企业主机安全

用户指南（吉隆坡区域）

发布日期　2025-10-09

目 录

1 产品介绍 1
1.1 什么是企业主机安全 1
1.2 产品优势 2
1.3 应用场景 3
1.4 产品功能 4
1.5 HSS 权限管理 37
1.6 约束与限制 38
1.7 HSS 与其他云服务的关系 45
1.8 基本概念 46
2 通过 IAM 授予使用 HSS 的权限 48
2.1 创建用户并授权使用 HSS 48
2.2 HSS 自定义策略 49
2.3 HSS 授权项说明 50
3 并接入 HSS 54
3.1 接入流程 54
3.2 为主机安装 Agent 54
3.2.1 为云平台主机安装 Agent 54
3.2.2 线下 IDC 通过专线和代理服务器接入 HSS 63
3.2.2.1 方案概述 63
3.2.2.2 资源规划 64
3.2.2.3 操作流程 64
3.2.2.4 实施步骤 65
3.2.2.4.1 创建专线连接 65
3.2.2.4.2 创建代理服务器 65
3.2.2.4.3 为代理服务器安装 Agent 65
3.2.2.4.4 为代理服务器安装配置 nginx 66
3.2.2.4.5 通过代理服务器制作 Agent 安装包或安装命令 70
3.2.2.4.6 为线下 IDC 安装 Agent 73
3.2.3 通过 CBH 安装 HSS 的 Agent 74
3.3 为容器安装 Agent 76
3.3.1 为云 CCE 集群安装 Agent 76
3.3.2 为非集群节点安装 Agent 78

3.4 开启防护 79
3.4.1 开启基础版/企业版/旗舰版防护 83
3.4.2 开启网页防篡改版防护 85
3.4.3 开启容器版防护 87
4 查看防护总览 89
5 资产管理 97
5.1 资产概览 97
5.2 主机指纹 98
5.2.1 采集主机资产指纹 98
5.2.2 查看主机资产指纹 101
5.3 容器指纹 103
5.3.1 采集容器资产指纹 103
5.3.2 查看容器资产指纹 107
5.4 主机管理 112
5.4.1 开启主机防护 112
5.4.2 查看主机防护状态 115
5.4.3 导出主机列表 117
5.4.4 部署防护策略 117
5.4.5 管理服务器组 119
5.4.6 管理服务器重要性 120
5.4.7 忽略服务器 121
5.4.8 关闭主机防护 122
5.4.8.1 关闭基础版/企业版/旗舰版防护 122
5.4.8.2 关闭网页防篡改版防护 123
5.5 容器管理 124
5.5.1 开启容器防护 124
5.5.2 查看容器节点防护状态 127
5.5.3 导出容器节点列表 128
5.5.4 管理本地镜像 128
5.5.5 管理仓库镜像 131
5.5.6 查看容器信息 138
5.5.7 处置风险容器 139
5.5.8 卸载集群 Agent 140
5.5.9 关闭容器防护 141
6 风险预防 143
6.1 漏洞管理 143
6.1.1 漏洞管理概述 143
6.1.2 扫描漏洞 146
6.1.3 查看漏洞详情 149
6.1.4 导出漏洞列表 151
6.1.5 处理漏洞 152

6.1.6 管理漏洞白名单 161
6.1.7 查看漏洞历史处置记录 162
6.2 基线检查 163
6.2.1 基线检查概述 163
6.2.2 执行基线检查 166
6.2.3 查看并处理基线检查结果 169
6.2.4 导出基线检查报告 174
6.2.5 管理手动基线检查策略 175
6.3 容器镜像安全 176
6.3.1 查看 SWR 镜像仓库漏洞 176
6.3.2 查看镜像恶意文件 176
7 主机防御 178
7.1 应用防护 178
7.1.1 应用防护概述 178
7.1.2 开启应用防护 182
7.1.3 查看应用防护 183
7.1.4 管理应用防护策略 185
7.1.5 关闭应用防护 188
7.2 网页防篡改 189
7.2.1 网页防篡改概述 189
7.2.2 开启网页防篡改防护 191
7.2.3 添加防护目录 193
7.2.4 配置远端备份 195
7.2.5 开启动态网页防篡改 198
7.2.6 查看网页防篡改防护事件 199
7.2.7 添加特权进程 199
7.2.8 定时启停静态网页防篡改 200
7.3 勒索病毒防护 201
7.3.1 勒索病毒防护概述 201
7.3.2 开启勒索病毒防护 202
7.3.3 开启勒索备份 205
7.3.4 查看并处理勒索病毒防护事件 207
7.3.5 管理勒索病毒防护策略 208
7.3.6 恢复服务器数据 211
7.3.7 管理服务器备份 213
7.3.8 关闭勒索病毒防护 216
7.4 应用进程控制 216
7.4.1 应用进程控制概述 216
7.4.2 创建白名单策略 218
7.4.3 确认学习结果 220
7.4.4 开启应用进程控制防护 221
7.4.5 查看并处理可疑进程 222

7.4.6 扩展进程白名单 223
7.4.7 重新学习服务器 223
7.4.8 关闭应用进程控制防护 224
7.5 文件完整性管理 225
7.5.1 文件完整性管理概述 226
7.5.2 查看文件变更记录 226
7.6 病毒查杀 229
7.6.1 病毒查杀概述 229
7.6.2 扫描病毒 231
7.6.3 查看并处理病毒 238
7.6.4 管理自定义查杀策略 240
7.6.5 管理文件隔离箱 242
7.7 动态端口蜜罐 243
7.7.1 动态端口蜜罐概述 243
7.7.2 创建动态端口蜜罐防护策略 245
7.7.3 查看并处理蜜罐防护事件 247
7.7.4 管理动态端口蜜罐防护策略 249
7.7.5 管理关联服务器 251
8 容器防御 253
8.1 容器防火墙 253
8.1.1 容器防火墙概述 253
8.1.2 设置网络防御策略（容器隧道网络） 255
8.1.3 设置网络防御策略（VPC 网络） 258
8.2 容器集群防护 260
8.2.1 容器集群防护概述 260
8.2.2 开启容器集群防护 261
8.2.3 配置容器集群防护策略 262
8.2.4 查看容器集群防护事件 264
8.2.5 关闭容器集群防护 264
9 检测与响应 266
9.1 主机安全告警 266
9.1.1 主机安全告警事件概述 266
9.1.2 查看主机告警事件 274
9.1.3 处理主机告警事件 278
9.1.4 导出主机告警事件 281
9.1.5 管理文件隔离箱 281
9.2 容器安全告警 283
9.2.1 容器安全告警事件概述 283
9.2.2 查看容器告警事件 289
9.2.3 处理容器告警事件 293
9.2.4 导出容器告警事件 294
9.3 白名单管理 295

9.3.1 管理登录告警白名单 295
9.3.2 管理告警白名单 296
9.3.3 管理系统用户白名单 298
10 安全运营 300
10.1 策略管理 300
10.1.1 策略管理概述 300
10.1.2 配置策略 304
10.1.3 创建自定义策略组 326
10.1.4 删除自定义策略组 327
10.2 历史处置记录 328
10.3 容器审计 328
10.3.1 容器审计概述 328
10.3.2 查看容器审计日志 329
10.4 安全报告 330
10.4.1 安全报告概述 330
10.4.2 创建安全报告 331
10.4.3 查看安全报告 332
10.4.4 管理安全报告 333
10.5 免费体检 335
11 安装与配置 337
11.1 主机安装与配置 337
11.1.1 Agent 管理 337
11.1.1.1 Agent 概述 337
11.1.1.2 安装主机 Agent 338
11.1.1.3 升级主机 Agent 340
11.1.1.4 卸载主机 Agent 341
11.1.2 安全配置 343
11.1.2.1 配置常用登录地 343
11.1.2.2 配置常用登录 IP 343
11.1.2.3 配置 SSH 登录 IP 白名单 344
11.1.2.4 开启恶意程序隔离查杀 345
11.1.3 双因子认证 346
11.2 容器安装与配置 347
11.2.1 集群管理 347
11.2.1.1 修改集群 Agent 安装信息 347
11.2.1.2 升级或卸载集群 Agent 349
11.2.1.3 查看集群节点列表和权限列表 350
11.2.2 非集群节点管理 350
11.2.2.1 安装非集群节点 Agent 351
11.2.2.2 升级或卸载非集群节点 Agent 353
11.2.3 接入三方镜像仓 354
11.3 告警配置 356

11.4 授权管理 364
11.5 插件配置 366
11.5.1 插件配置概述 366
11.5.2 查看插件信息 367
11.5.3 安装插件 368
11.5.4 卸载插件 369
12 监控与审计 371
12.1 使用 CES 监控 HSS 371
12.1.1 HSS 支持的监控指标 371
12.1.2 HSS 支持监控的事件 372
12.1.3 创建监控告警规则 373
12.1.4 查看监控指标 376
12.2 使用 CTS 审计 HSS 操作事件 376
12.2.1 支持云审计的 HSS 操作列表 376
13 常见问题 379
13.1 产品咨询 379
13.1.1 什么是主机安全？ 379
13.1.2 什么是容器安全？ 380
13.1.3 什么是网页防篡改？ 380
13.1.4 镜像、容器、应用的关系是什么？ 382
13.1.5 HSS 是否和其他安全软件有冲突？ 382
13.1.6 HSS 与 WAF 有什么区别？ 382
13.1.7 什么是 HSS 的 Agent？ 383
13.1.8 HSS 是否支持病毒查杀？ 384
13.2 Agent 相关 384
13.2.1 Agent 是否和其他安全软件有冲突？ 384
13.2.2 如何卸载 Agent？ 385
13.2.3 Agent 安装失败应如何处理？ 387
13.2.4 Agent 状态异常应如何处理？ 388
13.2.5 Agent 的默认安装路径是什么？ 389
13.2.6 Agent 运行时占用多少 CPU、内存和磁盘资源？ 390
13.2.7 购买不同版本 HSS，可以共用同一 Agent 吗？ 391
13.2.8 如何查看未安装 Agent 的主机？ 391
13.2.9 Agent 安装成功后显示未安装怎么处理？ 391
13.2.10 升级失败怎么处理？ 392
13.2.11 不升级有什么影响？ 393
13.2.12 无法访问 Windows 或 Linux 版本 Agent 下载链接？ 394
13.2.13 升级 Agent 失败，提示“替换文件失败” 395
13.3 漏洞管理 395
13.3.1 如何处理漏洞？ 395
13.3.2 漏洞修复后，仍然提示漏洞存在？ 395
13.3.3 漏洞管理显示的主机不存在？ 396

13.3.4 漏洞修复完成后，要重启主机吗？ 396
13.3.5 漏洞修复失败怎么办？ 396
13.3.6 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？ 403
13.4 检测与响应 404
13.4.1 主机被挖矿攻击，怎么办？ 404
13.4.2 已添加告警白名单，进程还是被隔离？ 407
13.4.3 HSS 为什么没有检测到攻击？ 407
13.4.4 源 IP 被 HSS 拦截后，如何解除？ 408
13.4.5 未手动解除的 IP 拦截记录，为什么显示已解除？ 408
13.4.6 恶意程序检测、隔离查杀周期是多久？ 408
13.4.7 HSS 拦截的 IP 是否需要处理？ 408
13.4.8 如何防御勒索病毒攻击？ 408
13.4.9 如何为高危命令执行类告警添加白名单？ 409
13.5 异常登录 409
13.5.1 添加登录白名单后，还有异地登录告警？ 409
13.5.2 如何查看异地登录的源 IP？ 410
13.5.3 如何取消主机登录成功的告警通知？ 411
13.5.4 是否可以关闭异地登录检测？ 411
13.5.5 如何确认入侵账号是否登录成功？ 411
13.6 账户暴力破解 412
13.6.1 HSS 如何拦截暴力破解？ 412
13.6.2 账户被暴力破解，怎么办？ 414
13.6.3 如何预防账户暴力破解攻击？ 417
13.6.4 如何手动解除误拦截 IP？ 418
13.6.5 频繁收到 HSS 暴力破解告警 418
13.6.6 暴力破解记录未显示修改后的端口 420
13.7 基线检查 420
13.7.1 关闭弱口令检测策略后，还有弱口令事件告警？ 420
13.7.2 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略？ 420
13.7.3 如何在 Windows 主机上设置口令复杂度策略？ 422
13.7.4 如何处理配置风险？ 423
13.7.5 如何查看配置检查的报告？ 423
13.7.6 出现弱口令告警，怎么办？ 424
13.7.7 如何设置安全的口令？ 425
13.8 网页防篡改 426
13.8.1 为什么要添加防护目录？ 426
13.8.2 如何修改防护目录？ 426
13.8.3 无法开启网页防篡改怎么办？ 427
13.8.4 开启网页防篡改后，如何修改文件？ 427
13.8.5 开启动态网页防篡改后，状态是“已开启未生效”，怎么办？ 427
13.8.6 HSS 与 WAF 的网页防篡改有什么区别？ 428
13.9 容器安全 429

13.9.1 如何关闭节点防护？ 429
13.9.2 如何开启节点防护？ 429
13.9.3 自建 K8s 容器如何开启 apiserver 审计功能？ 430
13.9.4 容器集群防护插件卸载失败怎么办？ 433
13.10 安全配置 436
13.10.1 不能通过 SSH 远程登录主机，怎么办？ 436
13.10.2 如何使用双因子认证？ 437
13.10.3 开启双因子认证后收不到验证码？ 438
13.10.4 开启双因子认证后登录主机失败？ 438
13.10.5 如何添加双因子认证的手机号或邮箱？ 439
13.10.6 是否可以不开启 HSS 告警通知？ 439
13.10.7 如何修改告警通知的通知项？ 440
13.10.8 如何关闭 SELinux 防火墙？ 440
13.11 其他 441
13.11.1 如何使用 Windows 远程桌面连接工具连接 Windows 主机？ 442
13.11.2 如何查看 HSS 的日志文件？ 442
13.11.3 如何开启登录失败日志开关？ 443
13.11.4 如何启停 Agent 自保护策略？ 444
13.11.5 HSS 自保护无法关闭怎么办？ 445
A 修订记录 447

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

主机安全是旨在增强主机整体安全性的服务，通过资产管理、漏洞检测、基线检查、入侵检测、勒索防护以及网页防篡改等功能，能够全面识别并管理主机内的信息资产，实时监测主机中潜在风险，并阻止非法入侵行为，帮助企业构建服务器安全体系，降低服务器所面临的安全威胁。

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，在管理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。 • 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全。 • Agent可安装在弹性云服务器（Elastic Cloud Server，ECS）/裸金属服务器（Bare Metal Server，BMS）、线下IDC以及第三方云主机中。 • 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。

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/BMS服务器、线下IDC以及第三方主机中，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。
- 账户安全保护

  提供覆盖事前、事中和事后的账户安全保护功能。支持双因子认证登录，防止用户云服务器上的账户遭受暴力破解攻击，提高云服务器的安全性。
- 主动安全防御

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

  提供主机全攻击路径检测能力，能够实时、准确地感知黑客入侵事件，并提供入侵事件的响应手段，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 产品功能

企业主机安全有基础版、企业版、旗舰版、网页防篡改版和容器版供您选择，主要功能包括：**总览**、**资产概览**、**主机管理**、**容器管理**、**主机指纹**、**容器指纹**、**漏洞管理**、**基线检查**、**应用防护**、**网页防篡改**、**勒索病毒防护**、**文件完整性管理**、**病毒查杀**、**动态端口蜜罐**、**容器防火墙**、**应用进程控制**、**容器集群防护**、**主机安全告警**、**容器安全告警**、**白名单管理**、**策略管理**、**历史处置记录**、**安全报告**、**容器审计**、**安装与配置**等。每个版本支持的功能存在差异，您可以根据自身的业务需求选择合适的版本。

- 如需用于测试或个人用户防护主机账户安全，可使用**基础版（无数量限制，只支持部分功能的检测能力，不支持防护能力）**。
- 如有网站或关键系统防篡改需求，推荐使用**网页防篡改版**。
- 如有镜像安全、容器运行时安全需求，以及容器化部署业务，推荐使用**容器版**。
- 如果主机涉及重要资产或存在高风险情况（例如：对外暴露EIP、保存有关键资产、存在数据库等），以及主机有应用安全防护需求，建议使用**旗舰版或者网页防篡改版**。

说明

- 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**。
- 本文表格中使用的标识含义如下：
  - √表示支持
  - ×表示不支持

总览

总览呈现云上资产整体安全评分和防护配置情况等，方便您掌握资产安全动态。

表 1-2 总览功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
总览	实时展示所有资产的安全评分、安全风险和防护地图，帮助您了解主机和容器的安全状态以及存在的安全风险。	√	√	√	√	√

资产概览

资产概览呈现资产状态和清点情况。

表 1-3 资产概览功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
资产概览	所有主机的资产状态、清点情况统计，包括Agent状态、防护状态、配额状态、资产指纹等。	√	√	√	√	√

主机管理

主机管理功能支持按照主机维度查看和管理目标服务器。

表 1-4 主机管理功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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，提供Linux主机的批量安装agent功能。	√	√	√	√	√

容器管理

容器管理功能支持按照容器维度查看和管理目标服务器、以及管理容器镜像和容器实例的安全风险。

表 1-5 容器管理功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
容器节点管理	所有容器节点管理，用户可为容器节点启停防护，以及部署防护策略。	×	×	×	×	√
容器镜像	提供本地镜像、三方镜像仓、SWR镜像安全扫描，并展示镜像扫描结果和漏洞、异常配置修复建议，帮助用户发现和解决镜像安全风险，避免不安全的镜像部署到生产环境。	×	×	×	×	√
容器	展示容器实例信息，如果存在不安全的容器实例，用户可执行隔离、停止操作。	×	×	×	×	√

主机指纹

主机指纹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，用户通过主机指纹功能集中清点主机中的各类资产信息，及时发现风险资产。

表 1-6 主机指纹功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统**：Linux、Windows。 **检测周期**：每小时自动检测。	×	√	√	√	√
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。 **支持的操作系统**：Linux、Windows。 **检测周期**：每30秒自动检测。	×	√	√	√	√
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。 **支持的操作系统**：Linux、Windows。 **检测周期**：每小时自动检测。	×	√	√	√	√
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。 **支持的操作系统**：Linux、Windows。 **检测周期**：每日自动检测。	×	√	√	√	√
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。 **支持的操作系统**：Linux、Windows。 **检测周期**：每小时自动检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows（仅支持MySQL）。 **检测周期：**1次/周（每周一凌晨04：10）。	×	√	√	√	√

容器指纹

容器指纹功能支持采集容器中的账号、端口、进程、集群、服务和工作负载等资产信息等，用户通过容器指纹功能集中清点容器中的各类资产信息，及时发现风险资产。

表 1-7 资产指纹功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
账号	检测的容器系统中的账号信息，帮助用户进行账户安全性管理。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	√
开放端口	检测容器系统中的开放的端口，帮助用户识别出其中的危险端口和未知端口。 **支持的操作系统：**Linux。 **检测周期：**每30秒自动检测。	×	×	×	×	√
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。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	√
软件	监测并记录当前容器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。 **支持的操作系统：**Linux。 **检测周期：**每日自动检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
自启动项	对容器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。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√
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； **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	√
集群列表	统计、展示集群的详细信息，您可以查看所有集群的类型、节点、版本、状态等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	√
服务	统计、展示服务和断点的详细信息，您可以查看所有服务的命名空间、所属集群等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	√
工作负载	统计、展示工作负载（有状态负载、无状态负载、守护进程集、普通任务、定时任务、容器组）的详细信息，您可以查看所有工作负载的状态、实例个数、命名空间等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	√
容器实例	统计、展示容器实例的详细信息，您可以查看所有容器实例的状态、所属POD、所属集群等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	√

漏洞管理

漏洞管理支持检测主机中的Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞和应急漏洞，帮助用户识别潜在风险。

表 1-8 漏洞管理功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
Linux漏洞检测	通过与漏洞库进行比对，检测主机的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。 **支持的操作系统：**Linux。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次，基础版不支持）、手动扫描（基础版不支持）。	√	√	√	√	√
Windows漏洞检测	通过同步微软官方的补丁公告，检测主机的Windows操作系统存在的漏洞。 **支持的操作系统：**Windows。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次，基础版不支持）、手动扫描（基础版不支持）。	√	√	√	√	×
Web-CMS漏洞检测	通过对主机中的Web目录和文件进行检测，识别Web-CMS漏洞，提升Web服务安全性。 **支持的操作系统：**Linux、Windows。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次）、手动扫描。	×	√	√	√	√
应用漏洞检测	检测主机中开源的jar包、elf文件等的漏洞，比如log4j、spring-core的漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**自动扫描（默认每周一自动扫描）、定时扫描（默认每周一次）、手动扫描。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
应急漏洞检测	通过软件版本比对和POC验证的方式，检测主机上运行的软件和依赖包是否存在漏洞，将存在风险的漏洞上报至控制台，并给您提供漏洞告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**定时扫描（需要手动配置开启）、手动扫描。	×	√	√	√	√

基线检查

基线检查支持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，且可自定义选择检测的子基线项、修复漏洞风险。

表 1-9 基线检查功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持检测的操作系统：**Linux。 **检测周期**：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。 **支持检测的操作系统：**Linux、Windows。 **检测周期：**每日凌晨自动检测、手动检测。	√	√	√	√	√
基线配置检查	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。 **支持检测的操作系统：**Linux、Windows。 **检测周期：**每日凌晨自动检测、手动检测。	×	√	√	√	√

容器镜像安全

容器镜像安全支持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。

表 1-10 容器镜像安全功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
SWR镜像仓库漏洞	通过与漏洞库进行比对，检测SWR镜像仓库存在的系统漏洞、应用漏洞，对当前镜像中存在的漏洞进行提醒。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	√
镜像恶意文件	检测镜像是否携带恶意文件（Trojan、Worm、Virus病毒和Adware垃圾软件等），帮助用户识别出存在的风险。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

应用防护

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。

表 1-11 应用防护功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
SQL注入	检测防御SQL注入（SQL Injection）攻击，检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
OS命令注入	检测防御远程OS命令注入（OS Command Injection）攻击，同时检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
XSS	检测防御存储型跨站脚本(Cross-Site Scripting，XSS)注入攻击。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
Log4j RCE漏洞检测	检测防御远程代码执行的控制攻击，并支持对攻击行为进行阻和拦截。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
上传Webshell	检测防御上传危险文件的攻击或将已有文件改名为危险文件扩展名的攻击，同时检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
内存马注入	检测防御内存马注入攻击。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
XXE	检测防御XXE注入（XML External Entity Injection）攻击，检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
反序列化输入	检测使用了危险类的反序列化攻击。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
文件目录遍历	获取访问文件的路径或目录，匹配是否在敏感目录或敏感文件下。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
Struts2 OGNL	OGNL代码执行检测。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
JSP执行操作系统命令	检测可疑行为—通过JSP请求执行操作系统命令。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
JSP删除文件	检测可疑行为—通过JSP请求删除文件失败。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
数据库连接异常	检测可疑异常—数据库连接抛出的认证和通讯异常。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
0 day漏洞	检测执行命令的堆栈哈希是否在Web应用的白名单堆栈哈希表里。 **支持的操作系统：**Linux。 检测周期：实时检测。	×	×	√	√	√
Security Manager权限检测异常	检测可疑异常，即SecurityManager抛出的异常。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√

网页防篡改

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

表 1-12 网页防篡改功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	×

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
动态网页防篡改	为Tomcat提供动态网页防篡改能力，防止网站数据库中动态网页内容被篡改。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	√	×

勒索病毒防护

勒索病毒防护支持自定义勒索防护策略，帮助您识别检测已知勒索病毒攻击，支持通过静态、动态诱饵识别部分未知的勒索攻击。

表 1-13 勒索病毒防护功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
勒索病毒防护	帮助您识别检测已知勒索病毒攻击，支持通过静态、动态诱饵识别部分未知的勒索攻击。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√

应用进程控制

应用程序控制功能支持检测并告警恶意进程运行，帮助用户构建安全的应用进程运行环境。

表 1-14 应用进程控制功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
应用进程控制	支持管控服务器中应用进程的运行，通过学习服务器运行的应用进程特征，将应用进程划分为可信进程、恶意进程和可疑进程，允许可疑、可信进程正常运行，对恶意进程运行进行告警，帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√

文件完整性管理

文件完整性管理支持检查并记录关键文件的更改。

表 1-15 文件完整性管理功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
文件完整性管理	检查Linux系统的关键文件，帮助用户及时发现发生了可能遭受攻击的更改。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√

病毒查杀

病毒查杀功能支持检测服务器中的病毒文件，可帮助用户清理潜在的恶意威胁。

表 1-16 病毒查杀功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
病毒查杀	病毒查杀功能使用特征病毒检测引擎，支持扫描服务器中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件，用户可根据自身需要，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”扫描任务，并及时处置检测到的病毒文件，增强业务系统的病毒防御能力。 **支持的操作系统：**Linux、Windows。 **检测周期：**手动检测。	×	√	√	√	√

动态端口蜜罐

动态端口蜜罐功能利用真实端口作为诱饵端口诱导攻击者访问，在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机。

表 1-17 动态端口蜜罐功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
动态端口蜜罐	动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√

容器防火墙

容器防火墙为容器环境提供的防火墙服务。

表 1-18 容器防火墙功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

容器集群防护

容器集群防护功能支持检测镜像中存在的不合规基线、漏洞恶意文件，防止不安全的容器镜像部署到集群。

表 1-19 容器集群防护功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
容器集群防护	支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

主机安全告警

主机安全告警支持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。

表 1-20 主机安全告警功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
病毒	对服务器进行实时检测，对在服务器资产发现的各种病毒进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
蠕虫	对服务器中入侵的蠕虫或已存在的蠕虫进行检测、查杀，并进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
木马	对隐藏在正常程序中具备破坏和删除文件、发送密码、记录键盘等特殊功能的程序进行检测，发现时立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
僵尸网络	检测主机资产中是否存在已被传播的僵尸程序，一旦发现立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
后门	实时检测服务器系统是否存在后门漏洞，对发现的后门病毒进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√
黑客工具	检测服务器是否存在用来控制服务器的非标工具，一旦发现立即上报告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
挖矿软件	实时检测服务器中是否存在挖矿软件，并对发现的软件进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
远程代码执行	实时检测服务器是否存在被远程调用的情况，一旦发现立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
反弹Shell	实时监控用户的进程行为，支持告警和阻断进程的非法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。 目前支持阻断的反弹shell类别：exec反弹Shell、Perl反弹Shell、AWK反弹Shell、Python反弹Shell.b、Python反弹Shell.a、Lua反弹Shell、mkfifo/openssl反弹Shell、PHP反弹Shell、Ruby反弹Shell、使用rssocks进行反向代理、Bash反弹Shell、Ncat反弹Shell、exec重定向反弹Shell、Node反弹Shell、Telnet双端口反弹Shell、nc反弹Shell、Socat反弹Shell、rm/mkfifo/sh/nc反弹Shell、socket/tchsh反弹Shell。 **支持的操作系统：**Linux。 **检测周期：**实时检测。 **说明** 启用反弹Shell自动阻断需确保满足以下条件： 1. 在“HIPS检测”策略中，开启“自动化阻断”。该功能默认关闭，需要手动开启。 2. 确保已开启恶意程序隔离查杀。该功能默认关闭，需要手动开启。	×	√	√	√	√
文件提权	检测当前系统对文件的提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
进程异常行为	检测主机进程信息，包括进程ID、命令行、进程路径、行为等，当进程出现无故崩溃、占用过多资源、产生网络连接等异常行为时进行告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
敏感文件访问	检测未经授权访问或修改敏感文件的行为。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统**：Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Windows。 **检测周期：**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。 **支持的操作系统：**Windows。 **检测周期：**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。 **支持的操作系统：**Windows。 **检测周期：**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。 **支持的操作系统：**Windows。 检测周期：实时检测。	×	√	√	√	×

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
可疑进程运行	检测未经过认证或授权的应用进程运行，一旦发现进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√
可疑进程文件访问	检测未经过认证或授权的进程访问指定的目录，一旦发现进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 • 如果账户暴力破解成功，登录到云主机，则触发安全事件告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**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）。 如果在非常用登录地登录，则触发安全事件告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Windows。 **检测周期：**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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
云蜜罐	检测到连接主机蜜罐端口的行为，进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√
异常外联行为	检测到服务器存在异常外联可疑ip的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux（仅支持5.10及以上内核版本）。 **检测周期：**实时检测。	×	√	√	√	√
端口转发检测	检测到利用可疑工具进行端口转发行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√
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。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	√	√	√	×

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Windows。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√
主机扫描	检测网络对主机规则覆盖（包含对ICMP、ARP、nbtscan是覆盖）的扫描活动，一旦发现立即上报告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√

容器安全告警

容器安全告警支持对Docker、Containerd容器引擎进行入侵行为检测，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。

表 1-21 容器安全告警功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
黑客工具	检测容器环境是否存在用来控制容器的非标工具，一旦发现立即上报告警。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
反弹Shell	实时监控容器环境用户的进程行为，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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
文件提权	检测当前容器系统对文件的提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
进程提权	检测容器环境以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
关键文件变更	对于容器场景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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
进程异常行为	检测容器进程信息，包括进程ID、命令行、进程路径、行为等，当进程出现无故崩溃、占用过多资源、产生网络连接等异常行为时进行告警。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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:[...]) **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
容器镜像阻断	在Docker环境中容器启动前，告警并阻断中指定的不安全容器镜像运行。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。 **检测周期：**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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。 **说明** 目前暂仅支持Docker容器运行时的暴力破解检测告警。	×	×	×	×	√
非法系统账号	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。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
用户密码窃取	检测容器环境中系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
异常外联行为	检测到容器环境中存在异常外联可疑ip的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux（仅支持5.10及以上内核版本）。 **检测周期：**实时检测。	×	×	×	×	√
端口转发检测	检测到容器环境中利用可疑工具进行端口转发行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
Kubernetes事件删除	检测集群中删除Kubernetes事件的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
Pod异常行为	检测集群中存在创建特权pod、静态pod及敏感配置pod的异常行为，以及对现存pod执行的异常操作，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
枚举用户信息	检测存在枚举集群用户的权限以及可执行操作列表的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√
绑定集群用户角色	检测绑定、创建高权限集群角色或Service Account的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

白名单管理

白名单功能包含**告警白名单**、**登录白名单**和**系统用户白名单**，如需避免某些告警误报发生，可以将告警事件加入对应的白名单。

表 1-22 白名单管理功能介绍

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√

功能名称	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
登录告警白名单	将目标登录端IP和登录端用户名加入登录告警白名单，HSS将对白名单内的IP和用户的访问行为进行忽略，不再告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√

策略管理

用户可以根据需要进行**策略管理**配置，自定义安全检测规则，并可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。

表 1-23 策略管理功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
策略管理	支持自定义检测策略配置与下发，能够为每组或每台主机灵活配置检测规则，便于精细化安全运营。 ● 查看策略组列表 ● 依据默认策略组和已创建的策略组添加策略组 ● 自定义策略 ● 修改和删除策略组 ● 针对策略组包含的策略，进行修改和关闭策略 ● 在“主机管理”页面可以对主机进行批量部署策略 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√（仅支持默认企业版策略组）	√	√	√

历史处置记录

历史处置记录呈现漏洞、安全告警事件等的处置历史。

表 1-24 历史处置记录功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
历史处置记录	提供漏洞、安全告警事件等的历史处置记录，方便您查看相关处理时间和处理人等信息。	×	√	√	√	√

安全报告

HSS支持以天、周、月的形式输出用户资产的安全报告。

表 1-25 安全报告功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。	×	√	√	√	√

容器审计

容器审计支持监控和记录集群容器、非集群容器的各类操作和活动，以日志记录呈现在HSS控制台供用户查看和分析。

表 1-26 容器审计功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
容器审计	容器审计功能支持对容器集群中的各种操作和活动进行监控和记录，可帮助用户洞察容器生命周期的各个阶段，包括创建、启动、停止和销毁等。用户通过审计和分析，可以及时发现并处理安全问题，从而确保容器集群的安全性、稳定性。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√

安装与配置

安装与配置提供Agent管理、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、双因子认证、告警配置等功能，可满足不同应用场景的主机/容器安全需求。

表 1-27 安装与配置功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√
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。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√
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。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Linux。	√	√	√	√	√
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。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√
双因子认证	通过密码+短信/邮件认证的方式，彻底防范账号暴力破解行为。 **支持的操作系统：**Linux、Windows。	按需：×	√	√	√	√
告警配置	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。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√
插件管理	对插件进行安装、卸载、升级及统一管理。 **支持的操作系统：**Linux。	×	×	×	×	√
容器安装与配置	提供集群接入HSS入口，同时支持集群、非集群容器的Agent升级、卸载操作。 **支持的操作系统：**Linux。	√	√	√	√	√

主机安全自保护

主机安全自保护是企业主机安全的自我保护功能。

表 1-28 主机安全自保护功能介绍

服务功能	功能概述	基础版	企业版	旗舰版	网页防篡改版	容器版
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。 **支持的操作系统：**Windows。	×	×	√	√	×

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，可以帮助您安全地控制云资源的访问。

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1-29所示，包括了HSS的所有系统权限。

表 1-29 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和BSS Administrator角色。
HSS FullAccess	企业主机安全所有权限。	系统策略	无
HSS ReadOnlyAccess	企业主机安全的只读访问权限。	系统策略	无

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

1.6 约束与限制

主机防护限制

HSS支持对云平台主机进行防护，具体支持防护的主机类型包括：

- 弹性云服务器（Elastic Cloud Server，ECS）

- 裸金属服务器（Bare Metal Server，BMS）
- 线下数据中心（IDC）

操作系统限制

企业主机安全的Agent、系统漏洞扫描功能对操作系统有一定限制，部分操作系统暂不支持。

HSS对操作系统的限制请参见：

- **表 HSS对Windows操作系统的限制（x86架构）**
- **表 HSS对Linux操作系统的限制（x86架构）**
- **表 HSS对Linux操作系统的限制（Arm架构）**

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！
- 本文表格中使用的标识含义如下：
  - √表示支持
  - ×表示不支持

表 1-30 HSS 对 Windows 操作系统的限制（x86 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
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)	√	√
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 2019 数据中心版 64位英文(40GB)	√	√

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
Windows Server 2019 数据中心版 64位简体中文(40GB)	√	√
Windows Server 2022 数据中心版 64位英文(40GB)	√	×
Windows Server 2022 数据中心版 64位简体中文(40GB)	√	×
Windows Server 2022 标准版 64位 英文(40GB)	√	×
Windows Server 2022 标准版 64位 简体中文(40GB)	√	×

表 1-31 HSS 对 Linux 操作系统的限制（x86 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 7.4（64位）	√	√
CentOS 7.5（64位）	√	√
CentOS 7.6（64位）	√	√
CentOS 7.7（64位）	√	√
CentOS 7.8（64位）	√	√
CentOS 7.9（64位）	√	√
CentOS 8.1（64位）	√	×
CentOS 8.2（64位）	√	×
CentOS 8（64位）	√	×
Debian 9（64位）	√	√
Debian 10（64位）	√	√
Debian 11（64位）	√	√
Debian 12（64位）	√ **说明** 暂不支持暴力破解检测。	×
EulerOS 2.2（64位）	√	√
EulerOS 2.3（64位）	√	√
EulerOS 2.5（64位）	√	√

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
EulerOS 2.7（64位）	√	×
EulerOS 2.9（64位）	√	√
EulerOS 2.10（64位）	√	√
EulerOS 2.11（64位）	√	√
EulerOS 2.12（64位）	√	√
Fedora 28（64位）	√	×
Fedora 31（64位）	√	×
Fedora 32（64位）	√	×
Fedora 33（64位）	√	×
Fedora 34（64位）	√	×
Ubuntu 16.04（64位）	√	√
Ubuntu 18.04（64位）	√	√
Ubuntu 20.04（64位）	√	√
Ubuntu 22.04（64位）	√	√
Ubuntu 24.04（64位）	√ **说明** 暂不支持暴力破解检测。	×
AlmaLinux 8.4（64位）	√	√
AlmaLinux 9.0（64位）	√	×
AlmaLinux 9.2（64位）	√	×
AlmaLinux 9.4（64位）	√	×
RockyLinux 8.4（64位）	√	×
RockyLinux 8.5（64位）	√	×
RockyLinux 8.6（64位）	√	√
RockyLinux 8.10（64位）	√	√
RockyLinux 9.0（64位）	√	×
RockyLinux 9.4（64位）	√	√
RockyLinux 9.5（64位）	√	√
HCE 1.1 CentOS兼容版 （64位）	√	√
HCE 2.0 标准版 （64位）	√	√

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
SUSE Linux Enterprise Server 12 SP5（64位）	√	√
SUSE Linux Enterprise Server 15（64位）	√	×
SUSE Linux Enterprise Server 15 SP1（64位）	√	√
SUSE Linux Enterprise Server 15 SP2（64位）	√	√
SUSE Linux Enterprise Server 15 SP3（64位）	√	×
SUSE Linux Enterprise Server 15.5（64位）	√	×
SUSE Linux Enterprise Server 15 SP6（64位）	√ **说明** 暂不支持暴力破解检测。	×
银河麒麟V10（64位）	√	√
银河麒麟V10 SP1（64位）	√	√
银河麒麟V10 SP2（64位）	√	√
银河麒麟V10 SP3（64位）	√	×
统信UOS 1050u2e	√ **说明** 暂不支持文件逃逸检测。	√

表 1-32 HSS 对 Linux 操作系统的限制（Arm 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 7.4（64位）	√	√
CentOS 7.5（64位）	√	√
CentOS 7.6（64位）	√	√
CentOS 7.7（64位）	√	√
CentOS 7.8（64位）	√	√
CentOS 7.9（64位）	√	√
CentOS 8.0（64位）	√	×
CentOS 8.1（64位）	√	×

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 8.2（64位）	√	×
CentOS 9（64位）	√	×
Debian 11（64位）	√	√
Debian 12（64位）	√ **说明** 暂不支持暴力破解检测。	×
EulerOS 2.8（64位）	√	√
EulerOS 2.9（64位）	√	√
EulerOS 2.10（64位）	√	√
EulerOS 2.11（64位）	√	√
EulerOS 2.12（64位）	√	√
Fedora 29（64位）	√	×
Ubuntu 18.04（64位）	√	√
Ubuntu 20.04（64位）	√	√
Ubuntu 22.04（64位）	√	√
Ubuntu 24.04（64位）	√ **说明** 暂不支持暴力破解检测。	×
中标麒麟V7（64位）	√	×
银河麒麟V10（64位）	√	√
银河麒麟V10 SP1（64位）	√	√
银河麒麟V10 SP2（64位）	√	√
银河麒麟V10 SP3（64位）	√	×
HCE 2.0 标准版（64位）	√	√
统信UOS V20（64位）	√	√ **说明** 仅统信UOS V20服务器E版、D版支持系统漏洞扫描。
统信UOS V20 1050e（64位）	√	√
统信UOS V20 1060e（64位）	√	√
RockyLinux 9.5（64位）	√	√
CTyunOS 3-23.01（64位）	√	√

Agent 限制

- 如果服务器安装了第三方安全防护软件，请先卸载再安装主机安全Agent；第三方安全软件与主机安全Agent存在不兼容的情况，会影响主机安全的防护功能。
- 主机或容器节点安装Agent后，Agent可能修改如下系统文件或配置：
  - Linux系统文件：
    - /etc/hosts.deny
    - /etc/hosts.allow
    - /etc/rc.local
    - /etc/ssh/sshd_config
    - /etc/pam.d/sshd
    - /etc/docker/daemon.json
    - /etc/sysctl.conf
    - /sys/fs/cgroup/cpu/（在该目录下新建HSS进程的子目录）
    - /sys/kernel/debug/tracing/instances（在该目录下新建CSA实例）
  - Linux系统配置：iptables规则
  - Windows系统配置：
    - 防火墙规则
    - 系统登录事件审核策略及登录安全层和认证方式配置
    - Windows Remote Management信任主机列表

暴力破解防护限制

- 在为Windows主机开启防护时，需要您同步授权开启Windows防火墙，用于拦截暴力破解的攻击源IP；如果不开启，HSS仅会在检测到暴力破解攻击时进行告警而不会拦截。
  - 开启Windows防火墙，HSS将自动添加允许流量全入（hostguard_AllowAnyIn）和全出（hostguard_AllowAnyOut）的防火墙规则，确保防火墙启用不会干扰您的正常业务运行。同时，当HSS检测到暴力破解攻击时，将在防火墙中添加一条入站规则用于拦截暴力破解的攻击源IP，不会对您的主机造成任何不利的影响。
  - 使用HSS期间请勿关闭Windows防火墙，如果关闭Windows防火墙，HSS无法拦截暴力破解的攻击源IP；即使手动关闭后开启Windows防火墙，也可能导致HSS不能拦截暴力破解的攻击源IP。
- 暴力破解攻击检测暂不支持操作系统Debian 12、Ubuntu 24.04、SUSE Linux Enterprise Server 15 SP6。

1.7 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，为集群中所有可用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。

消息通知服务

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

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

关于SMN的详细内容，请参见《消息通知服务用户指南》。

统一身份认证服务

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

关于IAM的详细内容，请参见《统一身份认证服务用户指南》。

云审计服务

云审计服务（Cloud Trace Service，CTS），是一个专业的日志审计服务。云审计服务能够记录主机中用户对企业主机安全的操作，方便您对主机执行安全分析、合规审

计、资源跟踪和问题定位等审计工作。云审计服务是管理日志的基础服务，无需付费即可使用。

关于CTS的详细内容，请参见《云审计服务用户指南》。

1.8 基本概念

账户破解

账户破解指入侵者通过各种手段，如暴力破解、字典攻击等方式，获取系统或应用账号密码的行为。一旦账号被破解成功，入侵者可能非法登录系统，窃取数据、破坏系统。

基线

基线是指操作系统、数据库、中间件、应用需要满足的最低安全配置要求，基线范围包括账号管理，口令策略配置，授权管理，服务管理，配置管理，网络配置，权限管理等。

弱口令

弱口令指密码强度低，容易被攻击者猜测和破解的密码。一旦攻击者破获密码，可直接登录系统，读取、篡改、破坏系统数据。

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，按传播方式，恶意程序可分为后门、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。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，用户将无法读取原来正常的文件，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。

安全告警事件

安全告警事件是指HSS在检测到主机或容器中的安全威胁（例如恶意程序、漏洞利用）时自动生成的事件通知与记录，其核心目的在于及时提醒用户注意并采取措施解决系统面临的潜在安全风险，从而有效地提升系统整体的安全性。

双因子认证

双因子认证是指一种结合密码和验证码两种条件对用户登录行为进行认证，从而增强账户安全性的方法。

网页防篡改

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

集群

集群指容器运行所需要的云资源组合，关联了若干云服务器节点、负载均衡等云资源。您可以理解为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

每一个节点对应一台服务器（可以是虚拟机实例或者物理服务器），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。镜像在开发、部署及运行的过程中，可能引入各类安全风险，例如已知或未知漏洞、恶意文件，如果这类镜像未经安全检查即被应用于生产环境，将极大增加系统被入侵的风险，可能导致数据泄露、资源滥用等严重后果。因此，确保镜像安全是容器化应用部署过程中不可忽视的一环。

Pod

在Kubernetes中，Pod是部署应用或服务的最小基本单位。一个Pod可以封装一个或多个应用容器，多个容器通常共享存储和网络资源。

容器

容器（Container）是通过镜像创建的运行实例。在一个节点（宿主机）上可以运行多个容器。容器的实质是进程，但与直接在宿主机上执行的进程不同，容器进程运行于属于自己的独立的命名空间中。

容器运行时

容器运行时（Container Runtime）是Kubernetes最重要的组件之一，负责真正管理镜像和容器的生命周期。Kubelet通过Container Runtime Interface (CRI)与容器运行时交互，以管理镜像和容器。

项目

IAM中的项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个账户中可以创建多个项目。

2 通过 IAM 授予使用 HSS 的权限

2.1 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。

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2-1**所示。

表 2-1 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
HSS ReadOnlyAccess	企业主机安全的只读访问权限。	系统策略	无

示例流程

以下步骤，以仅授予用户HSS服务的管理员权限“HSS Administrator”为例，实现用户只能访问、管理HSS服务，无法访问其他云服务的权限管理目标。

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（当前用户权限仅包含“HSS Administrator”）：

   a. 在“服务列表”中选择企业主机安全，成功进入企业主机安全总览界面。

   b. 在“服务列表”中选择除了企业主机安全之外的任一服务，提示权限不足。

   表示“HSS Administrator”已生效。

2.2 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"
            ]
        }
    ]
}
```

2.3 HSS 授权项说明

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，IAM），如果登录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。

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

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

支持的授权项

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

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

企业主机安全（HSS）支持的自定义策略授权项如下所示：

授权列表

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

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

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

3 并接入 HSS

3.1 接入流程

初次使用企业主机安全HSS服务时，您可依据本文内容快速了解将主机和容器接入该云服务进行防护的流程。

企业主机安全服务提供资产管理、漏洞检测、基线检查、入侵检测、勒索防护及网页防篡改等功能，能够全面识别主机和容器面临的安全风险，阻止非法入侵，帮助用户构建安全的主机和容器环境。

接入流程说明

您可以通过以下几个步骤将主机或容器接入企业主机安全HSS开启防护。

表 3-1 接入流程说明

序号	步骤	说明
1	• 为主机安装Agent • 为容器安装Agent	Agent是企业主机安全提供的一款软件，安装在主机和容器节点上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机和容器的安全检测与防护。安装Agent后，您才能使用企业主机安全。
2	开启防护	

3.2 为主机安装 Agent

3.2.1 为云平台主机安装 Agent

操作场景

安装Agent后，您才能为服务器开启主机安全防护。本章节为您介绍如何为云平台主机安装Agent。

前提条件

- 安装Agent对安全组出方向端口以及第三方安全软件等有限制要求，为避免安装Agent失败，请您参考**安装前环境准备**，完成相关排查后再安装Agent。
- 安装Agent前，请先将VPCOperatePolicy和VPCEPOperatePolicy权限授予HSS，详细操作请参见**授权管理**。

Agent 安装模式说明

HSS提供两种类别的安装模式，两者的区别请参见**表3-2**。

表 3-2 安装模式说明

Agent安装模式	特点	适用场景
界面安装	操作便捷，比通过命令行安装Agent的效率更高。HSS仅需要您提供服务器账号密码或密钥，即可安装Agent，HSS不会保存您提交的密码文件。	待安装Agent的服务器所在VPC内已有至少1台Agent在线的服务器。
命令行/脚本安装	您需要登录服务器执行命令行或脚本安装Agent，操作比界面安装方式更复杂、效率更低。	• 首次安装Agent。 • 待安装Agent的服务器所在VPC内没有Agent在线的服务器。

通过账号密码为单台云平台主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：界面安装
- 选择服务器验证模式：账号密码方式
- 选择安装数量：单台

步骤9 选中目标服务器，并单击“下一步”。

步骤10 根据界面提示填写账号密码信息。

- Linux

  根据主机是否能通过root账号直接登录，填写信息。

  - 勾选“允许以root权限直连”

    表示服务器可以通过root账号直接登录，您填写服务器root密码、服务器登录端口后，HSS将通过您的root账号为主机安装Agent。
  - 不勾选“允许以root权限直连”

    表示服务器不能通过root账号直接登录，您填写其他可以登录主机的账号信息（其中root密码用于提权），HSS将通过您提供的账号信息为主机安装Agent。
- Windows

  填写登录用户名、登录密码。

步骤11 确认信息无误后，单击“确认”，Agent开始安装。

您可以查看“Agent状态”列，确认Agent安装进度。Agent状态显示“在线”，表示安装完成。

----结束

通过账号密码为多台云平台主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：界面安装
- 选择服务器验证模式：账号密码方式
- 选择安装数量：批量

步骤9 上传安装模板。

1. 单击“下载批量模板”，下载批量模板表格至本地。
2. 打开下载好的表格，按表格要求填写服务器相关信息并保存。
3. 单击“添加文件”，上传已填写完成的表格。

   HSS将根据IP地址自动匹配服务器。如果服务器匹配失败，您可以单击“查看失败主机”，确认失败原因。

步骤10 勾选目标服务器。

步骤11 确认信息无误后，单击“确认”，Agent开始安装。

您可以查看“Agent状态”列，确认Agent安装进度。Agent状态显示“在线”，表示安装完成。

----结束

通过 DEW 为单台或多台云平台主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：界面安装
- 选择服务器验证模式：密钥方式
- 选择密钥来源：云密钥（DEW）

步骤9 选中目标服务器，并单击“确认”，Agent开始安装。

可选服务器列表，仅展示已绑定云密钥（DEW）的服务器。

步骤10 在目标服务器所在行的“Agent状态”列，确认Agent安装进度。

Agent状态显示“在线”，表示安装完成。

----结束

通过自建密钥为单台或多台云平台主机安装 Agent（仅支持 Linux）

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：界面安装
- 选择服务器验证模式：密钥方式
- 选择密钥来源：自建密钥（仅支持Linux）

步骤9 上传安装模板。

1. 单击“下载批量模板”，下载批量模板表格至本地。
2. 打开下载好的表格，按表格要求填写服务器相关信息并保存。
3. 单击“添加文件”，上传已填写完成的表格。

   HSS将自动解析您填写的服务器。如果服务器解析失败，您可以单击“查看失败主机”，确认失败原因。

步骤10 确认信息无误后，单击“确认”，Agent开始安装。

步骤11 在目标服务器所在行的“Agent状态”列，确认Agent安装进度。

Agent状态显示“在线”，表示安装完成。

----结束

通过命令行为单台云平台 Linux 主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

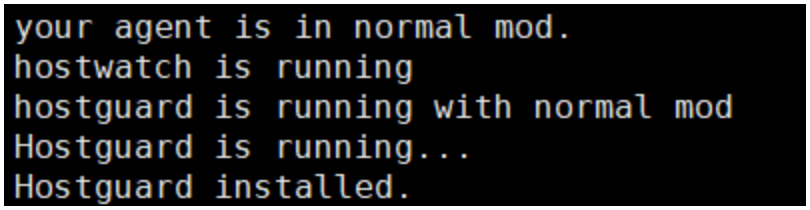
- 选择安装模式：命令行安装
- 选择服务器操作系统：Linux
- 选择安装数量：单台

步骤9 根据界面提示，安装Agent。

1. 单击控制台界面“安装主机安全Agent”对话框中 复制安装命令。
2. 以root账号登录服务器，并粘贴执行安装命令。

   界面回显如**图 Agent安装完成**所示，表示Agent安装完成。

图 3-1 Agent 安装完成



3. 等待5~10分钟，返回企业主机安全控制台，在“主机安装与配置 > Agent管理 > 已安装主机”页面，查看目标服务器Agent状态。

   Agent状态显示在线，表示Agent安装成功。

----结束

通过命令行为多台云平台 Linux 主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：命令行安装
- 选择服务器操作系统：Linux
- 选择安装数量：批量
- 选择服务器验证模式：根据服务器的验证方式，选择“账号密码方式”或“密钥方式”。

步骤9 根据界面提示，安装Agent。

在任一服务器执行如下操作即可。

1. 单击控制台界面“安装主机安全Agent”对话框中“linux-host-list.csv”下载模板。
2. 按模板“linux-host-list.csv”要求填写服务器信息并保存。

   请确保您填写的服务器验证信息与**步骤8**选择的验证模式一致。
3. 使用root账号远程登录任一目标主机。
4. 使用SSH客户端上传模板文件“linux-host-list.csv”至服务器/tmp目录下。
5. 返回HSS控制台，在“安装主机安全Agent”对话框中，单击复制安装命令。

6. 在主机中粘贴执行安装命令，安装Agent。
   界面返回如图3-2所示表示安装完成。

   图 3-2 Agent 安装完成

7. 等待5~10分钟，返回企业主机安全控制台，在“主机安装与配置 > Agent管理 > 已安装主机”页面，查看目标服务器Agent状态。
   Agent状态显示在线，表示Agent安装成功。

----结束

通过脚本为单台云平台 Windows 主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

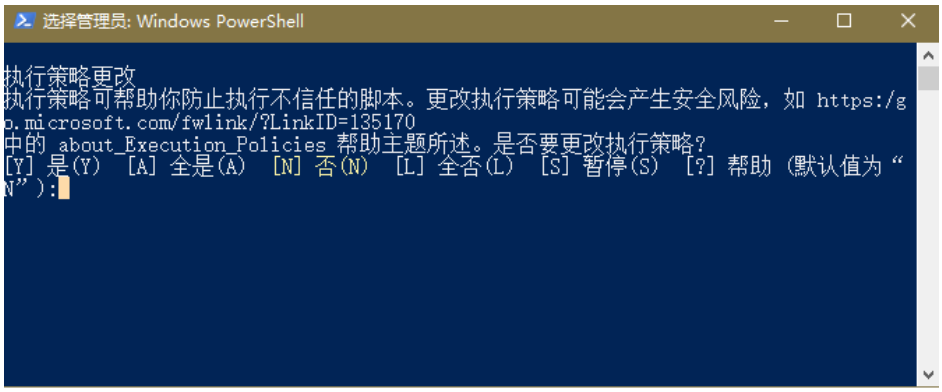
步骤8 选择安装方式。

- 选择安装模式：命令行安装
- 选择服务器操作系统：Windows
- 选择安装数量：单台

步骤9 根据界面提示，安装Agent。

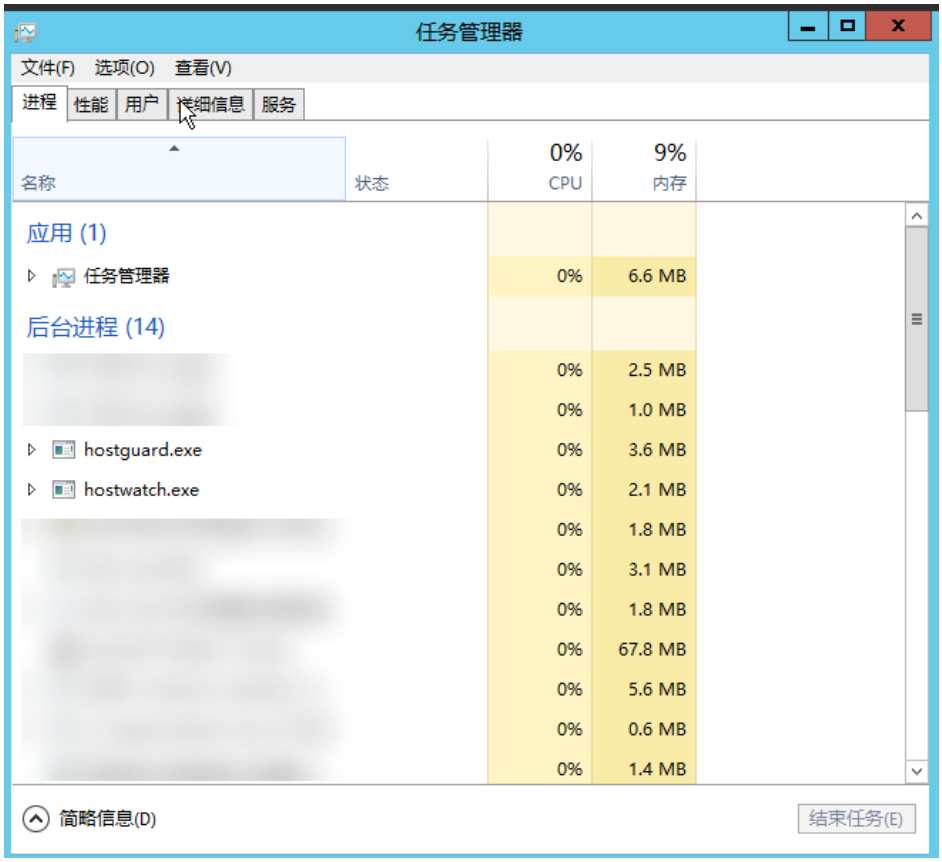
1. 单击控制台界面“安装主机安全Agent”对话框中“installAgent.ps1”，下载安装脚本。
2. 以Administrator用户登录待安装Agent的主机。
3. 将“installAgent.ps1”文件复制粘贴至待安装Agent主机的C:\Users录下。
4. 鼠标右键单击“installAgent.ps1”，选择“使用PowerShell运行”。
5. （可选）在弹出的对话框中，键入**Y**，运行安装脚本安装Agent。
   如果未出现对话框，请跳过此步骤。

图 3-3 更改执行策略



6. 运行完成后，打开任务管理器，查看存在“hostguard.exe”和“hostwatch.exe”表示Agent安装完成。

图 3-4 Agent 安装完成



7. 等待5~10分钟，返回企业主机安全控制台，在“主机安装与配置 > Agent管理 > 已安装主机”页面，查看目标服务器Agent状态。

   Agent状态显示在线，表示Agent安装成功。

----结束

通过脚本为多台云平台 Windows 主机安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在页面右上角，单击“安装主机安全Agent”，弹出“安装主机安全Agent”对话框。

步骤7 选择“弹性云服务器ECS安装”，并单击“开始配置”。

步骤8 选择安装方式。

- 选择安装模式：命令行安装
- 选择服务器操作系统：Windows
- 选择安装数量：批量

步骤9 根据界面提示，安装Agent。

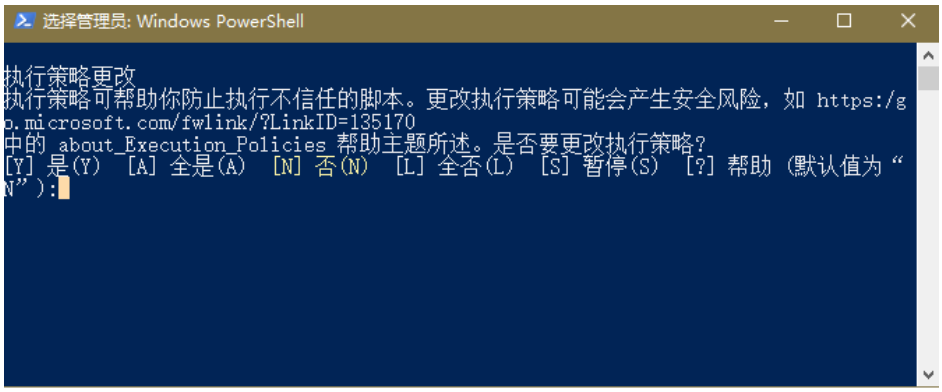
⚠ 注意

- 在任一服务器执行如下操作即可。
- 除了执行脚本的服务器，其他服务器需要设置安全组入方向允许执行脚本的服务器IP访问5985端口；如果安全组规则未允许，HSS会在安装Agent时暂时修改服务器的安全组规则，在Agent安装完成后，删除该规则。

1. 单击控制台界面“安装主机安全Agent”对话框中“windows-host-list.xlsx”，下载模板至本地。
2. 根据模板“windows-host-list.xlsx”要求，填写服务器信息并保存。
3. 返回企业主机安全控制台，单击“BatchInstallAgent.ps1”，下载安装脚本。
4. 以Administrator用户登录任意一台待安装Agent的主机。
5. 将“windows-host-list.xlsx”和“BatchInstallAgent.ps1”两个文件复制粘贴到该主机的C:\Users目录下。
6. 鼠标右键单击“BatchInstallAgent.ps1”，选择 “使用PowerShell运行”。
7. （可选）在弹出的对话框中，键入**Y**，运行安装脚本安装Agent。

   如果未出现对话框，请跳过此步骤。

图 3-5 更改执行策略



8. 脚本运行成功后，在C:\Users\Administrator目录下查看是否存在“BatchInstallAgent.log”文件。

   存在“BatchInstallAgent.log”文件表示Agent安装完成。

9. 等待5~10分钟，返回企业主机安全控制台，在“主机安装与配置 > Agent管理 > 已安装主机”页面，查看目标服务器Agent状态。

   Agent状态显示在线，表示Agent安装成功。

----结束

后续操作

在为主机安装Agent成功后，请**开启防护**。

3.2.2 线下 IDC 通过专线和代理服务器接入 HSS

3.2.2.1 方案概述

应用场景

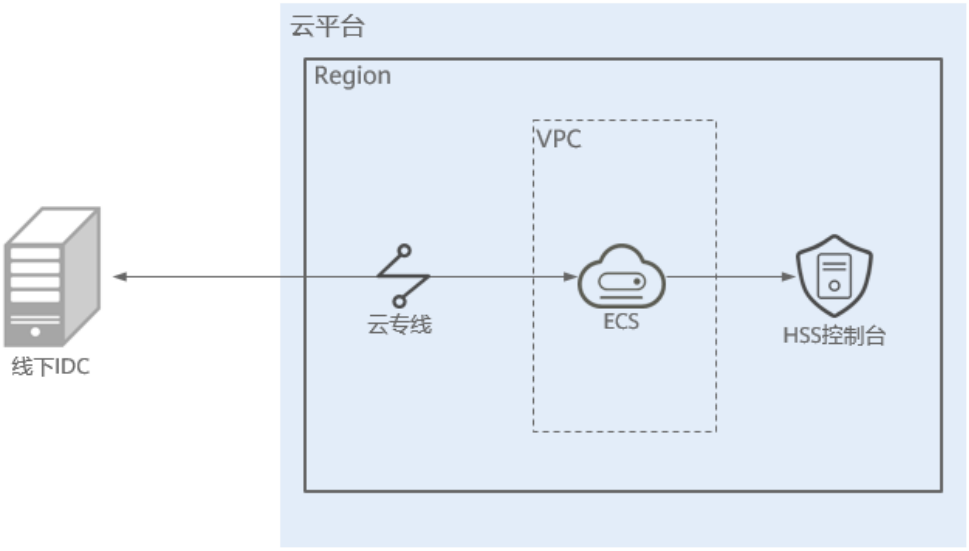
随着混合云的发展，用户对于云上云下资源实现统一安全管理的需求也越发强烈。企业主机安全支持线下IDC接入纳管，用户可以通过一个控制台实现一致的主机安全防护策略，避免因为不同平台安全水位不一致导致的攻击风险。

方案架构

线下IDC通过云专线服务与云上VPC实现网络互通，再通过云上弹性云服务器代理接入HSS，如**图3-6**所示。

- 云专线（Direct Connect），用于搭建用户本地数据中心与云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。
- 弹性云服务器（Elastic Cloud Server），是一种可随时自助获取、可弹性伸缩的云服务器，可帮助您打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。

图 3-6 线下 IDC 通过专线和代理服务器接入 HSS



3.2.2.2 资源规划

本方案示例中涉及的资源如下：

表 3-3 资源说明

资源	资源说明	数量
云专线（Direct Connect）	DC，作为连接第三方主机和云上资源的专属通道。	1
弹性云服务器（Elastic Cloud Server）	ECS，作为代理服务器，将线下IDC的请求转发至HSS后台。	1

3.2.2.3 操作流程

线下IDC通过专线和代理服务器接入HSS的流程如下：

1. **创建专线连接**
   线下IDC如果不能访问公网，需要创建专线连接云上VPC，实现网络互通。
2. **创建代理服务器**
   需要创建一台云上服务器，作为代理服务器，连接线下IDC。
3. **为代理服务器安装Agent**
   为代理服务器安装Agent，确保网络的畅通，辅助配置nginx的参数。
4. **为代理服务器安装配置nginx**
   nginx负责将线下IDC的请求转发至HSS管理后台。
5. **通过代理服务器制作Agent安装包或安装命令**
   根据线下IDC操作系统类型制作对应的安装命令（Linux）或安装包（Windows）。

6. **为线下IDC安装Agent**
   为线下IDC安装Agent，将线下IDC接入HSS实现统一管理。

3.2.2.4 实施步骤

3.2.2.4.1 创建专线连接

在不使用公网的情况下，线下IDC可以借助云专线服务，实现访问云上VPC内的服务器。

使用云专线将线下IDC接入云上VPC的详细操作请参见。

3.2.2.4.2 创建代理服务器

创建1台云上服务器，作为第三方服务器的代理服务器。

创建代理服务器

登录云控制台，申请弹性云服务器作为代理服务器，操作详情请参见《弹性云服务器用户指南》。

代理服务器规格要求如下：

- 代理服务器的CPU架构需要选择x86计算。
- 代理服务器的vCPUs需选择4vCPUs或以上规格，内存需选择8GiB或以上规格。
- 代理服务器的镜像需选择：可使用yum命令的Linux镜像。

3.2.2.4.3 为代理服务器安装 Agent

为代理服务器安装Agent，确保网络的畅通，辅助配置nginx的参数。

为代理服务器安装 Agent

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域和项目。

步骤3 单击页面左上方的 ，选择“安全 > 企业主机安全 HSS”，进入企业主机安全页面。

步骤4 在左侧导航栏选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”页面。

步骤5 选择“Agent管理 > 未安装主机”，进入“未安装主机”页面。

步骤6 在目标服务器的“操作”列，单击“安装Agent”，弹出“安装Agent”对话框。

步骤7 选择并填写服务器验证信息。

- 选择服务器验证模式：根据服务器验证方式进行选择，此处示例选择“账号密码方式”。
- 允许以root权限直连：根据服务器是否允许以root直连决定是否勾选。此处示例“勾选”。

- 服务器root密码：根据服务器实际信息进行填写。
- 服务器登录端口：根据服务器实际登录端口进行填写。此处示例“22”端口。

步骤8 单击“确认”，Agent开始安装。

步骤9 选择“已安装主机”页面，筛选查看目标服务器Agent状态。

Agent状态显示在线，表示Agent安装成功。

----结束

3.2.2.4.4 为代理服务器安装配置 nginx

nginx负责将线下IDC的请求转发至HSS后台管理后台。

为代理服务器安装配置 nginx

步骤1 登录代理服务器

步骤2 检查yum源

检查yum源是否有nginx软件包，如果没有nginx软件包需完成yum源配置，并临时绑定公网IP，待安装结束之后再解绑公网IP。

远程登录代理服务器，执行以下命令检查yum源中是否存在nginx包。

- EulerOS、CentOS、Red Hat等支持rpm安装软件的OS：**yum list nginx**
- Ubuntu、Debian等支持deb安装软件的OS：**apt list nginx**

显示如**图 nginx包存在（rpm）**或**图 nginx包存在（deb）**所示表示nginx包存在。

图 3-7 nginx 包存在（rpm）

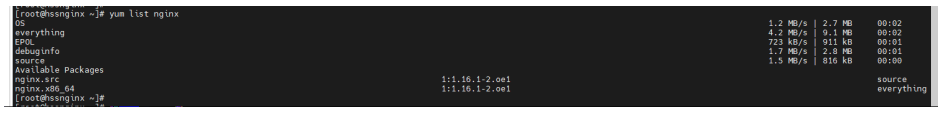
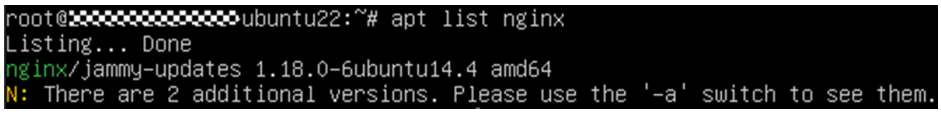


图 3-8 nginx 包存在（deb）



步骤3 安装nginx

1. 执行以下命令使用yum安装nginx。
   - EulerOS、CentOS、Red Hat等支持rpm安装软件的OS：**yum install -y nginx**
   - Ubuntu、Debian等支持deb安装软件的OS：**apt install -y nginx**

图 3-9 安装 nginx（yum）

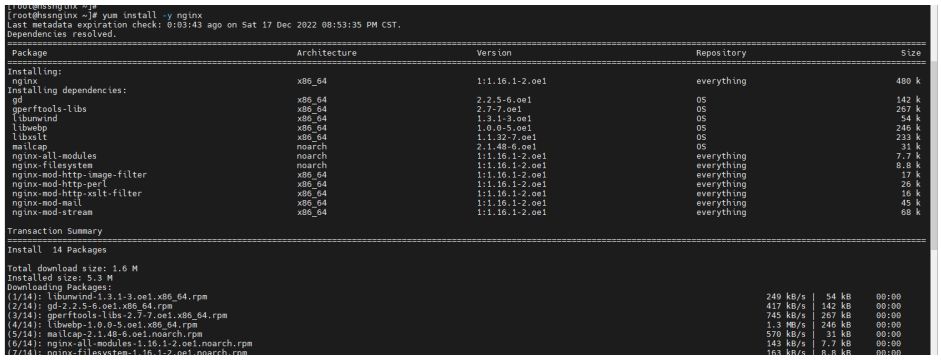
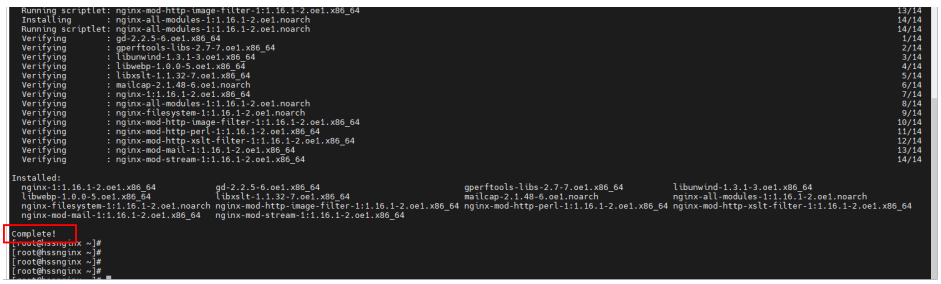


图 3-10 安装 nginx（apt）

2. 查看nginx是否安装成功。
   - EulerOS、CentOS、Red Hat等支持rpm安装软件的OS：

     自动执行安装，出现如**图 nginx安装成功（rpm）**所示“Complete!”表示安装成功。

     图 3-11 nginx 安装成功（rpm）

   - Ubuntu、Debian等支持deb安装软件的OS：

     执行命令**pkg –l nginx**，查看回显结果如**图 nginx安装成功（deb）**所示，表示安装成功。

     图 3-12 nginx 安装成功（deb）

步骤4 配置Nginx

1. 执行以下命令进入nginx目录。

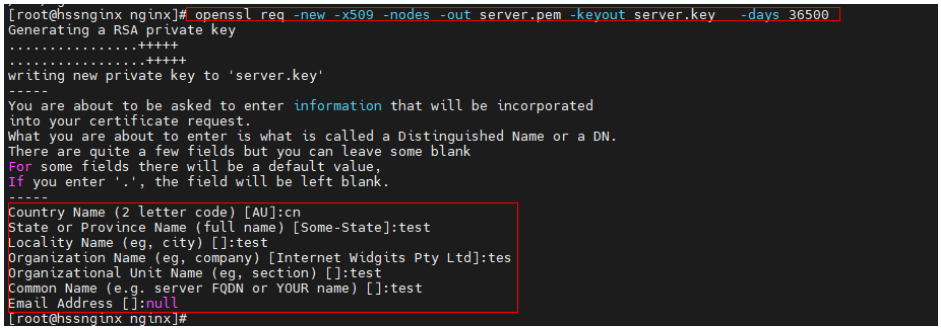
cd /etc/nginx/

2. 执行以下命令完成证书自签。

   openssl req -new -x509 -nodes -out server.pem -keyout server.key -days 36500

   命令执行后需填写证书相关信息，自定义填写即可。Country Name受长度限制，只能填写两个字符。

   图 3-13 自签证书



3. 执行以下操作修改nginx.conf。

   a. 依次执行以下命令修改nginx.conf。

      rm -f nginx.conf

      vi nginx.conf

   b. 按“i”键进入编辑模式，并将以下内容复制粘贴到nginx.conf中。

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    upstream backend_hss {
        server ADDR:10180;
    }

    server {
```

```
        listen  10180;

        server_name  ADDR;
        root         /usr/share/nginx/html;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;

        ssl    on;
        ssl_protocols   TLSv1.2;
        ssl_certificate "server.pem";
        ssl_certificate_key "server.key";
        ssl_session_cache shared:SSL:10m;
        ssl_session_timeout  10m;
        ssl_prefer_server_ciphers on;

        location / {

            limit_except GET POST PUT
            {
                deny all;
            }
            proxy_set_header Host ADDR;
            proxy_pass https://backend_hss;

            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";

       }

        error_page 404 /404.html;
            location = /40x.html {
        }

        error_page 500 502 503 504 /50x.html;
            location = /50x.html {
        }
    }
}
```

c. **可选:** 粘贴完成后，按Esc键，输入以下命令，按回车键退出，完成配置。

:wq!

d. 执行以下命令自动替换nginx.conf中的地址。

sed -i "s#ADDR#`cat /usr/local/hostguard/conf/connect.conf | grep master_address | cut -d '=' -f 2 | cut -d ':' -f 1`#g" nginx.conf

4. 执行以下操作，创建nginx的监控脚本。创建完成后，每分钟定时检测nginx运行状态

a. 依次执行以下命令，创建nginx的监控脚本。

echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab

vi /etc/nginx/nginx_monitor.sh

图 3-14 创建 nginx 监控脚本

```
[root@hss2 ~]#
[root@hss2 ~]# echo '*/1 * * * * root sh /etc/nginx/nginx_monitor.sh' >> /etc/crontab
[root@hss2 ~]#
[root@hss2 ~]#
[root@hss2 ~]# vi /etc/nginx/nginx_monitor.sh
```

b. 将以下内容复制粘贴到nginx_monitor.sh中。

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
fi
```

图 3-15 配置 nginx_monitor.sh

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
fi
~
~
~
```

c. 粘贴完成后，按Esc键，输入以下命令，按回车键退出，完成配置。

:wq!

5. 等待1分钟后，执行以下命令查看nginx进程是否已经启动。

ps -ef | grep nginx

界面回显如**图 nginx进程启动成功**所示，表示nginx进程已启动，继续执行**通过代理服务器制作Agent安装包或安装命令**。

图 3-16 nginx 进程启动成功

```
[root@hss2 ~]#
[root@hss2 ~]# ps -ef | grep nginx
root      5123     1  0 17:47 ?        00:00:00 nginx: master process /usr/sbin/nginx
nginx     5124  5123  0 17:47 ?        00:00:00 nginx: worker process
nginx     5125  5123  0 17:47 ?        00:00:00 nginx: worker process
root      5971  3592  0 17:48 tty1     00:00:00 grep --color=auto nginx
[root@hss2 ~]#
```

----结束

3.2.2.4.5 通过代理服务器制作 Agent 安装包或安装命令

根据线下IDC操作系统类型，通过代理服务器制作对应的Agent安装命令（Linux）或Agent安装包（Windows）。

通过代理服务器制作 Agent 安装命令（Linux）

步骤1 登录代理服务器

步骤2 执行以下命令进入tmp目录。

cd /tmp

步骤3 依次执行以下命令查看private_ip.conf中的IP是否为实际可用IP。

echo `hostname -I` > private_ip.conf

cat private_ip.conf

图 3-17 查看 IP

```
[root@hssnginx tmp]#
[root@hssnginx tmp]# echo `hostname -I` > private_ip.conf
[root@hssnginx tmp]# cat private_ip.conf
192.168.1.63
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

查看private_ip.conf中的IP是否为代理服务器实际可用IP，即线下IDC需可以正常连接该IP。如果该IP不是实际可用IP，需手动将该IP修改为实际可用IP。

步骤4 确认IP可用后，依次执行以下操作制作安装命令。

1. 依次执行以下命令，生成安装命令。
   - x86 rpm软件包镜像的命令：

     echo -e "# for Linux x86 CentOS EulerOS OpenSUSE Fedora\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.x86_64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > x86_rpm_install.sh
   - x86 deb软件包镜像的命令：

     echo -e "# for Linux x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh
   - Arm rpm软件包镜像的命令：

     echo -e "# for Linux ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.rpm' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && rpm -ivh hostguard.aarch64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm" > arm_rpm_install.sh
   - Arm deb软件包镜像的命令：

     echo -e "# for Linux ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh
2. 执行以下命令，替换可用IP。

   无需修改，执行即可。

   sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

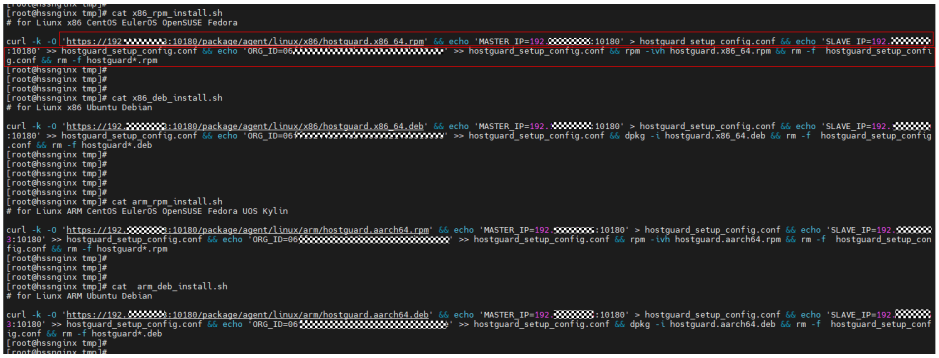
说明

- x86_rpm_install.sh中的安装命令适用于x86架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora。
- x86_deb_install.sh中的安装命令适用于x86架构，deb软件包管理的镜像，如Ubuntu、Debian。
- arm_rpm_install.sh中的安装命令适用于arm架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora、UOS、Kylin。
- arm_deb_install.sh中的安装命令适用于arm架构，deb软件包管理的镜像，如Ubuntu、Debian。

步骤5 执行如下命令，查看生成的安装命令。生成的安装命令将用于Linux服务器安装Agent。

- 查看x86 rpm软件包镜像的安装命令：**cat x86_rpm_install.sh**
- 查看x86 deb软件包镜像的安装命令：**cat x86_deb_install.sh**
- 查看Arm rpm软件包镜像的安装命令：**cat arm_rpm_install.sh**
- 查看Arm deb软件包镜像的安装命令：**cat arm_deb_install.sh**

图 3-18 查看 x86 rpm 软件包镜像生成的命令



----结束

通过代理服务器制作 Agent 安装包（Windows）

步骤1 执行以下命令进入tmp目录。

cd /tmp

步骤2 依次执行以下命令，制作Windows的Agent安装压缩包。

curl -k -O https://`cat private_ip.conf`:10180/package/agent/windows/hostguard_setup.exe && echo '[system]' > hostguard_setup_config.ini && echo 'master=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'slave=`cat private_ip.conf`:10180' >> hostguard_setup_config.ini && echo 'orgid='`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2` >> hostguard_setup_config.ini

zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini

说明

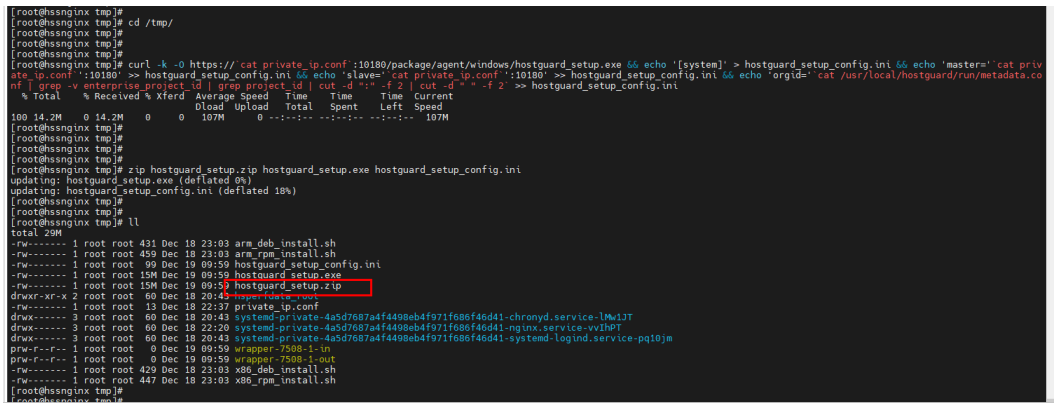
如果代理服务器没有zip命令，需先执行以下命令安装zip插件。

yum install -y zip

步骤3 执行以下命令查看生成的安装包，安装包将用于Windows服务器Agent的安装使用。

ll

图 3-19 Windows 安装包



----结束

3.2.2.4.6 为线下 IDC 安装 Agent

为线下IDC安装Agent，完成后可在HSS实现对服务器的统一管理。

为 Linux 服务器安装 Agent

步骤1 复制**通过代理服务器制作Agent安装命令（Linux）**制作的Linux安装命令。

步骤2 使用root账号登录目标Linux服务器，粘贴并执行Linux安装命令。

界面回显如**图 Agent安装完成**所示，表示Agent安装完成。

图 3-20 Agent 安装完成

步骤3 等待约10分钟后，在HSS控制台左侧导航栏，选择“资产管理 > 主机管理”，进入云服务器页面。

步骤4 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

为 Windows 服务器安装 Agent

步骤1 将**通过代理服务器制作Agent安装包（Windows）**制作的Windows安装包，拷贝到本地PC机。

步骤2 将安装包上传到需要安装Agent的目标Windows服务器。

步骤3 使用Administrator账号登录服务器。

步骤4 解压安装包，双击“hostguard_setup.exe”，根据安装向导安装Agent。

生成的zip安装包拷贝到本地后一定要进行解压后再执行安装，否则将无法安装。

步骤5 安装完成后，在“Windows任务管理器”中查看到进程“HostGuard.exe”和“HostWatch.exe”，表示Agent安装完成。

步骤6 等待约10分钟后，在HSS控制台左侧导航栏，选择“资产管理 > 主机管理”，进入云服务器页面。

步骤7 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

3.2.3 通过 CBH 安装 HSS 的 Agent

应用场景

如果您已申请并使用云堡垒机（Cloud Bastion Host，CBH）服务专业版，可通过云堡垒机服务为主机安装企业主机安全的Agent。此安装方式无需获取主机账户密码或执行复杂的安装命令，可便捷的为单台或多台主机安装Agent。

前提条件

- 已通过云堡垒机纳管主机资源。
- 待安装Agent的主机为SSH协议类型的Linux主机，且主机网络连接正常。
- 已获取云堡垒机的系统管理员账号。

操作步骤

步骤1 使用系统管理员账号登录云堡垒机系统。

步骤2 在左侧导航栏，选择“运维 > 快速运维”，进入“快速运维”界面。

步骤3 选择“脚本控制台”页签。

图 3-21 进入脚本控制台

步骤4 配置脚本运维信息。相关参数说明请参见**表 脚本运维参数说明**。

图 3-22 配置脚本运维信息

表 3-4 脚本运维参数说明

参数	说明
执行脚本	选择脚本“HSS-Agent.sh”。
脚本参数	不填写。
执行账户	单击“选择”，选择待安装Agent的主机账户或账户组。
更多选项	可选设置。脚本任务默认在主机的Sudoers文件下执行，当主机账户没有该文件的执行权限时，需勾选“提权执行”。

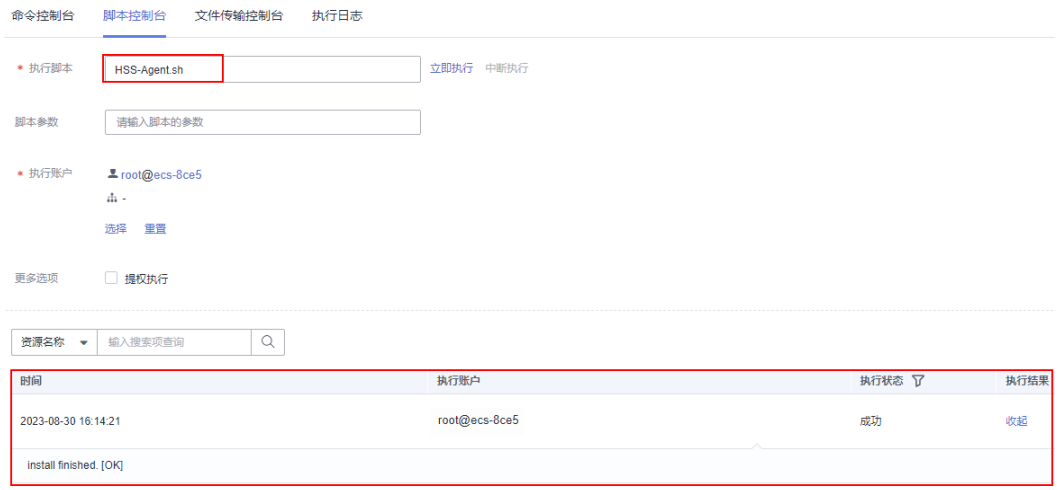
步骤5 单击“立即执行”，执行脚本任务。

图 3-23 执行脚本任务

步骤6 脚本任务执行成功后，在执行结果列单击“展开”，展开执行结果。

执行结果显示“install finished.[OK]”表示Agent安装成功。

图 3-24 脚本任务执行成功



步骤7 在企业主机安全控制台，确认Agent安装结果。

1. 登录企业主机安全控制台。
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。
3. 在“云服务器”页签，查看目标主机的Agent状态。

   Agent状态为“在线”，表示Agent安装成功。

----结束

3.3 为容器安装 Agent

3.3.1 为云 CCE 集群安装 Agent

操作场景

本指导适用于在云CCE集群上安装Agent，按照本指导配置完成后，HSS将自动在集群节点上安装Agent，并能够随集群扩容自动为新节点安装Agent，在集群缩容时同步卸载Agent。

前提条件

为CCE集群安装Agent前，请先将CCEOperatePolicy权限授予HSS，详细操作请参见**授权管理**。

约束与限制

- 容器运行时限制：Docker、Containerd。
- 集群类型限制：CCE标准版、CCE Turbo版。
- 节点资源剩余要求：内存必须50MiB及以上，CPU必须200m及以上。
- 在集群上安装Agent时，HSS会在集群上创建HSS的命名空间。

为云 CCE 集群安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 在“集群”页签，单击“安装容器安全Agent”，弹出“容器资产接入与安装”对话框。

步骤6 选择“CCE集群安装”，并单击“开始配置”。

步骤7 勾选目标集群，并单击“下一步”。

步骤8 配置Agent相关参数。参数说明如**表 Agent配置参数说明**所示。

表 3-5 Agent 配置参数说明

参数名称	参数说明
配置规则	选择Agent配置规则。 • 默认规则：容器运行时的sock地址为通用地址，Agent将默认安装在没有配置污点的节点上。 • 自定义规则：如果您的容器运行时sock地址非通用地址需要修改，或仅需要在指定的节点上安装Agent，可选择该规则。 **说明** • 如果容器运行时的sock地址不正确，可能导致集群接入HSS后，部分HSS功能不能正常使用。 • 在进行容器运行时配置时，建议全选所有运行时类型。

参数名称	参数说明
高级配置（可选）	配置规则选择“自定义规则”时，支持配置。 单击展开所有高级配置项，“开启Agent自动升级”项，默认为展开状态。 • 开启Agent自动升级 是否开启Agent自动升级，勾选即开启，开启后，每日00:00～06:00，企业主机安全将自动升级低版本的Agent为最新版，以便为您提供更好的服务。 • 节点选择器配置 填写需要安装Agent的节点标签的“键”和“值”，单击“确认添加”。不添加任何节点标签时，默认在所有没有配置污点的节点上安装Agent。 • 容忍度配置 如果在进行“节点选择器配置”时，添加了配有污点的节点标签，则请填写污点的“键”和值以及污点的效果，单击“确认添加”，允许在该节点上安装Agent。

步骤9 配置完成，单击“确认”，开始安装HSS Agent。

步骤10 在集群列表中，查看集群状态为“运行中”，表示集群接入HSS成功。

----结束

后续操作

在为集群安装Agent成功后，请为其**开启防护**。

3.3.2 为非集群节点安装 Agent

操作场景

如果您有非集群节点需要开启容器安全防护，需为该节点安装Agent。

前提条件

待安装Agent的节点所在VPC内已有至少一个Agent在线的节点。否则请参考**为主机安装Agent**中提供的命令行安装方式安装Agent。

为非集群节点安装 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“非集群节点”页签。

步骤6 找到Agent状态为“未安装”的节点，单击“操作”列的“安装Agent”。

步骤7 在安装Agent页面，选择服务器验证模式。

- **账号密码方式**
  - 勾选“允许以root权限直连”

    表示服务器可以通过root账号直接登录，您填写服务器root密码、服务器登录端口后，HSS将通过您的root账号为主机安装Agent。
  - 不勾选“允许以root权限直连”

    表示服务器不能通过root账号直接登录，您填写其他可以登录主机的账号信息（其中root密码用于提权），HSS将通过您提供的账号信息为主机安装Agent。
- **密钥方式**

  仅支持自建密钥。单击“上传密钥”，上传后缀为.pem的自建密钥文件。

步骤8 确认信息无误后，单击“确定”，Agent开始安装。

您可以查看“Agent状态”列，确认Agent安装状态。Agent状态显示“在线”，表示安装完成。

----结束

后续操作

在为节点安装Agent成功后，请为其**开启防护**。

3.4 开启防护

开启企业版/旗舰版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“资产管理 > 主机管理”，进入“云服务器”界面。

步骤5 单击“确认”，开启防护。目标主机的“防护状态”为“防护中”，则表示企业版/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。

步骤6 （可选）配置告警通知、防护策略、主机登录保护以及开启恶意程序隔离查杀。

- **配置告警通知**

  企业主机安全防护开启成功后，默认将检测到的风险告警信息呈现在控制台，如需及时了解主机、容器或网页存在的安全风险，您可以开启告警通知，开启后，

一旦企业主机安全检测到风险，将通过短信或邮件等方式通知您。具体操作请参见**告警配置**。

- **配置防护策略**

  每个企业主机安全版本都对应一组防护策略，这些策略默认预置了防护规则。您可以根据自身业务需求，开启或关闭防护策略、调整防护规则。具体操作请参见**策略管理**。

- **配置登录保护**

  您可以通过**双因子认证**、**配置常用登录地**、**配置常用登录IP**以及**配置SSH登录IP白名单**，来增强主机登录安全性。

- **开启恶意程序隔离查杀**

  开启恶意程序隔离查杀功能后，企业主机安全将自动隔离识别到的后门、木马、蠕虫等恶意程序，帮助您自动处理系统存在的安全风险。具体操作请参见**开启恶意程序隔离查杀**。

----结束

开启网页防篡改版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“主机防御 > 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5 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，单击“添加并开启防护”。

步骤6 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。

- 选择“主机防御 > 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防护已开启。

说明

- 开启网页防篡改后，如果需要更新网站请添加特权进程或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。

----结束

开启容器版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在目标服务器所在行的“操作”列，单击“开启防护”，弹出“您确认要对以下容器节点开启防护吗？”对话框。

步骤6 确认节点信息并选择开启方式。

注意

步骤7 阅读并勾选《容器安全服务免责声明》。

步骤8 单击“确定”，开启节点防护，目标节点的“容器防护状态”变更为“防护中”，说明该节点已开启防护。

步骤9 （可选）配置告警通知、防护策略、主机登录保护以及开启恶意程序隔离查杀。

- **配置告警通知**

  企业主机安全防护开启成功后，默认将检测到的风险告警信息呈现在控制台，如需及时了解主机、容器或网页存在的安全风险，您可以开启告警通知，开启后，一旦企业主机安全检测到风险，将通过短信或邮件等方式通知您。具体操作请参见**告警配置**。

- **配置防护策略**

  每个企业主机安全版本都对应一组防护策略，这些策略默认预置了防护规则。您可以根据自身业务需求，开启或关闭防护策略、调整防护规则。具体操作请参见**策略管理**。

- **配置登录保护**

  您可以通过**双因子认证**、**配置常用登录地**、**配置常用登录IP**以及**配置SSH登录IP白名单**，来增强主机登录安全性。

- **开启恶意程序隔离查杀**

  开启恶意程序隔离查杀功能后，企业主机安全将自动隔离识别到的后门、木马、蠕虫等恶意程序，帮助您自动处理系统存在的安全风险。具体操作请参见**开启恶意程序隔离查杀**。

----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。待检测完成后，您可以参考如下方式查看检测详情：

步骤1 在“资产管理 > 主机管理 > 云服务器”页面中，找到目标服务器。

步骤2 在目标服务器所在行的“风险状态”列，查看服务器风险检测状态。

表 3-6 风险状态说明

状态	说明
未检测	服务器未开启防护，未检测风险。
无风险	已对服务器进行了全面的安全检查，未发现风险，或者开启防护不久，还未检测到风险。

状态	说明
有风险	服务器存在安全风险。

步骤3 鼠标悬停在风险状态上方，可查看风险分布。

单击风险数值，可进入详情页面，查看具体内容。

----结束

高级防御功能

企业主机安全提供了系列高级防御功能，您可以结合业务实际情况选择开启或使用，以增强主机和容器的安全防护水平。具体请参见表3-7。

表 3-7 高级防御功能

功能	说明	版本限制
应用防护	应用防护功能旨在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。	旗舰版、网页防篡改版、容器版
勒索病毒防护	勒索病毒防护功能能够实现对勒索病毒的检测和防御；同时，还提供数据备份功能，支持定时自动备份和勒索即刻备份，帮助您抵御勒索病毒，降低业务受损风险。 开启容器版防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略。	旗舰版、网页防篡改版、容器版
应用进程控制	应用进程控制是一种用于保障服务器上运行的应用程序和进程安全的功能。它能够自动识别并分析应用进程，将其划分为可信、可疑及恶意三类，同时允许可信进程运行，针对可疑、恶意进程运行进行告警，可以帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。	旗舰版、网页防篡改版、容器版
病毒查杀	病毒查杀功能采用云端与本地相结合的病毒防护机制，能够全面扫描主机中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可以根据实际需求，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”任务，及时发现并清理病毒文件，增强业务系统的病毒防御能力。	专业版、企业版、旗舰版、网页防篡改版、容器版
动态端口蜜罐	动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。	旗舰版、网页防篡改版、容器版
容器防火墙	容器防火墙能够实现Pod、工作负载以及节点粒度的网络隔离，可有效抵御横向渗透攻击，确保业务权限最小化，从而保障用户业务的安全性和稳定性。	容器版

功能	说明	版本限制
容器集群防护	容器集群防护功能支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。	容器版

3.4.1 开启基础版/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。

如果您申请的是网页防篡改版，请在“主机防御 > 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“主机防御 > 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。

如果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

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

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。如果关闭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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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”。

说明

如果Linux主机安装的Agent版本为3.2.8及以上版本或Windows主机安装的Agent版本为4.0.16及以上版本，开启旗舰版防护时，系统会自动为主机开启勒索病毒防护，勒索病毒防护开启后，您可以根据自身业务情况配置指定的诱饵防护目录；另外，建议您同时开启勒索备份，提升勒索防护的事后恢复能力，最小化降低业务受损程度。详细操作请参见**修改防护策略**。

步骤6 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。

如果目标主机的“防护状态”为“开启”，则表示企业版/旗舰版防护已开启。

说明

- 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“有风险主机”，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。

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。

3.4.2 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 3-8 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网站内容更新。 2. 主动备份恢复 如果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 配置远端备份服务器后，HSS会在防护目录下的文件发生变化时触发备份。 如果本地主机上的文件目录和备份目录失效，用户可以登录到远端备份服务器，在备份路径下获取备份文件并手动恢复被篡改的网页。备份路径可在“管理远端备份服务器”页面查看，查看详细操作请参考**修改远端备份**。
动态网页防护	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；提供Tomcat应用运行时自我保护。

前提条件

- 在“主机防御 > 网页防篡改 > 防护配置”页面中，目标服务器的“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，目标服务器的“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，网页防篡改提供指定目录的保护：

- 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“主机防御 > 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5 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6 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。

- 选择“主机防御 > 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”，目标主机所在行的“防护状态”为“防护中”，且“版本”为“网页防篡改版”，则表示网页防篡改防护已开启。

----结束

须知

- 一个配额只能绑定一个主机，且只能绑定Agent在线的主机。
- 如果Linux主机安装的Agent版本为3.2.8及以上版本或Windows主机安装的Agent版本为4.0.16及以上版本，开启网页防篡改防护时，系统会自动为主机开启勒索病毒防护，勒索病毒防护开启后，您可以根据自身业务情况配置指定的诱饵防护目录；另外，建议您同时开启勒索备份，提升勒索防护的事后恢复能力，最小化降低业务受损程度。详细操作请参见**修改防护策略**、**开启勒索备份**。
- 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“主机防御 > 网页防篡改 > 防护配置”页面，选中目标主机，并单击“关闭防护”，关闭对目标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，如果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。

3.4.3 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。

如果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。

约束限制

HSS暂仅支持为Docker和Containerd容器提供安全防护。

前提条件

- 页面“容器节点管理”中，目标节点的“Agent状态”为“在线”、“防护状态”为“未防护”。
- 已在云容器引擎成功创建节点。

操作步骤

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 在弹出的提示框中，确认服务器信息。

步骤7 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。
- 如果Linux主机安装的Agent版本为3.2.8及以上版本或Windows主机安装的Agent版本为4.0.16及以上版本，开启容器版防护时，系统会自动为主机开启勒索病毒防护，勒索病毒防护开启后，您可以根据自身业务情况配置指定的诱饵防护目录；另外，建议您同时开启勒索备份，提升勒索防护的事后恢复能力，最小化降低业务受损程度。详细操作请参见**修改防护策略**、**开启勒索备份**。

----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。

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。

4 查看防护总览

企业主机安全在控制台提供总览页面，实时展示您所有资产的安全评分、安全风险、防护地图等，帮助您了解主机和容器的安全状态以及存在的安全风险。

查看防护总览

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“总览”，进入总览页。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看资产安全信息，相关信息说明请参见**表 总览页信息说明**。

表 4-1 总览页信息说明

区域	说明
资源概况	展示未防护主机或容器占比、待升级Agent数量。 • 单击未防护数值可跳转到主机或容器管理页面查看未防护列表。 • 单击待升级Agent数值可跳转到Agent管理页面查看并升级Agent。 **说明** 企业主机安全会持续优化提升服务能力，包括但不限于新增功能、优化缺陷，因此会定期迭代版本。请及时将主机上的Agent升级为最新版，以便您可以享受到更好的企业主机安全，具体操作请参见**升级Agent**。

区域	说明
安全评分	安全风险评分范围为0~100分，无风险资产默认为100分，HSS会根据资产中存在的基线风险、漏洞风险、入侵风险和资产风险等执行扣分，评分越低表示资产中存在的安全风险越多。为了保护的您资产安全，建议您及时处理安全风险，提高安全评分： 1. 在“安全评分”模块，单击“立即查看”。 2. 在“安全风险处理”弹窗中，查看扣分项，单击 ⌄ 展开扣分明细。 3. 单击扣分项右侧的“前往处理”，可跳转至对应的风险列表，您可以根据风险详情和修复建议进行修复。 具体各扣分项，提高评分的方法请参见**安全评分标准及提高评分方法**。 4. 修复风险后，单击“重新体检”，刷新评分。
热点资讯	展示最新的热点漏洞信息。
安全风险	展示HSS检测到您资产中存在的安全风险。 ● 主机风险 – 需紧急处理告警/总数（近24小时）：处理优先级为紧急的告警数量和告警总数。 单击需紧急处理的告警数值，可跳转到“安全告警事件”界面查看和处理告警，详细操作请参见**处理主机告警事件**。 – 紧急优先级修复漏洞/总数：修复优先级为紧急的漏洞数量和漏洞总数。 单击需紧急修复的漏洞数值，可跳转到“漏洞管理”界面查看和处理漏洞，详细操作请参见**处理漏洞**。 – 基线风险：待处理的基线风险总数。 单击待处理基线风险数值，可跳转到基线检查界面查看和修复基线风险，详细操作请参见**查看并处理基线检查结果**。 – 待处理可疑进程：待处理的可疑进程事件总数。 单击待处理可疑进程数值，可跳转到“应用进程控制”界面查看和处理可疑进程，详细操作请参见**查看并处理可疑进程**。 ● 容器风险 高优先级修复漏洞/总数：修复紧急度为高危的漏洞数量和漏洞总数。 单击高优先级修复漏洞数值，可跳转到“镜像漏洞”界面查看漏洞修复建议，详细操作请参见**镜像漏洞**。 ● 安全风险趋势 展示资产最近七天的安全风险趋势图。

区域	说明
防护地图	展示资产开启安全防护的情况。 • 资产总数：当前区域下的资产总数。 单击资产总数值，可跳转到“资产概览”界面，查看资产分布详情及防护状态统计。 • 未防护/主机总数：未防护主机数量和主机总数。 单击未防护主机数值，可跳转到“主机管理”界面，查看主机并开启防护，详细操作请参见**开启主机防护**。 • 未防护/容器总数：未防护容器数量和容器总数。 单击未防护容器数值，可跳转到“容器管理”界面，查看容器并开启防护，详细操作请参见**开启容器节点防护**。 • 漏洞库更新时间：最近一次漏洞库更新时间。 • 安全防护功能开启情况：对应防护功能的开启数量和防护功能累计扫描/检测项数量。 单击对应安全防护功能右侧的“查看详情”，可跳转到相应防护功能界面，查看防护情况。
相关安全服务	展示和HSS关联的安全服务，单击服务标识，可跳转到对应服务的控制台。

----结束

安全评分标准及提高评分方法

HSS安全评分满分100分表示无任何风险，分数越低表示安全风险越多。安全评分模块涉及主机开启防护后的防护项（漏洞、合规、入侵检测、资产、镜像）和未开启防护的资产，各模块发现一项风险执行一次扣分，直至该模块分扣完为止，各模块分值如下：

- 漏洞风险：无风险满分20分，扣分标准及提高评分的方法请参见**表 漏洞风险扣分标准及提高评分的方法**。
- 合规风险：无风险满分20分，扣分标准及提高评分的方法请参见**表 合规风险扣分标准及提高评分的方法**。
- 入侵风险：无风险满分30分，扣分标准及提高评分的方法请参见**表 入侵风险扣分标准及提高评分的方法**。
- 资产风险：无风险满分10分，扣分标准及提高评分的方法请参见**表 资产风险扣分标准及提高评分的方法**。
- 镜像安全风险：无风险满分10分，扣分标准及提高评分的方法请参见**表 镜像风险扣分标准及提高评分的方法**。
- 未开启防护的资产：无风险满分10分，扣分标准及提高评分的方法请参见**表 未开启防护的资产扣分标准及提高评分的方法**。

表 4-2 漏洞风险扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未处理漏洞	存在未处理的紧急漏洞	所有版本	10	√	按照漏洞修复建议进行漏洞修复，修复后重新扫描漏洞，更新评分。 • 修复漏洞操作请参见**处理漏洞**。 • 扫描漏洞操作请参见**扫描漏洞**。
	存在未处理的高危漏洞	所有版本	3	√	
	存在未处理的中危漏洞	所有版本	1	√	
	存在未处理的低危漏洞	所有版本	0.1	√	
未进行漏洞扫描	1个月内未进行漏洞扫描	所有版本	15	×	• 对于HSS基础版无漏洞扫描功能，建议升级到企业版或旗舰版后对主机进行漏洞扫描。 • 对于HSS企业版/旗舰版/网页防篡改版，建议执行漏洞扫描，详细操作请参见**扫描漏洞**。

表 4-3 合规风险扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未处理不合规项	存在未处理的高危不合规项	所有版本	10	√	按照基线修复建议修复基线检查不合规项，修复完成后，重新执行基线检查，更新评分。 • 修复基线风险操作请参见**查看并处理基线检查结果**。 • 执行基线检查的操作请参见**执行基线检查**。
	存在未处理的中危不合规项	所有版本	3	√	
	存在未处理的低危不合规项	所有版本	1	√	
存在弱口令	存在弱口令	所有版本	10	√	修改检测到的弱口令。

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未开启弱口令检查	未开启弱口令检查策略	所有版本	10	×	开启“弱口令检测”策略对主机进行弱口令检查，详细操作请参见**查看和编辑策略**。
未进行基线配置检查	1个月内未进行基线配置检查	所有版本	10	×	• 对于HSS基础版无基线检查的风险配置检查功能，建议升级到企业版或旗舰版对主机进行基线检查。 • 对于HSS企业版/旗舰版/网页防篡改版，建议开启“配置检测”策略并执行风险配置检查，详细操作请参见**查看和编辑策略**。

表 4-4 入侵风险扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未处理告警事件	存在未处理的致命告警事件	所有版本	10	√	按告警事件处置建议处置告警事件，处置完成后，HSS会自动更新评分，详细操作请参见**处理主机告警事件**和**处理容器告警事件**。
	存在未处理的高危告警事件	所有版本	3	√	
	存在未处理的中危告警事件	所有版本	1	√	
	存在未处理的低危告警事件	所有版本	0.1	√	

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未开启安全防护	未开启任何安全策略	所有版本	30	×	对于HSS企业版/旗舰版/网页防篡改版/容器版，需开启相关防护策略，详细操作请参见**查看和编辑策略**。 相应版本需开启的入侵检测策略如下： ● 企业版 – Linux：webshell检测、文件保护、HIPS检测、登录安全检测、恶意文件检测、进程异常行为、root提权、实时进程、rootkit检测。 – Windows：AV检测、webshell检测、HIPS检测、登录安全检测、实时进程。 ● 旗舰版/网页防篡改版 – Linux：集群入侵检测、webshell检测、文件保护、HIPS检测、登录安全检测、恶意文件检测、端口扫描检测、进程异常行为、root提权、实时进程、rootkit检测。 – Windows：AV检测、webshell检测、HIPS检测、登录安全检测、实时进程。 ● 容器版 集群入侵检测、容器逃逸、webshell检测、容器文件监控、容器进程白名单、镜像异常行为。
	未开启登录安全策略	所有版本	10	×	对于HSS企业版/旗舰版/网页防篡改版/容器版，需开启“登录安全检测”策略应用到主机，详细操作请参见**查看和编辑策略**。

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
	未开启勒索防护策略	旗舰版	15	×	对于HSS旗舰版/网页防篡改版/容器版支持勒索病毒防护功能，您需开启勒索防护策略、勒索备份策略（未配置扣10分）并应用到主机，提升主机勒索病毒防御能力，详细操作请参见**开启勒索病毒防护**。
	未开启网页防篡改策略	网页防篡改版	20	×	对于HSS网页防篡改版，需开启网页防篡改并应用到主机，详细操作请参见**网页防篡改版**。
	未开启容器运行时检测策略	容器安全版	20	×	对于HSS容器版，需开启“容器逃逸”、“容器进程白名单”、“容器文件监控”和“容器信息收集”策略并应用到主机，详细操作请参见**查看和编辑策略**。

表 4-5 资产风险扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
开放端口	开放的TCP/UDP高危端口	所有版本	1	√	建议您关闭不需要的端口，如果需要开放该端口，请前往“资产管理 > 主机指纹 > 开放端口”页面，对该端口执行忽略操作。
未开启资产发现	未开启资产发现策略	所有版本	5	×	• 对于HSS企业版无资产发现功能，建议升级到旗舰版为主机开启资产发现策略。 • 对于HSS旗舰版/网页防篡改版建议开启“资产发现”策略，详细操作请参见**查看和编辑策略**。

表 4-6 镜像风险扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
存在风险镜像	存在高风险的镜像	容器版	3	√	重新制作镜像后扫描镜像，更新评分。
	存在中风险的镜像	容器版	1	√	
	存在中风险的镜像	容器版	0.1	√	
未进行镜像安全扫描	1个月未进行镜像安全扫描	容器版	5	×	对于HSS容器版建议执行镜像安全扫描。详细操作请参见如下： ● **管理本地镜像**

表 4-7 未开启防护的资产扣分标准及提高评分的方法

分类	安全扣分项	影响HSS版本	单项扣分值	是否按风险个数叠加计算扣分	提高评分方法
未开启主机安全防护	未开启主机安全防护的主机	所有版本	0.1~1	√	对于未开启防护的主机，扣分标准为： ● 1个重要资产扣1分。 ● 1个一般资产扣0.5分。 ● 1个测试资产扣0.1分。 建议您尽快为主机开启安全防护，详细操作请参见**开启主机防护**。

5 资产管理

5.1 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。

查看资产概览

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“资产管理 > 资产概览”，进入资产概览总览页。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看资产状态和资产清点情况。

- **资产分布**：展示“主机节点”“、容器节点”分布数量。单击环形图占比分类，可跳转至对应的节点服务器列表页面。
- **Agent状态**：展示Agent状态为“在线”、“离线”、“未安装”三种状态的服务器分布数量。单击环形图占比分类，可跳转至对应的服务器列表页面。
- **主机节点防护状态**：展示“未防护”和“防护中”的服务器分布数量。单击环形图占比分类，可跳转至对应的服务器列表页面。如需开启防护请参见**开启防护**。
- **容器节点防护状态**：展示“未防护”和“防护中”的容器节点分布数量。单击环形图占比分类，可跳转至对应的节点服务器列表页面。如需开启防护请参见**开启防护**。
- **操作系统分布**：展示操作系统类型分布数量及占比。单击环形图占比分类，可跳转至对应的服务器列表页面。

- **资产清点**：展示资产清点情况，包括账号、开放端口、进程、软件、自启动项、Web应用、Web服务、Web框架、Web站点、中间件、数据库。单击各资产项数值，可跳转至对应的资产列表页面。

----结束

5.2 主机指纹

5.2.1 采集主机资产指纹

操作场景

HSS提供主机指纹采集功能，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。本章节为您介绍主机资产指纹采集项以及如何采集主机资产指纹。

约束与限制

主机指纹功能仅企业主机安全企业版、旗舰版、网页防篡改版、容器版支持。

主机资产指纹采集内容

主机资产指纹采集项如**表 主机资产指纹特性**所示，且每个采集项有固定的采集周期，资产指纹功能会定期自动采集主机资产指纹。如果您使用的HSS为旗舰版及以上版本，可自定义资产指纹采集周期，详细操作请参见**资产发现**。

表 5-1 主机资产指纹特性

功能项	功能描述	支持的操作系统	自动检测周期
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	每小时自动检测

功能项	功能描述	支持的操作系统	自动检测周期
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	每30秒自动检测
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	每小时自动检测
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

功能项	功能描述	支持的操作系统	自动检测周期
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	每小时自动检测
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04:10）
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04:10）
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04:10）
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04:10）
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04:10）
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04:10）

手动采集单个主机指纹最新数据

针对Web应用、Web服务、Web框架、Web站点、中间件、数据库这些资产，如果您想实时查看最新的数据，可手动采集指纹信息。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 单击指纹列表的目标类型，单击右侧列表上方“立即采集”任务自动创建完成。

目前仅支持Web应用、Web服务、Web框架、Web站点、中间件、数据库支持实时手动采集更新，其他类型每天会自动执行采集更新。

步骤8 自动执行完成之后，“最后采集时间”将会更新，可查看最新的主机资产信息。

----结束

后续操作

主机指纹采集完成后，即可查看最新的资产指纹数据，相关介绍请参见**查看主机资产指纹**。

5.2.2 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，如果发现有可疑资产信息，请手动处理。

本章节为您介绍如何在控制台查看采集到的主机资产指纹。关于各指纹的介绍请参见**采集主机资产指纹**。

约束与限制

主机指纹功能仅企业主机安全企业版、旗舰版、网页防篡改版、容器版支持。

查看所有主机资产信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“资产管理 > 主机指纹”，进入“主机指纹”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看主机指纹信息。

步骤7 单击指纹列表的目标指纹类型，查看对应资产信息。

步骤8 （可选）清理风险资产。

如果您清点后发现有风险的资产请及时排除。

对于危险端口，建议按如下进行处置：

- 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。
- 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。

----结束

查看单主机资产信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 单击指纹列表的目标指纹类型，查看对应资产信息。

步骤8 （可选）清理风险资产。

如果您清点后发现有风险的资产请及时排除。

对于危险端口，建议按如下进行处置：

- 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。
- 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。

----结束

5.3 容器指纹

5.3.1 采集容器资产指纹

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。本章节为您介绍容器资产指纹采集项以及如何采集容器资产指纹。

约束与限制

容器指纹功能仅企业主机安全容器版支持。

容器资产指纹采集内容

容器资产指纹采集项如**表 容器资产指纹特性**所示，除集群、服务、工作负载和容器实例外的其他采集项有固定的采集周期，资产指纹功能会定期自动采集这些容器资产指纹。您也可以自定义资产指纹采集周期，详细操作请参见**资产发现**。

表 5-2 容器资产指纹特性

功能项	功能描述	自动检测周期
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”。	每小时自动检测

功能项	功能描述	自动检测周期
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。	每30秒自动检测
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。	每小时自动检测
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	自动检测周期
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”。	每小时自动检测
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04：10）
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04：10）
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04：10）
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04：10）
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04：10）
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04：10）
集群列表	统计、展示集群的详细信息，您可以查看所有集群的类型、节点、版本、状态等信息。	-
服务	统计、展示服务和断点的详细信息，您可以查看所有服务的命名空间、所属集群等信息。	-
工作负载	统计、展示工作负载（有状态负载、无状态负载、守护进程集、普通任务、定时任务、容器组）的详细信息，您可以查看所有工作负载的状态、实例个数、命名空间等信息。	-
容器实例	统计、展示容器实例的详细信息，您可以查看所有容器实例的状态、所属POD、所属集群等信息。	-

采集单个容器指纹最新数据

针对Web应用、Web服务、Web框架、Web站点、中间件和数据库这些资产，如果您想实时查看最新的数据，可手动采集对应的资产。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 单击指纹列表的目标类型，单击右侧列表上方“立即采集”任务自动创建完成。

目前仅支持Web应用、Web服务、Web框架、Web站点、中间件和数据库支持实时手动采集更新，其他类型每天会自动执行采集更新。

步骤8 自动执行完成之后，“最后采集时间”将会更新，可查看最新的容器资产信息。

----结束

采集集群、服务、工作负载和容器信息

集群、服务、工作负载和容器这些资产信息，资产指纹功能不会自动采集，因此如果您的这些资产有变化，请参考本节手动采集最新的数据。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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。

----结束

后续操作

容器指纹采集完成后，即可查看最新的资产数据，相关介绍请参见**查看容器资产指纹**。

5.3.2 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。关于各指纹的介绍请参见**采集容器资产指纹**。

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击指纹列表的目标指纹类型，查看对应资产信息。

步骤7 （可选）清理风险资产。

如果您清点后发现有风险的资产请及时排除。

对于危险端口，建议按如下进行处置：

- 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。
- 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。

----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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 单击指纹列表的目标指纹类型，查看对应资产信息。

步骤8 （可选）清理风险资产。

如果您清点后发现有风险的资产请及时排除。

对于危险端口，建议按如下进行处置：

- 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。
- 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。

----结束

查看集群

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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7 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，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，查看集群基本信息、网络信息等。

----结束

查看服务

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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7 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、集群类型和创建时间信息。

- 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，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

查看端点

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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7 选择“服务 > 端点”，进入端点页面，查看端点相关信息。

端点页面展示了端点的名称、命名空间、所属集群、是否关联服务、服务名称、集群类型和创建时间信息。

- 搜索目标端点

  您可以在端点列表上方的搜索框中输入端点名称、命名空间等信息，查找目标端点。

- 查看目标端点详细信息

  单击目标端点名称，进入端点的详情页面，可以查看目标端点的Pod映射、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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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7 选择“工作负载”，进入工作负载页面。

步骤8 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，查找目标工作负载。

表 5-3 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 • 集群类型
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 • 集群类型

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 • 集群类型
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 • 集群类型
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 • 集群类型
容器组	• 名称 • 命名空间 • 所属集群 • 集群类型 • 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 “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7 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、集群类型、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，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

5.4 主机管理

5.4.1 开启主机防护

操作场景

本章节介绍如何为主机开启基础版、企业版或旗舰版防护。

前提条件

- 请确保已为主机安装Agent，且Agent状态为“在线”。安装Agent操作请参见**为云平台主机安装Agent**。

约束与限制

在为Windows主机开启防护时，需要您同步授权开启Windows防火墙，用于拦截暴力破解的攻击源IP；如果不开启，HSS仅会在检测到暴力破解攻击时进行告警而不会拦截。

- 开启Windows防火墙，HSS将自动添加允许流量全入（hostguard_AllowAnyIn）和全出（hostguard_AllowAnyOut）的防火墙规则，确保防火墙启用不会干扰您

的正常业务运行。同时，当HSS检测到暴力破解攻击时，将在防火墙中添加一条入站规则用于拦截暴力破解的攻击源IP，不会对您的主机造成任何不利的影响。

- 使用HSS期间请勿关闭Windows防火墙，如果关闭Windows防火墙，HSS无法拦截暴力破解的攻击源IP；即使手动关闭后开启Windows防火墙，也可能导致HSS不能拦截暴力破解的攻击源IP。

开启企业版/旗舰版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“资产管理 > 主机管理”，进入“云服务器”界面。

步骤5 单击“确认”，开启防护。目标主机的“防护状态”为“防护中”，则表示企业版/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。

步骤6 （可选）配置告警通知、防护策略、主机登录保护以及开启恶意程序隔离查杀。

- **配置告警通知**

  企业主机安全防护开启成功后，默认将检测到的风险告警信息呈现在控制台，如需及时了解主机、容器或网页存在的安全风险，您可以开启告警通知，开启后，一旦企业主机安全检测到风险，将通过短信或邮件等方式通知您。具体操作请参见**告警配置**。

- **配置防护策略**

  每个企业主机安全版本都对应一组防护策略，这些策略默认预置了防护规则。您可以根据自身业务需求，开启或关闭防护策略、调整防护规则。具体操作请参见**策略管理**。

- **配置登录保护**

  您可以通过**双因子认证**、**配置常用登录地**、**配置常用登录IP**以及**配置SSH登录IP白名单**，来增强主机登录安全性。

- **开启恶意程序隔离查杀**

  开启恶意程序隔离查杀功能后，企业主机安全将自动隔离识别到的后门、木马、蠕虫等恶意程序，帮助您自动处理系统存在的安全风险。具体操作请参见**开启恶意程序隔离查杀**。

----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。待检测完成后，您可以参考如下方式查看检测详情：

步骤1 在“资产管理 > 主机管理 > 云服务器”页面中，找到目标服务器。

步骤2 在目标服务器所在行的“风险状态”列，查看服务器风险检测状态。

表 5-4 风险状态说明

状态	说明
未检测	服务器未开启防护，未检测风险。
无风险	已对服务器进行了全面的安全检查，未发现风险，或者开启防护不久，还未检测到风险。
有风险	服务器存在安全风险。

步骤3 鼠标悬停在风险状态上方，可查看风险分布。

单击风险数值，可进入详情页面，查看具体内容。

----结束

高级防御功能

企业主机安全提供了系列高级防御功能，您可以结合业务实际情况选择开启或使用，以增强主机的安全防护水平。具体请参见表3-7。

表 5-5 高级防御功能

功能	说明	版本限制
应用防护	应用防护功能旨在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。	旗舰版
勒索病毒防护	勒索病毒防护功能能够实现对勒索病毒的检测和防御；同时，还提供数据备份功能，支持定时自动备份和勒索即刻备份，帮助您抵御勒索病毒，降低业务受损风险。 开启容器版防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略。	旗舰版
应用进程控制	应用进程控制是一种用于保障服务器上运行的应用程序和进程安全的功能。它能够自动识别并分析应用进程，将其划分为可信、可疑及恶意三类，同时允许可信进程运行，针对可疑、恶意进程运行进行告警，可以帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。	旗舰版
病毒查杀	病毒查杀功能采用云端与本地相结合的病毒防护机制，能够全面扫描主机中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可以根据实际需求，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”任务，及时发现并清理病毒文件，增强业务系统的病毒防御能力。	专业版、企业版、旗舰版

功能	说明	版本限制
动态端口蜜罐	动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。	旗舰版

5.4.2 查看主机防护状态

建议您定期查看主机防护状态，及时处理主机中存在的安全风险，避免威胁入侵造成您的资产损失或防护中断导致您的主机暴露在风险中。

查看主机防护状态

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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。

您也可以在“云服务器”界面，查看服务器名称、ID、IP地址、操作系统、运行状态以及所属企业项目等信息。服务器防护列表展示项，可通过单击列表右上角设置。

- **搜索目标服务器**

  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，可搜索查看目标服务器防护状态。
- **查看分类服务器**

  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。
- **查看服务器防护情况**

  服务器的“防护状态”列显示当前服务器是否被防护，服务器防护状态由“Agent状态”、“服务器运行状态”综合决定。服务器风险检测状态可在“风险状态”列查看。上述参数详细说明请参见表 防护情况说明。

表 5-6 防护情况说明

参数	说明
服务器运行状态	服务器只有处于“运行中”状态时，HSS才能为其提供防护。如果服务器处于“关机”或其他状态，您无法通过HSS对服务器执行安全检测、风险修复等操作。
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已经安装且运行正常。 – 离线：Agent已经安装完成，但当前Agent与HSS远端防护中心的连接中断，无法通信。此时，HSS无法提供安全防护功能。解决办法请参见**Agent状态异常应如何处理?** – 安装失败：在尝试安装过程中遇到错误或问题，导致安装未能完成。单击安装失败状态旁的查看具体原因，参考**Agent安装失败应如何处理?** 解决问题。 – 安装中：当前正在进行Agent安装。
防护状态	– 防护中：HSS为该服务器提供全面的安全防护。 – 未防护：目标未开启防护。Agent安装完成后，单击“操作”列“开启防护”可以开启防护。 – 防护中断：服务器关机、Agent离线或Agent被卸载导致防护中断。
风险状态	展示服务器当前的风险情况（数据存在24小时延迟）。 – 有风险：主机存在风险。鼠标悬停在风险分布图标上方，可查看风险分布详情；单击数值可跳转至风险详情页面查看详细信息。 – 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 进入“主机防御 > 网页防篡改 > 防护配置”界面。

步骤2 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤3 查看服务器的防护状态。

表 5-7 状态说明

参数名称	说明
动态防篡改状态	动态网页防篡改的状态。 • ：已开启动态网页防篡改。 • ：未开启动态网页防篡改。开启动态网页防篡改功能，要重启Tomcat才能生效。
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

5.4.3 导出主机列表

您可以参考本章节导出主机防护列表到本地。

导出主机列表至本地

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“资产管理 > 主机管理”，进入“云服务器”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在云服务器列表右上方单击“导出”，导出云服务器列表详情。

如需导出部分服务器信息，请勾选对应的服务器，然后单击“导出”。当前云服务器详情导出单次最大支持1000台服务器。

----结束

5.4.4 部署防护策略

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、旗舰版、网页防篡改版或容器版主机安全防护时，默认部署了对应版本的防护策略组，应用于服务器，无需手动部署策略。针对旗舰版、容器版策略组，支持通过复制的方式创建自定义策略组，您可以部署自定义策略组替换默认策略组，方便您灵活管理服务器防护策略。

创建策略组

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 在弹出的对话框中，输入“策略组名称”和“描述”。

- 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8 单击“确定”，将会创建一个新的策略组。

步骤9 单击已创建的策略组名称，进入策略组的策略页面。

步骤10 单击“策略名称”，修改具体的策略内容，详细信息请参见**配置策略**。

步骤11 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 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2 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”。

说明

服务器在开启防护后，已经默认部署了对应防护版本的防护策略；针对使用旗舰版和容器版防护的主机，支持新建并部署不同的防护策略。

步骤3 在弹出的对话框中，选择策略组后，单击“确定”，完成部署策略操作。

部署完成后，单击服务器列表右上角，在自定义显示列选中“策略组”并单击“确定”，即可在服务器列表中查看服务器的所属策略组。

说明

- 如果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

5.4.5 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“资产管理 > 主机管理”，进入主机管理界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在“云服务器”界面，选择“服务器组”，单击“创建服务器组”。

步骤7 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。

- 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8 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

如果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。一个云服务器只能分配到一个服务器组。

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。

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。

分配完成后，单击服务器列表右上角 ，在自定义显示列选中“服务器组”并单击“确定”，即可在服务器列表中查看服务器的所属服务器组。

----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

5.4.6 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 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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 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2 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤3 勾选目标服务器，单击列表上方的“关联资产重要性”。

步骤4 在弹窗中“资产重要性”项选择对应的资产重要等级。

步骤5 确认无误，单击“确认”，完成关联。

关联完成后，在左下方“资产重要性”栏中选择重要性等级，查验服务器关联的资产重要性是否正确。

----结束

5.4.7 忽略服务器

对于无需进行防护的服务器，如果呈现在服务器列表中对您统计服务器防护情况造成干扰，您可以忽略该服务器。已忽略的服务器将不再被HSS防护，且HSS不会同步该服务器的信息变更。

忽略服务器

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“资产管理 > 主机管理”，进入主机管理界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“云服务器”页签。

步骤7 通过筛选条件，筛选出“未防护”的服务器。

步骤8 选中目标服务器，并单击服务器列表上方的“更多 > 忽略”，忽略服务器。

在服务器类型栏，选择“已忽略服务器”，可查看已忽略的服务器。

----结束

取消忽略服务器

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“资产管理 > 主机管理”，进入主机管理界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“云服务器”页签。

步骤7 在服务器类型栏，选择“已忽略服务器”，查看已忽略服务器列表。

步骤8 在目标服务器所在行的操作列，单击“取消忽略”，取消忽略操作完成。

在服务器类型栏，选择“全部服务器”，可在全部服务器列表中，查看取消忽略后的服务器。

----结束

5.4.8 关闭主机防护

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。

5.4.8.1 关闭基础版/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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤5 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

5.4.8.2 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤5 单击目标服务器“操作”列的“关闭防护”。

如需批量关闭，请勾选所有目标服务器，并在服务器列表上方单击“关闭防护”。

步骤6 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7 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

5.5 容器管理

5.5.1 开启容器防护

操作场景

企业主机安全容器版提供对容器全生命周期的安全防护能力。本章节介绍如何为容器节点开启防护。

前提条件

- 请确保已为容器节点安装Agent，且Agent状态为“在线”。为单一节点安装Agent请参见**为云平台主机安装Agent**。为集群安装Agent请参见**为容器安装Agent**。

约束限制

企业主机安全暂仅支持为Docker、Containerd、CRI-O、Podman、isulad运行时的容器提供安全防护。

开启容器版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在目标服务器所在行的“操作”列，单击“开启防护”，弹出“您确认要对以下容器节点开启防护吗？”对话框。

步骤6 确认节点信息并选择开启方式。

⚠ 注意

步骤7 阅读并勾选《容器安全服务免责声明》。

步骤8 单击“确定”，开启节点防护，目标节点的“容器防护状态”变更为“防护中”，说明该节点已开启防护。

步骤9 （可选）配置告警通知、防护策略、主机登录保护以及开启恶意程序隔离查杀。

- **配置告警通知**

  企业主机安全防护开启成功后，默认将检测到的风险告警信息呈现在控制台，如需及时了解主机、容器或网页存在的安全风险，您可以开启告警通知，开启后，一旦企业主机安全检测到风险，将通过短信或邮件等方式通知您。具体操作请参见**告警配置**。

- **配置防护策略**

  每个企业主机安全版本都对应一组防护策略，这些策略默认预置了防护规则。您可以根据自身业务需求，开启或关闭防护策略、调整防护规则。具体操作请参见**策略管理**。

- **配置登录保护**

  您可以通过**双因子认证**、**配置常用登录地**、**配置常用登录IP**以及**配置SSH登录IP白名单**，来增强主机登录安全性。

- **开启恶意程序隔离查杀**

  开启恶意程序隔离查杀功能后，企业主机安全将自动隔离识别到的后门、木马、蠕虫等恶意程序，帮助您自动处理系统存在的安全风险。具体操作请参见**开启恶意程序隔离查杀**。

----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。待检测完成后，您可以参考如下方式查看检测详情：

步骤1 在“资产管理 > 主机管理 > 云服务器”页面中，找到目标服务器。

步骤2 在目标服务器所在行的“风险状态”列，查看服务器风险检测状态。

表 5-8 风险状态说明

状态	说明
未检测	服务器未开启防护，未检测风险。

状态	说明
无风险	已对服务器进行了全面的安全检查，未发现风险，或者开启防护不久，还未检测到风险。
有风险	服务器存在安全风险。

步骤3 鼠标悬停在风险状态上方，可查看风险分布。

单击风险数值，可进入详情页面，查看具体内容。

----结束

高级防御功能

企业主机安全提供了系列高级防御功能，您可以结合业务实际情况选择开启或使用，以增强主机和容器的安全防护水平。具体请参见表3-7。

表 5-9 高级防御功能

功能	说明
应用防护	应用防护功能旨在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。
勒索病毒防护	勒索病毒防护功能能够实现对勒索病毒的检测和防御；同时，还提供数据备份功能，支持定时自动备份和勒索即刻备份，帮助您抵御勒索病毒，降低业务受损风险。 开启容器版防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略。
应用进程控制	应用进程控制是一种用于保障服务器上运行的应用程序和进程安全的功能。它能够自动识别并分析应用进程，将其划分为可信、可疑及恶意三类，同时允许可信进程运行，针对可疑、恶意进程运行进行告警，可以帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。
病毒查杀	病毒查杀功能采用云端与本地相结合的病毒防护机制，能够全面扫描主机中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可以根据实际需求，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”任务，及时发现并清理病毒文件，增强业务系统的病毒防御能力。
动态端口蜜罐	动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。
容器防火墙	容器防火墙能够实现Pod、工作负载以及节点粒度的网络隔离，可有效抵御横向渗透攻击，确保业务权限最小化，从而保障用户业务的安全性和稳定性。

功能	说明
容器集群防护	容器集群防护功能支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。

5.5.2 查看容器节点防护状态

节点列表展示了容器节点的防护状态、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。

查看容器节点防护状态

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看节点防护状态。节点列表参数说明如表5-10所示。

表 5-10 节点防护状态参数说明

参数名称	说明
服务器信息	服务器名称、IP地址等信息。鼠标悬停在服务器名称处，可查看服务器详细信息，包含服务器ID、操作系统、系统名称、系统版本等。
容器防护状态	节点的防护状态，包括： • 未防护：目标未开启防护。Agent安装完成后，单击“操作”列“开启防护”可以开启防护。 • 防护中：HSS为该服务器提供全面的主机安全防护。 • 防护中断：服务器关机、Agent离线或Agent被卸载导致防护中断。

参数名称	说明
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：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。 • 未安装：未安装Agent，或Agent已安装但未成功启动。

----结束

5.5.3 导出容器节点列表

您可以将参考本章节导出容器节点列表至本地查看。

导出容器节点列表至本地

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“资产管理 > 容器管理”，进入“容器管理”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“容器节点管理”页签。

步骤7 在容器列表上方，单击“导出”，导出列表。

如需导出部分容器节点信息，请勾选对应的容器节点，然后单击“导出”。

说明

单次最多支持导出1000条容器节点信息。

----结束

5.5.4 管理本地镜像

操作场景

企业主机安全支持对本地镜像手动执行漏洞和软件信息的扫描并提供扫描报告。本章节介绍如何对本地镜像执行安全扫描和如何查看扫描报告。

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。
- 镜像扫描仅支持扫描存储驱动为OverlayFS或OverlayFS2的节点，暂不支持扫描Device Mapper类节点。
- 镜像扫描不支持扫描镜像或版本名称为“--”的镜像。
- 镜像扫描默认路径为/var/run目录，对其他目录无访问权限，如果Docker Root Dir不为/var/run/目录时HSS无法完成镜像扫描。建议在Containerd主机上完成镜像扫描。

查看本地镜像

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤5 选择“容器镜像 > 本地镜像”，查看本地镜像信息。

您可以查看镜像的名称、版本、类型、安全风险等信息。

- 查看镜像关联主机信息

  在目标镜像所在行的服务器名称列，单击服务器名称，进入关联主机列表页面，可以查看镜像关联主机的详细信息。
- 查看镜像关联容器信息

  在目标镜像所在行的关联容器数列，单击关联数字，进入关联容器列表页面，可以查看镜像关联容器的详细信息。
- 查看镜像组件信息

  在目标镜像所在行的组件数列，单击数字，进入组件列表页面，可以查看镜像组件的详细信息。
- 查看镜像安全风险

  鼠标悬停至目标镜像所在行的安全风险列，可查看镜像风险分布数量，单击数值可跳转至风险详情页查看。

----结束

扫描本地镜像

您可以手动执行全量、批量或单镜像的安全扫描。安全扫描的时长主要取决于镜像的大小。一般情况下扫描一个镜像可以在三分钟之内完成，扫描完成后，单击“安全报告”查看安全报告。

本地镜像支持的安全扫描项如下：

扫描项	说明
漏洞	检测镜像中存在的系统漏洞。 系统漏洞扫描支持扫描的操作系统： ● EulerOS 2.2、2.3、2.5、2.8、2.9、2.10、2.11、2.12（64位） ● CentOS 7.4、7.5、7.6、7.7、7.8、7.9（64位） ● Ubuntu 16.04、18.04、20.04、22.04（64位） ● Debian 9、10、11（64位） ● 银河麒麟V10、V10 SP1、V10 SP2（64位） ● HCE 2.0（64位） ● SLES 12 SP5、15 SP1、15 SP2（64位） ● 统信UOS V20服务器E版、V20服务器D版、1050u2e、1050e、1060e（64位） ● Rocky Linux 8.6、8.10、9.4、9.5（64位） ● CTyunOS 3-23.01（64位） ● AlmaLinux 8.4（64位）
软件信息	统计镜像中的软件信息。

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航栏中，选择“资产管理 > 容器管理”，进入“容器管理”界面。

步骤3 选择“容器镜像 > 本地镜像”。

步骤4 为单个镜像或多个镜像执行安全扫描。

- 单个镜像安全扫描

  在目标镜像所在行的“操作”列，单击“安全扫描”，为单个目标镜像执行安全扫描。

- 批量镜像安全扫描

  勾选所有目标镜像并单击镜像列表上方的“批量扫描”，为多个目标镜像执行安全扫描。

- 全量镜像安全扫描

  单击镜像列表上方的全量扫描，为所有镜像执行安全扫描。

步骤5 在弹出的提示框中，单击“确定”，启动扫描任务。

全量扫描任务启动后，您可将鼠标悬停在置灰的全量扫描按钮上查看扫描进度。

步骤6 当镜像“扫描状态”更新为“扫描完成”，且“最近一次扫描完成时间”更新为最近任务执行时间，表示镜像安全扫描完成。

----结束

查看本地镜像漏洞报告和软件信息

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“容器镜像 > 本地镜像”。

步骤3 在目标镜像所在行的“操作”列，单击“安全报告”，进入安全扫描报告界面，查看漏洞报告和软件信息。

----结束

导出本地镜像漏洞报告

步骤1 登录管理控制台，进入企业主机安全页面。

步骤2 在左侧导航栏中，选择“资产管理 > 容器管理”，进入“容器管理”界面。

步骤3 选择“容器镜像 > 本地镜像”。

步骤4 单击镜像列表上方“漏洞导出”，导出漏洞报告。

如果您想要导出指定镜像的漏洞报告，您可以在漏洞列表上方的搜索框中选择指定类型的镜像后，再单击“漏洞导出”。

步骤5 在容器管理界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的信息。

须知

导出过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

5.5.5 管理仓库镜像

操作场景

仓库镜像中包含SWR私有镜像、SWR共享镜像、SWR企业版镜像和三方镜像；SWR相关的镜像是由容器镜像服务（SWR）同步到HSS，三方镜像您可参考**接入三方镜像仓**接入。

HSS为这些类型镜像提供安全扫描服务，支持漏洞、恶意文件、软件信息、文件信息、基线配置、敏感信息、软件合规、基础镜像信息等检查项，扫描项说明如**表5-11**所示。

您可以定期扫描镜像安全，以便及时发现并清理安全风险，以提升镜像安全性，让您的资产远离安全威胁。

表 5-11 镜像安全扫描项

检查项	说明
漏洞风险	检测镜像中存在系统漏洞、应用漏洞。 ● 系统漏洞扫描支持扫描的操作系统： – EulerOS 2.2、2.3、2.5、2.8、2.9、2.10、2.11、2.12（64位） – CentOS 7.4、7.5、7.6、7.7、7.8、7.9（64位） – Ubuntu 16.04、18.04、20.04、22.04（64位） – Debian 9、10、11（64位） – 银河麒麟V10、V10 SP1、V10 SP2（64位） – HCE 2.0（64位） – SLES 12 SP5、15 SP1、15 SP2（64位） – 统信UOS V20服务器E版、V20服务器D版、1050u2e、1050e、1060e（64位） – Rocky Linux 8.6、8.10、9.4、9.5（64位） – CTyunOS 3-23.01（64位） – AlmaLinux 8.4（64位） ● 应用漏洞扫描支持扫描的应用：fastjson、log4j-core、log4j-api、spring-core、shiro-core、struts-core、tomcat-embed-el、tomcat-jdbc、tomcat-embed-websocket、tomcat-juli、tomcat-annotations-ap、tomcat-embed-core、spring-jdbc、druid、commons-lang、commons-logging、commons-configuration、commons-collections、spring-cloud-netflix-archaius、mysql-connector-java、tensorflow、bootstrap、json、spring-beans、spring-context、spring-aop、spring-webmvc。
恶意文件	检测镜像中存在的恶意文件。
软件信息	统计镜像中的软件信息。
文件信息	统计镜像中的文件信息。
基线检查	● 配置检查： – 检测CentOS 7、Debian 10、EulerOS和Ubuntu16镜像的系统配置项。 – 检测SSH应用配置项。 ● 弱口令检查：检测Linux操作系统（SSH）账号的弱口令。 ● 口令复杂度检查：检测Linux操作系统中不安全的口令复杂度策略配置。

检查项	说明
敏感信息	检测镜像中含有敏感信息的文件。 ● 默认不检测的路径如下： – /usr/* – /lib/* – /lib32/* – /bin/* – /sbin/* – /var/lib/* – /var/log/* – *任意路径*/node_modules/*任意路径*/*任意名称*.md – *任意路径*/node_modules/*任意路径*/test/*任意路径* – */service/iam/examples_test.go – *任意路径*/grafana/public/build/*任意名称*.js **说明** ● 任意路径：指当前路径为自定义值，可以是系统中任意名称的路径。 ● 任意名称：指当前路径的文件名称为自定义值，可以是系统中以.md或.js后缀结束的任意名称。 ● 可在安全报告 > 敏感信息页面，单击“敏感文件过滤路径管理”，设置不需要检测的Linux路径，最多可添加20个路径。 ● 不检测的场景如下： – 文件大于20MB。 – 文件类型为二进制、常用进程和自动生成类型。
软件合规	检测不允许使用的软件和工具。
基础镜像信息	检测未使用基础镜像构建的业务镜像。

约束与限制

- 仅HSS容器版支持该功能。
- 仅支持对Linux镜像执行安全扫描。

查看仓库镜像信息

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 HSS”，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 > 容器管理”，进入容器管理页面。

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤4 选择“容器镜像 > 仓库镜像”，进入仓库镜像页面。

步骤5 查看仓库镜像信息。

您可以在镜像列表中查看镜像的版本、大小、安全风险等信息。

此外，您也可以做以下操作：

- 同步全量镜像

  单击“同步全量镜像”，可同步SWR所有类型的镜像。您可以在页面右上角，单击“任务管理”，选择“镜像资产同步”页签，查看镜像同步任务执行进度。

  说明

  在同步镜像时需要在SWR授权才能正常同步，操作详情请参见《容器镜像服务用户指南》中“授权管理”章节。

- 筛选最新版本的镜像

  勾选“仅关注最新版本的镜像”，可筛选所有不同镜像的最新版本镜像。

- 查看镜像详细信息

  鼠标悬停在目标镜像的“镜像信息”列，可查看镜像“所属组织”和“仓库类型”。单击镜像名称，可进入镜像详情页面，查看镜像版本和安全扫描状态等信息。

----结束

扫描仓库镜像

您可以手动扫描镜像或设置定时扫描策略定时扫描镜像。安全扫描的时长主要取决于镜像的大小，一般情况下扫描一个镜像可以在三分钟之内完成。

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 HSS”，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 > 容器管理”，进入容器管理页面。

步骤4 选择“容器镜像 > 仓库镜像”，进入仓库镜像页面。

步骤5 扫描镜像。

说明

- SWR共享镜像只有镜像状态为“有效”时，可执行安全扫描。
- 多架构镜像不支持手动扫描、定时扫描。

- **立即扫描单个镜像**

  a. 在目标镜像所在行的“操作”列，单击“立即扫描”，弹出安全扫描对话框。

  b. 确认镜像信息，并单击“确定”，开始扫描。

- **手动扫描多个镜像**

  a. 在页面右上方，单击“手动扫描”，弹出手动扫描对话框。

  b. 配置手动扫描参数，相关参数说明请参见**表 手动扫描参数说明**。

表 5-12 手动扫描参数说明

参数名称	参数说明	取值样例
扫描风险类型	勾选需要扫描的风险类型。HSS会默认扫描“软件信息”、“文件信息”和“基础镜像”信息，此处无需选择。	全选
三方镜像仓限速	如果您有大量三方镜像待扫描，但您担心集中扫描镜像时占用过多网络带宽，影响您的业务，您可以单击，选择扫描镜像的速度，限制每小时扫描镜像的数量。	不限制
扫描任务数量	由于1个扫描任务会占用您1个Pod资源，您可以设置集群上运行的扫描任务的数量。 例如设置扫描任务数量为2，则只允许集群上运行2个扫描任务。	2
扫描镜像范围	选择扫描“全部镜像”或“指定镜像”。全量扫描时间较长，且开始全量扫描后无法中断扫描，请谨慎操作！	全部镜像

c. 单击“确定”，开始扫描。

- **定时扫描镜像**

a. 在页面右上方，单击“定时扫描策略”，弹出定时扫描策略配置对话框。

b. 配置定时扫描参数，相关参数说明请参见**表 定时扫描策略参数说明**。

表 5-13 定时扫描策略参数说明

参数名称	参数说明	取值样例
定时扫描策略	定时扫描策略开关，开启后可查看和配置定时扫描参数。 ■ 表示关闭 ■ 表示开启	
定时扫描周期	单击可选择扫描周期，扫描时段固定为00:00:00 - 07:00:00。	每三天
扫描风险类型	勾选需要扫描的风险类型。HSS会默认扫描“软件信息”、“文件信息”和“基础镜像”信息，此处无需选择。	全选
三方镜像仓限速	如果您有大量镜像待扫描，但您担心集中扫描镜像时占用过多网络带宽，影响您的业务，您可以单击，选择扫描镜像的速度，限制每小时扫描镜像的数量。	不限速

参数名称	参数说明	取值样例
镜像时间范围	选择镜像更新的时间范围。时间范围决定哪些镜像会被扫描。 例如，扫描时间范围选择“最近15天”，那么HSS只会扫描最近15天内更新的镜像，更新时间超过15天的镜像，则不会被扫描。	最近15天
扫描任务数量	由于1个扫描任务会占用您1个Pod资源，您可以设置集群上运行的扫描任务的数量。 例如设置扫描任务数量为2，则只允许集群上运行2个扫描任务。	2
选择镜像仓	勾选需要扫描的镜像类型。	Swr-private

c. 单击“确定”，开始扫描。

步骤6 在页面右上角，单击“任务管理”，选择“镜像扫描”页签，可查看镜像扫描任务执行情况。

----结束

查看仓库镜像扫描结果

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 HSS”，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 > 容器管理”，进入容器管理页面。

步骤4 选择“容器镜像 > 仓库镜像”，进入仓库镜像页面。

步骤5 在目标镜像所在行的“操作”列，单击“查看结果”，进入镜像详情页面。

步骤6 查看镜像安全扫描结果。相关参数说明请参见**表 安全报告参数说明**。

表 5-14 安全报告参数说明

参数名称	参数说明
基本信息	展示镜像的基本信息，包括镜像名称、所属组织、镜像版本、镜像大小、漏洞个数、镜像版本最后更新时间以及扫描状态等。 如需重新扫描镜像安全，可以单击“重新扫描”。

参数名称	参数说明
漏洞报告	展示镜像系统漏洞和应用漏洞的检测结果。 ● 查看漏洞详情 单击漏洞名称，进入漏洞详情页面，查看漏洞基本信息以及受影响的镜像。 ● 查看漏洞CVEID、CVSS分值以及披露时间 单击目标漏洞名称前 ，展开查看漏洞CVEID、CVSS分值以及披露时间。 ● 查看漏洞解决方案 在目标漏洞所在行的“解决方案”列，单击解决方案描述，跳转至解决方案详情页面，查看漏洞解决方案详情。
恶意文件	展示镜像恶意文件的检测结果，检测结果包含恶意文件名称、路径、文件大小等信息。
软件信息	展示镜像软件信息的统计结果，统计结果包含软件名称、类型、版本以及软件漏洞个数。 单击软件名称前的，可查看该软件中漏洞的漏洞名称、修复紧急度和解决方案。
文件信息	展示镜像文件信息的统计结果，统计结果包含总文件数量、总文件大小以及文件大小排在前50的文件详情。
基线检查	展示镜像基线检查结果，检查结果包含配置检查、口令复杂度策略检查、经典弱口令检查结果。 ● 查看配置检查详情和修改建议 1. 在基线配置检查页签，勾选目标基线。 2. 在目标检测项所在行的检测项列，单击“检测详情，”右侧弹出检测详情页面，可以查看检测项描述以及修改建议。 ● 自定义经典弱口令 1. 在经典弱口令检测页签，单击“自定义弱口令管理”，进入自定义弱口令详情页面。 2. 输入弱口令完成后，单击“确定”。
敏感信息	展示镜像敏感信息的检测结果，检测结果包含敏感信息的危险程度、镜像层路径、文件路径、敏感信息内容等。 如需添加不检测敏感文件的路径，可以单击“敏感文件过滤路径管理”，添加需要过滤的文件路径。 ● 仅支持过滤Linux系统文件路径。 ● 最多可自定义添加20个路径，多个路径间用回车符号进行分隔。 ● 填写示例：/usr/或/lib/test.txt。
软件合规	展示镜像不合规软件的检测结果，检测结果包含不合规软件名称、软件版本、路径、镜像层信息。
基础镜像信息	展示未使用基础镜像构建的业务镜像检测结果，检测结果包含镜像名称、版本、镜像层路径信息。

----结束

导出镜像漏洞报告

多架构镜像不支持导出漏洞、基线报告。

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 HSS”，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 > 容器管理”，进入容器管理页面。

步骤4 选择“容器镜像 > 仓库镜像”，进入仓库镜像页面。

步骤5 单击镜像列表上方“导出”，选择导出报告类型，导出漏洞或基线报告。

如果您想要导出指定镜像的报告，您可以在漏洞列表上方的搜索框中选择指定类型的镜像后，再单击“导出”。

步骤6 在容器管理界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的信息。

须知

导出过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

5.5.6 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。

查看容器信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“资产管理 > 容器管理”，进入容器管理界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“容器”，进入容器页签。

步骤7 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、集群类型等相关信息。

- 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。

- 导出容器列表

  单击列表左上角“导出”，可导出容器列表至本地查看。

----结束

5.5.7 处置风险容器

操作场景

企业主机安全支持检测容器安全风险，并将容器安全风险分为以下几类：

- 致命：恶意程序等
- 高危：勒索攻击、恶意程序、反弹shell、逃逸攻击、危险命令等
- 中危：Webshell、异常启动、进程异常、敏感文件访问等
- 低危：暴力破解等

为避免有中危及以上安全风险容器影响其他容器的正常运行和使用，您可以通过隔离、暂停或停止容器的方式处置风险容器。

约束限制

- 仅HSS容器版支持该功能。
- 仅支持Linux容器。
- 仅有中危及以上安全风险的容器支持处置操作。

处置风险容器

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“资产管理 > 容器管理”，进入容器管理界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“容器”，进入容器页签。

步骤7 在容器列表上方搜索框中选择“安全风险 > 有风险”，筛选有风险的容器。

步骤8 在目标风险容器所在行的“操作”列，选择需要执行的处置操作。

仅有中危及以上风险且状态为“运行中”的容器支持处置操作，您可以将鼠标滑动至目标风险容器所在行的安全风险列，查看安全风险分布。对于集群容器支持停止容器操作，对于单机容器支持隔离、暂停、停止容器操作。

- **隔离容器**：容器被隔离后，在容器运行时，您将无法访问容器，且容器也无法访问主机的挂载目录以及容器自身的根系统文件。
  a. 单击“隔离”。
  b. 在弹出的对话框中确认信息无误后，单击“确认”。
     容器状态显示“已隔离”，表示隔离成功。
- **暂停容器**：冻结容器中运行的进程。
  a. 单击“暂停”。
  b. 在弹出的对话框中确认信息无误后，单击“确认”。
     容器状态显示“已暂停”，表示暂停成功。
- **停止容器**：终止运行中的容器进程，使容器处于终止状态，如果容器配置了AutoRemove，将无法恢复运行。
  a. 单击“停止容器”。
  b. 在弹出的对话框中确认信息无误后，单击“确认”。
     容器状态显示“已终止”，表示停止成功。

----结束

相关操作

恢复容器为“运行中”状态

将处于“已隔离”、“已暂停”或“终止”状态的容器恢复为“运行中”状态。

说明

处于终止状态的容器如果配置了AutoRemove，将无法恢复运行。

步骤1 在目标容器所在行的“操作”列单击“恢复”。

步骤2 在弹出的对话框中确认信息无误后，单击“确认”。

----结束

5.5.8 卸载集群 Agent

CCE 集群卸载 Agent

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“计算 > 云容器引擎”，进入云容器引擎界面。

步骤3 单击目标集群名称，进入集群详情页。

步骤4 在左侧导航栏，选择“工作负载”，进入“工作负载”界面。

步骤5 选择“守护进程集”页签，删除名称为“install-agent-ds”的工作负载。

在工作负载所在行的操作列，选择“更多 > 删除”，删除该工作负载。

步骤6 在页面左上角单击，选择“区域”，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤7 在控制台左上角，单击图标，选择区域或项目。

步骤8 在左侧导航栏，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤9 选择“Agent管理”页签，卸载目标CCE集群所有容器节点服务器的Agent。

详细操作请参见**卸载主机Agent**。

----结束

自建集群卸载 Agent

步骤1 登录k8s集群环境。

步骤2 执行以下命令删除名称为“install-agent-ds”的工作负载。

kubectl delete ds install-agent-ds -n default

步骤3 登录管理控制台。

步骤4 在控制台左上角，单击图标，选择区域或项目。

步骤5 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤6 在左侧导航栏，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”界面。

步骤7 选择“Agent管理”页签，卸载目标自建集群所有容器节点服务器的Agent。

详细操作请参见**卸载主机Agent**。

----结束

5.5.9 关闭容器防护

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。

关闭容器版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在目标服务器所在行的“操作”列，单击“关闭防护”。

您也可以勾选多个目标服务器，并在列表上方单击“关闭防护”，批量关闭防护。

步骤7 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8 关闭后在“资产管理 > 容器管理 > 容器节点管理”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

----结束

6 风险预防

6.1 漏洞管理

6.1.1 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、应用漏洞和应急漏洞，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。

说明

漏洞列表展示7天内扫描到的漏洞，如果扫描到主机存在漏洞后，您修改了主机的名称，未重新执行漏洞扫描，漏洞列表仍会显示原主机名称。

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 6-1 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。

漏洞分类	原理说明
应用漏洞	通过检测主机及容器宿主机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。
应急漏洞	通过软件版本比对和POC验证的方式，检测服务器上运行的软件和依赖包是否存在漏洞，将存在风险的漏洞上报至控制台，并给您提供漏洞告警。

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6-2**。

表中的标识含义如下：

- √表示支持
- ×表示不支持

表 6-2 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（默认每日自动扫描）	√	√	√	√	√
	定时扫描漏洞（默认每周一次）	×	√	√	√	√
	漏洞白名单	×	√	√	√	√
	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（默认每日自动扫描）	√	√	√	√	×
	定时扫描漏洞（默认每周一次）	×	√	√	√	×
	漏洞白名单	×	√	√	√	×

漏洞类型	功能	基础版	企业版	旗舰版	网页防篡改版	容器版
	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（默认每日自动扫描）	×	√	√	√	√
	定时扫描漏洞（默认每周一次）	×	√	√	√	√
	漏洞白名单	×	√	√	√	√
	手动扫描漏洞	×	√	√	√	√
	漏洞一键修复	×	×	×	×	×
应用漏洞	自动扫描漏洞（默认每周一自动扫描）	×	√	√	√	√
	定时扫描漏洞（默认每周一次）	×	√	√	√	√
	漏洞白名单	×	√	√	√	√
	手动扫描漏洞	×	√	√	√	√
	漏洞一键修复	×	×	×	×	×
应急漏洞	自动扫描漏洞	×	×	×	×	×
	定时扫描漏洞（默认未开启）	×	√	√	√	√
	漏洞白名单	×	×	×	×	×
	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、应急漏洞，不支持自动修复。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。

6.1.2 扫描漏洞

HSS支持扫描Linux漏洞、Windows漏洞、Web-CMS漏洞、应用漏洞和应急漏洞，并提供自动扫描、定时扫描和手动扫描三种扫描方式：

- 自动扫描

  默认每日自动扫描Linux漏洞、Windows漏洞以及Web-CMS漏洞，每周一自动扫描应用漏洞。应用漏洞自动扫描时间随中间件资产检测时间改变，中间件资产检测时间查看及设置的操作请参见**资产发现**。

  如果当日手动扫描过漏洞或执行过定时扫描漏洞任务，HSS当日不再自动扫描漏洞。

- 定时扫描

  默认每周定时执行一次全量服务器漏洞扫描，为了您的业务安全考虑，建议您设置合理的定时扫描周期和扫描服务器范围，定期扫描服务器漏洞。

- 手动扫描

  当您修复了漏洞需要查看漏洞修复情况或者您需要查看实时主机漏洞情况时，建议您手动执行漏洞扫描。

本章节为您介绍如何手动扫描漏洞、配置定时扫描策略。

约束限制

- Windows系统的Agent版本为4.0.18及以上版本时支持应用漏洞扫描，Linux系统的Agent版本为3.2.9及以上版本时支持扫描应急漏洞。升级Agent请参见**升级主机Agent**。
- 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。
- 企业主机安全各版本支持扫描的漏洞类型请参见**支持扫描和修复的漏洞类型**。
- Linux漏洞、Windows漏洞扫描支持的操作系统请参见**表 漏洞扫描支持的操作系统**；应急漏洞扫描支持x86架构的Ubuntu、CentOS、EulerOS、Debian、AlmaLinux系统。

表 6-3 漏洞扫描支持的操作系统

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)

操作系统类型	支持的操作系统版本
Linux	• EulerOS 2.2、2.3、2.5、2.8、2.9、2.10、2.11、2.12（64位） • CentOS 7.4、7.5、7.6、7.7、7.8、7.9（64位） • Ubuntu 16.04、18.04、20.04、22.04（64位） • Debian 9、10、11（64位） • 银河麒麟V10、V10 SP1、V10 SP2（64位） • HCE 2.0（64位） • SLES 12 SP5、15 SP1、15 SP2（64位） • 统信UOS V20服务器E版、V20服务器D版、1050u2e、1050e、1060e（64位） • Rocky Linux 8.6、8.10、9.4、9.5（64位） • CTyunOS 3-23.01（64位） • AlmaLinux 8.4（64位）

手动扫描漏洞

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 单击漏洞管理界面右上角“手动扫描”，弹出“漏洞扫描”对话框。

应急漏洞也可以在目标漏洞类型所在行的“操作”列，单击“立即扫描”，全量扫描服务器是否存在该类型漏洞。

步骤6 在“漏洞扫描”对话框中，设置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 6-4 手动扫描漏洞参数说明

参数	参数说明	取值样例
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 • 应急漏洞	全选

参数	参数说明	取值样例
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。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。	全部服务器

步骤7 单击“确定”，设置完成。

步骤8 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结果。

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

定时扫描漏洞

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在漏洞管理界面右上角，单击“定时扫描策略”，弹出“定时扫描策略配置”对话框。

步骤6 在对话框中，配置定时扫描漏洞的周期和范围等参数。

- 漏洞定时扫描策略：选择是否开启漏洞定时扫描，表示开启。
- 漏洞类型：选择需要扫描的漏洞类型。
- 扫描周期：选择每天、每三天或每周。扫描时间段默认00:00:00 - 07:00:00，不支持修改。
- 选择服务器：选择需要扫描的服务器。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结果。

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

6.1.3 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。漏洞管理页面提供主机和漏洞两个视图，方便您从漏洞视角、主机视角分析漏洞情况。

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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 6-5 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。

参数	说明
修复成功待重启主机	“Linux系统Kernel类漏洞”和“Windows系统漏洞”修复成功后，需要重启主机才能完成修复，否则HSS仍可能为您推送漏洞告警。 单击“修复成功待重启主机”区域的数字，您可以查看需要重启的主机。
今日/累计处理漏洞	今日处理的各类漏洞数量与累计处理的各类漏洞数量，单击数字，可以查看详情。累计处理漏洞的数据只统计一年内的累计处理数据，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。
累计扫描数	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。

  对于受影响服务器：

  - 鼠标滑动至受影响服务器名称处，您可以看到服务器状态、操作系统版本等信息，供您综合考虑漏洞影响。
  - 如果受影响服务器存在“关联进程”，单击服务器名称，进入服务器详情页，可以查看受漏洞影响的服务器进程信息。
- 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。

----结束

查看漏洞详情（主机视图）

基础版不提供主机视图。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在漏洞管理界面上方，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 6-6 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	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。
修复成功待重启主机	“Linux系统Kernel类漏洞”和“Windows系统漏洞”修复成功后，需要重启主机才能完成修复，否则HSS仍可能为您推送漏洞告警。 单击“修复成功待重启主机”区域的数字，您可以查看需要重启的主机。
今日/累计处理漏洞	今日处理的各类漏洞数量与累计处理的各类漏洞数量，单击数字，可以查看详情。累计处理漏洞的数据只统计一年内的累计处理数据，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。
累计扫描数	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。

----结束

6.1.4 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

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”。查看相关状态的详细操作请参见**查看主机防护状态**。

导出漏洞列表（漏洞视图）

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在漏洞管理界面左上角，选择“漏洞视图”页签。

步骤6 在漏洞列表上方，单击“导出”，导出漏洞列表。

单次最多支持导出3万条漏洞数据，如果您的漏洞数量较多，请分批导出。

步骤7 在漏洞管理界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的漏洞列表信息。

导出漏洞信息过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

导出漏洞列表（主机视图）

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在漏洞管理界面左上方，选择“主机视图”页签。

步骤6 导出漏洞列表。

- 导出漏洞明细：在漏洞列表上方，单击“导出明细”，导出漏洞列表。

  可以选择风险等级、漏洞处理状态或通过搜索条件等方式，筛选出目标主机漏洞信息，然后单击“导出明细”，导出您想要的漏洞明细。
- 导出漏洞报告：在漏洞列表上方，单击“导出报告”并选择报告格式。
  - 导出HTML格式的漏洞报告时，最多支持导出100台主机的漏洞信息。在导出的HTML格式漏洞报告中，您可以查看漏洞详细信息。
  - 导出PDF格式的漏洞报告时，最多支持导出主机数+漏洞数总和为140条数据。
  - 如需导出部分主机的漏洞报告，请勾选对应的主机，然后执行导出操作。

步骤7 在漏洞管理界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的漏洞列表信息。

导出漏洞信息过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

6.1.5 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、应用漏洞和应急漏洞，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。

- **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

- 企业主机安全各版本支持的漏洞处理操作请参见**支持扫描和修复的漏洞类型**。
- **表 官方已停止维护的操作系统**所示操作系统官方已停止维护，HSS不再支持自动修复漏洞，建议您使用正在维护的操作系统。

表 6-7 官方已停止维护的操作系统

操作系统	说明
CentOS 8	官方已停止维护，HSS使用Red Hat的补丁公告替代扫描，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。
Ubuntu 16.04、18.04、22.04	官方已停止维护，目前已不支持免费补丁更新，需要订阅Ubuntu Pro后才能安装升级包，未配置Ubuntu Pro会导致漏洞修复失败。
Debian 9、10	官方已停止维护，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。
Windows 2012 R2	官方已停止维护，由于官方不出补丁所以无法修复，建议使用正在维护的操作系统。

- 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主要分为紧急、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。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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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。
- 修复全量漏洞。

  单击漏洞列表左上角的“批量修复”，全量修复漏洞。
- 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6 在修复对话框中确认待修复的漏洞数量和影响资产数量。

对于Linux漏洞，您可以在修复对话框中单击查看修复命令，查看即将修复的组件名称。

步骤7 （可选）为服务器创建备份。

漏洞修复存在影响业务数据的风险，您可以使用HSS提供的自动创建备份功能在漏洞修复前为服务器创建备份。如果您无需备份可跳过此步骤。

1. 在修复对话框中，单击 ，开启备份。

   说明

   - 开启创建备份后，按钮下方会显示可备份的服务器数量，如果服务器没有绑定备份存储库将无法创建备份。
   - 开启创建备份后，当次修复漏洞操作仅支持为可创建备份的服务器修复漏洞，对于未成功创建备份的服务器，请重新执行漏洞修复操作。

2. 单击“管理”，系统弹出创建备份弹窗。
3. 在创建备份弹窗中，编辑服务器本次备份文件的名称并单击“确认”。

步骤8 在修复对话框中勾选知晓风险后，单击“自动修复”。

如果您已自行手动完成漏洞修复，可在修复对话框中单击“手动处置”。手动处置后漏洞的状态会显示为“修复成功”，如果实际漏洞并未修复成功，下一次漏洞扫描任务执行完成后，该漏洞仍然会展示在漏洞列表中等待您处理。

步骤9 单击漏洞名称，进入漏洞详情页面。

步骤10 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**。

说明

“Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要手动重启，否则HSS仍可能为您推送漏洞消息。

表 6-8 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。
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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在界面左上方，选择“主机视图”。

步骤6 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”；如果需要修复所有服务器的漏洞，不勾选任何服务器，直接单击“批量修复”。
  b. 在修复对话框中确认待修复的漏洞数量和影响资产数量。
     对于Linux漏洞，您可以在修复对话框中单击查看修复命令，查看即将修复的组件名称。
  c. （可选）为服务器创建备份。
     漏洞修复存在影响业务数据的风险，您可以使用HSS提供的自动创建备份功能在漏洞修复前为服务器创建备份。如果您无需备份可跳过此步骤。
     i. 在修复对话框中，单击，开启备份。
     说明
     - 开启创建备份后，按钮下方会显示可备份的服务器数量，如果服务器没有绑定备份存储库将无法创建备份。
     - 开启创建备份后，当次修复漏洞操作仅支持为可创建备份的服务器修复漏洞，对于未成功创建备份的服务器，请重新执行漏洞修复操作。
     ii. 单击“管理”，系统弹出创建备份弹窗。
     iii. 在创建备份弹窗中，编辑服务器本次备份文件的名称并单击“确认”。
  d. 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。
  e. 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**。
     说明
     “Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要手动重启，否则HSS仍可能为您推送漏洞消息。

- 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。如果需要修复所有漏洞，不勾选任何漏洞，直接单击“批量修复”。
  c. 在修复对话框中确认待修复的漏洞数量和影响资产数量。
     对于Linux漏洞，您可以在修复对话框中单击查看修复命令，查看即将修复的组件名称。
  d. （可选）为服务器创建备份。
     漏洞修复存在影响业务数据的风险，您可以使用HSS提供的自动创建备份功能在漏洞修复前为服务器创建备份。如果您无需备份可跳过此步骤。
     i. 在修复对话框中，单击 ，开启备份。
        说明
        - 开启创建备份后，按钮下方会显示可备份的服务器数量，如果服务器没有绑定备份存储库将无法创建备份。
        - 开启创建备份后，当次修复漏洞操作仅支持为可创建备份的服务器修复漏洞，对于未成功创建备份的服务器，请重新执行漏洞修复操作。
     ii. 单击“管理”，系统弹出创建备份弹窗。
     iii. 在创建备份弹窗中，编辑服务器本次备份文件的名称并单击“确认”。
  e. 勾选知晓风险后，单击“自动修复”。
     如果您已自行手动完成漏洞修复，可在修复对话框中单击“手动处置”。手动处置后漏洞的状态会显示为“修复成功”，如果实际漏洞并未修复成功，下一次漏洞扫描任务执行完成后，该漏洞仍然会展示在漏洞列表中等待您处理。
  f. 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**。
     说明
     “Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要手动重启，否则HSS仍可能为您推送漏洞消息。

表 6-9 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、应用漏洞和应急漏洞，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。
- 如果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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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

  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。

  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

  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。

  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

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。漏洞忽略后，HSS将不再为您告警。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在目标漏洞所在行的“操作”列，单击“忽略”。

步骤6 在弹出的对话框中，单击“确认”。

----结束

添加漏洞白名单

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。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“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“漏洞白名单配置”，进入“漏洞白名单配置”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 6-10 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 ■ 应急漏洞
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

在您手动修复漏洞完成后，建议您验证漏洞修复结果。

- **方式一**：在漏洞详情页面的“受影响服务器”页签，单击“更多 > 验证”，进行一键验证。该方式的约束与限制如下：
  - 应急漏洞：暂不支持该验证操作。
  - 应用漏洞：仅支持jar包类型的应用漏洞进行验证，非jar包类型的应用漏洞会被自动过滤不进行验证。
- **方式二**：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 6-11 验证修复命令

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

6.1.6 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修改和删除已添加的漏洞白名单。

编辑漏洞白名单

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在漏洞管理界面右上角，单击“漏洞白名单配置”，进入“漏洞白名单配置”页面。

步骤6 在目标漏洞白名单规则所在行的“操作”列，单击“编辑”。

步骤7 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 在漏洞管理界面右上角，单击“漏洞白名单配置”，进入“漏洞白名单配置”页面。

步骤6 在目标漏洞白名单规则所在行的“操作”列，单击“删除”。

步骤7 在弹窗中确认信息后，单击“确认”。

----结束

6.1.7 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）。

约束限制

- HSS基础版不支持该功能。
- 历史处置记录最多保留180天。

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 选择“漏洞管理”页签，查看所有漏洞的历史处置记录。

- 查看指定企业项目的漏洞处置记录

  在历史处置记录页面左上角，选择指定的企业项目，可查看该企业项目下服务器漏洞的处置记录。

- 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，通过选择属性筛选或输入关键词搜索，查看指定属性的漏洞处置记录。

----结束

6.2 基线检查

6.2.1 基线检查概述

什么是基线检查?

基线是指操作系统、数据库、中间件、应用应达到的推荐安全配置标准，包括权限配置、服务配置、网络配置、口令安全配置、等保合规配置等方面。

企业主机安全的基线检查提供口令复杂度策略检测、经典弱口令检测、配置检查功能，可检测不安全的口令配置和系统、关键软件中存在的配置类风险，并针对所发现的风险为用户提供修复建议，帮助用户正确的处理服务器内的各种风险配置。

基线检查内容

检查类型名称	检查详情说明	支持的HSS版本
基线配置检查	对常见的Tomcat配置、Nginx配置、SSH登录配置以及系统配置等进行检查，帮助用户识别不安全的配置项。 检查标准分为云安全实践、等保合规、通用安全标准： ● 云安全实践：基于多年云上安全实践经验，从账号管理、认证授权、口令策略、日志管理、服务管理、网络配置、补丁更新等方面进行检查系统和软件的安全性。 ● 等保合规：基于信息安全等级保护标准，对标权威机构测评要求，对系统、数据库等进行安全性检查。 ● 通用安全标准：基于国内外通用安全规范，从账号管理，口令策略，授权管理，服务管理，配置管理，网络管理，权限管理等多个角度检查系统和软件的安全性。 支持检测的系统、数据库、应用等包括： ● 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、HCE1.1、HCE2.0。 – 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS 7、CentOS 8、Debian 9、Debian 10、Debian 11、Redhat 6、Redhat 7、Redhat 8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma、SUSE 12、SUSE 15、HCE1.1。 – 通用安全标准：HCE1.1 **说明** Linux系统的MySQL基线检测基于MySQL5安全配置规范指导，如果您主机上装有版本号为8的MySQL软件，以下检查项因已废弃不会出现在检测结果中，只在MySQL版本为5的服务器中呈现检测结果。 ● 规则：old_passwords不能设置为 1 ● 规则：secure_auth设置为1或ON ● 规则：禁止设置skip_secure_auth ● 规则：设置log_warnings为2 ● 规则：配置MySQL binlog日志清理策略 ● 规则：sql_mode参数包含NO_AUTO_CREATE_USER ● 规则：使用MySQL审计插件 ● Windows系统： – 云安全实践：MongoDB、Apache2、MySQL、Nginx、Redis、Tomcat、Windows_2008、	企业版、旗舰版、网页防篡改版、容器版

检查类型名称	检查详情说明	支持的HSS版本
	Windows_2012、Windows_2016、Windows_2019、SqlServer。	
口令复杂度策略检测	口令复杂度策略指的是一种口令安全机制，用于规定用户设置的口令必须遵守的规则，以提升口令安全性，防止口令因复杂度过低而被暴力破解。 口令复杂度策略检测功能支持检测Linux系统账号的口令复杂度策略并给出修改建议，帮助用户提升口令安全性。 口令复杂度策略检测主要包括以下几个方面： ● 口令长度：检测口令复杂度策略设定的口令长度限制是否达到安全标准。 ● 大写字母：检测口令复杂度策略设定的大写字母数量限制是否达到安全标准。 ● 小写字母：检测口令复杂策略中设定的小写字母数量限制是否达到安全标准。 ● 数字：检测口令复杂策略中设定的数字数量限制是否达到安全标准。 ● 特殊字符：检测口令复杂策略中设定的特殊字符数量限制是否达到安全标准。	所有版本
经典弱口令检测	弱口令指的是密码强度低，容易被攻击者破解的口令。 经典弱口令检测功能通过将口令与弱口令库进行比对，检测账号口令是否属于常用的弱口令，提示用户修改不安全的口令。 经典弱口令检测功能检测限制如下： ● 支持检测的口令加密算法包括：SHA-256、SHA-512和Yescrypt ● 支持检测的账号类型包括： – Linux：MySQL、Tomcat、Redis及系统账号 – Windows：系统账号	所有版本

使用流程

表 6-12 使用流程

序号	操作项	说明
1	执行基线检查	基线检查功能支持自动和手动基线检查： • 自动执行基线检查：默认**每日凌晨01：00**左右将自动进行一次全量服务器的基线检查（配置检查、口令复杂度策略检测和经典弱口令检测）。 HSS旗舰版、网页防篡改版、容器版可自定义配置检查的自动检测周期，配置操作详情请参见**配置检测**。 HSS企业版、旗舰版、网页防篡改版、容器版可自定义弱口令、修改自动检测周期，配置操作详情请参见**弱口令检测**。 • 手动执行基线检查：如需查看指定服务器的实时基线风险，您可以手动执行基线检查。
2	查看并处理基线检查结果	基线检查完成后，您需要尽快查看并根据HSS提供的修复建议对基线配置风险进行处理。

6.2.2 执行基线检查

操作场景

基线检查功能支持自动和手动两种基线检查方式：

- 自动执行基线检查：基线检查功能会定期对服务器执行配置检查、口令复杂度策略检测、经典弱口令检测。
- 手动执行基线检查：如需查看指定服务器的实时基线风险，您可以手动执行基线检查。当服务器配置了多条基线检查策略时，系统将仅展示最近一次执行的基线检查结果。

自动执行基线检查

默认**每日凌晨01：00**左右将自动进行一次全量服务器的配置检查、口令复杂度策略检测、经典弱口令检测。您可以在自动检查完成后查看并处理资产中存在的风险项。

HSS旗舰版、网页防篡改版、容器版可自定义配置检查的自动检测周期，配置操作详情请参见**配置检测**。

HSS企业版、旗舰版、网页防篡改版、容器版可自定义弱口令、修改自动检测周期，配置操作详情请参见**弱口令检测**。

手动执行基线检查

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤5 （可选）新建手动基线检查策略。

在手动执行基线检查策略之前，您需要为目标服务器新建一条手动基线检查策略；如果您已经为目标服务器新建了策略，可跳过此步骤。

1. 单击页面右上角“策略管理”，进入策略列表页面。
2. 单击“新建策略”，填写配置策略信息，参数说明如**表 新建基线策略信息**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 6-13 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。	default_linux_security_check_policy
操作系统	选择基线检测的目标系统。 – Linux – Windows	Linux

参数名称	参数说明	取值样例
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、HCE1.1、HCE2.0。 ■ 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS 7、CentOS 8、Debian 9、Debian 10、Debian 11、Redhat 6、Redhat 7、Redhat 8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma、SUSE 12、SUSE 15、HCE1.1。 ■ 通用安全标准：HCE1.1 **说明** Linux系统的MySQL基线检测基于MySQL5安全配置规范指导，如果您主机上装有版本号为8的MySQL软件，以下检查项因已废弃不会出现在检测结果中，只在MySQL版本为5的服务器中呈现检测结果。 ■ 规则：old_passwords不能设置为 1 ■ 规则：secure_auth设置为1或ON ■ 规则：禁止设置skip_secure_auth ■ 规则：设置log_warnings为2 ■ 规则：配置MySQL binlog日志清理策略 ■ 规则：sql_mode参数包含NO_AUTO_CREATE_USER ■ 规则：使用MySQL审计插件 – Windows系统： ■ 云安全实践：MongoDB、Apache2、MySQL、Nginx、Redis、Tomcat、Windows_2008、Windows_2012、Windows_2016、Windows_2019、SqlServer。	云安全实践：全选

3. 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。
4. 确认无误，单击“确认”，在策略管理页面新增1条基线策略。

步骤6 在基线检查页面左上方，选择目标“基线检查策略”。

步骤7 单击页面右上角“手动检测”，执行检测。

步骤8 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，如果检测时间超过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**查看并处理基线检查结果**查看对应检查项结果及修改建议。

----结束

6.2.3 查看并处理基线检查结果

操作场景

当基线检查功能检测到并提示您服务器上存在的基线配置风险、弱口令以及口令复杂度策略风险时，请及时查看并处理基线配置风险为您的服务器进行安全加固。

当服务器配置了多条基线检查策略时，系统将仅展示最近一次执行的基线检查结果。

约束限制

仅企业主机安全企业版、旗舰版、网页防篡改版和容器版支持基线配置检查。

检测说明

Linux系统的MySQL基线检测基于MySQL5安全配置规范指导，如果您主机上装有版本号为8的MySQL软件，以下检查项因已废弃不会出现在检测结果中，只在MySQL版本为5的服务器中呈现检测结果。

- 规则：old_passwords不能设置为 1
- 规则：secure_auth设置为1或ON
- 规则：禁止设置skip_secure_auth
- 规则：设置log_warnings为2
- 规则：配置MySQL binlog日志清理策略
- 规则：sql_mode参数包含NO_AUTO_CREATE_USER
- 规则：使用MySQL审计插件

查看基线检查概览信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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 基线检查概览**所示。

如果您想查看不同的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 6-14 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，如果不存在高危，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。
口令度复杂度策略检测	对所有主机存在口令复杂度策略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

查看并处理配置检查结果

步骤1 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6-15**所示。

表 6-15 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 ● 通用安全标准
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。
描述	目标风险基线的描述说明。

步骤2 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3 处理风险项。

- **忽略风险**

  忽略后的风险项，将一直展示在已忽略列表中，且企业主机安全在对服务器执行基线检查时，将不会再告警该项。

  a. 在目标检查项“操作”列单击“忽略”，忽略单条风险检查项。或者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。

  b. 在系统弹出的对话框中，单击“确认”，完成忽略。

  您可以在检查项列表上方，选择“已忽略”，查看已忽略列表。

- **修复风险**

  a. 单击目标风险项“操作”列的“检测详情”，查看检查项详情。

  b. 查看“审计描述”、“修改建议”和“受影响服务器”等信息，根据“修改建议”修复所有受影响服务器中的异常信息。

  说明

  - 目前部分EulerOS基线和CentOS 8已支持一键修复，单击目标EulerOS或CentOS的“检查项”“操作”列的“修复”，可直接修复检查项，部分检查项修复时需填写参数值，保持默认值即可。
  - 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. 修复完成后，在“受影响服务器”页签，单击“验证”，验证受影响服务器的异常信息修复结果。

如果目标检查项已做修复处理，您可通过验证来更新目标检查项状态。验证限制如下：

- Windows暂不支持基线验证。
- 目标主机Agent状态必须为在线。
- 单次只能执行一条风险项验证，其他风险项需要等正在验证的风险项验证完成才能继续验证。
- Linux支持验证的基线：Apache2、Docker、MongoDB、Redis、MySQL5、Nginx、Tomcat、SSH、vsftp、CentOS7、CentOS8、EulerOS、Debian9、Debian10、Debian11、Red Hat6、Red Hat7、Red Hat8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Suse 12、Suse 15、HCE1.1、HCE2.0。

d. 单击“确认”，开始验证。

e. 返回检查项列表页面，查看目标风险项的状态。

“状态”变更为“验证中”，系统开始自动验证，验证结束后查看“状态”的变化。如果状态为修复失败，可单击“查看原因”查看修复失败的原因，排除问题后可再次进行修复。

----结束

查看并处理口令复杂度策略检测结果

步骤1 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6-16所示。

表 6-16 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公网/私网IP地址。
口令长度	目标服务器设置的口令长度策略是否符合标准。 • 符合 • 不符合
大写字母	目标服务器设置的口令大写字母策略是否符合标准。 • 符合 • 不符合
小写字母	目标服务器设置的口令小写字母策略是否符合标准。 • 符合 • 不符合

参数名称	参数说明
数字	目标服务器设置的口令数字策略是否符合标准。 • 符合 • 不符合
特殊字符	目标服务器设置的口令特殊字符策略是否符合标准。 • 符合 • 不符合
建议	对目标服务器的口令复杂度策略设置建议。

步骤2 根据建议，修改主机中的口令复杂度策略。

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

步骤3 完成口令复杂度策略修改后，单击“基线检查”页面上方的“手动检测”，查看修复结果。

如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

----结束

查看并处理经典弱口令检测结果

步骤1 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 经典弱口令检测参数说明**所示。

表 6-17 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公网/私网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。
弱口令使用时长（单位：天）	目标弱口令使用的时间周期。

步骤2 登录主机系统修改弱密码。

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。
- 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。

步骤3 完成弱口令修改后，单击“基线检查”页面上方的“手动检测”，查看修复结果。

如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

----结束

6.2.4 导出基线检查报告

操作场景

本章节为您介绍如何将基线检查结果导出至本地查看。

约束限制

仅企业主机安全企业版、旗舰版、网页防篡改版和容器版支持基线配置检查。

导出基线检查报告

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 根据不同的基线检查类型，参考如下方式导出检测结果。

- 配置检查

  选择“配置检查”页签，在列表左上角单击“导出”，在对话框中选择导出类型并单击“确定”，导出“配置检查”结果。

- 口令复杂度策略检测

  选择“口令复杂度策略检测”页签，在列表左上角单击“导出 > 导出全部数据到XLSX”，导出“口令复杂度策略检测”结果。

- 经典弱口令检测

  选择“经典弱口令检测”页签，在列表右上角单击，导出“经典弱口令检测”结果。

  可在列表右上方输入服务器名称、IP地址、账号名称并单击搜索目标内容进行下载。

----结束

6.2.5 管理手动基线检查策略

对于已创建的手动基线检查策略，如果不满足您的需求，您可以参考本章节修改。

编辑手动基线检查策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤5 单击页面右上角“策略管理”，进入策略列表页面。

步骤6 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。

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。

步骤7 确认修改无误，单击“下一步”，编辑需要应用的服务器。

步骤8 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

删除手动基线检查策略

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 HSS”，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”，进入基线检查界面。

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。

说明

仅支持删除自定义创建的策略，不支持删除系统默认生成的策略“default_linux_security_check_policy”和“default_windows_security_check_policy”。

----结束

6.3 容器镜像安全

6.3.1 查看 SWR 镜像仓库漏洞

您可以参考本章节查看SWR镜像仓库漏洞，并根据提示的解决方案修复漏洞。

前提条件

已开启容器节点防护。

约束限制

仅支持查看Linux镜像存在的漏洞。

查看 SWR 镜像仓库漏洞

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

步骤5 选择“SWR镜像仓库漏洞”页签，查看系统漏洞、应用漏洞列表。漏洞列表说明请参见**表 SWR镜像仓库漏洞列表参数说明**。

表 6-18 SWR 镜像仓库漏洞列表参数说明

参数名称	说明
漏洞名称	单击漏洞名称，可查看漏洞基本信息和受影响的镜像信息。
修复紧急度	漏洞修复紧急度；建议优先修复紧急度为高危、中危的漏洞。
受影响镜像数（个）	受该漏洞影响的镜像。
解决方案	HSS针对该漏洞给出的建议解决方案。单击解决方案描述，可前往解决方案详情页面，查看详细的解决描述。

----结束

6.3.2 查看镜像恶意文件

企业主机安全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

企业主机安全**每日凌晨**自动执行一次全面的检测。

约束限制

- 该功能仅企业主机安全容器版支持
- 仅支持检测Linux镜像存在的恶意文件。

查看镜像恶意文件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

步骤5 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

7 主机防御

7.1 应用防护

7.1.1 应用防护概述

什么是应用防护?

应用防护功能基于RASP（Runtime Application Self-Protection）技术，为运行时的应用提供安全检测和防护。用户无需修改应用文件，只需将探针注入到主机或容器环境的应用，即可为其提供强大的安全防护能力。

技术原理

通过动态代码注入技术在运行时将监控&保护代码（即探针）注入到应用程序的关键监控&保护点（即关键函数），探针根据预定义规则，结合通过保护点的数据、以及上下文环境（应用逻辑、配置、数据和事件流等），识别出攻击行为。

检测能力

表7-1中介绍应用防护功能支持检测的攻击类型。

表 7-1 应用防护功能检测攻击类型

攻击类型	说明	检测规则标识	检测规则描述
SQL注入	SQL注入（SQL Injection）是一种攻击技术，攻击者利用Web应用程序中构建动态SQL查询的漏洞缺陷，在用户输入字段中插入恶意代码，欺骗数据库执行SQL命令，从而窃取、篡改或破坏各类敏感数据，甚至是在数据库主机上执行危险的系统级命令。由于绝大多数网站和Web应用都需要使用SQL数据库，这使得SQL注入攻击成为了最古老、分布最广的网络攻击类型之一。	SQLI	检测防御SQL注入攻击，检测Web应用是否存在对应漏洞。
OS命令注入	OS命令注入（OS Command Injection）是一个Web程序漏洞，这种漏洞通常出现在需要用户输入命令的应用程序中，如果用户输入没有有效的过滤和验证机制，就可能导致该漏洞。它允许攻击者在运行应用程序的服务器上执行任意的操作系统命令。	CMDI	检测防御远程OS命令注入攻击，同时检测web应用是否存在对应漏洞。
XSS	XSS（Cross-Site Scripting，跨站脚本攻击）是一种典型的Web程序漏洞利用攻击。攻击者利用Web程序对用户输入检查不足的漏洞将可执行恶意脚本注入网站或Web应用，当用户访问网页时触发恶意脚本的执行，从而达到窃取用户个人数据、弹出广告，甚至篡改网页内容等攻击目的。	XSS	检测防御存储型跨站脚本注入攻击。
Log4j RCE漏洞	Log4j RCE是指Apache Log4j 2.x中的一个严重安全漏洞，该漏洞使得攻击者可以通过JNDI（Java Naming and Directory Interface）注入执行远程代码。	Log4jRCE	检测防御远程代码执行的控制攻击，并支持对攻击行为进行阻和拦截。

攻击类型	说明	检测规则标识	检测规则描述
上传Webshell	上传WebShell是一种网络攻击手段，攻击者通过漏洞或其他方式将Webshell这种恶意代码上传到服务器，从而获得对服务器的控制权限。	WebShellUpload	检测防御上传危险文件的攻击（主要针对jsp形式的Webshell文件）或将已有文件改名为危险文件扩展名的攻击（主要针对jsp形式的Webshell文件），同时检测Web应用是否存在对应漏洞。
内存马注入	内存马注入是一种高级的网络攻击技术，攻击者利用特殊的技术手段将恶意代码直接注入到内存中，可以有效绕过传统的安全防御机制，实现对目标系统的控制。	FilelessWebshell	实现对各类型Java无文件Webshell的检测。
XXE	XXE指XML外部实体注入（XML External Entity Injection）漏洞。如果应用程序在解析XML文件时，没有禁用外部实体引用，攻击者可通过构造恶意的XML内容，读取任意文件、执行系统命令等。	XXE	检测防御XXE注入攻击，检测Web应用是否存在对应漏洞。
反序列化输入	反序列化指的是将序列化的数据（字符串、字节流等）恢复为原始对象的过程。在生成反序列化对象过程中，攻击者可以通过构造特定的序列化数据输入，控制生成的对象，从而实现一些恶意攻击。	UntrustedDeserialization	检测使用了危险类的反序列化攻击。
文件目录遍历	文件目录遍历指的是攻击者通过修改URL或使用特殊字符绕过应用程序的安全检查，访问或读取服务器上的任意文件或文件夹。	FileDirAccess	获取访问文件的路径或目录，匹配是否在敏感目录或敏感文件下。
Struts2 OGNL	Struts2 OGNL指的是Java Web框中Struts2中的对象图导航语言（Object-Graph Navigation Language），当OGNL表达式外部可控时，攻击者可以通过构造恶意的OGNL表达式让程序执行恶意操作。	Struts2OGNL	OGNL代码执行检测。

攻击类型	说明	检测规则标识	检测规则描述
JSP执行操作系统命令	JSP（Java Server Pages）是一种开发动态网页的技术。攻击者可能利用JSP的安全漏洞执行非法的操作系统命令，导致数据泄露、服务中断等问题。	SuspiciousBehavior	检测可疑行为—通过JSP请求执行操作系统命令。
JSP删除文件	攻击者可能利用JSP的安全漏洞删除服务器上的文件。	SuspiciousBehavior	检测可疑行为—通过JSP请求删除文件失败。
数据库连接异常	数据库连接异常包括但不限于网络异常、配置错误、权限异常等，这些异常可能意味着应用程序正在遭受攻击。	SuspiciousException	检测可疑异常—数据库连接抛出的认证和通讯异常。
0 day漏洞	0 day漏洞（零日漏洞），又称零时差攻击，通常指还没有补丁的安全漏洞。如果这类漏洞被发现，黑客利用这些漏洞进行网络攻击，即零日攻击。	• ZeroDay • ZeroDayDetect	• 检测执行命令的堆栈是否匹配0 day漏洞的部分特征堆栈。 • 检测执行命令的堆栈哈希是否在Web应用的白名单堆栈哈希表里。
SecurityManager权限检测异常	SecurityManager是Java的一个安全管理器类，负责管理和控制应用程序的安全性。当SecurityManager检测到代码执行不允许的操作时，会抛出异常。	SuspiciousException	检测可疑异常，即SecurityManager抛出的异常。

应用场景及优势

- 上下文感知：应用防护功能可以利用应用程序的上下文环境，提供更准确的检测结果。
- 与WAF互补：应用防护技术在应用程序运行时检测内存中写的数据和检测未经授权的数据库访问，与WAF互补。
- 0 day漏洞防御：应用防护功能能够在应用程序运行时进行动态检测和防护，实时检测攻击行为，可有效拦截0 day漏洞攻击。

约束与限制

- 应用防护功能仅企业主机安全旗舰版、网页防篡改版、容器版支持。

应用防护使用流程

图 7-1 使用流程

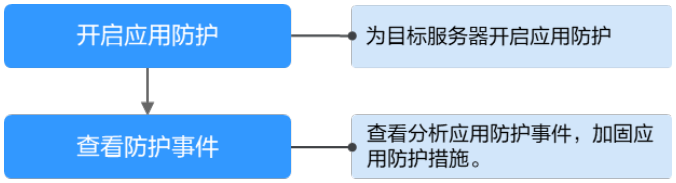


表 7-2 使用流程说明

操作项	说明
开启应用防护	为目标服务器开启应用防护，实时检测应用安全。
查看防护事件	通过分析应用防护过程中触发的防护事件，加固应用防护措施，提升应用安全。

7.1.2 开启应用防护

操作场景

如果您需要防护Linux服务器的Java应用，请为目标服务器开启应用防护。开启防护过程中，HSS会在服务器中安装微服务RASP防护插件，同时需要您配合配置启动参数。

开启应用防护

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 HSS”，进入“企业主机安全”页面。

步骤3 选择“主机防御 > 应用防护 > 防护设置”，进入“防护设置”页面。

步骤4 单击“添加防护服务器”，在弹窗中选择需要防护的服务器和策略。

说明

防护策略可自定义创建，未创建选择默认策略即可。

步骤5 单击“添加并开启防护”，服务器防护流程创建成功。

步骤6 回到“防护设置”页面，单击“微服务RASP防护”的状态，查看防护流程进度。

步骤7 在弹窗中查看防护的流程，等待安装软件流程自动执行安装过程，待进度条下方状态为“软件安装已完成”表示自动安装完成。

步骤8 登录主机，进入spring boot的启动路径，复制“配置启动参数”流程中微服务启动脚本粘贴到命令框，配置启动参数。

步骤9 启动参数配置完成后，执行流程第三步：重启微服务，重启微服务RASP后才能正常进行检测防护。

步骤10 重启后在“防护设置”页面查看目标服务器“微服务防护状态”为“已生效”表示目标服务器已正常开启微服务RASP防护。

----结束

7.1.3 查看应用防护

操作场景

当您为目标服务器开启应用防护成功后，可以在应用防护界面查看服务器应用防护状态、以及应用防护过程中触发的防护事件。您可以通过分析防护事件，加固应用防护措施，从而提升应用安全。

查看防护情况

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护设置”，进入“防护设置”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看服务防护情况，参数说明如表7-3所示。

表 7-3 防护设置参数说明

参数名称	参数描述
服务器名称/ID	服务器的名称和ID。
IP地址	目标服务器的私有地址和公网IP地址。
操作系统	目标服务器的操作系统。
服务器组名称	目标服务器所在的服务器组的名称。
防护策略	目标服务器绑定的检测策略。
防护状态	目标服务器当前Agent状态。 • 防护中：Agent在线。 • 未防护：Agent离线。

参数名称	参数描述
微服务防护状态	微服务的防护状态。 ● 已生效：表示微服务防护开启成功。 ● 正在安装：表示正在安装微服务RASP防护软件，防护未开启。 ● 已安装，未配置：表示微服务RASP防护软件安装成功，但未配置微服务启动参数，防护未开启。 ● 安装失败：表示微服务RASP防护软件安装失败。
微服务RASP防护	微服务RASP的防护开启状态。 当存在以下描述时，表示防护未开启成功，请参考**开启应用防护**检查是否有未处理的操作。 ● 正在安装：表示正在安装微服务RASP防护软件，防护未开启。 ● 已安装，未配置：表示微服务RASP防护软件安装成功，但未配置微服务启动参数，防护未开启。 ● 安装失败：表示微服务RASP防护软件安装失败。
微服务RASP攻击	RASP检测到的攻击事件数量。

----结束

查看防护事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护事件”，进入“防护事件”页面，参数说明如**表7-4**所示。

如果您需要查看某一台服务器的防护事件，可以单击目标服务器“操作”列的“查看报告”。

表 7-4 防护事件参数说明

参数名称	参数描述
告警级别	发现的告警事件的等级，可通过选择不同等级筛选同一告警级别的服务器。 ● 致命 ● 高危 ● 中危 ● 低危

参数名称	参数描述
服务器名称	目标告警对应的服务器。
告警名称	目标告警的名称。
告警时间	发现告警的时间。
攻击源IP	目标告警的IP地址。
攻击源URL	目标告警的URL地址。

步骤5 单击目标告警名称，可查看目标告警的取证信息（请求信息、攻击源IP等）和扩展信息（检测规则标识、探针规则描述），可根据取证信息和扩展信息排查问题、添加防护措施。

----结束

7.1.4 管理应用防护策略

操作场景

应用防护策略支持添加、编辑、删除，具体使用场景如下：

- 添加：企业主机安全提供了“默认策略”，其中包含应用防护全量检测规则。如果您需要为服务器定制防护策略，可单独添加防护策略，对策略中的检测规则项及规则配置进行自定义选择和设置。
- 编辑：对于您自定义添加的防护策略，如需修改，可编辑该策略。
- 删除：对于不需要的自定义防护策略（未关联服务器），可直接删除。

添加防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表7-5所示。

表 7-5 防护策略参数说明

参数名称	参数说明
防护策略名称	添加的防护策略的名称。
检测规则	目标策略支持的检测规则项。
关联服务器数	目标策略已绑定的服务器数。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击“添加防护策略”，在弹窗中配置防护策略参数，参数说明如表7-6所示。

表 7-6 应用防护策略参数说明

参数名称	参数说明
防护策略名称	自定义当前添加的策略名称。
启用	当前策略是否启用目标检测规则，需要启用则勾选目标检测规则即可，不启用则不勾选。
检测规则标识	目前支持自定义选择的所有检测规则标识。
防护动作	选择目标检测规则在检测时防护的动作。 • 检测：针对目标规则的检测对象进行检测，对检测的风险事件进行告警上报。 • 检测并阻断/拦截：针对目标规则的检测对象进行检测，对检测到的风险事件进行告警上报，同时会对检测到的风险项进行直接阻断或拦截。 **警告** 阻断或拦截可能导致业务中断风险，请谨慎操作。
检测规则描述	对目标防护策略的检测对象及行为的描述。

步骤7 单击“操作”列支持“检测规则配置”的项，可自定义修改目标检测规则的规则内容，支持的检测规则如表7-7所示。

表 7-7 支持自定义配置规则内容的检测项

支持自定义配置的检测项	配置的规则内容描述	配置规则样例
XXE	自定义配置XXE黑名单的协议。	.xml;.dtd;
XSS	自定义配置XSS的屏蔽规则。	xml;doctype;xmlns;import;entity
WebShellUpload	自定义配置检测为黑名单的文件后缀。	.jspx;.jsp;.jar;.phtml;.asp;.php;.ascx;.ashx;.cer
FileDirAccess	自定义配置检测为黑名单的路径。	/etc/passwd;/etc/shadow;/etc/gshadow;

步骤8 确认配置的规则及勾选的检测项无误，单击“确认”，可在防护策略页面查看是否添加完成。

----结束

编辑防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表7-8所示。

表 7-8 防护策略参数说明

参数名称	参数说明
防护策略名称	添加的防护策略的名称。
检测规则	目标策略支持的检测规则项。
关联服务器数	目标策略已绑定的服务器数。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击目标策略“操作”列的“编辑”，可对防护策略名称、支持的检测规则及规则内容进行选择和配置。

表 7-9 应用防护策略参数说明

参数名称	参数说明
防护策略名称	自定义当前添加的策略名称。
启用	当前策略是否启用目标检测规则，需要启用则勾选目标检测规则即可，不启用则不勾选。
检测规则标识	目前支持自定义选择的所有检测规则标识。
防护动作	选择目标检测规则在检测时防护的动作。 • 检测：针对目标规则的检测对象进行检测，对检测的风险事件进行告警上报。 • 检测并阻断/拦截：针对目标规则的检测对象进行检测，对检测的风险事件进行告警上报，同时会对检测到的风险项进行直接阻断或拦截。 **须知** 阻断或拦截可能导致业务中断风险，请谨慎操作。
检测规则描述	对目标防护策略的检测对象及行为的描述。

步骤7 确认配置的规则及勾选的检测项无误，单击“确认”，可在防护策略页面查看目标策略是否修改完成。

----结束

删除防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表7-10所示。

表 7-10 防护策略参数说明

参数名称	参数说明
防护策略名称	添加的防护策略的名称。
检测规则	目标策略支持的检测规则项。
关联服务器数	目标策略已绑定的服务器数。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击目标策略“操作”列的“删除”，在弹窗中确认策略信息无误，单击“确认”，策略删除完成。

须知

未关联服务器的策略才支持删除。

----结束

7.1.5 关闭应用防护

操作场景

如果您不再需要HSS继续提供应用安全防护，您可以参考本章节关闭应用防护。

关闭应用防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 应用防护 > 防护设置”，进入“防护设置”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击目标服务器“微服务RASP防护”的图标 或单击“操作”列的“关闭防护”。

步骤7 在弹窗中确认正在关闭微服务RASP防护的服务器信息，确认无误，单击“确认”，完成防护关闭。

说明

RASP防护关闭后，目标服务器会在“防护设置”页面进行自动删除，如果需为其他服务器开启防护，可按照**开启应用防护**操作步骤为其他服务器开启防护。

----结束

7.2 网页防篡改

7.2.1 网页防篡改概述

网页防篡改功能可实时检测并拦截篡改指定目录下文件的行为，并可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。

网页防篡改原理

网页防篡改功能支持静态、动态网页防护，防护原理如**表 网页防篡改原理**所示。

表 7-11 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网站内容更新。 2. 主动备份恢复 如果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 配置远端备份服务器后，HSS会在防护目录下的文件发生变化时触发备份。 如果本地主机上的文件目录和备份目录失效，用户可以登录到远端备份服务器，在备份路径下获取备份文件并手动恢复被篡改的网页。备份路径可在“管理远端备份服务器”页面查看，查看详细操作请参考**修改远端备份**。
动态网页防护	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；提供Tomcat应用运行时自我保护。

约束与限制

- 网页防篡改功能仅企业主机安全网页防篡改版支持。

- 动态网页防篡改当前仅支持JDK 8、JDK 11和JDK 17的Tomcat应用。
- 网页防篡改开启后，防护目录内的文件和文件夹将被设置为只读模式，防止未经授权的修改操作。如需修改，可添加特权进程进行修改。特权进程功能兼容Linux和Windows操作系统，但Linux仅支持内核版本大于或等于5.10的系统。

网页防篡改使用流程

图 7-2 使用流程图

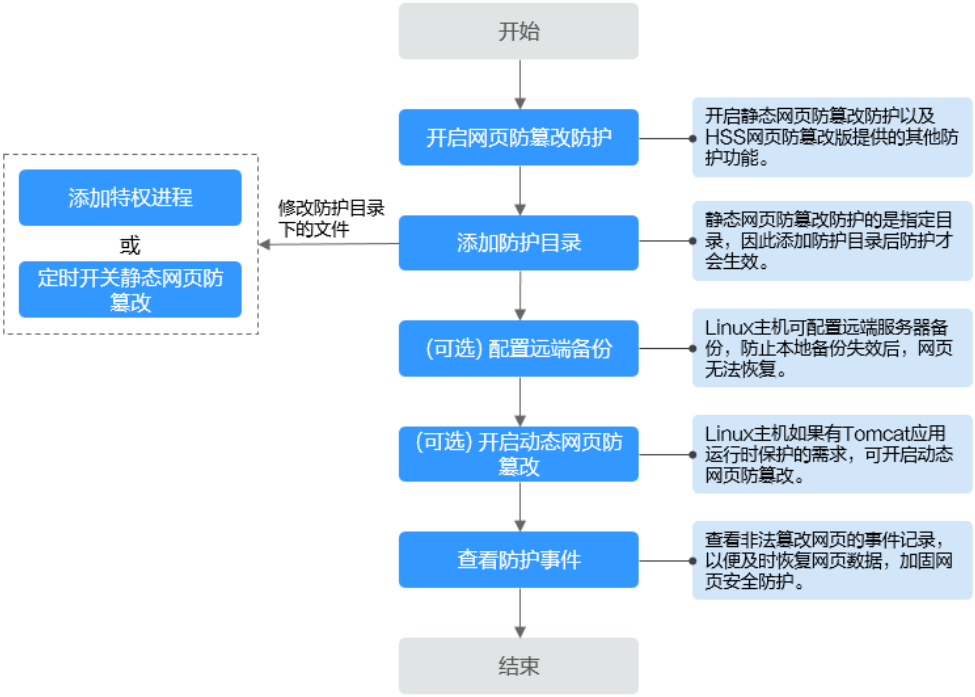


表 7-12 网页防篡改使用流程说明

操作项	描述
开启网页防篡改防护	您在开启“网页防篡改版”防护时，即开启了静态网页防篡改防护和其他防护功能。
添加防护目录	静态网页防篡改为指定的目录提供防护，因此您需要配置静态网页防篡改防护目录，否则静态网页防篡改功能无法生效。
配置远端备份（可选）	针对Linux主机，HSS默认会将防护目录下的文件备份在您添加防护目录时配置的本地备份路径下，为了防止本地备份被攻击者破坏，您可以配置远端备份，再为网页备份数据加一层保障。
开启动态网页防篡改（可选）	针对Linux主机，HSS提供Tomcat应用运行时自我保护，如果您有Tomcat应用相关的动态网页防篡改需求，可以开启动态网页防篡改防护。
查看网页防篡改防护事件	网页防篡改过程中发生的非法篡改事件会被记录并展示在防护事件列表供您查看。

操作项	描述
添加特权进程	开启静态网页防篡改防护后，防护目录中的内容是只读状态，不允许修改。如果您需要修改防护文件，可以添加特权进程，通过特权进程修改防护文件。
定时开关网页防篡改	由于特权进程对操作系统内核版本有限制，且每台服务器最多只能添加10个特权进程。因此对于不能添加特权进程的操作系统，如果您需要定时更新网页，可以设置定时开关静态网页防篡改，在固定时段关闭防护完成网页修改，再开启防护。

7.2.2 开启网页防篡改防护

操作场景

企业主机安全网页防篡改版不仅提供动静态网页防篡改能力，确保网站内容的安全性和完整性，还提供资产管理、漏洞检测、基线检查、入侵检测、勒索防护等与旗舰版相同的主机防护能力，能够有效检测各类针对主机的攻击行为。

本章节介绍如何开启网页防篡改防护。

前提条件

- 请确保已为主机安装Agent，且Agent状态为“在线”。安装Agent操作请参见为云平台主机安装Agent。

约束限制

在为Windows主机开启防护时，需要您同步授权开启Windows防火墙，用于拦截暴力破解的攻击源IP；如果不开启，HSS仅会在检测到暴力破解攻击时进行告警而不会拦截。

- 开启Windows防火墙，HSS将自动添加允许流量全入（hostguard_AllowAnyIn）和全出（hostguard_AllowAnyOut）的防火墙规则，确保防火墙启用不会干扰您的正常业务运行。同时，当HSS检测到暴力破解攻击时，将在防火墙中添加一条入站规则用于拦截暴力破解的攻击源IP，不会对您的主机造成任何不利的影响。
- 使用HSS期间请勿关闭Windows防火墙，如果关闭Windows防火墙，HSS无法拦截暴力破解的攻击源IP；即使手动关闭后开启Windows防火墙，也可能导致HSS不能拦截暴力破解的攻击源IP。

开启网页防篡改版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“主机防御 > 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5 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，单击“添加并开启防护”。

步骤6 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。

- 选择“主机防御 > 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防护已开启。

说明

- 开启网页防篡改后，如果需要更新网站请添加特权进程或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。

----结束

高级防御功能

企业主机安全提供了系列高级防御功能，您可以结合业务实际情况选择开启或使用，以增强主机的安全防护水平。具体请参见表3-7。

表 7-13 高级防御功能

功能	说明
应用防护	应用防护功能旨在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。
勒索病毒防护	勒索病毒防护功能能够实现对勒索病毒的检测和防御；同时，还提供数据备份功能，支持定时自动备份和勒索即刻备份，帮助您抵御勒索病毒，降低业务受损风险。 开启容器版防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略。
应用进程控制	应用进程控制是一种用于保障服务器上运行的应用程序和进程安全的功能。它能够自动识别并分析应用进程，将其划分为可信、可疑及恶意三类，同时允许可信进程运行，针对可疑、恶意进程运行进行告警，可以帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。
病毒查杀	病毒查杀功能采用云端与本地相结合的病毒防护机制，能够全面扫描主机中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可以根据实际需求，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”任务，及时发现并清理病毒文件，增强业务系统的病毒防御能力。
动态端口蜜罐	动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。

7.2.3 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。

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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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 添加防护目录参数说明**。

表 7-14 添加防护目录参数说明

参数名称	参数说明	取值样例
防护目录	添加需要防护的目录。 – 只能添加一个防护目录，目录长度不能超过256个字符。 – 请勿将操作系统目录添加为防护目录。 – 添加为防护目录后，防护目录下的文件和文件夹将为只读状态，无法直接修改。	– Linux：/etc/lesuo – Windows：d:\web
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。 最多可添加10个子目录，多个子目录用英文分号隔开，每个子目录长度不能超过256个字符。	– Linux：lesuo/test – Windows：web\test
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。 – 文件类型只能输入字母、数字，最多可添加10个文件类型，每个文件类型长度不能超过10个字符，多个文件类型以英文分号隔开。 – 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。	log;pid;text
本地备份路径	服务器操作系统为Linux的用户需要设置此项。 设置防护目录文件的本地备份路径，开启网页防篡改防护后，防护目录下的文件会自动备份到设置的本地备份路径中。 备份规则说明如下： – 本地备份路径须为合法路径，且本地备份路径不能与防护目录路径重叠。 – 被排除的子目录和文件类型不会备份。 – 防护目录下文件大小不同，备份时间也不同，一般约10分钟完成备份。 – 当检测到防护目录下的文件被篡改时，系统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。	/etc/backup

参数名称	参数说明	取值样例
排除文件路径列表	服务器操作系统为Linux的用户需要设置此项。 排除防护目录下不需要防护的文件。 最多可添加50个路径，多个路径请用英文分号隔开，每个路径长度不能超过256个字符。	lesuo/data;lesuo/list

2. 添加完成后，单击“确认”，完成添加防护目录的操作。

   如果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。

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

- 导出防护目录：如果您配置的防护目录较多不方便查看，您可以在防护目录配置页面单击 ，导出所有防护目录的配置信息保存到本地进行查看。
- 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，如果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。

7.2.4 配置远端备份

配置远端备份服务器后，HSS会在防护目录下的文件发生变化时触发备份；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。

如果本地主机上的文件目录和备份目录失效，用户可以登录到远端备份服务器，在备份路径下获取备份文件并手动恢复被篡改的网页。备份路径可在“管理远端备份服务器”页面查看，查看详细操作请参考**修改远端备份**。

约束与限制

- 仅Linux服务器支持配置远端备份。
- 用于远端备份的服务器，需满足以下条件：
  - 云平台Linux服务器。
  - “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备份服务器与防护服务器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服务器设置为备份服务器。
- 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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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。

表 7-15 添加远端备份服务器参数说明

参数名称	说明	取值样例
地址	该地址为主机的私网地址。	192.168.0.249
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。	8080

参数名称	说明	取值样例
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。 • 如果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”。 • 如果设置为远端备份服务器的主机开启了“网页防篡改”防护，那么该备份路径与自身的“防护目录”不能重叠，否则会导致远端备份失败。	/hss01

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

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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“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6 单击“确认”，启动远端备份。

----结束

修改远端备份

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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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”，进入管理远端备份服务器页面。单击“操作”列的“编辑”，修改远端备份服务器的信息。

步骤6 单击“确认”，完成修改远端备份服务器。

----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；如果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，您将无法恢复被篡改的网页，请谨慎操作。

7.2.5 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，如果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。
- 仅支持为JDK 8的Tomcat提供动态网页防篡改防护。

前提条件

主机为Linux操作系统。

开启动态网页防篡改

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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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

7.2.6 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。

前提条件

云服务器的“Agent状态”为“在线”且“防护状态”为“开启”。查看相关防护状态的操作请参见**查看主机防护状态**。

查看网页防篡改防护事件

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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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

7.2.7 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。如果没有添加特权进程，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。
- 对于Linux系统，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。

前提条件

在“主机防御 > 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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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”，如果进程无格式，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。

7.2.8 定时启停静态网页防篡改

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

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。

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
- 时间段以本地主机时间为准

定时启停静态网页防篡改

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 HSS”，进入“企业主机安全”页面。

步骤3 在“主机防御 > 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。

说明

如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

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。
   - 时间段以本地主机时间为准。
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

7.3 勒索病毒防护

7.3.1 勒索病毒防护概述

勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机出现业务中断、数据泄露或丢失等问题，主机所有者即使支付赎金也可能难以挽回所有损失。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。

约束与限制

- 仅企业主机安全旗舰版、网页防篡改版、容器版支持勒索病毒防护功能。
- 当Linux主机安装了3.2.10或以上版本的Agent，或者Windows主机安装了4.0.22或以上版本的Agent，开启企业主机安全旗舰版、网页防篡改版或容器版防护时，系统会**自动为主机开启勒索病毒防护**，但不会自动开启勒索备份，您可以根据需要手动开启勒索备份；如果主机安装的Agent版本非上述版本，您需要手动开启勒索病毒防护和勒索备份。
- 勒索防护是一项涉及安全管理、技术防御等多个方面的系统性工程。HSS作为其中的重要一环，能够有效提升在工作负载侧对勒索攻击的识别和拦截，但仅靠HSS无法做到100%防护。为了尽可能减少勒索带来的损失，建议您构建一套体系化防护方案，包括但不限于收敛互联网暴露面、加强网络访问控制、严格管理账号权限、搭建高可靠业务架构等，并定时备份重要业务数据，确保在遭受勒索攻击时，可通过备份快速恢复业务，减少业务中断风险。

勒索病毒防护使用流程

表 7-16 使用流程说明

操作项	说明
开启勒索病毒防护	为目标服务器开启勒索病毒防护，部署静态、动态勒索诱饵，实时检测勒索病毒攻击。 **注意** 如果开启勒索病毒防护后，您在服务器上发现可疑文件，可以联系技术支持确认该文件是否是企业主机安全部署的诱饵文件。诱饵文件用于检测勒索病毒攻击，不会对您的业务造成影响，也不包含任何恶意内容，并且不支持手动删除。 • 当Linux主机安装了3.2.10或以上版本的Agent，或者Windows主机安装了4.0.22或以上版本的Agent，开启企业主机安全旗舰版、网页防篡改版或容器版防护时，系统会**自动为主机开启勒索病毒防护，您可以根据自身业务需求修改默认的防护策略（如防护目录、防护动作等）**，具体操作请参见管理勒索病毒防护策略。 • 如果主机安装的Agent版本非上述版本，您需要手动开启勒索病毒防护。
查看并处理勒索病毒防护事件	在防护勒索病毒过程中，一旦触发勒索防护事件，请您及时分析并阻断勒索病毒运行，同时加固系统存在的安全薄弱项。

7.3.2 开启勒索病毒防护

操作场景

勒索病毒防护功能提供已知、未知勒索病毒的实时检测和防御，建议您为每台服务器都开启勒索病毒防护。

当主机已安装的Agent版本为以下版本时，开启企业主机安全旗舰版、网页防篡改版或容器安全版防护，企业主机安全会同步**为主机开启勒索病毒防护**，在主机上部署诱饵文件，并对可疑加密进程执行自动隔离（极小概率存在误隔离）。勒索病毒防护自动

开启后，您可以根据自身业务需求修改默认的防护策略（如防护目录、防护动作等），具体操作请参见**管理勒索病毒防护策略**。

- Linux：Agent版本大于或等于3.2.10。
- Windows：Agent版本大于或等于4.0.22。

如果主机安装的Agent版本非上述版本，或者关闭了勒索病毒防护功能需要重新开启，可参考本章节开启勒索病毒防护。

⚠ 注意

如果开启勒索病毒防护后，您在服务器上发现可疑文件，可以联系技术支持确认该文件是否是企业主机安全部署的诱饵文件。诱饵文件用于检测勒索病毒攻击，不会对您的业务造成影响，也不包含任何恶意内容，并且不支持手动删除。

步骤一：新建防护策略

开启勒索病毒防护前，需要创建勒索防护策略，设置诱饵防护目录、防护文件类型、防护动作等信息。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 ”，进入“勒索病毒防护”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“防护策略”页签，单击“添加防护策略”。

步骤7 设置防护策略参数，相关参数说明请参见**表 防护策略参数说明**。

表 7-17 防护策略参数说明

参数名称	参数说明	取值样例
服务器操作系统	选择服务器操作系统类型。	Linux
防护策略名称	设置防护策略的名称。	Anti_Ransomware
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：发现勒索病毒攻击时，告警并阻断加密文件的进程。 • 告警：发现勒索病毒攻击时，仅告警提示。	告警并自动隔离

参数名称	参数说明	取值样例
动态诱饵防护	此处诱饵指的是模拟真实业务文件的假文件，可以吸引攻击者注意，实时捕捉可能存在的勒索加密行为。 诱饵防护分为动态和静态诱饵防护，通常两者会同时启用以实现更全面的防护效果 开启动态诱饵防护后，系统会在诱饵防护目录和其他随机位置（不包括排除目录）中部署诱饵文件，在随机位置部署的诱饵文件每12小时会自动删除再重新随机部署。诱饵文件会占用小部分服务器资源，您可以将不需要部署诱饵文件的目录配置在排除目录内。 动态诱饵防护凭借其动态变化性，具备更出色的勒索攻击检测能力。 **仅Linux系统，需要设置此项。**	开启
诱饵防护目录	静态诱饵防护是在指定的防护目录下投放诱饵文件。如果您有重要业务目录或数据目录需要防护，可以将其添加为防护目录。诱饵文件部署在该目录（不包括子目录）下，可以分散攻击者注意，从而延缓攻击者攻击真实资源。 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：/root;/home;/opt;/var;/etc • Windows：C:\software
排除目录（选填）	无需部署诱饵文件进行防护的目录。 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：/bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc • Windows：C:\software\test
防护文件类型	需要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、证书密钥、备份等9大文件类型，共70+种文件格式。 **仅Linux系统，需要设置此项。**	全选

步骤8 单击“确认”，添加完成。

在防护策略列表中，查看到添加的防护策略，表示添加防护策略成功。

----结束

步骤二：开启勒索病毒防护

防护策略创建完成后，可参考本小节开启勒索病毒防护。

步骤1 在勒索病毒防护界面，选择“防护服务器”页签。

步骤2 在目标服务器勒索防护状态栏，单击“立即开启”。

您也可以选中多台操作系统类型相同的服务器，并单击列表上方的“开启勒索病毒防护”，批量为服务器开启防护。

步骤3 在“开启勒索病毒防护”弹窗中，确认服务器信息并选择防护策略。

步骤4 单击“确认”，开启防护。

服务器勒索防护状态显示已开启，表示开启勒索病毒防护成功。所有勒索防护状态的含义请参见**表7-18**。

表 7-18 勒索防护状态说明

勒索防护状态	说明
防护中	已成功开启勒索病毒防护。
未开启	未开启勒索病毒防护。
开启中	正在开启勒索病毒防护。
关闭中	正在关闭勒索病毒防护。
防护失败	勒索病毒防护失败。
防护降级	部分防护目录的诱饵文件部署失败，导致防护降级，请检查System群组是否拥有该防护目录的完全控制权限。

----结束

后续操作

目前没有任何工具能100%防护勒索病毒，建议您为服务器开启备份功能，如果发生勒索事件，可通过备份恢复数据，减少损失。具体操作请参见**开启勒索备份**。

7.3.3 开启勒索备份

操作场景

目前没有任何工具能100%防护勒索病毒，因此为服务器开启备份功能，可在勒索事件发生时，及时通过备份恢复数据，减少损失。

勒索备份功能提供**定时备份**和**勒索即刻备份**两种备份方式，用户可自定义设置定时备份策略周期性为服务器进行备份；同时，当企业主机安全检测到疑似勒索攻击时，也会触发勒索即刻备份，确保最大程度保存业务数据。

本章节为您介绍如何开启勒索备份。

步骤一（可选）：购买备份存储库

如果您未购买备份存储库，您可以参考本节在HSS控制台购买备份存储库，也可以前往云备份服务控制台购买备份存储库。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 ”，进入勒索病毒防护界面。

步骤5 鼠标滑动至置灰的“开启勒索备份”按钮上，在弹窗提示中单击“立即购买”。

步骤6 在弹出的对话框中设置需要购买的备份存储库容量等参数。

表 7-19 购买备份容量参数说明

参数名称	参数说明
计费模式	默认为按需计费：按实际的使用时长收费，以小时为单位，每小时整点结算，不设最低消费标准。
区域	当前购买备份存储库的区域。
备份容量	根据需求选择购买备份存储库的大小。
配置费用	根据备份容量计费默认生成费用。

步骤7 单击“确认”，完成购买。

----结束

步骤二：开启勒索备份

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 ”，进入“勒索病毒防护”界面。

步骤5 选择“防护服务器”页签。

步骤6 选中目标服务器，并在服务器列表上方单击“开启勒索备份”。

步骤7 在“开启备份”弹窗中，选择需要为服务器绑定的存储库。

同时满足以下条件的存储库支持绑定：

- 存储库状态为“可用”或“锁定”。
- 备份策略状态为“已启用”。
- 存储库有剩余可用备份容量。
- 存储库绑定的服务器数量少于256台。

步骤8 单击“确认”，开启备份。

目标服务器的存储库绑定状态为“已绑定”，表示勒索备份开启成功。

----结束

相关操作

如果您仅开启了勒索备份，勒索备份只能在勒索攻击发生后，恢复部分数据降低损失，建议您同步开启勒索病毒防护，实时检测和防御勒索病毒攻击。具体操作请参见**开启勒索病毒防护**。

7.3.4 查看并处理勒索病毒防护事件

操作场景

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。

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。

查看并处理勒索病毒防护事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 ”，进入“勒索病毒防护”界面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“防护事件”页签，查看防护事件。

单击告警名称，可查看告警的详细信息。

步骤7 确认告警的危害程度后，在目标事件的操作列单击“处理”，处理该事件。

您也可以勾选所有目标事件，并单击列表上方的“批量处理”，批量处理事件。

步骤8 在“处理告警事件”对话框中，选择处理方式。处理方式说明请参见**表 告警事件处理方式说明**。

表 7-20 告警事件处理方式说明

参数名称	参数说明
处理方式	• **手动处理** 手动处理事件，您可以添加“备注”信息，方便您记录手动处理该告警事件的详细信息。 • **忽略** 仅忽略本次告警。如果再次出现相同的告警信息，HSS会再次告警。 • **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，如果再次出现该告警事件，则HSS不会告警。 • **隔离查杀** 选择隔离查杀后，该程序的可执行文件将变为“只读”状态，同时该程序的进程将被立即终止，为避免对业务造成影响，请谨慎操作。HSS会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。 您可以在“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**。
批量处理	勾选，即同时批量处理不同时间触发的相同告警。如果您勾选后，没有相同告警信息，表示此前未发生过相同告警。
备注描述	您可以根据实际情况备注处理信息，方便后续回溯查看。

步骤9 单击“确认”，完成处理。

----结束

7.3.5 管理勒索病毒防护策略

操作场景

勒索病毒防护开启后，您可以根据实际需求调整勒索病毒防护策略。调整方式包括：

- **切换防护策略**：如果服务器当前绑定的防护策略无法满足您的需求，您可以为服务器绑定另一个更适合的防护策略。
- **修改防护策略**：如果您需要修改某些特定的防护设置（如诱饵防护目录或排除目录等），则可直接修改现有的防护策略。例如，当企业主机安全自动开启勒索病毒防护功能时，默认会配置一个防护策略（Linux系统的默认防护策略名称为tenant_linux_anti_default_policy，Windows系统的默认防护策略名称为tenant_Windows_anti_default_policy），可能不符合您的实际防护需求，您可以对防护策略做定制化修改。
- **删除防护策略**：当某个防护策略被废弃，且未关联任何服务器时，您可以删除该策略。

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。

切换防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护” ，进入“勒索病毒防护”界面。

步骤5 选择“防护服务器”页签。

步骤6 选中目标服务器，并在服务器列表上方单击“切换防护策略”。

您也可以目标服务器所在行的“操作”列，单击“更多 > 切换防护策略”。

步骤7 在“切换防护策略”弹窗中，选择防护策略。

步骤8 单击“确认”，完成切换。

----结束

修改防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 > 防护策略 ”。

步骤5 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 7-21 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。	Anti_Ransomware
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：发现勒索病毒攻击时，告警并阻断加密文件的进程。 ● 告警：发现勒索病毒攻击时，仅告警提示。	告警并自动隔离

参数名称	参数说明	取值样例
动态诱饵防护	此处诱饵指的是模拟真实业务文件的假文件，可以吸引攻击者注意，实时捕捉可能存在的勒索加密行为。 诱饵防护分为动态和静态诱饵防护，通常两者会同时启用以实现更全面的防护效果 开启动态诱饵防护后，系统会在诱饵防护目录和其他随机位置（不包括排除目录）中部署诱饵文件，在随机位置部署的诱饵文件每12小时会自动删除再重新随机部署。诱饵文件会占用小部分服务器资源，您可以将不需要部署诱饵文件的目录配置在排除目录内。 动态诱饵防护凭借其动态变化性，具备更出色的勒索攻击检测能力。 **仅Linux系统，需要设置此项。**	开启
诱饵防护目录	静态诱饵防护是在指定的防护目录下投放诱饵文件。如果您有重要业务目录或数据目录需要防护，可以将其添加为防护目录。诱饵文件部署在该目录（不包括子目录）下，可以分散攻击者注意，从而延缓攻击者攻击真实资源。 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：/root;/home;/opt;/var;/etc • Windows：C:\software
排除目录（选填）	无需部署诱饵文件进行防护的目录。 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：/bin;/boot;/lib;/lib32;/lib64;/lost+found;/proc;/run;/sbin;/selinux;/srv;/sys;/usr/bin;/usr/local/bin;/usr/local/sbin;/usr/sbin;/var/lib/container;/var/lib/kubelet;/var/lib/ntp/proc • Windows：C:\software\test
防护文件类型	需要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、证书密钥、备份等9大文件类型，共70+种文件格式。 **仅Linux系统，需要设置此项。**	全选

参数名称	参数说明	取值样例
进程白名单（选填）	添加自动忽略检测的进程文件路径，可在告警中获取。 **仅Windows系统，需要设置此项。**	-
关联服务器	策略关联的服务器信息，如果您需要解除服务器关联（关闭勒索防护功能），可删除策略。	-

步骤6 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。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 > 防护策略 ”。

步骤5 单击目标策略“操作”列的“删除”。

说明

删除策略后，关联的服务器将不再被防护，风险系数将会升高，建议删除策略前将目标策略关联的服务器绑定其他策略开启防护。

步骤6 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

7.3.6 恢复服务器数据

操作场景

如果您为服务器开启了勒索备份功能，当服务器遭受勒索攻击，不幸失陷时，您可以通过备份恢复服务器数据将损失降到最小化。通过备份数据恢复服务器业务数据时，请在还原之前验证备份是否正常，验证无误后，首先还原业务关键型系统。

前提条件

已开启勒索备份，详细操作请参见**开启勒索备份**。

恢复服务器数据

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在导航树选择“主机防御 > 勒索病毒防护”，选择“防护服务器”，在目标服务器的“操作”列单击“恢复数据”。

步骤5 在弹窗中查看目标服务器的信息，通过筛选备份状态和搜索备份名称检索需要恢复的备份数据源，参数说明如**表 备份数据源参数说明**所示。

表 7-22 备份数据源参数说明

参数名称	参数说明	取值样例
备份名称	备份的数据存储文件名称。	-
备份状态	服务器数据备份的状态。 • 可用：备份数据源的状态正常，可用于数据恢复。 • 正在创建：正在创建备份。 • 正在删除：正在删除备份。 • 正在恢复：正在进行数据备份恢复。 • 错误：备份存在错误。	可用
备份标识	服务器数据备份的原因。 • 定时周期：系统根据备份策略配置的备份周期，自动执行的周期性数据备份。 • 勒索加密：服务器遭到勒索攻击时立即执行的数据备份。	定时周期
创建时间	目标备份数据源的备份时间。	-

步骤6 在目标备份数据源的“操作”列单击“恢复数据”。

步骤7 在弹出的对话框中确认服务器、是否重启等信息，确认无误，单击“确认”，执行自动恢复。

步骤8 在“备份统计”栏，单击备份恢复任务的数值，查看备份恢复进度。

----结束

相关操作

删除备份

如果您确认某个服务器上已备份的数据已没有保留的必要，您可以将该服务器已备份的数据删除。备份删除后，无法恢复，请谨慎操作。

1. 在目标服务器所在行的“已有备份数”列，单击数值，系统弹出已有备份列表。
2. 在目标备份所在行的“操作”列，单击“删除”，系统弹出删除备份对话框。
3. 确认要删除的备份信息，单击“确定”，删除备份。

7.3.7 管理服务器备份

操作场景

勒索备份开启后，备份存储库会按备份策略为您的服务器定期备份，并且当HSS检测到了勒索攻击时也会立即执行备份。

- 如果备份存储库未绑定备份策略，备份存储库将无法执行定时备份，请您为备份存储库**绑定备份策略**。
- 如果备份存储库的容量不足，则无法继续备份，您可以**扩充备份容量**。
- 如果备份策略的备份周期、备份保留规则不满足您的备份需求，您可以**修改备份策略**。

前提条件

已开启勒索备份，详细操作请参见**开启勒索备份**。

绑定备份策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“主动防御 > 勒索病毒防护”，进入勒索病毒防护页面。

步骤5 在目标服务器所在行的“备份策略状态”列，单击“绑定备份策略”。

步骤6 在弹出窗口的备份策略下拉框中，选择目标备份策略。

如果没有已有的备份策略可选择，或者您需要为备份存储库创建一个新的备份策略，可单击“前往CBR创建策略”。创建完成后返回企业主机安全控制台，选择创建好的策略。

步骤7 选择完成后，单击“确定”。

目标服务器的“备份策略状态”显示“已启动”，且策略名称为您绑定的目标策略，表示绑定备份策略成功。

----结束

扩充备份容量

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“主机防御 > 勒索病毒防护”，进入勒索病毒防护页面。

步骤5 单击目标服务器“操作”列的“扩容”。

步骤6 在弹出窗口中输入“新增容量（GB）”。

步骤7 确认无误，单击“确认”，页面跳转至支付页面，支付完成后可返回“防护服务器”页面查看目标服务器存储容量。

如果未完成支付，目标服务器的“存储状态”会显示“被锁定”，支付后，状态恢复正常。

----结束

修改备份策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“主机防御 > 勒索病毒防护”，进入勒索病毒防护页面。

步骤5 单击目标服务器“备份策略状态”列的策略名称，系统弹出“修改备份策略”对话框。

步骤6 在对话框修改备份规则，参数详情如**表 策略参数说明**所示。

表 7-23 修改备份规则参数说明

参数名称	参数说明	取值样例
备份周期	选择按周或按天自动执行备份。 • 按周：指定备份策略在每周的周几进行备份，可以多选。 • 按天：指定备份策略每隔几天进行一次备份，可设置1～30天。选择按天备份时，理论上第一次备份的时间为备份策略创建当天。如果当天备份策略创建的时间已经晚于设置的备份时间，那么将会等到第二个备份周期再进行第一次备份。	每1天
备份时间	设置备份任务执行的时间点。 只支持在整点进行备份，同时支持选择多个整点进行备份。建议选择无业务或者业务量较少的时间进行备份。 备份规则案例： • 规则1：备份周期选择“按周（周三、周六）”，备份时间选择“00:00”和“13:00”；表示在每周三和每周六的00:00、13:00两个时间点执行备份任务。 • 规则2：备份周期选择“按天（每隔2天）”，备份时间选择“02:00”、“14:00”。表示从设置备份规则之日起，每隔2天的02:00、14:00执行备份任务。	00:00、07:00

参数名称	参数说明	取值样例
时区	选择备份时间所属的时区。	UTC+08：00

步骤7 确认无误，单击“下一步”，配置备份数据保留规则，选择不同的保留类型会配置不同的参数。

- “保留类型”：“按数量”

  配置备份规则参数说明如**表 按数量配置保留规则参数说明**所示。

  表 7-24 按数量配置保留规则参数说明

参数名称	参数说明	取值样例
配置详情	配置单个云服务器保留的备份总数。取值范围为2~99999个。 此处配置的备份保留数量为最终保留的备份份数，不受高级选项的规则影响。 例：“配置详情”填写保留备份数量为“30”，“高级选项”填写“月备份规则”值为“3”（即3个月，约90天），最终系统保留的备份数量为最新的30份 。	30
高级选项（可选）	设置长期保留规则，长期保留规则与按数量保留之间互不影响，共同生效，最终的保留结果是取两者的并集。 – 日备份规则：保留N天内每天最新的一个备份。N的取值范围为0到100。 – 周备份规则：保留M周内每周最新的一个备份。M的取值范围为0到100。 – 月备份规则：保留P个月内每月最新的一个备份。P的取值范围为0到100。 – 年备份规则：保留Q年内每年最新的一个备份。Q的取值范围为0到100。	月备份规则：3

- “保留类型”：“按时间”

  配置备份规则参数说明如**表 按时间配置保留规则参数说明**所示。

  表 7-25 按时间配置保留规则参数说明

参数名称	参数说明	取值样例
配置详情	可设置备份数据的保留时间为1个月、3个月、6个月、1年的固定期限，也可以根据实际需求自定义保留时长，自定义保留时长的取值范围为2～99999天。 当备份数据的保留期超出设定的保留时长时，系统将自动删除该备份。	3个月

- “保留类型”：“永久保留”
  备份数据永久保留。

  说明

  如果该策略曾经产生过备份副本，并且过去是“按时间”管理，历史备份仍然按照保留时间规则进行删除。

步骤8 配置完成，单击“确认”，完成备份策略修改。

----结束

7.3.8 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 勒索病毒防护 > 防护服务器 ”。

步骤5 单击目标服务器“操作”列的“更多 > 关闭防护”。

步骤6 确认关闭信息无误，单击“确认”，完成关闭。

----结束

7.4 应用进程控制

7.4.1 应用进程控制概述

应用进程控制功能支持管控应用进程运行，通过学习服务器中运行的应用进程特征，将应用进程划分为可信进程、恶意进程和可疑进程，允许可疑、可信进程正常运行，对恶意进程运行进行告警，帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。

约束与限制

- 应用进程控制功能仅企业主机安全旗舰版、网页防篡改版、容器版支持。
- 使用应用进程控制功能，需确保服务器安装的Agent版本为以下版本，升级Agent的操作，请参见**升级主机Agent**。
  - Linux：3.2.7及以上版本。

- Windows：4.0.19及以上版本。

应用进程控制使用流程

图 7-3 使用流程图

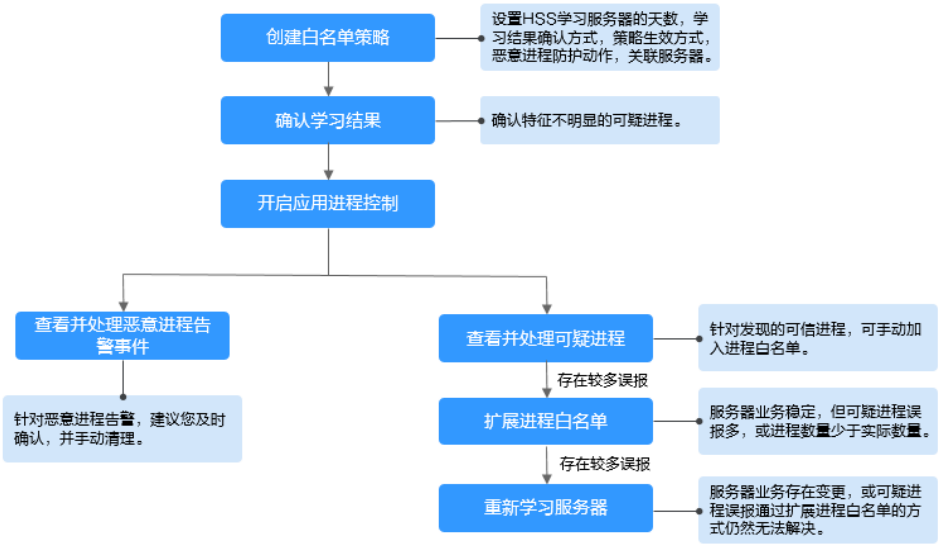


表 7-26 应用进程控制使用流程说明

操作项	描述
创建白名单策略	白名单策略是管理HSS学习服务器行为和应用进程防护动作的规则，只有关联了白名单策略的服务器才能开启应用进程防护。
确认学习结果	HSS学习完服务器中的应用进程后，可能存在某些可疑应用进程的特征不明显，HSS无法完全定义为恶意进程或可信进程，这些不确定具体分类的可疑进程需要您进行确认。
开启应用进程控制	开启策略关联服务器的应用进程控制防护。
查看并处理可疑进程	对于可疑进程运行事件，由于HSS根据学习到的应用进程特征无法判断其是否可信，因此需要您根据这些进程的详细信息判断分析是否可信，然后将它们“加入进程白名单”。
查看并处理恶意进程告警事件	一旦HSS发现恶意进程告警事件将会上报到“检测与响应 > 安全告警事件 > 主机安全告警”页面，您可以前往该页面处理告警，并及时清理恶意进程。
（可选）扩展进程白名单	如果HSS完成服务器学习后，您认为学习到的应用进程数量少于资产指纹功能采集到的进程指纹数量，或者可疑进程事件中存在较多可信的应用进程运行事件，您可以设置HSS扩展进程白名单，通过比对HSS已学习到的应用进程和资产指纹功能采集到的进程指纹，进一步扩展HSS应用进程情报库，补充可信进程白名单。

操作项	描述
（可选）重新学习服务器	已完成进程白名单扩展，但仍然存在较多可信进程运行误报或您的服务器业务存在变更，您可以设置HSS重新学习服务器，校准HSS的应用进程情报数据，避免误报。

7.4.2 创建白名单策略

操作场景

在开启应用进程控制防护前，您需要为服务器创建白名单策略，设置HSS学习服务器应用进程的学习天数、学习结果确认方式以及对恶意进程的防护动作等；HSS后续将根据策略设置为服务器提供相应的应用进程控制防护能力。

创建白名单策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签，单击“创建策略”。

步骤6 在“创建策略”弹窗中，设置策略参数，相关参数说明请参见表 创建白名单策略参数说明。

表 7-27 创建白名单策略参数说明

参数名称	参数说明	取值样例
策略模式	应用进程控制防护策略模式。 默认配置下日常运营模式允许可信、可疑进程运行，仅对恶意进程进行告警。	-
白名单策略名称	系统默认会生成白名单策略名称，建议您自定义修改，后续方便区分和管理。	test
智能学习天数	HSS学习服务器应用进程的天数。学习天数越多，学习结果越准确。	7

参数名称	参数说明	取值样例
学习结果确认方式	当HSS学习完策略关联的服务器后，对于特征不明显可疑进程的确认方式。 ● 自动确认可疑进程：HSS根据应用进程特征库，自动确认并标记特征不明显的可疑应用进程。 ● 手动确认可疑进程：当HSS根据策略配置完成进程学习后，需要您在“应用进程控制 > 白名单策略”页面，单击策略名称，进入策略详情页，选择“进程文件”页签，筛选“待确认状态”的进程，根据实际业务情况确认并手动标记特征不明显的可疑进程。	自动确认可疑进程
策略生效方式	当HSS学习完策略关联的服务器后，开启应用进程控制的方式。 ● 学习完成后自动开启：系统自动开启策略关联的服务器的应用进程控制。 ● 学习完成后手动开启：您根据业务情况手动开启应用进程控制。开启方式请参见**开启应用进程控制防护**。	学习完成后自动开启
防护动作	当发现恶意进程后的防护动作。对恶意进程进行告警。	告警
选择服务器	选择需要防护的服务器。当服务器的防护状态为“防护中”时，才会在列表中呈现，查看服务器状态的操作请参见**查看主机防护状态**。	-

步骤7 单击“确认”，完成创建。

您策略列表中可以查看已创建的策略及策略当前状态。策略相关状态含义请参见**表7-28**。

表 7-28 策略状态说明

策略状态	说明
学习中	HSS正在学习服务器的应用进程特征，请耐心等待。
学习完成，未生效	策略关联的服务器特征已学习完成，请您确认学习结果，具体操作请参见**确认学习结果**。
学习完成，防护中	服务器已开启应用进程控制防护。

----结束

相关操作

编辑白名单策略

如果创建策略完成后，您需要修改策略模式、防护动作或防护的服务器，您可以编辑白名单策略。

步骤1 在目标策略所在行的操作列，单击“编辑”。

步骤2 在编辑策略弹窗中完成信息修改后，单击“确认”。

----结束

删除白名单策略

如果不再需要HSS为您的某个策略中关联的所有服务器提供应用进程控制防护，且无需保留HSS已学习到的应用进程信息，您可以删除白名单策略。删除后，如果后续再次开启应用进程控制，HSS需要重新学习服务器，请谨慎操作！

步骤1 在目标策略所在行的操作列，单击“删除”。

步骤2 在弹窗中，单击“确认”。

----结束

7.4.3 确认学习结果

操作场景

HSS学习完白名单关联的服务器后，输出的学习结果中可能存在一些特征不明显的可疑进程需要再次进行确认，您可以手动或设置系统自动确认这些可疑进程，并分类标记为可疑、恶意或可信进程。

学习结果确认方式，仅在**创建白名单策略**时可设置：

- “学习结果确认方式”选择的“自动确认可疑进程”：HSS将根据应用进程情报自动对可疑进程进行分类标记。
- “学习结果确认方式”选择的“手动确认可疑进程”：您需要手动对可疑进程进行分类标记。具体操作您可以参考本章节。

前提条件

已完成策略创建，且策略状态为“学习完成，未生效”。具体操作请参见**创建白名单策略**。

确认学习结果

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 单击策略状态为“学习完成，未生效”的策略名称，进入“策略详情”界面。

步骤7 选择“进程文件”页签。

步骤8 单击待确认进程数量，查看待确认进程。

步骤9 根据进程名称和进程文件路径等信息，确认应用进程是否可信。

步骤10 在已确认进程所在行的操作列，单击“标记”。

您也可以批量勾选所有应用进程，单击进程列表左上方的“批量标记”，进行批量标记。

步骤11 在标记弹窗中，选择进程“信任状态”。

可选择可疑、可信和恶意三种信任状态。

步骤12 单击“确认”，完成标记。

----结束

后续操作

学习结果确认完成，即可开启应用进程防护，具体操作请参见**开启应用进程控制防护**。

7.4.4 开启应用进程控制防护

操作场景

应用进程控制功能支持分类控制服务器中的应用进程运行，允许可疑、可信进程运行，告警恶意进程运行，为服务器进程运行提供安全防护，防止服务器遭受恶意进程的破坏。

开启应用进程控制防护的方式仅在**创建白名单策略**时可设置：

- “策略生效方式”选择“学习完成后自动开启”：系统完成策略关联服务器学习后，自动为该策略的服务器开启应用进程控制防护。
- “策略生效方式”选择“学习完成后手动开启”：您可根据实际业务情况手动为服务器开启应用进程控制防护。具体操作您可以参考本章节。

前提条件

已创建白名单策略并完成策略学习结果确认，具体操作请参见**创建白名单策略**和**确认学习结果**。

开启应用进程控制防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 在目标策略所在行的操作列，单击“开启防护”。

您也可以批量选中所有目标策略，在策略列表左上方，单击“开启防护”，批量为多个策略开启防护。

步骤7 在开启防护弹窗中，单击“确认”。

步骤8 在策略列表中，查看目标策略的策略状态为“学习完成，防护中”，表示开启应用进程防护成功。

----结束

后续操作

开启应用进程控制防护后，服务器中出现的可疑或恶意进程运行事件将触发告警，处理相关事件请参见：

- 处理可疑进程运行事件：**查看并处理可疑进程**。
- 处理恶意进程运行事件：**处理主机告警事件**。

7.4.5 查看并处理可疑进程

操作场景

在应用进程控制防护过程中，如有新增的应用进程启动，HSS会将其展示在可疑进程列表中；您可以根据实际情况判断该进程是否可信，如果该进程是正常业务进程，您可以将其加入进程白名单。

查看并处理可疑进程

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“可疑进程”页签，查看存在的可疑进程。

步骤6 根据可疑进程HASH和文件路径等信息，判断可疑进程是否为可信进程。

- 进程可信：执行**步骤7**。
- 进程不可信：手动清理该进程。

步骤7 在可疑进程所在行的“操作”列，单击“处理”。

您也可以批量勾选可疑进程，在列表左上方单击“批量处理”，批量处理可疑进程。

步骤8 在处理弹窗中，选择“处理方式”。

可选择“加入进程白名单”。

步骤9 单击“确认”，完成处理。

----结束

相关操作

一旦HSS发现恶意进程运行事件将会上报到“检测与响应 > 安全告警事件 > 主机安全告警”页面，您可以前往该页面处理告警，并及时清理恶意进程。详细操作请参见**处理主机告警事件**。

7.4.6 扩展进程白名单

操作场景

如果白名单策略学习完成后，您认为HSS学习到的应用进程数量少于资产指纹功能采集到的进程指纹数量，或者可疑进程事件中存在较多可信的应用进程运行事件，您可以扩展进程白名单。该功能将通过比对白名单策略已学习的应用进程和资产指纹功能采集到的进程指纹，进一步扩展应用进程情报库，补充可信进程白名单。

确认应用进程白名单学习结果请参见**确认学习结果**，查看进程指纹请参见**查看主机资产指纹**。

扩展进程白名单

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤7 选择“关联服务器”页签。

步骤8 在目标服务器所在行的操作列，单击“更多 > 进程白名单扩展”

步骤9 单击“开始匹配”，比对服务器进程指纹和白名单学习到的应用进程。

步骤10 将比对出的可信进程选中，并单击“添加”，完成进程白名单扩展。

可选择进程文件页签，查看添加的白名单进程。

----结束

7.4.7 重新学习服务器

操作场景

如果您已**扩展进程白名单**，但仍然存在较多可信进程运行误报，或者您的服务器业务存在变更，建议您设置HSS重新学习服务器，校准HSS的应用进程情报数据，避免误报。

重新学习服务器

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤7 选择“关联服务器”页签。

步骤8 勾选需要目标服务器，并单击列表左上方的“重新学习”。

步骤9 在弹窗中单击“确认”，开始重新学习。

重新学习将根据策略设置的智能学习时间完成学习，学习完成后，请及时确认学习结果，具体操作请参考**确认学习结果**。

----结束

7.4.8 关闭应用进程控制防护

操作场景

如果不再需要HSS为您的服务器提供应用进程控制防护，您可以参考本章节关闭应用进程控制防护。

关闭策略关联的所有服务器防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 关闭应用进程防护

- 关闭防护，但保留HSS学习到的服务器应用进程特征。
  a. 在目标策略所在行的操作列，单击“关闭防护”。或者批量选中所有目标策略，并在策略列表左上方单击“关闭防护”，批量为多个策略关闭防护。
  b. 单击“确认”。
- 关闭防护，并删除HSS学习到的服务器应用进程特征。
  a. 在目标策略所在行的操作列，单击“删除”。
  b. 单击“确认”。

步骤7 在策略列表中，查看目标策略。

- 关闭防护，但保留HSS学习到的服务器应用进程特征。
  查看目标策略的策略状态为“学习完成，未生效”，表示关闭应用进程防护成功。
- 关闭防护，并删除HSS学习到的服务器应用进程特征。
  目标策略已从策略列表中删除，表示关闭应用进程防护成功。

----结束

关闭单台服务器防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“主机防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤5 选择“白名单策略”页签。

步骤6 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤7 选择“关联服务器”页签。

步骤8 关闭应用进程防护

- 关闭防护，但保持服务器和当前策略的关联关系。
  a. 在目标策略所在行的操作列，单击“关闭防护”。或者批量选中所有目标策略，并在策略列表左上方单击“关闭防护”，批量为多个策略关闭防护。
  b. 单击“确认”。
- 关闭防护，并解除服务器和当前策略的关联关系。

  说明

  如果您需要为服务器切换防护策略，请先在当前策略中删除该服务器，再新建或编辑防护策略关联该服务器。

  a. 在目标策略所在行的操作列，单击“删除”。
  b. 单击“确认”。

步骤9 在服务器列表中，查看目标服务器，确认关闭防护是否成功。

- 关闭防护，但保持服务器和当前策略的关联关系。
  查看目标服务器的策略状态为“学习完成，未生效”，表示关闭应用进程防护成功。
- 关闭防护，并解除服务器和当前策略的关联关系。
  目标服务器已从列表中删除，表示关闭应用进程防护成功。

----结束

7.5 文件完整性管理

7.5.1 文件完整性管理概述

文件完整性管理功能可实时监控Linux服务器上的关键文件，对新增、修改、删除文件内容的操作进行告警和记录，可帮助用户及时发现可能遭受攻击的更改。

文件完整性监控原理

通过比对上一次扫描的文件状态和当前文件状态，分析确定文件是否遭到可疑的更改。

文件完整性监控范围

HSS预置了部分文件监控路径，具体如表7-29所示。

如果您需要自定义添加或删除监控文件，您可以修改“文件保护”策略中“关键文件完整性检测”部分的内容，详细操作请参考配置策略。

表 7-29 默认文件监控路径

类型	监控文件
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

7.5.2 查看文件变更记录

文件完整性管理为您提供变更统计、变更类别、以及文件变更记录等，让您实时了解监控文件的变更情况，及时发现恶意变更。

查看文件变更概况

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“主机防御 > 文件完整性管理”，进入文件完整性管理界面，查看文件变更概况。

表 7-30 文件变更概况参数说明

参数名称	参数说明
服务器统计	存在文件变更的服务器数量统计。
变更统计	• 总变更数：所有文件和注册表变更的总数量。 • 文件数：所有文件变更的数量。 • 注册表：所有注册表变更的数量。
变更类别	• 修改：所有文件和注册表修改的数量。 • 新增：所有文件和注册表新增的数量。 • 删除：所有文件和注册表删除的数量。

----结束

查看单个服务器文件变更记录

步骤1 在云服务器列表中，可查看服务器对应的文件、注册表变更数量和最后变更时间。

步骤2 单击服务器名称进入服务器变更详情页，可查看单个服务器的文件变更详细记录。

表 7-31 服务器文件变更参数说明

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 • 注册表	文件

参数名称	参数说明	取值样例
变更类别	变更文件的类别。 • 新增 • 修改 • 删除	修改
最后变更时间	目标文件最后一次发生变更的时间。	-

----结束

查看全量服务器文件变更记录

在变更文件列表中，可查看所有文件变更记录，参数说明可参见**表7-31**。

文件变更处置建议

文件完整性管理界面会一直保留文件变更记录（服务器一直开启HSS防护的情况下），方便您回溯取证攻击者的行为活动。当您在文件完整性管理界面查看到文件变更记录时，请及时确认该文件的变更是否为异常事件。

- 确认文件变更事件是异常事件，建议您在确认对业务无影响的情况下，手动阻断相关进程并隔离对应文件。
- 确认文件变更事件是正常业务操作，您可以进行忽略，或修改文件完整性监控范围，修改监控范围请参见**配置策略**中“文件保护”策略的“关键文件完整性检测”部分。

当有文件变更时会同步触发“文件/目录变更”告警，建议您同步处理告警。具体操作如下：

1. 在“文件完整性管理”页面，确认存在文件变更的服务器，复制服务器名称。
2. 在左侧导航栏选择“检测与响应 > 安全告警事件”，进入安全告警事件页面。
3. 在“主机安全告警”页签，选择“告警类型”为“系统异常行为 > 文件/目录变更”的告警。
4. 在右侧搜索栏中，通过服务器名称搜索到该服务器存在的“文件/目录变更”告警事件。
5. 单击告警名称查看告警详情，结合在“文件完整性管理”界面查看到的文件变更信息，判断文件变更事件是否是异常事件。
6. 确认完成后，可在告警详情页面下方单击处理方式。

   告警处理后，仅影响是否告警，文件完整性管理界面的变更记录会一直保留。

   a. 我已手动处理：表示您已经手动阻断相关进程并隔离对应的文件，风险已不存在。
   b. 忽略：表示文件变更无影响，可忽略告警。
   c. 加入告警白名单：表示文件变更为正常业务操作导致，需要加入告警白名单，无需告警。

7.6 病毒查杀

7.6.1 病毒查杀概述

什么是病毒查杀?

病毒是指植入服务器系统中，破坏服务器功能或数据，影响服务器使用或能够自我复制的指令或程序代码。一旦病毒进入用户服务器，会对其造成不同程度的危害，轻则占用系统内存导致系统运行速度减慢，重则导致重要资料丢失、信息泄露、系统崩溃等后果，带来难以估量的损失。

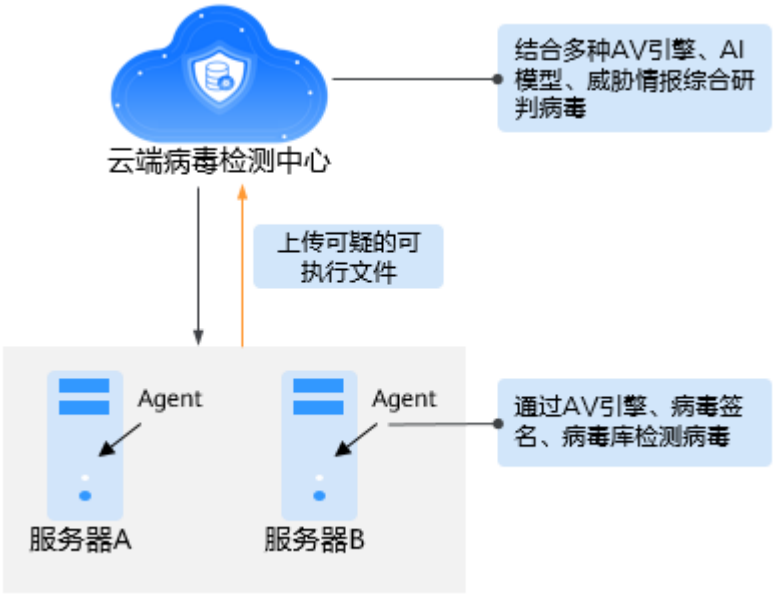
为了应对病毒威胁，企业主机安全为用户提供了病毒查杀功能，帮助用户检测和清理病毒，保护服务器免受病毒侵害。

企业主机安全的病毒查杀功能采用云端与本地相结合的病毒防护机制，能够全面扫描主机中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可以根据实际需求，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”任务，及时发现并清理病毒文件，增强业务系统的病毒防御能力。

病毒查杀原理

企业主机安全的病毒查杀功能采用云端与本地相结合的病毒检测和防御机制，在主机本地，利用病毒签名库以及Agent侧AV引擎快速扫描所有静态文件，一旦发现恶意文件立即实施隔离，对于可疑的可执行文件，则会将其上传至云端病毒检测中心；云端病毒中心采用多种AV引擎、AI模型以及威胁情报等技术手段，进一步对可疑文件进行全面评估，深度查杀病毒。

图 7-4 病毒查杀原理



病毒查杀可查杀的病毒类型

病毒查杀可查杀勒索病毒、挖矿程序、DDoS木马、木马程序、后门程序、恶意程序、高危程序、蠕虫病毒、可疑程序及自变异木马等。

病毒查杀的优势

- **快速、精准识别文件类型**

  集成了专用的文件类型识别算法，针对文件真实内容进行检测，有效鉴别仿冒的文件后缀或内容，可以快速、精确识别上百种文件类型。

- **深度解析恶意文件**

  采用云端+本地协同的病毒检测机制，对二进制文件、复合文档和各类脚本文件进行分析，还原完整的文件内容，深度识别潜藏的恶意行为。

约束与限制

- 病毒查杀功能仅企业主机安全企业版、旗舰版、网页防篡改版、容器版支持。
  - 专业版：支持快速查杀。
  - 企业版及其他版本：支持快速查杀、全盘查杀、自定义查杀。
- 使用病毒查杀功能，需确保服务器安装的Agent为以下版本，升级Agent的操作，请参见**升级主机Agent**。
  - Linux：3.2.9及以上版本。
  - Windows：4.0.20及以上版本。
- 病毒查杀功能依赖AV检测策略进行检测，请确保“AV检测”策略开启。详细操作请参见**配置策略**。

病毒查杀使用流程

图 7-5 病毒查杀使用流程

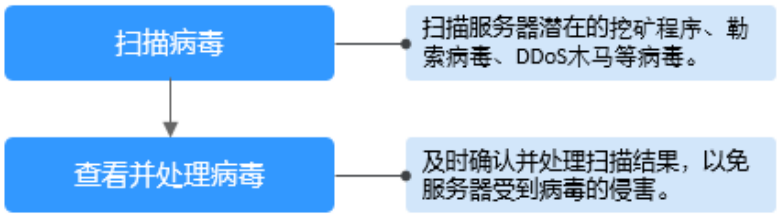


表 7-32 病毒查杀使用流程说明

操作项	说明
扫描病毒	病毒查杀功能提供快速查杀、全盘查杀、自定义查杀三种病毒扫描方式，您可以通过这些方式深度扫描服务器中潜在的挖矿程序、勒索病毒、DDoS木马等病毒。

操作项	说明
查看并处理病毒	对于扫描出的病毒文件，企业主机安全提供多种处理方式，包括隔离查杀、加白和忽略。您可以通过隔离查杀功能，有效清除各种类型的病毒。 建议您在病毒扫描完成后，及时查看并处理扫描结果，以确保服务器免受病毒的侵害。

7.6.2 扫描病毒

操作场景

病毒文件一旦启动就可能化身恶意进程，成为服务器的巨大安全隐患，因此建议您及时为服务器扫描并清理病毒。

企业主机安全的病毒查杀功能，提供快速查杀、全盘查杀、自定义查杀三种扫描方式供您选择，具体介绍请参见表7-33。

表 7-33 病毒扫描方式说明

扫描方式	说明	扫描文件类型	扫描目录范围
快速查杀	节约时间成本的快速病毒扫描任务，查杀预置的系统关键文件和目录。	• Windows 进程（活动进程、隐藏进程、Docker进程）、内核模块、已安装程序、动态库劫持、服务、计划任务、开机自启动项、敏感目录、office文件、图片、视频、执行脚本、压缩包等。 • Linux 进程（活动进程、隐藏进程、Docker进程）、内核模块、已安装程序、动态库劫持、服务、计划任务、开机自启动项、敏感目录、office文件、图片、视频、执行脚本、压缩包等。	• Windows – 用户的桌面、下载、文档目录 – 开始菜单启动项 – 系统目录 C:\Windows\System、C:\Windows\System32、C:\Windows\SysWOW64 – 临时目录 C:\Users\[用户名]\AppData\Local\Temp\、C:\Temp、C:\Windows\Temp – 浏览器下载目录 Chrome浏览器、Edge浏览器、Firefox浏览器 • Linux – 标准系统目录 /bin、/sbin、/lib、/lib64、/usr/bin、/usr/sbin、/usr/lib、/usr/lib64、/usr/local/lib、/usr/local/lib64、/usr/local/bin、/usr/local/sbin – 其他重要目录 /tmp、/root、/home、/boot、/opt、/data、/var/tmp、/var/run、/var/lib、/dev/shm、/etc、/etc/sysconfig、/usr/local/src、/usr/share、根目录/ – 启动项对应可执行文件目录 /etc/rc.d、/etc/init.d

扫描方式	说明	扫描文件类型	扫描目录范围
全盘查杀	比较耗费时间的全磁盘病毒扫描任务，全面清扫服务器中的病毒文件。	• 可执行：可执行文件和动态链接库，常见exe、dll、so等。 • 压缩：压缩包和安装包文件，常见zip、rar、tar等。 • 脚本：脚本文件，常见的bat、py、ps1等。 • 文档：文档文件，常见的txt、doc、pdf等。 • 图片：图片文件，常见的bmp、jpg、gif等。 • 音视频：音视频文件，常见的mp3、mp4、flv等。	除网络目录外的所有目录。不扫描网络目录的主要原因如下： • 扫描效率低 网络目录通常包含大量文件，总容量可能达到上百TB，这将显著降低扫描效率。 • 占用网络带宽 访问网络目录时需要占用网络带宽，大规模扫描可能导致带宽被完全占满，进而影响到您正常业务的运行，包括但不限于网络速度变慢、网络延迟增加等。 如需扫描网络目录，可以使用自定义查杀任务。
自定义查杀	您可以根据自身需求自定义的病毒扫描任务。	用户可自定义扫描可执行、压缩、脚本、文档、图片或音视频文件。	用户自定义

约束限制

- 病毒查杀过程中会占用较多的内存、CPU、IO等资源，请在服务器空闲时进行病毒查杀。
- 全盘查杀不扫描网络目录。

快速查杀

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击“快速查杀”，弹出“快速查杀”对话框。

步骤6 根据界面提示，填写“快速查杀”任务相关参数。

表 7-34 快速查杀参数说明

参数名称	参数说明	取值样例
任务名称	企业主机安全会根据任务创建时间（精确到秒）自动生成一个任务名称，您可以按需修改。	快速查杀-20250425173536
选择服务器	选择需要执行快速查杀的服务器。 满足以下所有条件的服务器，支持选择并执行病毒查杀。 • Agent在线，且Windows Agent版本≥4.0.20，Linux Agent版本≥3.2.9。安装Agent请参见**为主机安装Agent**。 • 已开启AV检测策略。开启AV检测策略请参见**配置策略**。 • 当前不在扫描中。	-
处置策略	选择检测到的病毒文件后的处理方式。 • 自动处置：企业主机安全自动隔离检测到的恶意文件，部分未被确认为病毒的可疑文件会打上“可疑”标签需用户确认后手动处置。 **注意** 存在极小概率的误隔离情况，若误隔离，您可以在文件隔离箱中恢复隔离文件，具体操作请参见**恢复已隔离文件** • 人工处置：仅对检测到的病毒文件进行告警，不自动隔离，需人工确认后进行处置。	自动处置

步骤7 单击“开始扫描”，立即启动查杀任务。

----结束

全盘查杀

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击“全盘查杀”，弹出“全盘查杀”对话框。

步骤6 根据界面提示，填写“全盘查杀”任务相关参数。

表 7-35 全盘查杀参数说明

参数名称	参数说明	取值样例
任务名称	企业主机安全会根据任务创建时间（精确到秒）自动生成一个任务名称，您可以按需修改。	全盘查杀-20250425174038
选择服务器	选择需要执行全盘查杀的服务器。 满足以下所有条件的服务器，支持选择并执行病毒查杀。 • Agent在线，且Windows Agent版本≥4.0.20，Linux Agent版本≥3.2.9。安装Agent请参见**为主机安装Agent**。 • 已开启AV检测策略。开启AV检测策略请参见**配置策略**。 • 当前不在扫描中。	-
处置策略	选择检测到的病毒文件后的处理方式。 • 自动处置：企业主机安全自动隔离检测到的恶意文件，部分未被确认为病毒的可疑文件会打上“可疑”标签需用户确认后手动处置。 **注意** 存在极小概率的误隔离情况，若误隔离，您可以在文件隔离箱中恢复隔离文件，具体操作请参见**恢复已隔离文件** • 人工处置：仅对检测到的病毒文件进行告警，不自动隔离，需人工确认后进行处置。	自动处置

步骤7 单击“开始扫描”，立即启动查杀任务。

----结束

自定义查杀

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击“自定义查杀”，弹出“自定义查杀”对话框。

步骤6 根据界面提示，配置“自定义查杀”策略参数。参数说明请参见**表 自定义查杀策略参数说明**。

表 7-36 自定义查杀策略参数说明

参数名称	参数说明	取值样例
任务名称	企业主机安全会根据任务创建时间（精确到秒）自动生成一个任务名称，您可以按需修改。	自定义查杀-20250425180036
启动类型	选择查杀任务的执行方式。 ● 立即启动：立即执行一次查杀任务。 ● 稍后启动：按您设置的稍后启动时间执行一次查杀任务。 ● 周期启动：按您设置的扫描周期，周期执行查杀任务。	稍后启动
稍后启动时间	仅启动类型选择“稍后启动”时，需要配置病毒查杀执行的启动时间。稍后启动时间可选一个月内的时间。	2025/04/25 18:10
扫描周期	仅启动类型选择“周期启动”时，需要配置病毒查杀执行的周期。	-
防护文件类型	扫描文件类型，勾选即对该文件类型进行扫描。当前支持扫描的文件类型： ● 可执行：可执行文件和动态链接库，常见exe、dll、so等。 ● 压缩：压缩包和安装包文件，常见zip、rar、tar等。 ● 脚本：脚本文件，常见的bat、py、ps1等。 ● 文档：文档文件，常见的txt、doc、pdf等。 ● 图片：图片文件，常见的bmp、jpg、gif等。 ● 音视频：音视频文件，常见的mp3、mp4、flv等。	全选
目录设置（可选）	需要扫描病毒文件的目录。不配置时，默认进行全盘扫描，全盘扫描不扫描网络目录。 **警告** 不建议扫描网络目录，原因如下： ● 扫描效率低 网络目录通常包含大量文件，总容量可能达到上百TB，这将显著降低扫描效率。 ● 占用网络带宽 访问网络目录时需要占用网络带宽，大规模扫描可能导致带宽被完全占满，进而影响到您正常业务的运行，包括但不限于网络速度变慢、网络延迟增加等。	-
排除指定目录（可选）	无需扫描病毒文件的目录。	-

参数名称	参数说明	取值样例
选择服务器	选择需要查杀服务器。 满足以下所有条件的服务器，支持选择并执行病毒查杀。 ● Agent在线，且Windows Agent版本≥4.0.20，Linux Agent版本≥3.2.9。安装Agent请参见**为主机安装Agent**。 ● 已开启AV检测策略。开启AV检测策略请参见**配置策略**。 ● 符合策略启动要求： – 启动类型为“立即启动”的策略：服务器当前不在扫描中。 – 启动类型为“稍后启动”的策略：服务器未关联与当前策略“稍后启动时间”相同的自定义查杀策略。 – 启动类型为“周期启动”的策略：服务器未关联“周期启动”自定义查杀策略。	-
处置策略	选择检测到的病毒文件后的处理方式。 ● 自动处置：企业主机安全自动隔离检测到的恶意文件，部分未被确认为病毒的可疑文件会打上“可疑”标签需用户确认后手动处置。 **注意** 存在极小概率的误隔离情况，若误隔离，您可以在文件隔离箱中恢复隔离文件，具体操作请参见**恢复已隔离文件** ● 人工处置：仅对检测到的病毒文件进行告警，不自动隔离，需人工确认后进行处置。	自动处置

步骤7 单击“开始扫描”，启动查杀任务。

----结束

后续操作

- 查看扫描任务执行状态
  a. 在病毒查杀界面，单击“扫描任务”，查看病毒扫描任务执行状态。
     如果您需要停止正在执行的扫描任务，您可以在目标扫描任务所在行的“操作”列，单击“取消”。
  b. 单击扫描任务前的 ，可展开查看具体各服务器的扫描状态和已扫描的文件数量等信息。
     如果您需要停止扫描某台服务器，您可以在目标服务器所在行的“操作”列，单击“取消”。
- 查看并处理病毒
  病毒查杀任务执行完成后，对于检测到的病毒文件，您需要根据自身业务情况判断并进行人工处置，详细操作请参见**查看并处理病毒**。

7.6.3 查看并处理病毒

操作场景

病毒扫描任务执行完成后，企业主机安全会根据您创建查杀任务时选择的处置策略处置检测到的病毒文件，相关处置策略如下：

- 自动处置：企业主机安全自动隔离检测到的恶意文件，部分未被确认为病毒的可疑文件会打上“可疑”标签需用户确认后手动处理。
- 人工处置：仅对检测到的病毒文件进行告警不自动隔离，需人工确认后进行处理。

无论您选择哪种处置策略，您都需要及时确认并处理扫描结果，以确保您的服务器不受病毒的威胁。

本章节为您介绍如何查看并人工处置病毒文件。

前提条件

已执行病毒查杀任务，详细操作请参见**扫描病毒**。

查看并处理病毒

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

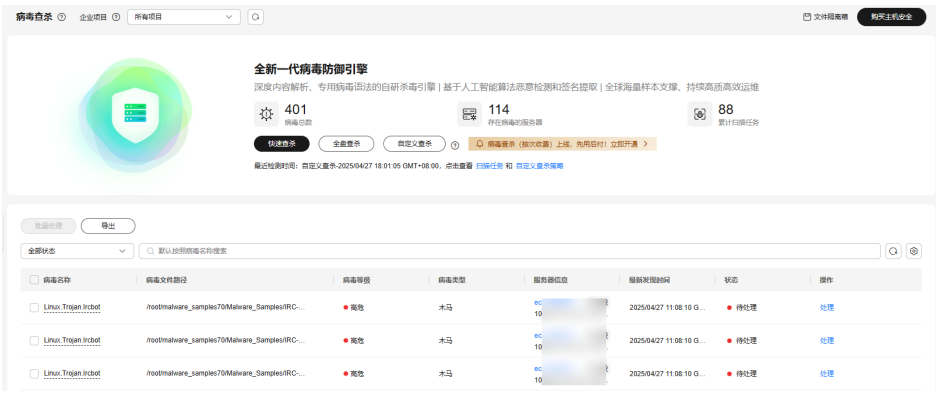
步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 查看扫描到的病毒文件。

鼠标悬停在病毒名称上方，可查看文件路径、文件HASH、属主、属性、大小、创建时间等信息。

图 7-6 病毒文件列表



步骤6 在目标病毒文件所在行的“操作”列，单击“处理”。

您也可以勾选多个病毒文件，并在列表上方单击“批量处理”，批量处理多个文件。

步骤7 在“处理病毒文件”弹窗中，选择病毒文件处理方式。处理方式说明请参见**表 病毒文件处理方式说明**。

表 7-37 病毒文件处理方式说明

参数名称	参数说明
手动处理	如果您要在主机上手动处理当前病毒文件，请选择手动处理。
忽略	忽略本次病毒文件告警，如果再次检测到该病毒文件，主机安全将正常进行告警。
加入告警白名单	如果您排查后确认该病毒文件为误报，您可以将其加入告警白名单，加入白名单后，后续主机安全不再对该病毒文件进行告警。
手动隔离文件	隔离该病毒文件，隔离后，该病毒文件将变为“只读”状态，为避免对业务造成影响，请谨慎操作。 被成功隔离的文件会添加到“文件隔离箱”中，无法再对主机造成威胁，您也可以根据自身需要恢复或删除已隔离文件，详细操作请参见**文件隔离箱**。

步骤8 单击“确认”，完成处理。

处理后，病毒文件告警事件状态变更为“已处理”。

----结束

导出病毒告警事件

如果病毒告警事件数量较多，您想要导出到本地进行查看，可参考本小节操作。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 在病毒文件告警事件列表上方，单击“导出”，导出所有病毒文件告警事件到本地。

步骤6 在导出弹窗中，单击“确认”。

步骤7 在病毒查杀界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的病毒文件信息。

导出过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

7.6.4 管理自定义查杀策略

操作场景

每创建一次周期启动、稍后启动的自定义查杀任务都会生成一条自定义查杀策略，针对这些策略您可以修改策略内容或删除不需要的策略。

例如，“稍后启动”的自定义查杀策略，执行过一次后即失效（带有已失效标签），您可以通过编辑修改其启动时间，再次启用该策略。

编辑自定义查杀策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击“自定义查杀策略”，查看已自定义的查杀策略。

步骤6 在目标策略所在行的“操作”列，单击“编辑”，进入编辑策略页面，修改策略。相关参数说明请参见**表7-38**。

表 7-38 自定义查杀策略参数说明

参数名称	参数说明	取值样例
任务名称	企业主机安全会根据任务创建时间（精确到秒）自动生成一个任务名称，您可以按需修改。	自定义查杀-20250425180036
启动类型	选择查杀任务的执行方式。 • 立即启动：立即执行一次查杀任务。 • 稍后启动：按您设置的稍后启动时间执行一次查杀任务。 • 周期启动：按您设置的扫描周期，周期执行查杀任务。	稍后启动
稍后启动时间	仅启动类型选择“稍后启动”时，需要配置病毒查杀执行的启动时间。稍后启动时间可选一个月内的时间。	2025/04/25 18:10
扫描周期	仅启动类型选择“周期启动”时，需要配置病毒查杀执行的周期。	-

参数名称	参数说明	取值样例
防护文件类型	扫描文件类型，勾选即对该文件类型进行扫描。当前支持扫描的文件类型： • 可执行：可执行文件和动态链接库，常见exe、dll、so等。 • 压缩：压缩包和安装包文件，常见zip、rar、tar等。 • 脚本：脚本文件，常见的bat、py、ps1等。 • 文档：文档文件，常见的txt、doc、pdf等。 • 图片：图片文件，常见的bmp、jpg、gif等。 • 音视频：音视频文件，常见的mp3、mp4、flv等。	全选
目录设置（可选）	需要扫描病毒文件的目录。不配置时，默认进行全盘扫描，全盘扫描不扫描网络目录。 **警告** 不建议扫描网络目录，原因如下： • 扫描效率低 网络目录通常包含大量文件，总容量可能达到上百TB，这将显著降低扫描效率。 • 占用网络带宽 访问网络目录时需要占用网络带宽，大规模扫描可能导致带宽被完全占满，进而影响到您正常业务的运行，包括但不限于网络速度变慢、网络延迟增加等。	-
排除指定目录（可选）	无需扫描病毒文件的目录。	-
选择服务器	选择需要查杀服务器。 满足以下所有条件的服务器，支持选择并执行病毒查杀。 • Agent在线，且Windows Agent版本≥4.0.20，Linux Agent版本≥3.2.9。安装Agent请参见**为主机安装Agent**。 • 已开启AV检测策略。开启AV检测策略请参见**配置策略**。 • 符合策略启动要求： – 启动类型为“立即启动”的策略：服务器当前不在扫描中。 – 启动类型为“稍后启动”的策略：服务器未关联与当前策略“稍后启动时间”相同的自定义查杀策略。 – 启动类型为“周期启动”的策略：服务器未关联“周期启动”自定义查杀策略。	-

参数名称	参数说明	取值样例
处置策略	选择检测到的病毒文件后的处理方式。 • 自动处置：企业主机安全自动隔离检测到的恶意文件，部分未被确认为病毒的可疑文件会打上“可疑”标签需用户确认后手动处置。 **注意** 存在极小概率的误隔离情况，若误隔离，您可以在文件隔离箱中恢复隔离文件，具体操作请参见**恢复已隔离文件** • 人工处置：仅对检测到的病毒文件进行告警，不自动隔离，需人工确认后进行处置。	自动处置

步骤7 单击“确认”，完成修改。

----结束

删除自定义查杀策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击“自定义查杀策略”，查看已自定义的查杀策略。

步骤6 在目标策略所在行的“操作”列，单击“删除”。

您也可以选中多条策略，并在策略列表左上方，单击“删除”，批量删除策略。

步骤7 单击“确认”，完成删除。

----结束

7.6.5 管理文件隔离箱

操作场景

被成功隔离的病毒文件会添加到“文件隔离箱”中，无法再对主机造成威胁。您也可以根据自身需要参考本章节恢复或删除已隔离文件。

- **恢复已隔离文件**：如果被隔离的文件确认是正常业务文件，非病毒文件，您可以选择恢复该文件。
- **删除已隔离文件**：如果被隔离的文件确认已经感染病毒，是病毒文件，可删除该文件，彻底清除病毒。

恢复已隔离文件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击界面右上角“文件隔离箱”，弹出“文件隔离箱”弹窗。

步骤6 单击文件隔离箱列表中“操作”列的“恢复”，弹出“恢复已隔离文件”对话框。

步骤7 单击“确认”，恢复文件。

文件恢复后可正常使用，则表示恢复文件成功。

----结束

删除已隔离文件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤5 单击界面右上角“文件隔离箱”，弹出“文件隔离箱”弹窗。

步骤6 单击文件隔离箱列表中“操作”列的“删除”，弹出“删除已隔离文件”对话框。

如需批量删除已隔离文件，您可以勾选多个目标已隔离文件，并单击已隔离文件列表左上角的“删除”。

步骤7 单击“确认”，完成删除。

在文件隔离箱中确认无该文件，则表示删除成功。

----结束

7.7 动态端口蜜罐

7.7.1 动态端口蜜罐概述

什么是动态端口蜜罐?

动态端口蜜罐功能是一种主动防御措施，通过利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。

用户可选择系统推荐端口或自定义端口开启动态端口蜜罐，诱捕失陷主机，降低真实资源被入侵的风险。

动态端口蜜罐防护原理

动态端口蜜罐防护原理如图7-7所示，以下是详细解释：

1. 创建防护策略

   用户选择目标服务器设置蜜罐端口。蜜罐端口一般是常见业务端口，但在实际业务中未使用。

2. 监听蜜罐端口

   企业主机安全对用户设置的蜜罐端口开启实时监听。

3. 连接蜜罐端口

   当攻击者扫描网络或尝试连接时，如果连接了蜜罐端口，企业主机安全会记录连接事件，并拒绝连接。

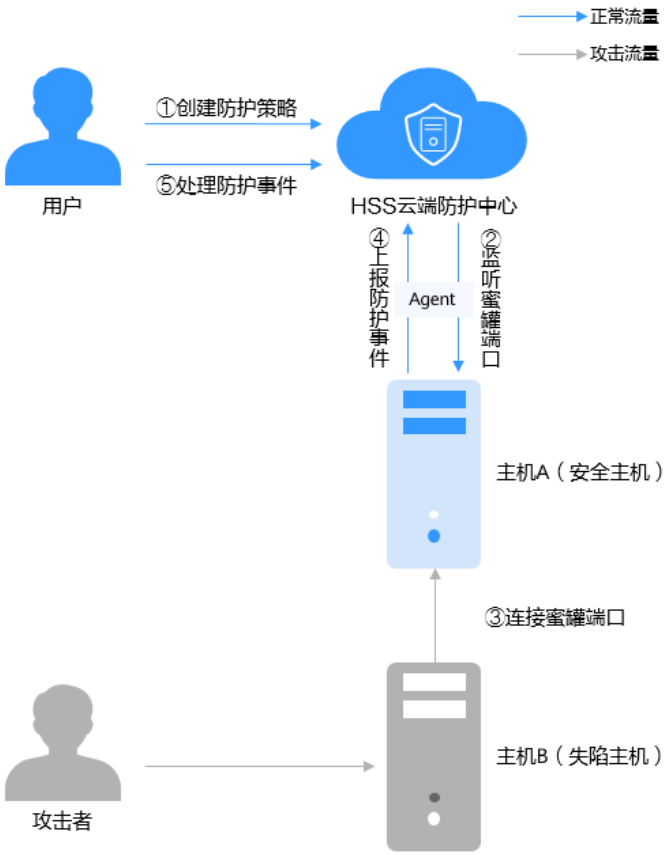
4. 上报防护事件

   一旦蜜罐端口被连接，企业主机安全将立即告警，并将相关事件信息展示在防护事件列表。

5. 处理防护事件

   用户根据蜜罐端口防护事件，并结合其他攻击防护事件，排查内网是否存在失陷主机。

图 7-7 动态端口蜜罐防护原理



动态端口蜜罐的应用场景

与传统以防御为主的安全技术不同，动态端口蜜罐采用主动出击的方式，在内网环境下诱捕潜在攻击者，不仅能够及时发现失陷主机，在一定程度上也能干扰和延缓攻击者的行为活动。

如何使用动态端口蜜罐?

表 7-39 动态端口蜜罐使用流程说明

序号	操作项	说明
1	创建动态端口蜜罐防护策略	设置蜜罐端口，添加源IP白名单以及绑定目标服务器（未绑定EIP）等。
2	查看处理蜜罐防护事件	如果有疑似失陷主机连接蜜罐端口，动态端口蜜罐功能将上报告警事件，您可以根据自身业务情况处理这些告警。

约束与限制

- 动态端口蜜罐功能仅支持防护未绑定弹性公网IP的服务器。
- 动态端口蜜罐功能仅企业主机安全旗舰版、网页防篡改版、容器版支持。
- 使用动态端口蜜罐功能，需确保服务器安装的Agent为以下版本。升级Agent的操作，请参见升级主机Agent。
  - Linux：3.2.10及以上版本。
  - Windows：4.0.22及以上版本。

7.7.2 创建动态端口蜜罐防护策略

操作场景

动态端口蜜罐功能是以真实端口作为诱饵端口诱导攻击者访问，因此开启动态端口蜜罐防护时，用户需要创建防护策略以添加服务器端口作为蜜罐端口开启防护。

本章节介绍如何创建动态端口蜜罐防护策略。

约束与限制

- 一台服务器最多支持添加50个蜜罐端口。
- 一个蜜罐端口只能绑定一个协议，支持TCP和TCP6协议。

创建动态端口蜜罐防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在“防护配置”页签，单击“创建防护策略”，弹出“创建防护策略”对话框。

步骤7 根据界面提示，创建防护策略。

1. 配置策略，配置完成后单击“下一步”。相关参数说明请参见**表 创建动态端口蜜罐防护策略参数说明**。

   表 7-40 创建动态端口蜜罐防护策略参数说明

参数名称	参数说明
策略名称	可保持默认名称，您也可以自定义输入一个易识别的名称。
操作系统类型	选择要添加端口蜜罐的服务器操作系统类型。
防护端口	设置蜜罐端口。HSS默认提供了部分常用端口，Linux系统默认提供Windows常用端口，Windows系统默认提供Linux常用端口，您可以根据自身需求修改端口。 **说明** 请您确定添加的防护端口未被其他服务占用，如果端口被占用会导致动态端口蜜罐功能开启失败。
源IP白名单（可选）	动态端口蜜罐功能默认主动连接蜜罐端口的主机都是内网失陷主机，一旦检测到可疑的连接行为将会上报告警。 因此如果有您信任的主机会连接蜜罐端口，建议您将该主机的IP加到源IP白名单。 可输入IP地址或网段，最多可添加50个IP地址或网段，多个IP地址或网段以英文逗号分隔。

2. 勾选绑定目标服务器，单击“保存并启用”，创建防护策略完成。

   需要注意的是，满足以下所有条件的服务器，才支持勾选配置动态端口蜜罐。

   - 服务器已开启旗舰版及以上版本主机安全防护。
   - 服务器Agent在线，且Windows Agent版本≥4.0.22，Linux Agent版本≥3.2.10。
   - 服务器未绑定动态端口蜜罐防护策略。
   - 服务器操作系统类型符合**步骤7.1**选择的类型。
   - 服务器未绑定EIP。

步骤8 在创建好的目标策略所在行的“关联服务器”列，单击数值，弹出“关联服务器”对话框。

步骤9 在关联服务器所在行的“端口启用情况”列，查看服务器端口启用情况。

端口启用失败后系统不会重新尝试启用端口，如果需要重新尝试启用端口，请通过“编辑策略”操作先去勾选服务器并保存，再通过“编辑策略”操作重新勾选绑定该服务器。编辑策略详细操作请参见**编辑策略**。

----结束

常见问题

端口启用失败怎么办?

- 可能原因一：端口被其他服务占用

  解决办法：通过“编辑策略”操作，添加其他空闲的端口。
- 可能原因二：系统资源不足

  解决办法：清理部分系统资源后，请通过“编辑策略”操作先去勾选服务器并保存，再通过“编辑策略”操作重新勾选绑定该服务器。编辑策略详细操作请参见**编辑策略**。

7.7.3 查看并处理蜜罐防护事件

操作场景

动态端口蜜罐默认主动连接蜜罐端口的主机都是内网失陷主机，一旦检测到可疑的连接行为将会上报蜜罐防护告警事件。蜜罐防护事件中会包含发起连接的主机IP，但不会提供具体的进程细节。您可以将蜜罐防护事件作为辅助线索，结合其他攻击防护事件进行综合分析，从而有效地排查和定位内网中潜在的失陷主机。

本章节介绍如何查看并处理蜜罐防护事件。

查看并处理蜜罐防护事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 在操作指引下方，查看防护信息概览。

- 您可以查看防护策略数量、防护服务器数量、防护事件数量等信息。
- 如果您有新增主机需要默认开启动态端口蜜罐功能时，可开启“新增主机自动绑定默认策略”，按钮状态为表示开启。

步骤6 选择“防护事件”页签，查看蜜罐防护事件。防护事件列表的参数说明请参见**表 防护事件列表参数说明**。

表 7-41 防护事件列表参数说明

参数名称	参数说明
告警名称	告警事件名称。单击告警名称，可查看告警详情，告警详情信息请参见**表 告警详情参数说明**。
告警等级	告警威胁等级，蜜罐防护事件分为以下两个等级： ● 高危：远端主机多次连接蜜罐端口。 ● 中危：远端主机连接了蜜罐端口。

参数名称	参数说明
告警摘要	告警事件关键信息摘要，您可以根据这些信息了解疑似失陷的主机和该主机与蜜罐端口建立的连接行为。
影响资产	疑似失陷主机连接的动态端口蜜罐服务器。
告警发生时间	告警发生的时间。
状态	告警处理状态，分为“已处理”和“待处理”。

步骤7 确认告警信息后，在“状态”为“待处理”的防护事件所在行的“操作”列，单击“处理”，弹出“处理告警事件”对话框。

如果您需要批量处理多个告警事件，可在告警事件列表左上角，单击“批量处理”。

步骤8 选择处理措施。处理措施说明请参见**表 处理告警事件参数说明**。

表 7-42 处理告警事件参数说明

参数名称	参数说明
处理方式	• **忽略**：忽略本次防护告警事件，当下一次威胁事件发生时仍为您告警。 • **手动处理**：您自行手动对失陷主机进行隔离端口等处理。 • **加入告警白名单**：触发告警事件的主机是您信任的主机，将该告警事件加入到告警白名单中，后续类似威胁事件发生时不再告警。
批量处理	如果您需要同时处理相同告警事件，可以勾选。
备注描述（可选）	为了方便后续易辨别本次处理操作的情况，可做补充描述。

步骤9 单击“确认”，完成处理。

----结束

告警详情参数说明

告警详情页的相关参数说明请参见**表 告警详情参数说明**。

表 7-43 告警详情参数说明

参数名称	参数说明
情报引擎	HSS采用的检测引擎，包括病毒检测引擎、AI检测引擎、恶意情报检测引擎。
攻击状态	当前威胁攻击服务器的状态。
首次告警发生时间	首次发生告警的时间。

参数名称	参数说明
告警ID	告警的唯一ID。
Att&CK阶段	攻击者在各阶段用到的攻击技术模型。
最新告警发生时间	最近一次发生告警的时间。
告警信息	告警的详细信息说明，包括告警说明、告警摘要、受影响资产和处置建议。
调查取证	动态端口蜜罐功能排查溯源定位到攻击源的网络取证信息。
相似告警	与本次告警事件相似的告警。您可以根据相似告警的处置方法处理本次告警。

筛选不同处理状态的防护事件

在防护事件列表左上方的状态下拉框中，选择目标处理状态的防护事件进行查看。

7.7.4 管理动态端口蜜罐防护策略

操作场景

动态端口蜜罐防护策略创建成功后，您可以根据自身的防护需求管理防护策略。

- **停用策略**：仅暂时关闭动态端口蜜罐功能。
- **启用策略**：将已停用的动态端口蜜罐功能重新启用。
- **编辑策略**：修改动态端口蜜罐防护策略信息，例如添加或删除蜜罐端口、解绑或绑定服务器。
- **删除策略**：删除动态端口蜜罐防护策略并停用动态端口蜜罐防护功能。

约束与限制

默认策略不支持删除。

停用策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标防护策略所在行的“操作”列，单击“停用策略”，弹出“停用策略”对话框。

步骤7 确认信息无误后，单击“确认”，完成停用。

----结束

启用策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标防护策略所在行的“操作”列，单击“启用策略”，弹出“启用策略”对话框。

步骤7 确认信息无误后，单击“确认”，完成启用。

----结束

编辑策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标防护策略所在行的“操作”列，单击“编辑策略”，弹出“编辑防护策略”对话框。

步骤7 配置策略。

可修改策略名称、防护端口、源IP白名单。

步骤8 单击“下一步”。

步骤9 选择绑定服务器。

步骤10 单击“确认”，完成编辑。

----结束

删除策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标防护策略所在行的“操作”列，单击“删除”，弹出“删除策略”对话框。

步骤7 确认信息无误后，单击“确认”，完成删除。

----结束

7.7.5 管理关联服务器

操作场景

针对单个防护策略关联的服务器，您可以为服务器**切换防护策略**或**解除策略绑定**。

切换防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标策略所在行的“关联服务器”列，单击数值，弹出“关联服务器”弹窗。

步骤7 在目标服务器所在行的操作列，单击“切换防护策略”，弹出“切换防护策略”对话框。

如需为多台服务器切换防护策略，您可以勾选所有目标服务器并单击列表左上角的“切换防护策略”。

步骤8 根据界面提示，选择防护策略。

步骤9 单击“确认”，完成切换。

----结束

解除策略绑定

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“主机防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在目标策略所在行的“关联服务器”列，单击数值，弹出“关联服务器”弹窗。

步骤7 在目标服务器所在行的操作列，单击“解除绑定”，弹出“解除绑定”对话框。

如需为多台服务器解除绑定，您可以勾选所有目标服务器并单击列表左上角的“解除绑定”。

步骤8 确认信息无误后，单击“确认”，解除绑定。

----结束

8 容器防御

8.1 容器防火墙

8.1.1 容器防火墙概述

什么是容器防火墙?

相较于传统虚拟机，容器技术以其轻量化、高效性和可移植性等优势逐渐成为主流。然而，由于在单一节点上可以运行几十甚至上百个容器，容器的安全边界相对模糊，传统的安全防护手段也难以有效识别和控制出入容器的流量，这也带来了横向渗透、权限滥用、数据泄露等潜在的安全风险。

针对这一挑战，企业主机安全推出了容器防火墙功能。容器防火墙能够实现Pod、工作负载以及节点粒度的网络隔离，可有效抵御横向渗透攻击，确保业务权限最小化，从而保障用户业务的安全性和稳定性。

容器防火墙原理及限制说明

容器防火墙功能由企业主机安全容器版提供。

关于容器防火墙的原理及相关限制说明请参见**表8-1**。

表 8-1 容器防火墙原理及限制说明

集群类型	CCE Standard集群		CCE Turbo集群	三方k8s集群
容器网络	**容器隧道网络**	**VPC网络**	**云原生网络2.0**	**k8s原生网络**
容器防火墙防护原理	通过Kubernetes内置的网络策略（Network Policy）限制Pod之间的通信，以及Pod对外部网络的访问。	通过安全组控制进出节点的流量，从而达到间接防护Pod安全的目的。	通过为工作负载绑定安全组，基于安全组规则控制出入工作负载的流量，实现对工作负载的网络隔离。	通过Kubernetes内置的网络策略（Network Policy）限制Pod之间的通信，以及Pod对外部网络的访问。
入规则支持的集群版本	所有版本	所有版本	v1.19及以上集群版本	所有版本
出规则支持的集群版本	v1.23及以上集群版本	所有版本	v1.19及以上集群版本	v1.23及以上集群版本
入规则支持的选择方式	• namespaceSelector • podSelector	不涉及	不涉及	• namespaceSelector • podSelector
出规则支持的选择方式	• namespaceSelector • podSelector • ipBlock	不涉及	不涉及	• namespaceSelector • podSelector • ipBlock
支持的操作系统	• EulerOS • CentOS • HCE 2.0	无约束	无约束	无约束
是否支持IPv6网络策略	不支持	不涉及	不涉及	不支持
是否支持通过工作负载的标签限制ClusterIP的访问	不支持	不涉及	不涉及	不支持
权限依赖	由于操作集群内的资源对象需要获取对应的操作权限，因此使用容器防火墙功能时，用户账号需要具备以下两类权限之一： • IAM权限：Tenant Administrator或CCE Administrator。 • 命名空间权限（Kubernetes RBAC授权）：运维权限。			无依赖

相关概念

- **网络策略**

  网络策略（NetworkPolicy）是一种Kubernetes资源对象，用于定义集群中Pod的网络访问控制规则。它通过标签选择器（podSelector等）指定目标Pod，并通过ingress和egress规则定义允许或拒绝的入站和出站流量。

- **安全组**

  安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组中包括入方向规则和出方向规则，您可以针对每条入方向规则指定来源、端口和协议，针对出方向规则指定目的地、端口和协议，用来控制安全组内实例入方向和出方向的网络流量。

- **namespaceSelector**

  namespaceSelector是一个标签选择器，用于选择特定的命名空间（namespace）。NetworkPolicy 可以通过namespaceSelector指定允许或拒绝来自或去往这些命名空间中所有Pod的流量。

- **podSelector**

  podSelector是一个标签选择器，用于选择特定的Pod。NetworkPolicy通过podSelector指定目标Pod，并定义允许或拒绝的流量规则。

- **ipBlock**

  ipBlock用于指定IP地址范围（CIDR格式），表示允许或拒绝来自或去往这些IP段的流量。

相关操作

- 设置网络防御策略（容器隧道网络）
- 设置网络防御策略（VPC网络）

8.1.2 设置网络防御策略（容器隧道网络）

操作场景

如果未为Pod设置网络防御策略，默认情况下允许所有流量进出Pod。这表示Pod之间可以自由通信，并且可以访问集群外部网络，存在潜在的安全风险。

本文为您介绍如何为容器隧道网络模型的集群设置网络防御策略，限制Pod之间的通信，以及Pod对集群外部网络的访问，从而提升集群的网络安全性。

约束与限制

- 当前容器防火墙功能仅支持对运行在EulerOS、CentOS、HCE 2.0节点上的Pod设置网络策略。
- CCE Standard集群1.23及以上版本支持入方向和出方向规则，CCE Standard集群1.23以下版本仅支持入方向规则。
- 不支持对IPv6地址的网络进行隔离。
- 不支持通过工作负载的标签限制ClusterIP的访问。

通过 YAML 创建网络策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“ > 容器防火墙”，进入“容器防火墙”页面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在集群列表上方，单击“手动同步”，同步所有集群已创建的策略。

同步任务大概执行1~2分钟，请您稍作等待后单击列表右上方，刷新查看最新数据。

步骤7 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8 单击策略列表上方“YAML创建”。

步骤9 在YAML创建界面输入或单击“导入”数据。

以下为通过YAML创建的网络策略示例：通过网络策略限制Pod只能被带有特定标签的Pod访问，且只能访问指定Pod

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: access-demo4
  namespace: default
spec:
  policyTypes:
  - Ingress
  - Egress
  podSelector:                # 规则对具有role=db标签的Pod生效
    matchLabels:
      role: db
  ingress:                    # 表示入规则
  - from:
    - podSelector:            # 只允许具有role=frontend标签的Pod访问
        matchLabels:
          role: frontend
    ports:                    # 只能使用TCP协议访问6379端口
    - protocol: TCP
      port: 6379
  egress:                     # 表示出规则
  - to:
    - podSelector:            # 只允许访问具有role=web标签的Pod
        matchLabels:
          role: web
```

步骤10 输入完成后，单击“确认”。

您可以在策略管理列表中查看新创建的策略。

----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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“ > 容器防火墙”，进入“容器防火墙”页面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在集群列表上方，单击“手动同步”，同步所有集群已创建的策略。

同步任务大概执行1~2分钟，请您稍作等待后单击列表右上方，刷新查看最新数据。

步骤7 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8 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：在下拉框中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。
- 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 8-2 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 8-3 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。

参数	参数说明
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9 设置完成后，单击“确定”。

您可以在策略管理列表中查看新创建的策略。

----结束

相关操作

修改或删除网络策略

步骤1 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤2 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3 单击网络策略列表上方“手动同步”。

同步任务大概执行1~2分钟，请您稍作等待后单击列表右上方，刷新查看最新数据。

步骤4 定位目标网络策略，选择需要执行的管理操作。

- 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

8.1.3 设置网络防御策略（VPC 网络）

操作场景

如果未为Pod设置网络防御策略，默认情况下允许所有流量进出Pod。这表示Pod之间可以自由通信，并且可以访问集群外部网络，存在潜在的安全风险。

本文为您介绍如何为VPC网络模型的集群设置网络防御策略，控制进出节点的流量，从而提升集群的网络安全性。

创建网络防御策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“ > 容器防火墙”，进入“容器防火墙”页面。

步骤5 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤6 在集群列表上方，单击“手动同步”，同步所有集群已创建的策略。

同步任务大概执行1~2分钟，请您稍作等待后单击列表右上方，刷新查看最新数据。

步骤7 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8 在目标节点所在行的“操作”列，单击“配置策略”。

步骤9 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10 选择“安全组”页签，查看安全组规则。

步骤11 单击安全组ID，系统自动跳转到安全组页面。

步骤12 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

相关操作

修改或删除网络防御策略

步骤1 （可选）如果您已开通企业项目，可在界面上方的“企业项目”下拉列表中选择目标主机所在的企业项目。

步骤2 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3 单击节点列表上方的“手动同步”，同步节点信息。

同步任务大概执行1~2分钟，请您稍作等待后单击列表右上方，刷新查看最新数据。

步骤4 在目标节点所在行的“操作”列，单击“配置策略”。

步骤5 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6 选择“安全组”页签，查看安全组规则。

步骤7 单击“配置规则”，系统自动跳转到安全组页面。

步骤8 选择相应规则页签，管理规则。

- 修改规则
  在目标规则所在行的“操作”列，单击“修改”，完成修改后，单击“确认”。
- 删除规则
  在目标规则所在行的“操作”列，单击“删除”，在弹出的对话框中，单击“确认”。

----结束

8.2 容器集群防护

8.2.1 容器集群防护概述

容器集群防护功能支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。

用户可根据自身业务场景灵活配置容器集群防护策略，加固集群安全防线，防止含有漏洞、恶意文件和不合规基线等安全威胁的镜像部署到集群，降低容器生产环境的安全风险。

约束与限制

- 容器集群须为云容器引擎（Cloud Container Engine，简称CCE）服务中申请的集群，且集群版本为1.20及以上版本。
- 容器集群防护功能仅企业主机安全容器版支持。

容器集群防护使用流程

图 8-1 使用流程图

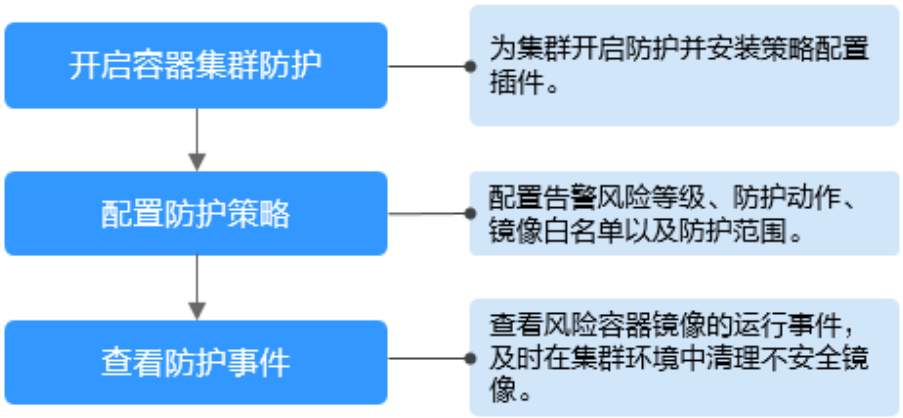


表 8-4 容器集群防护使用流程说明

操作项	描述
开启容器集群防护	为集群开启防护，保护业务和关键数据安全；开启防护时，HSS会自动在集群上安装策略管理插件。

操作项	描述
配置防护策略	根据自身业务情况，配置基线、漏洞和恶意文件触发告警的风险等级，容器集群防护范围，镜像白名单以及告警事件发生后HSS执行的防护动作。
查看防护事件	您可以在HSS控制台查看被告警或阻断的未授权或含高危安全风险的容器镜像运行事件，及时排查并清理不安全的容器镜像。

8.2.2 开启容器集群防护

容器集群防护可在容器镜像启动时检测其中存在的基线、漏洞和恶意文件风险，并支持告警和阻断不安全容器镜像的运行。您可以开启容器集群防护，提升容器集群的风险防御能力，保护容器资产安全。

约束限制

开启容器集群防护后，需要配置防护策略才能成功启动集群防护，配置防护策略操作请参见**配置容器集群防护策略**。

开启容器集群防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“ > 容器集群防护”，进入“容器集群防护”界面。

步骤5 选择“防护集群”页签。

步骤6 单击“手动同步”，同步实时集群数据。

步骤7 在目标集群所在行的操作列，单击“开启防护”，弹出“开启防护”页面。

您也可以勾选所有目标集群，并在集群列表左上方单击“开启防护”，批量为集群开启防护。

注意

- 开启容器集群防护时，会在集群上安装策略管理功能插件，插件会占用部分集群资源。
- 在开启容器集群防护过程中，请勿在该集群上执行任何操作，否则会导致开启防护失败。

步骤8 单击“确认”，开启防护。

容器集群“防护状态”显示“已启用，未配置”，表示已为集群完成相关防护配置且安装策略管理插件成功，但HSS还未开始防护您的集群，您需要配置防护策略，启动容器集群防护。配置防护策略操作请参见**配置容器集群防护策略**。

----结束

8.2.3 配置容器集群防护策略

您可以根据自身业务情况，配置容器集群防护策略，例如配置触发告警的风险（基线、漏洞、恶意文件）等级、容器集群防护范围、镜像白名单以及告警事件发生后HSS执行的防护动作等。

创建防护策略

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“ > 容器集群防护”，进入“容器集群防护”界面。

步骤5 选择“防护策略”页签，单击“创建策略”。

步骤6 在创建策略弹窗中，配置策略参数。相关参数说明请参见**表 配置容器集群防护策略参数说明**。

表 8-5 配置容器集群防护策略参数说明

参数名称	参数说明	取值样例
策略模板	选择策略生效模板，操作如下： 1. 单击“选择策略模板”，弹出选择策略模板对话框。 2. 选中任一策略模板，单击“确定”，选择成功。您可以根据策略说明，选择符合您需求的策略模板。 选择策略模板后，需要根据策略模板要求，填写一些策略参数值，您可以根据参数说明提示进行填写。	K8sPSPPrivilegedContainer
策略名称	自定义输入策略名称。名称只能由中文字符、英文字母、数字、逗号、句号、空格、下划线（_）和短横线（-）组成。	test
策略描述	自定义输入策略用途，做策略区分。描述只能由中文字符、英文字母、数字、逗号、句号、空格、下划线（_）和短横线（-）组成。	测试

参数名称	参数说明	取值样例
防护动作	选择当HSS发现集群中存在基线、漏洞或恶意脚本风险的镜像启动时的防护动作。 ● 告警：在“容器集群防护 > 防护事件”页面生成一个防护动作为“告警”的事件。 ● 阻断：阻断风险镜像运行，并在“容器集群防护 > 防护事件”页面生成一个防护动作为“阻断”的事件。 ● 放行：在“容器集群防护 > 防护事件”页面生成一个防护动作为“放行”的事件。	阻断
防护范围	选择集群的防护范围。 当选择镜像阻断策略时，需要额外设置镜像、标签防护范围。	-
加白名单（可选）	填写需要加入白名单的镜像名称。加入白名单的镜像启动时，HSS将不会进行安全检测。 填写格式为“镜像名称:镜像版本”，镜像名称只能包含数字、字母、下划线、中划线、点；多个镜像名称以换行符进行区分。 填写示例如下： ● 单个镜像 image:1.0 ● 多个镜像 image1:1.0 image2:1.0	-

步骤7 单击“创建”，完成策略创建。

您可以在防护策略列表中查看创建的防护策略。

----结束

编辑或删除集群防护策略

步骤1 进入“容器集群防护 > 防护策略”页签。

步骤2 在防护策略所在行的“操作”列，单击需要执行操作。

- 查看YAML：查看YAML格式的防护策略内容。
- 编辑：修改防护策略信息。
- 删除：删除不需要的防护策略。删除策略后，策略关联的容器集群将停止防护，请谨慎操作！

步骤3 单击“确认”，完成编辑或删除。

----结束

8.2.4 查看容器集群防护事件

HSS防护容器集群过程中发现的安全风险事件会展示在防护事件列表中，方便您了解容器集群中的安全风险。您可以参考本章节查看容器集群防护事件。

查看容器集群防护事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“ > 容器集群防护”，进入“容器集群防护”界面。

步骤5 选择“防护事件”页签，查看集群中发现的风险事件。

如需导出防护事件至本地查看，请在防护事件列表左上角，单击“导出”。

步骤6 单击告警名称，查看告警事件影响的资源详细信息。

----结束

8.2.5 关闭容器集群防护

如果您不再需要HSS对容器集群进行防护，您可以参考本章节关闭防护。

关闭容器集群防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“ > 容器集群防护”，进入“容器集群防护”界面。

步骤5 选择“防护集群”页签。

步骤6 在目标集群所在行的操作列，单击“关闭防护”。

您也可以勾选所有目标集群，并在集群列表左上方单击“关闭防护”，批量为集群关闭防护。

步骤7 在关闭防护弹窗中，确认是否勾选“关闭防护后删除集群的功能插件”。

- 勾选：删除容器集群防护策略和策略配置插件。如果后续需要重新开启防护，需要再次安装策略配置插件，配置防护策略。
- 不勾选：删除容器集群防护策略，不删除策略配置插件。如果后续需要重新开启防护，仅需配置防护策略。如果后续需要删除策略配置插件，请重复以上关闭防护步骤，并勾选删除插件。

步骤8 单击“确认”，关闭防护。

- 未勾选删除功能插件，关闭防护后，集群“防护状态”变更为“已启用，未配置”，表示关闭防护成功。

- 勾选了删除功能插件，关闭防护后，集群“防护状态”变更为“未防护”，表示关闭防护成功。

----结束

常见问题

当集群网络异常或插件正在工作时，通过HSS控制台卸载插件可能会失败，您可以参考**容器集群防护插件卸载失败怎么办？**。

9 检测与响应

9.1 主机安全告警

9.1.1 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。

说明

AV检测和HIPS检测的告警分类会按照具体的告警情况在不同的告警类型中呈现。

- AV检测告警结果只在恶意软件下的不同类别呈现。
- HIPS检测的告警结果会根据实际种类在所有类型的子类别中呈现。

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	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。	×	√	√	√	√	√
	病毒	检测服务器资产中存在的各种病毒，进行告警上报，支持对告警信息进行自动或手动隔离查杀。	×	√	√	√	√	√
	蠕虫	对服务器中入侵的蠕虫或已存在的蠕虫进行检测、查杀，并进行告警上报。	×	√	√	√	√	√
	木马	对服务器中入侵的木马或已存在的木马病毒进行检测、查杀，并进行告警上报。	×	√	√	√	√	√
	僵尸网络	对服务器中入侵的僵尸网络或已存在的僵尸网络进行检测、查杀，并进行告警上报。	×	√	√	√	√	√
	后门	检测服务器中存在的后门，并进行告警上报。	×	√	√	√	√	√
	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。	×	√	√	√	√	×

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	加入告警白名单	隔离查杀
	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。	×	×	√	√	√	√（部分支持）
	黑客工具	对服务器中入侵的黑客工具或已存在的黑客工具进行检测、查杀，并进行告警上报。	×	√	√	√	√	√
	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**。 隔离查杀：支持自动、手动隔离查杀。	×	×	√	√	√	×
	挖矿软件	对服务器中入侵的挖矿软件或已存在的挖矿软件进行检测、查杀，并进行告警上报。	×	√	√	√	√	√
漏洞利用	远程代码执行	实时检测利用漏洞入侵主机的行为，对发现的入侵行为进行告警上报。	×	√	√	√	√	×
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”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。	×	×	√	√	√	×

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	加入告警白名单	隔离查杀
	文件提权	检测当前系统对文件的提权操作并进行告警。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×（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。	×	√	√	√	√	×

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	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。	×	√	√	√	√	×
	敏感文件访问	检测未经授权访问或修改敏感文件的行为。	×	√	√	√	√	×
	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。	×	×	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	可疑进程运行	检测未经过认证或授权的应用进程运行，一旦发现进行告警上报。	×	√	√	√	√	×

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	加入告警白名单	隔离查杀
	可疑进程文件访问	检测未经过认证或授权的进程访问指定的目录，一旦发现进行告警上报。	×	√	√	√	√	×
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。默认拦截时间为12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。	√	√	√	√	√	×
	异常登录	检测“异地登录”和“账户暴力破解成功”等异常登录。如果发生异常登录，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”。 如果在非常用登录地登录，则触发安全事件告警。 ● 如果账户暴力破解成功，登录到云主机，则触发安全事件告警。	√	√	√	√	√	×

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	加入告警白名单	隔离查杀
	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；如果存在可疑账号、克隆账号等，则触发告警。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
网络异常访问	云蜜罐	检测到连接主机蜜罐端口的行为，进行告警上报。	×	×	√	√	√	×
	异常外联行为	检测到服务器存在异常外联可疑ip的行为，一旦发现进行告警上报。	×	√	√	√	√	×
	端口转发检测	检测到利用可疑工具进行端口转发行为，一旦发现进行告警上报。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
	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。	×	√	√	√	√	×
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。	×	×	√	√	×	×
	主机扫描	检测网络对主机规则覆盖ICMP ARP nbtscan的扫描活动，一旦发现立即上报告警。	×	×	√	√	√	×

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	加入告警白名单	隔离查杀
无文件攻击	进程注入	检测将恶意代码注入到正在运行的进程的行为，一旦发现立即告警上报。	×	√	√	√	√	×
	动态库注入进程	检测通过劫持动态链接库中的函数，从而实现白加黑注入代码的行为，一旦发现立即告警上报。	×	√	√	√	√	×
	内存文件进程	检测通过memfd_create的系统调用，创建一个只存在于RAM中的匿名恶意文件，从而执行恶意文件的行为，一旦发现立即告警上报。	×	√	√	√	√	×

安全告警等级说明

企业主机安全根据告警事件对业务系统的威胁程度，将告警划分为致命、高危、中危、低危四个等级，表9-1详细解释了各告警等级的含义。

表 9-1 安全告警等级说明

告警等级	说明
致命	致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。
高危	高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。
中危	中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。
低危	低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。

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

9.1.2 查看主机告警事件

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需紧急处理告警、告警总数、存在告警的服务器、已拦截IP和已隔离文件等。

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”。

说明

AV检测和HIPS检测的告警分类会按照具体的告警情况在不同的告警类型中呈现。

- AV检测告警结果只在恶意软件下的不同类别呈现。
- HIPS检测的告警结果会根据实际种类在所有类型的子类别中呈现。

约束与限制

- 如果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。

查看主机告警事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，单击“检测与响应 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 查看主机告警信息。

表 9-2 主机安全告警统计说明

参数名称	告警事件状态说明
企业项目	自定义选择企业项目，按照企业项目的维度查看告警详情。
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
需紧急处理告警	展示需紧急处理告警的数量。
告警总数	展示资产中存在的所有告警数量。
存在告警的服务器	展示存在告警的服务器数量。 当查看“最近24小时”存在告警情况时，您可以单击存在告警的服务器数值，跳转到“主机管理”界面查看相应的服务器列表。
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** • Linux 3.2.10及以上版本的Agent已全面支持IPv6的拦截功能；低于该版本的Agent，支持TCP Wrapper的拦截方式，暂无IPTables拦截IPv6地址功能。 • 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也不支持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**。

- **根据告警类型或ATT&CK攻击阶段查看告警列表**

  您可以在待处理告警栏，通过选择告警类型和ATT&CK攻击阶段，查看对应类型的告警事件列表。关于ATT&CK攻击阶段的含义请参见**表 ATT&CK攻击阶段说明**。

  说明

  ATT&CK的全称为Adversarial Tactics, Techniques, and Common Knowledge，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。

  表 9-3 ATT&CK 攻击阶段说明

ATT&CK攻击阶段	说明
侦查	攻击者尝试发现您的系统或网络中的漏洞。
初始访问	攻击者尝试进入您的系统或网络。
执行	攻击者尝试运行恶意代码。
持久化	攻击者尝试保持住它们入侵的进攻点。
权限提升	攻击者尝试获取更高等级的权限。
防御绕过	攻击者尝试避免被检测到。
凭据访问	攻击者尝试盗取账号名称和密码。

ATT&CK攻击阶段	说明
命令与控制	攻击者尝试与被攻击的机器通信并对其进行控制。
影响破坏	攻击者尝试操控，中断或者破坏您的系统或者数据。

- **查看主机安全告警事件详细信息**

  单击目标告警事件的告警名称，可查看告警的详细信息。告警信息说明如**表 告警详细信息参数说明**所示。

  说明

  - 对于部分HSS已确定为恶意软件的告警，HSS会将告警源文件保存在云端中心，支持下载。您可以将告警源文件下载到本地进行分析查看，告警源文件压缩包解压密码为“unlock”。
  - 对于未确认为恶意软件的告警，暂不支持告警源文件下载，您需要根据实际业务情况判断文件是否为恶意文件或误报。

  表 9-4 告警详细信息参数说明

参数名称	参数说明
防护引擎	HSS采用的检测引擎，包括病毒检测引擎、AI检测引擎、恶意情报检测引擎。
攻击状态	当前威胁攻击服务器的状态。
首次告警发生时间	首次发生攻击告警的时间。
告警ID	告警的唯一ID。
Att&CK阶段	攻击者在各阶段用到的攻击技术模型，详细说明请参见**表 ATT&CK攻击阶段说明**。
最新告警发生时间	最新发生攻击告警的时间。
告警信息	告警的详细信息说明，包括告警说明、告警摘要、受影响资产和处置建议。

参数名称	参数说明
调查取证	HSS根据告警类型调查到的攻击触发路径或病毒类型等信息，帮助您快速排查溯源定位处理攻击源。 - 进程树：当告警事件含进程信息时，调查取证栏目会展示进程树。进程树信息包含进程ID、进程文件路径、进程命令行、进程启动时间、进程文件hash等信息，您可以根据这些进程信息定位恶意进程。 - 文件取证信息：当告警事件含文件信息时，调查取证栏目会展示文件取证信息。文件取证信息包含文件路径、文件hash等，您可以根据这些信息定位文件。 - 网络取证信息：当告警事件含网络相关信息时，调查取证栏目会展示网络取证信息。网络取证信息包含本地IP地址、本地端口、远程IP地址、远程端口以及协议等，您可以根据这些信息判断是否为非法用户行为。 - 用户取证信息：当告警事件含用户行为信息时，调查取证栏目会展示用户取证信息。用户取证信息包含用户名称、用户登录IP、登录的服务类型、登录服务端口、最后一次登录事件以及登录失败次数等，您可以根据这些信息判断是否为非法访问行为。 - 注册表取证信息：当告警事件含注册表信息时，调查取证栏目会展示注册表取证信息。注册表取证信息包含注册表KEY、注册表VALUE等，您可以根据这些信息定位注册表风险。 - 异常登录取证信息：当告警事件含异常登录信息时，调查取证栏目会展示异常登录取证信息。异常登录取证信息包含登录IP、端口等，您可以根据这些信息定位是否为可信登录。 - 恶意软件取证信息：当告警事件含软件信息时，调查取证栏目会展示恶意软件取证信息。恶意软件取证信息包含恶意软件家族、病毒名称、病毒类型、置信度等信息。您可以根据这些信息定位恶意软件。 - 自启动项取证信息：当告警事件含自启动项信息时，调查取证栏目会展示自启动项取证信息。自启动项取证信息包含用户、命令、自启动项信息、进程文件命令行等信息。您可以根据这些信息定位自启动项。 - 内核取证信息：当告警事件含内核信息时，调查取证栏目会展示内核取证信息。内核取证信息包含系统函数、内核函数等信息。您可以根据这些信息定位内核风险。
相似告警	与本次告警的主机和事件类型相同的告警。您可以根据相似告警的处置方法处理本次告警。

----结束

9.1.3 处理主机告警事件

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需紧急处理告警、告警总数、存在告警的服务器、已拦截IP和已隔离文件等。

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”。

说明

AV检测和HIPS检测的告警分类会按照具体的告警情况在不同的告警类型中呈现。

- AV检测告警结果只在恶意软件下的不同类别呈现。
- HIPS检测的告警结果会根据实际种类在所有类型的子类别中呈现。

约束与限制

- 如果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。

处理主机告警事件

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

说明

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

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，单击“检测与响应 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击告警名称，查看告警信息和处理建议。

步骤7 处理告警事件。

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”。

- 处理单个告警事件

  在目标告警事件所在行的操作列，单击“处置”。
- 批量处理告警事件

  勾选所有目标告警事件，并在告警事件列表上方单击“批量处理”。

- 全量处理告警事件

  在告警列表左侧的“待处理告警”栏，选择一类告警类型，并在告警事件列表上方单击“全量处理”。

步骤8 在“处理告警事件”弹窗中，选择处理方式。处理方式说明请参见**表 告警事件处理方式说明**。

处理单个告警事件或批量处理告警事件时，可在“处理告警事件”弹窗中勾选“同时处理重复告警”，将重复告警一并处理。

表 9-5 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。如果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，如果隔离查杀有误报，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。
加入进程白名单	如果确认是可信进程的运行触发告警事件，您不希望HSS再上报该告警，您可以将应用进程告警事件加入进程白名单。
加入登录告警白名单	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告警白名单。 HSS不会对登录告警白名单内的登录事件上报告警。加入登录告警白名单后，如果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告警白名单。 ● 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，如果再次出现该告警事件，则HSS不会告警。 选中“加入告警白名单”后，可单击“新增规则”，自定义设置白名单规则；可定义的规则类型因告警类型而不同，包括文件路径、进程路径、进程命令行、远程IP和用户名。当HSS检测到的告警事件相等或包含您填写的规则信息时，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**。

步骤9 单击“确认”，完成处理。

告警事件处理完成后，您可以查看已处理的告警记录，详细操作请参见**历史处置记录**。

----结束

取消处理主机告警事件

对于处理完成的告警事件，支持取消处理。

步骤1 在告警事件列表，筛选“已处理”的告警。

步骤2 在目标告警事件所在行的“操作”列，单击“处理”。

步骤3 在“处理告警事件”弹窗中，单击“确认”，取消上次处理。

----结束

9.1.4 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。

导出主机告警事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“检测与响应 > 安全告警事件”，进入“安全告警事件”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“主机安全告警”页签。

步骤7 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

步骤8 在安全告警事件界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的告警事件信息。

须知

导出过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

9.1.5 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或删除。

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，单击“检测与响应 > 安全告警事件 > 主机安全告警”，进入“主机安全告警”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 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”上方的数值，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

恢复已隔离文件

如果您需要将已隔离文件解除隔离，您可以执行恢复操作。恢复后，文件将拥有隔离前的权限，请谨慎操作。

步骤1 单击文件隔离箱列表中“操作”列的“恢复”，弹出“恢复已隔离文件”对话框。

步骤2 单击“确认”，恢复的文件将重新回到告警事件列表中。

----结束

删除已隔离文件

如果您需要将已隔离文件彻底删除，您可以执行删除操作。

步骤1 单击文件隔离箱列表中“操作”列的“删除”，弹出“删除已隔离文件”对话框。

如需批量删除已隔离文件，您可以勾选多个目标已隔离文件，并单击已隔离文件列表左上角的“删除”。

步骤2 单击“确认”，完成删除。

----结束

9.2 容器安全告警

9.2.1 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。

容器安全告警介绍

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。
	黑客工具	检测利用漏洞或者黑客工具的恶意行为，一旦发现进行告警上报。
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

事件类型	告警名称	原理说明
	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。
系统异常行为	反弹Shell	实时监控用户的进程行为，并支持告警和阻断进程的非法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检测和自动化阻断，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。 您也可以在“策略管理”的“HIPS检测”策略中配置自动化阻断反弹Shell行为。
	文件提权	检测利用SUID、SGID程序漏洞进行root提权的行为，一旦发现进行告警上报。
	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。
	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。
	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。HSS实时监控容器进程，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。

事件类型	告警名称	原理说明
	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Kubernetes 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。

事件类型	告警名称	原理说明
		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。 **说明** 需**安装Docker插件**。
	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。

事件类型	告警名称	原理说明
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；如果存在可疑账号、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。
	用户密码窃取	检测到通过非法手段获取用户密钥行为，一旦发现进行告警上报。
网络异常访问	异常外联行为	检测到服务器存在异常外联可疑ip的行为，一旦发现进行告警上报。
	端口转发检测	检测到利用可疑工具进行端口转发行为，一旦发现进行告警上报。
集群异常行为	Pod异常行为	检测集群中存在创建特权pod、静态pod及敏感配置pod的异常行为，以及对现存pod执行的异常操作，一旦发现进行告警上报。
	枚举用户信息	检测存在枚举集群用户的权限以及可执行操作列表的行为，一旦发现进行告警上报。
	绑定集群用户角色	检测绑定、创建高权限集群角色或Service Account的行为，一旦发现进行告警上报。
	Kubernetes事件删除	检测集群中删除Kubernetes事件的行为，一旦发现进行告警上报。

安全告警等级说明

企业主机安全根据告警事件对业务系统的威胁程度，将告警划分为致命、高危、中危、低危四个等级，表9-6详细解释了各告警等级的含义。

表 9-6 安全告警等级说明

告警等级	说明
致命	致命级别的告警表示系统已经受到严重的攻击，可能导致数据丢失、系统崩溃或者长时间的服务中断。例如，发现勒索加密行为或恶意程序感染。建议您立即处理，避免对系统造成更严重的损害。

告警等级	说明
高危	高危级别的告警表示系统可能正在受到攻击，但尚未造成严重的损害。例如，检测到未授权的登录尝试或执行了危险命令（如删除关键系统文件或修改系统设置的命令）。建议您及时调查并采取措施，以防止攻击蔓延。
中危	中危级别的告警表示系统存在潜在的安全威胁，但目前没有明显遭受攻击的迹象。例如，检测到文件或目录的异常修改，表明系统可能存在潜在的攻击路径或配置错误。建议您进一步分析并采取适当的防范措施，以确保系统的安全。
低危	低危级别的告警表示系统存在轻微的安全威胁，不会对系统的正常运行产生显著影响。例如，检测到一些端口扫描行为，这些行为通常是攻击者尝试寻找系统漏洞的前奏。这类告警可以在合适的时间进行处理，不需要立即采取紧急措施。如果您的资产安全等级要求较高，可以关注该等级的安全告警。

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

9.2.2 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需紧急处理告警、告警总数、存在告警的容器、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。

查看容器告警事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中选择“检测与响应 > 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。

表 9-7 容器安全告警统计说明

参数名称	参数说明
需紧急处理的告警	展示需紧急处理的告警数量，单击数值可查看对应的告警事件。
告警总数	展示资产中存在告警事件的总数，单击数值可查看全部告警事件。
存在告警的容器	展示存在告警的容器数量。
已处理告警事件	展示已经处理完成的告警事件数量。

- **根据告警类型或ATT&CK攻击阶段查看告警列表**

  在“待处理告警”栏，选择告警类型或ATT&CK攻击阶段，查看同类告警列表。关于ATT&CK攻击阶段的含义请参见表 ATT&CK攻击阶段说明。

  说明

  ATT&CK的全称为Adversarial Tactics, Techniques, and Common Knowledge，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。

  表 9-8 ATT&CK 攻击阶段说明

ATT&CK攻击阶段	说明
侦查	攻击者尝试发现您的系统或网络中的漏洞。
初始访问	攻击者尝试进入您的系统或网络。
执行	攻击者尝试运行恶意代码。
持久化	攻击者尝试保持住它们入侵的进攻点。
权限提升	攻击者尝试获取更高等级的权限。

ATT&CK攻击阶段	说明
防御绕过	攻击者尝试避免被检测到。
凭据访问	攻击者尝试盗取账号名称和密码。
命令与控制	攻击者尝试与被攻击的机器通信并对其进行控制。
影响破坏	攻击者尝试操控，中断或者破坏您的系统或者数据。

- **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，可查看告警说明及处置建议、HSS调查取证发现的告警路径/地址、相似告警处置记录等。告警信息说明如**表 告警详细信息参数说明**所示。

  说明

  对于部分HSS已确定为恶意软件的告警，HSS会将告警源文件保存在云端中心，支持下载。您可以将告警源文件下载到本地进行分析查看，告警源文件压缩包解压密码为“unlock”。

  对于未确认为恶意软件的告警，暂不支持告警源文件下载，您需要根据实际业务情况判断文件是否为恶意文件或误报。

  表 9-9 告警详细信息参数说明

参数名称	参数说明
情报引擎	HSS采用的检测引擎，包括病毒检测引擎、AI检测引擎、恶意情报检测引擎。
攻击状态	当前威胁攻击服务器的状态。
首次告警发生时间	首次发生攻击告警的时间。
告警ID	告警的唯一ID。
Att&CK阶段	攻击者在各阶段用到的攻击技术模型，详细说明请参见**表 ATT&CK攻击阶段说明**。
最新告警发生时间	最新发生攻击告警的时间。
告警信息	告警的详细信息说明，包括告警说明、告警摘要、受影响资产和处置建议。

参数名称	参数说明
调查取证	HSS根据告警类型调查到的攻击触发路径或病毒类型等信息，帮助您快速排查溯源定位处理攻击源。 - 进程树：当告警事件含进程信息时，调查取证栏目会展示进程树。进程树信息包含进程ID、进程文件路径、进程命令行、进程启动时间、进程文件hash等信息，您可以根据这些进程信息定位恶意进程。 - 文件取证信息：当告警事件含文件信息时，调查取证栏目会展示文件取证信息。文件取证信息包含文件路径、文件hash等，您可以根据这些信息定位文件变更。 - 网络取证信息：当告警事件含网络相关信息时，调查取证栏目会展示网络取证信息。网络取证信息包含本地IP地址、本地端口、远程IP地址、远程端口以及协议等，您可以根据这些信息判断是否为非法用户行为。 - 用户取证信息：当告警事件含用户行为信息时，调查取证栏目会展示用户取证信息。用户取证信息包含用户名称、用户登录IP、登录的服务类型、登录服务端口、最后一次登录事件以及登录失败次数等，您可以根据这些信息判断是否为非法访问行为。 - 注册表取证信息：当告警事件含注册表信息时，调查取证栏目会展示注册表取证信息。注册表取证信息包含注册表KEY、注册表VALUE等，您可以根据这些信息定位注册表风险。 - 异常登录取证信息：当告警事件含异常登录信息时，调查取证栏目会展示异常登录取证信息。异常登录取证信息包含登录IP、端口等，您可以根据这些信息定位是否为可信登录。 - 恶意软件取证信息：当告警事件含软件信息时，调查取证栏目会展示恶意软件取证信息。恶意软件取证信息包含恶意软件家族、病毒名称、病毒类型、置信度等信息。您可以根据这些信息定位恶意软件。 - 自启动项取证信息：当告警事件含自启动项信息时，调查取证栏目会展示自启动项取证信息。自启动项取证信息包含用户、命令、自启动项信息、进程文件命令行等信息。您可以根据这些信息定位自启动项。 - 内核取证信息：当告警事件含内核信息时，调查取证栏目会展示内核取证信息。内核取证信息包含系统函数、内核函数等信息。您可以根据这些信息定位内核风险。 - 容器取证信息：当告警事件含容器信息时，调查取证栏目会展示容器取证信息。容器取证信息包含容器名称、镜像ID等信息。您可以根据这些信息定位容器风险。
相似告警	与本次告警的主机和事件类型相同的告警。您可以根据相似告警的处置方法处理本次告警。

- **查看容器告警事件Pod详情。**

单击目标告警事件的Pod名称，进入Pod详情页面，可以查看节点IP、命名空间、Pod IP、Pod标签、容器列表等信息。

----结束

9.2.3 处理容器告警事件

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。

处理容器告警事件

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

说明

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

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，单击“检测与响应 > 安全告警事件 > 容器安全告警”，进入“容器安全告警”页面。

步骤5 单击告警名称，查看告警信息和处理建议。

步骤6 处理告警事件。

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”。

- 处理单个告警事件

  在目标告警事件所在行的操作列，单击“处置”。
- 批量处理告警事件

  勾选所有目标告警事件，并在告警事件列表上方单击“批量处理”。
- 全量处理告警事件

  在告警列表左侧的“待处理告警”栏，选择一类告警类型，并在告警事件列表上方单击“全量处理”。

步骤7 在“处理告警事件”弹窗中，选择处理方式。处理方式说明请参见**表 告警事件处理方式说明**。

处理单个告警事件或批量处理告警事件时，可在“处理告警事件”弹窗中勾选“同时处理重复告警”，将重复告警一并处理。

表 9-10 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。如果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。
加入登录告警白名单	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告警白名单。 HSS不会对登录告警白名单内的登录事件上报告警。加入登录告警白名单后，如果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告警白名单。 • 暴力破解 • 异常登录
加入进程白名单	如果确认是可信进程的运行触发告警事件，您不希望HSS再上报该告警，您可以将应用进程告警事件加入进程白名单。
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，如果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**容器安全告警事件概述**。

步骤8 单击“确认”，完成处理。

告警事件处理完成后，您可以查看已处理的告警，详细操作请参见**历史处置记录**。

----结束

取消处理容器告警事件

对于处理完成的告警事件，支持取消处理。

步骤1 在告警事件列表，筛选“已处理”的告警。

步骤2 在目标告警事件所在行的“操作”列，单击“处理”。

步骤3 在“处理告警事件”弹窗中，单击“确认”，取消上次处理。

----结束

9.2.4 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。

导出容器告警事件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“检测与响应 > 安全告警事件”，进入“安全告警事件”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“容器安全告警”页签。

步骤7 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

如果您只需要导出某一类告警或某个ATT&CK攻击阶段的告警，您可以在待处理告警栏，选中相应的告警事件类型或ATT&CK攻击阶段，再单击“导出”。

步骤8 在安全告警事件界面上方查看导出状态，待导出成功后，在主机本地默认下载文件地址，获取导出的告警事件信息。

导出过程中，请勿关闭浏览器页面，否则会导致导出任务中断。

----结束

9.3 白名单管理

9.3.1 管理登录告警白名单

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告警白名单添加，添加后HSS对白名单内IP、用户名的登录、访问行为进行忽略不再告警。

您可以通过以下两种方式添加登录告警白名单：

- 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告警白名单，详细信息请参见**查看主机告警事件**。
- 在“登录告警白名单”页面，添加登录告警白名单。

约束与限制

- 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进行忽略不再告警，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**。
- 如果要解除登录拦截，请在“登录安全检测”策略的白名单内添加IP，详细操作请参见**登录安全检测**。

添加登录告警白名单

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“检测与响应 > 白名单管理 > 登录告警白名单”，进入“登录告警白名单”页面，单击“添加”。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在“添加登录告警白名单”页面中，输入“服务器IP”、“登录IP”和“登录用户名”。

表 9-11 登录告警白名单参数说明

参数名称	参数说明	取值样例
服务器IP	目标服务器的IP地址或IP掩码。 • IP地址：例如192.168.1.1或16A0::1 • IP掩码：例如192.168.7.0/24或16A0:10:AB00:1E::/64	192.168.1.1
登录IP		
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
同时处理历史相关告警	勾选后，对于已经生成的登录告警同步进行处理。	勾选

步骤7 单击“确认”，完成登录告警白名单的添加。

----结束

删除登录告警白名单

如果需要删除已添加的登录告警白名单，勾选待删除的登录告警白名单，单击“删除”，或者在待删除服务器IP地址“操作”列单击“删除”，删除登录告警白名单。

9.3.2 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。

添加告警白名单

表 9-12 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

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“检测与响应 > 白名单管理”，进入“白名单管理”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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 告警白名单列表参数说明**所示。

表 9-13 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。
加白字段	加白的目标文件字段。
通配符	加白的规则用到的逻辑，相等或包含。
描述	目标白名单的说明。
加白的规则	加白规则ID。
标记时间	目标告警添加白名单的时间。
企业项目	所属目标企业项目。
今日触发次数	今日符合白名单条件的告警事件触发次数。
累计触发次数	累计符合白名单条件的告警事件触发次数。默认不展示。

----结束

删除告警白名单

如果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，如果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“检测与响应 > 安全告警事件”页面，在告警事件所在行的操作列单击“处理”，选择“删除告警白名单”。

9.3.3 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。

添加系统用户白名单

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“检测与响应 > 白名单管理”，进入“白名单管理”页面。

步骤5 （可选）在白名单管理页面左上方，“企业项目”选择主机所属的企业项目或“所有项目”。

如果您没有开通企业项目，可跳过此步骤。

步骤6 选择“系统用户白名单”页签，单击“添加”。

步骤7 在“添加系统用户白名单”页面中填写主机ID、系统用户名以及备注信息。

步骤8 单击“确认”，添加完成。

----结束

修改系统用户白名单

步骤1 （可选）在白名单管理页面左上方，“企业项目”选择主机所属的企业项目或“所有项目”。

如果您没有开通企业项目，可跳过此步骤。

步骤2 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3 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 （可选）在白名单管理页面左上方，“企业项目”选择主机所属的企业项目或“所有项目”。

如果您没有开通企业项目，可跳过此步骤。

步骤2 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3 在弹出的窗口，单击“确认”。

----结束

10 安全运营

10.1 策略管理

10.1.1 策略管理概述

什么是策略组?

企业主机安全提供了多个版本，包括基础版、企业版、旗舰版、网页防篡改版和容器版；除了基础版外，企业主机安全其他每个防护版本都有对应的默认防护策略组；策略组是多个策略的集合，这些策略应用于主机上，用于集中管理和配置企业主机安全检测和防护主机的灵敏度、规则、范围等。

企业主机安全旗舰版、容器版支持创建自定义策略组，如果您有多台旗舰版或容器版主机，但防护需求不同时，可以创建自定义策略组为不同主机部署不同的防护策略组，详细操作请参见**创建自定义策略组**。

策略组包含哪些策略?

企业主机安全每个版本提供的策略略有不同，具体如**表10-1**所示，如果您在使用企业主机安全过程中，对资产管理、基线检查、入侵检测等检测策略有定制化需求，可以根据业务需求自定义配置策略。具体操作请参见**配置策略**。

表 10-1 策略列表

功能类型	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
资产管理	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	×	√	√	√

功能类型	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
基线检查	弱口令检测	检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改。	Linux，Windows	√	√	√	√
	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	×	×	×	√
	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	×	√	√	√
入侵检测	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“检测与响应 > 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。	Linux，Windows	√	√	√	×
	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	×	×	×	√
	容器信息模块	用户可以基于容器的名称、镜像所属组织的名称以及命名空间自定义配置可信容器白名单，白名单内容器不进行检测及告警。	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	√	√	√	√

功能类型	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
	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	×	×	×	√
	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	×	×	×	√
	无文件攻击检测	对检测用户资产中存在的进程注入、动态库注入和内存文件进程行为的管控。	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。	Linux、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、Windows	√	√	√	√
	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	√	√	√	√

功能类型	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
	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	×	√	√	√
	进程异常行为	通过对运行进程的管控，全局监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	√	√	√	√

功能类型	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
自保护	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	×	√	√	×

10.1.2 配置策略

操作场景

主机开启防护后，您可以根据自身业务需求配置主机防护策略。

约束限制

- 已开启企业版、旗舰版、网页防篡改版、容器版中任一版本。
- 默认策略组有默认配置，不建议修改。
- 策略内容的修改只在策略所属策略组内生效。

进入策略管理

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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 策略组列表字段说明**所示。

表 10-2 策略组列表字段说明

字段	说明
策略组名称	策略组的名称。系统预置策略组名称如下： • 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。
ID	策略组的ID号，对策略组的唯一标识。
描述	策略组的详细描述。
支持的版本	策略组支持的企业主机安全版本。
支持的操作系统	策略组支持的操作系统类型。
关联服务器数	策略组关联的服务器数。单击数值，可查看策略组关联的服务器。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

- 选择“所有项目”时，策略更改将应用于所有企业项目下的主机。
- 选择特定的企业项目时，策略更改仅影响该企业项目的主机。

步骤6 单击目标策略组名称，进入策略详情列表。

步骤7 在目标策略所在行的“操作”列，可单击“开启”或“关闭”策略。

策略关闭后，企业主机安全将不再执行对应策略的检测。

步骤8 单击目标策略名称对不同策略进行修改，各策略说明如下所示。

----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10-3所示。

表 10-3 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。 偏移时间指在设置的目标时间向后做自动调节执行检测。 • 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。 • 中间件/Web框架：可一起选择检测日和时间。 • 内核模块：需根据需求独立设置检测日和时间。 • Web应用/Web站点/Web服务/数据库：可一起选择检测日和时间。
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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，如果密码被破解，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10-4所示。

表 10-4 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。
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。
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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 10-5 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。

----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检测功能会扫描Web站点路径和您指定的扫描路径。

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10-6**所示。

表 10-6 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	执行Webshell检测的Web目录，系统已默认配置部分Web目录，您也可以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。 **请勿将网络目录添加为扫描目录**，即使添加了HSS也不会进行扫描，主要原因如下： • 检测效率低 网络目录通常包含大量文件，总容量可能达到上百TB，这将显著降低检测效率。 • 占用网络带宽 访问网络目录时需要占用网络带宽，大规模检测可能导致带宽被完全占满，进而影响到您正常业务的运行，包括但不限于网络速度变慢、网络延迟增加等。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-7所示。

如下图片以Linux策略为例。

表 10-7 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。

参数	说明
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。
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。 • 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。 – 文件或目录路径：需要监控的文件或目录路径。添加前，请确认是合法路径；最多可添加50个文件或目录路径。 – 别名：文件或目录路径的别名，您可以定义一个易区分的名称。 – 监控子目录：勾选后会监控对应子目录的所有文件。不勾选，则不监控子目录文件。 – 监视创建、删除、移动、修改等：请您根据业务实际情况选择是否勾选。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

HIPS 检测

步骤1 单击“HIPS检测”，弹出“HIPS检测”策略详情页面。

步骤2 修改策略内容，相关参数说明如**表 HIPS检测策略内容参数说明**所示。

表 10-8 HIPS 检测策略内容参数说明

参数名称	参数说明
自动化阻断	开启后，对检测到的注册表、文件及进程等异常变更行为进行阻断，例如反弹Shell、高危命令等。 • ：开启。 • ：关闭。
可信进程	添加可信进程的文件路径。单击“添加”可增加一条路径输入框，单击“删除”可删除进程文件路径。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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**表 登录安全检测策略内容参数说明**所示。

表 10-9 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”。
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。

参数	说明
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-10所示。

表 10-10 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。
忽略的反弹shell本地端口	无需扫描反弹shell的本地端口。
忽略的反弹shell远程地址	无需扫描反弹shell的远程地址。
反弹shell检测	
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。
异常shell检测	• 选择是否开启异常shell检测。开启后，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，建议开启。 – ：开启。 – ：关闭。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-11**所示。

表 10-11 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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-12**所示。

表 10-12 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。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-13所示。

表 10-13 实时进程策略内容参数说明

参数	说明
高危命令	检测包含关键词的高危命令。命令输入只能包含字母、数字、下划线、空格和符号（ /*\=>. : ' " +- ）。 暂不支持检测Shell内置命令。
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；同时可填写需要加白的命令行的正则表达式，命令行正则表达式非必填。 示例： • 进程全路径或程序名：/usr/bin/sleep • 命令行正则表达式：^[A-Za-z0-9[:space:]*\\.\\\":_'\\(>=-]+$

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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 10-14 rootkit 检测策略内容参数说明

参数名称	参数说明	取值样例
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-15所示。

表 10-15 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。 • 自动处置：检出的高危病毒文件默认自动隔离，其余病毒文件仅上报病毒事件，不自动隔离。 • 人工处置：检出的所有病毒文件仅上报病毒事件，不自动隔离。	自动处置

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-16所示。

表 10-16 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。 白名单比黑名单优先级更高，如果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。	/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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-17所示。

表 10-17 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	根据您具体的业务需求选择检测项，相关介绍如下： ● **高权限RoleBinding**：检测高权限角色绑定行为。角色绑定（RoleBinding）用于将账户与角色绑定，黑客可以通过将普通账户绑定到高权限角色来实现权限获取。 ● **高权限ClusterRoleBinding**：检测高权限集群角色绑定行为。集群角色绑定（ClusterRoleBinding）用于将账户与集群角色绑定，黑客可以通过将普通账户绑定到高权限角色来实现权限获取。 ● **ServiceAccount创建**：检测创建服务账号的行为。服务账户（ServiceAccount）是Kubernetes的重要凭证，黑客可通过创建服务账户并将其绑定到高权限角色，达到控制集群的目的。 ● **List Secrets操作**：检测List Secrets操作。Kubernetes Secret是一种允许用户在集群中存储和管理敏感信息（如密码和连接字符串）的对象。List Secrets可在Pod配置中通过引用使用。有权限从API服务器检索机密的攻击者（例如，通过使用Pod的服务账户）可以访问敏感信息，其中可能包括各种服务的凭证。 ● **创建DaemonSet**：检测创建DaemonSet的行为。攻击者可能试图通过创建新容器在集群中运行其代码，守护进程集（DaemonSet）是控制Kubernetes中所有节点的最佳方式。 ● **创建Cronjob**：检测创建Cronjob的行为。Kubernetes Job可用于运行执行批处理任务的容器，这些任务通常是有限的。 ● **Pod中exec使用交互式shell**：检测Pod中exec使用交互式shell的行为。黑客可能利用交互式bash、sh这类shell程序在容器内部开展操作。 ● **创建特权Pod**：检测创建特权Pod的行为。创建特权容器以实现容器逃逸是黑客最常用的逃逸技术之一。 ● **创建敏感目录Pod**：检测创建敏感目录Pod的行为。黑客可能通过创建敏感的主机挂载来实现权限提升，例如挂载/、/root、/etc等目录。 ● **创建主机网络Pod**：检测创建主机网络Pod的行为。黑客可能创建使用主机网络的容器以实现逃逸或监听流量。 ● **创建主机pid空间Pod**：检测创建主机pid空间Pod的行为。黑客可能创建使用主机PID命名空间的容器以实现逃逸。 ● **无权限访问Apiserver**：检测无权限访问Apiserver的行为。黑客攻击可能会发送API请求来探测集	全选。

参数名称	参数说明	取值样例
	群，并获取有关集群中容器、机密和其他资源的信息，而这些探测行为通常会触发针对未授权访问API服务器的警报。 ● **使用curl访问APIServer**：检测使用curl访问APIServer的行为。一般来说，容器内不太可能存在kubectl等工具，使用curl入侵Pod进行API服务器探测是最常见的方式之一。 ● **系统管理空间执行exec**：检测是否存在针对kube-apiserver等管理组件的exec命令。 ● **Ingress漏洞**：检测Ingress漏洞。能够创建或更新Ingress对象的用户可利用自定义片段功能获取集群中的所有机密。 ● **Ingress-alias**：检测Ingress-alias。具备创建或更新Ingress对象权限的用户，可利用Ingress对象（位于networking.k8s.io 或extensions API组）中的spec.rules[].http.paths[].path字段，获取ingress-nginx控制器的凭证。在默认配置下，该凭证有权访问集群中的所有机密信息。 ● **SelfSubjectRulesReview场景**：检测查询SelfSubjectRulesReview的行为。当黑客进入一个Pod时，需要确认该Pod所持有的服务账户（SA）权限，或确认通过该Pod窃取的令牌权限。 ● **系统管理空间创建Pod**：检测在系统管理空间创建Pod的操作。通常情况下，K8s集群稳定后，kube-system命名空间下的资源不会被随意创建或删除，而攻击者往往会伪造管理组件以实现持久化操作。 ● **静态Pod创建**：检测创建静态Pod的操作。黑客会利用静态Pod来达到某种目的，因为静态Pod无法通过API服务器删除。 ● **中间人攻击**：检测中间人攻击（MITM 攻击）中危漏洞（CVE-2020-8554）。 ● **蠕虫挖矿木马**：检测使用常见的蠕虫、挖坑、木马镜像创建pod。 ● **K8s事件删除**：检测删除Kubernetes事件的操作。Kubernetes事件有助于识别集群中已发生的变更。因此，攻击者可能希望删除这些事件（例如，通过使用kubectl delete events --all命令），以避免其在集群中的活动被检测到。	

参数名称	参数说明	取值样例
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	类型：ip过滤 值： 192.168.x.x

步骤3 确认无误，单击“确认”，完成修改。

- 如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。
- 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。

----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 10-18 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，多个镜像名以回车换行隔开，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全路径，进程全路径只能包含字母、数字、下划线、中划线，多个进程名以回车换行隔开，最多可添加100个进程路径。
POD名称白名单	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名以回车换行隔开，最多可添加100个POD名。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

容器信息模块

步骤1 单击“容器信息模块”，弹出“容器信息模块”策略详情页面。

步骤2 根据界面提示，修改策略内容。策略内容相关参数说明请参见**表 容器信息模块策略参数说明**。

表 10-19 容器信息模块策略参数说明

参数名称	参数说明
自定义容器名称白名单	自定义填写需要入侵检测功能忽略不进行检测的容器名称。 • 基于Docker运行时的容器可以配置简单名称，HSS会自行模糊匹配；其他运行时的容器会根据名称进行精确匹配。 • 多个容器名称以回车换行分隔，最多可添加100个白名单。
自定义组织白名单	自定义填写需要入侵检测功能忽略不进行检测的镜像所属组织名称。 多个组织名称以回车换行分隔，最多可添加100个白名单。

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

容器文件监控

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10-20**所示。

表 10-20 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。
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-21所示。

表 10-21 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
动态白名单	开启动态白名单后，企业主机安全默认容器是单进程模式，即容器只运行容器启动参数中配置的进程命令行。当容器启动时，企业主机安全会自动识别容器启动的entrypoint配置，以此来确定主进程，如果容器运行过程，运行了主进程外的其他进程则会触发告警。	
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。	sha256:732aab547cfe56841c02fb83921db4b91f04a1e636cc2cad76e224897056f140
进程	执行检测的目标镜像下的进程全路径。	/tmp/testw

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-22所示。

表 10-22 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。	-
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10-23。	-

表 10-23 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。

权限名称	权限说明
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）。
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。

权限名称	权限说明
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。
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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10-24**所示。

表 10-24 端口扫描检测策略参数说明

参数名称	参数说明	取值样例
扫描源IP白名单	输入IP或IP范围，多个IP或IP范围用英文逗号分隔。 例如，192.168.0.1,192.168.0.2,192.168.10-192.168.100。	192.168.0.1
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。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

无文件攻击检测

步骤1 单击“无文件攻击检测”，弹出“无文件攻击检测”策略详情界面。

步骤2 在策略详情界面中，查看或修改“策略内容”，参数说明如表所示。

表 10-25 无文件攻击检测策略参数说明

参数名称	参数说明	取值样例
进程注入	• **进程注入**：开启/关闭进程注入检测。 – ：开启。 – ：关闭。 • **白名单匹配规则**：即您配置好的“路径白名单”匹配规则，单击选择白名单匹配规则，可选项如下： – 全量匹配，区分大小写 – 全量匹配，不区分大小写 – 模糊匹配 • **路径白名单**：输入无需对“进程注入”威胁进行检测的路径，多个路径可通过回车换行分隔。	• • 模糊匹配 • /usr/sbin/hald

参数名称	参数说明	取值样例
LD劫持	• **LD劫持**：开启/关闭LD劫持检测。 – ：开启。 – ：关闭。 • **全量进程检测**：开启/关闭对全量进程的LD劫持威胁检测。 – ：开启。 – ：关闭。 • **白名单匹配规则**：即您配置好的“路径白名单”匹配规则，单击选择白名单匹配规则，可选项如下： – 全量匹配，区分大小写 – 全量匹配，不区分大小写 – 模糊匹配 • **路径白名单**：输入无需对“LD劫持”威胁进行检测的路径，多个路径可通过回车换行分隔。	• • • 模糊匹配 • /usr/sbin/hald
内存型进程	• 内存型进程：开启/关闭内存型进程检测。 – ：开启。 – ：关闭。 • **全量进程检测**：开启/关闭对全量进程的内存型进程威胁检测。 – ：开启。 – ：关闭。 • **白名单匹配规则**：即您配置好的“路径白名单”匹配规则，单击选择白名单匹配规则，可选项如下： – 全量匹配，区分大小写 – 全量匹配，不区分大小写 – 模糊匹配 • **路径白名单**：输入无需对“内存型进程”威胁进行检测的路径，多个路径可通过回车换行分隔。	• • • 模糊匹配 • /usr/sbin/hald

步骤3 确认无误，单击“确认”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----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。

10.1.3 创建自定义策略组

操作场景

对于旗舰版、容器版策略组，支持通过复制的方式创建自定义策略组，您可以部署自定义策略组替换默认策略组，以匹配不用应用场景的主机安全需求。

创建自定义策略组

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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 策略组列表字段说明**所示。

表 10-26 策略组列表字段说明

字段	说明
策略组名称	策略组的名称。系统预置策略组名称如下： • 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。
ID	策略组的ID号，对策略组的唯一标识。

字段	说明
描述	策略组的详细描述。
支持的版本	策略组支持的企业主机安全版本。
支持的操作系统	策略组支持的操作系统类型。
关联服务器数	策略组关联的服务器数。单击数值，可查看策略组关联的服务器。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择旗舰版或容器版策略组，单击策略组“操作”列的“复制”。

步骤7 在弹出的对话框中，输入“策略组名称”和“描述”。

- 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8 单击“确认”，创建一个新的策略组。

策略组创建完成后，您可以配置策略组中各个策略的生效规则。详细操作请参见**配置策略**。

----结束

后续操作

完成策略组创建和策略配置后，您可以将新建的策略组部署应用到主机，详细操作请参见**部署防护策略**。

10.1.4 删除自定义策略组

操作场景

系统预置的策略组不支持删除，您可以删除自定义创建的旗舰版、容器版策略组。

操作须知

如果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”。您需要重新参考**部署防护策略**为主机部署策略组。

删除策略组

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 单击目标策略组“操作”列的“删除”。

您也可以勾选多个策略，并单击策略列表左上方的“删除”，批量删除多个策略组。

步骤6 单击“确认”，完成删除。

----结束

10.2 历史处置记录

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

查看历史处置记录

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 选择需要查看的记录类型，查看相应的历史处置记录。

- 查看指定企业项目的历史处置记录

  在历史处置记录页面左上角，选择指定的企业项目，可查看该企业项目下服务器的历史处置记录。

- 查看指定属性的历史处置记录

  在列表上方搜索框中，通过选择属性筛选或输入关键词搜索，查看指定属性的事件处置记录。

----结束

10.3 容器审计

10.3.1 容器审计概述

什么是容器审计?

容器审计功能支持对容器集群中的各种操作和活动进行监控和记录，可帮助用户洞察容器生命周期的各个阶段，包括创建、启动、停止和销毁等，以及容器之间的网络通信和数据传输情况。用户通过审计和分析，可以及时发现并处理安全问题，从而确保容器集群的安全性、稳定性。

支持审计的类型

- 集群容器：K8s审计日志、K8s事件、容器日志、容器运行指令。

- 非集群容器：容器日志、容器运行指令。
- SWR镜像仓：镜像仓日志。

应用场景

容器环境异常事件排查分析：当容器环境出现异常操作或活动时，可通过容器审计日志定位异常事件发生时间和行动轨迹，从而总结出解决办法。

约束与限制

集群容器或非集群容器已开启容器版防护。

使用说明

完全启用容器审计功能，需满足以下条件：

1. 集群容器或非集群容器已接入HSS并开启容器版防护。
   接入容器资产操作请参见**为容器安装Agent**，开启防护操作请参见**开启容器版防护**。
2. 完成部分审计类型的审计前提操作，具体如**表 审计前提说明**所示。

表 10-27 审计前提说明

对象	审计类型	审计前提
云CCE集群	K8s审计日志	在CCE管理控制台开启“kubernetes事件”、“kubernetes审计日志”、“容器日志”采集。
	K8s审计事件	
	容器日志	
SWR私有镜像仓库	镜像仓日志审计	您使用了容器镜像服务SWR，并授予了HSS云审计服务的操作权限（CTSOperatePolicy），授权操作请参见**授权管理**。

启用容器审计后，集群内的各类操作和活动日志将记录在HSS控制台，供您查看，查看审计日志的详细操作请参见**查看容器审计日志**。

10.3.2 查看容器审计日志

操作场景

本章节为您介绍如何查看容器审计日志。

查看容器审计日志

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 容器审计”，进入“容器审计”页面。

步骤5 根据以下操作查看不同类型的审计日志。

- 查看集群容器审计
  a. 选择“集群容器审计”页签。
  b. 单击目标集群名称，进入集群容器审计详情页面，查看容器运行指令的日志记录。
- 查看容器实例审计
  a. 选择“容器实例审计”页签。
  b. 单击目标容器实例名称，进入容器实例审计详情页面，查看容器日志、容器运行指令的日志记录。
- 查看镜像仓日志审计
  选择镜像仓日志审计页签，查看镜像仓日志审计的记录。

----结束

10.4 安全报告

10.4.1 安全报告概述

企业主机安全提供安全报告，支持以日报、周报、月报或自定义周期报告的形式，统计并展示用户已防护主机的安全趋势和关键事件、风险。

约束与限制

- 安全报告功能仅企业主机安全专业版、企业版、旗舰版、网页防篡改版、容器版支持。
- 安全报告生成后将保存6个月。

安全报告使用说明

HSS默认预置了周报和月报，您的资产开启防护后，默认报告会自动生成，报告内容和生成时间如下：

- 报告内容：
  - 安全总览：风险趋势 、风险分布、TOP5风险主机、TOP5暴力破解攻击来源。
  - 风险预防：漏洞统计、资产账号变动记录、危险开放端口、弱口令。
  - 入侵检测：风险账号、异地登录、恶意程序、网站后门、账号破解、关键文件变更。
- 报告生成时间：
  - 默认周报（default weekly security report）：每周一06:00~12:00，生成统计周期为每周一00:00~周日24:00的安全报告。
  - 默认月报（default monthly security report）：每周一06:00~12:00，生成统计周期为每月1号00:00~月度最后一天24:00的安全报告。

报告生成后，您可以查看安全报告，详细操作请参见**查看安全报告**。

如果默认预置的报告，不满足您的需求，您可以自定义创建新的报告或编辑默认报告，详细操作请参见**创建安全报告**、**编辑安全报告**。

10.4.2 创建安全报告

如果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，您可通过本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。

创建安全报告

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 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5 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6 对报告基本信息进行配置，参数说明如**表10-28**所示。

表 10-28 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

参数名称	参数说明	取值样例
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
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
报告logo	选择报告使用的logo。 • 不需要：报告无logo。 • 默认logo：默认云logo。 • 自定义：自定义上传logo图片。图片格式仅支持jpg、png、jpeg、bmp，且图片大小不得超过20KB。	不需要

步骤7 确认信息无误，单击页面右下角“下一步”，配置报告内容。

步骤8 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

10.4.3 查看安全报告

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

本章节为您介绍如何查看这些生成的报告。

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。

安全报告概览

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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10-29所示。

表 10-29 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

10.4.4 管理安全报告

如果需对已订阅的报告内容进行修改、取消或关闭订阅，请参考本章节操作。

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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 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5 单击目标报告的“编辑”按钮，对报告进行编辑。

步骤6 对报告基本信息进行编辑，参数说明如表10-30所示。

表 10-30 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
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7 确认信息无误，单击页面右下角“下一步”，编辑报告内容。

步骤8 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

开启/关闭订阅

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 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5 单击目标报告右上角的按钮，开启或关闭订阅。

- ：表示关闭订阅，报告将停止生成。
- ：表示开启订阅，报告将按时生成。

----结束

删除报告

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。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 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5 单击目标报告的“删除”，对目标报告进行删除。

----结束

10.5 免费体检

HSS对未开启防护的主机提供免费扫描体检，针对频繁出现的漏洞、口令、资产风险生成安全报告供查看。

- 主机免费体检

  检测ECS服务器中存在的漏洞、口令、资产风险并生成报告。

  如果有漏洞管理、基线检查、应用防护、网页防篡改、勒索防护、入侵检测、文件完整性检测、病毒查杀等检测或防护需求，您可开启专业版及以上版本防护。
- 容器免费体检

  检测CCE集群中存在的镜像漏洞、集群配置、特权容器风险和端口、软件信息，并生成报告。

  如果有资产管理、镜像安全扫描、容器防火墙、容器集群防护等防护需求，您可开启容器版防护。

免费体检说明

- 针对未开启防护的ECS服务器，HSS每月提供一次全量的免费安全体检，自动执行扫描检测时间为每月1号凌晨5点（以主机所处时区为准）。

- 主机免费体检报告中单一体检项仅支持展示总结果数的一半，且最多支持展示5条体检结果。
- 免费体检的报告每月1日生成，生成后仅支持线上查看，不支持下载。

查看主机免费体检

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 安全报告”，进入安全报告页面。

步骤5 选择“免费体检 > 主机免费体检”页签，查看未开启防护服务器的体检结果。

步骤6 单击目标服务器“操作”列“查看报告”，可在线查看目标服务器的体检详情。

----结束

查看容器免费体检

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安全运营 > 安全报告”，进入安全报告页面。

步骤5 选择“免费体检 > 容器免费体检”页签，查看未开启防护集群容器的体检结果。

步骤6 单击目标集群“操作”列“查看报告”，可在线查看目标集群的体检详情。

----结束

11 安装与配置

11.1 主机安装与配置

11.1.1 Agent 管理

11.1.1.1 Agent 概述

什么是 Agent?

Agent是企业主机安全提供的一款软件，安装在云服务器上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机和容器的安全检测和防护。如果不安装Agent，将无法使用企业主机安全。

Agent每日凌晨定时执行安全检测任务，全量扫描主机或容器，实时监测主机或容器的安全状态，并将收集的主机或容器信息（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；此外Agent也会根据您配置的安全策略，阻止攻击者对主机或容器的攻击行为。

Agent 支持的操作系统

Agent目前支持部分主流的操作系统，具体请参见**操作系统限制**。对于Agent不支持的操作系统，与Agent可能存在兼容性问题，建议为主机安装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 运行时的进程

- **Linux主机**

  Agent运行账号为“root”，运行时包含的进程如**表 Linux主机Agent运行进程**所示。

表 11-1 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主机**

  Agent运行账号为“system”，运行时包含的进程如**表 Windows主机Agent运行进程**所示。

表 11-2 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

11.1.1.2 安装主机 Agent

操作场景

Agent是企业主机安全提供的一款软件，安装在主机上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机的安全检测和防护。安装Agent后，您才能使用企业主机安全服务。

步骤一：安装前环境准备

步骤1 请确认服务器的操作系统在Agent**操作系统限制**列表内。

不在该列表中的操作系统不支持安装Agent。

步骤2 请确认服务器为正常运行状态。

非运行状态无法安装Agent。

步骤3 请确认预备安装Agent的磁盘容量大于300MB。

不足300MB会导致Agent安装失败。Agent安装路径不支持选择，默认如下：

- Linux：/usr/local/hostguard/
- Windows：C:\Program Files\HostGuard

步骤4 请确认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）。

该端口用于与HSS服务端通信。查看、修改安全组出方向规则的操作请参见。

步骤5 请卸载第三方安全软件。

第三方安全软件与主机安全agent存在不兼容的情况，会影响主机安全的防护功能，如果服务器安装了第三方安全软件，请先卸载它们再安装主机安全Agent。

步骤6 （可选）Linux主机，请关闭SElinux防火墙。

SElinux防火墙可能会导致Agent安装失败，您可以在Agent安装成功之后再打开。

----结束

步骤二：安装主机 Agent

企业主机安全支持防护云主机、第三方主机，对应主机的Agent安装操作请参见：

- **为云平台主机安装Agent**
- **线下IDC通过专线和代理服务器接入HSS**
- **通过CBH安装HSS的Agent**

修改安全组

安装Agent时，需要确保服务器安全组出方向允许访问100.125.0.0/16网段的10180端口。您可以参考本节查看、修改ECS安全组规则。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在管理控制台左上角，单击，选择“计算 > 弹性云服务器 ECS”，进入“弹性云服务器”页面。

步骤4 在弹性云服务器列表中，单击目标ECS名称。

步骤5 在ECS服务器详情页面，选择“安全组”页签，单击展开目标安全组信息，单击安全组ID，进入安全组页面。

步骤6 选择“出方向规则”页签，按如**表 安全组规则**所示添加规则。

表 11-3 安全组规则

协议	端口范围或ICMP类型	类型	目的地址	描述
TCP	10180	IPv4	• IP地址 • 100.125.0.0/16	与HSS服务端进行通信。

----结束

11.1.1.3 升级主机 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。

Agent 升级说明

- 升级Agent操作为免费，不收取任何费用。
- 升级过程中不影响您在云服务器上业务的正常使用。
- 建议在业务空闲时进行升级操作，避免升级Agent版本导致Agent异常，无法对您的主机进行防护等情况。

Agent 手动升级

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 主机安装与配置”，进入“Agent管理”页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 选择“已安装主机”页签，筛选待升级Agent的服务器。

步骤7 在目标服务器的“操作”列，单击“升级Agent”。

您也可以批量选中目标服务器，在服务器列表左上方单击“批量升级Agent”，批量为服务器升级Agent。

步骤8 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9 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

Agent 自动升级

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 主机安装与配置”，进入Agent管理页面。

步骤5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 单击，开启Agent自动升级。

开启后，HSS会于每日的00:00～06:00检测您资产中待升级的Agent并自动升级Agent为最新版。只有Agent状态为“在线”时，才能执行自动升级。

----结束

11.1.1.4 卸载主机 Agent

如果不再需要企业主机安全为您的服务器提供防护，您可以参照本文卸载Agent，Agent卸载后企业主机安全将停止对服务器的检测和防护。

卸载方式说明

Agent提供如下两种卸载方式：

- 一键卸载：通过企业主机安全控制台的卸载功能一键卸载，具体操作请参见**在企业主机安全控制台一键卸载Agent**。
- 手动卸载：在主机本地手动卸载，具体操作请参见**在主机本地手动卸载Agent**。

建议您优先选择一键卸载的方式卸载Agent，该方式操作简单高效。如果在控制台上发现Agent状态为“离线”，无法执行卸载操作时，您可以选择手动卸载的方式来卸载Agent。

在企业主机安全控制台一键卸载 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 主机安装与配置 > Agent管理”，进入Agent管理页面。

步骤5 选择“已安装主机”页签，筛选Agent在线的服务器。

步骤6 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”，开始卸载。

您也可以勾选需卸载Agent的目标服务器，并单击列表上方的“批量卸载Agent”，批量为服务器卸载Agent。

步骤7 等待5~10分钟左右，选择“未安装主机”页签，查找到目标服务器，目标服务器的Agent状态为“未安装”表示卸载Agent成功。

----结束

在主机本地手动卸载 Agent

- **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，并执行如下命令切换到**root**用户。

     su - root

  b. 在任意目录执行如下命令，卸载Agent。

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。

- 针对EulerOS、CentOS、Red Hat等支持rpm安装软件的OS，执行命令：**rpm -e hostguard**
- 针对Ubuntu、Debian等支持deb安装软件的OS，执行命令：**dpkg -P hostguard**

当界面回显如下类似信息，则表示卸载Agent完成，无需再执行下一步，等待15分钟左右企业主机安全控制台上服务器的Agent状态会更新为“未安装”或“离线”。如果卸载失败请执行**c**。

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

c. （可选）当执行**b**卸载Agent失败时，可参考如下方式卸载Agent。

- 针对EulerOS、CentOS、Red Hat等支持rpm安装软件的OS。
  1) 执行如下命令，删除安装记录。
     rpm -e --justdb hostguard
  2) 执行如下命令，查询是否有hostguard残留进程。
     ps -ef | grep hostguard
     如果有残留，请执行命令**kill -9“进程pid”**停止所有残留进程。
  3) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。
     ll /usr/local/hostguard
     如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。
  4) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。
     ll /etc/init.d/hostguard
     如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。
- 针对Ubuntu、Debian等支持deb安装软件的OS。
  1) 执行如下命令，查询是否有hostguard残留进程。
     ps -ef | grep hostguard
     如果有残留，请执行命令**kill -9“进程pid”**停止所有残留进程。
  2) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。
     ll /usr/local/hostguard
     如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。
  3) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。
     ll /etc/init.d/hostguard
     如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。

- **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C:\Program Files\HostGuard目录下，双击“unins000.exe”，启动卸载程序。
- 如果安装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卸载向导”提示框中，单击“是”，开始卸载。

d. （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。

11.1.2 安全配置

11.1.2.1 配置常用登录地

操作场景

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。

配置常用登录地

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“安装与配置 > 主机安装与配置 > 安全配置 > 常用登录地”，单击“添加常用地登录”。

步骤5 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6 返回“常用登录地”页面查看新增的常用登录地，查看到新增的常用登录地表示添加成功。

----结束

11.1.2.2 配置常用登录 IP

操作场景

常用登录IP指的是您经常用来登录主机使用的设备所对应的IP地址。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。

配置常用登录 IP

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“安装与配置 > 主机安装与配置 > 安全配置 > 常用登录IP”，单击“添加常用登录IP”。

步骤5 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，确认无误单击“确认”，添加操作完成。相关参数说明请参见表11-4。

表 11-4 添加常用登录 IP 参数说明

参数名称	参数说明
常用登录IP	请输入IP地址或网段。要求如下： ● 单次只能添加一个IP或网段，若需添加多个，请重复执行添加操作。 例如： – IP：192.78.10.3或fe80::1。 – 网段：192.78.10.0/255.255.255.0、192.78.10.0/24或者fe80::1:0/112。 ● 最多支持添加20个登录IP。
常用登录IP配置生效的服务器	勾选常用登录IP所生效的服务器。可同时选择多个服务器。

步骤6 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

11.1.2.3 配置 SSH 登录 IP 白名单

操作场景

SSH登录IP白名单功能是防止账户遭受暴力破解攻击的重要措施，主要作用是限制能够通过SSH登录服务器的IP地址。配置了SSH登录IP白名单的服务器，企业主机安全仅允许白名单内的IP地址通过SSH登录服务器，而白名单外的IP地址将被禁止登录。

约束限制

- 单一账号最多可添加10个SSH登录IP白名单。
- 如果您的服务器无需通过SSH登录，则无需配置SSH登录IP白名单。
- 配置SSH登录IP白名单时，请确保所有要通过SSH登录服务器的IP地址都加入到白名单。

- 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。

配置 SSH 登录 IP 白名单

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“安装与配置 > 主机安装与配置 > 安全配置 > SSH登录IP白名单”，单击“添加白名单IP”。

步骤5 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，确认无误单击“确认”，添加操作完成。相关参数说明请参见**表11-5**。

表 11-5 添加 SSH 登录 IP 白名单参数说明

参数名称	参数说明
白名单IP	请输入IP地址或网段。要求如下： • 单次只能添加一个IP或网段，若需添加多个，请重复执行添加操作。 例如： – IP：192.78.10.3或fe80::1。 – 网段：192.78.10.0/255.255.255.0、192.78.10.0/24或者fe80::1:0/112。 • 最多支持添加10个白名单IP。
常用白名单IP配置生效的服务器	勾选SSH登录IP白名单所生效的服务器。可同时选择多个服务器。

步骤6 返回“SSH登录IP白名单”页面查看新增的白名单IP，查看到新增的白名单IP表示配置成功。

----结束

11.1.2.4 开启恶意程序隔离查杀

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

说明

您可以在HSS控制台选择“检测与响应 > 安全告警事件”，进入安全告警事件页面，单击恶意程序告警名称，进入“恶意程序”告警详情页查看恶意程序置信度。

开启恶意程序隔离查杀

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“安装与配置 > 主机安装与配置 > 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，如果需正常使用，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5 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“检测与响应 > 安全告警事件”页面中，单击“文件隔离箱”页签，查看被隔离的恶意程序。在此您可以对指定的恶意程序执行取消隔离、忽略等操作，详情请参见**查看主机告警事件**。

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，如果隔离查杀有误报，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“检测与响应”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

11.1.3 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

- 主机已开启防护。具体操作请参见**开启防护**。
- 开启双因子认证需要关闭SElinux防火墙。
- 在Windows主机上，双因子认证功能可能会和“网防G01”软件、服务器版360安全卫士存在冲突，建议停止“网防G01”软件和服务器版360安全卫士。

约束与限制

- 开启双因子认证后，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。
- Windows云服务器使用双因子认证功能时，不支持使用Windows系统的“用户每次登录时须更改密码”功能，如果您需要正常使用该功能，须关闭双因子认证。

开启双因子认证

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“安装与配置 > 主机安装与配置 > 双因子认证”，进入“双因子认证”页面。

步骤5 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6 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。
  - 如果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。如果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。

步骤7 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。

当通过开启了双因子认证功能的Windows主机远程登录其他Windows主机时，需要在开启双因子认证的Windows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。

添加凭证操作：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

11.2 容器安装与配置

11.2.1 集群管理

11.2.1.1 修改集群 Agent 安装信息

操作场景

如遇下列情况您可以修改接入信息：

- 需要修改安装Agent的集群节点范围。修改后，所有集群节点上的Agent会自动卸载并重新安装。
- 需要修改容器运行时类型、sock地址。修改后，所有集群节点上的Agent会自动卸载并重新安装。

- 需要启/停Agent自动升级。

修改接入信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“集群”页签。

步骤6 在目标集群所在行的“操作”列，单击“编辑接入信息”，弹出“编辑接入信息”对话框。

步骤7 修改接入信息。可修改的参数说明请参见**表 修改接入信息参数说明**。

表 11-6 修改接入信息参数说明

参数名称	参数说明
配置规则	选择Agent配置规则。 • 默认规则：容器运行时的sock地址为通用地址，Agent将默认安装在没有配置污点的节点上。 • 自定义规则：如果您的容器运行时sock地址非通用地址需要修改，或仅需要在指定的节点上安装Agent，可选择该规则。 **说明** • 如果容器运行时的sock地址不正确，可能导致集群接入HSS后，部分HSS功能不能正常使用。 • 在进行容器运行时配置时，建议全选所有运行时类型。
高级配置（可选）	配置规则选择“自定义规则”时，支持配置。 单击展开所有高级配置项。 • 开启Agent自动升级 是否开启Agent自动升级，勾选即开启，开启后，每日00:00～06:00，企业主机安全将自动升级低版本的Agent为最新版，以便为您提供更好的服务。 • 节点选择器配置 选择需要安装Agent的节点标签。不选择，默认在所有没有配置污点的节点上安装Agent。 • 容忍度配置 如果在进行“节点选择器配置”时，选择了污点节点标签，需要在该污点节点上安装Agent，可选择容忍节点污点。

步骤8 单击“完成”，完成修改。

如果您修改了容器运行时类型、容器运行时sock地址、节点选择配置、容忍度配置等，所有集群节点上的Agent会自动卸载并重新安装，请您耐心等待Agent安装完成。

----结束

11.2.1.2 升级或卸载集群 Agent

操作场景

本章节为您介绍如何为集群升级、卸载Agent。

前提条件

目标集群状态为“运行中”。

升级集群 Agent

企业主机安全会定期迭代版本，优化升级服务能力，因此建议您及时将Agent升级为最新版。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“集群”页签。

步骤6 在目标CCE集群所在行的“操作”列，单击“升级Agent”。

如需批量升级，请先勾选所有目标CCE集群，并单击“批量升级Agent”。

步骤7 确认待升级相关信息后，单击“确认”，开始升级。

等待5~10分钟后，在集群列表查看Agent为最新版，且升级Agent按钮置灰，表示升级成功。

----结束

卸载集群 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“集群”页签。

步骤6 在目标集群所在行的“操作”列，单击“卸载集群”。

CCE集群如需批量卸载，请先勾选所有目标集群，并单击“批量卸载Agent”。其他类型集群不支持批量卸载。

步骤7 确认待卸载相关信息后，单击“确认”，开始卸载。

等待5~10分钟后，在集群列表中查看无该集群，表示卸载Agent成功。

----结束

11.2.1.3 查看集群节点列表和权限列表

操作场景

本章节为您介绍如何查看集群节点列表、权限列表。

查看集群节点列表和权限列表

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“集群”页签。

步骤6 单击“同步接入状态”，刷新集群接入状态。

步骤7 单击“同步最新资产”，同步最新资产信息。

步骤8 查看集群接入情况。

如需导出集群列表，可在列表上方单击“导出”。

步骤9 单击目标集群名称，进入集群节点详情页面，查看节点和权限列表。

- 节点列表

  节点列表展示了所有节点的信息以及Agent状态和版本。

- 权限列表

  权限列表展示了企业主机安全提供的容器相关功能特性，该集群是否有权限使用。CCE集群不涉及权限列表。

----结束

11.2.2 非集群节点管理

11.2.2.1 安装非集群节点 Agent

操作场景

Agent是企业主机安全提供的一款软件，安装在主机上，用于与企业主机安全的云端防护中心进行数据交互，实现对主机的安全检测和防护。安装Agent后，您才能使用企业主机安全服务。

前提条件

待安装Agent的节点所在VPC内已有至少一个Agent在线的节点。否则请参考**为主机安装Agent**中提供的命令行安装方式安装Agent。

步骤一：安装前环境准备

步骤1 请确认服务器的操作系统在Agent**操作系统限制**列表内。

不在该列表中的操作系统不支持安装Agent。

步骤2 请确认服务器为正常运行状态。

非运行状态无法安装Agent。

步骤3 请确认预备安装Agent的磁盘容量大于300MB。

不足300MB会导致Agent安装失败。Agent安装路径不支持选择，默认如下：

- Linux：/usr/local/hostguard/
- Windows：C:\Program Files\HostGuard

步骤4 请确认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）。

该端口用于与HSS服务端通信。查看、修改安全组出方向规则的操作请参见。

步骤5 请卸载第三方安全软件。

第三方安全软件与主机安全agent存在不兼容的情况，会影响主机安全的防护功能，如果服务器安装了第三方安全软件，请先卸载它们再安装主机安全Agent。

步骤6 （可选）Linux主机，请关闭SElinux防火墙。

SElinux防火墙可能会导致Agent安装失败，您可以在Agent安装成功之后再打开。

----结束

步骤二：安装非集群节点 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“非集群节点”页签。

步骤6 找到Agent状态为“未安装”的节点，单击“操作”列的“安装Agent”。

步骤7 在安装Agent页面，选择服务器验证模式。

- **账号密码方式**
  - 勾选“允许以root权限直连”

    表示服务器可以通过root账号直接登录，您填写服务器root密码、服务器登录端口后，HSS将通过您的root账号为主机安装Agent。
  - 不勾选“允许以root权限直连”

    表示服务器不能通过root账号直接登录，您填写其他可以登录主机的账号信息（其中root密码用于提权），HSS将通过您提供的账号信息为主机安装Agent。
- **密钥方式**

  仅支持自建密钥。单击“上传密钥”，上传后缀为.pem的自建密钥文件。

步骤8 确认信息无误后，单击“确定”，Agent开始安装。

您可以查看“Agent状态”列，确认Agent安装状态。Agent状态显示“在线”，表示安装完成。

----结束

后续操作

为非集群节点安装Agent成功后，请为其**开启防护**。

修改安全组

安装Agent时，需要确保服务器安全组出方向允许访问100.125.0.0/16网段的10180端口。您可以参考本节查看、修改ECS安全组规则。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在管理控制台左上角，单击，选择“计算 > 弹性云服务器 ECS”，进入“弹性云服务器”页面。

步骤4 在弹性云服务器列表中，单击目标ECS名称。

步骤5 在ECS服务器详情页面，选择“安全组”页签，单击展开目标安全组信息，单击安全组ID，进入安全组页面。

步骤6 选择“出方向规则”页签，按如**表 安全组规则**所示添加规则。

表 11-7 安全组规则

协议	端口范围或ICMP类型	类型	目的地址	描述
TCP	10180	IPv4	• IP地址 • 100.125.0.0/16	与HSS服务端进行通信。

----结束

11.2.2.2 升级或卸载非集群节点 Agent

操作场景

本章节为您介绍如何为非集群节点升级、卸载Agent。

前提条件

目标节点的Agent状态为“在线”。

升级非集群节点的 Agent

企业主机安全会定期迭代版本，优化升级服务能力，因此建议您及时将Agent升级为最新版。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击 图标，选择区域或项目。

步骤3 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“非集群节点”页签。

步骤6 通过以下方式升级Agent。

- 自动升级

  节点列表右上角Agent自动升级处，单击 开启自动升级。开启后，每日00:00～06:00，企业主机安全将自动升级所有Agent为最新版。您可以在次日06:00后，查看节点的Agent版本确认是否升级成功。

- 手动升级

  a. 在目标节点所在行的操作列单击“升级Agent”。

  如需批量升级，请先勾选所有目标节点，并单击“批量升级”。

  b. 确认待升级相关信息后，单击“确认”，开始升级。

  等待5~10分钟后，查看到目标节点的Agent版本为最新版，表示升级成功。

----结束

卸载非集群节点的 Agent

如果您不再需要使用企业主机安全可参考本节卸载Agent。本节介绍Agent状态为在线的卸载方式，如果Agent状态为离线，请参考**在主机本地手动卸载Agent**。

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“非集群节点”页签。

步骤6 在目标节点所在行的“操作”列，单击“卸载Agent”。

如需批量卸载，请先勾选所有目标节点，并单击“批量卸载”。

步骤7 确认待卸载相关信息后，单击“确认”，开始卸载。

等待5~10分钟后，查看到目标节点的Agent状态为“未安装”，表示卸载成功。

----结束

11.2.3 接入三方镜像仓

HSS支持接入三方镜像仓，并为镜像提供漏洞、基线、恶意文件等多方位的安全检测和管理能力，可帮助用户及时发现镜像中存在的安全风险。您可以参考本章节将三方镜像仓接入HSS。

前提条件

已将镜像仓关联的集群（承载集群）接入HSS，且集群状态为“运行中”。相关操作请参见**为容器安装Agent**。

接入三方镜像仓

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 容器安装与配置”，进入“容器安装与配置”页面。

步骤5 选择“三方镜像仓”页签。

步骤6 单击“接入三方镜像仓”，弹出“接入三方镜像仓”对话框。

步骤7 根据页面提示， 填写接入所需信息。各项参数说明请参见**表 接入镜像仓参数说明**。

表 11-8 接入镜像仓参数说明

参数名称	参数说明	取值样例
选择承载集群	选择承载镜像仓的集群。	cluster01

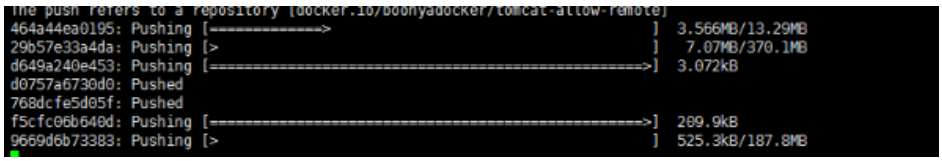
参数名称	参数说明	取值样例
扫描组件获取方式	镜像扫描组件用于拉取镜像，扫描并分析所需的元信息后，将这些元数据传输给服务端，服务端对这些元数据执行漏洞、基线、恶意文件、敏感信息等安全检测。 镜像扫描组件需要上传到镜像仓中，您可以选择镜像扫描组件的获取方式： • **从SWR获取扫描组件**：集群与SWR网络互通，集群可以通过SWR获取镜像扫描组件。 • **手动上传扫描组件**：集群与SWR网络不通，需手动上传镜像扫描组件到镜像仓。	从SWR获取扫描组件
镜像仓名称	输入镜像仓的完整名称。	test
镜像仓类型	单击，选择镜像仓所属类型。	Harbor
镜像仓接口版本	单击，选择镜像仓接口版本。	V1
镜像仓项目	扫描组件获取方式选择“手动上传扫描组件”，且镜像仓类型为“Harbor”时，需要输入镜像仓项目信息。	-
通信类型	选择镜像仓的通信协议类型。 • http • https	https
镜像仓地址	输入镜像仓地址。 可以输入镜像仓“网址”或者“IP:端口”。 例如myharbor.com	myharbor.com
镜像仓用户名	输入登录用户名。	-
镜像仓密码	输入登录用户密码。	-

步骤8 （可选）扫描组件获取方式选择“手动上传扫描组件”时，在填写完接入信息后，请按如下操作配置扫描组件。

1. 在“接入三方镜像仓”弹窗中，单击“生成命令”。
2. 在“接入三方镜像仓”弹窗中，单击“复制镜像获取指令”，复制镜像获取指令。

3. 登录任意一台可以访问公网的Linux主机，粘贴并执行**步骤8.2**复制的指令，下载扫描组件镜像。
4. 将下载完成的扫描组件镜像，拷贝到承载集群上的任一节点上。
5. 在“接入三方镜像仓”弹窗中，单击“复制命令”，并在“扫描组件镜像”所在集群节点执行复制的命令上传扫描组件到镜像仓。
6. 界面回显如**图 上传扫描组件成功**所示，表示手动上传扫描组件成功。

图 11-1 上传扫描组件成功



步骤9 单击“确定”，开始接入镜像仓。

步骤10 在三方镜像仓页面，目标镜像仓的“镜像仓状态”列，查看镜像仓接入结果。

----结束

11.3 告警配置

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，如果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，如果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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 告警配置”，进入“告警配置”页面。

步骤5 （可选）如果您的服务器已通过企业项目的模式进行管理，您可在页面上方“企业项目”下拉框中选择目标企业项目后配置目标企业项目的告警通知。

- 选择单个企业项目，配置的告警通知信息仅在对应的企业项目内生效。
- 选择“所有项目”，配置的告警通知信息将生效于所有企业项目。

步骤6 根据页面提示，配置告警通知。配置参数说明请参见**表11-9**。

表 11-9 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。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7 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。告警通知发送给消息主题的订阅终端，订阅终端支持的协议包括短信、邮件等。

  创建新的主题以及添加订阅终端的具体操作如下：

  a. 创建主题。

  b. 为创建的主题添加一个或多个订阅。

  c. 添加订阅后，按接收到的短信或邮件等提示，完成订阅确认。

     主题订阅确认的信息可能被当成垃圾短信拦截，如未收到，请查看是否设置了垃圾短信拦截。

  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。

步骤8 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 11-10 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。

通知项	通知内容	通知内容说明
	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。
	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。

通知项	通知内容	通知内容说明
	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。 ● 如果账户暴力破解成功，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）。 如果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。
	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。

通知项	通知内容	通知内容说明
	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。
	可疑进程运行	检测未经过认证或授权的应用进程运行，一旦发现进行告警。
	可疑进程文件访问	检测未经过认证或授权的进程访问指定的目录，一旦发现进行告警。

- **实时告警通知**
  事件发生时，及时发送告警通知。

  表 11-11 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。

通知项	通知内容	通知内容说明
	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。
	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。

通知项	通知内容	通知内容说明
	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）。 如果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。
	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。

通知项	通知内容	通知内容说明
	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。
	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。
	可疑进程运行	检测未经过认证或授权的应用进程运行，一旦发现进行告警。
	可疑进程文件访问	检测未经过认证或授权的进程访问指定的目录，一旦发现进行告警。
账户登录	登录成功	对登录成功的账户进行通知。
主机防御	勒索防护关闭	对勒索病毒防护异常关闭或手动关闭的情况发送告警通知。

11.4 授权管理

操作场景

HSS部分功能对其他云服务资源有依赖，需要您将相关云服务资源的操作权限委托给HSS，让HSS以您的身份使用执行一些任务调度和资源运维等工作，这些功能才能正常访问和使用。

HSS需要您委托授权的其他云服务资源权限如**表11-12**所示。

表 11-12 其他云服务资源权限依赖

功能	所需权限	对应云服务权限		权限用途
		权限	授权项（Action）	
容器审计（镜像仓审计）	CTSOperatePolicy	查询审计事件	cts:trace:list	获取镜像操作日志（SWR服务的CTS日志）
主机安装与配置	VPCOperatePolicy	创建端口	vpc:ports:create	创建网卡、修改安全组等，保证安装Agent使用的端口畅通
		删除端口	vpc:ports:delete	
		创建安全组规则	vpc:securityGroupRules:create	
		删除安全组规则	vpc:securityGroupRules:delete	

功能	所需权限	对应云服务权限		权限用途
		权限	授权项（Action）	
		查询端口列表或详情	vpc:ports:get	
		查询网络列表或详情	vpc:networks:get	
		查询子网列表或详情	vpc:subnets:get	
	VPCEPOperatePolicy	创建终端节点	vpcep:endpoints:create	Agent和HSS云端防护中心（Master）的网络通道维护
		查询终端节点列表	vpcep:endpoints:list	
		删除终端节点	vpcep:endpoints:delete	
• 容器安装与配置 • 仓库镜像定时同步	CCEOperatePolicy	查询集群信息	cce:cluster:get	管理CCE集群下的HSS-Daemonset以及Configmap的生命周期
		查询指定项目下的集群	cce:cluster:list	
		查询指定条件下的委托列表	iam:agencies:listAgencies	
仓库镜像定时同步	SWROperatePolicy	查询组织列表	swr:namespace:listNamespaces	获取SWR服务的镜像信息，包括组织、仓库和制品等。
		查询镜像列表	swr:repo:listRepos	
		查询镜像Tag列表	swr:repo:listRepoTags	
		查询共享镜像列表	swr:repo:listSharedRepos	
		获取实例列表	swr:instance:list	
		获取同步仓库详情	swr:instance:getRegistry	
		获取仓库详情	swr:repository:getRepository	
		获取实例详情	swr:instance:get	
		获取仓库列表	swr:repository:listRepositories	
		获取制品列表	swr:repository:listArtifacts	

授权云服务资源权限

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 授权管理”，进入“授权管理”页面。

步骤5 单击“新增授权”，弹出“新增授权”对话框。

步骤6 勾选需要授权的权限，单击“确认”，完成授权。

----结束

删除云服务资源权限

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“安装与配置 > 授权管理”，进入“授权管理”页面。

步骤5 在目标权限所在行的操作列，单击“删除”，弹出“删除授权”对话框。

或者勾选多条权限，并在列表上方单击“删除”，批量删除授权。

步骤6 确认要删除的权限信息后，在对话框中输入“DELETE”，并单击“确定”。

查看权限列表中无该权限信息，表示取消授权成功。

----结束

11.5 插件配置

11.5.1 插件配置概述

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：

- 当您需要保证容器镜像的安全质量，避免因为使用不可信或过时的镜像而导致安全风险时，您可以**配置镜像阻断策略**，指定阻断的漏洞等级或白名单。
- 当您需要遵循一些行业或法规的安全要求，例如：PCI DSS、CIS等，您可以**配置镜像阻断策略**，指定阻断的安全基线或合规检查项。

- 当您需要实现容器DevSecOps的最佳实践，将安全检查和防御嵌入到容器生命周期的每个阶段时，您可以**配置镜像阻断策略**，实现从源头到终端的安全保障。

约束与限制

安装Docker插件需满足以下条件：

- 已开启企业主机安全容器版防护。
- 仅支持Docker类容器使用本插件。
- Docker Engine版本在18.06.0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。

11.5.2 查看插件信息

插件配置页面会展示服务器列表以及服务器对应的插件信息，如果服务器未安装插件，插件相关信息为空。您可通过查看服务器的插件信息，判断需要安装插件的服务器。

查看插件信息

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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 11-13 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

11.5.3 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。

安装插件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 插件配置”，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5 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。
- 如果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6 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤7 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
```

如果存在多个不同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 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。

如果无法下载安装包，请确认DNS是否可以正常解析安装命令中的域名。

步骤10 反馈“remote_install finished. [OK]”则安装成功，等待3-5分钟可查看面板服务器的Docker插件状态。

```
remote_install finished. [OK]
```

----结束

11.5.4 卸载插件

当您无需使用镜像阻断功能，您可以参考本章节卸载Docker插件。

卸载 Docker 插件

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 插件配置”，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5 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。
- 如果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6 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤7 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
```

如果存在多个不同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 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10 反馈“remote_uninstall finished. [OK]”则卸载成功，等待3-5分钟可查看服务器的Docker插件状态。

```
remote_uninstall finished. [OK]
```

----结束

12 监控与审计

12.1 使用 CES 监控 HSS

12.1.1 HSS 支持的监控指标

功能说明

本节定义了企业主机安全上报云监控服务的监控指标的命名空间、监控指标列表和维度列表，用户可以通过云监控服务提供的管理控制台或API接口来检索企业主机安全产生的监控指标和告警信息。

命名空间

SYS.HSS

监控指标

表 12-1 企业主机安全支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
host_num	服务器总数	该指标用于统计服务器总数	≥0	Count	不涉及	企业项目	300秒
unprotected_host_num	未开启防护服务器数量	该指标用于统计未开启防护的服务器数量	≥0	Count	不涉及	企业项目	300秒

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
risky_host_num	有风险服务器数量	该指标用于统计经检测判定存在风险的服务器的数量	≥0	Count	不涉及	企业项目	300秒
uninstalled_or_offline_agent_num	未安装/已离线agent数量	该指标用于统计未安装agent或者状态为离线的agent的数量	≥0	Count	不涉及	企业项目	300秒

维度

表 12-2 维度列表

key	Value
hss_enterprise_project_id	企业项目，取值为企业项目ID。

12.1.2 HSS 支持监控的事件

功能说明

通过云监控服务，对Agent状态进行监控，当出现Agent异常离线和Agent防护状态异常事件时进行告警，方便您及时了解企业主机安全的防护情况。

开启事件告警通知后，出现相关事件时，即可在云监控服务的事件监控页面查看事件详情。

命名空间

SYS.HSS

事件监控支持的事件列表

表 12-3 企业主机安全支持监控的事件

事件名称	事件ID	事件级别	事件说明	处理建议	事件影响
企业主机安全服务Agent异常离线	hssAgentAbnormalOffline	重要	一般是由于Agent与服务器通信异常，主机中的Agent进程异常等原因导致。	排查网络故障，待网络恢复正常后，若长时间Agent状态仍为“离线”，可能是Agent进程异常，需要登录主机，重启Agent进程。	业务中断
企业主机安全服务Agent防护状态异常	hssAgentAbnormalProtection	重要	一般是由于底层资源不足造成Agent工作模式异常等原因导致。	登录主机检查资源，如发现内存或者其他系统资源过高等情况，建议优先扩容处理。如果资源够用,重启Agent进程后还是异常，提交工单让运维处理。	业务中断

12.1.3 创建监控告警规则

通过设置HSS告警规则，您可自定义监控目标与通知策略，设置告警规则名称、监控对象、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解HSS防护状况，从而起到预警作用。

HSS支持通过云监控服务监控服务指标和事件，本文介绍如何创建指标和事件的告警规则。

创建指标监控告警规则

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 单击页面左上方的，选择“管理与部署 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”界面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 根据界面提示，填写告警规则信息。相关参数说明请参见表12-4。

表 12-4 创建指标监控告警规则参数说明

参数名称	参数说明	取值样例
名称	系统会随机产生一个名称，您也可以进行修改。	alarm-hss
描述	告警规则描述。非必填项。	-
告警类型	告警规则的类型，可选择指标或者事件。	指标
云产品	当告警类型选择“指标”时，需配置告警规则监控的服务名称。 在下拉列表中选择“主机安全服务-主机安全”或“主机安全服务-主机实例”。 ● “主机安全服务-主机安全”：表示企业项目维度的监控指标，指标包括“服务器总数”、“未开启防护服务器数量”、“有风险服务器数量”、“未安装/已离线agent数量”。 ● “主机安全服务-主机实例”：表示主机维度的监控指标，指标包括“主机防护状态”、“Agent运行状态”。	主机安全服务-主机安全
资源层级	监控对象的资源层级。 当告警类型选择“指标”时，需选择告警规则的资源层级，可选择云产品或子维度。推荐选择云产品。	云产品
监控范围	告警规则适用的资源范围。 ● 选择“全部资源”时，则当前云产品下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 ● 选择“资源分组”时，该分组下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 ● 选择“指定资源”时，在“监控对象”单击“选择指定资源”进行指定资源的选择。	全部资源
触发规则	根据需要可选择关联模板或自定义创建。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。	自定义创建
告警策略	当触发规则选择“自定义创建”时，需要设置触发告警规则的告警策略。	-
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知。	开启

参数名称	参数说明	取值样例
通知方式	需要发送告警通知的对象，根据实际选择。	通知策略

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

创建事件监控告警规则

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 单击页面左上方的，选择“管理与部署 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”界面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 根据界面提示，填写告警规则信息。相关参数说明请参见表12-5。

表 12-5 创建事件监控告警规则参数说明

参数名称	参数说明	取值样例
名称	系统会随机产生一个名称，您也可以进行修改。	alarm-hss
描述	告警规则描述。非必填项。	-
告警类型	告警规则的类型，可选择指标或者事件。	事件
事件类型	当告警类型选择“事件”时，需要选择事件类型，可选择“系统事件”或“自定义事件”。	主机安全服务-主机安全
事件来源	当告警类型选择“事件”时，需要设置事件来源。 • 当事件类型选择“系统事件”时，在下拉列表中选择事件来源的云服务名称。 • 当事件类型选择“自定义事件”时，事件来源需要与上报的字段一致，格式需要为service.item形式。	系统事件
触发规则	根据需要可选择关联模板或自定义创建。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。	自定义创建
告警策略	当触发规则选择“自定义创建”时，需要设置触发告警规则的告警策略。	-
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知。	开启

参数名称	参数说明	取值样例
通知方式	需要发送告警通知的对象，根据实际选择。	通知策略

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

12.1.4 查看监控指标

您可以通过管理控制台，查看企业主机安全的各项监控指标，及时了解企业主机安全的防护情况。

查看监控指标

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 单击页面左上方的，选择“管理与部署 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“云服务监控 > 主机安全服务”，进入“云服务监控”页面。

步骤5 在目标企业项目ID所在行的“操作”列中，单击“查看监控指标”，查看企业项目下的服务器防护指标详情。

----结束

12.2 使用 CTS 审计 HSS 操作事件

12.2.1 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12-6所示。

表 12-6 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

操作名称	资源类型	事件名称
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
添加登录告警白名单	hss	addLoginWhiteList
删除登录告警白名单	hss	removeLoginWhiteList
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

操作名称	资源类型	事件名称
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
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

13 常见问题

13.1 产品咨询

13.1.1 什么是主机安全?

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。

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。

各组件功能及工作流程说明如下：

表 13-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	• 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。 • 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全。 • Agent可安装在弹性云服务器（Elastic Cloud Server，ECS）/裸金属服务器（Bare Metal Server，BMS）、线下IDC以及第三方云主机中。 • 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。

13.1.2 什么是容器安全?

容器安全指的是企业主机安全容器版，一个提升容器安全性的安全服务。

企业主机安全容器版提供资产管理、镜像安全扫描、集群防护、运行时入侵检测等容器安全防御能力，能够为容器提供全生命周期防护，帮助企业解决传统安全软件无法感知容器环境问题，有效防护容器安全运行时安全。

- 在部署阶段，HSS可扫描镜像仓库，检测镜像中存在的漏洞、恶意文件、风险配置等，并提供修复指导，帮助用户获得安全的镜像。
- 在容器运行阶段，HSS提供实时监控和日志管理功能，及时检测和响应异常活动，同时通过入侵检测系统和自动化响应机制应对潜在的安全威胁。此外，HSS提供容器防火墙功能，用户可自定义对容器实施网络策略和隔离措施，可有效防范集群中东西向网络的潜在风险，保障容器间的安全通信。

13.1.3 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。

网页防篡改的操作流程和主要功能概览。操作流程如图13-1所示，主要功能概览请参考表13-2。

图 13-1 网页防篡改操作流程

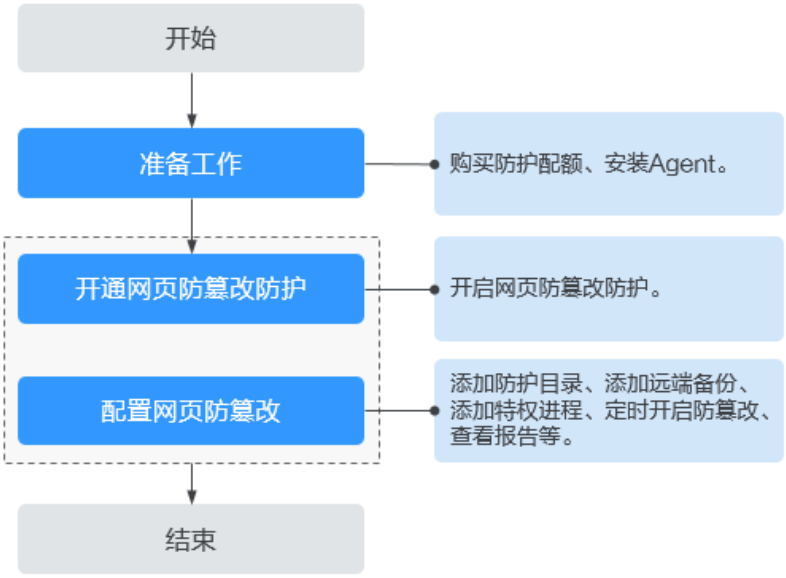


表 13-2 主机安全防篡改操作流程及功能说明

操作类型	操作	描述与参考
准备工作	购买防护配额	您需要购买防护配额后，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。
开通网页防篡改防护	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。

操作类型	操作	描述与参考
	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。

13.1.4 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。

13.1.5 HSS 是否和其他安全软件有冲突?

企业主机安全可能会和“DenyHosts”、“网防G01”或“360安全卫士服务器版”冲突。

Agent 软件可能与“DenyHosts”有冲突

详情请参见：**Agent是否和其他安全软件有冲突?**

双因子认证功能可能与“网防 G01”或“360 安全卫士服务器版”冲突

开启企业主机安全的Windows主机，在使用双因子认证功能时，可能会和“网防G01”软件或360安全卫士服务器版的登录认证功能产生冲突，您可以根据实际情况，选择使用企业主机安全的双因子认证功能、“网防G01”或“360安全卫士服务器版”的登录认证功能。

13.1.6 HSS 与 WAF 有什么区别?

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 13-3 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 • 检测与响应 • 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

13.1.7 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。
- 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 13-4 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 13-5 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

13.1.8 HSS 是否支持病毒查杀?

支持。

企业主机安全提供病毒查杀功能，病毒查杀功能基于特征病毒检测引擎，支持扫描服务器中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可根据自身需要，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”扫描任务。

病毒查杀详细的使用介绍请参见**病毒查杀**。

13.2 Agent 相关

13.2.1 Agent 是否和其他安全软件有冲突?

Agent可能会和DenyHosts这款软件产生冲突。

- 冲突表现：登录主机的IP地址被HSS识别为攻击IP后，被HSS封禁，解封后仍然不能使用该IP地址登录主机。
- 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**用户登录服务器。
  b. 执行以下命令，检查是否安装了DenyHosts。
     ps -ef | grep denyhosts.py
     如果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;

13.2.2 如何卸载 Agent?

如果不再需要企业主机安全为您的服务器提供防护，您可以参照本文卸载Agent，Agent卸载后企业主机安全将停止对服务器的检测和防护。

卸载方式说明

Agent提供如下两种卸载方式：

- 一键卸载：通过企业主机安全控制台的卸载功能一键卸载，具体操作请参见**在企业主机安全控制台一键卸载Agent**。
- 手动卸载：在主机本地手动卸载，具体操作请参见**在主机本地手动卸载Agent**。

建议您优先选择一键卸载的方式卸载Agent，该方式操作简单高效。如果在控制台上发现Agent状态为“离线”，无法执行卸载操作时，您可以选择手动卸载的方式来卸载Agent。

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”。

在企业主机安全控制台一键卸载 Agent

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“安装与配置 > 主机安装与配置 > Agent管理”，进入Agent管理页面。

步骤5 选择“已安装主机”页签，筛选Agent在线的服务器。

步骤6 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”，开始卸载。

您也可以勾选需卸载Agent的目标服务器，并单击列表上方的“批量卸载Agent”，批量为服务器卸载Agent。

步骤7 等待5~10分钟左右，选择“未安装主机”页签，查找到目标服务器，目标服务器的Agent状态为“未安装”表示卸载Agent成功。

----结束

在主机本地手动卸载 Agent

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，并执行如下命令切换到**root**用户。

     su - root

  b. 在任意目录执行如下命令，卸载Agent。

     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。

     - 针对EulerOS、CentOS、Red Hat等支持rpm安装软件的OS，执行命令：**rpm -e hostguard**
     - 针对Ubuntu、Debian等支持deb安装软件的OS，执行命令：**dpkg -P hostguard**

     当界面回显如下类似信息，则表示卸载Agent完成，无需再执行下一步，等待15分钟左右企业主机安全控制台上服务器的Agent状态会更新为“未安装”或“离线”。如果卸载失败请执行**c**。

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

  c. （可选）当执行**b**卸载Agent失败时，可参考如下方式卸载Agent。

     - 针对EulerOS、CentOS、Red Hat等支持rpm安装软件的OS。
       1) 执行如下命令，删除安装记录。

          rpm -e --justdb hostguard

       2) 执行如下命令，查询是否有hostguard残留进程。

          ps -ef | grep hostguard

          如果有残留，请执行命令**kill -9“进程pid”**停止所有残留进程。

       3) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。

          ll /usr/local/hostguard

          如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。

       4) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。

          ll /etc/init.d/hostguard

          如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。

     - 针对Ubuntu、Debian等支持deb安装软件的OS。
       1) 执行如下命令，查询是否有hostguard残留进程。

          ps -ef | grep hostguard

          如果有残留，请执行命令**kill -9“进程pid”**停止所有残留进程。

       2) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。

          ll /usr/local/hostguard

          如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。

3) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。

ll /etc/init.d/hostguard

如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。

- **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C:\Program Files\HostGuard目录下，双击“unins000.exe”，启动卸载程序。
- 如果安装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卸载向导”提示框中，单击“是”，开始卸载。

d. （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。

13.2.3 Agent 安装失败应如何处理?

如果为首次安装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 确认主机是否已绑定弹性IP。

- 是：请执行下一步骤。
- 否：请绑定弹性IP后重新安装。

步骤3 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4 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5 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

13.2.4 Agent 状态异常应如何处理?

Agent状态主要分为以下三种，如果Agent的运行状态为“未安装”或者“离线”时，表示Agent状态异常。

- 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“约束与限制”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。
- 主机内存不足。
- Agent进程异常。

处理方法

步骤1 为主机安装Agent已超过10分钟，控制台Agent状态显示“离线”或者“未安装”。

- 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 请确认主机的操作系统是否在产品介绍中“约束与限制”说明范围内。

- 是：请执行**步骤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 请确认主机是否可正常访问网络。

- 否：请确保您的主机能正常访问网络后，再前往HSS控制台查看Agent状态。

步骤4 请确认待安装Agent的磁盘容量是否大于300MB。

对于Linux主机，Agent默认安装在/usr/local/hostguard/路径下，您需要确认该路径所在磁盘分区剩余容量是否大于300MB。对于Windows主机，Agent默认安装在C:\Program Files\HostGuard路径下，您需要确认C盘剩余容量是否大于300MB。

- 是：请执行**步骤5**。
- 否：主机内存不足将导致Agent离线，请扩充内存容量，容量扩充完成后，Agent将恢复上线。

步骤5 Agent进程异常，请按如下操作重启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

  如果回显以下信息，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：

- 如果Agent状态为“在线”，则故障清除。
- 如果Agent状态仍为“未安装”或者“离线”，请卸载Agent，再重新安装Agent。
  a. 卸载Agent请参见**如何卸载Agent?** 。

     卸载操作执行完成后，请等待5~10分钟，确认服务器展示在HSS控制台的“主机安装与配置 > Agent管理 > 未安装主机”页面后，再执行安装Agent操作。
  b. 安装Agent请参见**为主机安装Agent**。

----结束

13.2.5 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13-6**所示。

表 13-6 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

13.2.6 Agent 运行时占用多少 CPU、内存和磁盘资源?

HSS服务采用轻量级Agent，占用资源极少，不会影响主机和容器的正常业务运行。

本文为您介绍Agent在执行检测任务时，在主机和容器节点中占用的CPU、内存以及磁盘资源情况。Agent定时检测任务会基于使用地时间在每日00：00-04：00执行，全量扫描主机和容器，不会影响主机和容器的正常运行。

CPU 占用峰值

Agent在主机或容器节点上运行时，一般情况下CPU占用控制在**1vCPU**的20%以内；如果Agent正在执行病毒查杀任务，由于病毒查杀程序会额外占用部分CPU，CPU占用会控制在最多不超过多核CPU的30%。CPU实际占用比例与您申请的云服务器规格有关，详见**表13-7**。

如果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。如果CPU占用比例超过1vCPU的25%，Agent将自动重启。

表 13-7 不同 vCPU 规格下 Agent 的 CPU 占用情况

vCPUs	占用CPU资源比例（峰值）	执行病毒查杀时，占用CPU资源比例（峰值）
1vCPUs	20%	50%
2vCPUs	10%	40%
4vCPUs	5%	35%
8vCPUs	2.5%	32.5%
12vCPUs	约1.67%	约31.67%
16vCPUs	约1.25%	约31.25%
24vCPUs	约0.84%	约30.84%
32vCPUs	约0.63%	约30.63%
48vCPUs	约0.42%	约30.42%
60vCPUs	约0.34%	约30.34%
64vCPUs	约0.32%	约30.32%

内存占用峰值

Agent在主机上运行时，一般情况下内存最多占用**500MB**，如果Agent正在执行病毒查杀任务，由于病毒查杀程序会额外占用部分内存，内存占用会控制在**均值800MB**。

Agent在容器节点上运行时，内存占用区分以下两种情况：

- **单节点安装**：如果您是参考**为主机安装Agent**为节点逐一安装的Agent，一般情况下Agent最多占用内**500MB内存**，如果Agent正在执行病毒查杀任务，由于病毒查杀程序会额外占用部分内存，内存占用会控制在**均值800MB**。
- **集群安装**：如果您是参考**为容器安装Agent**将整个集群接入HSS，Agent将以守护进程集（DaemonSet）的形式运行。一般情况下Agent最多占用**1100MB**内存，如果Agent正在执行病毒查杀任务，由于病毒查杀程序会额外占用部分内存，内存占用会控制在**均值1400MB**。

如果Agent内存占用超过最大内存限制，Agent会在5分钟内自动重启。

磁盘占用峰值

Agent在主机或容器节点上运行时，磁盘占用情况如下：

- Linux：安装目录位于/usr/local/hostguard，最多占用**600MB**。日志目录位于/var/log/hostguard/，最多占用**250MB**。
- Windows：安装目录和日志目录均位于C:\Program Files\HostGuard，最多占用**700MB**。

13.2.7 购买不同版本 HSS，可以共用同一 Agent 吗?

可以。

同一服务器安装一次Agent即可满足所有版本的使用。

13.2.8 如何查看未安装 Agent 的主机?

查看未安装Agent的主机的操作如下：

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“安装与配置 > 主机安装与配置”，进入Agent管理页面。

步骤5 选择“未安装主机”页签，查看未安装Agent的主机。

----结束

13.2.9 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：如果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。

如果您正在使用旧版，新版显示Agent未安装，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。升级成功后，新版界面显示Agent已安装，旧版界面显示未安装。

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。

13.2.10 升级失败怎么处理?

Agent 升级说明

- 无论升级前还是升级后同一台主机都会同时在企业主机安全新、旧版呈现，服务器状态以使用的控制台版本为准。
- 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。
- 升级后将在新版conosle进行计费，旧版停止计费。
- 升级后云服务器在企业主机安全（新版）继续被防护，企业主机安全（旧版）将停止防护。

失败常见原因

说明

自动执行升级完成后，需要等待5~10分钟左右Agent才会自动刷新Agent状态。

Agent升级失败或超过等待时间仍不显示可能原因如下：

1. 10180端口被限制访问：Agent升级需要通过端口10180进行访问。
2. 可用内存不足：Agent升级需要占用一定内存，主机剩余内存小于300M会影响正常升级。

原因排查及解决办法

- **10180端口被限制访问。**

  待安装或升级Agent的线上主机需要与网段相通，要求您的服务器安全组出方向的设置允许访问100.125.X.X/16网段的10180端口。

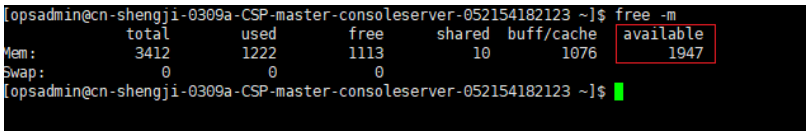
  - 排查步骤

i. 在页面左上角选择“区域”，单击 ☰，选择“计算 > 弹性云服务器”。
ii. 单击目标服务器名称，进入服务器详情页面，单击“安全组”，查看安全组规则。
iii. 选择“出方向规则”，查看禁止策略中是否有10180端口。
1) 如果没有，表示非端口被限制访问问题。
2) 如果存在，表示端口被限制访问。

– 解决办法
端口被限制访问，需要将端口策略修改为允许。

- **可用内存不足。**
– 排查步骤
▪ Linux主机
1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
2) 执行以下命令，查看目标云服务器的内存使用情况。
free -m
3) 执行命令反馈信息如图13-2所示，查看free项的数值。
如果available数值小于300M，则表示内存不足。

图 13-2 查看内存



▪ Windows主机
1) 通过远程管理工具（如：mstsc、rdp）远程登录目标云服务器。
2) 打开任务管理器。
3) 选择“性能 > 内存”，进入“内存”页面，查看剩余可用内存。
如果可用内存小于300M，则表示内存不足。

– 解决办法
▪ 关闭一些高内存占用的应用程序。

13.2.11 不升级有什么影响?

HSS（旧版）在没有被HSS（新版）完全替换前可继续正常使用。

升级至 HSS（新版）的必要性

- 后续产品演进，HSS（新版）将完全替换HSS（旧版），届时HSS（旧版）将会下线。
- 在HSS（新版）中，新增了部分功能以及对部分功能的能力做了大幅度提升，升级后可提升服务器的安全防护能力，大致如下：

表 13-8 HSS（新版）主要功能迭代情况

功能名称	功能描述	功能形态
资产指纹管理	深度扫描服务器中的资产，将资产划分为账号、端口、进程、Web目录、软件信息等不同维度进行统计展示和管理。	新增
资产重要性	您可对名下所有服务器按照服务器资产绑定资产重要性等级，绑定后可按照不同等级的资产进行批量管理，包括但不限于部署策略、开启/关闭防护、分配组、安装Agent。	新增
应用漏洞	漏洞扫描新增对应用漏洞的扫描，包括检测Web服务、Web框架、Web站点、中间件、内核模块等资产信息存在的漏洞。	新增
基线报告导出	您可对基线检查的配置检查和经典弱口令检测的结果进行筛选导出。	新增
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。包括但不限于对SQL注入、命令注入、反序列化输入、文件遍历、JSP执行操作系统命令等漏洞的扫描检测。	新增
Agent安装	支持一键批量安装Agent。	新增
基线检查	支持自定义勾选等保合规的基线检测项，生成检测结果。	新增
告警事件管理	支持对勒索软件、反弹Shell告警的隔离查杀处理。 支持对一般漏洞利用、Redis漏洞利用、Hadoop漏洞利用、MySQL漏洞利用的检测告警。 。	新增
安全报告	支持自定义报告周期、报告内容、发送时间。	升级
勒索病毒	实时监控全盘新增文件及运行中的进程，动态生成诱饵文件进行主动诱捕，识别勒索软件，同时可自定义策略对服务器进行定期备份。	升级
容器安全防护	将原有的容器安全服务合并至HSS（新版），将服务器负载进行统一管理。	合并

13.2.12 无法访问 Windows 或 Linux 版本 Agent 下载链接?

问题原因

Agent下载链接为云内网地址，因此在下载Agent前，您需要先为主机配置云内网DNS地址。如果没有配置云内网DNS地址，主机将访问不了下载链接。

解决办法

联系交付或运维人员配置正确的内网DNS地址，配置完成后访问对应系统版本的Agent下载链接，重新执行命令安装Agent。

13.2.13 升级 Agent 失败，提示“替换文件失败”

问题现象

在企业主机安全控制台“安装与配置 > 主机安装与配置 > Agent管理”页面，升级Agent后，Agent升级状态显示“升级失败”，鼠标滑动至升级失败文字处查看到提示“替换文件失败”。

解决办法

企业主机安全Agent 3.2.4及以下版本不能平滑升级至新版本，因此您需要手动卸载3.2.4及以下版本Agent，再重新安装新版本Agent，详细操作请参考：

1. **卸载Agent**。
2. **为主机安装Agent**。

13.3 漏洞管理

13.3.1 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

13.3.2 漏洞修复后，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

建议您参考处理漏洞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，可以使用镜像源进行漏洞修复。

- **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 13-9 验证修复命令

操作系统	修复命令
CentOS/Fedora /Euler/Red Hat/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。

13.3.3 漏洞管理显示的主机不存在?

漏洞列表展示7天内扫描到的漏洞，如果扫描到主机存在漏洞后，您修改了主机的名称，未重新执行漏洞扫描，漏洞列表仍会显示原主机名称。

13.3.4 漏洞修复完成后，要重启主机吗?

“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。

13.3.5 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 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7 选择“修复任务”页签，查看漏洞修复结果。

----结束

Linux 漏洞修复失败原因及解决方法

⚠ 注意

- 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。
- Kernel类的漏洞修复完成后，需要重启主机，不重启主机漏洞仍会显示存在。
- 失败原因只截取了部分关键字段，具体信息请以企业主机安全控制台显示为准。

失败原因	原因说明	解决办法
timeout	修复超时	请等待1小时后重试修复漏洞。
This agent version does not support vulnerability verification	Agent版本太低	服务器安装的Agent版本过低，请升级Agent后进行漏洞修复。
Agent status is not normal	Agent状态异常	Agent已离线，无法完成漏洞修复。请参考**Agent状态异常应如何处理?** 使Agent状态恢复正常后，进行漏洞修复。

Error: software has multiple versions	存在漏洞的软件版本未删除	• 如果是普通软件出现此问题，可以删除旧版本包，重新检测漏洞是否存在。
		执行以下命令测试删除旧版本包有无报错。
		`rpm -e --test XXX`
		说明
		“XXX”表示软件带版本号的完整组件名，可通过**rpm -qa**命令查询完整组件名。
		– 删除有报错：表示有软件包依赖，不可删除，建议您忽略该漏洞。
		– 删除无报错：可执行以下命令删除旧版本包。
		`rpm -e XXX`
		• 如果是Kernel、Glibc等内核相关组件出现此问题，删除旧版本包可能会引起操作系统问题，建议您忽略该漏洞。

失败原因	原因说明	解决办法
No package marked for update Error: software info not update Error: kernel is not update is already the newest version Dependencies resolved. Nothing to do. Complete!	未找到新版本升级包	失败原因表示软件已经升级为当前镜像源支持的最高版本，但漏洞仍然存在。 **说明** • CentOS 8官方已停止维护，HSS使用Red Hat的补丁公告替代检测，由于官方不出补丁所以无法修复，建议您使用正在维护的操作系统。 • Ubuntu 16.04、18.04、22.04版本，目前已不支持免费补丁更新，需要订阅Ubuntu Pro才能安装升级包。 • Debian 9、10官方已停止维护，由于官方不出补丁所以无法修复，建议您使用正在维护的操作系统。 • 可能原因一：镜像源配置错误。 请配置镜像源，更新镜像源后，重新修复漏洞。 • 可能原因二：主机禁止内核漏洞修复。 修复内核漏洞可能导致功能不可用，请勿修复内核漏洞。 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，请勿升级内核组件。
Error: Failed to download metadata for repo One of the configured repositories failed Errors during downloading metadata for repository Error: Cannot retrieve repository metadata Failed connect to E: Failed to fetch	无法连接到yum源	主机无法连接镜像源，请检查主机是否无法正常连接外网。
Error: kernel is not update Error: kernel info not update	内核未更新	• 可能原因一：漏洞修复后未重启。 解决办法：重启主机。kernel漏洞修复后，需要重启主机才会生效，否则下次漏洞扫描时仍判定该漏洞未修复。 • 可能原因二：主机禁止内核漏洞修复。 修复内核漏洞可能导致功能不可用，请勿修复内核漏洞。

失败原因	原因说明	解决办法
Please install a package which provides this module, or verify that the module is installed correctly	yum命令不可用	请根据失败原因中提示的方法，修复命令不可用问题。
command not found		
Error downloading packages	下载升级包失败	请确认主机是否可正常连接外网： ● 是：镜像源配置错误，请参考配置镜像源，更新镜像源后，重新修复漏洞。 ● 否：请保证您的主机可以正常连接外网后，重新修复漏洞。
There are no enabled repositories	未配置可用的源	失败原因表示是镜像源配置错误，请参考配置镜像源，更新镜像源后，重新修复漏洞。
Error: Cannot find a valid baseurl for repo		
There are no enabled repos		
dpkg was interrupted	dpkg命令不可用	请根据失败原因中提示的方法，修复命令不可用问题。
Error: grub.conf still use old version.	操作系统缺少GRUB相关软件，导致安装新版本内核后grub.conf文件内容没有更新为新的内核版本	请检查服务器是否安装了grub2-pc-modules、grub2-tools-extra、grub2-pc三个软件，若未安装则按以下步骤处理： 1. 执行以下命令，在主机上安装上述三个软件。 **yum install grub2-pc-modules grub2-tools-extra grub2-pc -y** 2. 执行以下命令，查看当前运行的内核版本。 **uname -r** 3. 执行以下命令，查看当前已安装的所有内核组件版本。 **rpm -qa | grep kernel-[0-9]** 4. 执行以下命令，卸载掉版本高于当前运行内核的组件。 **yum remove [带版本号的完整软件名]** 5. 重新修复漏洞。

Windows 漏洞修复失败原因及解决方法

⚠ 注意

- Windows补丁安装后，需要重启主机，不重启主机会产生以下影响：
  - 补丁不生效。
  - 在安装其他系统补丁或软件时，可能会导致系统蓝屏、无法启动。
- 失败原因只截取了部分关键字段，具体信息请以企业主机安全控制台显示为准。

失败原因	原因说明	解决办法
timeout	修复超时	请等待1小时后重试修复漏洞。
Agent status is not normal	Agent状态异常	Agent已离线，无法完成漏洞修复。请参考**Agent状态异常应如何处理？**使Agent状态恢复正常后，进行漏洞修复。
This agent version does not support vulnerability verification	Agent版本太低	主机安装的Agent版本过低，请升级Agent后进行漏洞修复。
Search patch failed: Search failed, errmsg(Unknown error 0x8024401C)	查找补丁失败	失败原因表示主机上系统的Windows Update组件出现问题。请按以下操作恢复Windows Update组件后，重新修复漏洞： 1. 打开cmd命令提示符窗口。 2. 逐一执行以下命令尝试恢复。 net stop wuauserv reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate net start wuauserv

失败原因	原因说明	解决办法
Search patch failed: Search failed, errmsg(Unknown error 0x8024402C)	查找补丁失败	失败原因表示Windows Update客户端无法连接到Windows更新服务器。请按以下方法尝试恢复Windows Update组件后，重新修复漏洞： 1. 检查主机网络连接是否正常。 请确保您的主机可以连接互联网。 2. 清除Windows Update缓存。 a. 打开控制面板。 b. 进入“系统和安全 > 管理工具 > 服务”。 c. 选中“Windows Update”服务，单击右键，选择“停止”。 d. 打开C:\Windows文件夹，找到并删除“SoftwareDistribution”文件。 e. 选中“Windows Update”服务，单击右键，选择“启动”。 3. 执行以下命令重置Windows Update组件。 net stop wuauserv net stop cryptSvc net stop bits net stop msiserver ren C:\Windows\SoftwareDistribution SoftwareDistribution.old ren C:\Windows\System32\catroot2 catroot2.old net start wuauserv net start cryptSvc net start bits net start msiserver
Search patch failed: Search failed, errmsg(Unknown error 0x80070422)	查找补丁失败	失败原因表示主机上的Windows Update服务被关闭。请按以下操作启动服务后，重新修复漏洞： 1. 打开控制面板。 2. 进入“系统和安全 > 管理工具 > 服务”。 3. 双击“Windows Update”服务。 4. 在“Windows Update的属性”窗口，选择启动类型为“自动”。 5. 单击“确定”。

<table>
<tr><th>失败原因</th><th>原因说明</th><th>解决办法</th></tr>
<tr><td>Search patch failed: Get updates count is 0</td><td>查找补丁失败</td><td rowspan="8">失败原因表示主机的Windows Update故障，请按以下步骤排查问题：
1. 检查主机网络连接是否正常。
● 是：执行步骤2。
● 否：待主机网络连接正常后，重新进行漏洞修复。
2. 打开Windows Update，确认检查更新是否能检查出待安装补丁。
● 是：安装补丁并重启主机。
● 否：
如果修复失败原因中含错误码，请根据错误码在微软官网搜索对应的解决方案。
如果修复失败原因中不含错误码，尝试重置Windows Update。</td></tr>
<tr><td>Search patch failed: Search failed,errmsg</td><td>查找补丁失败</td></tr>
<tr><td>Not install security patch</td><td>查找补丁失败</td></tr>
<tr><td>Add patch to update collection failed: Update collection count is 0</td><td>查找补丁失败</td></tr>
<tr><td>Not find patch</td><td>没有找到补丁</td></tr>
<tr><td>Add patch to update collection failed</td><td>安装补丁失败</td></tr>
<tr><td>Com init failed</td><td>调用Windows更新失败</td></tr>
<tr><td>Download patch failed</td><td>下载补丁失败</td></tr>
<tr><td></td><td></td><td>● 可能原因一：Windows Update配置问题；仅Windows2008、2012可能会出现此种问题。在主机控制面板中找到“Windows Update > 更改设置”，按如下配置：
– 重要更新：选择下载更新，但是让我选择是否安装更新。
– 推荐更新：勾选。
– Microsoft更新：去勾选。
配置完成后，打开Windows Update，单击“检查更新”，待检查出待安装补丁后，安装补丁并重启主机。
● 可能原因二：主机长时间未打补丁，导致Windows Update异常。
1. 登录主机并打开Windows Update。
2. 单击“检查更新”。
3. 检查出待安装补丁后，安装补丁并重启主机。
说明
此场景漏洞可能一次无法完全修复，请反复检查更新直至安装完所有补丁。</td></tr>
</table>

失败原因	原因说明	解决办法
Some vulnerabilities have been fixed. You need to restart the server for the patch to take effect before fixing the remaining vulnerabilities.	未更新系统到最新版本	该漏洞一次无法完全修复，请重启主机，再次修复漏洞直至漏洞修复完成。

13.3.6 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 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

13.4 检测与响应

13.4.1 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 排查进程异常行为，如果出现主机挖矿行为，会触发HSS发送“进程异常行为”告警。

选择“检测与响应 > 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“处置”，对挖矿程序进行隔离查杀。

步骤5 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 > 主机指纹”，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。
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。
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	说明	操作步骤
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。

13.4.2 已添加告警白名单，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，但是不会取消隔离。因此如果您的进程被隔离，请手动恢复。

隔离查杀恶意程序

- 方式一：在“安装与配置 > 主机安装与配置 > 安全配置 > 恶意程序隔离查杀”页面中，开启自动隔离查杀。
- 方式二：在“检测与响应 > 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

1. 在“检测与响应 > 安全告警事件 > 主机告警事件”页面中，单击“已隔离文件”区域的数值，弹出“已隔离文件”页面。
2. 在目标服务器的所在行的“操作”列，单击“恢复”，弹出恢复确认对话框。
3. 单击“确认”，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。

13.4.3 HSS 为什么没有检测到攻击?

- 如果您的主机在开启HSS之前已被入侵，HSS可能无法检测出来。
- 如果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，如果攻击为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）。

13.4.4 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

- 如果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，默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。
- 如果您确认源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“检测与响应 > 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。

  如果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。如果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。

13.4.5 未手动解除的 IP 拦截记录，为什么显示已解除?

如果被拦截的IP在12小时内没有再继续暴力破解，HSS就会自动解除IP拦截。

13.4.6 恶意程序检测、隔离查杀周期是多久?

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。

说明

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产品功能。
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。

13.4.7 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。

13.4.8 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，且勒索病毒攻击发展迅速，目前没有任何工具能100%的防护服务器免受攻击。

建议您合理使用勒索病毒防护工具（如企业主机安全），并提升自身的“免疫力”，以消减勒索攻击造成的损害。

详细操作请参考**勒索病毒防护概述**。

13.4.9 如何为高危命令执行类告警添加白名单?

如果您在服务器上执行了正常业务相关命令，HSS进行“高危命令执行”告警，您可以添加白名单，避免告警。

添加命令告警白名单方式如下：

1. 登录管理控制台。
2. 在控制台左上角，单击 图标，选择区域或项目。
3. 在页面左上角单击 ，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。
4. 在左侧导航树中选择“安全运营 > 策略管理”，进入“策略管理”页面。
5. 找到服务器对应防护版本的策略组，单击策略组名称，进入策略组管理页面。
6. 单击“实时进程”策略名称。
7. 添加命令白名单。参数说明如下：
   - 进程全路径或程序名：填写进程的全路径或者程序名称，例如/usr/bin/sleep或sleep。
   - 命令行正则表达式：填写需要加白的命令行的正则表达式，例如^[A-Za-z0-9[:space:]*\\.\\\":_'\\(>=-]+$
8. 单击“确认”，保存修改。

13.5 异常登录

13.5.1 添加登录白名单后，还有异地登录告警?

HSS提供的“SSH登录IP白名单”、“登录告警白名单”和“异地登录”功能，功能差异如**表13-10**所示。

表 13-10 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。 请确保将所有需要发起SSH登录的IP地址都加入白名单中。	-
登录告警白名单	将IP加入登录告警白名单，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“检测与响应 > 白名单管理 > 登录告警白名单”将IP加入登录告警白名单，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 > 主机安装与配置 > 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。

13.5.2 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“检测与响应 > 安全告警事件> 主机安全告警”，进入主机安全告警页面。

步骤5 在左侧类型栏选择“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

- Linux主机

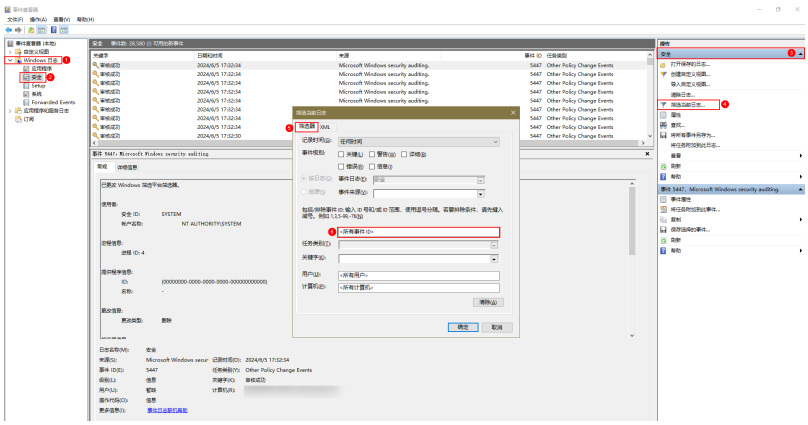
  您可以在“/var/log/secure”和“/var/log/message”路径下查看主机登录日志，或使用**last**命令查看登录记录中是否有异常登录。

- Windows主机

  您可以参考以下步骤查看主机登录日志：

  a. 打开“控制面板”。
  b. 选择“管理工具 > 事件查看器”，进入“事件查看器”页面。
  c. 在左侧导航栏选择“Windows日志 > 安全”，进入“安全”页面。
  d. 在右侧导航栏选择“安全 > 筛选当前日志”，弹出“筛选当前日志”窗口。
  e. 在“筛选器”页签，找到“<所有事件ID>”。

图 13-3 筛选器



f. 输入登录事件ID并单击“确认”，筛选需要查看的目标登录事件。

- 登录成功：4624
- 登录失败：4625

13.5.3 如何取消主机登录成功的告警通知?

- 如果您在“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。
- 如果您所有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。
- 如果系统账户由多人管理，或者不同主机由不同管理员负责管理，那么运维人员可能会因为频繁收到不相关的告警而对运维工作造成困扰，此时建议您登录企业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。

13.5.4 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。

13.5.5 如何确认入侵账号是否登录成功?

- 如果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“检测与响应”页面在线查看攻击IP的拦截情况。
- 如果想进一步确定，请参考如下方式：

- Linux主机

  您可以在“/var/log/secure”和“/var/log/message”路径下查看主机登录日志，或使用**last**命令查看登录记录中是否有异常登录。

- Windows主机

  您可以参考以下步骤查看主机登录日志：

  i. 打开“控制面板”。

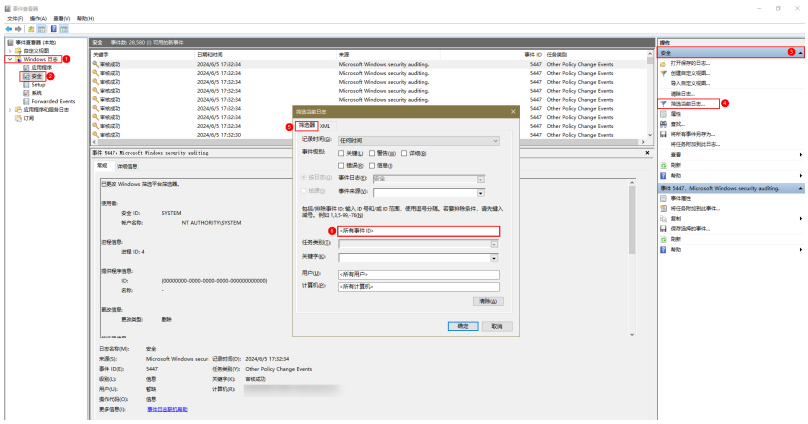
  ii. 选择“管理工具 > 事件查看器”，进入“事件查看器”页面。

  iii. 在左侧导航栏选择“Windows日志 > 安全”，进入“安全”页面。

  iv. 在右侧导航栏选择“安全 > 筛选当前日志”，弹出“筛选当前日志”窗口。

  v. 在“筛选器”页签，找到“<所有事件ID>”。

  图 13-4 筛选器

  vi. 输入登录事件ID并单击“确认”，筛选需要查看的目标登录事件。

  - 登录成功：4624
  - 登录失败：4625

13.6 账户暴力破解

13.6.1 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 ： SQL Server(暂不支持自动拦截) 、RDP
- Linux系统：MySQL、vfstpd、SSH

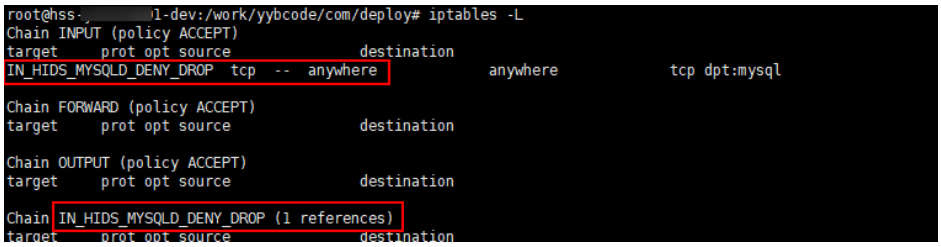
如果您的服务器上安装了MySQL、vfstpd或SSH，开启主机安全防护之后，Agent会在iptables中新增一些规则，用于暴力破解防护。当检测到暴破行为后会将暴破IP加入到阻断列表里面。

- MySQL新增规则：IN_HIDS_MYSQLD_DENY_DROP
- vfstpd新增规则：IN_HIDS_VSFTPD_DENY_DROP

- SSH新增规则：如果主机上的SSH不支持TCP Wrapper的拦截方式，SSH会使用iptables进行拦截，因此会在iptables中新增IN_HIDS_SSHD_DENY_DROP规则；如果您配置了SSH登录白名单，则会在iptables中新增IN_HIDS_SSHD_DENY_DROP、IN_HIDS_SSHD_WHITE_LIST两条规则。

以MySQL为例，新增的规则如**图 MySQL新增规则**所示。

图 13-5 MySQL 新增规则



说明

不建议删除已添加的iptables规则，如果删除iptables规则，HSS将无法防护MySQL、vfstpd或SSH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，如果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，默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。

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“检测与响应 > 安全告警事件”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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“检测与响应 > 安全告警事件”，进入安全告警事件页面。

步骤5 选择查看主机或容器的暴力破解检测结果。

- 查看主机的暴力破解检测结果
  a. 选择主机告警事件页签，进入主机告警事件页面。
  b. 在左侧类型栏，选择“用户异常行为 > 暴力破解”，查看防护的主机上的暴力破解告警事件记录。
  c. 单击已拦截IP区域的数值，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

       默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。
- 查看容器的暴力破解检测结果
  a. 选择容器告警事件页签，进入容器告警事件页面。
  b. 在左侧类型栏，选择“用户异常行为 > 暴力破解”，查看防护的容器上的暴力破解告警事件记录。

----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**。

  如果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。如果再次发生多次密码输错，该IP会再次被HSS拦截。

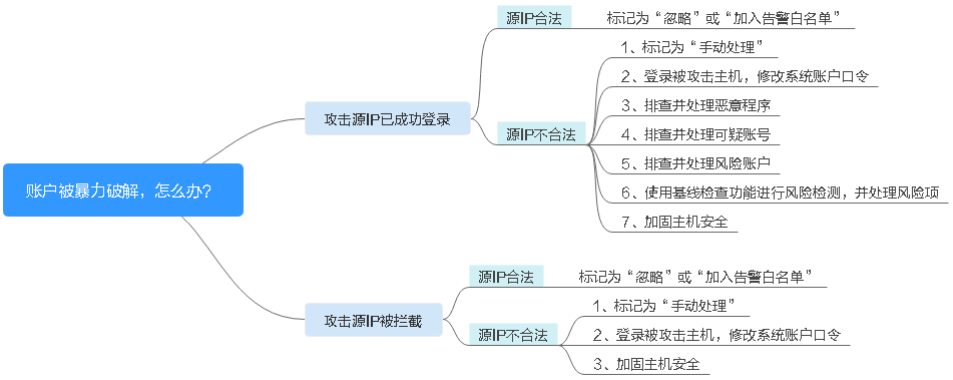
13.6.2 账户被暴力破解，怎么办?

- 如果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。
- 如果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 13-6 排查思路



账户被暴力破解，攻击源 IP 已成功登录

如果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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 判断源IP的合法性。

1. 在左侧导航栏选择“检测与响应 > 安全告警事件”页面，进入安全告警事件页面。
2. 在事件类型栏选择“用户异常行为 > 异常登录”，筛选异常登录告警事件。
3. 单击告警事件名称，弹出告警事件详情页面，查看成功登录主机的源IP是否为合法IP。
   - 如果源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。
   - 如果源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5 排查并处理恶意程序。

1. 在左侧导航栏选择“检测与响应 > 安全告警事件”页面，进入安全告警事件页面。
2. 在左侧类型栏选择“恶意软件 > 未分类恶意程序”，筛选未分类恶意程序告警事件。
3. 选择查看告警名称为“恶意程序”的告警事件，排查系统是否被植入了恶意程序。

   单击告警名称，可查看告警事件详细信息。
   - 如果被植入了恶意程序，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，在目标恶意程序告警事件所在行的“操作”列，单击“处理”，选择“隔离查杀”，立即终止恶意程序进程。

- 如果没有被植入恶意程序，请执行步骤6。

步骤6 排查账号可疑变动记录。

1. 在左侧导航栏选择“资产管理 > 主机指纹”，进入主机指纹页面。
2. 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7 排查并处理非法账号。

1. 在左侧导航栏选择“检测与响应 > 安全告警事件”，进入安全告警事件页面。
2. 在左侧类型栏选择“用户异常行为 > 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8 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HSS基础版及以上防护，HSS会为您的主机提供暴力破解防护。

基础版以上版本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：当同一IP地址在30秒内连续输入错误密码达5次及以上，或者1小时内累计输入错误密码达15次及以上时，HSS将不区分具体的登录用户，根据最后一次尝试登录的用户名进行告警，并拦截登录源IP（默认拦截12小时），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

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。如果关闭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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 选择“检测与响应 > 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5 建议您立即确认源IP是否是已知的合法IP。

- 如果源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“加入登录告警白名单”。

    将该事件“忽略”或者“加入登录告警白名单”，均不会解除拦截的IP。
  - 如果需要解除拦截的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。默认拦截时间为12小时。
- 如果源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?**

13.6.3 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 13-11 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。

13.6.4 如何手动解除误拦截 IP?

当同一IP地址在30秒内连续输入错误密码达5次及以上，或者1小时内累计输入错误密码达15次及以上时，HSS将不区分具体的登录用户，根据最后一次尝试登录的用户名进行告警，并拦截登录源IP（默认拦截12小时），禁止其再次登录，防止主机因账户破解被入侵。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。

如果已拦截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。如果再次发生多次密码输错，该IP仍会被HSS拦截。

手动解除拦截 IP

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树中，选择“检测与响应 > 安全告警事件 > 主机安全告警”。

步骤5 在安全告警统计栏，单击“已拦截IP”。

步骤6 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。

步骤7 等待1~2分钟，查看目标攻击源IP的“拦截状态”显示为“已解除拦截”，表示解除拦截成功。

----结束

13.6.5 频繁收到 HSS 暴力破解告警

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 13-12 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RDP、SQL Server、MySQL、vsftpd、SSH等账户遭受的口令破解攻击。

默认情况下，当同一IP地址在30秒内连续输入错误密码达5次及以上，或者1小时内累计输入错误密码达15次及以上时，HSS将不区分具体的登录用户，根据最后一次尝试登录的用户名进行告警，并拦截登录源IP（默认拦截12小时），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HSS基础版以上（不含基础版）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“检测与响应 > 安全告警事件”页面，单击“已拦截IP”上方的数值进行查看。

13.6.6 暴力破解记录未显示修改后的端口

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。

13.7 基线检查

13.7.1 关闭弱口令检测策略后，还有弱口令事件告警?

如果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，该弱口令事件不会再重复出现。

如果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。

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

安装 PAM

如果当前主机中未安装PAM（Pluggable Authentication Modules），HSS就无法为主机提供口令复杂度策略检测功能。未安装PAM的主机，HSS会在“风险预防 > 基线检查 > 口令度复杂度策略检测”页面，提供的建议中提示需安装PAM。

如果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13-13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 13-13 参数说明

参数	说明	示例
minlen	口令最小长度配置项。 如果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

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

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

13.7.3 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。
- 当策略应用于服务器时，域策略优先生效于服务器上本地定义的策略。

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 使用Windows+R组合键，打开运行界面。

步骤4 输入“cmd”并单击“确认”，进入命令提示符窗口。

步骤5 执行以下命令，刷新策略。

gpupdate/force

刷新成功后，以上设置被应用于系统中。

----结束

13.7.4 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. 登录管理控制台。

  b. 在控制台左上角，单击图标，选择区域或项目。

  c. 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

  d. 在左侧导航栏，选择“资产管理>主机管理”，进入“主机管理”页面。

  e. （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

  f. 在云服务器页签，单击目标云服务器名称，查看服务器的详细信息，选择“基线检查 > 配置检查”。

  g. 单击目标基线名称前的 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，建议您目标检查项所在行的“操作”列，单击“验证”，待验证完成后，查看配置项修复结果。

13.7.5 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。

查看配置检查报告

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，进入“基线检查”页面。

步骤5 在“配置检查”页签，单击配置检查基线名称，进入检测规则详情页面。

步骤6 在目标检查项所在行的“操作”列，单击“检测详情”，查看检查项详细信息和受影响服务器。

步骤7 您可以根据检查项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

13.7.6 出现弱口令告警，怎么办?

如果您收到弱口令告警，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，如果密码被破解，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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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

系统名称	修改登录口令	说明
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 **passwd [<user>]**	“user”为登录用户名。如果不输入登录用户名，则修改的是当前用户的口令。 命令执行完成后，请根据提示输入新的口令。
MySQL数据库	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 **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。 如果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>;**	“password”为登录口令。 • 如果已存在登录口令，则将其修改为复杂口令。 • 如果不存在登录口令，则添加为新口令。
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

13.7.7 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，如果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。

13.8 网页防篡改

13.8.1 为什么要添加防护目录?

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

13.8.2 如何修改防护目录?

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航栏中，选择“主机防御 > 网页防篡改”，进入“网页防篡改”界面。

----结束

13.8.3 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。

13.8.4 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。

13.8.5 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，如果已生成该文件，则重启Tomcat即可成功开启动态网页防篡改。

如果您开启网页防篡改后，状态是“已开启未生效”：

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

13.8.6 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13-14所示。

表 13-14 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 如果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 如果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

13.9 容器安全

13.9.1 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。

关闭容器版防护

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 （可选）如果您已开通企业项目，可在页面上方“企业项目”下拉框中选择企业项目，查看目标企业项目下的相关信息和数据。

步骤6 在目标服务器所在行的“操作”列，单击“关闭防护”。

您也可以勾选多个目标服务器，并在列表上方单击“关闭防护”，批量关闭防护。

步骤7 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8 关闭后在“资产管理 > 容器管理 > 容器节点管理”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

----结束

13.9.2 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 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 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6 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

13.9.3 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
```

步骤5 重启kube-apiserver使配置生效。

不同环境下重启kube-apiserver的方法不同，请您根据实际情况进行重启。

如果kube-apiserver是通过systemd管理的，可执行以下命令重启服务。

```
systemctl restart kube-apiserver.service
```

----结束

13.9.4 容器集群防护插件卸载失败怎么办?

故障原因

当集群网络异常或插件正在工作时，通过HSS控制台卸载插件可能会失败。

解决措施

在可以使用kubectl命令访问API Server的任意集群节点执行如下操作，即可卸载容器集群防护插件。

步骤1 登录任意一个可以使用Kubectl命令访问API Server的集群节点。

步骤2 在/tmp目录下新建plugin.yaml文件，并将如下脚本内容拷贝至plugin.yaml文件中。

```
apiVersion: v1
kind: Namespace
metadata:
  labels:
    admission.gatekeeper.sh/ignore: no-self-managing
    control-plane: controller-manager
    gatekeeper.sh/system: "yes"
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/audit-version: latest
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/enforce-version: v1.24
    pod-security.kubernetes.io/warn: restricted
    pod-security.kubernetes.io/warn-version: latest
  name: gatekeeper-system
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assign.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignimage.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignmetadata.mutations.gatekeeper.sh
```

```
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: configs.config.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constraintpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplates.templates.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplate.expansion.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: modifyset.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
```

```
  labels:
    gatekeeper.sh/system: "yes"
  name: mutatorpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: providers.externaldata.gatekeeper.sh
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
  namespace: gatekeeper-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-mutating-webhook-configuration
---
apiVersion: admissionregistration.k8s.io/v1
```

```
kind: ValidatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-validating-webhook-configuration
```

步骤3 在/tmp目录下新建uninstall.sh文件，并将如下脚本内容拷贝至uninstall.sh文件中。

```
#!/bin/bash
kubectl delete -f /tmp/plugin.yaml
kubectl delete ns cgs-provider
```

步骤4 执行如下命令卸载容器集群防护插件。

```
bash /tmp/uninstall.sh
```

回显如下图类似信息，表示插件卸载完成。

```
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
```

----结束

13.10 安全配置

13.10.1 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，请按如下步骤操作：

a. 登录控制台。
b. 在左侧导航树选择“检测与响应 > 安全告警事件”，进入“安全告警事件”页面。
c. 选择“主机告警事件”页签，单击“已拦截IP”区域的数值，弹出“已拦截IP”页面。
d. 选中目标攻击源IP，单击列表上方“解除拦截”，解除IP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

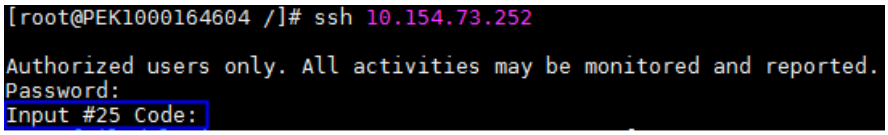
13.10.2 如何使用双因子认证?

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 13-7 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. 如果已开启双因子认证，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。

13.10.3 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
     如果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。

13.10.4 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

说明

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。

13.10.5 如何添加双因子认证的手机号或邮箱？

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。

13.10.6 是否可以不开启 HSS 告警通知？

可以不开启HSS告警通知。

如果您开启了主机防护，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。如果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，如果您想设置告警通知，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，如果您不想收到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。

13.10.7 如何修改告警通知的通知项?

开启主机安全防护后，如果您不想收到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。

修改告警通知的通知项

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 选择“告警配置”页签，进入“告警配置”页面。

步骤6 选择无需发送告警的屏蔽事件。

步骤7 选择消息主题。

步骤8 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。

如果涉及多个**消息通知主题**更改，请重复**步骤6**~**步骤8**操作。

----结束

13.10.8 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少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。

如果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。

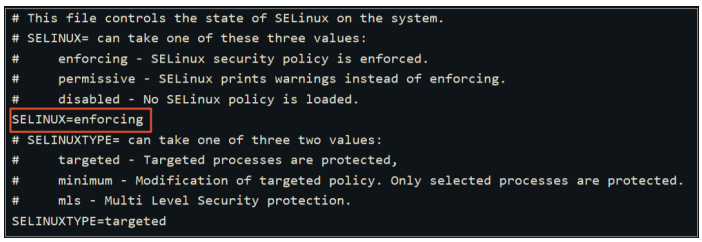
- **永久关闭**

  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 13-8 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

13.11 其他

13.11.1 如何使用 Windows 远程桌面连接工具连接 Windows 主机?

使用Windows远程连接工具连接Windows主机的操作如下：

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

13.11.2 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。	10MB	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。	10MB	保留8个最新的日志文件。	
upgrade.log	记录版本升级时相关日志。	10MB	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）。	100kB	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）。	10kB	保留2个最新的日志文件。	
engine.log	记录服务退出时相关日志。	10kB	保留2个最新的日志文件。	

13.11.3 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13-9所示的日志记录。

图 13-9 日志记录

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

----结束

13.11.4 如何启停 Agent 自保护策略?

约束限制

- 仅Linux Agent版本≥3.2.12或Windows Agent版本≥4.0.18时，支持Agent自保护功能。
- Windows系统的Agent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Agent自保护才会生效。确认或开启这些功能的具体操作请参见：
  - 勒索病毒防护：。
  - AV检测、HIPS检测：。
- 开启自保护策略后的影响如下：
  - **Windows系统**
    - 不能通过控制面板卸载Agent，支持通过企业主机安全控制台卸载Agent。
    - Agent安装路径C:\Program Files\HostGuard下除了log目录、data目录（如果Agent升级过，则包含upgrade目录）外的其他目录无法访问。
    - 企业主机安全相关的进程无法被强制结束。
  - **Linux系统**
    - 不能通过命令卸载Agent，支持通过企业主机安全控制台卸载Agent。
    - 通过命令停止或重启企业主机安全，需要输入验证码（验证码为执行停止或重启命令后界面回显的字符）。
    - 企业主机安全相关的进程信息将被隐藏。

操作步骤

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 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5 单击目标策略组名称，进入策略组详情页面。

目标策略组指的是您需要开启企业主机安全自保护的服务器所属策略组。

- 如果您未新建新的策略组，那您的服务器都以系统默认的策略组进行防护，您选择系统默认的策略组。“tenant_XXX_XXX_default_policy_group”即可。
- 如果您新建了策略组，您要选择您的服务器所属策略组，您可以通过以下方式确认服务器所属策略组：
  a. 在左侧导航栏选择。
  b. 在云服务器页签，查看服务器所属策略组。

步骤6 在自保护策略所在行的“操作”列，单击“开启”或“关闭”。

步骤7 在弹窗中，单击“确认”。

----结束

13.11.5 HSS 自保护无法关闭怎么办?

问题根因

正常情况下，您可以在策略组中直接关闭自保护功能，具体操作请参见**如何启停Agent自保护策略?** 。

但是，当服务器网络不通时，会导致Agent无法通信（Agent接收不到HSS控制台下发的关闭自保护的指令），从而使得Windows自保护无法关闭。

解决方法

步骤1 登录管理控制台。

步骤2 在控制台左上角，单击图标，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 企业主机安全 HSS”，进入“企业主机安全”页面。

步骤4 在左侧导航树选择“资产管理 > 主机管理”。

步骤5 在“云服务器”页面，单击服务器防护列表右上角，勾选展示“Agent ID”。

步骤6 在服务器防护列表上方，输入服务器名称或ID，按回车键，查找待关闭HSS自保护的Windows服务器。

步骤7 在目标Windows服务器所在行的Agent ID列，复制Agent ID前八位字符。

步骤8 使用Administrator身份运行cmd命令行窗口。

步骤9 执行如下命令，关闭HSS自保护。

"C:\Program Files\HostGuard\bin\HssClient.exe" 1234abcd

说明

命令中包含的**1234abcd**表示Agent ID前八位字符。以Agent ID的前八位字符作为执行HSSClient.exe时的验证码，是为了防止恶意程序关闭自保护和用户误操作而做的验证防护，只有输入正确的Agent ID前八位字符才能关闭自保护

步骤10 界面回显“Disable self protect succeed.”表示关闭HSS自保护成功。

----结束

A 修订记录

发布日期	修改说明
2025-1-30	第一次正式发布。