限做了分类，通过授予特定的权限集合，能控制容器进程的操作范围，避免出现严重问题。容器启动时默认开启了一些常用能力，通过修改启动配置可以放开所有系统权限。 告警名称为“容器安全选项”，告警内容中提示“capabilities:[xxx]”，表示该容器启动时拥有所有能力集过大，存在风险。 ● 建议启用seccomp（seccomp=unconfined） Seccomp(secure computing mode)是Linux的一种内核特性，用于限制进程能够调用的系统调用，减少内核的攻击面。如果容器启动时设置“seccomp=unconfined”，将不会对容器内的系统调用执行限制。 告警名称“容器安全选项”，告警内容中提示“seccomp=unconfined”，表示该容器启动时没有启动seccomp，存在风险。 **说明** 启用seccomp后，由于每次系统调用Linux内核都需要执行权限校验，如果容器业务场景会频繁使用系统调用，开启seccomp对性能会有一定影响。具体影响建议在实际业务场景测试分析。 ● 限制容器获取新的权限(no-new-privileges:false) 进程可以通过程序的suid位或者sgid位获取附加权限，通过sudo提权执行更高权限的操作。容器默认配置限制不允许进行权限提升。 如果容器启动时指定了“ –no-new-privileges=false”，则该容器拥有权限提升的能力。 告警名称为“容器安全选项”，告警内容中提示“no-new-privileges:false”，表示该容器关闭了提权限制，存在风险。 ● 危险目录映射(mounts:[...]) 容器启动时可以将宿主机目录映射到容器内，方便容器内业务直接读写宿主机上的资源。这是一种存在风险的使用

事件类型	告警名称	原理说明
		方式，如果容器启动时映射了宿主机操作系统关键目录，容易造成从容器内破坏宿主机系统的事件。 HSS监控到容器启动时mount了宿主机危险路径时触发告警，定义的宿主机危险目录包括：“/boot”，“/dev”，“/etc”，“/sys”，“/var/run”等。 告警名称为“容器挂载目录”，告警内容中提示“mounts:[{"source":"xxx","destination":"yyy"...]”，表示该容器映射的文件路径存在风险，需要按照告警中的目录映射关系排查是否存在危险的映射，可以将认为安全的挂载路径配置到容器信息收集的策略中。 **说明** 对于docker容器常用的需要访问的宿主文件如“/etc/hosts”、“/etc/resolv.conf”不会触发告警。 ● 禁止启动命名空间为host的容器 容器的命名空间需要与主机隔离开，如果容器配置了与主机相同的命名空间，则该容器可以访问并修改主机上的内容，易造成容器逃逸的安全事件，存在安全风险。因此HSS会检测容器的pid，network，ipc命名空间是否为host。 告警名称为“容器命名空间”，告警内容中提示“容器pid命名空间模式”、“容器ipc命名空间模式”、“容器网络命名空间模式”，表示启动了命名空间为host的容器，需要按照告警中的提示排查容器的启动选项，如果存在业务需要，可以将该告警事件忽略。
	容器镜像阻断	在Docker环境中容器启动前，HSS检测到**镜像异常行为策略**中指定的不安全容器镜像运行时触发告警。
用户异常行为	非法系统用户账号	黑客可能通过风险账号入侵容器，以达到控制容器的目的，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。
	暴力破解	检测容器场景下“尝试暴力破解”和“暴力破解成功”等暴破异常行为，发现暴破行为时触发告警。 支持检测容器场景下SSH、Web和Enumdb暴破行为。 **说明** 目前暂仅支持Docker容器运行时的暴力破解检测告警。

关键文件变更监控路径

类型	Linux
bin	/bin/ls /bin/ps /bin/bash /bin/login
usr	/usr/bin/ls /usr/bin/ps /usr/bin/bash /usr/bin/login /usr/bin/passwd /usr/bin/top /usr/bin/killall /usr/bin/ssh /usr/bin/wget /usr/bin/curl

7.1.2.2 查看容器告警事件

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容器、待处理告警事件、已处理告警事件。

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

告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

约束限制

未开启防护的服务器不支持告警事件相关操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中选择“入侵检测 > 安全告警事件 > 容器安全告警”，进入“容器安全告警”页面，查看容器告警事件信息。

- 查看容器告警事件概览。
  - 安全告警统计：您可以查看存在告警的容器数量，以及待处理和已处理告警事件数量。
  - 威胁等级：您可以查看容器存在的告警等级分布数量。

- 查看容器告警事件分类列表。

  在“事件类型”栏，选择告警事件类型，查看每个事件类型对应的告警事件列表。在告警事件列表中可以查看告警威胁等级、告警名称、受影响容器实例名称、容器状态、POD名称等信息。

- 查看容器告警事件详细信息。

  单击目标告警事件的告警名称，进入告警事件详情页面，可以查看容器ID、IP地址、虚拟机名称、镜像ID等信息。

----结束

7.1.2.3 处理容器告警事件

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

告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

约束限制

未开启防护的服务器不支持告警事件相关操作。

操作步骤

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

说明

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

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，单击“入侵检测 > 安全告警事件 > 容器安全告警”，进入“容器安全告警”页面。

表 7-5 安全告警统计说明

告警事件状态	告警事件状态说明
存在告警的服务器	展示存在告警容器的数量。
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。
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。

步骤4 处理告警事件。

说明

告警事件展示在“容器安全告警”页面中，事件列表仅展示最近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。

- 批量处理全量告警
  a. 通过“事件类型”选中需要全量处理的告警项，单击“事件列表”下方的“全量处理”。
  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成全量告警处理，处理方式详情如表7-6所示。

  说明

  批量处理后的告警无法进行二次批量处理，若需二次处理告警事件，只能逐条处理。
- 批量处理勾选的告警
  a. 任意选中“事件类型”，在事件列表勾选多个目标告警，单击“事件列表”下方的“批量处理”。
  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成勾选告警处理，处理方式详情如表7-6所示。
- 处理单个告警
  a. 选中目标“事件类型”，单击目标告警事件“操作”类的“处理”。
  b. 在弹窗中选择处理方式，确认无误，单击“确认”，完成单个告警处理，处理方式详情如表7-6所示。

表 7-6 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。
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。

----结束

7.1.2.4 导出容器告警事件

本章节为您介绍如何将容器安全告警事件导出到本地进行查看。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“入侵检测 > 安全告警事件”，进入“安全告警事件”页面。

步骤4 选择“容器告警事件”页签。

步骤5 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

----结束

7.2 白名单管理

7.2.1 管理登录白名单

通过配置目标服务器IP、登录端IP以及登录端用户名完成登录白名单添加，添加后HSS对白名单内IP、用户名的登录、访问行为进行忽略。

说明

- 配置的目标服务器IP、登录端IP以及登录端用户名需同时满足白名单配置的信息，检测时才会忽略。
- 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**查看主机告警事件**。

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**查看主机告警事件**。
- 在“登录白名单”页面，添加登录白名单。

约束限制

需开启旗舰版、网页防篡改版、容器版任一防护版本。

添加登录告警白名单

步骤1 登录管理控制台。

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

步骤3 选择“入侵检测 > 白名单管理 > 登录白名单”，进入“白名单管理”页面，单击“添加”。

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

表 7-7 登录安全白名单参数说明

参数名称	参数说明	取值样例
服务器IP	• 支持IPv4地址。 • 支持单个IP、IP范围、IP掩码，以英文逗号分隔。	• 192.168.1.1 • 192.168.2.1-192.168.6.1 • 192.168.7.0/24
登录IP		

参数名称	参数说明	取值样例
登录用户名	当前登录用户名。	hss_test
备注	可自定义目标白名单说明。	测试

步骤5 单击“确认”，完成登录白名单的添加。

----结束

其他操作

删除登录白名单

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

7.2.2 管理告警白名单

白名单管理提供告警白名单的展示与删除功能，用户可以通过配置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“安全告警事件”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，后续主机安全平台不会再对该事件进行告警和统计。

约束限制

需开启旗舰版、网页防篡改版、容器版任一防护版本。

添加告警白名单

表 7-8 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 以下类型的告警事件加入“告警白名单”： • 反弹Shell • 勒索软件 • 恶意程序 • Webshell • 进程异常行为 • 进程提权 • 文件提权 • 高危命令执行 • 恶意软件 • 关键文件变更 • 文件/目录变更 • 异常Shell • Crontab可疑任务 • 非法系统账号 • 一般漏洞利用 • Redis漏洞利用 • Hadoop漏洞利用 • MySQL漏洞利用

查看告警白名单

加入告警白名单后，您可以查看已添加的告警白名单，操作步骤如下所示。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“入侵检测 > 白名单管理”，进入“白名单管理”页面。

步骤4 选择“告警白名单”页签，查看已添加的告警白名单列表，参数说明如表7-9所示。

表 7-9 告警白名单列表参数说明

参数名称	参数说明
告警类型	白名单的告警类型名称。

参数名称	参数说明
SHA256	目标文件哈希。
描述	目标白名单的说明。
标记时间	目标告警添加白名单的时间。

----结束

相关操作

删除告警白名单

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

说明

- 删除告警白名单后，若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！
- 删除告警白名单后，该告警白名单关联的告警事件不会联动更新处置状态，如果需要更改相关告警事件的处置状态，请前往“入侵检测 > 安全告警事件”页面，在告警事件所在行的操作列单击“处置”，选择“删除告警白名单”。

7.2.3 管理系统用户白名单

HSS会对主机新添加的root用户组权限用户（非root用户）进行“风险账号”告警。如果是您信任的用户，您可以将该用户添加到系统用户白名单，添加后，HSS将不再对其进行“风险账号”告警。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“入侵检测 > 白名单管理”，进入“白名单管理”页面。

步骤4 选择“系统用户白名单”页签，单击“添加”。

步骤5 在“添加系统用户白名单”弹窗中填写主机ID、系统用户名以及备注信息。

步骤6 单击“确认”，添加完成。

----结束

相关操作

修改系统用户白名单

步骤1 在需要修改的系统用户白名单所在行的“操作”列，单击“修改”。

步骤2 在“修改系统用户白名单”弹窗中完成信息修改后，单击“确认”。

----结束

删除系统用户白名单

步骤1 在需要删除的系统用户白名单所在行的“操作”列，单击“删除”。

当多个系统用户白名单需要删除时，您可以勾选所有目标系统用户白名单，在系统用户白名单列表左上角，单击“删除”。

步骤2 在弹出的窗口，单击“确认”。

----结束

8 安全运营

8.1 策略管理

8.1.1 查看策略组

企业主机安全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、主机、容器节点应用不同的策略，以满足不同应用场景的主机安全需求。

约束限制

需开启企业版、旗舰版、网页防篡改版、容器版中任一版本。

操作须知

- 开启企业版主机防护时，默认绑定“租户侧企业版策略组”（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”或者“网页防篡改赠送旗舰版”后，开启旗舰版/网页防篡改版防护时，默认绑定了“租户侧旗舰版策略组”。

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

策略列表

策略名称	策略说明	支持的操作系统	企业版	旗舰版	网页防篡改版	容器版
资产发现	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	×	√	√	√

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	容器版
AV检测	检测服务器资产，对发现的病毒进行上报、隔离查杀。 检测的告警结果将按照病毒类别在“入侵检测 > 安全告警事件 > 主机安全告警 > 事件类型 > 恶意软件”下的子类别中分别呈现。 开启AV检测后资源占用情况如下： CPU资源占用不超过单vCPUs的40%，实际占用情况需根据主机情况而定。	Windows	√	√	√	×
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	×	√	√	√
容器信息收集	收集主机中的所有容器相关信息，包括端口、目录等，对存在风险的信息进行告警上报。	Linux	×	×	×	√
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	√	√	√	√
集群入侵检测	检测容器高权限的变动，在关键信息中的创建及病毒入侵等异常行为。	Linux	×	×	×	√
容器逃逸	检测容器是否容器逃逸行为，存在容器逃逸行为即进行告警上报。	Linux	×	×	×	√
Webshell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	√	√	√	√
容器文件监控	检测违反安全策略的文件异常访问，安全运维人员可用于判断是否有黑客入侵并篡改敏感文件。	Linux	×	×	×	√
容器进程白名单	检测违反安全策略的进程启动。	Linux	×	×	×	√

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	容器版
镜像异常行为	配置目标黑白名单，自定义权限对异常行为进行忽略或告警上报。	Linux	×	×	×	√
HIPS检测	主要针对注册表、文件及进程进行检测，对异常变更等操作行为进行告警上报。	Windows	√	√	√	√
文件保护	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	√	√	√	√
登录安全检测	检测SSH、FTP、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（连续输入错误密码）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。	Linux，Windows	√	√	√	√
恶意文件检测	• 反弹shell：实时监控用户的进程行为，可及时发现并阻断进程的非法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、复制、硬链接、访问权限变化。	Linux	√	√	√	√
端口扫描检测	检测用户指定的端口存在被扫描或者嗅探的行为，一旦发现进行告警上报。	Linux	×	√	√	√

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	容器版
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。	Linux	×	√	√	√
root提权	检测当前系统文件路径的root提权行为。	Linux	√	√	√	√
实时进程	检测进程中高危命令的执行行为，发生高危命令执行时，触发告警。	Linux，Windows	√	√	√	√
rootkit检测	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。	Linux	√	√	√	√
自保护	保护企业主机安全的文件、进程、软件，防止恶意程序卸载企业主机安全Agent、篡改企业主机安全文件或停止企业主机安全进程。 • 自保护功能依赖AV检测、HIPS检测或者勒索病毒防护功能使能驱动才能生效，只有这三个功能开启一个以上时，开启自保护才会生效。 • 开启自保护策略后的影响如下： – 企业主机安全的Agent不支持通过主机的控制面板卸载，支持通过企业主机安全控制台卸载。 – 企业主机安全的进程无法被终止。 – Agent安装路径C:\Program Files\HostGuard下除了log目录、data目录（如果Agent升级过，再加上upgrade目录）外的其他目录无法访问。	Windows	×	√	√	×

查看策略组列表

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”界面，查看显示的策略组，字段说明如表8-1所示。

说明

- tenant_linux_container_default_policy_group：容器版linux系统预置策略，可通过复制该策略组来创建新的策略组。tenant_linux_enterprise_default_policy_group：企业版linux系统预置策略，仅可被查看，不可被复制和删除。
- tenant_windows_enterprise_default_policy_group：企业版windows系统预置策略，仅可被查看，不可被复制和删除。
- tenant_linux_premium_default_policy_group：旗舰版linux系统预置策略，可通过复制该策略组来创建新的策略组。
- tenant_windows_premium_default_policy_group：旗舰版windows系统预置策略，可通过复制该策略组来创建新的策略组。
- 可在列表右上角单击，手动刷新当前列表。
- 可单击关联服务器数的数量，查看策略组关联的服务器。

表 8-1 策略组列表字段说明

字段	说明
策略组名称	策略组的名称。
ID	策略组的ID号，对策略组的唯一标识。
描述	对策略组的描述。
支持的版本	策略组支持的企业主机安全的版本。
支持的操作系统	策略支持的操作系统类型。
关联服务器数	策略关联的服务器数。

步骤4 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。

说明

- “租户侧企业版策略组”中的所有策略默均为“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。

步骤5 单击策略名称，可以查看策略的详情。

说明

若需要修改或配置策略，请参见**编辑策略内容**。

----结束

8.1.2 创建策略组

您可根据自己服务器不同使用情况创建对应的策略组，创建后可对目标服务器进行更有力的扫描检测。

前提条件

已开启旗舰版。

说明

目前仅支持对旗舰版的策略组进行自定义创建，若没有开启旗舰版防护的主机，创建后不会生效。

创建策略组

以下以旗舰版的Linux策略为例。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”界面，查看显示的策略组，字段说明如表8-2所示。

说明

- tenant_linux_container_default_policy_group：容器版linux系统预置策略，可通过复制该策略组来创建新的策略组。tenant_linux_enterprise_default_policy_group：企业版linux系统预置策略，仅可被查看，不可被复制和删除。
- tenant_windows_enterprise_default_policy_group：企业版windows系统预置策略，仅可被查看，不可被复制和删除。
- tenant_linux_premium_default_policy_group：旗舰版linux系统预置策略，可通过复制该策略组来创建新的策略组。
- tenant_windows_premium_default_policy_group：旗舰版windows系统预置策略，可通过复制该策略组来创建新的策略组。
- 可在列表右上角单击，手动刷新当前列表。
- 可单击关联服务器数的数量，查看策略组关联的服务器。

表 8-2 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	策略组支持的的版本。
支持的操作系统	策略支持的操作系统类型。

字段	说明
关联服务器数	策略关联的服务器数。

步骤4 选择tenant_linux_premium_default_policy_group或tenant_windows_premium_default_policy_group策略组，单击该策略组“操作”列的“复制”。

以下以Linux策略组为例。

步骤5 在弹出的对话框中，输入“策略组名称”和“描述”。

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。

步骤6 单击“确认”，将会创建一个新的策略组。

步骤7 单击已创建的策略组名称，进入策略组的策略页面。

步骤8 单击策略名称，修改具体的策略内容，详细信息请参见**编辑策略内容**。

步骤9 策略内容修改完成后，单击策略所在行的“开启”或者“关闭”，开启或者关闭对应的策略。

----结束

相关操作

删除策略组

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

步骤1 进入“策略管理”列表界面，可对策略进行单项删除或批量删除。

说明

单项删除策略：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。

批量删除策略：勾选多个策略名称前的选框，单击上方的“删除”，删除多个策略组。

步骤2 在弹出对话框中，单击“确定”，完成策略组的删除。

----结束

8.1.3 编辑策略内容

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编辑。

须知

- 策略内容的修改，只在当前所修改的策略组生效。
- 默认策略组有默认配置，不建议修改。
- Windows的HIPS策略目前不支持修改。

约束限制

需开启企业版、旗舰版、网页防篡改版、容器版中任一版本。

进入策略管理

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”界面，查看显示的策略组，字段说明如表8-3所示。

说明

- tenant_linux_container_default_policy_group：容器版linux系统预置策略，可通过复制该策略组来创建新的策略组。tenant_linux_enterprise_default_policy_group：企业版linux系统预置策略，仅可被查看，不可被复制和删除。
- tenant_windows_enterprise_default_policy_group：企业版windows系统预置策略，仅可被查看，不可被复制和删除。
- tenant_linux_premium_default_policy_group：旗舰版linux系统预置策略，可通过复制该策略组来创建新的策略组。
- tenant_windows_premium_default_policy_group：旗舰版windows系统预置策略，可通过复制该策略组来创建新的策略组。
- 可在列表右上角单击，手动刷新当前列表。
- 可单击关联服务器数的数量，查看策略组关联的服务器。

表 8-3 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	策略组支持的的版本。
支持的操作系统	策略支持的操作系统类型。
关联服务器数	策略关联的服务器数。

步骤4 单击目标策略组名称，进入策略详情列表，单击策略名称对不同策略进行修改。

----结束

资产发现

步骤1 单击“资产发现”，弹出“资产发现”策略详情界面。

步骤2 在弹出的资产管理界面中，修改“策略内容”，参数说明如表8-4所示。

表 8-4 资产管理策略内容参数说明

参数名称	参数说明
检测时间	针对不同资产自动执行检测的固定时间点。 • 账号：Linux每小时自动检测一次，Windows实时检测。 • 开放端口：每30秒自动检测一次。 • 进程：每小时自动检测一次。 • 软件：每天自动检测一次。 • 自启动项：每小时自动检测一次。
需要获取信息的软件名称	• 软件名称中不能包含空格且内容长度不得超过5000字符，多个软件名称用逗号分隔。 • 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。
指定待扫描web目录	需要扫描的web目录。
web目录扫描深度	指定web目录扫描的层级深度。

步骤3 确认无误，单击“确认”，完成修改。

----结束

弱口令检测

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

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

步骤1 单击“弱口令检测”，弹出“弱口令检测”策略详情界面。

步骤2 在弹出的“策略内容”界面中，修改“策略内容”，参数说明如表8-5所示。

表 8-5 弱口令检测策略内容参数说明

参数	说明
检测时间	配置弱口令检测的时间，可具体到每一天的每一分钟。

参数	说明
随机偏移时间（秒）	检测配置的弱口令时间的随机偏移时间，在“检测时间”的基础上偏移，可配置范围为“0~7200秒”。
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。
检测休息时间(ms)	检测配置的单个账号的时间间隔，可配置范围为“0ms~2000ms”。 例如：配置为“50”，检测“/bin/ls”后，等待“50”毫秒再检测“/bin/ls”。
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。 填写多个弱口令时，每个弱口令之间需换行填写，最多可添加300条。

步骤3 确认无误，单击“确认”，完成修改。

----结束

配置检测

步骤1 单击“配置检测”，弹出“配置检测”策略详情界面。

步骤2 在“配置检测”界面，修改“策略内容”。

表 8-6 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。
随机偏移时间（秒）	配置系统检测的随机偏移时间，可配置范围为“0~7200秒”。
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。
系统默认基线库	系统已经配置好的检测基线，只需要勾选需要扫描检测的基线即可，所有值均为默认，不可修改。

步骤3 勾选需要检测的基线或自定义基线。

步骤4 确认无误，单击“确认”，完成修改。

----结束

Webshell 检测

如果未设置“用户指定扫描路径”，Webshell检测功能默认扫描您资产中的Web站点路径。设置“用户指定扫描路径”后，Webshell检测功能仅扫描您指定的路径。

步骤1 单击“Webshell检测”，弹出“Webshell检测”策略详情界面。

步骤2 在弹出的“Webshell检测”界面中，修改“策略内容”，参数说明如表8-7所示。

表 8-7 Webshell 检测策略内容参数说明

参数	说明
检测时间	配置Webshell检测的时间，可具体到每一天的每一分钟。
随机偏移时间（秒）	配置随机偏移时间，可配置范围为“0~7200秒”。
检测日	Webshell检测日期，勾选周一到周日的检测Webshell的时间。
用户指定扫描路径	手动添加需要检测的Web目录。 • 文件路径以“/”开头，不能以“/”结尾。 • 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”。

步骤3 确认无误，单击“确认”，完成修改。

----结束

文件保护

步骤1 单击“文件保护”，弹出“文件保护”策略详情界面。

步骤2 在弹出的文件保护界面中，修改“策略内容”，参数说明如表8-8所示。

表 8-8 文件保护策略内容参数说明

参数	说明
文件提权检测	• 启用：是否开启文件提权检测。 –  ：开启。 –  ：关闭。 • 忽略的文件路径：填写需要忽略的文件路径。文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。
关键文件完整性检测	• 启用：是否开启关键文件完整性检测。 –  ：开启。 –  ：关闭。 • 监控文件：配置监控文件。

参数	说明
关键文件目录变更检测	• 启用：是否开启关键文件目录变更检测。 –  ：开启。 –  ：关闭。 • 开启Audit：是否开启Audit检测功能，开启后，请注意系统的inotify使用限制，超过限制，部分文件目录变更将检测不到。 –  ：开启。 –  ：关闭。 • 会话IP白名单：如果操作文件的进程属于以上IP的会话，则不予审计。 • 忽略监控文件类型后缀：忽略监控的文件类型的后缀。 • 忽略监控的文件路径：配置忽略监控文件的路径。 • 监控登录密钥：是否开启监控登录密钥。 –  ：开启。 –  ：关闭。
文件目录监控	• 监控模式：监控文件或目录路径的模式。 • 文件或目录路径：系统预置了部分文件或目录监控路径，您可以自行修改需要检测的文件更改类型以及添加需要监控的文件或目录路径。

步骤3 确认无误，单击“确认”，完成修改。

----结束

登录安全检测

步骤1 单击“登录安全检测”，弹出“登录安全检测”策略详情界面。

步骤2 在弹出的“登录安全检测”策略内容中，修改“策略内容”，参数说明如所示。

表 8-9 登录安全检测策略内容参数说明

参数	说明
封禁时间（分钟）	可设置被阻断攻击IP的封禁时间，封禁时间内不可登录，封禁时间结束后自动解封，可配置范围为“1~43200”。
破解行为判断阈值（秒）	与“破解行为判断阈值（登录失败次数）”一起配置使用。可配置范围为“5~3600”。 例如：破解行为判断阈值“30”，破解行为判断阈值（登录失败次数）“5”，表示“30秒内同一IP发生5次登录失败会被判定为账户爆破行为。”

参数	说明
破解行为判断阈值（登录失败次数）	与破解行为判断阈值一起配置使用，可配置范围为“1~36000”。
慢破解行为判断阈值（秒）	与慢破解行为判断阈值（登录失败次数）一起配置使用。可配置范围为“600~86400”。 例如：慢破解行为判断阈值“3600”，慢破解行为判断阈值（登录失败次数）“15”，表示“3600秒内同一IP发生15次登录失败会被判定为账户爆破行为。”
慢爆破行为判断阈值（登录失败次数）	与慢破解行为判断阈值一起配置使用。可配置范围为“6~100”。
是否审计登录成功	• 开启此功能后，HSS将上报登录成功的事件。 –  ：开启。 –  ：关闭。
阻断攻击IP（非白名单）	开启阻断攻击IP后，HSS将阻断爆破行为的IP（非白名单）登录。
白名单爆破行为是否告警	• 开启后，HSS将对白名单IP产生的爆破行为进行告警。 –  ：开启。 –  ：关闭。
白名单	将IP添加到白名单后，HSS不会阻断白名单内IP的爆破行为。最多可添加50个IP或网段到白名单，且同时支持IPV4和IPV6。

步骤3 确认无误，单击“确认”，完成修改。

----结束

恶意文件检测

步骤1 单击“恶意文件检测”，弹出“恶意文件检测”策略详情界面。

步骤2 在弹出的恶意文件检测界面中，修改“策略内容”，参数说明如表8-10所示。

表 8-10 恶意文件检测策略内容参数说明

参数	说明
反弹shell忽略的进程文件路径	反弹shell忽略的进程文件的路径。 文件路径以“/”开头，不能以“/”结尾。多个路径通过回车换行分隔且名称中不能包含空格。
反弹shell扫描周期（秒）	反弹shell扫描的周期，可配置范围为“30-86400”。

参数	说明
Audit检测增强	• 选择是否开启Audit检测增强，建议开启。 –  ：开启。 –  ：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”。
反弹shell检测	• 选择是否开启反弹shell检测，建议开启。 –  ：开启。 –  ：关闭。
反弹Shell自动化阻断	选择是否开启反弹Shell自动阻断，建议开启。 •  ：开启。 •  ：关闭。
异常shell检测	• 选择是否开启异常shell检测，建议开启。 –  ：开启。 –  ：关闭。

步骤3 确认无误，单击“确认”，完成修改。

----结束

进程异常行为

步骤1 单击“进程异常行为”，弹出“进程异常行为”策略详情界面。

步骤2 在弹出的进程异常行为管理界面中，修改“策略内容”，参数说明如表8-11所示。

表 8-11 进程异常行为策略内容参数说明

参数	说明	取值样例
检测扫描周期（秒）	检测主机运行程序的时间周期，可配置范围为“30-1800”。	1800

参数	说明	取值样例
检测模式	选择进程异常行为的检测模式 • 高检出模式：对所有进程进行深度、全量的检测扫描，可能存在一定误报，适用于护网重保等场景。 • 均衡模式：对所有进程进行全量的检测扫描，检测结果准确性和异常进程的检出率均得到一定平衡，适用于日常防护。 • 低误报模式：对所有进程进行全量的检测扫描，重点提升检测结果的准确性，减少误报的情况，适用于误报较多的场景。	均衡模式

步骤3 确认无误，单击“确认”，完成修改。

----结束

root 提权

步骤1 单击“root提权”，弹出“root提权”策略详情界面。

步骤2 在弹出的root提权界面中，修改“策略内容”，参数说明如表8-12所示。

表 8-12 root 提权策略内容参数说明

参数	说明
忽略的进程文件路径	忽略的进程文件的路径。 文件路径以“/”开头，不能以“/”结尾。多个路径通过回车换行分隔且名称中不能包含空格。
检测时间间隔（秒）	进程文件检测时间间隔，可配置范围为“5~3600”。

步骤3 确认无误，单击“确认”，完成修改。

----结束

实时进程

步骤1 单击“实时进程”，弹出“实时进程”策略详情界面。

步骤2 在弹出的实时进程界面中，修改“策略内容”，参数说明如表8-13所示。

表 8-13 实时进程策略内容参数说明

参数	说明
全量进程上报时间间隔（秒）	所有进程上报间隔的时间周期，可配置范围为“3600~86400”。
高危命令	检测包含关键词的高危命令。

参数	说明
白名单（不记录/不上报）	添加检测时放行、忽略的路径或程序名；同时可添加命令行正则表达式进一步定位进程，命令行正则表达式非必填。

步骤3 确认无误，单击“确认”，完成修改。

----结束

rootkit 检测

步骤1 单击“rootkit检测”，弹出“rootkit检测”策略详情界面。

步骤2 在弹出的rootkit检测界面中，修改“策略内容”。

表 8-14 rootkit 检测策略内容参数说明

参数名称	参数说明	取值样例
检测的时间间隔（秒）	策略执行检测的间隔时间周期，可配置范围为“60~86400”。	86400
根据知识库检查	检测时按照已有知识库内容检查，包括对文件和文件夹的检查，建议开启。 •  ：开启。 •  ：关闭。	 ：开启。
根据内核空间检查	检测时按照内核模块为单位进行检查，包括对所有内核模块的检查，建议开启。 •  ：开启。 •  ：关闭。	 ：开启。
内核模块白名单	自定义填写检测时忽略的内核模块名称。 可填写多个，不同模块名称之间用换行隔开，最多可添加10个。	xt_conntrack virtio_scsi tun

步骤3 确认无误，单击“确认”，完成修改。

----结束

AV 检测

步骤1 单击“AV检测”，弹出“AV检测”策略详情界面。

步骤2 在弹出的AV检测界面中，修改“策略内容”，参数说明如表8-15所示。

表 8-15 AV 检测策略内容参数说明

参数名称	参数说明	取值样例
是否开启实时防护	开启后，执行该策略时AV检测提供实时检测防护，建议开启。 •  ：开启。 •  ：关闭。	 ：开启。
防护文件类型	自定义勾选自动实时检测的文件的类型。 • 全部：选中所有文件类型。 • 可执行：常见的exe，dll，sys等。 • 压缩：常见的zip，rar，jar等。 • 文本：常见的php，jsp，html，bash等。 • OLE：复合型文档，常见的office格式文件（ppt，doc）和保存的邮件文件（msg）。 • 其他：除开以上类型的其他类型。	全部
防护动作	目标检测告警的防护动作。 • 自动处理：检测为高危等级病毒文件将自动执行隔离，其余风险等级病毒不自动隔离。 • 人工处理：检测的病毒无论是什么风险等级，都不会自动隔离，需手动处理。	自动处理

步骤3 确认无误，单击“确认”，完成修改。

----结束

容器信息收集

步骤1 单击“容器信息收集”，弹出“容器信息收集”策略详情界面。

步骤2 在弹出的容器信息收集界面中，修改“策略内容”，参数说明如表8-16所示。

说明

白名单优先级更高，若白名单和黑名单配置了一样的目录，则目录以白名单为基准，允许挂载。

表 8-16 容器信息收集策略参数说明

参数名称	参数说明	取值样例
挂载目录白名单	填写允许挂载的目录。	/test/docker或/root/* 注：路径以*结束表示目标路径下的所有子目录，不包括主目录。 如：设置/var/test/*为白名单目录，表示：目录/var/test/下的所有子目录为白名单目录，不包括test这层。
挂载目录黑名单	填写不允许挂载的目录，如user、bin为主机关键信息文件路径，不建议作为挂载目录，否则重要信息可能存在暴露风险。	

步骤3 确认无误，单击“确认”，完成修改。

----结束

集群入侵检测

步骤1 单击“集群入侵检测”，滑出“集群入侵检测”策略详情界面。

步骤2 在弹出的集群入侵检测界面中，修改“策略内容”，参数说明如表8-17所示。

表 8-17 集群入侵检测策略参数说明

参数名称	参数说明	取值样例
基础检测case	提供所有支持基础检测的检测项，根据需求勾选即可。	全选。
白名单	自定义添加在检测中需要忽略的类型及对应的值，且可自定义进行添加的删除。 支持的类型如下： • ip过滤 • pod名称过滤 • image名称过滤 • 执行用户过滤 • pod标签过滤 • namespace过滤 **说明** 每一种类型只能使用一次。	类型：ip过滤 值：192.168.x.x

说明

该策略配置完成后，还需开启日志审计功能，且企业主机安全Agent需要部署在集群的管理节点上（APIServer所在的节点）才能正常生效。

步骤3 确认无误，单击“确认”，完成修改。

----结束

容器逃逸

步骤1 单击“容器逃逸”，系统弹出“容器逃逸”策略详情页面。

步骤2 在弹出的“容器逃逸”策略页面中，编辑策略内容，参数说明如**表 容器逃逸策略参数说明**所示。

如果没有需要添加白名单的镜像、进程、POD，可不填写对应的白名单。

表 8-18 容器逃逸策略参数说明

参数名称	参数说明
镜像白名单	填写无需检测容器逃逸行为的镜像名称，镜像名只能包含字母、数字、下划线、中划线，多个镜像名以换行符隔开，最多可添加100个镜像名。
进程白名单	填写无需检测容器逃逸行为的进程名称，进程名只能包含字母、数字、下划线、中划线，多个进程名以换行符隔开，最多可添加100个进程名。
POD白名单	填写无需检测容器逃逸行为的POD名称，POD名只能包含字母、数字、下划线、中划线，多个POD名以换行符隔开，最多可添加100个POD名。

步骤3 单击“确认”，完成修改。

----结束

容器文件监控

须知

当被监控的文件路径位于挂载路径下，而非容器在主机上的可写层时，无法触发容器文件修改的告警。此类文件可以通过主机的**文件保护策略**进行防护。

步骤1 单击“容器文件监控”，滑出“容器文件监控”策略详情界面。

步骤2 在弹出的容器文件监控界面中，修改“策略内容”，参数说明如**表8-19**所示。

表 8-19 容器文件监控策略参数说明

参数名称	参数说明	取值样例
模糊匹配	是否启动对目标文件的模糊匹配，建议勾选。	勾选。
禁止新增可执行文件	对新增可执行文件行为进行监控，勾选后可禁止新增可执行的文件，建议勾选。	勾选。
镜像名称	执行检测的目标镜像的名称。	test_bj4

参数名称	参数说明	取值样例
镜像ID	执行检测的目标镜像的ID。	-
文件	执行检测的目标镜像下的文件名称。	/tmp/testw.txt

步骤3 确认无误，单击“确认”，完成修改。

----结束

容器进程白名单

步骤1 单击“容器进程白名单”，滑出“容器进程白名单”策略详情界面。

步骤2 在弹出的容器进程白名单界面中，修改“策略内容”，参数说明如表8-20所示。

表 8-20 容器进程白名单策略参数说明

参数名称	参数说明	取值样例
模糊匹配	是否启动对目标文件的模糊匹配，建议勾选。	勾选。
镜像名称	执行检测的目标镜像的名称。	test_bj4
镜像ID	执行检测的目标镜像的ID。	-
进程	执行检测的目标镜像下的文件路径。	/tmp/testw

步骤3 确认无误，单击“确认”，完成修改。

----结束

镜像异常行为

步骤1 单击“镜像异常行为”，滑出“镜像异常行为”策略详情界面。

步骤2 在弹出的镜像异常行为界面中，修改“策略内容”，参数说明如表8-21所示。

表 8-21 镜像异常行为策略参数说明

参数名称	参数说明	取值样例
规则名称	不同规则的名称。	-
规则描述	不同规则的简要描述。	-

参数名称	参数说明	取值样例
规则模板	• 选择不同的规则进行配置，支持的规则项如下： – 镜像白名单 – 镜像黑名单 – 镜像标签白名单 – 镜像标签黑名单 – 创建容器白名单 – 创建容器黑名单 – 容器mount proc白名单 – 容器seccomp unconfined – 容器特权白名单 – 容器capabilities白名单 • 规则填写参数说明如下： – 精准匹配：通过目标镜像名称来检测，填写目标镜像名称匹配镜像，多个名称以英文分号隔开，最多填写20个。 – 正则匹配：通过正则来检测，填写正则表达式匹配镜像，多个表达式以英文分号隔开，最多填写20个。 – 前缀匹配：通过前缀名称来检测，填写前缀名称匹配镜像，多个前缀以英文分号隔开，最多填写20个。 – 标签名称：通过标签及标签值来筛选检测，最多可添加20个标签项。 – 权限类型：通过选择权限进行指定检测或忽略检测，权限说明详情请参见**表8-22**。	-

表 8-22 镜像异常行为权限说明

权限名称	权限说明
AUDIT_WRITE	将记录写入内核审计日志的。
CHOWN	对文件UID和GID进行任意更改的。
DAC_OVERRIDE	绕过文件读、写和执行权限检查。
FOWNER	绕过权限检查通常要求进程的文件系统UID与文件UID匹配的操作。
FSETID	修改文件时不清除set-user-ID和set-group-ID权限位。
KILL	放通发送信号的权限检查。
MKNOD	使用mknod创建特殊文件。
NET_BIND_SERVICE	将socket绑定到internet域特权端口（端口号小于1024）。

权限名称	权限说明
NET_RAW	使用原始socket和数据包socket。
SETFCAP	设置文件功能。
SETGID	对进程GID和补充GID列表进行任意操作。
SETPCAP	修改进程能力。
SETUID	对进程UID进行任意操作。
SYS_CHROOT	使用chroot，更改根目录。
AUDIT_CONTROL	启用和禁用内核审计；更改审计筛选规则；检索审计状态和筛选规则。
AUDIT_READ	允许通过组播网络链接套接字读取审计日志。
BLOCK_SUSPEND	允许防止系统挂起。
BPF	允许创建BPF映射、加载BPF类型格式（BTF）数据、检索BPF程序的JITed代码等。
CHECKPOINT_RESTORE	允许检查点/恢复相关操作。
DAC_READ_SEARCH	绕过文件读取权限检查和目录读取和执行权限检查。
IPC_LOCK	锁定内存(mlock、mlockall、mmap、shmctl)。
IPC_OWNER	绕过对System V IPC对象的操作的权限检查。
LEASE	在任意文件上建立租赁。
LINUX_IMMUTABLE	设置FS_APPEND_FL和FS_IMMUTABLE_FL i节点标志。
MAC_ADMIN	允许MAC配置或状态更改。
MAC_OVERRIDE	覆盖强制访问控制(MAC)。
NET_ADMIN	执行各种与网络相关的操作。
NET_BROADCAST	进行socket广播，并侦听组播。
PERFMON	允许使用perf_events、i915_perf和其他内核子系统进行系统性能和可观察性特权操作。
SYS_ADMIN	执行一系列系统管理操作。
SYS_BOOT	使用重新启动和kexec_load，重新启动并加载新内核以便以后执行。
SYS_MODULE	加载和卸载内核模块。
SYS_NICE	提升进程良好值（良好，设置优先级)，并更改任意进程的良好值。

权限名称	权限说明
SYS_PACCT	使用账户，打开或关闭进程记账。
SYS_PTRACE	使用ptrace跟踪任意进程。
SYS_RAWIO	执行I/O端口操作(ipl和ioperm)。
SYS_RESOURCE	覆盖资源限制。
SYS_TIME	设置系统时钟(settimeofday、stime、adjtimex)；设置实时（硬件）时钟。
SYS_TTY_CONFIG	使用vhangup；在虚拟终端上使用各种特权ioctl操作。
SYSLOG	执行特权系统日志操作。
WAKE_ALARM	触发将唤醒系统的东西。

步骤3 确认无误，单击“确认”，完成修改。

----结束

端口扫描检测

步骤1 单击“端口扫描检测”，滑出“端口扫描检测”策略详情界面。

步骤2 在弹出的端口扫描检测界面中，修改“策略内容”，参数说明如表8-23所示。

表 8-23 端口扫描检测策略参数说明

参数名称	参数说明	取值样例
重新获取进程信息的时间间隔（秒）	获取进程的间隔时间。	勾选。
扫描源IP白名单	填写IP白名单，多个用英文分号隔开。	test_bj4
单端口最大告警包数	-	-
待检测端口列表	待检测的端口号和协议类型详情。	-

步骤3 确认无误，单击“确认”，完成修改。

----结束

自保护

自保护策略是保护企业主机安全的软件、进程和文件不被恶意程序破坏的策略，不支持自定义策略内容。

8.2 历史处置记录

HSS支持查看漏洞、安全告警事件的历史处置记录，方便您查看漏洞和事件的处理人、处理时间。

查看所有漏洞的历史处置记录

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“安全运营 > 历史处置记录”，进入“历史处置记录”页面。

步骤4 选择“漏洞管理”页签，查看所有漏洞的历史处置记录。

- 查看指定属性的漏洞处置记录
  在漏洞处置记录列表上方搜索框中，输入漏洞类型、漏洞名称、服务器IP等并单击，可查看指定属性的漏洞处置记录。

----结束

9 安全报告

9.1 查看安全报告

企业主机安全支持订阅**日报**、周报、月报和**自定义**，展现不同周期主机安全趋势以及关键安全事件与风险。

说明

- 勾选订阅报告后，第二天即可查看、下载。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

安全报告概览

步骤1 登录管理控制台。

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

步骤3 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤4 单击目标报告的“获取报告”，跳转至报告预览页，可查看报告信息、下载、发送报告。

----结束

查看报告发送记录

发送记录存储了邮件发送报告的发送详情。

步骤1 单击安全报告概览页右上角的“报告发送记录”查看报告发送记录。

步骤2 在弹窗中查看报告发送记录，参数说明如**表9-1**所示。

表 9-1 报告发送记录参数

参数名称	参数说明
报告名称	已发送报告的名称。
统计周期	目标发送报告内容的统计周期。
报告类型	目标发送报告的统计周期类型。 • 安全周报 • 安全月报 • 安全日报 • 自定义报告
邮件发送时间	目标报告发送的时间。

步骤3 单击“操作”列的“获取报告”可查看历史发送的报告信息，同时可预览和下载报告。

----结束

9.2 订阅安全报告

指导您通过控制台的预设模板快速实现以周为单位或以月为单位的安全报告订阅。如需自定义，操作详情请参见**创建安全报告**。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

订阅说明

- 安全报告是为所有已开启防护的主机生成报告，不支持选择特定主机生成报告。
- 订阅安全报告均为免费，但报告内容会受防护配额版本支持的功能限制。

操作步骤

步骤1 登录管理控制台。

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

步骤3 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤4 单击按月或按周的报告开关状态为开启状态，开启安全报告的订阅，如需对报告进行编辑详情请参见**编辑安全报告**。

----结束

9.3 创建安全报告

若已有模板的报告类型和报告内容无法满足您对安全报告的订阅需求，您可通过该章节创建需要生成报告的周期和内容。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

操作步骤

步骤1 登录管理控制台。

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

步骤3 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤4 创建新报告

- 按模板创建按月或按周的安全报告
  - 单击按月或按周模板报告中的“复制”（按需选择即可），进入报告基本信息配置页面。
- 自定义创建其他周期的安全报告
  - 单击页面中的“创建新报告”，进入报告基本信息配置页面。

步骤5 对报告基本信息进行配置，参数说明如表9-2所示。

表 9-2 报告基本信息参数说明

参数名称	参数说明	取值样例
报告名称	默认的报告名称。	ecs security report
报告类型	报告的统计周期类型名称。 • 安全日报（统计周期为每天00:00-24:00） • 安全周报（统计周期为周一00:00-周日24:00） • 安全月报（统计周期为每月1号00:00-月度最后一天24:00） • 自定义报告（自定义统计周期，周期范围应介于1天（包含）至3个月（包含）之间。 • 所有类型报告将在生成后的次日自动发送至您设置的报告接收人。	安全月报

参数名称	参数说明	取值样例
报告发送时间	报告自动发送时间。	-
报告接收方式	生成的安全报告接收方式。 • 消息主题：为HSS单独创建的主题，设置告警通知接收人。可选择短信或邮件接收通知。 • 无需发送到邮箱：不发送报告至邮箱。	消息主题

步骤6 确认信息无误，单击页面右下角“下一步”，配置报告内容。

步骤7 在左侧勾选需要生成的报告项，右侧可预览，确认无误，单击右下角“保存”，开启安全报告的订阅。

----结束

9.4 管理安全报告

若需对已订阅的报告内容进行修改、取消或关闭订阅，该章节将指导您完成相关操作。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

编辑安全报告

步骤1 登录管理控制台。

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

步骤3 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤4 单击目标报告的“编辑”按钮，对报告进行编辑。

步骤5 对报告基本信息进行编辑，参数说明如表9-3所示。

表 9-3 报告基本信息参数说明

参数名称	参数说明	取值样例
报告名称	默认的报告名称。	default monthly security report
报告类型	报告的统计周期类型名称，不可编辑。	安全月报

参数名称	参数说明	取值样例
报告发送时间	报告自动发送时间。	-
报告接收方式	生成的安全报告接收方式。 ● 消息主题：为HSS单独创建的主题，设置告警通知接收人。可选择短信或邮件接收通知。 ● 无需发送到邮箱：不发送报告至邮箱。	消息主题

步骤6 确认信息无误，单击页面右下角“下一步”，编辑报告内容。

步骤7 在左侧勾选或取消报告项，右侧可预览，确认无误，单击“保存”，报告修改成功。

----结束

关闭订阅

步骤1 登录管理控制台，进企业主机安全页面。

步骤2 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤3 单击目标报告的开关，使其状态为  ，表示目标报告订阅已关闭。

----结束

删除报告

说明

默认的按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板不可删除。

步骤1 登录管理控制台，进企业主机安全页面。

步骤2 左侧选择“安全报告”进入安全报告概览页面。

服务预设了按月（default monthly security report）和按周（default weekly security report）统计的两个安全报告模板，可直接使用。

步骤3 单击目标报告的“删除”，对目标报告进行删除。

----结束

10 安装与配置

10.1 Agent 管理

10.1.1 查看 Agent 状态

可分类查看所有服务器是否安装Agent，同时可安装或卸载服务器的Agent，并提供安装指导及Agent下载链接。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent不在线（X）”，查看Agent未安装或离线的服务器；选择Agent在线（X），查看Agent在线的服务器。

步骤5 单击“Agent安装指南”可查看Agent安装的快速指导。

步骤6 单击“Agent版本说明”，可查看Agent的最新版本、历史版本及变更内容。

----结束

10.1.2 安装 Agent

指导您在console对目标服务器安装Agent，Agent安装后HSS才能对服务器进行正常检测和防护。

单服务器安装 Agent

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent不在线（X）”，查看Agent未安装或离线的服务器列表，详情请参见**表10-1**。

表 10-1 Agent 不在线列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器所属的公网IP或私网IP。
操作系统	目标服务器的操作系统。 • linux • windows
Agent状态	目标服务器的Agent状态。 • 离线 • 未安装 • 安装失败
Agent版本	目标服务器当前安装的Agent版本。
Agent升级状态	目标服务器在Agent升级过程中的状态。

步骤5 单击目标服务器“操作”列的“离线原因”，查看目标服务器Agent离线原因。

步骤6 单击目标服务器“操作”列的“安装Agent”，选择不同架构以及不同系统的链接进行下载安装，linux系统安装详情请参见**安装Linux版本Agent**，windows系统安装详情请参见**安装Windows版本Agent**。

----结束

批量安装 Agent（服务器账号、密码不同）

您可对不同账号密码的多台服务器进行批量安装。

约束限制

- 目前仅支持云上Linux系统的服务器进行不同账号密码的Agent批量安装。
- 批量安装Agent的服务器在同一安全组或能连接的安全组。

前提条件

- 批量安装的所有服务器需要支持ssh登录。
- 批量安装的所有服务器需要提供正确的登录账号、端口、密码。
- 批量安装的主机“服务器状态”必须为“运行中”。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 单击“Agent安装指南”，复制“批量安装”的命令。

步骤5 远程登录待安装Agent的云主机。

须知

登录服务器后先执行以下命令检查服务器是否具备expect命令，若不具备需配置yum源。

/bin/expect -v

步骤6 执行以下命令进入tmp目录。

cd /tmp/

步骤7 按照以下命令格式执行命令，创建文件linux-host-list.txt并将需要批量安装的节点私有ip添加至创建的文件中。

命令格式：echo "IP地址 端口 root rootPassword" >> linux-host-list.txt

或echo "IP地址 端口 user userPassword rootPassword" >> linux-host-list.txt

示例：echo "127.8.10.8 22 root rootPassword" >> linux-host-list.txt

或echo "127.8.10.9 22 user userPassword rootPassword" >> linux-host-list.txt

若存在多个不同IP，则不同IP的命令之间用换行符隔开。

示例：echo "127.8.10.1 22 root rootPassword" >> linux-host-list.txt

echo "127.8.10.8 22 user userPassword rootPassword" >> linux-host-list.txt

echo "127.8.10.3 22 root rootPassword" >> linux-host-list.txt

步骤8 键入回车保存IP，执行命令cat linux-host-list.txt查询是否添加完成。

步骤9 粘贴复制的安装命令，以root权限执行，在主机中安装Agent。

若界面回显如下信息，则表示Agent安装成功。

remote_install finished. [OK]

步骤10 安装成功后可在“安装与配置 > Agent管理 > Agent在线”页面查看目标服务器的“Agent状态”为“在线”，表示Agent服务运行正常。

----结束

10.1.3 升级 Agent

企业主机安全会持续优化提升服务能力，包括不限于新增功能、优化缺陷，请您及时将服务器的Agent升级为最新版，以便您可以享受到更好的企业主机安全。

单服务器升级 Agent

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent在线（X）”，查看Agent已安装的服务器列表，详情请参见**表10-2**。

表 10-2 Agent 在线服务器列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器所属的公网IP或私网IP。
操作系统	目标服务器的操作系统。 • linux • windows
Agent状态	目标服务器的Agent状态。 • 在线

步骤5 单击目标服务器“操作”列的“升级Agent”，在弹窗中确认升级信息无误，单击“确认”，开始自动执行升级。

步骤6 升级完成后，可查看目标服务器的“Agent版本”变更为最新版表示升级完成。

----结束

批量升级 Agent

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“区域”，选择“安全 > ”，进入“ ”页面。

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent在线（X）”，查看Agent已安装的服务器列表，详情请参见**表10-3**。

表 10-3 Agent 在线服务器列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器所属的公网IP或私网IP。

参数名称	参数说明
操作系统	目标服务器的操作系统。 • linux • windows
Agent状态	目标服务器的Agent状态。 • 在线

步骤5 勾选需升级Agent的目标服务器。

说明

- 勾选“服务器名称/ID”前的选框，则选中当前页全部服务器。
- 勾选“选中全部”选框，选中所有待升级Agent的服务器进行Agent升级。

步骤6 单击上方“批量升级Agent”，在弹窗中确认即将升级Agent的服务器，确认无误，单击“确认”，开始执行自动升级。

步骤7 升级完成后，可查看目标服务器的“Agent版本”变更为最新版表示升级完成。

----结束

10.1.4 卸载 Agent

如果不再需要HSS为您的服务器提供防护，您可以参照本文卸载Agent，Agent卸载后HSS将停止对服务器的检测和防护。

单服务器一键卸载 Agent

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent在线（X）”，查看Agent已安装的服务器列表，详情请参见表10-4。

表 10-4 Agent 在线服务器列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器所属的公网IP或私网IP。
操作系统	目标服务器的操作系统。 • linux • windows

参数名称	参数说明
Agent状态	目标服务器的Agent状态。 • 在线

步骤5 单击目标服务器“操作”列的“卸载Agent”，在弹窗中确认卸载信息无误，单击“确认”，完成卸载。

----结束

批量服务器一键卸载 Agent

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > Agent管理”，进入Agent管理页面。

步骤4 选择“Agent在线（X）”，查看Agent已安装的服务器列表，详情请参见**表10-5**。

表 10-5 Agent 在线服务器列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器所属的公网IP或私网IP。
操作系统	目标服务器的操作系统。 • linux • windows
Agent状态	目标服务器的Agent状态。 • 在线

步骤5 勾选需卸载Agent的目标服务器。

说明

勾选“服务器名称/ID”前的选框，则选中当前页全部服务器。

步骤6 单击上方“批量卸载Agent”，在弹窗中确认即将卸载Agent的服务器，确认无误，单击“确认”，完成卸载。

----结束

Linux 服务器手动卸载 Agent

步骤1 远程登录待卸载Agent的Linux服务器。

- 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、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。

步骤2 执行以下命令，卸载Agent。

说明

不可以在/usr/local/hostguard/目录下执行卸载命令，可以在其他任意目录下执行卸载命令。

- EulerOS、CentOS、RedHat等支持rpm安装方式的OS的卸载命令：**rpm -e hostguard;**
- Ubuntu、Debian等支持deb安装方式的OS的卸载命令：**dpkg -P hostguard;**

步骤3 查看Linux服务器的/usr/local/hostguard/目录不存在，表示Agent卸载完成。

----结束

Windows 服务器手动卸载 Agent

步骤1 远程登录待卸载Agent的Windows服务器。

- 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：mstsc、rdp等）登录主机，并使用管理员账号在主机中安装Agent。

步骤2 进入Windows服务器的C:\Program File\HostGuard目录下。

步骤3 双击“unins000.exe”文件，卸载Agent。

步骤4 在“HostGuard卸载向导”弹窗中，单击“是”，完全删除HostGuard及其所有组件。

步骤5 （可选）重启主机。

- 如果您开启了网页防篡改，卸载Agent需要重启主机。在“HostGuard卸载向导”弹窗中，单击“是”，重启主机。
- 如果您未开启网页防篡改，无需重启主机。在“HostGuard卸载向导”弹窗中，单击“否”，不重启主机。

步骤6 查看Windows服务器的C:\Program Files\HostGuard目录不存在，表示卸载Agent完成。

----结束

10.2 安全配置

通过添加常用登录地、常用IP、白名单IP以及开启恶意程序隔离查杀进一步保障服务器的安全运行。

操作详情请参见**常用安全配置**。

10.3 插件管理

10.3.1 插件配置概述

插件管理功能支持对多种插件进行管理，您可根据需求按照插件指导安装和管理需要的插件。

插件类型

当前仅支持Docker插件的管理。

Docker 插件应用场景

开通容器安全防护后，如果您需要使用镜像阻断功能，您需要**安装Docker插件**。

Docker插件是实现镜像阻断能力的一个插件。镜像阻断是一种容器安全防御功能， 它可以在Docker环境中容器启动前阻断具有高危漏洞或不符合安全标准的容器镜像的运行。

镜像阻断的应用场景如下：

10.3.2 查看插件详情

呈现所使用的服务器使用插件详情。

可自定义对插件进行安装、升级、卸载操作。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > 插件配置”，进入插件配置页面，查看插件列表详情。插件列表参数说明请参见**表 Docker插件列表参数说明**。

插件列表默认展示所有服务器，如果服务器安装了插件，插件列表会展示插件的详细信息，如果服务器未安装插件，插件信息为空。

表 10-6 Docker 插件列表参数说明

参数名称	参数说明
服务器名称/ID	服务器的名称和ID信息。
IP地址	服务器的IP地址。
操作系统	服务器的操作系统类型。
插件名称	服务器安装的插件名称。
插件版本	服务器安装的插件版本。

参数名称	参数说明
插件状态	插件当前状态。 ● 已创建：插件已创建，还未启动。 ● 运行中：插件正常运行。 ● 已暂停：插件暂停运行。 ● 重启中：插件正在重启。 ● 移除中：插件正在被删除。 ● 已退出：插件已停止运行。 ● 消亡：插件已无法启动或删除。
插件升级状态	插件升级状态。 ● 未升级：插件未升级至最新版本。 ● 正在升级中：插件正在升级。 ● 升级成功：插件升级至新版本成功。 ● 升级失败：插件升级失败。

----结束

10.3.3 安装插件

开通容器安全防护后，如果您需要使用镜像阻断功能，请参照本章节安装Docker插件。

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启企业主机安全容器版本。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件安装指南”，在滑出面板的“安装步骤”中获取安装命令，单击“复制”。

步骤4 以root权限远程登录待安装插件的主机。

- 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：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装插件

步骤5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量安装的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

若存在多个不同IP，则不同IP的命令之间用换行符隔开。

示例：

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

步骤7 键入回车保存IP，执行命令cat linux-host-list.txt查询是否添加完成。

步骤8 将批量安装的命令复制粘贴至命令框，键入回车，开始自动执行安装。

步骤9 反馈“remote_install finished. [OK]”则安装成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

```
remote_install finished. [OK]
```

----结束

10.3.4 插件升级

可自行对目标服务器的插件进行升级。

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启企业主机安全容器版本。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件升级指南”，在滑出面板的“升级步骤”中获取升级命令，单击“复制”。

步骤4 以root权限远程登录待升级插件的主机。

- 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：PuTTY、Xshell等）登录主机，并使用root账号在主机中升级插件。

步骤5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量升级的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

若存在多个不同IP，则不同IP的命令之间用换行符隔开。

示例：

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

步骤7 键入回车保存IP，执行命令cat linux-host-list.txt查询是否添加完成。

步骤8 将批量升级的命令复制粘贴至命令框，键入回车，开始自动执行升级。

步骤9 反馈“remote_upgrade finished. [OK]”则升级成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

```
remote_upgrade finished. [OK]
```

----结束

10.3.5 卸载插件

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启企业主机安全容器版本。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件卸载指南”，在滑出面板的“卸载步骤”中获取卸载命令，单击“复制”。

步骤4 以root权限远程登录待卸载插件的主机。

- 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：PuTTY、Xshell等）登录主机，并使用root账号在主机中卸载插件。

步骤5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量卸载的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

若存在多个不同IP，则不同IP的命令之间用换行符隔开。

示例：

```
echo 127.8.8.1 22 root rootPassword >> linux-host-list.txt
echo 127.8.8.2 22 user userPassword rootPassword >> linux-host-list.txt
echo 127.8.8.3 22 root rootPassword >> linux-host-list.txt
```

步骤7 键入回车保存IP，执行命令cat linux-host-list.txt查询是否添加完成。

步骤8 将批量卸载的命令复制粘贴至命令框，键入回车，开始自动执行卸载。

步骤9 反馈“remote_uninstall finished. [OK]”则卸载成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

```
remote_uninstall finished. [OK]
```

----结束

11 审计

11.1 支持云审计的 HSS 操作列表

企业主机安全通过云审计服务（Cloud Trace Service，CTS）为用户提供云服务资源的操作记录，记录内容包括用户从管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果，供用户查询、审计和回溯使用。

云审计服务支持的HSS操作列表如**表11-1**所示。

表 11-1 云审计服务支持的 HSS 操作列表

操作名称	资源类型	事件名称
取消忽略端口	hss	notIgnorePortStatus
忽略端口	hss	ignorePortStatus
取消忽略配置检测项	hss	notIgnoreCheckRuleStat
忽略配置检测项	hss	ignoreCheckRuleStat
重新进行基线检测	hss	runBaselineDetect
解绑配额	hss	cancelHostsQuota
关闭容器防护	hss	closeContainerProtectStatus
开启容器防护	hss	openContainerProtectStatus
解除已拦截IP	hss	changeBlockedIp
处理事件状态	hss	changeEvent
恢复已隔离文件	hss	changeIsolatedFile
删除告警白名单	hss	removeAlarmWhiteList
添加登录白名单	hss	addLoginWhiteList
删除登录白名单	hss	removeLoginWhiteList

操作名称	资源类型	事件名称
新增服务器组	hss	addHostsGroup
分配到服务器组	hss	associateHostsGroup
修改服务器组	hss	changeHostsGroup
删除服务器组	hss	deleteHostsGroup
关闭主机防护	hss	closeHostsProtectStatus
开启主机防护	hss	openHostsProtectStatus
卸载agent	hss	uninstallAgents
运行镜像扫描	hss	runImageScan
从SWR服务同步镜像列表	hss	runImageSynchronizeTask
更新并扫描SWR镜像	hss	runSwrImageScan
重新体检	hss	resetRiskScore
添加策略组	hss	addPolicyGroup
删除策略组	hss	deletePolicyGroup
部署策略组	hss	deployPolicyGroup
修改策略内容	hss	modifyPolicyDetail
修改策略组	hss	modifyPolicyGroup
关闭自动隔离查杀	hss	closeAutoKillVirusStatus
开启自动隔离查杀	hss	openAutoKillVirusStatus
设置常用登录IP	hss	modifyLoginCommonIp
设置常用登录地	hss	modifyLoginCommonLocation
设置SSH登录白名单	hss	modifyLoginWhiteIp
修复漏洞	hss	changeVulStatus
添加防护目录	hss	addHostProtectDirInfo
添加特权进程	hss	addPrivilegedProcessInfo
添加定时关闭防护配置	hss	addTimingOffConfigInfo
删除远端备份服务器	hss	deleteBackupHostInfo
删除防护目录	hss	deleteHostProtectDirInfo
删除特权进程	hss	deletePrivilegedProcessInfo
删除定时关闭防护配置	hss	deleteTimingOffConfigInfo

操作名称	资源类型	事件名称
设置定时关闭防护周期	hss	setDateOffConfigInfo
修改防护目录开启状态	hss	setProtectDirSwitchInfo
修改动态网页防篡改状态	hss	setRaspSwitch
设置远端备份服务器	hss	setRemoteBackupInfo
修改定时关闭防护状态	hss	setTimingOffSwitchInfo
关闭网页防篡改防护	hss	closeWtpProtectionStatus
开启网页防篡改防护	hss	openWtpProtectionStatus
修改远端备份服务器	hss	updateBackupHostInfo
修改防护目录	hss	updateHostProtectDirInfo
修改特权进程	hss	updatePrivilegedProcessInfo
修改Tomcat bin目录	hss	updateRaspPathInfo
修改定时关闭防护时间段	hss	updateTimingOffConfigInfo

11.2 查看审计日志

开启了云审计服务后，系统开始记录HSS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 HSS 的云审计日志

步骤1 登录管理控制台。

步骤2 单击页面上方的 ☰，选择“管理与监控 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。

  在下拉框中选择查询条件。
  - “事件类型”选择“管理事件”。
  - “事件来源”选择“HSS”。
  - “筛选类型”选择“按事件名称”时，还需选择某个具体的事件名称；选择“按资源ID”时，还需选择或者手动输入某个具体的资源ID；选择“按资源名称”时，还需选择或手动输入某个具体的资源名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。

- “事件级别”：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- “时间范围”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

步骤5 单击“查询”，查看对应的操作事件。

步骤6 在需要查看的记录左侧，单击 ﹀ 展开该记录的详细信息，展开记录。

步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，显示了该操作事件结构的详细信息。

----结束

12 权限管理

12.1 创建用户并授权使用 HSS

如果您需要对您所拥有的HSS进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用HSS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将HSS资源委托给更专业、高效的其他云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用HSS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如图12-1所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的HSS权限，并结合实际需求进行选择，HSS系统策略如表12-1所示。

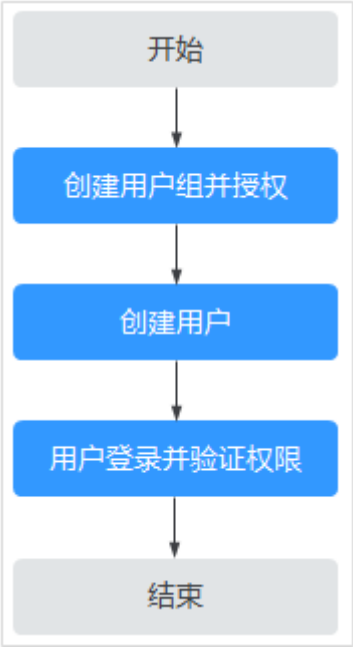
表 12-1 HSS 系统权限

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

系统角色/策略名称	描述	类别	依赖关系
HSS ReadOnlyAccess	企业主机安全的只读访问权限。	系统策略	无

示例流程

图 12-1 给用户授权服务权限流程



1. 创建用户组并授权。在IAM控制台创建用户组，并授予HSS服务的管理员权限“HSS Administrator”。
2. 创建用户并加入用户组。在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 用户登录并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在“服务列表”中选择除企业主机安全外（假设当前策略仅包含“HSS Administrator”）的任一服务，若提示权限不足，表示“HSS Administrator”已生效。

12.2 HSS 自定义策略

如果系统预置的HSS权限，不满足您的授权要求，可以创建自定义策略。

具体创建步骤请参见《统一身份认证服务》的“创建自定义策略”章节。本章为您介绍常用的HSS自定义策略样例。

HSS 自定义策略样例

- 示例1：授权用户查询主机防护列表

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

- 示例2：拒绝用户卸载Agent

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

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

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hss:agent:uninstall"
            ]
        },
    ]
}
```

- 多个授权项策略

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

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


13 手动升级 HSS

13.1 升级概述

主机安全升级至新版需要先将旧版主机安全中的Agent进行卸载，确认卸载成功后在新版HSS控制台安装新版的Agent后即完成升级。

升级说明

- 整个升级Agent过程均为免费。
- 升级过程中不影响您在云服务器上业务的正常使用。
- 升级期间主机安全风险可能会增加，关闭防护后尽快执行Agent的卸载、安装操作，尽量缩短主机未防护的时间。

升级流程

13.2 步骤一：关闭旧版 HSS 防护

升级前需要关闭旧版主机防护，关闭防护后才能正常卸载旧版的Agent。

关闭防护说明

- 关闭防护不影响您在云服务器上业务的正常使用。
- 关闭防护期间安全风险可能会增加，关闭后尽快执行Agent的卸载、安装操作，尽量缩短主机未防护的时间。

关闭操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“主机管理”，进入“云服务器”界面。

步骤4 单击目标主机“操作”列的“关闭防护”，对需要升级的主机进行关闭防护操作。

也可勾选多个列表前的选框，选择多台主机，单击上方的“关闭防护”，进行批量关闭。

----结束

13.3 步骤二：在旧版卸载 Agent

主机安全只能安装一个Agent，旧版主机安全的Agent对新版主机安全的部分特性存在不兼容问题，因此需要对旧版主机安全的Agent进行卸载。

卸载说明

卸载Agent提供两种不同的方式：

- 一键批量卸载：在主机安全旧版控制台通过选择多台主机进行一键卸载。
- 本地命令卸载：通过逐一登录需要卸载Agent的主机，针对不同系统的主机执行不同的操作执行卸载操作，不支持批量卸载。

控制台一键卸载 Agent

步骤1 登录管理控制台。

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

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

步骤4 在弹出的“卸载Agent”界面中，勾选需要卸载Agent的云服务器。

步骤5 确认勾选无误，单击“确定”自动开始执行卸载。

执行结束后在“主机管理 > 云服务器”列表中查看目标服务器的“Agent状态”显示为“离线”，表示Agent卸载成功。

----结束

主机本地卸载

本地卸载会根据服务器的操作系统执行不同的卸载操作。

- **卸载Linux版本Agent**
  a. 登录需要卸载Agent的云服务器，并执行以下命令切换到**root**用户。
  ```
  su - root
  ```
  b. 在任意目录执行以下命令，卸载Agent。
     i. 针对“.rpm”格式的Agent安装包，执行命令：**rpm -e --nodeps hostguard**
     ii. 针对“.deb”格式的Agent安装包，执行命令：**dpkg -P hostguard**
  c. 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**
  a. 登录需要卸载Agent的云服务器。
  b. 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。

c. 在“HostGuard卸载”提示框中，单击“是”，开始卸载。

d. 卸载完成后单击“确定”。

13.4 步骤三：在新版安装 Agent

新版主机安全迭代了部分功能特性，需要新版Agent才能更好地兼容运行。

前提条件

- 确定目标主机的旧版Agent已卸载干净，否则可能导致安装失败。
- 确定目标主机的操作系统版本是官网正常维护的，官网停止维护的操作系统版本Agent可能无法正常安装。
- Linux主机在本地已安装远程管理工具（如：Xftp、SecureFX、PuTTY、Xshell等）。
- Windows主机在本地已安装远程管理工具（如：pcAnywhere、UltraVNC）。

约束限制

- 关闭Selinux防火墙，防止Agent安装失败，安装成功后再打开。
- 您的云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。

安装说明

- 安装成功后，需要等待3~10分钟左右才会刷新Agent状态，请前往“资产管理 > 主机管理 > 云服务器”界面查看状态。
- 安装Agent时，建议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，防止Agent安装失败。
- 安装Agent需要在新版控制台获取安装命令后登录服务器进行安装。

安装 Linux 服务器的 Agent

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3~10分钟左右控制台才会刷新。

步骤1 登录管理控制台。

步骤2 在页面左上角单击☰，选择“安全与合规 > ”，进入云工作负载保护平台页面。

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

步骤4 选择“安装与配置 > Agent管理 > Agent不在线(X)”页签，在目标服务器的“操作”列单击“安装Agent”。

步骤5 在弹窗中，根据该服务器的系统架构和操作系统选择安装命令，单击“复制”获取目标命令。

步骤6 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、PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。

步骤7 粘贴复制的安装命令，以root权限执行，在主机中安装Agent。

若界面回显信息与如下信息类似，则表示Agent安装成功。

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

步骤8 使用以下命令，查看Agent的运行状态。

```
service hostguard status
```

若界面回显如下信息，则表示Agent已安装成功正常运行。

```
Hostguard is running
```

----结束

安装 Windows 服务器的 Agent

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > ”，进入云工作负载保护平台页面。

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

步骤4 选择“安装与配置 > Agent管理 > Agent不在线(X)”页签，在目标服务器的“操作”列单击“安装Agent”。

步骤5 在弹窗中，根据该服务器的系统架构和操作系统选择安装命令，单击“复制”获取目标命令。

步骤6 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。

步骤7 在待安装Agent的主机中，通过IE浏览器访问**步骤5**中获取的链接，下载Agent安装脚本。

步骤8 下载完成后，请使用管理员权限运行Agent安装脚本。

步骤9 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”。

若进程存在，则表示Agent已安装成功正常运行。

----结束

13.5 步骤四：在新版 HSS 开启防护

13.5.1 开启企业版/旗舰版防护

开启防护后主机安全将继续为服务器进行防护，将提供更多、更可靠的防护能力。

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

- “云工作负载保护平台 > 资产管理 > 主机管理 > 云服务器”页面中目标服务器的“Agent状态”为“在线”。
- 已有未绑定服务器的企业版/旗舰版配额。

约束条件

Windows操作系统

- 开启主机防护时，需要授权开启Windows防火墙，且使用期间请勿关闭Windows防火墙。若关闭Windows防火墙，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，也可能导致不能拦截账户暴力破解的攻击源IP。

开启防护

为达到更好的防护效果，建议在“安装与配置 > 安全配置”页面完成相关信息的配置。

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > ”，进入云工作负载保护平台页面。

步骤3 在左侧导航栏中，选择“资产管理 > 主机管理 > 云服务器”，进入“云服务器”界面。

步骤4 选择所需开启安全防护的主机，单击“操作”列“开启防护”，在“开启防护”对话框中，选择主机配额版本。

步骤5 单击“确认”，开启防护。开启防护后，请在控制台上查看的开启状态。

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

说明

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，主机安全将根据您开启的服务版本，自动对您的主机执行服务版本对应的安全检测。

----结束

13.5.2 开启网页防篡改版防护

前提条件

- 在“主动防御 > 网页防篡改 > 防护配置”页面中目标服务器“Agent状态”为“在线”、“防护状态”为“关闭”。
- 已有未绑定服务器的网页防篡改配额。

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。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。

开启防护

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > ”，进入云工作负载保护平台页面。

步骤3 在左侧导航树中，选择“主动防御 > 网页防篡改”，单击“添加防护服务器”。

步骤4 在“添加防护服务器”页面，选择需要开启防护的服务器，单击“添加并开启防护”。

说明

已开启防护、未安装Agent和Agent不在线的服务器无法开启防护。

步骤5 开启网页防篡改防护服务后，可在控制台上查看的开启状态，同时旗舰版防护能力会同步开启。

选择“主动防御 > 网页防篡改”，目标服务器所在行的“防护状态”为“防护中”，则表示网页防篡改版已开启。

----结束

13.5.3 开启容器版防护

检测周期

服务每日凌晨进行全量检测。

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看到检测结果。

前提条件

- 已在云容器引擎成功创建节点。
- “云工作负载保护平台 > 资产管理 > 容器管理 > 容器节点管理”页面的“节点列表”中目标节点的“Agent状态”为“在线”。
- 节点的“防护状态”为“未防护”。

开启防护

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > ”，进入云工作负载保护平台页面。

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 在“节点列表”的“操作”列，单击“开启防护”，为需要开启防护的节点开启防护。

步骤5 单击“确定”，开启节点防护，节点的“防护状态”为“已开启”，说明该节点已开启防护。

说明

一个容器安全配额防护一个集群节点。

----结束

14 常见问题

14.1 产品咨询

14.1.1 什么是企业主机安全?

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

工作原理

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

企业主机安全的组件功能及工作流程说明如下：

表 14-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	• 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。

组件	说明
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：10180。 • 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。 • 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、容器安全与主机安全共用同一个Agent，您只需在同一主机安装一次。

14.1.2 什么是容器安全?

容器安全能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、容器文件监控、容器信息收集和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

14.1.3 什么是网页防篡改?

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

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

表 14-2 主机安全防篡改操作流程及功能说明

操作类型	操作	描述与参考
准备工作	--	使用企业主机安全前，若无VDC业务员账号，需要运营管理员创建VDC和VDC管理员，VDC管理员创建VDC业务员。
开通网页防篡改防护	申请防护配额	您需要申请防护配额后，才能开启网页防篡改防护。
	安装Agent	Agent是HSS提供的客户端，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。 安装Agent后，您才能开启网页防篡改防护。

操作类型	操作	描述与参考
	设置告警通知	设置告警通知功能后，您能接收到HSS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，无法收到告警信息。
	开启主机防护	开启主机防护时，您需为指定的主机分配一个配额。
配置网页防篡改防护	添加防护目录	网页防篡改实时监控网站目录，开启网页防篡改前请添加防护目录。
	添加远端备份	HSS默认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，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。
	添加特权进程	开启网页防篡改防护后，防护目录中的内容是只读状态，如果您需要修改防护目录中的文件或更新网站，可以添加特权进程。
	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。
	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。
	查看网页防篡改报告	开启网页防篡改防护后，HSS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。

14.1.4 镜像、容器、应用的关系是什么?

- 镜像是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数（如匿名卷、环境变量、用户等）。镜像不包含任何动态数据，其内容在构建之后也不会被改变。
- 容器和镜像的关系，像程序设计中的实例和类一样，镜像是静态的定义，容器是镜像运行时的实体。容器可以被创建、启动、停止、删除、暂停等。
- 一个镜像可以启动多个容器。
- 应用可以包含一个或一组容器。

14.1.5 HSS 与 WAF 有什么区别?

云平台提供的HSS、WAF服务，帮助您全面从主机、网站、Web应用等层面防御风险和威胁，提升系统安全指数。建议搭配使用。

表 14-3 HSS、WAF 的区别

服务名称	所属分类	防护对象	功能差异
企业主机安全（HSS）	基础安全	提升主机整体安全性。	• 资产管理 • 漏洞管理 • 入侵检测 • 基线检查 • 网页防篡改
Web应用防火墙（WAF）	应用安全	保护Web应用程序的可用性、安全性。	• Web基础防护 • CC攻击防护 • 准确访问防护

14.1.6 什么是 HSS 的 Agent?

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

Agent 的作用

- 每日凌晨定时执行检测任务，全量扫描主机/容器；实时监测主机/容器的安全状态；并将收集的主机/容器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/容器的攻击行为。

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。

Linux Agent 相关进程

Agent进程运行账号：root。

Agent包含以下进程：

表 14-4 Linux 主机 Agent 运行进程

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

Windows Agent 相关进程

Agent进程运行账号：system。

Agent包含以下进程：

表 14-5 Windows 主机 Agent 运行进程

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、Agent进程的守护和监控。	C:\Program Files\HostGuard\HostGuard.exe
HostWatch.exe	该进程用于Agent进程的守护和监控。	C:\Program Files\HostGuard\HostWatch.exe
upgrade.exe	该进程用于Agent升级。	C:\Program Files\HostGuard\upgrade.exe

14.2 Agent 问题

14.2.1 Agent 是否和其他安全软件有冲突?

Agent可能会和DenyHosts这款软件产生冲突。

- 冲突表现：若登录主机的IP地址被识别为攻击IP，但是无法被“解封”。
- 冲突原因：企业主机安全和DenyHosts会同时封禁可能为攻击IP的登录IP地址，企业主机安全无法解封DenyHosts中封禁的IP地址。
- 处理方法：建议停止DenyHosts。
- 操作步骤：
  a. 以**root**用户登录ECS。
  b. 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
     ```

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

14.2.2 如何卸载 Agent?

提供一键卸载和手动本地卸载两种方式。

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。
- 企业主机安全升级Agent失败，需要排查执行Agent卸载。

前提条件

通过控制台一键卸载Agent时，云服务器的“Agent状态”为“在线”。

控制台一键卸载 Agent

用户可以通过企业主机安全控制台直接卸载Agent，方便用户操作。

说明

卸载Agent后企业主机安全将无法为该服务器提供任何防护。

步骤1 登录管理控制台。

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

步骤3 在左侧导航中，选择“安装与配置”，进入“安装与配置”界面。

步骤4 选择“Agent管理 > Agent在线”，在需要卸载Agent的云服务器所在行的“操作”列，单击“卸载Agent”。

步骤5 在弹出的卸载Agent对话框中，单击“确认”。

云服务列表“Agent状态”显示为“离线”，卸载Agent成功。

----结束

主机本地卸载

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

说明

卸载Agent后企业主机安全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**

a. 登录需要卸载企业主机安全Agent的云服务器。
b. 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。

c. 在“HostGuard卸载”提示框中，单击“是”，开始卸载。
d. 卸载完成后单击“确定”。

14.2.3 Agent 安装失败应如何处理?

若为首次安装Agent出现安装失败，请参考本文排查处理。

问题现象

使用命令安装失败，安装Agent后，控制台防护列表页面仍然显示“未安装”。

可能原因

- Selinux防火墙未关闭。
- 安装时未使用root账号安装。
- 安装命令错误。
- 卸载Agent时有残留信息。

解决方案

步骤1 确认是否已关闭主机Selinux防火墙。

- 已关闭：请执行下一步骤。
- 未关闭：请关闭Selinux防火墙后重新安装。

步骤2 请根据主机所在区域、主机操作系统，确认安装命令是否正确。

1. 正确地选择主机所在的区域。
2. 根据主机操作系统复制正确的安装命令。
   - 主机中32位的系统，只能使用32位系统对应的操作命令。
   - 主机中64位的系统，只能使用64位系统对应的操作命令。

- 是：请执行下一步骤。
- 否：请使用正确的命令重新安装。

步骤3 确认安装账号是否为**root**账号。

- 是：请执行下一步骤。。
- 否：请使用root账号重新安装。

步骤4 使用root账号**卸载Agent**后强制安装。

- 安装成功：结束操作。

- 安装失败：请联系技术支持。

----结束

14.2.4 Agent 状态异常应如何处理?

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

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

可能的原因

- 控制台Agent状态未更新。
  安装Agent后，不会立即生效，需要等待5-10分钟左右控制台才会刷新。
- 操作系统不支持。
  HSS目前支持的操作系统请参见产品介绍中使用约束说明。
- 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。

处理方法

步骤1 在主机上安装Agent成功已超过10分钟，控制台Agent状态仍显示“离线”。

- 是：请执行**2**。
- 否：请您耐心等待Agent上线，无需执行后续操作。安装Agent成功后，不会立即生效，需要等待5-10分钟左右控制台才会刷新状态。

步骤2 主机的操作系统是否在产品介绍中使用约束说明范围内。

- 是：请执行**3**。
- 否：企业主机安全的Agent无法正常安装和运行在您的主机上，请升级为企业主机安全支持的操作系统后再尝试安装Agent。

步骤3 主机网络是否正常。

- 是：请执行**4**。
- 否：待主机能正常访问网络后，再查看Agent状态。

步骤4 Agent进程异常，需要重启Agent。

- Windows操作系统
  a. 以管理员**administrator**权限登录主机。
  b. 打开“任务管理器”。
  c. 在“服务”页签选中“HostGuard”。
  d. 单击鼠标右键，选择“重新启动”，完成重启Agent。
- Linux操作系统
  请以**root**用户在命令行终端执行以下命令，完成重启Agent。

service hostguard restart

若回显以下信息，则表示重启成功。

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

重启进程后等待2-3分钟：

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

----结束

14.2.5 Agent 的默认安装路径是什么？

在Linux/Windows操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装在以下路径中，如表14-6所示。

表 14-6 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\HostGuard

14.2.6 Agent 检测时占用多少 CPU 和内存资源？

HSS服务采用轻量级Agent，占用资源极少，不会影响主机系统的正常业务运行。

具体占用的CPU、内存资源如下：

CPU 占用峰值

Agent运行时，CPU占用控制在**1vCPU**的20%以内。因此，实际占用比例与您申请的云服务器规格有关，详见**不同规格主机Agent资源占用一览**。

若CPU占用比例超过1vCPU的20%，Agent会自动降CPU；自动降CPU后，Agent检测主机时间会延长，但不影响服务使用。若CPU占用比例超过1vCPU的25%，Agent将自动重启。

说明

Agent定时检测任务会基于使用地时间在每日00：00-04：00执行，全量扫描主机，不会影响主机系统的正常运行。

内存占用峰值

Agent运行时，内存占用控制在**500MB**以内。若内存占用达到500MB，Agent会在5分钟内自动重启。

不同规格主机 Agent 资源占用一览

Agent运行时，不同规格的云服务器CPU、内存占用情况如表14-7所示。

表 14-7 Agent 资源占用一览

vCPUs规格	Agent运行占用CPU资源比例（峰值）	内存占用（峰值）
1vCPUs	20%	500MB
2vCPUs	10%	500MB
4vCPUs	5%	500MB
8vCPUs	2.5%	500MB
12vCPUs	约1.67%	500MB
16vCPUs	约1.25%	500MB
24vCPUs	约0.84%	500MB
32vCPUs	约0.63%	500MB
48vCPUs	约0.42%	500MB
60vCPUs	约0.34%	500MB
64vCPUs	约0.32%	500MB

14.2.7 网页防篡改、容器安全与主机安全共用 Agent 吗?

是的。

同一服务器安装一次Agent即可满足所有版本的使用。

14.2.8 如何查看未安装 Agent 的主机?

步骤1 登录管理控制台。

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

步骤3 在安装与配置页面，选择“Agent管理 > Agent不在线”页签，查看未安装Agent的云服务器。

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“离线原因”，您可以查看导致Agent不在线的可能原因。

----结束

14.2.9 Agent 安装成功后显示未安装怎么处理?

Agent 使用说明

同一主机Agent成功安装一次即可。

安装成功后，建议重启主机后再执行开启防护及绑定配额操作。

显示未安装原因

目前企业主机安全新版和旧版共存使用，由于一台主机只能安装单一Agent，但主机会在两个平台显示，因此Agent状态及防护情况只能在新版或旧版其中一个平台正常显示，Agent在另一版本则显示未安装。

示例：若A主机已经在旧版console正常安装了Agent，那么在新版console中Agent状态为未安装，此时在新版console安装Agent仍会显示安装成功，但安装后仍会显示未安装。

解决办法

由于Agent对于主机的唯一性，企业主机安全新版和旧版您只能使用一个平台。

若您正在使用旧版，您可通过升级Agent使用新版企业主机安全，整个升级过程均为免费，且不影响业务使用。

说明

目前企业主机安全新版相对于旧版新增了应用防护等能力，建议您使用新版企业主机安全。

14.2.10 ECS 在 Agent 安装以后会访问哪些地址?

云服务器在安装Agent后通常情况会访问的设备、IP、端口如**表14-8**所示。

表 14-8 新装 Agent 访问情况说明

源设备	源IP	源端口	目的设备	目的IP	目的端口（监听）	协议	访问说明	备注
HSS Agent	Agent管理 IP	随机	HSS服务端	HSS服务端-ip1 HSS服务端-ip2	10180	TCP	HSS Agent访问HSS服务端节点，主要是获取服务器端下发的策略/配置/指令、下载Agent软件包/升级包、下载特征库、上报告警事件/资产指纹数据库/基线检查结果和在用户授权许可下上传可疑的可执行程序文件。	每个Region的HSS服务端IP地址不同，Agent通过域名访问，每个Region会有差异，每个Region的具体域名可以通过Agent安装指南中的安装命令看到HSS服务器域名地址。
			元数据服务节点	元数据服务节点IP	80		HSS Agent获取Agent所在服务器的metadata信息，包括获取ECS的uuid、availability_zone、project_id和enterprise_project_id信息。	-

14.3 账户暴力破解问题

14.3.1 HSS 如何拦截暴力破解?

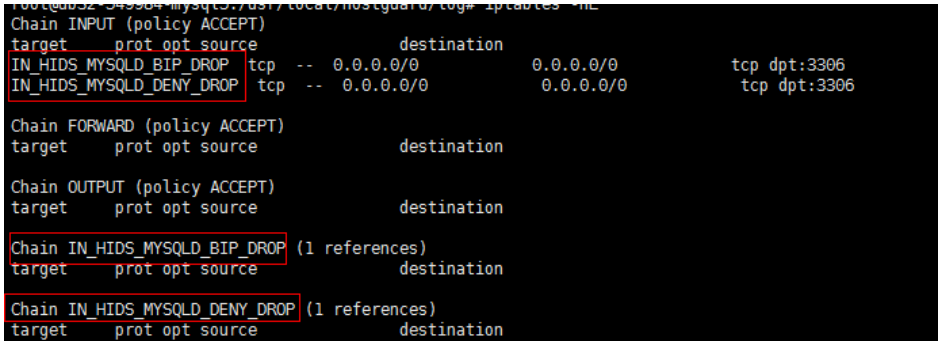
可检测的暴力破解攻击类型

HSS可检测到的暴力破解攻击类型如下：

- Windows系统： SqlServer(暂不支持自动拦截) 、Rdp
- Linux系统：MySQL、vfstp、ssh

若您的服务器上安装了MySQL或者vsftp，开启主机安全防护之后，Agent会在iptables里面新增一些规则，用于MySQL/vsftp爆破防护。当检测到爆破行为后会将爆破IP加入到阻断列表里面，新增的规则如图14-1所示。

图 14-1 新增规则



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。

暴力破解拦截原理

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**。

说明

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

告警策略

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

查看暴力破解检测结果

步骤1 登录管理控制台。

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

步骤3 进入“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。

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

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

说明

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

----结束

处理拦截 IP

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

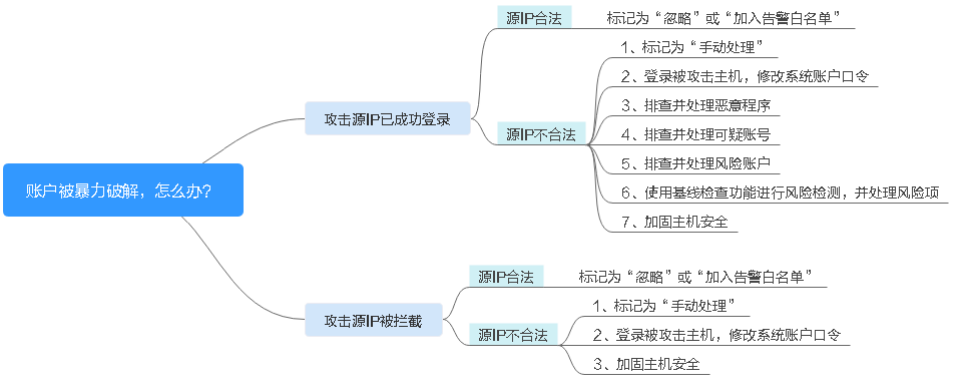
14.3.2 账户被暴力破解，怎么办?

- 若您的主机被暴力破解成功，攻击者很可能已经入侵并登录您的主机，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。
- 若您的主机被尝试暴力破解，攻击源IP被HSS拦截，请及时采取有效的措施预防账户暴力破解事件。

排查思路

以下排查思路按照收到账户暴力破解告警通知的状态进行逐层细化，您可以根据账户暴力破解的实际情况选择对应的分支进行排查。

图 14-2 排查思路



账户被暴力破解，攻击源 IP 已成功登录

若您收到账户暴力破解成功的告警信息，例如**“【账户被爆破告警】企业主机安全当前检测到您XX区域的云服务器XX的账户被破解，已成功登录：攻击源IP：10.108.1.1，攻击类型：ssh”**，则说明您的主机被暴力破解成功，建议您尽快加固您的主机安全。

步骤1 登录管理控制台。

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

步骤3 判断源IP的合法性。

选择“入侵检测 > 安全告警事件”页面，进入“异常登录”页面，查看成功登录主机的源IP是否为合法IP。

- 若源IP合法（多次输错口令，但未达到拦截IP条件，成功登录），您可以单击“处理”，忽略该事件。
- 若源IP不合法，是未知IP，那么您主机系统已经被入侵成功。

  请单击该事件并标记为“手动处理”，并登录被攻击的主机，尽快修改该主机的系统账户口令，口令设置方法请参见**如何设置安全的口令?**

步骤4 排查并处理恶意程序。

选择“恶意程序”排查系统是否被植入了恶意程序。

- 若被植入了恶意程序，请根据检测结果中提示的“恶意程序路径”、“运行用户”、“程序启动时间”等信息，分析、判断哪些确实是恶意程序。

  针对恶意程序，单击恶意程序告警事件，并单击“处理”，选择“隔离查杀”，立即终止恶意程序进程。
- 若没有被植入恶意程序，请执行**步骤8**。

步骤5 排查账号可疑变动记录。

选择“资产管理 > 资产指纹”，排查系统中账号的变动记录是否可疑，防止攻击者创建新的账户或更改账户权限（例如：将某个原来不具备登录权限的账户修改为具备登录权限）。

步骤6 排查并处理非法账号。

选择“入侵检测 > 安全告警事件”中的“非法系统账号”查看所有非法账号的告警，对告警信息进行处理。

步骤7 使用基线检查功能进行风险检测，并根据建议处理风险项。

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

----结束

账户被尝试破解，攻击源 IP 被拦截

如果您为主机开启了主机安全防护，HSS会为您的主机提供暴力破解防护。

您可以通过配置登录安全检测策略限定暴力破解的判断方式和封禁时间。

如果您未配置过登录安全检测策略，登录安全检测策略默认为：如果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侵。

如果您收到了攻击源IP被拦截的告警，请及时确认该源IP是否为可信IP。

约束与限制

- 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。

操作步骤

步骤1 登录管理控制台。

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

步骤3 选择“入侵检测 > 安全告警事件”，选择“暴力破解”，查看账户暴力破解事件。

出现账户暴力破解告警事件，说明您的主机可能存在被暴力破解风险。

- 系统存在弱口令，同时正在遭受暴力破解攻击，攻击IP被拦截。
- 数次口令输错后，源IP被拦截。

步骤4 建议您立即确认源IP是否是已知的合法IP。

- 若源IP合法。
  - 选择账户暴力破解事件，单击“处理”，并标记为“忽略””或者“加入登录白名单”。

    将该事件“忽略”或者“加入登录白名单”，均不会解除拦截的IP。
  - 若需要解除拦截的IP，请单击“已拦截IP”，立即解除拦截的IP，或者当HSS检测到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。

    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。
- 若源IP不合法，是未知IP。

  请选择发生的账户暴力破解事件，单击“处理”，并标记为“手动处理””。

  立即登录主机系统，修改并设置安全的账户密码，并加固您的主机安全。

----结束

相关问题

- **HSS如何拦截暴力破解?**
- **如何手动解除误拦截IP?**

14.3.3 如何预防账户暴力破解攻击?

账户破解风险

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

如何预防

- **配置SSH登录白名单**

  SSH登录白名单功能是防护账户破解的一个重要方式，配置后，只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。

- **开启双因子认证**

  双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次身份认证。

  在“双因子认证”页面，勾选需要开启双因子的主机，单击“开启双因子认证”，开启双因子认证。

- **修改默认端口**

  将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。

- **设置安全组规则，限制攻击源IP访问您的服务端口**

  说明

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

  您可以通过配置安全组规则来限制攻击源IP访问您的服务端口。如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。

  例：仅允许特定IP地址（例如，192.168.20.2）通过SSH协议访问Linux操作系统的弹性云服务器的22端口，安全组规则如下所示：

  表 14-9 仅允许特定 IP 地址远程连接云服务器

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

- **设置安全强度高的口令**

  HSS的基线检查包含口令复杂度策略检测和弱口令检测，可检测出主机系统中使用弱口令的账户，您可以在控制台查看并处理主机中的口令风险。

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

故障原因

主机系统中SSHD服务没有依赖libwrap.so。

说明

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

解决方法

登录云服务器安装企业主机安全Agent，然后执行下面的命令：

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

存在问题的镜像版本

- 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）

14.3.5 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。

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。

手动解除拦截 IP

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“入侵检测 > 安全告警事件 > 主机安全告警”。

步骤4 在安全告警统计栏，单击“已拦截IP”。

步骤5 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。

----结束

14.3.6 频繁收到 HSS 暴力破解告警如何处理?

收到告警事件通知说明您的云服务器被攻击过，不代表已经被破解入侵。您可在收到告警后，及时对告警进行分析、排查，采取相应的防护措施即可。

频繁被暴力破解的可能原因

由于您服务器的远程连接端口没做访问控制，导致网络上的病毒频繁攻击您服务器端口。

处理办法

您可通过以下方式来改善被频繁暴破攻击的情况，降低风险：

- **配置SSH登录白名单**

  SSH登录白名单功能是防护账户破解的一个重要方式，配置后，只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。

- **开启双因子认证**

  双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次身份认证。

  在“双因子认证”页面，勾选需要开启双因子的主机，单击“开启双因子认证”，开启双因子认证。

- **修改默认端口**

  将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。

- **设置安全组规则，限制攻击源IP访问您的服务端口**

  说明

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

  您可以通过配置安全组规则来限制攻击源IP访问您的服务端口。如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。

  例：仅允许特定IP地址（例如，192.168.20.2）通过SSH协议访问Linux操作系统的弹性云服务器的22端口，安全组规则如下所示：

  表 14-10 仅允许特定 IP 地址远程连接云服务器

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

- **设置安全强度高的口令**

  HSS的基线检查包含口令复杂度策略检测和弱口令检测，可检测出主机系统中使用弱口令的账户，您可以在控制台查看并处理主机中的口令风险。

HSS 如何拦截暴力破解?

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

默认情况下，如果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侵。

如果您为主机开启了主机安全防护，您可以通过配置登录安全检测策略限定暴力破解的判断方式和封禁时间。

HSS拦截的IP可在控制台“入侵检测 > 安全告警事件”页面，单击“已拦截IP”上方的数值进行查看。

14.3.7 服务器远程端口已修改，为什么暴力破解记录仍显示旧端口?

问题描述

服务器远程端口已修改，但是暴力破解告警记录中的服务器远程端口仍显示为旧端口。

解决方案

企业主机安全的Agent在启动时才会读取服务器远程端口配置，如果您修改了服务器远程端口，请按如下方式重启Agent。

- Windows：以administrator权限登录主机，在任务管理器中，选中“HostGuard”，单击鼠标右键，选择“重新启动”。
- Linux：以root权限执行**service hostguard restart**命令。

14.4 弱口令和风险账号问题

14.4.1 出现弱口令告警，怎么办?

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

出现弱口令告警的原因

- 设置的自动生成密码的方式过于简单，与弱口令检测的密码库相重合。
- 将同一密码用于多个子账号，会被系统判定为弱密码。

排查弱口令

步骤1 登录管理控制台。

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

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

步骤4 根据经典弱口令列表中的“服务器名称/IP地址”、“账号名称”、“账号类型”和“弱口令使用时长（单位：天）”，登录待修改弱口令的主机，修改弱口令。

----结束

修改常见的服务器弱口令

系统名称	修改登录口令	说明
Windows系统	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  ，弹出“Windows设置”窗口。 3. 在“Windows设置”窗口中，单击“账户”。 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。	无
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 **passwd [<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	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 **SELECT user, host, authentication_string From user;** 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 From user;** 3. 执行以下命令，根据查询结果及弱密码告警信息，修改具体用户的密码。 **SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');** 4. 执行以下命令，刷新修改的密码信息。 **flush privileges;**	无
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 **requirepass <password>;**	● 若已存在登录口令，则将其修改为复杂口令。 ● 若不存在登录口令，则添加为新口令。 **说明** “password”为登录口令。

系统名称	修改登录口令	说明
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

14.4.2 如何设置安全的口令?

请按如下建议设置口令：

- 使用复杂度高的密码。
  建议密码复杂度至少满足如下要求：
  a. 密码长度至少8个字符。
  b. 包含如下至少三种组合：
     i. 大写字母（A~Z）
     ii. 小写字母（a~z）
     iii. 数字（0~9）
     iv. 特殊字符
  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/账号使用不同的密码。
- 根据不同应用设置不同的账号密码，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。
- 账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。
- 新建系统中的账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。

14.4.3 关闭弱口令策略后，之前扫描的弱口令事件为什么还会重复出现?

若您在关闭弱口令策略前，已经修改弱口令事件，进行重新检测并符合弱口令检测要求，该弱口令事件不会在重复出现。

若您在关闭弱口令策略前，未修改弱口令事件，已经检测出来的结果不会改变，系统也将不再进行新的检测且历史检测结果会保留30天。

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

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

14.5 入侵告警问题

14.5.1 主机被挖矿攻击，怎么办?

黑客入侵主机后植入挖矿程序，挖矿程序会占用CPU进行超高运算，导致CPU严重损耗，并且影响主机上其他应用的运行。当您的主机被挖矿程序入侵，挖矿程序可能进行内网渗透，并在被入侵的主机上持久化驻留，从而获取最大收益。

当主机提示有挖矿行为时，请确定并清除挖矿程序，并及时对主机进行安全加固。

排查操作步骤

步骤1 登录管理控制台。

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

步骤3 排查进程异常行为，若出现主机挖矿行为，会触发HSS发送“进程异常行为”告警。

选择“入侵检测 > 安全告警事件 > 主机安全告警 ”，选择“系统异常行为 > 进程异常行为”，查看并处理发生的异常进程行为告警。您可以单击“处理”，对挖矿程序进行隔离查杀。

步骤4 排查其他自启动项，有的挖矿进程为了实现长期驻留，会向系统中添加自启动项来确保系统重启后仍然能重新启动，因此，需要及时清除可疑的自启动项。

选择“资产管理 > 资产指纹”，单击“自启动项”，选择“历史变动记录”，查看历史变动情况。

----结束

主机安全加固

挖矿程序清除后，为了保障主机安全，请及时对主机进行安全加固。

Linux加固建议

1. 使用HSS**每日凌晨**自动进行一次全面的检测，帮助您深度防御主机和应用方面潜在的安全风险。
2. 修改系统所有账号口令（包括系统账户和应用账户）为符合规范的强口令，或将主机登录方式改为密钥登录彻底规避风险。
   a. 设置安全口令，详细操作请参见**如何设置安全的口令？**。
   b. 使用密钥登录主机。
3. 严格控制系统管理员账户的使用范围，为应用和中间件配置各自的权限和并严格控制使用范围。
4. 使用安全组定义访问规则，根据业务需求对外开放端口，对于特殊业务端口，建议设置固定的来源IP（如：远程登录）或使用VPN、堡垒机建立自己的运维通道。

Windows加固建议

使用HSS全面体检并深度防御主机和应用方面潜在的安全风险，同时您还可以对您的Windows系统进行账户安全加固、口令安全加固和授权安全加固。

- **账户安全加固**

账户	说明	操作步骤
默认账户安全	• 禁用Guest用户 • 禁用或删除其他无用账户（建议先禁用账户三个月，待确认没有问题后删除）	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组 > 用户”。 4. 双击**Guest**用户，在弹出的Guest属性窗口中，勾选“账户已禁用”。 5. 单击“确定”，完成Guest用户禁用。
按照用户分配账户	根据业务要求，设定不同的用户和用户组。 例如，管理员用户，数据库用户，审计用户等。	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组”，根据业务要求，设定不同的用户和用户组，包括管理员用户，数据库用户，审计用户等。
定期检查并删除无关账户	定期删除或锁定与设备运行、维护等与工作无关的账户。	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组”。 4. 单击“用户”或者“用户组”，在用户或者用户组页面，删除或锁定与设备运行、维护等与工作无关的账户。

账户	说明	操作步骤
不显示最后的用户名	配置登录登出后，不显示用户名称。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 安全选项”。 4. 双击“交互式登录：不显示最后的用户名”。 5. 在弹出的“交互式登录：不显示最后的用户名”属性窗口中，选择“启用”，并单击确定。

- **口令安全加固**

口令	说明	操作步骤
复杂度	必须满足**如何设置安全的口令**的要求。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 密码策略”。 4. 确认“密码必须符合复杂性要求”已启用。
密码最长留存期	对于采用静态口令认证技术的设备，账户口令的留存期不应长于90天。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 密码策略”。 4. 配置“密码最长使用期限”不大于90天。
账户锁定策略	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次后，锁定该用户使用的账户。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 账户锁定策略”。 4. 配置“账户锁定阈值”不大于10次。

- **授权安全加固**

授权	说明	操作步骤
远程关机	在本地安全设置中，从远端系统强制关机权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“从远端系统强制关机”，权限只分配给Administrators组。

授权	说明	操作步骤
本地关机	在本地安全设置中关闭系统权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“关闭系统”，权限只分配给Administrators组。
用户权限指派	在本地安全设置中，取得文件或其它对象的所有权的权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“取得文件或其他对象的所有权”，权限只分配给Administrators组。
授权账户登录	在本地安全设置中，配置指定授权用户允许本地登录此计算机。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“允许本地登录”，权限给指定授权用户。
授权账户从网络访问	在本地安全设置中，只允许授权账号从网络访问（包括网络共享等，但不包括终端服务）此计算机。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“从网络访问此计算机”，权限给指定授权用户。

14.5.2 添加告警白名单后，为什么进程还是被隔离?

告警白名单仅用于忽略告警，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。

隔离查杀恶意程序

- 方式一：在“安装与配置 > 安全配置 > 恶意程序隔离查杀”中，开启自动隔离查杀。
- 方式二：在“入侵检测 > 安全告警事件 > 主机安全告警 > 事件列表”中，将恶意程序手动隔离查杀。

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。

恢复隔离查杀文件

- 在“入侵检测 > 安全告警事件 > 已隔离文件”中，选择“主机安全告警”，单击“已隔离文件”的“查看详情”，单击目标服务器的“恢复”，恢复隔离文件。

被隔离查杀的程序恢复隔离后，文件的“读/写”权限将会恢复，但被终止的进程不会再自动启动起来。

14.5.3 提示主机有挖矿行为怎么办?

当主机提示有挖矿行为时：

1. 建议备份数据，关闭不必要的端口。
2. 增强主机密码。
3. 使用企业主机安全（HSS），HSS提供账户破解防护、异地登录检测恶意程序检测、网站后门检测等入侵检测功能，以及软件漏洞、一键查杀恶意程序或修复系统漏洞等功能。

14.5.4 服务器遭受攻击为什么没有检测出来?

- 若您的主机在开启HSS之前已被入侵，HSS可能无法检测出来。
- 若您申请了企业主机安全配额但是没有开启防护，HSS无法检测出来。
- HSS主要是防护主机层面的攻击，若攻击为web层面攻击，无法检测出来。建议咨询安全SA提供安全解决方案，或者推荐使用安全的其他产品（WAF，DDOS等）。

14.5.5 源 IP 被 HSS 拦截后，如何解除?

源IP被账户暴力破解、源IP隶属于全网IP黑名单，以及开启IP白名单后，源IP不在IP白名单中时，均会被拦截，请根据具体场景解除拦截。

账户暴力破解

- 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**。
- 若您确认源IP是可信的IP（比如运维人员因为记错密码，多次输错密码导致被封禁），可单击“入侵检测 > 安全告警事件”页面下“已拦截IP”的“查看详情”，在弹出的页面，可手动解除被拦截的可信IP。

  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。若再次发生多次口令输错，该IP会再次被HSS拦截。

全网 IP 黑名单

不能手动解除拦截。

14.5.6 没有手动解除的 IP 拦截记录为什么会显示已解除?

如果被拦截的IP在24小时内没有再继续暴力破解就会自动解除IP。

14.5.7 HSS 的恶意程序检测周期、隔离查杀是多久一次?

检测周期：实时检测。

隔离查杀周期：

- 已开启自动隔离查杀：系统实时查杀（出现告警，立刻自动查杀）。

- 未开启自动隔离查杀：需人工查杀，逐一处理。

须知

1. HSS的隔离查杀支持对“恶意程序（云查杀）”和“进程异常行为”实时检测的告警进行查杀，检测能力详情请参见服务版本差异。
2. HSS隔离查杀分为自动隔离查杀和人工隔离查杀。
   - 开启自动隔离查杀：详情请参见安全配置中的“开启恶意程序隔离查杀”章节。
   - 人工隔离查杀：操作详情请参见管理文件隔离箱中的“选择隔离查杀”章节。

14.5.8 HSS 拦截的 IP 是否需要处理?

在收到有拦截IP的告警时，需要您对拦截的IP进行判断，被拦截IP是否为正常业务所使用。

- 如果是您正在使用的业务所属IP，您需将拦截IP添加至白名单。
- 如果是非正常业务所使用，则无需处理。

14.5.9 如何防御勒索病毒攻击?

勒索病毒一般通过挂马、邮件、文件、漏洞、捆绑、存储介质进行传播。

因此在云服务器使用期间可通过**预防帐户暴力破解攻击的措施**，及时对企业主机安全检测发现的告警进行处理，通常可以达到防止勒索病毒入侵的。

14.6 异常登录问题

14.6.1 添加登录白名单后，为什么还有异地登录告警?

HSS提供的“SSH登录IP白名单”、“登录白名单”和“异地登录”功能，功能差异如**表14-11**所示。

表 14-11 功能差异

功能名称	实现机制	屏蔽告警
SSH登录IP白名单	将IP加入SSH登录IP白名单，只允许白名单内的IP通过SSH登录指定服务器。 **须知** 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。	-
登录白名单	将IP加入登录白名单，用于忽略由该IP登录指定主机发生的账户暴力破解告警事件。	在“入侵检测 > 白名单管理 > 登录白名单”将IP加入登录白名单，HSS将不会对该IP的“账户暴力破解”登录事件进行告警。

功能名称	实现机制	屏蔽告警
异地登录	当不是来自“常用登录地”或者“常用登录IP”的登录行为时，将会进行异地登录告警。 提醒您有新的IP登录您的主机。	在“安装与配置 > 安全配置”中，将登录地与登录IP添加到“常用登录地”与“常用登录IP”，HSS将不会对来自“常用登录地”和“常用登录IP”的登录行为进行异地告警。

14.6.2 如何查看异地登录的源 IP?

告警策略

异地登录检测功能**实时检测**您服务器上的异地登录行为，您配置常用登录地后，对于在非常用登录地的登录行为HSS会立即进行告警。

在控制台查看异地登录记录

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“入侵检测 > 安全告警事件> 主机安全告警”，进入主机安全告警页面。

步骤4 在事件类型栏选择“用户异常行为 > 异常登录”，单击告警名称“异地登录”查看详情。

----结束

本地查看登录记录

对于linux主机，您可以在“/var/log/secure”和“/var/log/message”路径下查看日志，或使用**last**命令查看登录记录中是否有异常登录。

14.6.3 收到主机登录成功的告警，怎么处理?

- 若您在“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。
- 若您所有ECS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。
- 若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主机安全控制台关闭该告警项。
- 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。

14.6.4 是否可以关闭异地登录检测?

不可以关闭异地登录检测。

如果不想接收异地登录的告警通知，您可以将登录地点添加到常用登录地，或者取消勾选告警通知，操作步骤如下所示。

- 在“常用登录地”页面，单击“添加常用地登录”，将登录地点添加到常用登录地。添加到常用登录地的登录行为，HSS不会进行异地登录告警。
- 在“安装与配置 > 告警通知”页签，在屏蔽事件中勾选“异常登录”。

  异常登录包含异地登录、发生账户被黑客破解并登录成功事件。如果勾选“异常登录”告警通知的选项，当发生账户被黑客暴力破解时，您将不能实时接收到账户破解的告警通知，请谨慎操作。

14.6.5 如何确认入侵账号是否登录成功?

- 若已开启入侵检测告警通知，当有账号被破解，或有账号破解风险时，您会立即收到告警通知。
- 也可以在“入侵检测”页面在线查看攻击IP的拦截情况。
- 若想进一步确定，可以在Linux主机上的“/var/log/secure”和“/var/log/message”查看日志，或使用**last**命令查看是否有异常登录记录。

14.7 配置风险问题

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

安装 PAM

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

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

说明

CentOS、Fedora、EulerOS系统默认安装了PAM并默认启动。

设置口令复杂度策略

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

说明

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

- 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统

  man pam_pwquality
- 其他Linux系统

  man pam_cracklib

- CentOS、Fedora、EulerOS操作系统

  a. 执行以下命令，编辑文件“/etc/pam.d/system-auth”。

  vi /etc/pam.d/system-auth

b. 找到文件中的以下内容。

- 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统：
  password requisite pam_pwquality.so try_first_pass retry=3 type=
- 其他CentOS、Fedora、EulerOS系统：
  password requisite pam_cracklib.so try_first_pass retry=3 type=

c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表14-12所示。

示例：

password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

说明

“dcredit”、“ucredit”、“lcredit”、“ocredit”中均需要配置为负数。

表 14-12 参数说明

参数	说明	示例
minlen	口令最小长度配置项。 若需要设置最小口令长度为8，则minlen的值应该设置为8。	minlen=8
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”。
vi /etc/pam.d/common-password

b. 找到文件中的以下内容：
password requisite pam_cracklib.so retry=3 minlen=8 difok=3

c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表14-12所示。

示例：

password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

14.7.2 如何在 Windows 主机上设置口令复杂度策略?

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

设置本地安全策略中的账户策略步骤如下：

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

说明

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

步骤2 选择“账户策略 > 密码策略”后执行以下操作。

- 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。

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

----结束

14.7.3 如何处理配置风险?

企业主机安全对主机执行配置检测后，您可以根据检测结果中的相关信息，修复主机中含有风险的配置项或忽略可信任的配置项。

- 修改有风险的配置项

  查看检测规则对应的详情信息，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。

- 忽略可信任的配置项

  a. 单击云服务器名称，查看服务器的详细信息，选择“基线检查 > 配置检查”。

  b. 单击目标风险项前的 展开检查项，单击目标风险项“操作”列的“忽略”进行单个忽略。也可以勾选多个检测规则单击界面上方的“忽略”进行批量忽略。

  对于已经忽略的检测规则，单击已忽略页签可“取消忽略”，也可以批量选中想要取消忽略的规则“取消忽略”。

- 修复验证

完成配置项的修复后，建议您在“风险预防 > 漏洞管理”页面单击“漏洞检测”立即执行手动检测，查看配置项修复结果。

14.7.4 如何查看配置检查的报告?

支持在线查看配置检查的检测详情。

操作步骤

步骤1 在“配置检查”页面，单击配置检查基线名称。

步骤2 在检测规则详情页面，单击“检测详情”。

步骤3 您可以根据配置检测报告中的描述信息和修改建议，修复主机中含有风险的配置项或忽略可信任的配置项。

----结束

14.8 漏洞管理

14.8.1 如何处理漏洞?

处理方法和步骤

步骤1 查看漏洞检测结果。

步骤2 按照漏洞检测结果给出的漏洞修复紧急度和解决方案逐个进行修复漏洞。

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

步骤3 企业主机安全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验证，核实修复结果。

----结束

14.8.2 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：

说明

建议您参考漏洞修复与验证章节对您服务器上的漏洞进行修复。

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**修复命令**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。

  表 14-13 验证修复命令

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

- **内核漏洞修复后，未重启主机**

  内核漏洞修复完成后，需要重启主机，不重启主机漏洞仍会显示存在。

14.8.3 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。

14.8.4 漏洞修复完毕后是否需要重启主机?

“Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后，需要重启服务器，重启服务器后漏洞修复才会生效，否则企业主机安全仍认为您的漏洞未完成修复，将持续为您告警。其他类型的漏洞修复后，则无需重启服务器

14.8.5 HSS 如何查询漏洞、基线已修复记录?

查看已修复漏洞

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中选择“风险预防 > 漏洞管理”，进入“漏洞管理”页面

步骤4 在各类漏洞页签，筛选查看已修复的漏洞。

须知

漏洞仅在漏洞列表保留展示七天，因此您只能查看最近七天已修复的漏洞。

----结束

查看已修复基线

口令复杂度策略、经典弱口令风险项修复后，不支持查看历史修复记录。您可以参考本小节查看已修复的配置检查项。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中选择“风险预防 > 基线检查”，进入“基线检查”页面

步骤4 选择“配置检查”页签。

步骤5 单击基线名称，进入基线详情页。

步骤6 选择“检查项 > 已通过”页签，查看已修复的检查项。

----结束

14.8.6 漏洞修复失败怎么办?

如果在企业主机安全控制台修复Linux和Windows系统漏洞时失败，请参考本文进行排查处理。

查看漏洞修复失败原因

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在“漏洞管理”界面右上角，单击“任务管理”，进入任务管理页面。

步骤5 选择“修复任务”页签，查看漏洞修复结果。

- ：该图标旁显示的数字，表示修复成功的服务器数量。
- ：该图标旁显示的数字，表示修复失败的服务器数量。

步骤6 单击图标，在修复失败详情对话框中，查看修复失败的“失败原因”和“原因说明”。

您可以根据失败原因处理漏洞修复失败问题。

----结束

14.8.7 手动扫描漏洞或批量修复漏洞时，为什么选不到目标服务器?

问题原因

在手动扫描漏洞或批量修复漏洞时，以下服务器不能被选中执行漏洞扫描或修复操作：

- 使用企业主机安全“基础版”的服务器。
- 非“运行中”状态的服务器。
- Agent状态为“离线”的服务器。

解决办法

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“资产管理 > 主机管理”，进入“主机管理”页面。

步骤4 在“云服务器”页签，查看服务器的运行状态、Agent状态以及服务器使用的企业主机安全版本。

确认相关信息后，请参考如下方式处理问题：

- 使用企业主机安全“基础版”的服务器。

  企业主机安全基础版不支持手动扫描漏洞和修复漏洞功能，如果您需要使用手动扫描漏洞和修复漏洞功能或更多企业主机安全功能，您可以升级企业主机安全版本。

- 非“运行中”状态的服务器。

  请排查服务器状态，确保服务器状态为“运行中”。

- Agent状态为“离线”的服务器。

  Agent离线后，无法接收控制台下发的指令，请参考**Agent状态异常应如何处理?**，使Agent恢复为“在线”状态。

步骤5 在左侧导航栏选择“风险预防 > 漏洞管理”，进入漏洞管理页面，重新手动扫描漏洞或批量修复漏洞，目标服务器能勾选即表示问题解决。

----结束

14.9 网页防篡改常见问题

14.9.1 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。

14.9.2 如何修改防护目录?

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面。

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

步骤5 单击“设置”，在右侧的“防护目录设置”页面中，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。

步骤6 在“编辑防护目录”弹框中进行修改，单击“确认”完成修改。

----结束

14.9.3 无法开启网页防篡改怎么办?

可能的原因及解决方法如下：

Agent 状态异常

- **现象**

  网页防篡改页面防护列表中“Agent状态”为“离线”或者“未安装”。

- **解决方法**

  请参见Agent状态异常进行处理，确保主机列表中“Agent状态”为“在线”。

开启了基础版/企业版/旗舰版防护

- **现象**

  企业主机安全页面主机列表中“防护状态”为“开启”。

- **解决方法**

  请先关闭主机防护，再开启网页防篡改。

  说明

  主机防护包含基础版、企业版、旗舰版以及网页防篡改版防护。如果已开启基础版、企业版或者旗舰版防护，需要先关闭主机防护，才能开启网页防篡改。

位置选择错误

请在“网页防篡改 > 防护列表”页面开启防护。

说明

申请企业主机安全“网页防篡改版”后，您可以使用“旗舰版”中的所有功能，此时您只能通过“网页防篡改”页面开启防护，当开启网页防篡改防护时会同步开启旗舰版防护。

14.9.4 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：

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。

14.9.5 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。

14.9.6 HSS 与 WAF 的网页防篡改有什么区别?

HSS网页防篡改版是专业的锁定文件不被修改，实时监控网站目录，并可以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，是政府、院校及企业等组织必备的安全服务。

WAF网页防篡改为用户提供应用层的防护，对网站的静态网页进行缓存，当用户访问网站时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网页防篡改的区别

HSS与WAF网页防篡改的区别，如**表14-14**所示。

表 14-14 HSS 和 WAF 网页防篡改的区别

类别	HSS	WAF
静态网页	• 锁定驱动文件、Web文件 锁定驱动级文件目录、Web文件目录下的文件，禁止攻击者修改。 • 特权进程管理 配置特权进程白名单后，网页防篡改功能将主动放行可信任的进程，确保正常业务进程的运行。	• 缓存服务端静态网页 • 不支持特权进程管理
动态网页	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。	不支持
备份恢复	• 主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。 • 远端备份恢复 若本地主机上的文件目录和备份目录失效，可通过远端备份服务恢复被篡改的网页。	不支持
防护对象	网站防护要求高，手动恢复篡改能力差	网站防护要求低，仅需要对应用层进行防护

如何选择网页防篡改

防护对象	选择网页防篡改
普通网站	WAF网页防篡改+HSS企业版
网站防护+高要求网页防篡改	WAF网页防篡改+HSS网页防篡改

14.10 容器安全常见问题

14.10.1 如何关闭节点防护?

操作须知

关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 根据需求可选择批量关闭防护和单服务器关闭防护。

- **单服务器关闭防护**
  a. 在“节点列表”中目标服务器的“操作”列单击“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。
  c. 关闭后在“资产管理 > 容器管理 > 节点列表”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

  ⚠ 注意

  关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

- **批量关闭防护**
  a. 在“节点列表”中勾选多个目标服务器前的选框，单击上方“关闭防护”。
  b. 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。
  c. 关闭后在“资产管理 > 容器管理 > 节点列表”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

  ⚠ 注意

  关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。

----结束

14.10.2 容器安全的日志处理机制是什么?

容器安全每隔10分钟更新一次log文件，如果文件大于30M，则将最近30M的日志信息写入对应的日志备份文件，当前日志文件内容清空。

日志备份文件的文件名为日志源文件名加上“ .last ”后缀，如 “shield.log”的备份文件为 “shield.log.last”。

14.10.3 容器安全如何切换至企业主机安全控制台?

您可将原容器安全迁移至企业主机安全控制台实现服务器负载的统一管理，同时可享受新增的功能特性。

新版&旧版功能说明

目前容器安全服务已整合至企业主机安全控制台进行统一管理，优化了既有功能的能力，同时新增了部分新功能。

表 14-15 新版&旧版 CGS 功能说明

功能项	CGS旧版（原CGS）	CGS新版（HSS新版）
容器资产指纹管理	×	√
容器节点管理	√	√
私有镜像管理	√	√
本地镜像管理	√	√
官方镜像管理	√	×
共享镜像管理	×	√
镜像漏洞检测	√	√
镜像恶意文件检测	√	√
镜像基线检查	√	√
漏洞逃逸攻击	√	√
文件逃逸攻击	√	√
容器进程异常	√	√
容器配置异常	√	√
容器异常启动	√	√
容器恶意程序	√	√
高危系统调用	√	√
敏感文件访问	√	√
容器软件信息	√	√
容器文件信息	√	√
白名单管理	√	√
容器策略管理	√	√

切换流程

将CGS整体切换至HSS的过程需要您先关闭原CGS、再申请HSS容器版本并开启防护即可。

步骤一：关闭原 CGS 防护

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 容器安全服务”，进入容器安全服务平台界面。

步骤3 进入容器安全“防护列表”，查看集群防护列表。

步骤4 单击目标集群“操作”列的“关闭防护”，释放集群防护状态。

说明

为了方便管理，建议将所有集群的防护都进行关闭。

----结束

步骤二：安装 Agent

旧版CGS与HSS新版是独立存在的，因此在HSS开启容器版防护需要不同的Agent。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 在“节点列表”中查看已关闭防护的节点是否在列表中存在。

须知

- 若在HSS新版console查看已有，则无需安装Agent。
- 若在HSS新版console查看没有，则需要重新在HSS新版控制台。

----结束

步骤三：开启防护

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入“容器节点管理”页面。

步骤4 在“节点列表”中单击目标服务器“操作”列的“开启防护”，为需要开启防护的节点开启防护。

步骤5 单击“确定”，开启节点防护，目标服务器“容器防护状态”变更为“防护中”，说明该节点已开启防护。

说明

一个容器安全配额防护一个集群节点。

----结束

14.10.4 如何开启节点防护?

开启节点防护的同时，系统会自动为该节点安装容器安全插件。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入容器管理界面。

步骤4 在节点列表的“操作”列，单击“开启防护”，为需要开启防护的节点开启防护。

步骤5 单击“确定”，开启节点防护，节点的“防护状态”为“已开启”，说明该节点已开启防护。

说明

- 一个企业主机安全配额防护一个集群节点。

----结束

14.10.5 自建 k8s 容器如何开启 apiserver 审计功能?

适用场景

用户自建k8s容器。

前提条件

- 已开启容器防护。
- 已确认apiserver审计功能未开启，确认步骤如下：
  a. 登录到kube-apiserver所在的节点。
  b. 查看kube-apiserver.yaml文件或者已经启动的kube-apiserver进程。
     - 进入/etc/kubernetes/manifest目录，查看kube-apiserver.yaml中是否存在--audit-log-path和--audit-policy-file，不存在即表示apiserver审计功能未正常开启。
     - 执行**ps**命令，查看kube-apiserver的进程命令行中是否存在--audit-log-path和--audit-policy-file，不存在即表示apiserver审计功能未正常开启。

开启 apiserver 审计功能

步骤1 将以下yaml内容复制并保存至yaml文件，并将yaml文件命名为“audit-policy.yaml”。

该yaml内容为k8s审计功能的配置文件，您可以直接使用或者根据实际业务情况编写。

```
apiVersion: audit.k8s.io/v1 # This is required.
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  # Kube-Proxy running on each node will watch services and endpoint objects in real time
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
```



```
    - group: "" # core
      resources: ["endpoints", "services"]
 # Some health checks
 - level: None
   users: ["kubelet"] # legacy kubelet identity
   verbs: ["get"]
   resources:
     - group: "" # core
       resources: ["nodes"]
 - level: None
   userGroups: ["system:nodes"]
   verbs: ["get"]
   resources:
     - group: "" # core
       resources: ["nodes"]
 - level: None
   users: ["system:apiserver"]
   verbs: ["get"]
   resources:
     - group: "" # core
       resources: ["namespaces"]
 # Some system component certificates reuse the master user, which cannot be accurately distinguished
from user behavior,
 # considering that subsequent new functions may continue to add system operations under kube-system,
the cost of targeted configuration is relatively high,
 # in terms of the overall strategy, it is not recommended (allowed) for users to operate under the kube-
system,
 # so overall drop has no direct impact on user experience
 - level: None
   verbs: ["get", "update"]
   namespaces: ["kube-system"]
 # Don't log these read-only URLs.
 - level: None
   nonResourceURLs:
     - /healthz*
     - /version
     - /swagger*
 # Don't log events requests.
 - level: None
   resources:
     - group: "" # core
       resources: ["events"]
 # Don't log leases requests
 - level: None
   verbs: [ "get", "update" ]
   resources:
     - group: "coordination.k8s.io"
       resources: ["leases"]
 # Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
 # so only log at the Metadata level.
 - level: Metadata
   resources:
     - group: "" # core
       resources: ["secrets", "configmaps"]
     - group: authentication.k8s.io
       resources: ["tokenreviews"]
 # Get responses can be large; skip them.
 - level: Request
   verbs: ["get", "list", "watch"]
   resources:
     - group: "" # core
     - group: "admissionregistration.k8s.io"
     - group: "apps"
     - group: "authentication.k8s.io"
     - group: "authorization.k8s.io"
     - group: "autoscaling"
     - group: "batch"
     - group: "certificates.k8s.io"
     - group: "extensions"
```



```
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
 # Default level for known APIs
 - level: RequestResponse
   resources:
    - group: "" # core
    - group: "admissionregistration.k8s.io"
    - group: "apps"
    - group: "authentication.k8s.io"
    - group: "authorization.k8s.io"
    - group: "autoscaling"
    - group: "batch"
    - group: "certificates.k8s.io"
    - group: "extensions"
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
 # Default level for all other requests.
 - level: Metadata
```

步骤2 将audit-policy.yaml文件上传至/etc/kubernetes/路径下。

步骤3 进入/etc/kubernetes/manifests目录，将以下内容填写至配置文件kube-apiserver.yaml中，开启apiserver审计功能。

```
--audit-policy-file=/etc/kubernetes/audit-policy.yaml
--audit-log-path=/var/log/kubernetes/audit/audit.log
--audit-log-maxsize=100
--audit-log-maxage=1
--audit-log-maxbackup=10
```

说明

- --audit-policy-file：指定审计功能所使用的配置文件。
- --audit-log-path：指定用来写入审计事件的日志文件路径。不指定此标志会禁用日志后端。
- --audit-log-maxsize：定义审计日志文件轮转之前的最大大小（兆字节）。
- --audit-log-maxage：定义保留旧审计日志文件的最大天数。
- --audit-log-maxbackup：定义要保留的审计日志文件的最大数量。
- 将上述启动参数填写至配置文件kube-apiserver.yaml时，注意与kube-apiserver.yaml中的启动参数格式保持一致，且不能存在制表符（tab）。

步骤4 （可选）如果您的kube-apiserver是以Pod形式存在，请按如下步骤将审计日志持久化到主机上。

1. 在kube-apiserver.yaml中找到volumeMounts字段，按如下配置挂载数据卷。

```
volumeMounts:
  - mountPath: /etc/kubernetes/audit-policy.yaml
    name: audit
    readOnly: true
  - mountPath: /var/log/kubernetes/audit/
    name: audit-log
    readOnly: false
```

2. 在kube-apiserver.yaml中找到volumes字段，按如下配置挂载。

```
volumes:
- name: audit
  hostPath:
    path: /etc/kubernetes/audit-policy.yaml
    type: File
- name: audit-log
  hostPath:
```



```
path: /var/log/kubernetes/audit/
type: DirectoryOrCreate
```

----结束

14.11 安全配置问题

14.11.1 如何清除 HSS 中配置的 SSH 登录 IP 白名单?

您可以“禁用”或者“删除”配置的SSH登录IP白名单。

清除 SSH 登录 IP 白名单

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“安装与配置”，进入安装与配置页面，选择“安全配置 > SSH登录IP白名单”，进入“SSH登录IP白名单”页签。

步骤4 在目标白名单IP所在行的“操作”列单击“禁用”或者“删除”，清除配置的SSH登录IP白名单。

----结束

14.11.2 不能通过 SSH 远程登录主机，怎么办?

问题现象

可以通过管理控制台登录到主机，但是无法通过SSH远程登录主机。

可能原因

- 因账户暴力破解（例如：输入密码错误次数过多，30秒内，错误次数达到5次及以上），导致主机IP被拦截。
- 开启了SSH登录IP白名单，但需要通过SSH登录主机的IP没有添加到IP白名单。

  开启SSH登录IP白名单后，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。

解决方案

步骤1 确认是否因为账户暴力破解，导致主机IP被拦截。

- 是，请到“事件管理”页面，单击“已拦截IP”，解除IP的拦截。
- 否，请执行**步骤2**。

步骤2 确认是否已开启SSH登录白名单，且登录主机的IP没有添加到IP白名单。

- 是，将登录主机的IP加入到SSH登录IP白名单。
- 否，请联系技术支持工程师。

----结束

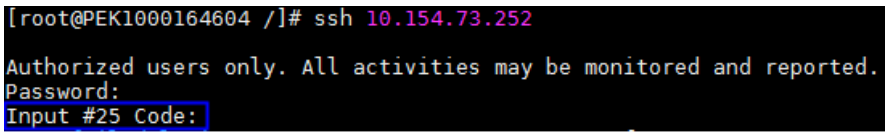
14.11.3 如何使用双因子认证?

本章节指导用户如何使用双因子认证。

登录与使用

- 登录Linux主机
  a. 使用PuTTY/Xshell登录云主机。
     登录时，请选择“Keyboard Interactive”，输入用户身份验证。
     - PuTTY
       身份验证方法选择“Keyboard Interactive”，并单击“确定”。
     - Xshell
       在会话属性框中，选择“连接 > 用户身份验证 > 方法”，单击“方法”下拉选项，选择“Keyboard Interactive”，单击“确定”。
  b. 输入云主机的账户与密码。
  c. 开启双因子认证后，需输入订阅终端接收到的验证码。

     图 14-3 输入验证码

- 登录Windows主机
  a. 单击“开始”菜单，在搜索栏中输入“远程桌面连接”，按“Enter”，打开远程桌面连接。
  b. 在“计算机”栏输入云主机的IP地址，并单击“连接”。
  c. 若已开启双因子认证，需要输入预留手机号或邮箱，单击“获取验证码”。
  d. 获取验证码后，在登录界面输入验证码、云主机账号和密码，单击，登录云主机。

14.11.4 开启双因子认证失败，怎么办?

问题现象

- 在双因子认证列表下，没有待开启双因子认证的主机。
- 开启双因子认证后，不生效。
- 开启双因子认证失败。

可能原因

- 主机未开启防护。
- 开启双因子认证不会立即生效，需要等大约5分钟才生效。
- Linux主机没有关闭“密钥对”登录方式。
- 没有关闭Selinux防火墙。

解决方案

步骤1 确认待开启双因子认证的主机，是否已开启主机安全防护。

- 是：请执行**步骤2**。
- 否：请将待开启双因子认证的主机开启主机安全防护。

步骤2 确认开启双因子认证后，是否已等待5分钟。

- 是：请执行**步骤3**。
- 否：请等待5分钟后，再确认开启的双因子认证是否生效。

步骤3 确认是否为Linux主机，且使用“密钥对”方式登录。

- 是：请关闭“密钥对”登录方式，开启“密码”登录方式。
- 否：请执行**4**。

步骤4 确认主机是否已关闭Selinux防火墙。

- 是：请执行**步骤5**。
- 否：请执行以下命令，关闭Selinux防火墙。
  - 临时关闭Selinux防火墙。
    setenforce 0 #临时关闭
  - 永久关闭Selinux防火墙。
    vi /etc/selinux config
    selinux=disabled #永久关闭

步骤5 请联系技术支持。

----结束

14.11.5 开启双因子认证后收不到验证码?

- 开启双因子认证功能后，不会立即生效。
  需要等大约5分钟才生效。
- 开启双因子认证需要关闭Selinux防火墙。
  请**关闭Selinux防火墙**后重试。
- Linux主机需要使用“密码”登录方式。
  请按以下步骤切换密钥登录为密码登录：
  a. 使用密钥登录Linux云服务器，设置root密码。
     sudo passwd root
     若密钥文件丢失或损坏，请重置root密码。
  b. 使用root身份编辑云服务器的ssh登录方式。
     su root
     vi /etc/ssh/sshd_config
     修改如下配置项：
     - 把PasswordAuthentication no 改为 PasswordAuthentication yes
       或去掉PasswordAuthentication yes 前面的#注释掉。

- 把PermitRootLogin no 改为 PermitRootLogin yes
  或去掉PermitRootLogin yes 前面的#注释掉。

c. 重启sshd使修改生效。
   service sshd restart
d. 重启云服务器就可以使用root用户和新设置的密码登录了。

说明

防止非授权用户使用原来的密钥文件访问Linux云服务器，请将/root/.ssh/authorized_keys文件删除或清空authorized_keys文件内容。

14.11.6 为什么开启双因子认证后登录主机失败?

登录主机失败的原因可能为文件配置错误或登录方式错误导致。

文件配置错误

您可检查配置文件是否正确。

配置文件路径：/etc/ssh/sshd_config

需要确认的配置文件项：

PermitEmptyPasswords no

UsePAM yes

ChallengeResponseAuthentication yes

须知

如果您使用的是root登录，还需要配置文件项为：
PermitRootLogin yes

登录方式错误

失败原因：开启双因子认证后，可能是通过以下方式登录云主机导致登录失败。

- 通过CloudShell工具登录云主机。
- Linux主机中，通过云堡垒机登录云主机。

根本原因：双因子的验证实现是通过内置模块进行验证，由于以上登录方式无法弹出交互页面，导致验证失败。

解决办法：您可参照**如何使用双因子认证?** 重新登录认证。

14.11.7 开启双因子认证时，如何添加接收验证通知的手机号或邮箱?

当您开启双因子认证，选择“短信邮件验证”，才可以在消息通知服务主题中添加手机号/邮箱接收验证码。

“选择消息通知服务”下拉列表中，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。创建完成后，单击“添加订阅”，设置需要接受通知的手机号码或邮箱。
- 如果已有主题，需要添加或者修改手机号码、邮箱：
  - 添加手机号码或邮箱

    单击“查看消息通知服务主题”进入主题页面，单击“添加订阅”，添加需要接受消息通知的手机号码或邮箱。
  - 删除手机号码或邮箱

    单击“查看消息通知服务主题”进入主题页面，单击主题名称，进入主题详情页面，选择订阅总数页签，单独删除或批量删除目标终端即可。

14.11.8 双因子认证中，验证码是一个固定的验证码吗?

当您开启双因子认证无法用手机/邮箱接收验证码时，您可以选择“验证码验证”。当您每次登录云主机时，HSS均会生成一个随机验证码发送到您的登录界面，您直接输入随机验证码即可登录该云主机。

14.11.9 如何修改接收告警通知的手机号或邮箱?

开启告警通知功能后，HSS通过您设置的手机号或邮箱向您发送告警通知，帮助您及时了解主机/网页内的安全风险。

修改告警通知的手机号或邮箱

如果接收告警通知的订阅终端（手机号或邮箱）变更，需要删除订阅后，重新添加接收告警通知的手机号或邮箱。

例如：需要删除HSS告警通知的消息主题名称是“HSS-warning”，消息订阅终端是“test@example.com”。

前提条件

拥有SMN administrator权限。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择区域后，单击 ☰，选择“应用服务 > 消息通知服务”。

步骤3 单击“订阅”，进入订阅页面，搜索待删除订阅终端（手机号或者邮箱）。

步骤4 请根据“订阅终端”和“主题名称”，确认该订阅终端接收的是HSS的告警通知。

步骤5 单击“删除”，删除订阅。

说明

删除订阅后，消息订阅者将无法接收HSS推送的消息，请谨慎操作。

步骤6 删除订阅后，选择“主题”，查询到指定主题，为主题添加新的订阅。

----结束

14.11.10 配置告警通知时选不到消息主题?

未创建主题

在“告警通知”页面，单击“查看消息通知服务主题”，进入SMN服务，创建新的主题。

主题未订阅

创建主题后，您需要为该主题添加一个或多个订阅，并按接收到的消息提示确认订阅，否则将无法选到该主题。

14.11.11 是否可以不开启 HSS 告警通知?

可以不开启HSS告警通知。

若您开启了主机防护，没有设置告警通知，您将无法接收到HSS发送的告警通知，无法及时了解主机/网页的安全风险。若需要了解主机的安全风险，您只能登录管理控制台自行查看。

设置告警通知

开启主机安全防护后，若您想设置告警通知，可以通过以下步骤进行设置：

1. 登录主机安全控制台。
2. 选择“安装与配置 > 告警配置”，进入告警配置页面，设置告警通知。

取消告警通知

开启主机安全防护后，若您不想收到HSS的告警通知，您可以取消设置HSS告警通知。取消告警通知后，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警短信或邮件。

取消设置HSS告警通知方式，如下所示：

- 方式一：删除消息通知主题
  删除主题后，您配置的告警通知将不会生效。
- 方式二：删除消息通知主题中的订阅
  删除订阅后，您将不会收到告警通知。
- 方式三：取消或关闭消息通知主题中的订阅
  取消订阅后，您将不会收到告警通知。

14.11.12 如何修改告警通知的通知项?

开启主机安全防护后，若您不想收到HSS的某项告警通知，您可以屏蔽不想接收告警的事件。屏蔽后，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警短信或邮件。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“安装与配置”，进入安装与配置界面。

步骤4 选择“告警通知”页签，进入“告警通知”页面。

步骤5 选择无需发送告警的屏蔽事件。

步骤6 选择消息主题。

步骤7 单击“应用”，完成修改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。

若涉及多个**消息通知主题**更改，请重复**步骤5**~**步骤7**操作。

----结束

14.11.13 如何关闭 SELinux 防火墙?

SELinux(Security Enhanced Linux)安全增强型linux系统，是一个linux内核模块，也是linux的一个安全子系统。

SELinux的主要作用是最大限度地减小系统中服务进程可访问的资源（最小权限原则）。

关闭说明

- SELinux关闭后不会影响业务使用。
- SELinux关闭可根据需求选择临时关闭或永久关闭。

关闭场景

使用HSS的双因子认证功能时，需要将SELinux防火墙进行永久关闭。

关闭操作

步骤1 远程登录目标服务器。

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：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。

步骤2 在命令窗口执行关闭命令。

- **临时关闭**

  在命令窗口执行以下命令临时关闭SELinux。

  ```
  setenforce 0
  ```

  说明

  在重启系统后将恢复开启状态。

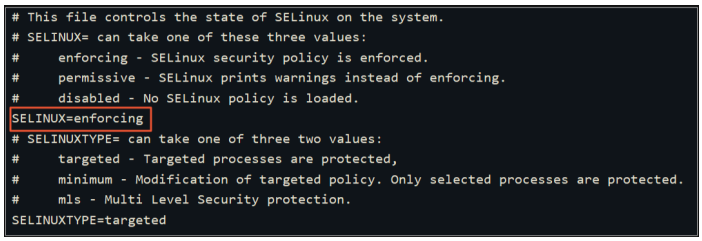
- **永久关闭**

  a. 在目录窗口执行以下命令，编辑SELinux的config文件。


```
vi /etc/selinux/config
```

b. 找到SELINUX=enforcing，按i进入编辑模式，将参数修改为SELINUX=disabled。

图 14-4 编辑 selinux 状态



c. 修改完成后，按下键盘Esc键，执行以下命令保存文件并退出。

```
:wq
```

步骤3 执行永久关闭命令并保存退出后，执行以下命令立即重启服务器。

```
shutdown -r now
```

说明

执行永久关闭的命令后不会立即生效，重启服务器后才会生效。

步骤4 重启后运行以下命令，验证SELinux的状态为disabled，表明SELinux已关闭。

```
getenforce
```

----结束

14.12 其他

14.12.1 如何使用 Windows 远程桌面连接工具连接主机?

操作步骤

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

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

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

步骤4 在弹出的对话框中，输入主机的用户密码，单击“确定”，连接至主机。

----结束

14.12.2 如何查看 HSS 的日志文件?

日志路径

您需要根据主机的操作系统，查看日志文件。

操作系统	日志所在路径	日志文件
Linux	/var/log/hostguard/	• hostwatch.log • hostguard.log • upgrade.log • hostguard-service.log • config_tool.log • engine.log
Windows	C:\Program Files\HostGuard\log	• hostwatch.log • hostguard.log • upgrade.log

日志保留周期

日志文件	日志描述	文件大小限制	路径下保留的文件	保留周期
hostwatch.log	记录守护进程运行时相关日志。	10M	保留8个最新的日志文件。	不超过文件大小限制，只要不卸载HSS Agent，会一直保留日志信息。
hostguard.log	记录工作进程运行时相关日志。	10M	保留8个最新的日志文件。	
upgrade.log	记录版本升级时相关日志。	10M	保留8个最新的日志文件。	
hostguard-service.log	记录服务启动时相关日志（脚本）。	100k	保留2个最新的日志文件。	
config_tool.log	记录服务启动时相关日志（程序）。	10M	保留2个最新的日志文件。	
engine.log	记录服务退出时相关日志。	10M	保留2个最新的日志文件。	

14.12.3 如何开启登录失败日志开关?

MySQL

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

步骤1 使用root权限登录主机。

步骤2 查询log_warnings值，命令如下：

show global variables like 'log_warnings'

步骤3 修改log_warnings值，命令如下。

set global log_warnings=2

步骤4 修改配置文件。

- Linux系统中，修改配置文件my.conf，在[MySQLd]中增加log_warnings=2。

----结束

vsftp

本节指导用户开启vsftp的登录失败日志开关。

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

vsftpd_log_file=log/file/path

dual_log_enable=YES

步骤2 重启vsftp服务。设置成功后，登录时，会返回如图14-5所示的日志记录。

图 14-5 日志记录

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

----结束

14.12.4 怎么去除由于修复软件漏洞造成的关键文件变更告警?

告警通知检测到关键文件变更，如果您确认是正常操作可以不用关注，7天后自动消除。

14.12.5 HSS 是否能以软件形式线下输出?

不支持线下软件的形式。

14.12.6 ECS 服务器已经删除，为什么 HSS 的服务器列表仍显示有该服务器?

ECS服务器删除后，HSS不会立即同步相关信息，所以您在HSS的服务器列表可能查看到已经删除的服务器。

当您进入HSS的“资产管理 > 主机管理”页面后，HSS会立即启动同步任务，预计十分钟内完成服务器信息同步。十分钟后，您刷新主机管理页面，即可查看最新的服务器列表信息。

A 修订记录

发布日期	修改说明
2023-11-30	第一次正式发布。