主机安全服务

用户指南

文档版本 21

发布日期 2024-03-25

华为云计算技术有限公司

商标声明


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

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 接入 HSS

1.1 接入指引

主机/容器接入主机安全服务HSS进行防护的流程如**图 接入HSS流程**所示。

图 1-1 接入 HSS 流程

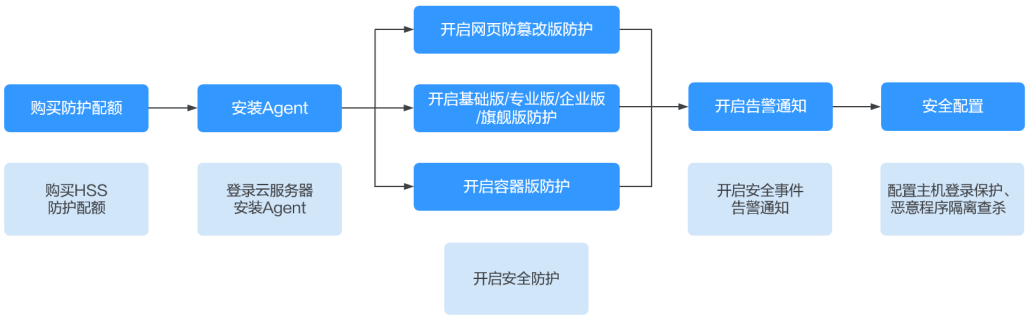


表 1-1 接入 HSS 流程说明

序号	步骤	说明
1	**购买防护配额**	主机安全服务HSS提供基础版、专业版、企业版、旗舰版、网页防篡改版和容器版供您选择，每个版本支持的功能特性存在差异，您需要根据对主机或容器的防护需求，购买对应的防护版本。HSS各版本的区别请参见**服务版本差异**。
2	**安装Agent**	Agent是主机安全服务提供的一款软件，安装在云服务器上，用于与主机安全服务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，您才能使用主机安全服务。
3	**开启防护**	完成购买防护配额、安装Agent后，HSS还未对云服务器进行防护，您需要为云服务器开启防护。

序号	步骤	说明
4	开启告警通知	默认情况下，HSS在防护主机/容器过程中发现的安全风险展示在管理控制台，您需要登录管理控制台查看。如果您需要及时了解主机/容器的安全风险，可以开启告警通知，开启后，HSS会将安全风险通过短信或邮件的方式发送给您。
5	常用安全配置	您可以根据实际业务需求，配置如下云服务器安全保护项，提升云服务器安全性： • 常用登录地：允许常用登录地登录云服务器，对非常用登录地登录云服务器的行为进行告警。 • 常用登录IP：允许常用登录IP登录云服务器，对非常用登录IP登录云服务器的行为进行告警。 • SSH登录IP白名单：允许白名单内的IP通过SSH登录云服务器，拒绝白名单以外的IP登录。 • 双因子认证：双因素身份验证机制，结合短信/邮箱验证码，对登录云服务器行为进行二次认证。 • 恶意程序隔离查杀：对识别出的后门、木马、蠕虫等恶意程序进行自动隔离查杀。

1.2 购买防护配额

通过本节介绍，您将了解如何购买主机防护配额。

购买说明

- 配额只能在购买时所选择的区域使用。
- 一个配额只能绑定一个主机，且只能绑定Agent在线的主机。
- HSS暂仅支持为Docker和Containerd容器提供安全防护，在购买容器版配额时请确认您的容器类型。
- 为了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都部署主机安全服务。
- 购买主机安全防护配额后，请到主机安全服务控制台“主机管理”页面开启主机防护。
- 购买网页防篡改赠送旗舰版，包含旗舰版所有功能。

须知

- 为防止未防护主机感染勒索、挖矿等病毒后传染给其他主机，导致企业内网整体沦陷，**建议您的云上主机全部署主机安全服务**。
- 购买企业版选择“按需计费”模式时，当ECS关机后，主机安全服务将停止计费。

购买场景

表 1-2 配额购买场景

主机类型	主机所在区域	如何购买配额
华为云弹性云服务器ECS 华为云裸金属服务器BMS 华为云云耀云服务器HECS 华为云云桌面Workspace	在主机防护支持的区域	请在ECS/BMS/HECS/Workspace所在区域购买主机防护配额。 HSS不支持跨区域使用，主机与防护配额不在同一区域，请退订配额后，重新购买主机所在区域的配额。
第三方云主机	-	目前仅部分区域支持接入非华为云主机，具体区域请参见**哪些区域支持接入非华为云主机?**，请在支持接入非华为云主机的区域购买主机防护配额，然后使用非华为云主机的Agent安装方式，将主机接入配额所在区域。
线下主机	-	

前提条件

账号具备BSS Administrator、HSS Administrator权限，如果没有相应权限请使用主账号购买配额或使用主账号对子账号进行授权后进行购买配额。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全合规 > 主机安全服务”，进入主机安全服务界面。

步骤3 在界面右上角，单击“购买主机安全”，进入“购买主机安全配额”界面。

步骤4 在“购买主机安全配额”界面，选择购买的规格，参数说明如**表 购买主机安全参数说明**所示。

表 1-3 购买主机安全参数说明

参数名称	参数说明	取值样例
计费模式	根据您的需求选择“包年/包月”或“按需”计费模式。 ● 包年/包月：在版本选择时可选择基础版、专业版、企业版、旗舰版、网页防篡改版和容器版，单次购买固定的版本使用周期，费用方面比“按需”付费方式每月优惠30%，如果您长期使用，建议包周期购买。 ● 按需：当前购买页支持选择企业版，开启防护需要在服务器列表页开启。按实际使用的时长收费，以小时为单位，每小时整点结算，不设最低消费标准。 **说明** 开启按需防护步骤： 1. 在购买页选择按需，默认选择企业版，在页面右下角单击“立即开通”，页面跳转到云服务器列表页面。 2. 在云服务器列表的“操作”列单击“开启防护”，“计费模式”选择“按需计费”，“主机安全版本”选择“企业版”。 3. 确认信息无误，单击“确认”完成开启。	包年/包月
区域	● 配额的“区域”建议与主机的“区域”相同。	中国-香港
版本选择	支持购买的版本有“基础版”、“专业版”、“企业版”、“旗舰版”、“网页防篡改版”和“容器版”。各版本的功能差异详情请参见服务版本差异。 **须知** ● 首次开启基础版可免费体验30天，体验结束后进行购买即可。 ● 如果您购买的是基础版/企业版/旗舰版配额，请在“资产管理 > 主机管理 > 云服务器”页面开启防护。 ● 如果您购买的是网页防篡改版配额，请在“主动防御 > 网页防篡改 > 防护配置”页面开启防护。 ● 如果您购买的是容器版配额，请在“资产管理 > 容器管理 > 容器节点管理”页面开启防护。	企业版
企业项目	企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请联系您的客户经理申请开通。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 从下拉列表中选择所在的企业项目。 **说明** ● 选择企业项目后，产生的费用和资源均在企业项目内。 ● “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 ● 只有注册的华为账号购买HSS时，“企业项目”下拉列表中才可以选择到“default”。	default

参数名称	参数说明	取值样例
购买时长	• 根据您的需求选择时长，“按需”模式无需选择。 • 为避免因服务到期未及时续费导致您的主机遭受攻击，建议勾选“自动续费”。 • 勾选“自动续费”后，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。 • 如果未勾选自动“自动续费”，在即将到期时，请手动续费。	1年
防护主机数量	输入购买主机安全服务防护配额的数量，“按需”模式无需选择。 **须知** • 为防止未防护主机感染勒索、挖矿等病毒后传染给其他主机，导致企业内网整体沦陷，购买的主机安全服务数量建议与使用的主机数量保持一致。 • 购买成功后不支持增加配额，如需增加配额，请重新购买即可。	20
标签	标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。 如果需要该功能，您的账号需要具备TMS administrator权限，没有该权限您无法为防护配额添加标签并且界面会有“permission error”的错误提示。 “按需”模式无需填写。	data
配额管理	开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。 • 主机：按“旗舰版 > 企业版 > 专业版 > 基础版”的顺序自动绑定空闲可用的包年/包月配额。 • 容器节点：按“容器版 > 旗舰版 > 企业版 > 专业版 > 基础版”的顺序自动绑定空闲可用的包年/包月配额。	勾选

步骤5 在页面右下角，单击“立即购买”，进入“订单确认”界面。

费率标准请参见**产品价格详情**。

步骤6 确认订单无误后，请阅读《主机安全免责声明》并勾选“我已阅读并同意《主机安全免责声明》”。

步骤7 单击“去支付”，进入付款页面，单击“确认付款”，完成支付，购买成功。

----结束

后续操作

配额购买完成后，您需要为主机安装Agent并开启防护，详细操作请参见**安装Agent**、**开启防护**。

相关操作

当您购买的配额版本或区域有误时，您可以退订已购买配额，再重新购买正确的配额。

1.3 安装 Agent

1.3.1 Agent 概述

什么是 Agent?

Agent是主机安全服务提供的一款软件，安装在云服务器上，用于与主机安全服务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。如果不安装Agent，将无法使用主机安全服务。

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**支持的操作系统**。对于Agent不支持的操作系统，与Agent可能存在兼容性问题，建议重装或者升级为Agent支持的操作系统版本，以便获得主机安全服务更好的服务体验。

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 1-4 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 1-5 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

安装 Agent

- **单台Linux主机安装Agent**
- **单台Windows主机安装Agent**
- **批量Linux主机安装Agent**

1.3.2 安装 Agent 前配置确认

安装Agent对安全组出方向端口、DNS服务器地址以及第三方安全软件等有限制要求，为了保证您能成功安装Agent，请参考**安装Agent前配置确认**确认能符合对应的要求后，再安装Agent。

安装 Agent 前配置确认

步骤1 请确认服务器的操作系统在Agent**支持的操作系统**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，且可正常访问公网。

步骤3 请确认预备安装Agent的磁盘容量大于300M。

Agent默认安装路径如下：

- 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。

服务器默认允许访问该端口，您需要确认是否修改了规则。查看、修改安全组出方向规则的操作请参见**修改安全组**。

步骤5 请确认您服务器的DNS服务器地址为华为云内网DNS地址。

查看、修改DNS服务器地址的操作请参见**修改DNS（服务器本地方式）**或**修改DNS（管理控制台方式）**。

步骤6 请您关闭或卸载第三方安全软件。

如果服务器安装了第三方安全软件，可能会导致主机安全服务Agent无法正常安装。

步骤7 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

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 在管理控制台左上角选择区域和项目。

步骤3 在管理控制台左上角，单击，选择“计算 > 弹性云服务器”。

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“配置规则”。

进入目标安全组详情页面。

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 1-6 安全组规则

优先级	策略	类型	协议端口		目的地址	描述
1	允许	IPv4	TCP	10180	100.125.0.0/16	与HSS服务端进行通信。

----结束

修改 DNS（服务器本地方式）

安装Agent时，需要确保DNS服务器地址为华为云内网DNS地址。您可以查看、修改DNS服务器地址。

- Linux服务器

  本节介绍通过Linux命令行添加域名解析地址至resolv.conf文件的操作步骤和方法。

  a. 使用root账号，登录服务器。

  b. 执行以下命令，打开resolv.conf文件。

  vi /etc/resolv.conf

  c. 执行以下命令添加域名解析地址。

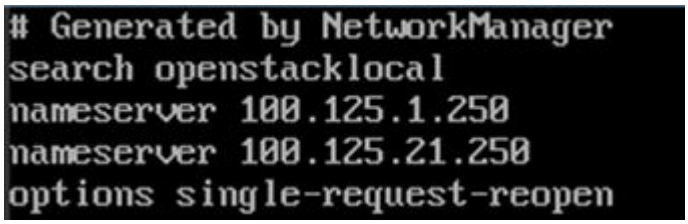
  nameserver 华为云内网DNS地址

  说明

  不同区域的内网DNS地址不同，详细请参考**华为云内网DNS地址**。

  以“华北-北京一”为例，完整命令为“nameserver 100.125.1.250”和“nameserver 100.125.21.250”。

图 1-2 添加域名解析地址



d. 输入“wq”，按“Enter”保存并退出。

- Windows服务器

  本节介绍通过Windows图形化界面添加域名解析地址的操作步骤和方法。

  a. 使用管理员账号，登录服务器。
  b. 打开“控制面板 > 网络与共享中心”，单击“更改适配器配置”。
  c. 鼠标右键单击使用的网络，打开设置。
  d. 双击“Internet协议版本4（TCP/IPv4）”,进入属性界面。
  e. 勾选“使用下面的DNS服务器地址”，然后输入华为云内网DNS服务器地址。

  说明

  不同区域的内网DNS地址不同，详细请参考**华为云内网DNS地址**。

修改 DNS（管理控制台方式）

本节以ECS为例介绍登录管理控制台后修改DNS配置的操作步骤和方法。

1. 登录管理控制台。
2. 在管理控制台左上角选择区域和项目。
3. 在管理控制台左上角，单击，选择“计算 > 弹性云服务器”。

   进入“弹性云服务器”页面。
4. 在弹性云服务器列表中，单击目标ECS名称。
5. 在ECS服务器详情页面，单击“虚拟私有云”对应的VPC名称。

   进入“虚拟私有云”页面。
6. 在“虚拟私有云”页面的VPC列表中，单击“子网”列的子网数量。

   进入“子网”页面。
7. 在“子网”页面，单击子网列表中的子网名称。

   在子网“基本信息”的“网关和DNS”区域可查看当前ECS服务器使用的DNS服务器地址。
8. 在子网“基本信息”的“网关和DNS”区域，单击“DNS服务器地址”后面的。
9. 修改子网的“DNS服务器地址”为华为云内网DNS。

   说明

   不同区域的内网DNS地址不同，详细请参考**华为云内网DNS地址**。

1.3.3 单台 Linux 主机安装 Agent

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单台Linux主机安装Agent。

前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考**修改云服务器的DNS服务器地址**和**华为云内网DNS地址**。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。
- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。

约束限制

- 主机安全服务支持防护64位主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见**支持的操作系统**。
- 华为云云桌面Workspace镜像中已预置HSS Agent，购买云桌面23.6.0及以后版本将会自动安装Agent，无需您手动安装。如果您购买的云桌面是23.6.0以前的版本，可以参照本文手动为云桌面安装Agent。

安装路径

在Linux操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装路径为“/usr/local/hostguard/”。

安装步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击  ，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

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 选择“Agent管理”页签。

步骤5 复制安装Agent命令。

- 华为云主机
  a. 单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。
  b. 在目标服务器的“操作”列，单击“安装Agent”。

图 1-3 安装 Agent

c. 在弹窗中，单击“复制”，复制安装Agent的命令。

- 非华为云主机

  说明

  a. 单击“接入多云资产”。

  图 1-4 接入多云资产

  b. 在Agent安装指南弹窗中，根据服务器操作系统选择并复制安装Agent的命令。

步骤6 远程登录待安装Agent的主机。

步骤7 粘贴复制的安装命令，以root权限执行，在主机中安装Agent。

如果界面回显信息如**图 Agent安装成功**所示，则表示Agent安装成功。

图 1-5 Agent 安装成功

```
Preparing...                          ########################################## [100%]
Updating / installing...
   1:hostguard-3.2.8-1                ########################################## [100%]
hostguard starting ...
memory cgroup is disabled
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
Hostguard is running...
Hostguard installed.
```

步骤8 执行以下命令，查看Agent的运行状态。

service hostguard status

如果界面回显如**图 Agent运行正常**所示，则表示Agent运行正常。

图 1-6 Agent 运行正常

```
your agent is in normal mod.
hostwatch is running
hostguard is running with normal mod
```


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

----结束

后续操作

安装Agent成功后，请为主机开启安全防护，详细操作请参考**开启防护**。

常见问题

- Agent状态及异常处理的详细操作请参见**Agent状态异常应如何处理?**
- Agent安装失败，请参见**Agent安装失败应如何处理?**
- 卸载Agent的详细操作请参见**如何卸载Agent?**

1.3.4 单台 Windows 主机安装 Agent

安装Agent后，您才能为云服务器开启主机安全防护。本章节为您介绍如何为单台Windows主机安装Agent。

前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考**修改云服务器的DNS服务器地址**和**华为云内网DNS地址**。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。
- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。

约束限制

- 主机安全服务支持防护64位主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见**支持的操作系统**。
- 华为云云桌面Workspace镜像中已预置HSS Agent，购买云桌面23.6.0及以后版本将会自动安装Agent，无需您手动安装。如果您购买的云桌面是23.6.0以前的版本，可以参照本文手动为云桌面安装Agent。

安装路径

在Windows操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认路径为“C:\Program Files\HostGuard”。

安装步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全合规 > 主机安全服务”，进入主机安全服务界面。

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

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 选择“Agent管理”页签。

步骤5 复制Agent安装包下载地址。

- 华为云主机
  a. 单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。
  b. 在目标服务器的“操作”列，单击“安装Agent”。

  图 1-7 安装 Agent

  c. 在弹窗中，单击“复制”，复制Agent安装包下载地址。
- 非华为云主机

  说明

  a. 单击“接入多云资产”。

  图 1-8 接入多云资产

  b. 在Agent安装指南弹窗中，根据服务器操作系统选择并复制Agent安装包下载地址。

步骤6 远程登录待安装Agent的主机。

步骤7 在待安装Agent的主机中，通过IE浏览器访问复制的Agent下载地址，下载Agent安装包并解压。

步骤8 使用管理员权限运行Agent安装程序。

步骤9 根据提示完成Agent安装。

对于非华为云主机，请安装Agent界面复制Org ID，如**图 获取Org ID（非华为云主机）**所示，在界面输入Org ID，然后按界面提示完成Agent安装。

须知

安装界面中务必保证Org ID正确，否则可能导致Agent安装后页面仍然显示未安装Agent。

图 1-9 获取 Org ID（非华为云主机）

步骤10 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”。

如果进程不存在，则表示Agent安装失败，请尝试重新安装Agent。安装成功后，Agent不会立即生效，需要等待3~5分钟左右控制台才会刷新。

----结束

后续操作

安装Agent成功后，请为主机开启安全防护，详细操作请参考**开启防护**。

常见问题

- Agent状态及异常处理的详细操作请参见**Agent状态异常应如何处理?**
- Agent安装失败，请参见**Agent安装失败应如何处理?**
- 卸载Agent的详细操作请参见**如何卸载Agent?**

1.3.5 批量 Linux 主机安装 Agent

主机安全服务支持批量为Linux主机安装Agent，避免安装Agent占用您过多的时间。暂不支持批量为Windows主机安装Agent，敬请谅解！

前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考**修改云服务器的DNS服务器地址**和**华为云内网DNS地址**。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。

- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。
- 待安装Agent的服务器支持SSH登录。

约束限制

- 主机安全服务支持防护64位主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见**支持的操作系统**。
- 华为云云桌面Workspace镜像中已预置HSS Agent，购买云桌面23.6.0及以后版本将会自动安装Agent，无需您手动安装。如果您购买的云桌面是23.6.0以前的版本，可以参照本文手动为云桌面安装Agent。

安装路径

在Linux操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装路径为“/usr/local/hostguard/”。

批量 Linux 服务器安装 Agent（控制台一键方式）

前提条件

- 待安装Agent的服务器所属VPC内已有一台Agent在线的服务器。如果没有Agent在线的服务器请参考**单台Linux主机安装Agent**，先为一台服务器安装Agent。
- 待安装Agent的所有服务器的账号密码相同，且已获取服务器的登录账号、端口、密码。

约束限制

单次最多可为50台服务器批量安装Agent。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 勾选需要所有目标服务器，并在列表上方单击“批量安装Agent”，弹出“批量安装Agent”对话框。

图 1-10 批量安装 Agent

步骤5 确认已选服务器信息，并单击“下一步”。

图 1-11 已选服务器

步骤6 输入“服务器root密码”和“服务器登录端口”。

说明

- 系统默认系统端口为22，如果需查询Linux SSH端口，远程登录目标服务器后，在Linux服务器中执行以下命令即可查询。
  ```
  cat /etc/ssh/sshd_config | grep Port
  ```
- 如果服务器密码包含字符“$”，请填写为“\$”。

步骤7 单击“确认”，服务器将自动执行Agent安装。

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

----结束

批量 Linux 服务器安装 Agent（命令行安装方式）

前提条件

已获取服务器的登录账号、端口、密码。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务界面。

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装与配置”界面。

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 选择“Agent管理”页签。

步骤5 单击“接入多云资产”。

图 1-12 接入多云资产

步骤6 在“Agent安装指南”页面中，复制“批量安装”的命令。

图 1-13 复制批量安装命令

步骤7 远程登录待安装Agent的华为云主机。

须知

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

/bin/expect -v

步骤8 执行以下命令进入tmp目录。

cd /tmp/

步骤9 按照以下命令格式执行命令，创建文件“linux-host-list.txt”并将需要批量安装的节点私有ip添加至创建的文件中。

- 命令格式一：echo "IP地址 端口 root rootPassword" >> linux-host-list.txt
  完整命令示例：echo "127.8.10.8 22 root rootPassword" >> linux-host-list.txt
- 命令格式二：echo "IP地址 端口 user userPassword rootPassword" >> linux-host-list.txt
  完整命令示例：echo "127.8.10.9 22 user userPassword rootPassword" >> linux-host-list.txt

上述命令格式任选择一种即可；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 "127.8.10.1 22 root rootPassword" >> linux-host-list.txt

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

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

步骤10 键入回车保存IP，执行以下命令查询是否添加完成。

cat linux-host-list.txt

步骤11 粘贴6复制的安装命令，以root权限执行，在主机中安装Agent。

如果界面回显如下信息，则表示Agent安装成功。

remote_install finished. [OK]

步骤12 前往“安装与配置 > Agent管理”页面，查看目标服务器的“Agent状态”为“在线”，表示Agent服务运行正常。

步骤13 执行以下命令，删除“linux-host-list.txt”文件，避免泄露密码。

rm -rf linux-host-list.txt

----结束

1.4 开启防护

1.4.1 开启基础版/专业版/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。

如果您购买的是网页防篡改版，请在“主动防御 > 网页防篡改 > 防护配置”页面开启防护，具体请参见**开启网页防篡改版防护**。

说明

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

检测周期

主机防护每日凌晨会进行全量检测。

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

- “主机安全服务 > 资产管理 > 主机管理”页面“云服务器”中“Agent状态”为“在线”。
- 如果开启包周期防护，请确认已在所选区域购买了充足可用的配额。
- 为达到更好的防护效果，建议在开启防护前进行安全配置。

约束条件

- Linux操作系统

  使用鲲鹏计算EulerOS（EulerOS with ARM）的主机，在遭受SSH账户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警。
- Windows操作系统
  - 开启主机防护时，需要授权开启Windows防火墙，且使用主机安全服务期间请勿关闭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 在页面左上角选择“区域”，单击，选择“安全合规 > 主机安全服务”，进入主机安全服务界面。

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

说明

云服务器列表仅显示以下主机的防护状态：

- 在所选区域购买的华为云主机
- 已接入所选区域的非华为云主机

步骤4 选择所需开启安全防护的主机，单击“操作”列“开启防护”。

您可以根据自己的实际场景选择“包年/包月”或者“按需计费”，开启主机防护。

说明

- 按需计费：仅支持选择企业版。
- 包年/包月模式出现配额不足时需购买主机安全配额；
- 如果Linux主机安装的Agent版本为3.2.10及以上版本或Windows主机安装的Agent版本为4.0.22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，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）；此外，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**开启勒索备份**。

- **包年/包月**

  在“开启方式”对话框中，“计费模式”选择“包年/包月”，选择目标版本、分配防护配额，阅读并确认“《主机安全免责声明》”。

  “选择配额”分配方式：

  - 随机分配：下拉框选择“随机选择配额”，系统优先为主机分发服务剩余时间较长的配额。
  - 指定分配：下拉框选择具体配额ID，您可以为主机分配指定的配额。

- **按需计费**

  在“开启方式”对话框中，“计费模式”选择“按需计费”，选择目标版本，阅读并勾选“《主机安全免责声明》”。

步骤5 单击“确认”，开启防护。开启主机安全防护后，请在控制台上查看主机安全服务的开启状态。

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

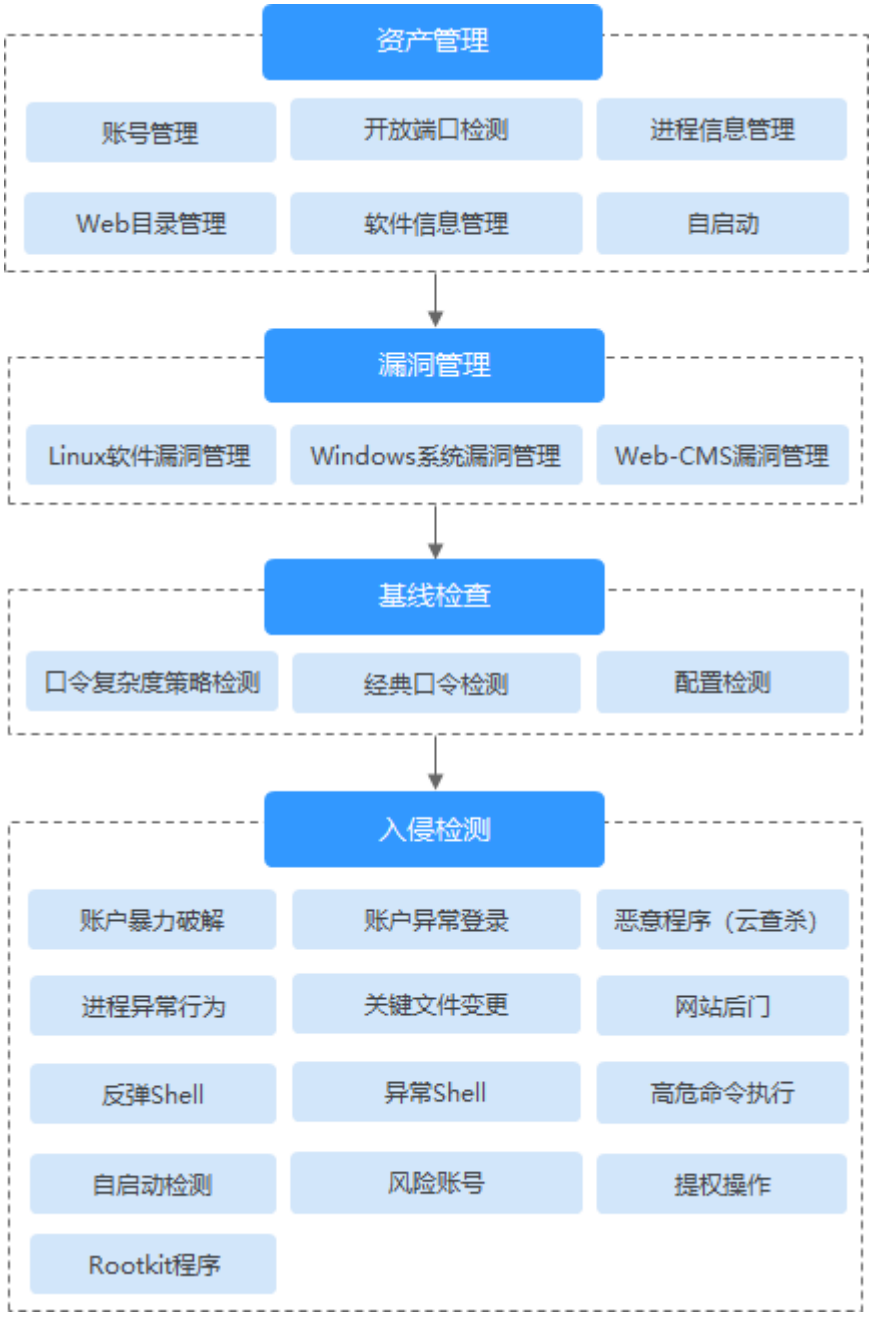
说明

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

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

版本之间的差异请参见**服务版本差异**。

图 1-14 自动执行的安全检测



----结束

查看检测详情

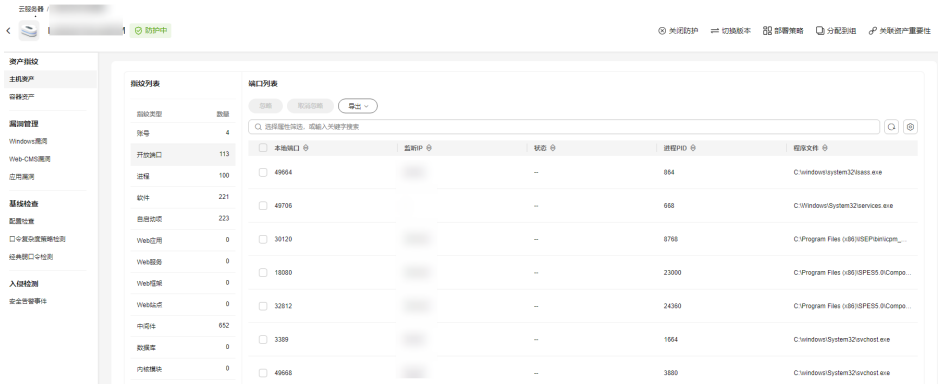
开启防护后，主机安全服务将立即对主机执行全面的检测，检测时间可能较长，请您耐心等待。

在防护列表的左侧，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。

图 1-15 查看有风险项

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。

图 1-16 查看检测结果



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。

版本之间的功能差异请参见**服务版本差异**。

图 1-17 手动配置的检测项

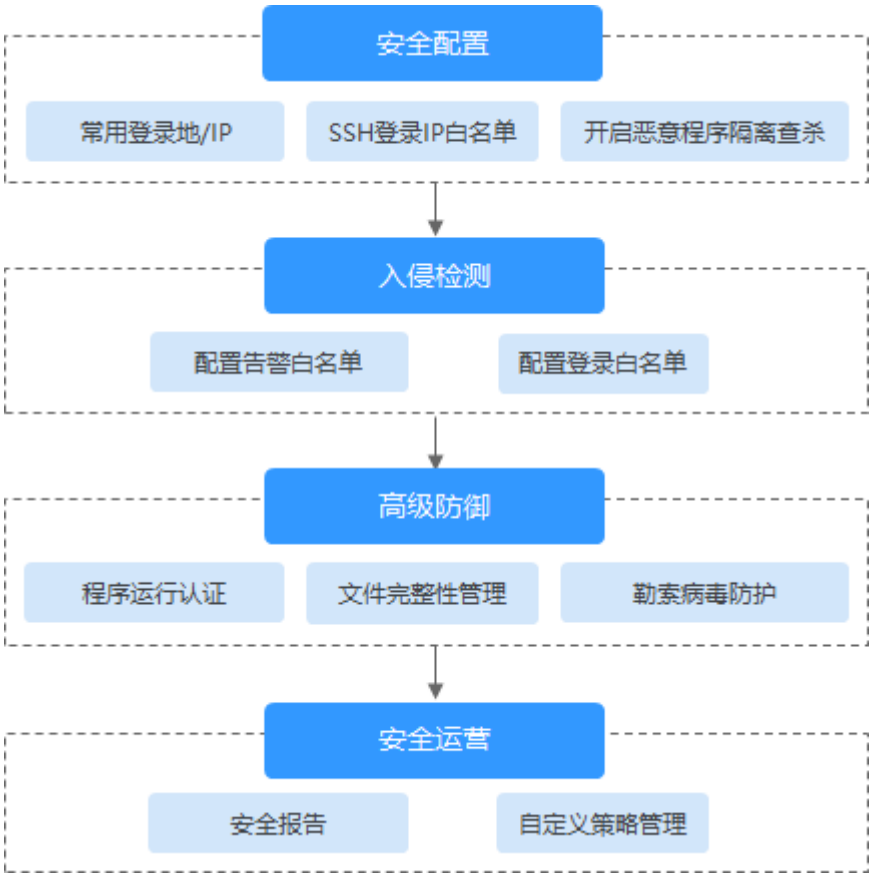


表 1-7 手动配置检测项

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

相关操作

关闭主机防护

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

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

须知

- 关闭主机防护前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免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。

解绑配额

您可以在“资产管理 > 主机管理 > 防护配额”页面的“操作”列中，单击“解除绑定”，解除绑定后，该配额的使用状态将从“使用中”变更为“空闲”。HSS将自动关闭关联主机的防护。

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

1.4.2 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，关闭主机安全服务或删除主机后，该配额可分配给其他的主机使用。

开启网页防篡改防护时会同步开启主机安全的旗舰版防护。

网页防篡改原理

表 1-8 网页防篡改原理

防护类型	原理说明
静态网页防护	1. 锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站管理员可通过特权进程进行更新网站内容。 2. 主动备份恢复 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 如果本地主机上的文件目录和备份目录失效，还可通过远端备份服务恢复被篡改的网页。

防护类型	原理说明
动态网页防护	提供Tomcat应用运行时自我保护，防护原理如下： 1. 基于RASP过滤恶意行为 采用华为自研RASP检测应用程序行为，有效阻断攻击者通过应用程序篡改网页内容的行为。 2. 网盘文件访问控制 精细化定义网盘文件中的文件访问权限，包括新增，修改，查询等，确保防篡改同时不影响网站内容发布。

前提条件

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

设置防护目录

网页防篡改功能需要有防护目录才能起到防护作用，网页防篡改提供指定目录的保护：

- 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。

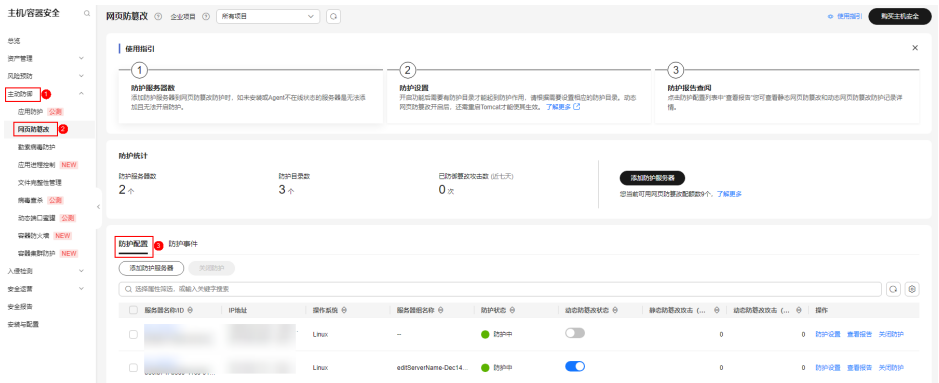
开启网页防篡改

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全合规 > 主机安全服务”，进入主机安全服务界面。

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

图 1-18 添加防护服务器



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

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

“网页防篡改版”开启后，旗舰版防护会同步开启。

- 选择“主动防御 > 网页防篡改”，目标服务器所在行的“防护状态”为“防护中”，则表示网页防篡改版已开启。
- 选择“资产管理 > 主机管理 > 云服务器”，目标主机所在行的“防护状态”为“防护中”，且“版本/到期时间”为“网页防篡改版”，则表示网页防篡改赠送的旗舰版已开启。

----结束

须知

- 您也可以通过在“资产管理 > 主机管理 > 防护配额”页面，单击“绑定主机”，为主机绑定防护配额，HSS自动为主机开启网页防篡改防护。
- 一个配额只能绑定一个主机，且只能绑定Agent在线的主机。
- 如果Linux主机安装的Agent版本为3.2.10及以上版本或Windows主机安装的Agent版本为4.0.22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，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）；此外，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**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“主动防御 > 网页防篡改 > 防护配置”列表的“操作”列中，单击“关闭防护”，关闭对指定主机的网页防篡改防护。

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

须知

- 关闭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。

解绑配额

您可以在“资产管理 > 主机管理 > 防护配额”页面的“操作”列中，单击“解除绑定”，解除绑定后，该配额的使用状态将从“使用中”变更为“空闲”。HSS将自动关闭关联主机的网页防篡改防护。

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

1.4.3 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

主机安全服务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

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

图 1-19 开启容器防护

步骤5 您可以根据自己的实际场景选择“包年/包月”或者“按需计费”，开启节点防护。

- **包年/包月**

  在“您确定要对以下集群开启防护吗？”对话框中，“计费模式”选择“包年/包月”，阅读并确认“《容器安全服务免责声明》”。

  “防护配额”分配方式：

  - 随机分配：下拉框选择“随机选择配额”，系统优先为主机分发服务剩余时间较长的配额。
  - 指定分配：下拉框选择具体配额ID，您可以为主机分配指定的配额。

- **按需计费**

  在“您确定要对以下集群开启防护吗？”对话框中，“计费模式”选择“按需计费”，阅读并确认“《容器安全服务免责声明》”。

步骤6 在弹出的提示框中，阅读“《容器安全服务免责声明》”后，并勾选“我已阅读并同意《容器安全服务免责声明》”。

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3.2.10及以上版本或Windows主机安装的Agent版本为4.0.22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，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）；此外，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**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。

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

须知

- 关闭节点防护前，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。

1.5 开启告警通知

开启告警通知功能后，您能接收到主机安全服务发送的告警通知，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。
- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。

开启告警通知

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置”，选择“告警配置”页签，进入“告警配置”页面，配置参数说明请参见**表1-9**。

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。

图 1-20 告警配置

表 1-9 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，主机安全服务将主动检测主机系统中的账号、Web目录、漏洞、恶意程序及关键配置等，汇总各项检测结果后，将检测结果发送给您在“消息中心”中添加的消息接收人，或者在“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，主机安全服务将按照选定的“消息中心”或者“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。主机安全服务实时监测主机中的安全情况，能监测到攻击者入侵主机的行为，接收实时告警通知能快速处理攻击者入侵主机的行为。 • 由于实时告警中通知项的内容紧急度较高，如果您使用的“消息通知服务”，接收告警通知，建议您选择“订阅终端”配置为“短信”的“消息通知服务主题”。
告警等级	自定义勾选通知的告警等级。	选择全部。

通知项	说明	选择建议
屏蔽事件	选择无需发送告警通知的事件。 展开选框可自定义选择不发送告警的事件类型。	根据**告警通知项说明**的内容说明判断需要屏蔽的事件。

步骤4 设置事件告警的通知方式。

- **消息中心**

  告警通知默认发送给账号联系人的消息中心，可登录系统在右上角查看。

  如需修改接收人，单击“消息接收管理”，跳转至消息中心，在“安全消息 > 安全事件通知”单击“操作”列的“修改”，编辑消息接收人，如**图1-21**所示。

  图 1-21 编辑消息接收人

- **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。

  创建新的主题，即配置接收告警通知的手机号码或邮箱地址，具体操作如下：

  a. 参见**创建主题**创建一个主题。

  b. 配置接收告警通知的手机号码或邮箱地址，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。

  c. 确认订阅。添加订阅后，按接收到的短信或邮件提示，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。更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤5 单击“应用”，完成配置主机安全告警通知的操作。界面弹出“告警通知设置成功”提示信息，则说明告警通知设置成功。

----结束

告警通知项说明

- **每日告警通知**

  每日凌晨检测主机中的风险，汇总并统计检测结果后，将检测结果于每日上午10：00发送给您添加的手机号或者邮箱。

表 1-10 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主机安全服务Agent的服务器数量，通知用户及时对这些服务器安装Agent进行防护。
漏洞管理	需紧急修复漏洞	检测系统中的紧急漏洞，通知用户尽快修复，防止攻击者利用该漏洞会对主机造成较大的破坏。
基线检查	配置检查	检测系统中的关键应用，如果采用不安全配置，有可能被黑客利用作为入侵主机系统的手段。
	经典弱口令	检测MySQL、FTP及系统账号的弱口令。
入侵检测	未分类恶意软件	对运行中的程序进行检测，识别出其中的后门、木马、挖矿软件、蠕虫和病毒等恶意程序。
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。
	Webshell	检测云服务器上Web目录中的文件，判断是否为Webshell木马文件，支持检测常见的PHP、JSP等后门文件类型。 ● 网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略可信文件。 ● 您可以使用手动检测功能检测主机中的网站后门。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	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。

通知项	通知内容	通知内容说明
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。
	关键文件变更	对于系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。
	文件/目录变更	对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。
	进程异常行为	检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。
	高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、复制、硬链接、访问权限变化。
	Crontab可疑任务	检测并列出当前所有主机系统中自启动服务、定时任务、预加载动态库、Run注册表键或者开机启动文件夹的汇总信息。 帮助用户通过自启动变更情况，及时发现异常自启动项，快速定位木马程序的问题。
	容器镜像阻断	在Docker环境中容器启动前，对镜像异常行为策略中指定的不安全容器镜像进行告警并阻断。
	暴力破解	检测“尝试暴力破解”和“暴力破解成功”等暴力破解。 ● 检测账户遭受的口令破解攻击，封锁攻击源，防止云主机因账户破解被入侵。 ● 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。

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

- **实时告警通知**
  事件发生时，及时发送告警通知。

表 1-11 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。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。
	文件提权	检测当前系统对文件的提权。
	进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。
	关键文件变更	对于系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。
	文件/目录变更	对于系统文件/目录进行监控，文件/目录被修改时告警，提醒用户文件/目录存在被篡改的可能。

通知项	通知内容	通知内容说明
	进程异常行为	检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。
	高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、复制、硬链接、访问权限变化。
	Crontab可疑任务	检测并列出当前所有主机系统中自启动服务、定时任务、预加载动态库、Run注册表键或者开机启动文件夹的汇总信息。 帮助用户通过自启动变更情况，及时发现异常自启动项，快速定位木马程序的问题。
	容器镜像阻断	在Docker环境中容器启动前，对镜像异常行为策略中指定的不安全容器镜像进行告警并阻断。
	异常登录	检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。 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。

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

1.6 常用安全配置

1.6.1 配置主机登录保护

开启防护后，您可配置常用登录地、常用登录IP、SSH登录IP白名单，提升云服务器登录安全性。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

----结束

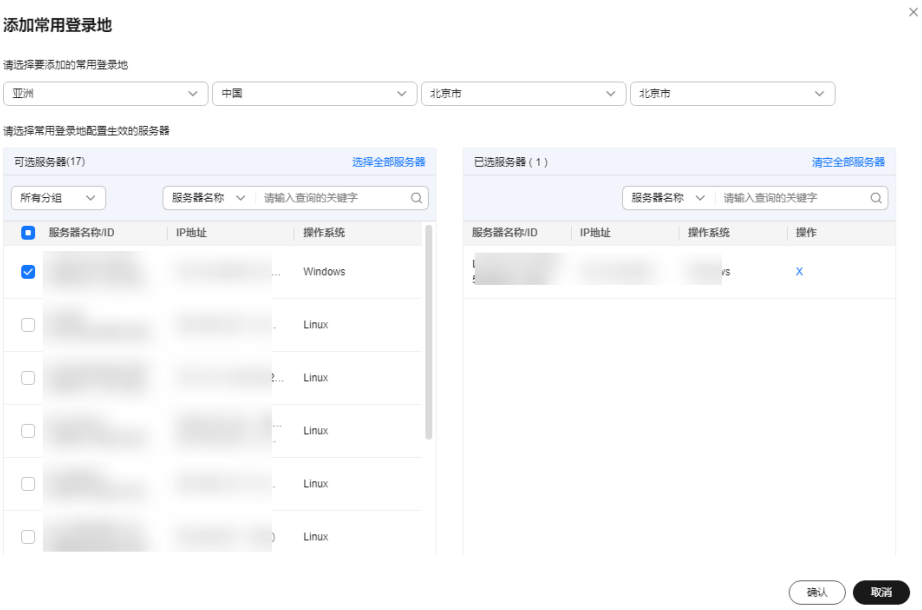
配置常用登录地

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

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

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

图 1-22 填写常用登录地信息



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

说明

对于异地登录告警，HSS有个学习的过程，因此添加完常用登录地之后，登录的前三个登录地会被视作常用登录地，第四个以后的非常用登录地才会被告警。

----结束

配置常用登录 IP

配置常用登录IP，主机安全服务将对非常用IP登录主机的行为进行告警。

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

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

说明

- “常用登录IP”必须填写公网IP或者IP段。如果设置的非公网IP地址，您将无法SSH远程登录您的服务器。
- 单次只能添加一个IP，如果需添加多个IP，需重复操作添加动作，直至全部IP添加完成，且最多可添加20个登录IP。

图 1-23 填写常用登录 IP

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

----结束

配置 SSH 登录 IP 白名单

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

说明

- 单一账号最多可添加10个SSH登录IP白名单。
- 配置了白名单的服务器，只允许白名单内的IP通过SSH登录到服务器，拒绝白名单以外的IP：
  - 启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中，否则您将无法SSH远程登录您的服务器。

    如果您的业务需要访问主机，但不需要SSH登录，则可以不用添加到白名单。
  - IP加入白名单后，账户破解防护功能将不再对来自白名单中的IP登录行为进行拦截，该IP对您加入白名单的服务器登录访问将不受任何限制，请谨慎操作。

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

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

说明

- “常用登录IP”必须填写公网IP或者IP段。如果设置的非公网IP地址，您将无法SSH远程登录您的服务器。
- 单次只能添加一个IP，如果需添加多个IP，需重复操作添加动作，直至全部IP添加完成。

图 1-24 填写白名单 IP 信息

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

----结束

1.6.2 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。

自动隔离查杀功能根据可疑程序的置信度得分进行隔离查杀，置信度得分越高，被检测程序是恶意程序的可能性越高，因此为避免误隔离查杀可信程序导致服务器的功能不可用，自动隔离查杀功能只查杀置信度95分及以上的可疑程序，95分以下的可疑程序您如果判断为恶意程序可参考**处理主机告警事件**手动隔离查杀。

说明

您可以在HSS控制台选择“入侵检测 > 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得分。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“安装与配置 > 安全配置 > 恶意程序隔离查杀”，分别单击“恶意程序隔离查杀”和“恶意软件云查杀”的开关，开启“恶意程序隔离查杀”和“恶意软件云查杀”。

说明

开启后将应用至主机安全服务全局服务器，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。

图 1-25 开启隔离查杀

步骤4 在弹出的对话框中单击“确认”，开启“恶意程序隔离查杀”和“恶意软件云查杀”。

自动隔离查杀有可能发生误报。您可以在主机安全服务控制台“入侵检测”页面中，选择“事件管理”页签，查看被隔离的恶意程序。在此您可以对指定的恶意程序执行取消隔离、忽略等操作，详情请参见**查看主机告警事件**。

须知

- 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，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“入侵检测”的“安全告警事件”中，查看“恶意程序”中的告警信息，并对恶意程序进行隔离查杀。

----结束

1.6.3 开启双因子认证

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

前提条件

- 用户已创建“协议”为“短信”或“邮箱”的消息主题。
- 主机已开启防护。
- 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。

操作步骤

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

图 1-26 开启双因子认证

步骤2 在弹出的“开启双因子认证”的对话框中，选择“验证方式”。

- **短信邮件验证**

  短信邮件验证需要选择消息通知服务主题。
  - 下拉框只展示状态已确认的消息通知服务主题。
  - 如果没有主题，请单击“查看消息通知服务主题”进行创建。具体操作请参见**创建主题**。
  - 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。

  图 1-27 短信邮件验证

- **验证码验证**

  选择验证码验证，仅通过实时收到的验证进行验证。

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

须知

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

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

----结束

2 总览

主机安全服务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。

查看总览

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击三，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“总览”，进入总览页查看资产安全信息，相关信息说明请参见表总览页信息说明。

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。

图 2-1 总览

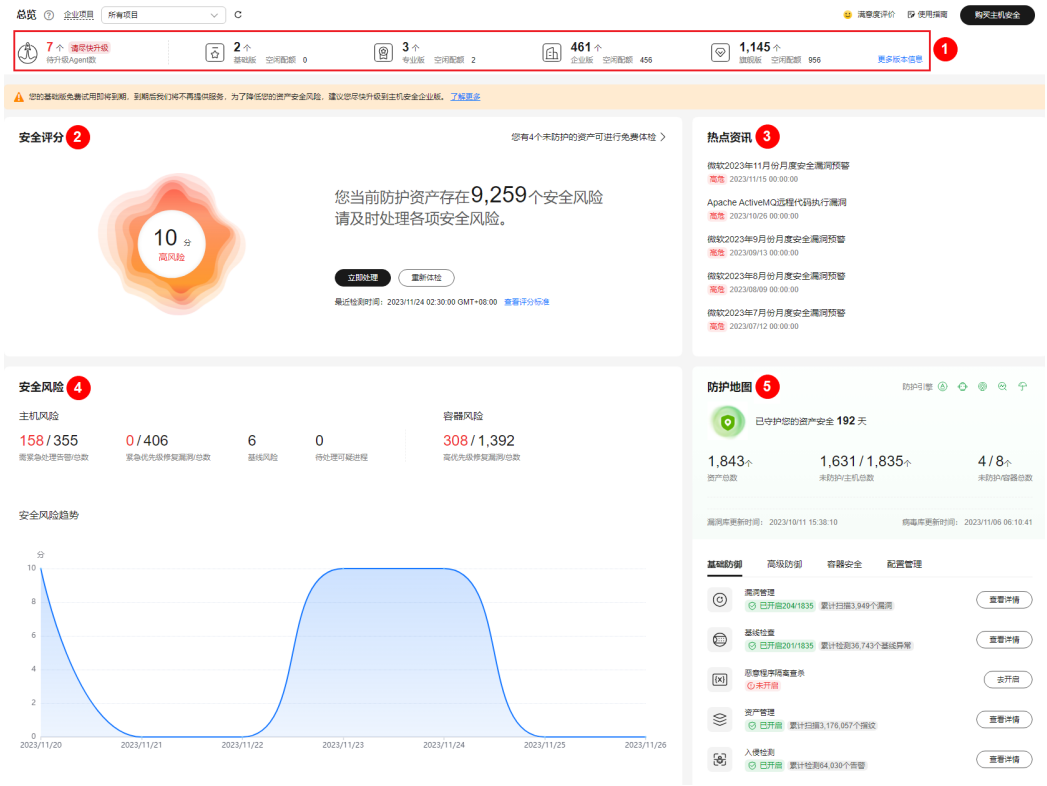


表 2-1 总览页信息说明

区域	说明
配额数量及待升级Agent数 （图 总览中所示区域①）	展示当前您已购买的各版本HSS防护配额总数和使用情况，以及待升级Agent数量。 • 单击对应防护配额的总数值，可跳转到防护配额界面查看防护配额列表。 • 单击待升级Agent数值，可跳转到Agent管理界面查看并升级Agent。 **说明** 主机安全服务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主机安全服务，具体操作请参见**升级Agent**。

区域	说明
安全评分 （图 总览中所示区域②）	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“立即处理”。 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 （图 总览中所示区域③）	展示最新的热点漏洞信息。
安全风险 （图 总览中所示区域④）	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：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 （图 总览中所示区域⑤）	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。 • 漏洞库或病毒库更新时间：最近一次漏洞库、病毒库更新时间。 • 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。
最佳实践	展示HSS的最佳实践文档，单击文档标题可查看对应文档内容。
常见问题	展示HSS的常见问题文档，单击文档标题可查看对应文档内容。
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 2-2 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，升级操作请参见**配额版本升级**。 • 对于HSS专业版/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 2-3 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。安全的口令设置方法请参见**如何设置安全的口令**。

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/专业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，升级操作请参见**配额版本升级**。 • 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 2-4 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专业版/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： ● 专业版/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专业版/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 2-5 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基础版/专业版/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，详细操作请参见**配额版本升级**。 • 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 2-6 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**容器镜像**。

表 2-7 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**。

3 资产管理

3.1 资产概览

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

约束限制

未开启防护不支持查看资产概览。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

- 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。
- 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。
- 防护配额：展示防护配额类型以及使用状态分布数量。单击“主机防护配额”或“容器防护配额”，可跳转至对应的防护配额列表页面。
- 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、数据库和内核模块。单击各资产项数值，可跳转至对应的资产列表页面。

----结束

3.2 主机指纹

3.2.1 采集主机资产指纹

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。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。

前提条件

服务器已开启HSS企业版、旗舰版、网页防篡改版或容器版防护。

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 3-1 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）
内核模块	统计、展示运行在内核层的全量程序模块文件，您可查看所有模块所关联的服务器、版本号、模块描述、驱动文件路径、文件权限、文件哈希等信息。	Linux	1次/周（每周一凌晨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）

功能项	功能描述	支持的操作系统	自动检测周期
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）

采集单个主机资产指纹最新数据

针对Web应用、Web服务、Web框架、Web站点、中间件、数据库和内核模块这些资产，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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

步骤5 单击指纹列表的目标类型，单击右侧列表上方“立即采集”任务自动创建完成。

说明

目前仅支持Web应用、Web服务、Web框架、Web站点、中间件、数据库和内核模块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6 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

3.2.2 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。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。

前提条件

服务器已开启HSS企业版、旗舰版、网页防篡改版或容器版防护。

查看所有主机资产信息

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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，常见危险端口如危险端口列表所示，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。

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。

图 3-1 查看主机资产信息

表 3-2 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
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

功能项	功能描述	支持的操作系统	自动检测周期
进程	检测主机系统中运行的进程，对运行中的进程进行收集及呈现，便于自主清点合法进程发现异常进程。 根据主机中“进程路径”以及具体进程对应的“服务器名称/IP”、“启动参数”、“启动时间”、“运行用户”、“文件权限”、“进程PID”以及“文件HASH”，您能够快速排查主机中的异常进程。 进程信息管理检测的机制是30天检测不到进程后，自动清除进程信息管理列表中的进程信息。	Linux、Windows	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
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）

功能项	功能描述	支持的操作系统	自动检测周期
中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。	Linux、Windows	1次/周（每周一凌晨04:10）
内核模块	统计、展示运行在内核层的全量程序模块文件，您可查看所有模块所关联的服务器、版本号、模块描述、驱动文件路径、文件权限、文件哈希等信息。	Linux	1次/周（每周一凌晨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）

----结束

查看单服务器的主机资产信息

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

步骤5 单击指纹列表的目标指纹类型，查看对应资产信息，资产指纹类型特性如**表 主机资产指纹特性**所示。

----结束

危险端口列表

表 危险端口列表列举了主机安全服务资产指纹功能检测判定“危险程度”为“危险”的危险端口。如果您的资产中有危险端口开放，请及时排查是否是正常业务使用，并在业务使用完成后关闭该端口。

表 3-3 危险端口列表

端口	说明	协议类型
31	木马MasterParadise、HackersParadise	TCP，UDP
456	木马HACKERSPARADISE	TCP，UDP
555	木马PhAse1.0、StealthSpy、IniKiller开放此端口	TCP，UDP
666	木马AttackFTP、SatanzBackdoor	TCP，UDP
1001	木马Silencer、WebEx	TCP，UDP
1011	木马DolyTrojan	TCP，UDP
1025	木马netspy	TCP，UDP
1033	木马netspy	TCP，UDP
1070	木马StreamingAudioTrojan、PsyberStreamServer、Voice	TCP，UDP
1234	木马SubSeven2.0、UltorsTrojan	TCP，UDP
1243	木马SubSeven1.0/1.9	TCP，UDP
1245	木马Vodoo	TCP，UDP
1270	MOM-Encrypted 服务	TCP
1492	木马FTP99CMP	TCP，UDP
1600	木马Shivka-Burka	TCP，UDP
1807	木马SpySender	TCP，UDP
1981	木马ShockRave	TCP，UDP
1999	木马BackDoor	TCP，UDP
2000	木马GirlFriend1.3、Millenium1.0	TCP，UDP
2001	木马Millenium1.0、TrojanCow	TCP，UDP
2023	木马PassRipper	TCP，UDP

端口	说明	协议类型
2115	木马Bugs	TCP，UDP
2140	木马DeepThroat1.0/3.0	TCP，UDP
3150	木马DeepThroat1.0/3.0	TCP，UDP
6711	木马SubSeven1.0/1.9	TCP，UDP
6776	木马SubSeven2.0、UltorsTrojan、SubSeven1.0/1.9	TCP，UDP

3.2.3 查看资产历史变动记录

HSS提供的资产管理，主动对账号信息、软件信息及自启动的变动情况进行记录，您可根据维度和时间进行选择查看对应的信息变动详情。

前提条件

服务器已开启HSS企业版、旗舰版、网页防篡改版或容器版防护。

查看历史变动记录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“资产管理 > 主机指纹 > 历史变动记录”，进入“历史变动记录”页面，选择维度和时间段，查看账号、软件、自启动项的历史变动记录。

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。

----结束

账号信息管理

历史变动状态说明：

- 变动状态：新建（新建了账号）、删除（删除了账号）、修改（修改了账号名、管理员权限或用户组等信息）。
- 最近扫描时间：服务器周期内最新的扫描时间。

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

软件信息管理

历史变动状态说明：

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

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

自启动项

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

您可以查看自启动项对应的服务器名称/IP、变动状态、路径、文件HASH、运行用户和最近扫描时间。

3.3 容器指纹

3.3.1 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。

前提条件

服务器已开启HSS容器版防护。

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 3-4 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示例的状态、所属POD、所属集群等信息。	-

采集单个容器资产指纹最新数据

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

步骤5 单击指纹列表的目标类型，单击右侧列表上方“立即采集”任务自动创建完成。

说明

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6 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，请参看本节手动采集最新的数据。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

----结束

3.3.2 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。

约束限制

- 仅HSS容器版支持容器指纹功能
- 仅支持Linux系统。

查看所有容器的资产指纹数据

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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，常见危险端口如危险端口列表所示，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。

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。

图 3-2 查看容器资产信息

表 3-5 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示例的状态、所属POD、所属集群等信息。	-

----结束

查看单容器的资产指纹数据

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

步骤5 单击指纹列表的目标指纹类型，查看对应资产信息。

----结束

查看集群

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

步骤6 在“集群列表”页面，查看集群相关信息。

集群列表页面展示了集群的名称、类型、可用节点、版本、创建时间和状态信息。

- 搜索目标集群

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

- 查看目标集群详细信息

  a. 单击目标集群名称，跳转到CCE控制台。

  b. 在CCE控制台，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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

步骤6 选择“服务 > 服务”，进入服务页面，查看服务相关信息。

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

- 搜索目标服务

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

- 查看目标服务详细信息

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

----结束

查看端点

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

步骤6 选择“服务 > 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，单击，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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

步骤6 选择“工作负载”，进入工作负载页面。

步骤7 选择不同的工作负载，查看相关工作负载的信息。

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

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

表 3-6 工作负载信息项

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

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

----结束

查看容器实例

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器指纹”，进入“容器指纹”页面。

步骤4 选择“集群列表”，单击集群列表左上角“手动同步”，创建同步任务。

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

步骤6 选择“容器实例”，进入容器实例页面，查看容器实例相关信息。

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

- 搜索目标容器

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

- 查看目标容器详细信息

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

----结束

3.4 主机管理

3.4.1 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。

主机管理的云服务器列表中仅显示以下主机的防护状态：

- 在所选区域购买的华为云主机
- 已接入所选区域的非华为云主机

说明

- 如果未找到您的主机，请切换到正确的区域后再进行查找。
- 如果您已开通企业项目，您可以在“企业项目”下拉列表中，选择您所在的企业项目，查看您所在企业项目的主机。

查看主机防护状态

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

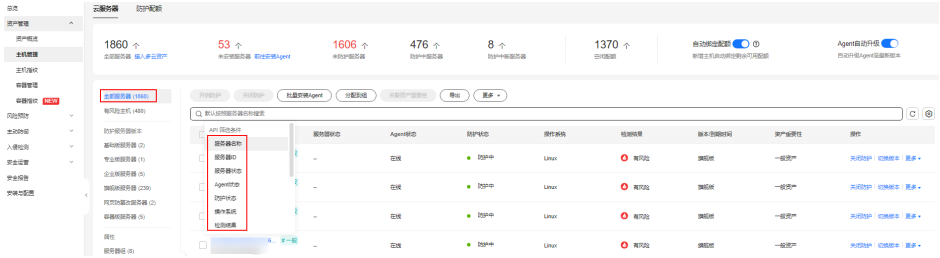
说明

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。

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。

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

图 3-3 搜索防护服务器



- 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。

表 3-7 防护状态说明

参数	说明
Agent状态	• 未安装：未安装Agent，或Agent已安装但未成功启动。 单击“安装Agent”，您可以根据弹出框给出的安装提示，进行Agent的安装，详细操作请参见**安装Agent**。 • 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。 **说明** 线下主机Agent离线30天后，主机管理页面会自动删除该主机信息。
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。
检测结果	• 有风险：主机存在风险。 • 无风险：主机暂未发现风险。 • 未检测：主机未开启防护。

----结束

查看网页防篡改防护状态

步骤1 登录管理控制台，进入主机安全服务页面。

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

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。

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

图 3-4 防篡改服务器列表

表 3-8 状态说明

参数名称	说明
防护状态	防护中：HSS为该服务器提供静态网页防篡改防护。
动态防篡改状态	动态网页防篡改的状态。 •  ：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

3.4.2 关闭防护

3.4.2.1 关闭基础版/专业版/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。

按需计费的企业版防护配额在关闭防护同时即停止计费，如果您要退订按需计费的企业版防护配额，关闭防护即可，无需再操作退订。

关闭防护

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 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”。

  图 3-5 单服务器关闭防护

  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”。

  图 3-6 批量关闭防护

  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

3.4.2.2 关闭网页防篡改版防护

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

操作须知

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 3-7 进入防护配置

步骤4 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”。

图 3-8 关闭网页防篡改防护

步骤5 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。

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

注意

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

----结束

3.4.3 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“资产管理 > 主机管理”，进入“云服务器”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4 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”。

说明

当前云服务器详情导出单次最大支持1000台服务器。

----结束

3.4.4 切换主机防护配额版本

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

防护配额切换说明

服务器支持切换绑定的防护配额版本为基础版、专业版、企业版、旗舰版。

如需使用“网页防篡改版”或“容器版”，请先购买“网页防篡改版”或“容器安全”的配额，再开启网页防篡改版或容器版防护，购买操作请参见**购买防护配额**。

前提条件

- 待切换防护配额的服务器防护状态为“防护中”。
- 切换为“包年/包月”计费的防护配额时，需要保证相应版本的防护配额数量充足，购买配额的操作请参见**购买防护配额**。
- 切换为低版本防护配额前，请对主机执行相应的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

说明

云服务器列表仅显示以下主机的防护状态：

- 在所选区域购买的华为云主机
- 已接入所选区域的非华为云主机

步骤4 根据需要可为单台服务器或多服务器切换防护配额版本。

- 单台服务器切换防护配额版本
  a. 在目标服务器所在行的“操作”列，单击“切换版本”。
  b. 在“选择开启方式”区域，依次选择计费模式、版本及配额，相关参数说明请参见**表 切换版本参数配置说明**。切换版本时可选择的目标版本请参见**表 切换版本说明**。

表 3-9 切换版本参数配置说明

参数	参数说明
计费模式	选择防护配额的计费模式。 ■ 包年/包月 ■ 按需计费
版本选择	选择服务器切换绑定的防护配额版本。 ■ 基础版：用于测试、个人用户防护主机账户安全，**无数量限制，只支持部分功能的检测能力，不支持防护能力，不支持等保认证**，首次开启可免费体验30天。 ■ 专业版：介于基础版和企业版之间，支持对文件目录变更、异常Shell的检测，策略管理等功能。 ■ 企业版：满足**等保认证**的需求，支持资产指纹管理、漏洞管理、恶意程序检测、Webshell检测、进程异常行为检测等能力。 ■ 旗舰版：满足**等保认证**的需求，支持应用防护、勒索防护、高危命令检测、提权检测、异常shell检测等能力。 更多版本介绍详情请参见**版本功能特性**。

参数	参数说明
选择配额	选择“包年/包月”计费模式时，需要为服务器选择已购买的防护配额。 ■ 随机选择配额：随机分配防护配额至服务器。 ■ 目标配额ID：选择为服务器绑定目标配额。批量开启时选择的配额只能绑定一台服务器，其余未绑定的服务器将随机绑定目标版本配额。 **说明** 如果提示可用配额为0时，表示配额不足，需要进行购买才可开启防护。
标签（可选）	选择“按需计费”计费模式时，您可以为按需防护配额添加标签。 标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

表 3-10 切换版本说明

计费模式	当前防护配额版本	可选择切换的防护目标版本
包年/包月	基础版	■ 包年/包月：专业版、企业版、旗舰版 ■ 按需计费：企业版
	专业版	■ 包年/包月：基础版、企业版、旗舰版 ■ 按需计费：企业版
	企业版	包年/包月：基础版、专业版、旗舰版
	旗舰版	■ 包年/包月：基础版、专业版、企业版 ■ 按需计费：企业版
按需计费	企业版	包年/包月：基础版、专业版、旗舰版

c. 阅读并勾选《主机安全免责声明》。

- 批量服务器切换防护配额版本
  a. 勾选多台目标服务器前的选框，单击服务器列表上方的“开启防护”。
  b. 在弹窗中确认服务器信息，依次选择计费模式、版本及配额，相关参数说明请参见**表 切换版本参数配置说明**。
  c. 阅读并勾选《主机安全免责声明》。

步骤5 单击“确定”切换版本。

切换主机安全服务版本后，请在云服务器列表页面查看目标服务器的版本。如果目标服务器的“版本”为切换后的主机安全服务版本，则表示主机安全服务版本已切换成功。

----结束

后续操作

- 切换版本后，您可将空余的配额分配给其他主机继续使用，避免造成配额资源的浪费。
- 切换为低版本后，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。
- 切换为高版本后，请及时对主机执行安全检测、处理主机中的安全隐患并配置必要的功能。

3.4.5 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

开启专业版、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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

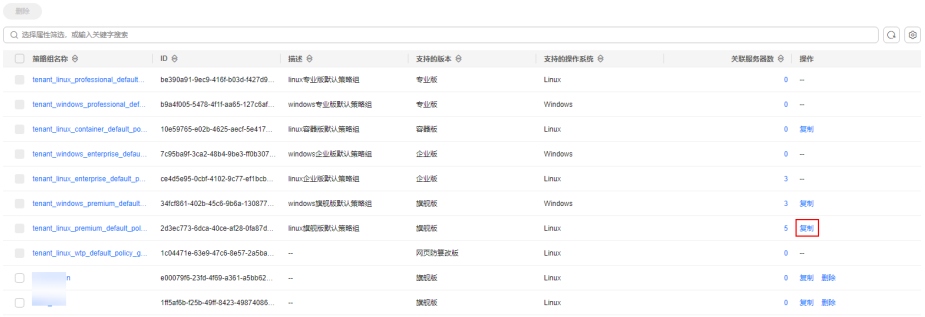
步骤4 复制策略组。

说明

目前仅旗舰版和容器版策略支持复制。

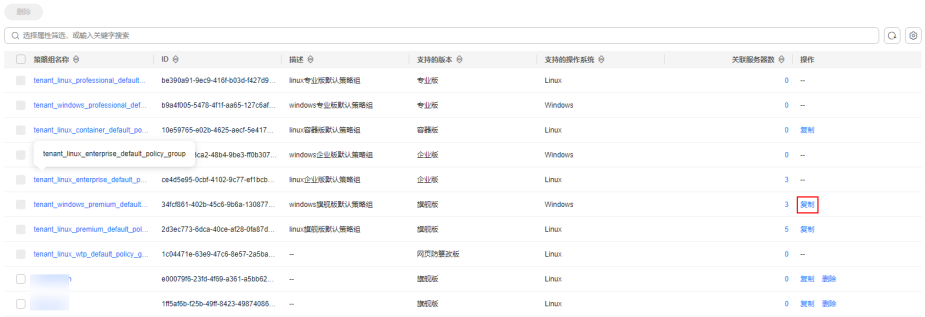
- 复制linux策略组：选择“tenant_linux_premium_default_policy_group”策略组，在该策略组所在行的“操作”列中，单击“复制”。

图 3-9 复制 linux 策略组



- 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”。

图 3-10 复制 windows 策略组



步骤5 在弹出的对话框中，输入“策略组名称”和“描述”。

说明

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

步骤6 单击“确认”，将会创建一个新的策略组。

步骤7 单击已创建的策略组名称，进入策略组的策略页面。

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

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

----结束

部署策略

步骤1 登录管理控制台，进入主机安全服务页面。

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

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

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。

图 3-11 部署策略

步骤4 在弹出的对话框中，选择策略组后，单击“确定”，完成部署策略操作。

说明

- 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

3.4.6 管理服务器组

用户可以创建服务器组，并将主机分配到服务器组，将主机进行分类管理。

用户可以根据创建的服务器组，查看该服务器组内的服务器数量、有风险服务器的数量、以及未防护的服务器数量。

创建服务器组

创建服务器组后，可将服务器按照一定类别分配到组进行统一管理。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 3-12 进入服务器组页面

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

说明

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

步骤5 设置完成后，单击“确认”，完成服务器组的创建。

----结束

分配服务器到组

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。

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。

图 3-13 分配到服务器组

说明

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

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

说明

一个云服务器只能分配到一个服务器组。

----结束

相关操作

编辑服务器组

步骤1 选择“主机管理 > 云服务器”下的“服务器组”页签。

步骤2 在待修改的服务器组所在行的“操作”列，单击“编辑”，修改服务器组。

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

步骤4 完成修改后，单击“确认”，完成服务器组的修改。

----结束

删除服务器组

步骤1 选择“主机管理 > 云服务器”下的“服务器组”页签。

步骤2 在需要删除的服务器组所在行的“操作”列，单击“删除”，删除单个服务器组。

说明

服务器组被删除后，隶属于该服务器组的所有云服务器将被划分到“未分组”中。

----结束

3.4.7 管理服务器重要性

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

资产重要等级分类如下：

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

查看资产重要等级

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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

----结束

关联资产重要等级

步骤1 登录管理控制台，进入主机安全服务页面。

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

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3 勾选目标服务器，单击列表上方的“关联资产重要性”。

图 3-14 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。

----结束

3.4.8 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。

前提条件

服务器未开启防护。

忽略服务器

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”。

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 选择“云服务器”页签。

步骤5 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。

图 3-15 忽略服务器

----结束

取消忽略服务器

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“资产管理 > 主机管理”。

说明

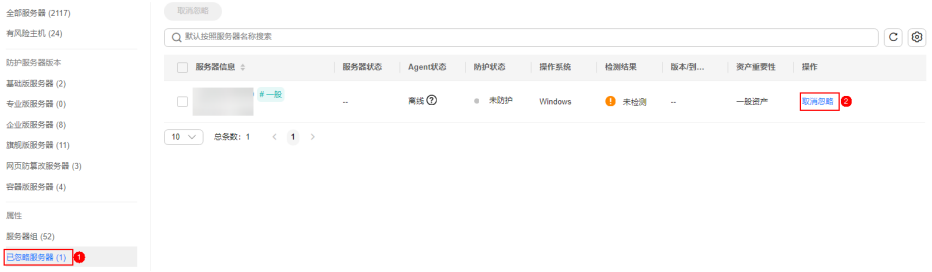
如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

步骤4 选择“云服务器”页签。

步骤5 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6 在目标服务器所在行的操作列，单击“取消忽略”，忽略操作完成。

图 3-16 取消忽略服务器



----结束

3.5 容器管理

3.5.1 查看容器节点防护状态

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

约束限制

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

查看容器节点防护列表

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击三，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 查看节点防护状态。节点列表参数说明如表3-11所示。

说明

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

表 3-11 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。
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。 **说明** 线下主机Agent离线30天后，节点管理页面会自动删除该主机信息。 • 未安装：未安装Agent，或Agent已安装但未成功启动。

----结束

3.5.2 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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”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4 选择“容器节点管理”页签。

步骤5 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

3.5.3 关闭容器版防护

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

操作须知

- 关闭防护对业务不会产生影响，但关闭后服务器被入侵的风险会急剧上升，建议保持开启防护的状态。
- 按需计费的容器安全版防护配额在关闭防护同时即停止计费，如果您要退订按需计费的容器安全版防护配额，关闭防护即可，无需再操作退订。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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5 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。

步骤6 关闭后在“资产管理 > 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。

⚠ 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

3.5.4 容器镜像

3.5.4.1 本地镜像

主机安全服务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，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 仅支持Docker引擎的本地镜像上报到主机安全服务控制台。
- 仅支持对Linux镜像执行安全扫描。

查看本地镜像

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，进入容器管理界面。

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 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

本地镜像安全扫描

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	检测镜像中存在的漏洞。
软件信息	统计镜像中的软件信息。

步骤1 登录管理控制台，进入主机安全服务页面。

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。

须知

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！

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，进入主机安全服务页面。

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。

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3 选择“容器镜像 > 本地镜像”。

步骤4 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，进入主机安全服务页面。

步骤2 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

3.5.4.2 SWR 私有镜像管理

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

约束限制

- 仅HSS容器版支持该功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。

- 仅支持对Linux镜像执行安全扫描。

查看私有镜像

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，进入容器管理界面。

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 选择“容器镜像 > 私有镜像（SWR）”，查看私有镜像信息。

步骤5 单击“从SWR更新自有镜像”，可以同步SWR所有自有镜像。

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SWR授权方法。

----结束

手动扫描私有镜像

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。

SWR私有镜像支持的安全扫描项如下：

扫描项	说明
漏洞	检测镜像中存在系统漏洞、应用漏洞。
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：检测镜像中存在的弱口令。 • 口令复杂度检查：检测镜像中不安全的口令复杂度策略。

扫描项	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。

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”。

步骤4 为单个镜像或多个镜像执行安全扫描。

说明

- 多架构镜像不支持批量扫描、全量扫描操作。
- 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！

- 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 待目标镜像“扫描状态”列显示为“扫描完成”，即扫描结束。

----结束

查看私有镜像漏洞报告

扫描完成后，可查看安全报告。

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-17 安全报告

步骤4 选择“漏洞报告”，查看漏洞报告。

- 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。

----结束

查看私有镜像恶意文件报告

扫描完成后，可查看镜像上存在的恶意文件。本节介绍查看镜像版本中存在的恶意文件。

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-18 安全报告

步骤4 选择“恶意文件”页签，查看镜像上存在的恶意文件。

----结束

查看私有镜像软件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-19 安全报告

步骤4 选择“软件信息”页签，查看该镜像版本包含的软件、软件类型和软件中存在的漏洞数。

步骤5 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。

----结束

查看私有镜像文件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-20 安全报告

步骤4 单击“文件信息”页签，查看镜像上的文件信息。

包含：文件个数，总文件大小以及文件大小排在前五十的文件详情。

图 3-21 文件信息

----结束

查看私有镜像基线检查报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-22 安全报告

步骤4 选择“基线检查”，查看基线检查报告。

您可以查看目标镜像的配置检查、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
  a. 在基线配置检查页签，勾选目标基线。
  b. 在目标检测项所在行的检测项列，单击“检测详情，”右面弹出检测详情页面，可以查看检测项描述以及修改建议。
- 自定义经典弱口令

a. 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。

b. 输入弱口令完成后，单击“确认”。

----结束

查看私有镜像敏感信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”，单击“操作”列的“安全报告”，查看该镜像版本的报告详情。

图 3-23 安全报告

步骤4 单击“敏感信息”页签，查看镜像敏感信息详情，并可对风险告警进行忽略处理。

步骤5 单击“敏感文件过滤路径管理”，查看自定义的白名单路径信息，同时可进行编辑。

图 3-24 编辑敏感文件路径白名单

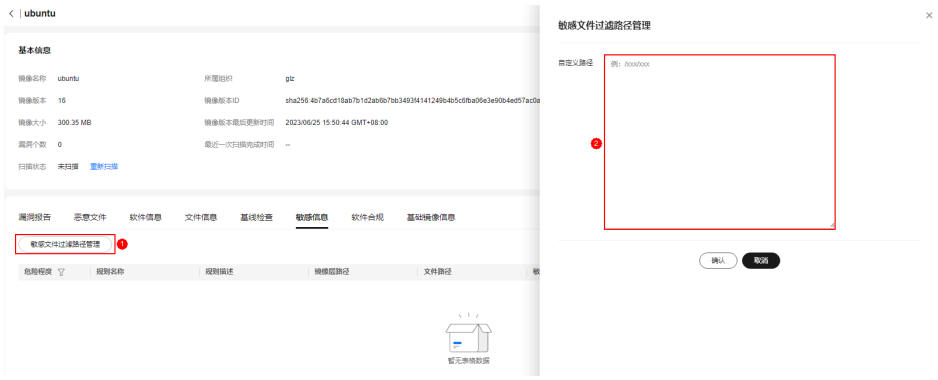


表 3-12 自定义路径配置说明

路径规格项	规格描述	取值样例
支持系统	仅支持Linux。	-
填写规范	最多自定义20个路径，多路径配置时不同路径之间用回车符号进行分隔。	/usr/ /lib/test.txt

路径规格项	规格描述	取值样例
默认白名单路径	默认支持的白名单目录或文件格式如下，无需配置。 ● /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。	-
不扫描场景	● 文件大于20MB。 ● 以下文件类型中时不进行扫描： – 常用二进制文件类型 – 常用程序文件类型 – 自动生成文件类型	● jpg|png|gif|mov|avi|mpeg|pdf|mp4|mp3|svg|tar|gz|zip ● js|jar|java||md|cpp|cxx|scala|pl ● [0-9a-zA-Z_-]{32,64}

----结束

查看私有镜像软件合规报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 >（SWR）”。

步骤4 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。

步骤5 选择“软件合规”，查看软件合规报告。

您可以查看不合规软件的名称、软件版本、路径、镜像层信息。

----结束

查看私有镜像基础镜像信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

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 > 私有镜像（SWR）”。

步骤4 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。

步骤5 选择“基础镜像信息”，查看基础镜像信息报告。

您可以查看未使用基础镜像构建的业务镜像的名称、版本、镜像层路径信息。

----结束

导出私有镜像漏洞报告或基线报告

说明

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，进入主机安全服务页面。

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 > 私有镜像（SWR）”。

步骤4 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

3.5.4.3 SWR 共享镜像管理

SWR共享镜像源于容器镜像服务(SWR)的共享镜像，主机安全服务支持对这些共享镜像手动执行漏洞、恶意文件、软件信息、文件信息、基线检查、敏感信息、软件合规和基础镜像信息的扫描并提供扫描报告。本章节介绍如何对SWR共享镜像进行安全扫描和如何查看安全扫描报告。

约束限制

- 仅HSS容器版支持该功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 仅支持对Linux镜像执行安全扫描。

查看 SWR 共享镜像

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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4 选择“容器镜像 > 共享镜像（SWR）”，查看共享镜像信息。

您可以查看共享镜像的版本、大小、所属组织、安全风险、拥有者等相关信息。

图 3-25 查看共享镜像

- 更新共享镜像

  单击“从SWR更新共享镜像”，更新共享镜像列表信息。
- 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。

----结束

共享镜像安全扫描

您可以为状态“有效”的SWR共享镜像手动执行安全扫描，支持扫描项如下：

扫描项	说明
漏洞	检测镜像中存在系统漏洞、应用漏洞。
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。

扫描项	说明
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：检测镜像中存在的弱口令。 ● 口令复杂度检查：检测镜像中不安全的口令复杂度策略。
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。

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 在左侧导航栏选择“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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 为单个镜像或多个镜像执行安全扫描。

说明

- 只有镜像状态为“有效”时，可执行安全扫描。
- 多架构镜像不支持批量扫描、全量扫描操作。
- 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！

- 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 SWR 共享镜像漏洞扫描报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“漏洞报告”，查看漏洞报告。

- 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。

----结束

查看 SWR 共享镜像恶意文件报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“恶意文件”，查看恶意文件报告。

您可以查看目标镜像中恶意文件的名称、路径、大小和描述等信息。

----结束

查看 SWR 共享镜像软件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“软件信息”，查看软件信息报告。

您可以查看目标镜像中的软件名称、类型、版本、漏洞个数等信息。

----结束

查看 SWR 共享镜像文件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“文件信息”，查看文件信息报告。

您可以查看目标镜像中的文件个数，总文件大小以及文件大小排在前五十的文件详情。

----结束

查看 SWR 共享镜像基线检查报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“基线检查”，查看基线检查报告。

您可以查看目标镜像的配置检查、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

a. 在基线配置检查页签，勾选目标基线。
b. 在目标检测项所在行的检测项列，单击“检测详情，”右面弹出检测详情页面，可以查看检测项描述以及修改建议。

- 自定义经典弱口令
  a. 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。
  b. 输入弱口令完成后，单击“确认”。

----结束

查看 SWR 共享镜像敏感信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“敏感信息”，查看敏感信息报告。

您可以查看目标镜像中含有敏感信息的文件的路径、敏感信息内容、危险程度。

- 忽略敏感信息提示
  在目标敏感信息文件所在行的“操作”列，单击“忽略”，忽略您认为安全的敏感信息提示。
- 配置敏感文件过滤路径
  a. 单击“敏感文件过滤路径管理”，右面弹出敏感信息过滤路径管理弹窗。
  b. 在弹窗中设置不需要检测的文件路径（Linux路径），并单击“确定”。
  最多可自定义20个路径，多路径配置时不同路径之间用回车符号进行分隔。

----结束

查看 SWR 共享镜像软件合规报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“软件合规”，查看软件合规报告。

您可以查看不合规软件的名称、软件版本、路径、镜像层信息。

----结束

查看 SWR 共享镜像基础镜像信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“基础镜像信息”，查看基础镜像信息报告。

您可以查看未使用基础镜像构建的业务镜像的名称、版本、镜像层路径信息。

----结束

导出 SWR 共享镜像漏洞或基线报告

说明

多架构镜像不支持导出漏洞报告。

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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

3.5.4.4 SWR 企业版镜像

SWR企业版镜像源于容器镜像服务(SWR)的企业版镜像，主机安全服务支持对这些企业版镜像手动执行漏洞、恶意文件、软件信息、文件信息、基线检查、敏感信息、软件合规和基础镜像信息的扫描并提供扫描报告。本章节介绍如何对SWR企业版镜像进行安全扫描和如何查看安全扫描报告。

约束限制

- 仅HSS容器版支持该功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 仅支持对Linux镜像执行安全扫描。

查看 SWR 企业版镜像

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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4 选择“容器镜像 > 企业版镜像（SWR）”，查看企业版镜像信息。

您可以查看企业版镜像的版本、大小、所属组织、安全风险、拥有者等相关信息。

图 3-26 查看企业版镜像

- 更新企业版镜像

  单击“从SWR更新企业版镜像”，更新企业版镜像列表信息。

- 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。

----结束

SWR 企业版镜像安全扫描

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。

SWR企业版镜像支持的安全扫描项如下：

扫描项	说明
漏洞	检测镜像中存在系统漏洞、应用漏洞。
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。

扫描项	说明
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：检测镜像中存在的弱口令。 ● 口令复杂度检查：检测镜像中不安全的口令复杂度策略。
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。

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 为单个镜像或多个镜像执行安全扫描。

说明

- 多架构镜像不支持批量扫描、全量扫描操作。
- 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！

- 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

查看企业版镜像（SWR）漏洞扫描报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“漏洞报告”，查看漏洞报告。

- 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。

----结束

查看 SWR 企业版镜像恶意文件报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“恶意文件”，查看恶意文件报告。

您可以查看目标镜像中恶意文件的名称、路径、大小和描述等信息。

----结束

查看 SWR 企业版镜像软件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 共享镜像（SWR）”。

步骤4 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。

步骤5 选择“软件信息”，查看软件信息报告。

您可以查看目标镜像中的软件名称、类型、版本、漏洞个数等信息。

----结束

查看 SWR 企业版镜像文件信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“文件信息”，查看文件信息报告。

您可以查看目标镜像中的文件个数，总文件大小以及文件大小排在前五十的文件详情。

----结束

查看 SWR 企业版镜像基线检查报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“基线检查”，查看基线检查报告。

您可以查看目标镜像的配置检查、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
  a. 在基线配置检查页签，勾选目标基线。
  b. 在目标检测项所在行的检测项列，单击“检测详情，”右面弹出检测详情页面，可以查看检测项描述以及修改建议。
- 自定义经典弱口令

a. 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。
b. 输入弱口令完成后，单击“确认”。

----结束

查看 SWR 企业版镜像敏感信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“敏感信息”，查看敏感信息报告。

您可以查看目标镜像中含有敏感信息的文件的路径、敏感信息内容、危险程度。

- 忽略敏感信息提示

  在目标敏感信息文件所在行的“操作”列，单击“忽略”，忽略您认为安全的敏感信息提示。
- 配置敏感文件过滤路径
  a. 单击“敏感文件过滤路径管理”，右面弹出敏感信息过滤路径管理弹窗。
  b. 在弹窗中设置不需要检测的文件路径（Linux路径），并单击“确定”。

  最多可自定义20个路径，多路径配置时不同路径之间用回车符号进行分隔。

----结束

查看 SWR 企业版镜像软件合规报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“软件合规”，查看软件合规报告。

您可以查看不合规软件的名称、软件版本、路径、镜像层信息。

----结束

查看 SWR 企业版镜像基础镜像信息报告

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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。

步骤5 选择“基础镜像信息”，查看基础镜像信息报告。

您可以查看未使用基础镜像构建的业务镜像的名称、版本、镜像层路径信息。

----结束

导出 SWR 企业版镜像漏洞或基线报告

说明

多架构镜像不支持导出漏洞报告。

步骤1 登录管理控制台，进入主机安全服务页面。

步骤2 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3 选择“容器镜像 > 企业版镜像（SWR）”。

步骤4 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

3.5.5 查看容器信息

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

约束限制

- 仅HSS容器版支持该功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 仅支持Docker引擎的本地镜像上报到主机安全服务控制台。
- 仅支持对Linux镜像执行安全扫描。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“资产管理 > 容器管理”，进入“容器管理”页面。

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 选择“容器”，进入容器页签。

步骤5 查看容器信息和安全状态。

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

- 查看容器详细信息。

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

- 查看容器安全风险分布。

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

----结束

3.5.6 处置风险容器

操作场景

主机安全服务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、暂停或杀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，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 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。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 选择“容器”，进入容器页签。

步骤5 在容器列表上方搜索框中输入“有风险”并单击，筛选有安全风险的容器。

步骤6 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。

对于集群容器支持杀容器操作，对于单机容器支持隔离、暂停、杀容器操作。

说明

仅有中危及以上风险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。

- **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”。
- **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”。
- **杀容器**：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“杀容器”。
  b. 在弹出的对话框中确认信息无误后，单击“确认”。

----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

3.5.7 集群 Agent 管理

3.5.7.1 集群安装 Agent

如果您想要为CCE集群的所有node节点或自建k8s集群所有节点安装Agent，可以通过集群Agent管理功能为集群安装Agent，使用该功能后，后续集群节点或Pod扩容时，无需您手动安装Agent。

CCE 集群安装 Agent

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，进入“容器管理”界面。

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 选择“集群Agent管理 > CCE集群”页签。

步骤5 在目标集群所在行的操作列，单击“安装Agent”。

您也可以勾选所有目标集群，并单击列表左上方的“安装Agent”，批量为CCE集群安装Agent。

步骤6 在弹窗中单击“确认”，为CCE集群所有节点主机安装Agent。

安装Agent预计耗时10分钟，请您等待10分钟后，鼠标滑动至“节点Agent安装状态”列查看节点Agent安装情况。单击Agent未安装/已安装的节点数值，可跳转到对应集群的主机Agent安装详情页面。

图 3-27 查看 Agent 安装状态

----结束

自建集群安装 Agent

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，进入“容器管理”界面。

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 选择“集群Agent管理 > 自建集群”页签。

步骤5 单击“接入自建集群”。

步骤6 在“接入自建集群”弹窗中，填写集群信息并单击“生成命令”。

您可以在弹窗中，单击“保存”，保存本次生成的命令。

步骤7 在可执行k8s命令的主机中创建一个新的yaml文件，例如abcd.yaml。

步骤8 将生成的命令拷贝到abcd.yaml中。

步骤9 在主机中执行以下命令，运行abcd.yaml，安装Agent。安装Agent预计耗时10分钟，请您耐心等待。

kubectl apply -f abcd.yaml

步骤10 命令运行完成后，返回HSS控制台。

步骤11 在左侧导航栏，选择“安装与配置”，进入“安装与配置”界面。

步骤12 选择“Agent管理”页签，查看集群服务器的Agent状态为“在线”，表示Agent安装成功。

----结束

修改自建集群信息

- 如果后续您需要修改自建集群信息或查看命令，可在自建集群所在行的操作列单击“编辑”。
- 如果您不再需要HSS保存某个自建集群的信息，可在自建集群所在行的操作列单击“删除”。

后续操作

Agent安装完成后，请为容器开启防护，详细操作请参见**开启容器版防护**。

3.5.7.2 集群卸载 Agent

如果不再需要HSS为您的集群容器提供安全防护，您可以为集群卸载Agent。Agent卸载后，HSS将停止对容器的检测和防护，且已检测到的告警、漏洞信息等数据都将被删除。

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“容器 > 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。

图 3-28 删除 install-agent-ds

步骤6 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤7 在左侧导航栏，选择“安装与配置”，进入“安装与配置”界面。

步骤8 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤5 在左侧导航栏，选择“安装与配置”，进入“安装与配置”界面。

步骤6 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Agent**。

----结束

3.6 防护配额管理

3.6.1 查看防护配额

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

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

查看主机配额

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面，单击目标选项可进行筛选查看。

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 在防护配额页面，查看主机安全防护配额，参数详情请参见表3-13。

表 3-13 主机防护配额参数说明

参数名称	参数说明
配额ID	配额的唯一标识ID。
版本类型	• 基础版 • 专业版 • 企业版 • 旗舰版 • 网页防篡改版
使用状态	• 使用中：该配额已被使用，下方显示“使用该配额的服务器名称”。 • 空闲：该配额未被使用。
配额状态	• 正常：您购买的服务配额未到期，且能正常使用。 • 已过期：配额已到期，在此期间您仍然可以正常使用配额。 • 已冻结：冻结期间，HSS将不再防护您的主机；冻结期满，该配额将被彻底删除。
计费模式	• 包年/包月 • 按需计费
企业项目名称	目标配额所属的企业项目名称。
标签	资源分类标签。

说明

- 绑定主机

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

  一个配额只能绑定一个主机，且只能绑定agent在线的主机。

- 解除绑定

  您也可以在“资产管理 > 主机管理 > 防护配额”页面的“操作”列中，单击“解除绑定”，解除绑定后，HSS将自动关闭关联主机的防护，该配额的使用状态变更为“空闲”状态。

- 导出列表

  单击配额列表右上角的  按钮。可将当前页列表的配额信息进行导出。

----结束

查看容器配额

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击  ，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏中，选择“资产管理 > 容器管理”，在“容器节点管理”界面，选择“防护配额”页签，进入防护配额列表页面。

步骤4 在防护配额页面，查看容器安全防护配额，参数详情请参见表3-14。

表 3-14 容器配额参数说明

参数名称	参数说明
配额ID	配额的ID。
配额版本	企业版。
配额状态	• 正常：配额状态。 • 已过期：配额已到期，在此期间您仍然可以正常使用配额。 • 已冻结：冻结期间，HSS将不再防护您的容器；冻结期满，该配额将被彻底删除。
使用状态	• 使用中：该配额已被使用，下方显示“使用该配额的服务器名称”。 • 空闲：该配额未被使用。
计费模式	• 包年/包月 • 按需计费
标签	资源分类标签。

说明

- 续费

  您可以在需要续费的资源所在行的“操作”列，单击“续费”，为购买的容器安全续费，详细操作请参见**如何续费**。

- 退订

  您可以在需要退订的资源所在行的“操作”列，单击“退订”，退订不需要使用的配额，详细操作请参见**如何退订**。

----结束

3.6.2 绑定防护配额

将购买的防护配额与服务器绑定，绑定后目标服务器将开启配额版本所支持能力的安全防护。

前提条件

- 主机已安装Agent，且Agent状态为“在线”，安装操作请参见**安装Agent**。
- 购买的防护配额的“配额状态”为“正常”，“使用状态”为“空闲”。
- 一个配额只绑定一个主机，且只能绑定agent在线的主机。

手动绑定主机配额

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面，单击目标选项可进行筛选查看。

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 在防护配额列表页面，单击目标配额“操作”列“绑定主机”。

说明

为主机绑定网页防篡改防护配额，需要在“主动防御 > 网页防篡改 > 防护配置”页面的“操作”列中，单击“开启防护”，HSS自动为主机开启网页防篡改防护。

步骤5 在弹出的绑定主机窗口中，选择一个待绑定的主机。

图 3-29 勾选需绑定的主机

步骤6 单击“确定”，完成主机的绑定，HSS自动为主机开启防护。

----结束

手动绑定容器配额

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 容器管理”页面，选择“防护配额”页签，进入防护配额列表页面。

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 在防护配额列表页面，单击目标配额“操作”列“绑定主机”。

步骤5 在弹出的绑定主机窗口中，选择一个待绑定的主机。

步骤6 单击“确定”，完成主机的绑定，HSS自动开启防护。

----结束

自动绑定配额

自动绑定说明

开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。

- 主机：按“旗舰版>企业版>专业版>基础版”的顺序自动绑定空闲可用的包年/包月配额。
- 容器节点：按“容器版>旗舰版>企业版>专业版>基础版”的顺序自动绑定空闲可用的包年/包月配额。
- 如果Linux主机安装的Agent版本为3.2.10及以上版本或Windows主机安装的Agent版本为4.0.22及以上版本，开启旗舰版、网防篡改版和容器版防护时，系统会自动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）；此外，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**开启勒索备份**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“资产管理 > 主机管理”，进入主机管理界面。

说明

自动绑定配额开关也存在购买防护配额页面、容器管理页面，您任选一个页面配置即可。

步骤4 单击，开启自动绑定配额。

图 3-30 开启自动绑定配额

----结束

3.6.3 解绑防护配额

解绑配额后，HSS会关闭主机防护，无法检测主机存在的潜在风险，请谨慎操作。

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

前提条件

主机已绑定配额。

解绑主机配额

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面，单击目标选项可进行筛选查看。

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 在防护配额列表页面，单击目标配额“操作”列“解除绑定”，解除配额。

如果您需要批量解绑配额，您可以勾选所有要解绑配额的主机，单击配额列表左上角的“批量解绑”。

说明

解绑配额后，HSS将无法检测您主机存在的潜在风险，请谨慎操作。

步骤5 在弹出的解绑配额对话框中，单击“确定”，解除绑定。

----结束

解绑容器配额

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面，单击目标选项可进行筛选查看。

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 在防护配额列表页面，单击目标配额“操作”列“解除绑定”。

如果您需要批量解绑配额，您可以勾选所有要解绑配额的主机，单击配额列表左上角的“批量解绑”。

说明

解绑配额后，HSS将无法检测您主机存在的潜在风险，请谨慎操作。

步骤5 在弹出的解绑配额对话框中，单击“确定”，解除绑定。

----结束

3.6.4 升级防护配额

当已购买版本的能力无法满足防护需求，您可通过升级当前版本来满足安全防护需求。

升级说明

- 旗舰版、网页防篡改版、容器版为高配置版本，不支持升级，您可以单独购买这些配额。
- 基础版、专业版、企业版支持升级为更高配置的配额版本。
  - 基础版：可升级为专业版、企业版或旗舰版。
  - 专业版：可升级为企业版或旗舰版。

- 企业版：可升级为旗舰版。

前提条件

- 准备进行升级的防护配额“使用状态”必须为“空闲”。
- 准备进行升级的防护配额“配额状态”必须为“正常”。

升级至专业版/企业版/旗舰版

升级时目标配额如果绑定服务器处于使用中状态，您需要关闭该服务器防护，释放配额，释放后进行升级操作。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面，单击目标选项可进行筛选查看。

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 在防护配额列表页面，可筛选出基础版或企业版空闲的配额，勾选需升级的配额，单击“升级规格”。

说明

- 如果需要升级的配额处于绑定状态，则需要先对目标配额进行**解除绑定**，然后按照此步骤进行升级。
- 解除绑定不影响业务使用。

步骤5 进入页面规格确认页面，确认升级规格信息。

说明

如果升级的目标版本为基础版，则升级规格版本可选择企业版或旗舰版，如果升级的版本为企业版，则默认升级后规格版本为旗舰版。

图 3-31 确认升级规格信息

步骤6 确认升级版本无误，单击“立即购买”。

说明

升级购买只需支付新增部分的价格。

步骤7 进入购买信息确认页面，确认购买信息无误，勾选“我已阅读同意《主机安全免责声明》”，单击“去支付”。

步骤8 支付完成后，回到**查看配额**页面，通过配额ID找到目标配额，查看版本类型为需要升级的目标版本，表示升级成功。

步骤9 升级成功后按照**绑定配额**的操作进行重新绑定目标服务器即可开启防护。

----结束

升级至网页防篡改

升级的目标规格为网页防篡改版时，需购买网页防篡改版本配额，购买后如果目标服务器处于防护状态需将目标服务器防护关闭，重新为目标服务器绑定网页防篡改版配额。

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在界面右上角，单击“购买主机安全”，进入“购买主机安全配额”界面。

步骤4 在“购买主机安全配额”界面，选择网页防篡改版，参数说明如**表3-15**所示。

表 3-15 购买主机安全参数说明

参数名称	参数说明	取值样例
计费模式	根据您的需求选择“包年/包月”或“按需”计费模式。 ● 包年/包月：在版本选择时可选择基础版、专业版、企业版、旗舰版、网页防篡改版和容器版，单次购买固定的版本使用周期，费用方面比“按需”付费方式每月优惠30%，如果您长期使用，建议包周期购买。 ● 按需：当前购买页支持选择企业版，开启防护需要在服务器列表页开启。按实际使用的时长收费，以小时为单位，每小时整点结算，不设最低消费标准。 **说明** 开启按需防护步骤： 1. 在购买页选择按需，默认选择企业版，在页面右下角单击“立即开通”，页面跳转到云服务器列表页面。 2. 在云服务器列表的“操作”列单击“开启防护”，“计费模式”选择“按需计费”，“主机安全版本”选择“企业版”。 3. 确认信息无误，单击“确认”完成开启。	包年/包月
区域	● 配额的“区域”建议与主机的“区域”相同。	中国-香港

参数名称	参数说明	取值样例
版本选择	支持购买的版本有“基础版”、“专业版”、“企业版”、“旗舰版”、“网页防篡改版”和“容器版”。各版本的功能差异详情请参见服务版本差异。 **须知** • 首次开启基础版可免费体验30天，体验结束后进行购买即可。 • 如果您购买的是基础版/企业版/旗舰版配额，请在“资产管理 > 主机管理 > 云服务器”页面开启防护。 • 如果您购买的是网页防篡改版配额，请在“主动防御 > 网页防篡改 > 防护配置”页面开启防护。 • 如果您购买的是容器版配额，请在“资产管理 > 容器管理 > 容器节点管理”页面开启防护。	企业版
企业项目	企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请联系您的客户经理申请开通。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 从下拉列表中选择所在的企业项目。 **说明** • 选择企业项目后，产生的费用和资源均在企业项目内。 • “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 • 只有注册的华为账号购买HSS时，“企业项目”下拉列表中才可以选择到“default”。	default
购买时长	• 根据您的需求选择时长，“按需”模式无需选择。 • 为避免因服务到期未及时续费导致您的主机遭受攻击，建议勾选“自动续费”。 • 勾选“自动续费”后，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。 • 如果未勾选自动“自动续费”，在即将到期时，请手动续费。	1年
防护主机数量	输入购买主机安全服务防护配额的数量，“按需”模式无需选择。 **须知** • 为防止未防护主机感染勒索、挖矿等病毒后传染给其他主机，导致企业内网整体沦陷，购买的主机安全服务数量建议与使用的主机数量保持一致。 • 购买成功后不支持增加配额，如需增加配额，请重新购买即可。	20

参数名称	参数说明	取值样例
标签	标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。 如果需要该功能，您的账号需要具备TMS administrator权限，没有该权限您无法为防护配额添加标签并且界面会有“permission error”的错误提示。 “按需”模式无需填写。	data
配额管理	开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。 ● 主机：按“旗舰版 > 企业版 > 专业版 > 基础版”的顺序自动绑定空闲可用的包年/包月配额。 ● 容器节点：按“容器版 > 旗舰版 > 企业版 > 专业版 > 基础版”的顺序自动绑定空闲可用的包年/包月配额。	勾选

步骤5 在页面右下角，单击“立即购买”，进入“订单确认”界面。

费率标准请参见**产品价格详情**。

步骤6 确认订单无误后，请阅读《主机安全免责声明》并勾选“我已阅读并同意《主机安全免责声明》”。

步骤7 在弹窗中选择验证方式，单击“获取验证码”，输入验证码后单击“确认”完成支付，购买成功。

步骤8 在左侧导航树中，选择“主动防御 > 网页防篡改”，进入“防护配置”界面，单击“添加防护服务器”。

须知

- 选择“资产管理 > 主机管理 > 云服务器”，进入“云服务器”界面，如果目标服务器的“防护状态”为“防护中”，需单击“操作”列的“关闭防护”，解除目标服务器与原配额的绑定关系。
- 解除绑定不影响业务正常运行。

步骤9 单击“添加防护服务器”，选择目标服务器，单击“添加并开启防护”。

图 3-32 勾选目标服务器

步骤10 开启防护后，在“资产管理 > 主机管理 > 云服务器”查看目标服务器的“版本/到期时间”为“网页防篡改版”表示升级成功。

说明

升级成功后，原配额版本可绑定至其他服务器继续防护，如果不再需要，可在“资产管理 > 主机管理 > 防护配额”页面单击“操作”列“更多”选择“退订”。

----结束

3.6.5 导出防护配额列表

您可以参考本章节导出主机防护配额列表到本地查看；容器防护配额列表暂不支持导出，敬请谅解！

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“资产管理 > 主机管理”。

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 选择防护配额页签。

步骤5 在防护配额列表上方，单击“导出 > 导出全部数据到XLSL”，导出主机防护配额列表。

如果您仅需导出指定的防护配额信息，请选中目标配额，单击“导出 > 导出已选中数据到XLSL”

图 3-33 导出全部主机防护配额数据

步骤6 在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

4 风险预防

4.1 漏洞管理

4.1.1 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 4-1 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 HSS各版本支持扫描和修复的漏洞类型**。

表中的标识含义如下：

- √表示支持
- ×表示不支持

表 4-2 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	专业版	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（随软件资产采集周期上报）	√	√	√	√	√	√
	定时扫描漏洞（默认每周一次，可通过漏洞策略配置修改扫描周期）	×	√	√	√	√	√
	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）	√（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（随软件资产采集周期上报）	√	√	√	√	√	×

漏洞类型	功能	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
	定时扫描漏洞（默认每周一次，可通过漏洞策略配置修改扫描周期）	×	√	√	√	√	×
	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）	√（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（随软件资产采集周期上报）	×	√	√	√	√	√
	定时扫描漏洞（默认每周一次，可通过漏洞策略配置修改扫描周期）	×	√	√	√	√	√
	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（随中间件资产采集周期上报）	×	×	√	√	√	√
	定时扫描漏洞（默认每周一次，可通过漏洞策略配置修改扫描周期）	×	×	√	√	√	√
	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	×	×	×	×	×	×

漏洞类型	功能	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
	定时扫描漏洞（默认未开启，可通过漏洞策略配置开启）	×	√	√	√	√	√
	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。

4.1.2 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（漏洞策略配置）和手动扫描三种扫描方式：

- 自动扫描

  HSS在采集资产指纹时，会同步自动扫描漏洞，对于Linux漏洞、Windows漏洞以及Web-CMS漏洞按软件采集周期进行扫描，对于应用漏洞按中间件采集周期进行扫描。资产指纹采集周期请参见**采集主机资产指纹**。

  如果资产指纹采集周期内，手动扫描过漏洞或触发过定时扫描漏洞任务，那HSS将在下一次采集资产指纹时再同步自动扫描漏洞，此采集方式，因受其他两种扫描方式的影响，扫描周期不固定，不方便您定期维护服务器漏洞，建议您采用其他两种扫描方式。

- 定时扫描

  默认HSS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。

- 主机安全服务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Ubuntu、CentOS、EulerOS、Debian、AlmaLinux系统。

表 4-3 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)
Linux	• EulerOS 2.2、2.3、2.5、2.8、2.9（64位） • CentOS 7.4、7.5、7.6、7.7、7.8、7.9（64位） • Ubuntu 16.04、18.04、20.04、22.04（64位） • Debian 9、10、11（64位） • kylin V10（64位） • HCE 1.1、2.0（64位） • Suse 12 SP5、15 SP1、15 SP2（64位） • 统信UOS V20服务器E版、V20服务器D版（64位）

手动扫描漏洞

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 单击漏洞管理界面右上角“手动扫描”。

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

表 4-4 手动扫描漏洞参数说明

参数	参数说明
漏洞类型	选择扫描的漏洞类型。目前支持扫描的漏洞类型如下： ● Linux系统漏洞 ● Windows系统漏洞 ● Web-CMS软件漏洞 ● 应用漏洞 ● 应急漏洞
扫描范围	选择扫描哪些服务器。 ● 全部服务器 ● 指定服务器 您可以选择服务器组或通过服务器名称、ID、公网IP、私网IP搜索目标服务器。 **说明** 以下服务器不能被选中执行漏洞扫描： ● 使用主机安全服务“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6 单击“确定”。

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

单击扫描情况列红色图形旁的数字，可以查看扫描失败的服务器信息。

说明

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

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

----结束

定时扫描漏洞（漏洞策略配置）

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

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

- 漏洞类型：选择需要扫描的漏洞类型。

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

    说明

    以下服务器不能被选中执行漏洞扫描：

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

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

单击扫描情况列红色图形旁的数字，可以查看扫描失败的服务器信息。

----结束

4.1.3 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 在页面左上角选择“区域”，单击  ，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面查看漏洞相关信息。

图 4-1 查看漏洞详情

- 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 4-5 漏洞扫描概览参数说明

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

- 查看漏洞详情

  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，鼠标滑动至服务器名称，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。

- 查看待处理或已处理漏洞

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

- 导出漏洞列表

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

说明

单次最多支持导出30000条漏洞数据。

----结束

查看漏洞详情（主机视图）

说明

基础版不支持该操作。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面左上方，选择“主机视图”，查看漏洞相关信息。

图 4-2 查看漏洞详情

- 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 4-6 漏洞扫描概览参数说明

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

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

- 查看主机详情和主机存在的漏洞
  a. 单击目标服务器名称，进入主机详情页面，您可以查看该主机的详细信息和存在的各类漏洞。
  b. 单击目标漏洞名称，进入漏洞详情页面，您可以查看该漏洞的漏洞CVE详情、受影响服务器、历史处置记录等信息。
- 查看待处理或已处理漏洞

  在漏洞列表上方，漏洞处理状态选框中选择“待处理”或“已处理”，筛选查看待处理或已处理的漏洞。
- 导出存在漏洞的主机列表

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

  说明

  单次最多支持导出30000条漏洞数据。

----结束

4.1.4 导出漏洞列表

您可以参考本章节导出漏洞列表到本地。

前提条件

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

导出漏洞列表（漏洞视图）

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面左上角，选择“漏洞视图”页签。

步骤5 在漏洞列表上方，单击“导出”，导出漏洞列表。

步骤6 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。

须知

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”。

步骤4 在漏洞管理界面左上方，选择“主机视图”页签。

步骤5 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。
  - 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6 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。

须知

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

4.1.5 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，您可以在主机安全服务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。下一次漏洞扫描任务执行后，HSS仍然会向您告警该漏洞。

- **添加漏洞白名单**

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

约束限制

- 主机安全服务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**。
- CentOS 6和CentOS 8官方已停止维护，HSS使用Redhat的补丁公告替代扫描，因此这两个操作系统的漏洞无法修复，建议您切换为其他操作系统。
- Ubuntu 18.04及以下版本目前已不支持免费补丁更新，需要购买配置Ubuntu Pro后才能安装升级包，未配置Ubuntu Pro会导致漏洞修复失败。
- CCE、MRS、BMS的主机不能修复内核漏洞，贸然修复可能导致功能不可用。
- CCE主机的内核漏洞不支持自动修复，主机安全服务在执行批量自动修复漏洞任务时会自动过滤不修复这类漏洞。
- 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，详细操作请参见**创建云服务器备份**。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。如果主机无法访问Internet，或者外部镜像源提供的服务不稳定时，可以使用华为云提供的镜像源进行漏洞修复。为了保证漏洞修复成功，请在执行在线升级漏洞前，确认主机中已配置华为云提供的对应操作系统的镜像源，详细的配置操作请参见**配置镜像源**。

漏洞修复优先级

漏洞修复优先级是由漏洞最高CVSS分值、漏洞发布时间和漏洞影响的资产重要性进行加权计算得出，反映了漏洞修复的紧急程度。

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。

处理漏洞

您可以选择以下方式处理漏洞。

自动修复漏洞（漏洞视图）

仅Linux系统漏洞和Windows系统漏洞支持控制台一键自动修复漏洞。

说明

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

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 修复Linux漏洞和Windows漏洞

- 修复单个漏洞。

  在目标漏洞所在行的“操作”列，单击“修复”。
- 修复多个漏洞。

  勾选当前页面所有目标漏洞，单击漏洞列表左上角的“批量修复”，批量修复漏洞。
- 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5 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6 （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，绑定存储库的操作请参见**绑定存储库**。
- 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。

图 4-3 创建备份

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

步骤7 在修复对话框中勾选知晓风险后，单击“自动修复”。

步骤8 单击漏洞名称，进入漏洞详情页面。

步骤9 选择“历史处置记录”页签，您可以查看目标漏洞“状态”列的修复状态。漏洞修复状态含义请参见**表 漏洞修复状态说明**。

表 4-7 漏洞修复状态说明

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

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

----结束

自动修复漏洞（主机视图）

仅Linux系统漏洞和Windows系统漏洞支持控制台一键自动修复漏洞。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 修复Linux漏洞和Windows漏洞。

- 修复服务器存在的所有Linux或Windows漏洞
  a. 在目标漏洞服务器所在行的“操作”列，单击“修复”。
  您也可以选中多台服务器，并在列表上方单击“批量修复”；如果需要修复所有服务器的漏洞，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，绑定存储库的操作请参见绑定存储库。
  - 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。

图 4-4 创建备份

ii. 单击“管理”，系统弹出创建备份弹窗。

iii. 在创建备份弹窗中，选择备份存储库、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**。

- 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。如果需要修复所有服务器的漏洞，不勾选任何服务器，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，绑定存储库的操作请参见**绑定存储库**。
- 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。

图 4-5 创建备份

ii. 单击“管理”，系统弹出创建备份弹窗。

iii. 在创建备份弹窗中，选择备份存储库、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”。

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**。

表 4-8 漏洞修复状态说明

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

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

----结束

手动修复漏洞

对于Web-CMS漏洞、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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 单击目标漏洞名称，进入漏洞详情页面，查看修复建议。

----结束

参考漏洞修复方案进行漏洞修复

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

- 方案一：创建新的虚拟机执行漏洞修复
  a. 为需要修复漏洞的ECS主机创建镜像，详细操作请参见**通过云服务器创建整机镜像**。
  b. 使用该镜像创建新的ECS主机，详细操作请参见**通过镜像创建云服务器**。
  c. 在新启动的主机上执行漏洞修复并验证修复结果。
  d. 确认修复完成之后将业务切换到新主机。
  e. 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。
- 方案二：在当前主机执行修复

a. 为需要修复漏洞的ECS主机创建备份，详细操作请参见**创建云服务器备份**。

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，详细操作请参见**使用备份恢复服务器**。

说明

- 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。新创建的ECS主机建议采用按需计费的方式创建，待业务切换完成后可以根据需要转换为包周期计费模式。如果漏洞修复不成功可以随时释放以节省开销。
- 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。
- 手动修复漏洞完成后，建议您**验证修复结果**。

忽略漏洞

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

忽略后，主机安全服务将不会对该漏洞告警。

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在目标漏洞所在行的“操作”列，单击“忽略”。

步骤5 在弹出的对话框中，单击“确认”。

----结束

漏洞添加白名单

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

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

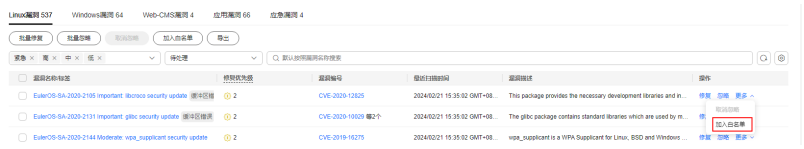
- 将漏洞影响的所有服务器加入白名单

  HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。

  a. 在目标漏洞所在行的“操作”列，选择“更多 > 加入白名单”。

  您也可以都选多个目标漏洞，单击漏洞列表上方的“加入白名单”。

图 4-6 将漏洞影响的所有服务器加入白名单



b. 在弹出的对话框中，单击“确认”。

- 将漏洞影响的单个或多个服务器加入白名单。

  HSS为这些服务器扫描漏洞时，不再关注漏洞。

  a. 单击目标漏洞的名称，进入漏洞详情页面。
  b. 选择“受影响服务器”页签。
  c. 在目标服务器所在行的“操作”列，选择“更多 > 加入白名单”。

     您也可以勾选多个服务器，单击服务器列表上方的“加入白名单”。

图 4-7 将漏洞影响的单个服务器加入白名单

d. 在弹出的对话框中，单击“确认”。

- 通过白名单规则将漏洞加入白名单。

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

图 4-8 配置白名单规则

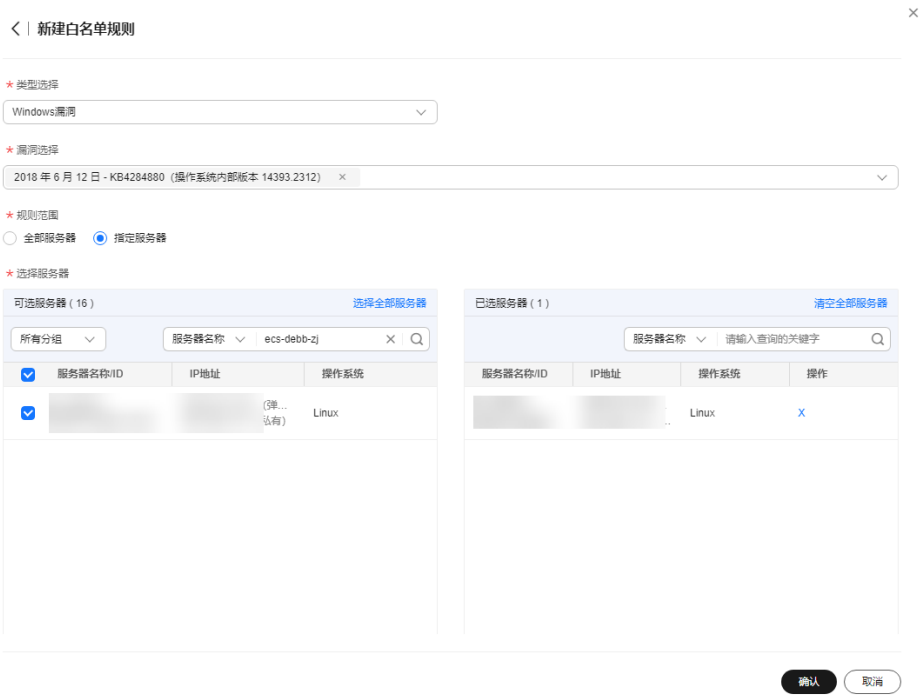


表 4-9 漏洞白名单规则参数说明

参数	说明
类型选择	选择添加白名单的漏洞类型： ■ Linux系统漏洞 ■ Windows系统漏洞 ■ Web-CMS软件漏洞 ■ 应用漏洞 ■ 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，单击“验证”，进行一键验证。

  说明

  - 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 4-10 验证修复命令

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

- **方式三**：手动执行漏洞检测查看漏洞修复结果。

4.1.6 管理漏洞白名单

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

本章节为您介绍漏洞如何加入白名单，以及如何修改和删除漏洞白名单。

约束限制

HSS基础版不支持该功能，购买和升级HSS的操作请参见购买主机安全防护配额和配额版本升级。

漏洞添加白名单

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

- 将漏洞影响的所有服务器加入白名单

  HSS扫描所有服务器存在的漏洞时，不再关注该漏洞。

a. 在目标漏洞所在行的“操作”列，选择“更多 > 加入白名单”。
您也可以都选多个目标漏洞，单击漏洞列表上方的“加入白名单”。

图 4-9 将漏洞影响的所有服务器加入白名单

b. 在弹出的对话框中，单击“确认”。

- 将漏洞影响的单个或多个服务器加入白名单。
HSS为这些服务器扫描漏洞时，不再关注漏洞。
a. 单击目标漏洞的名称，进入漏洞详情页面。
b. 选择“受影响服务器”页签。
c. 在目标服务器所在行的“操作”列，选择“更多 > 加入白名单”。
您也可以勾选多个服务器，单击服务器列表上方的“加入白名单”。

图 4-10 将漏洞影响的单个服务器加入白名单

d. 在弹出的对话框中，单击“确认”。

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

图 4-11 配置白名单规则

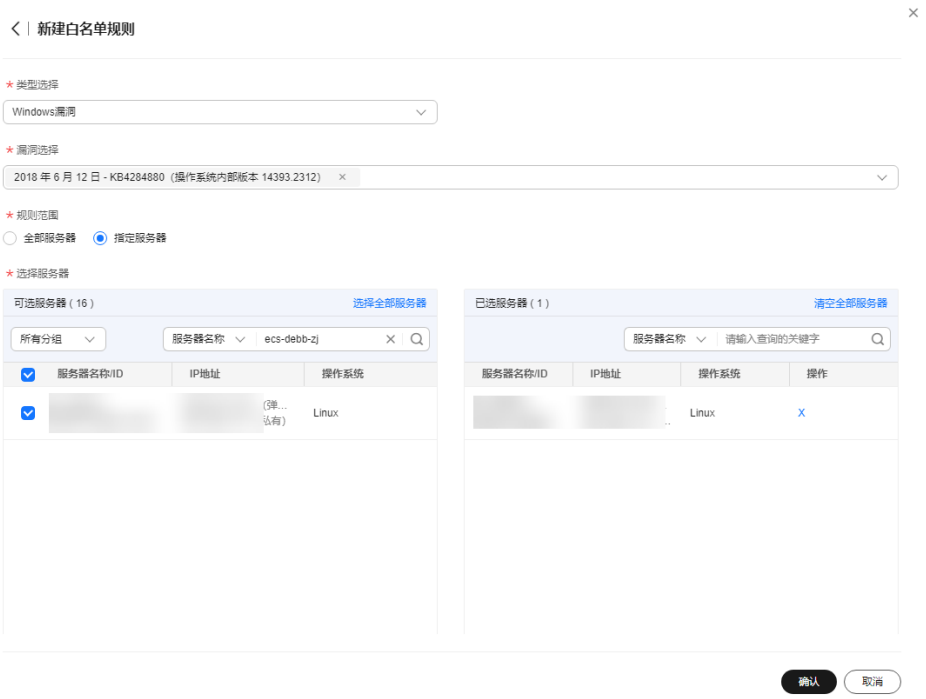


表 4-11 漏洞白名单规则参数说明

参数	说明
类型选择	选择添加白名单的漏洞类型： ■ Linux系统漏洞 ■ Windows系统漏洞 ■ Web-CMS软件漏洞 ■ 应用漏洞 ■ 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

编辑漏洞白名单

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。

步骤5 在目标漏洞白名单规则所在行的“操作”列，单击“编辑”。

步骤6 在编辑界面，完成信息修改后，单击“确认”。

----结束

删除漏洞白名单

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，单击“漏洞策略配置”，进入漏洞策略配置页面。

步骤5 在目标漏洞白名单规则所在行的“操作”列，单击“删除”。

步骤6 在弹窗中确认信息后，单击“确认”。

----结束

4.1.7 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，购买和升级HSS的操作请参见购买主机安全防护配额和配额版本升级。

查看单个漏洞的历史处置记录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 在已处理漏洞列表中，单击漏洞名称，进入漏洞详情页面。

图 4-12 选择已处理漏洞

步骤5 选择“历史处置记录”页签，查看单个漏洞的历史处置记录。

图 4-13 历史处置记录

----结束

查看所有漏洞的历史处置记录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 选择“漏洞管理”页签，查看所有漏洞的历史处置记录。

- 查看指定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，输入漏洞类型、漏洞名称、服务器IP等并单击，可查看指定属性的漏洞处置记录。

----结束

4.2 基线检查

4.2.1 基线检查概述

基线检查包含口令复杂度策略检测、经典弱口令检测、配置检查，可检测主机中不安全的口令配置、关键软件中含有风险的配置信息，并针对所发现的风险为您提供**修复建议**，帮助您正确地处理服务器内的各种风险配置信息。

基线检查内容

检查项名称	检查详情说明	支持的检查方式	支持的HSS版本
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。 目前支持的检测标准及类型如下： • Linux系统： – 云安全实践：Apache2、Docker、MongoDB、Redis、MySQL5、Nginx、Tomcat、SSH、vsftp、CentOS7、EulerOS、EulerOS_ext、Kubernetes-Node、Kubernetes-Master、MySQL5.7、Nginx1.17、Redis6.2、Apache2.4、Kafka、ZooKeeper3.6、GaussDB、Tomcat8、Tomcat9、HCE1.1、HCE2.0。 – 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS6、CentOS7、CentOS8、Debian9、Debian10、Debian11、Redhat6、Redhat7、Redhat8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma、SUSE 12、SUSE 15、HCE1.1。 • Windows系统： 云安全实践：MongoDB、Apache2、MySQL、Nginx、Redis、Tomcat、Windows_2008、Windows_2012、Windows_2016、Windows_2019、SqlServer。	• 自动执行基线检查 • 手动执行基线检查	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。	手动执行基线检查	所有版本

检查项名称	检查详情说明	支持的检查方式	支持的HSS版本
经典弱口令检测	通过与弱口令库对比，检测账号口令是否属于常用的弱口令，提示用户修改不安全的口令。 Linux支持MySQL、FTP及系统账号的弱口令检测，Windows支持系统账号的弱口令检测。	• 自动执行基线检查 • 手动执行基线检查	所有版本

使用流程

表 4-12 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：主机安全服务默认**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和经典弱口令检测自动检测周期，配置操作详情请参见**配置检测**、**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。

4.2.2 执行基线检查

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和经典弱口令检测。
- 手动执行基线检查：如需查看指定服务器的实时基线风险，或者进行口令复杂度策略检测，您可以手动执行基线检查。

自动执行基线检查

主机安全服务默认**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和经典弱口令检测自动检测周期，配置操作详情请参见**配置检测**、**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 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

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。

图 4-14 基线检查概览

步骤4 （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。

图 4-15 新建基线策略

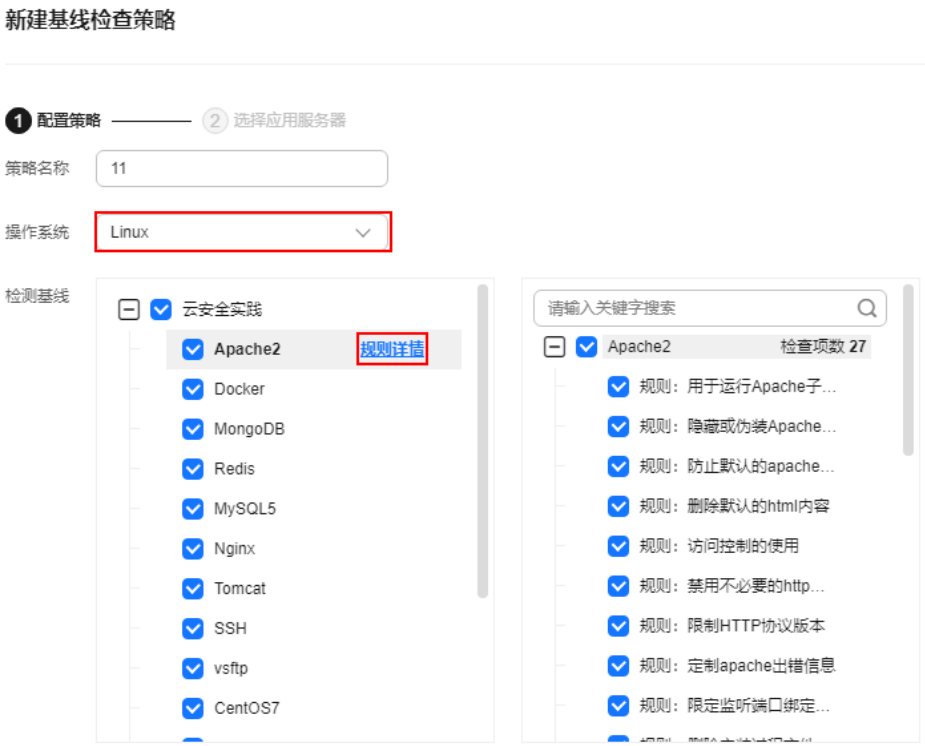


表 4-13 新建基线策略信息

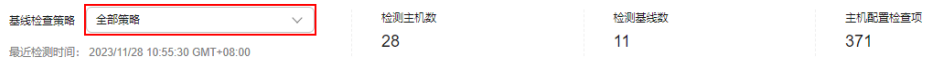
参数名称	参数说明	取值样例
策略名称	自定义策略名称。	linux_web1_security_policy
操作系统	选择基线检测的目标系统。 – Linux – Windows	Linux

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、MySQL5.7、Nginx1.17、Redis6.2、Apache2.4、Kafka、ZooKeeper3.6、GaussDB、Tomcat8、Tomcat9、HCE1.1、HCE2.0。 ▪ 等保合规：Apache2、MongoDB、MySQL5、Nginx、Tomcat、CentOS6、CentOS7、CentOS8、Debian9、Debian10、Debian11、Redhat6、Redhat7、Redhat8、Ubuntu12、Ubuntu14、Ubuntu16、Ubuntu18、Alma、SUSE 12、SUSE 15、HCE1.1。 – 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 等保合规：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5 在基线检查页面左上方，选择目标“基线检查策略”。

图 4-16 选择目标基线策略



步骤6 单击页面右上角“手动检测”，执行检测。

步骤7 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

4.2.3 查看并处理基线检查结果

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。

约束限制

仅企业版、旗舰版、网页防篡改版和容器版支持配置检查。

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

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“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手动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。

图 4-17 基线检查概览

表 4-14 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。
口令复杂度策略检测	对所有主机存在弱口令复杂度不满足基线标准的进行统计。
经典弱口令检测	按照主机的维度对存在弱口令的主机及涉及的账号进行统计。

----结束

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4-15所示。

图 4-18 查看配置检查统计

表 4-15 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
检查项	累计检查的配置项总数。
风险项	检查项中存在风险的配置项总数。
影响服务器数	目标风险基线所影响的服务器总数。
最新检测时间	最近一次检测的时间。
描述	目标风险基线的描述说明。

步骤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。

图 4-19 查看基线检查详情

步骤3 处理风险项。

- **忽略风险**

在目标检查项“操作”列单击“忽略”，忽略单条风险检查项。或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。

图 4-20 忽略风险

- **修复风险**
  a. 单击目标风险项“操作”列的“检查详情”，查看检查项详情。
  b. 查看“审计描述”、“修改建议”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。

     说明

     - 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、CentOS6、CentOS7、CentOS8、EulerOS、Debian9、Debian10、Debian11、Redhat6、Redhat7、Redhat8、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4-16所示。

图 4-21 查看口令复杂度策略检测统计

表 4-16 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	目标服务器的口令长度是否符合标准。 • 符合 • 不符合
大写字母	目标服务器的口令大写字母是否符合标准。 • 符合 • 不符合
小写字母	目标服务器的口令小写字母是否符合标准。 • 符合 • 不符合
数字	目标服务器的口令数字是否符合标准。 • 符合 • 不符合
特殊字符	目标服务器的口令特殊字符是否符合标准。 • 符合 • 不符合
建议	对目标服务器发现的口令风险的修改建议。

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。

图 4-22 查看经典弱口令检测

表 4-17 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

4.2.4 导出基线检查报告

您可以参考本章节导出基线检查报告到本地。

约束限制

仅企业版、旗舰版、网页防篡改版和容器版支持配置检查。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

步骤4 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，在列表右上角单击，导出“配置检查”结果。

  可单击“风险等级”和“标准类型”对告警信息进行筛选下载。

- 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

4.2.5 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

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。

图 4-23 基线检查概览

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“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6 确认修改无误，单击“下一步”，编辑需要应用的服务器。

步骤7 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 基线检查”，进入基线检查页面。

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。

图 4-24 基线检查概览

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

4.3 容器镜像安全

4.3.1 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，详细操作请参见**开启容器版防护**。

约束限制

仅支持查看Linux镜像存在的漏洞。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

步骤4 选择“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 4-18 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

4.3.2 镜像恶意文件

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

检测周期

容器安全服务**每日凌晨**自动执行一次全面的检测。

前提条件

已开启容器节点防护。

约束限制

仅支持检测Linux镜像存在的恶意文件。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击  ，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“风险预防 > 容器镜像安全”。

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

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

----结束

5 主动防御

5.1 应用防护

5.1.1 开启应用防护

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。

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。

前提条件

已开启主机安全服务版本为旗舰版、网页防篡改版或容器版。

约束限制

- 当前只支持操作系统为Linux的服务器。
- 目前仅支持Java应用接入。
- 仅旗舰版、网页防篡改版或容器版支持应用防护相关操作。

操作步骤

步骤1 登录管理控制台。

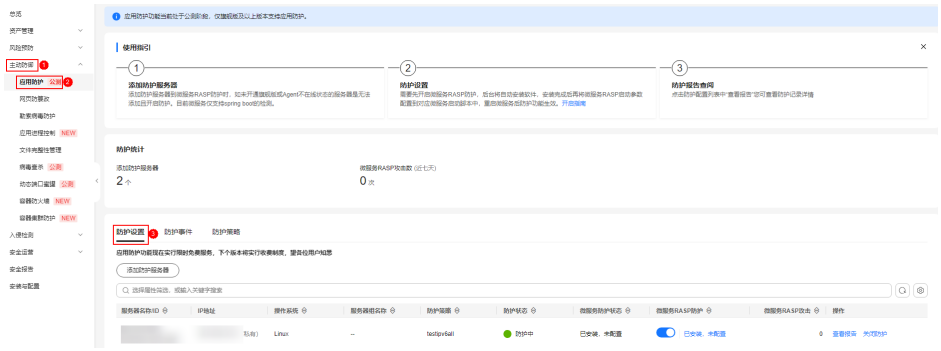
步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 应用防护 > 防护设置”，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。

图 5-1 查看防护配置

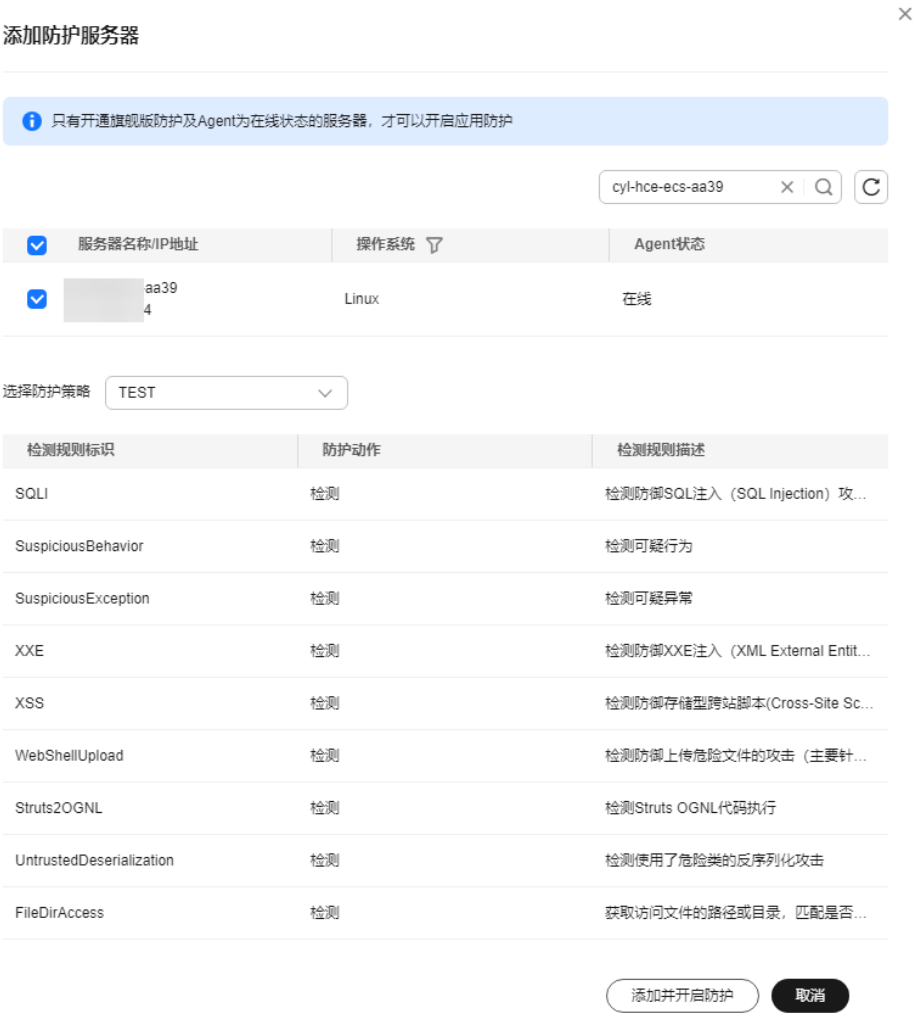


步骤4 单击“添加防护服务器”，在弹窗中选择需要防护的服务器和策略。

说明

防护策略可自定义创建，未创建选择默认策略即可。

图 5-2 选择目标服务器和策略



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。

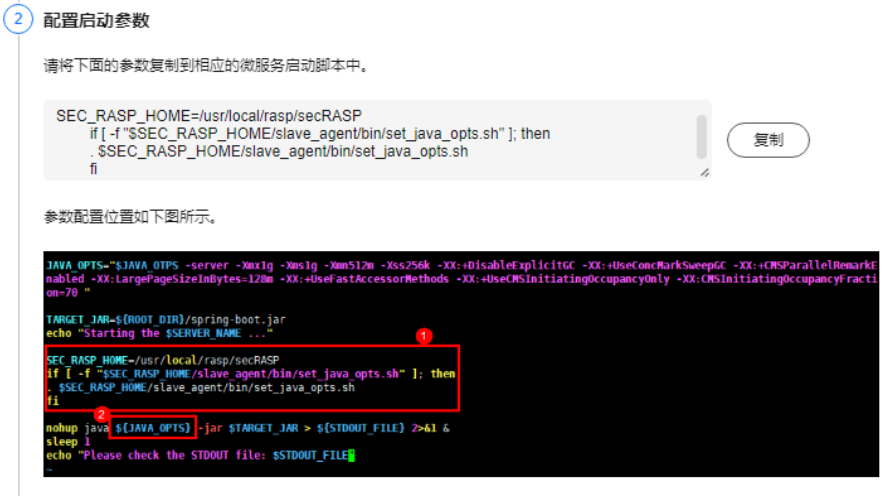
图 5-3 查看开启防护流程

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。

图 5-4 软件安装完成

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。

图 5-5 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

5.1.2 查看应用防护

开启应用防护后，您可以在应用防护界面查看应用防护状态、防护事件等信息，了解应用防护情况。

前提条件

已开启应用防护，详细操作请参见**开启应用防护**。

约束限制

- 当前只支持操作系统为Linux的服务器。
- 目前仅支持Java应用接入。
- 仅旗舰版、网页防篡改版或容器版支持应用防护相关操作。

查看防护设置

步骤1 登录管理控制台。

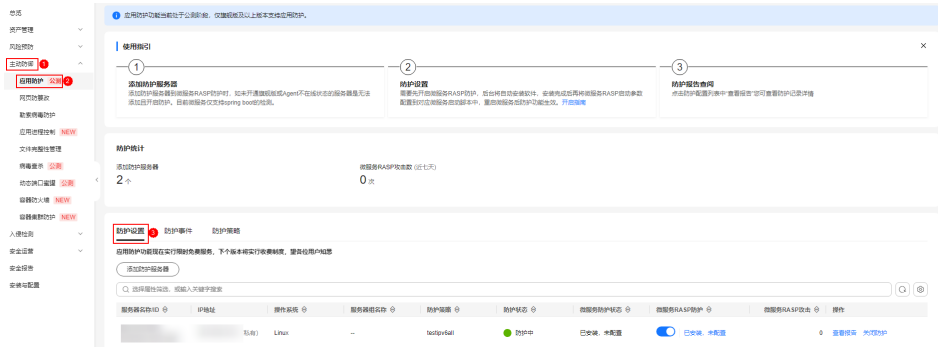
步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 应用防护 > 防护设置”，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。

图 5-6 查看防护配置



步骤4 选择“防护设置”页签，查看服务防护情况，参数说明如表5-1所示。

表 5-1 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。
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。

参数名称	参数描述
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。
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，进入主机安全服务页面。

步骤2 选择“主动防御 > 应用防护 > 防护事件”，进入“防护事件”页面，参数说明如**表5-2**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”。

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。

表 5-2 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
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3 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

5.1.3 管理应用防护策略

您可自定义添加、编辑、删除应用防护策略，可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。

约束限制

- 当前只支持操作系统为Linux的服务器。
- 目前仅支持Java应用接入。
- 仅旗舰版、网页防篡改版或容器版支持应用防护相关操作。

添加防护策略

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表5-3所示。

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。

表 5-3 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4 单击“添加防护策略”，在弹窗中填写策略名称，勾选该策略需要检测的规则，配置部分检测规则的内容详情，参数说明如表5-4所示。

图 5-7 添加防护策略

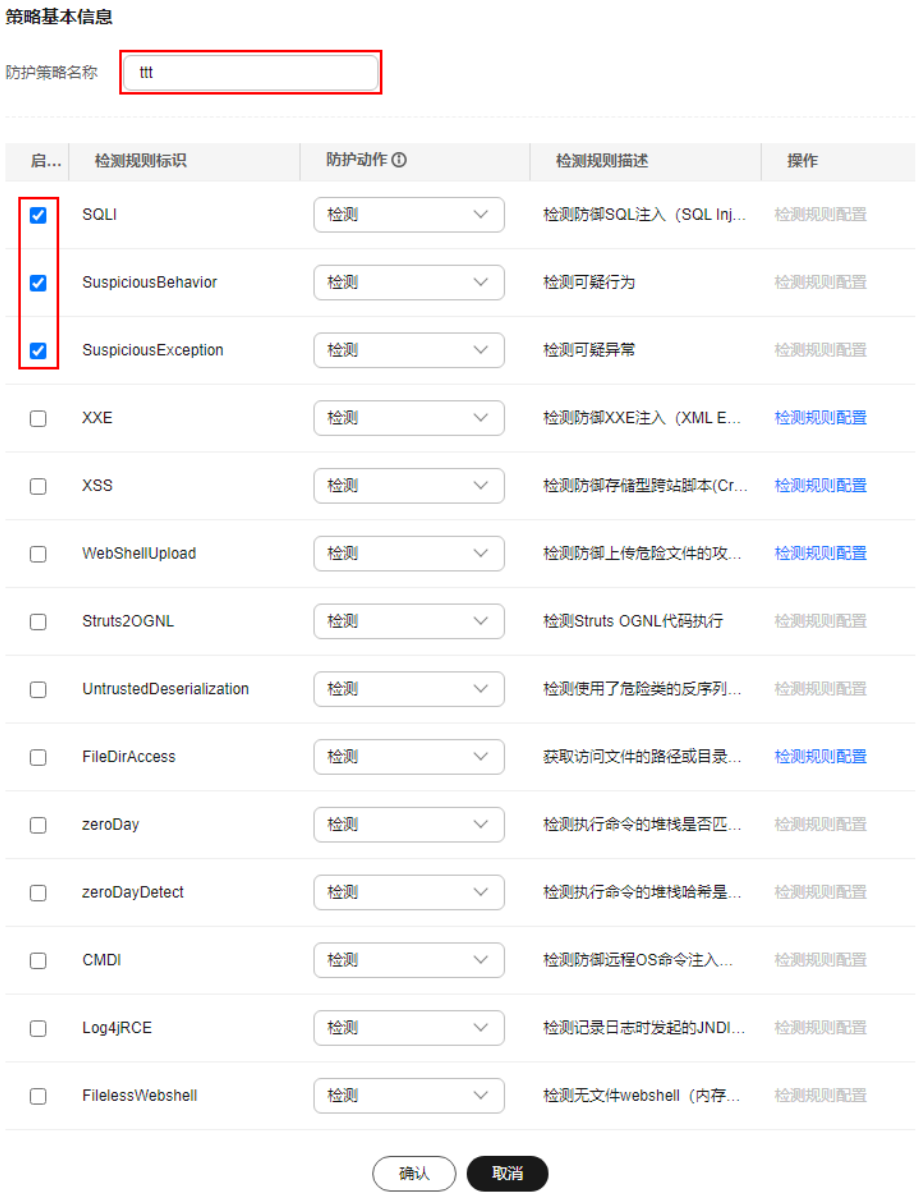


表 5-4 应用防护策略参数说明

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	目前支持自定义的选择的所有检测规则标识。

参数名称	参数说明
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5 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5-5所示。

表 5-5 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6 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，进入主机安全服务页面。

步骤2 选择“主动防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表5-6所示。

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。

表 5-6 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3 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 5-7 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	目前支持自定义的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4 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，进入主机安全服务页面。

步骤2 选择“主动防御 > 应用防护 > 防护策略”，进入“防护策略”页面，参数说明如表5-8所示。

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。

表 5-8 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3 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

删除的策略如果存在关联的服务器，需先将目标服务器绑定至不会删除的防护策略，否则目标策略删除按钮会处于隐藏状态，无法删除。

----结束

5.1.4 关闭应用防护

本章节为您介绍如何关闭应用防护。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 应用防护 > 防护设置”，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。

图 5-8 查看防护配置

步骤4 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5 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

5.2 网页防篡改

5.2.1 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。

使用约束

服务器已开启HSS网页防篡改版防护，购买和开启防护的操作，请参见**购买主机安全防护配额**、**开启网页防篡改防护**。

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 5-9 网页防篡改原理

防护类型	原理说明
静态网页防护	1. 锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站管理员可通过特权进程进行更新网站内容。 2. 主动备份恢复 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 如果本地主机上的文件目录和备份目录失效，用户可以在自己的远端备份服务器上手动获取备份文件恢复被篡改的网页。
动态网页防护	提供Tomcat应用运行时自我保护，防护原理如下： 1. 基于RASP过滤恶意行为 采用华为自研RASP检测应用程序行为，有效阻断攻击者通过应用程序篡改网页内容的行为。 2. 网盘文件访问控制 精细化定义网盘文件中的文件访问权限，包括新增，修改，查询等，确保防篡改同时不影响网站内容发布。

网页防篡改使用流程

图 5-9 使用流程图

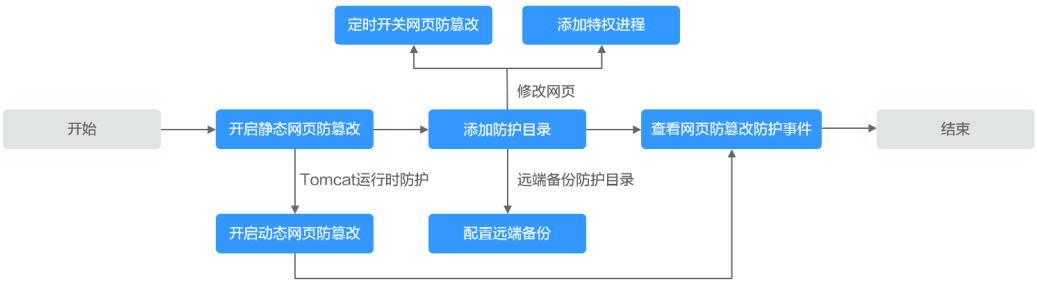


表 5-10 网页防篡改使用流程说明

操作项	描述
开启静态网页防篡改	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，HSS网页防篡改版支持的功能详情请参见服务版本差异。
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	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。
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。
开启动态网页防篡改	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	静态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。

5.2.2 添加防护目录

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

前提条件

已开启主机安全服务版本为网页防篡改版。

约束与限制

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

添加防护目录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-10 进入防护配置

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。

图 5-11 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5-11**。

图 5-12 添加防护目录

表 5-11 防护规则

参数	说明	限制
防护目录	防护目录下的文件和文件夹为只读。	请勿对操作系统目录进行防护。
排除子目录	- 排除防护目录下不需要防护的子目录，例如临时文件目录。 - 多个子目录请用英文分号隔开，最多可添加10个子目录。	排除子目录为防护目录中的相对目录。

参数	说明	限制
排除文件类型	- 排除防护目录下不需要防护的文件类型，例如Log类型的文件。 - 多个文件类型请用英文分号隔开。 - 为实时记录主机中的运行情况，请排除防护目录下Log类型的文件，您可以为日志文件添加等级较高的读写权限，防止攻击者恶意查看或篡改日志文件。	-
本地备份路径	- 仅支持Linux系统。 - 开启网页防篡改防护后，防护目录下的文件会自动备份到设置的本地备份路径中。 - 防护目录下文件大小不同，备份时间也不同，一般约10分钟备份完成。备份完成后，立即生效。 - 被排除的子目录和文件类型不会备份。 - 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。	本地备份路径与添加的防护目录不能重叠。
排除文件路径列表	- 排除防护目录下不需要防护的路径。 - 多个路径请用英文分号隔开，最多可添加50个路径，路径最长字符限制为256。 - 单个路径不能以空格开始，不能以/结束。	排除文件路径为防护目录的相对文件路径。

2. 添加完成后，单击“确认”，完成添加防护目录的操作。

   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**配置远端备份**。

1. 在“防护目录设置”页单击“启动远端备份”。

图 5-13 开启远端备份

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。

5.2.3 配置远端备份

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

如果本地主机上的文件目录和备份目录失效，用户可以在自己的远端备份服务器上手动获取备份文件恢复被篡改的网页。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

前提条件

设置为远端备份服务器的主机，需要满足以下条件：

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

须知

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

添加远端备份服务器

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-14 进入防护配置

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。

图 5-15 防护目录设置页面

步骤5 单击“管理远端备份服务器”，在弹出的对话框中，“添加远端备份服务器”，填写备份服务器信息，相关参数说明请参见表5-12。

图 5-16 填写备份服务器信息

表 5-12 添加远端备份服务器参数说明

参数名称	说明
地址	该地址为华为云主机的私网地址。
端口	请确保设置的端口未被安全组、防火墙等拦截，并且未被占用。
备份路径	将需要备份的防护目录下的内容备份在该远端备份服务器的目录下。 ● 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“网页放篡改”防护，那么该备份路径与自身的“防护目录”不能重叠，否则会导致远端备份失败。

步骤6 单击“确认”，完成添加备份服务器的操作。

----结束

启动远端备份

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-17 进入防护配置

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。

图 5-18 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-19 进入防护配置

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。

图 5-20 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。

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

添加特权进程

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

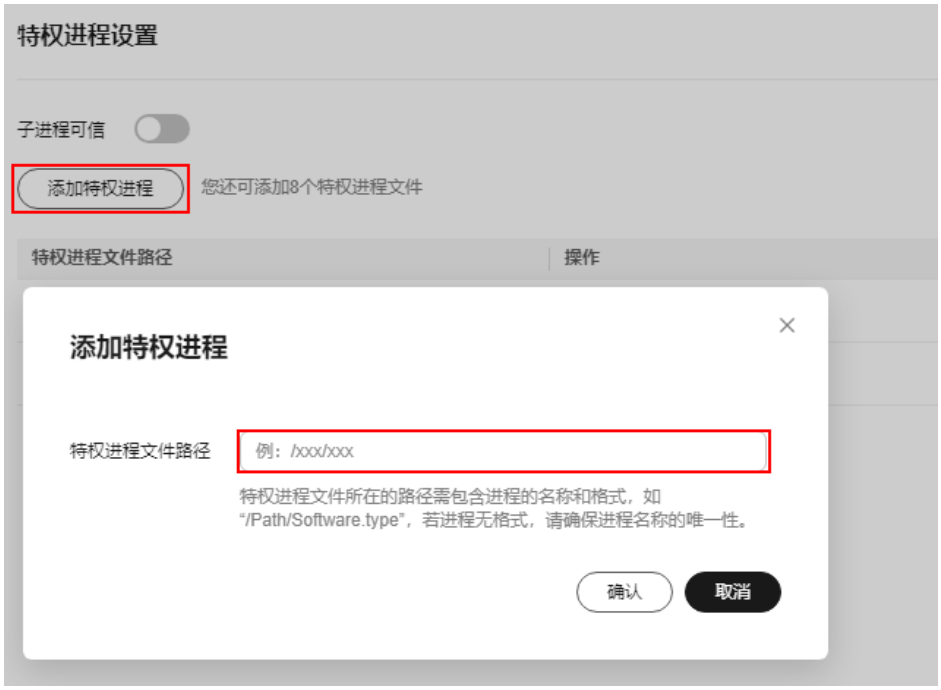
图 5-21 进入防护配置

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。

图 5-22 选择特权进程设置

步骤5 在“特权进程设置”页面，单击“添加特权进程”。

图 5-23 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。

步骤8 开启“子进程可信”开关，可开启对已添加特权文件路径下子进程的可信。

说明

开启后将对添加的所有特权进程文件下5个层级内的子进程可信。

----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。

5.2.5 定时开启/关闭静态网页防篡改

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

说明

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

关闭防护时段设置规则

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-24 进入防护配置

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。

图 5-25 设置定时防护参数

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。

   图 5-26 添加关闭时间段信息

   说明

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

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

   示例：勾选值为周一、周四、周六，则服务器在这些时间的关闭防护时间段自动关闭防篡改功能，关闭时间结束服务器自动启动静态网页防篡改。

图 5-27 勾选关闭防护周期

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。

图 5-28 开启定时开关

----结束

5.2.6 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 5-29 进入防护配置

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。

图 5-30 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。

图 5-31 设置 Tomcat 目录

步骤6 单击“确认”，开启动态网页防篡改。

----结束

5.2.7 查看网页防篡改防护事件

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

约束限制

仅开启网页防篡改版防护后才支持防篡改相关操作。

前提条件

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

操作步骤

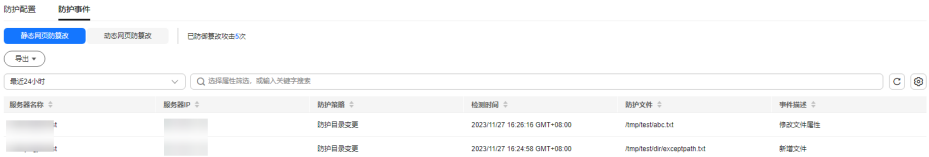
步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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”。

图 5-32 防护事件



----结束

5.3 勒索病毒防护

5.3.1 购买备份存储库

为了进一步提升您主机的勒索病毒防御能力，降低主机被勒索后的业务损失风险，建议您开启勒索防护备份，定期为服务器备份数据。在开启勒索备份之前，您需要购买备份存储库。

您可以参考本章节在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，在云备份购买备份存储库的操作请参见**创建云服务器备份**。

购买备份存储库

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护 ”，进入勒索病毒防护界面。

步骤4 选择“防护服务器”页签。

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 5-13 购买备份容量参数说明

参数名称	参数说明
计费模式	选择计费模式，支持“包年/包月”和“按需计费”。 ● 包年/包月：按照订单的购买周期进行结算。 ● 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。
购买时长	根据需求选择购买时长，当计费模式选择“按需计费”时无需选择。

参数名称	参数说明
配置费用	• 包年/包月：选择的备份存储库容量、购买时长所需的费用。 • 按需计费：选择的备份存储库容量每小时所需的费用。

步骤7 单击“确认”，根据不同的计费模式执行后续操作。

- “包年/包月”计费模式：
  a. 进入订单确认页面。
  b. 确认订单无误后，单击“确认付款”，完成支付，购买成功。
- “按需计费”计费模式：
  购买成功。

  说明

  请注意后续备份存储库使用过程中，会持续计费，请保证您账户中余额充足，避免因为备份存储库按需计费导致您的账户欠费。

----结束

5.3.2 开启勒索病毒防护

勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机业务中断、数据泄露或丢失，主机所有者即使支付赎金也可能难以挽回所有损失，因此勒索病毒是当今网络安全面临的最大挑战之一。主机安全服务支持静态、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。

如果Linux主机安装的Agent版本为3.2.10及以上版本或Windows主机安装的Agent版本为4.0.22及以上版本，开启主机安全服务旗舰版、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**，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）；此外，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**开启勒索备份**。

如果主机安装的Agent版本非上述版本，或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。

前提条件

- 已开启主机安全服务版本为旗舰版、网页防篡改版或容器安全版。
- 已创建防护策略，详细操作请参见**创建防护策略**。

约束限制

- 服务器勒索备份功能仅支持华为云主机。
- 仅旗舰版、网页防篡改版、容器版支持勒索病毒防护功能。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

步骤4 选择“防护服务器”页签。

步骤5 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6 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7 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。

----结束

5.3.3 开启勒索备份

为了进一步提升您主机的勒索病毒防御能力，降低主机被勒索后的业务损失风险，建议您开启勒索防护备份，定期为服务器备份数据。

前提条件

- 已开启主机安全服务版本为旗舰版、网页防篡改版或容器安全版。
- 已购买备份存储库，详细操作请参见**购买备份存储库**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护 ”，进入“勒索病毒防护”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4 选择“防护服务器”页签。

步骤5 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6 在“开启备份”弹窗中，选择需要为服务器绑定的存储库。

说明

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7 单击“确认”，开启备份。

----结束

5.3.4 查看并处理勒索病毒防护事件

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

前提条件

已开启主机安全服务版本为旗舰版、网页防篡改版或容器安全版。

约束限制

- 勒索备份功能仅支持华为云主机。
- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护 ”，进入“勒索病毒防护”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4 选择“防护事件”页签，查看防护事件。

步骤5 确认防护事件的危害程度后，在目标事件的操作列单击“处理”，处理该事件。处理方式说明请参见**表 告警事件处理方式说明**。

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。

表 5-14 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**。 **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	自行手动处理事件，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。

处理方式	处理方式说明
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”，自定义设置需要屏蔽的文件路径，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。

----结束

5.3.5 管理勒索病毒防护策略

如果系统预置的勒索病毒防护策略不满足您的防护需求，您可以为服务器切换防护策略，或者新建、修改勒索病毒防护策略。

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。

新建防护策略

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护 ”，进入“勒索病毒防护”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4 选择“防护策略”页签，单击“添加防护策略”。

步骤5 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**。

图 5-33 设置防护策略参数

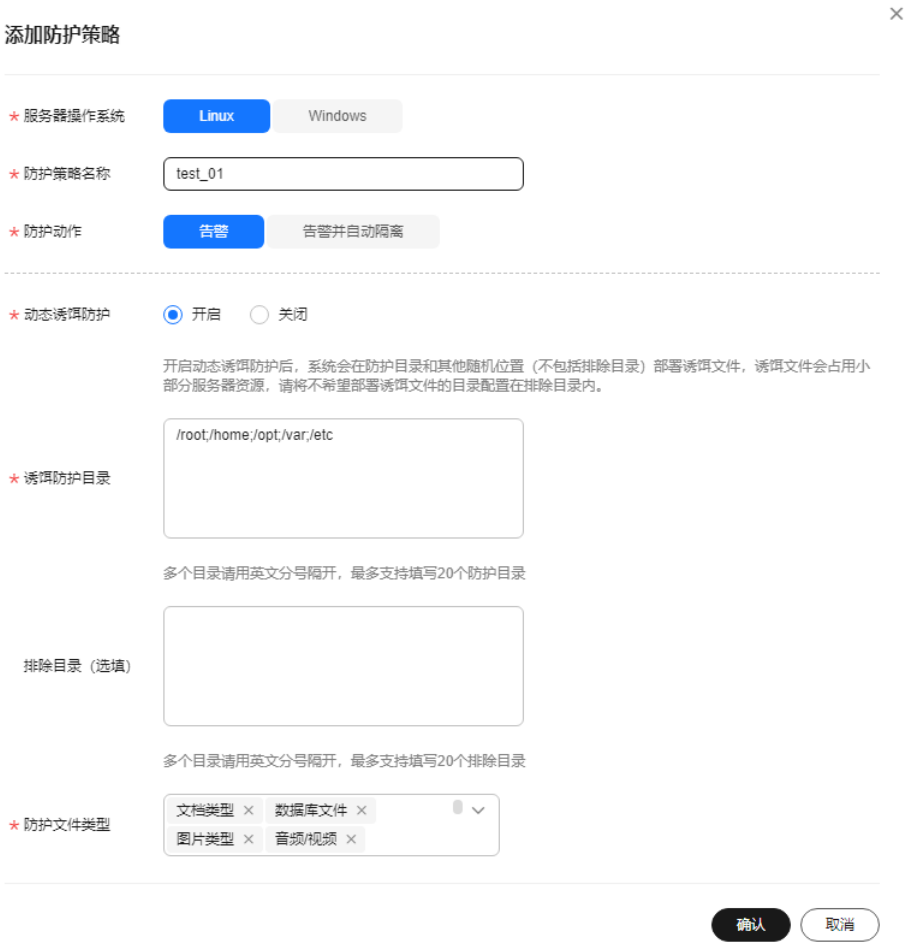


表 5-15 防护策略参数说明

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。	test
防护动作	发现勒索病毒事件后的处理方式。 • 告警并自动隔离 • 告警	告警并自动隔离

参数名称	参数说明	取值样例
动态诱饵防护	开启动态诱饵防护后，系统会在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，请将不希望部署诱饵文件的目录配置在排除目录内。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	需要部署静态诱饵进行防护的目录（不包括子目录），建议配置为重要业务目录或数据目录。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc Windows：C:\Test
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：/etc/lesuo Windows：C:\Test\ProData
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、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选
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。	-

步骤6 单击“确认”，添加完成。

----结束

切换防护策略

如果服务器当前的防护策略不满足您的防护需求，您可以为服务器切换防护策略。

步骤1 选择“防护服务器”页签。

步骤2 选中目标服务器，并在服务器列表上方单击“切换防护策略”。

步骤3 在“切换防护策略”弹窗中，选择防护策略。

步骤4 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，进入主机安全服务界面。

步骤2 选择“主动防御 > 勒索病毒防护 > 防护策略 ”。

步骤3 单击目标防护策略操作列的“编辑”，弹出防护策略编辑页面，对策略信息和关联服务器进行编辑，参数说明如表5-16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 5-16 防护策略参数说明

参数名称	参数说明	取值样例
防护策略名称	设置防护策略的名称。	test
防护动作	发现勒索病毒事件后的处理方式。 • 告警并自动隔离 • 告警	告警并自动隔离
动态诱饵防护	开启动态诱饵防护后，系统会在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。诱饵文件会占用小部分服务器资源，请将不希望部署诱饵文件的目录配置在排除目录内。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	需要部署静态诱饵进行防护的目录（不包括子目录），建议配置为重要业务目录或数据目录。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc Windows：C:\Test
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：/etc/lesuo Windows：C:\Test\ProData
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、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选
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。	-

参数名称	参数说明	取值样例
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4 确认信息无误，单击“确认”，完成防护策略修改。

----结束

删除防护策略

步骤1 登录管理控制台，进入主机安全服务界面。

步骤2 选择“主动防御 > 勒索病毒防护 > 防护策略 ”。

步骤3 单击目标策略“操作”列的“删除”。

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4 在弹窗确认正在删除的策略信息，确认无误，单击“确认”，完成删除。

----结束

5.3.6 管理服务器备份

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。如果备份存储库的容量、备份策略不满足您的需求，您可以扩充容量、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**。

扩充备份容量

步骤1 登录管理控制台，进入主机安全服务界面。

步骤2 在导航树选择“主动防御 > 勒索病毒防护”，进入防护服务器列表，单击目标服务器“操作”列的“扩容”。

步骤3 在弹出窗口中输入“新增容量（GB）”。

图 5-34 输入新增容量值

步骤4 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，进入主机安全服务界面。

步骤2 在导航树选择“主动防御 > 勒索病毒防护”，进入防护服务器列表，单击目标服务器“备份策略状态”列的策略名称。

步骤3 在弹出对话框中配置策略，参数详情如**表 策略参数说明**所示。

图 5-35 配置策略

表 5-17 策略参数说明

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：至少选择一周中的某一天。 • 按天：最少每隔1天、最大每隔30天执行自动备份。	按周
备份时间	选择固定的时间点进行自动备份。 **说明** 配置策略案例说明 策略1：备份周期选择按周（周三、周六），备份时间选择00：00、13：00。释义：在每周三和每周六的00：00、13：00两个时间点实行自动备份。 策略2：备份周期选择按天（每隔2天），备份时间选择02：00、14：00。释义：即日起，每隔两天之后的02：00、14：00执行自动备份。	00：00、07：00
时区	选择备份时间所属的时区。	UTC+08：00

步骤4 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。

图 5-36 按数量配置保留规则

表 5-18 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	配置保留最新备份的数量。 **须知** 此处配置的备份保留数量为系统最终保留的份数，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

参数名称	参数说明	取值样例
高级选项（可选）	以日、周、月、年为单位周期，配置保留周期内每天最新的一个备份。 - 日备份规则：以天为单位，保留自定义天以内每天最新的一个备份。 - 周备份规则：以周为单位，保留自定义周以内每天最新的一个备份。 - 月备份规则：以月为单位，保留自定义月以内每天最新的一个备份。 - 年备份规则：以年为单位，保留自定义年以内每天最新的一个备份。 **说明** 如果同时填写多个规则，保留备份按照时间最长的规则执行。	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。

图 5-37 按时间配置保留规则

表 5-19 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	选择自定义或固定保留备份数据的周期，选择后自动开启备份保留，满足周期备份数据后系统将自动删除更早的数据。 – 自定义：输入以天为单位的数值，备份数据满足自定义天数的保存周期后，系统自动删除最早产生的备份数据。 – 1个月：备份数据满足1个月的保存周期后，系统自动删除最早产生的备份数据。 – 3个月：备份数据满足3个月的保存周期后，系统自动删除最早产生的备份数据。 – 6个月：备份数据满足6个月的保存周期后，系统自动删除最早产生的备份数据。 – 1年：备份数据满足1年的保存周期后，系统自动删除最早产生的备份数据。	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，保留策略详情请参见**保留策略场景说明**。

步骤5 配置完成，单击“确认”，完成备份策略修改。

----结束

5.3.7 恢复服务器数据

如果服务器遭受勒索攻击，不幸失陷，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**。

操作步骤

步骤1 登录管理控制台，进入主机安全服务界面。

步骤2 在导航树选择“主动防御 > 勒索病毒防护”，选择“防护服务器”，在目标服务器的“操作”列选择“更多”单击“恢复数据”。

步骤3 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 5-20 备份数据源参数说明

参数名称	参数说明	取值样例l
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 • 正在创建 • 正在删除 • 正在恢复 • 错误 当为“可用”状态时，备份数据源可进行恢复。	可用
备份标识	服务器数据备份的原因。 • 定时周期：根据备份策略配置的备份周期执行的数据备份。 • 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4 在目标备份数据源的“操作”列单击“恢复数据”。

说明

仅可对“备份状态”为“可用”的备份数据进行恢复。

步骤5 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。

图 5-38 恢复服务器

步骤6 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

5.3.8 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 勒索病毒防护 > 防护服务器 ”。

步骤4 单击目标服务器“操作”列的“更多 > 关闭防护”。

步骤5 确认关闭信息无误，单击“确认”，完成关闭。

----结束

后续操作

关闭勒索病毒防护后，备份存储库仍在持续备份，如果当前主机不再需要备份您可以解绑资源，如果您不再需要存储库您可以。

5.4 应用进程控制

5.4.1 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。

使用约束

使用应用进程控制功能须满足以下条件：

- 服务器已开启HSS旗舰版、网页防篡改版或容器版防护，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 服务器已安装Agent的版本为以下版本，升级Agent的操作，请参见**Agent升级**。
  - 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 5-39 使用流程图

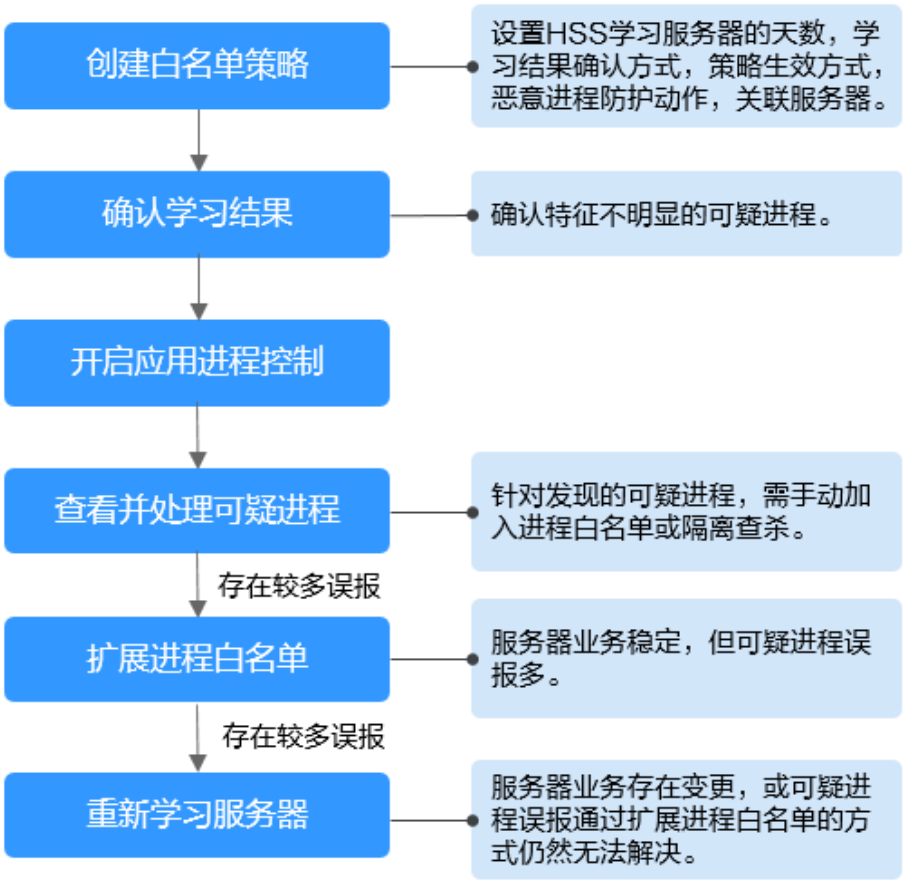


表 5-21 应用进程控制使用流程说明

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，因此这些不确定具体分类的可疑进程需要再次进行确认。
开启应用进程控制	开启策略关联服务器的应用进程控制。
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”或“隔离查杀”。
（可选）扩展进程白名单	如果HSS完成服务器学习后，发现的可疑进程事件中存在较多信任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扫描到的进程指纹，进一步扩展HSS应用进程情报库，补充可信进程白名单。
（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。

5.4.2 创建白名单策略

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特征的学习天数、学习结果确认方式和对可疑或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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签，单击“创建策略”。

步骤5 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。

图 5-40 创建白名单策略

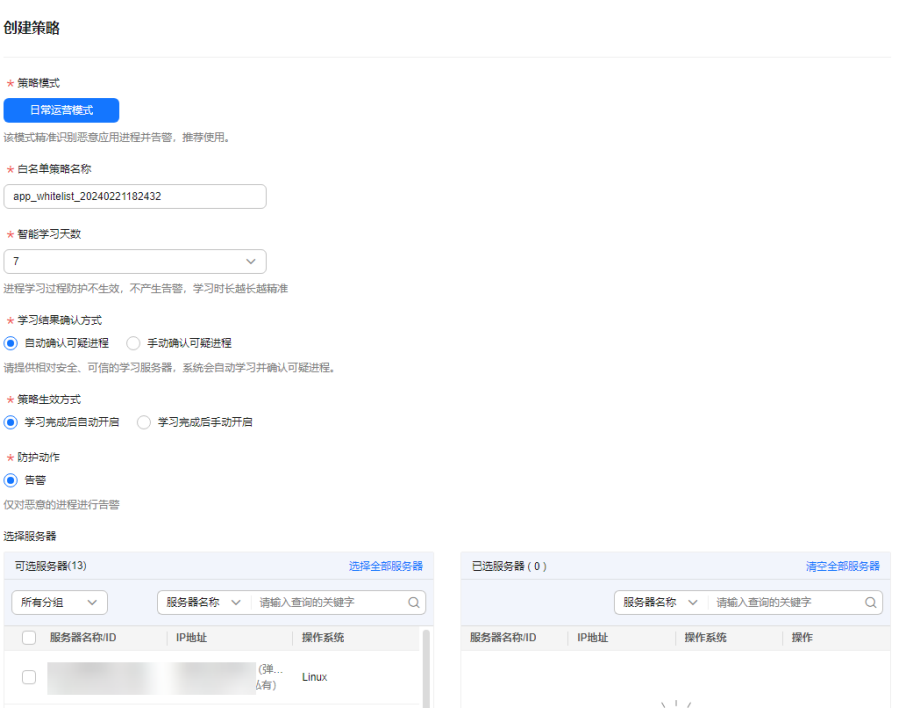


表 5-22 创建白名单策略参数说明

参数名称	参数说明
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。
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。
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：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。
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**。

参数名称	参数说明
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。
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6 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。

说明

创建白名单策略完成后，HSS会自动开始对策略关联的服务器进行学习，学习服务器中的应用进程特征。待策略状态变更为“学习完成，未生效”表示学习完成，可**确认学习结果**。

----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

5.4.3 确认学习结果

HSS学习完白名单策略关联的服务器后，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将这些可疑进程确认并分类标记为可疑、恶意或可信进程。

学习结果确认方式，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”：系统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“手动确认可以进程”：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**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

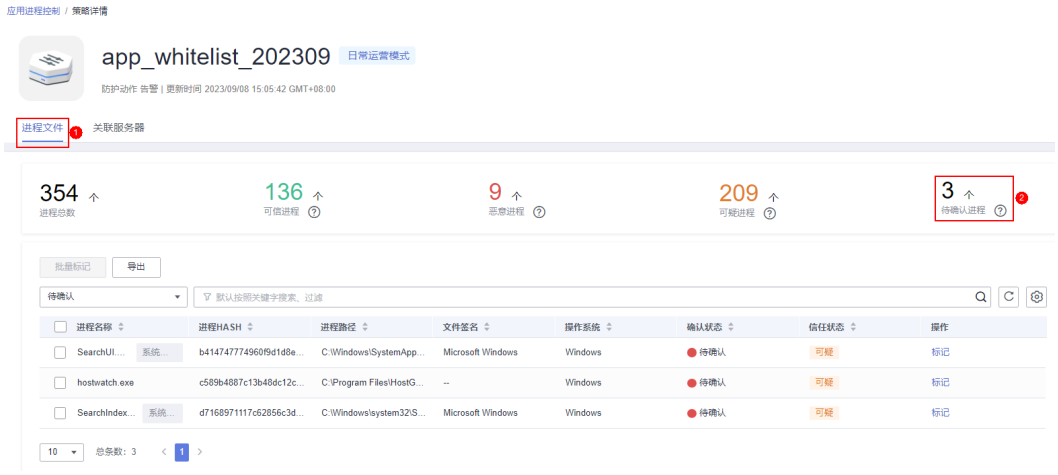
步骤4 选择“白名单策略”页签。

步骤5 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6 选择“进程文件”页签。

步骤7 单击待确认进程数量，查看待确认进程。

图 5-41 查看待确认进程



步骤8 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9 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10 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11 单击“确认”，完成标记。

----结束

5.4.4 开启应用进程控制防护

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**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签。

步骤5 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6 在开启防护弹窗中，单击“确认”。

步骤7 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

5.4.5 查看并处理可疑进程

在服务器防护过程中，如果HSS发现服务器中存在可疑进程运行事件，会将其展示在可疑进程运行事件列表中，但不会告警；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，因此需要您根据实际情况判断并将可疑进程手动加入进程白名单或隔离查杀，避免可信进程运行被持续告警或恶意进程持续运行危害服务器。

操作步骤

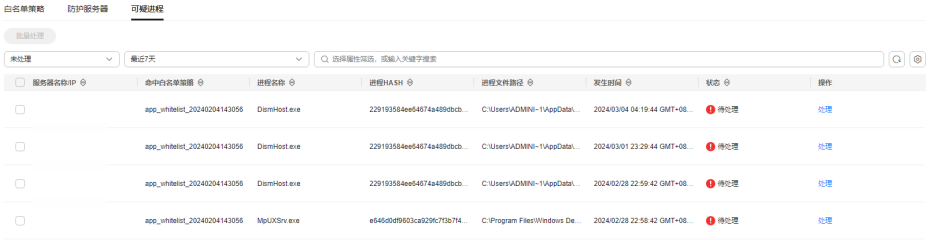
步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“可疑进程”页签，查看存在的可疑进程。

图 5-42 查看可疑进程



步骤5 根据可疑进程HASH和文件路径等信息，判断可疑进程是否为恶意进程。

步骤6 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7 在处理弹窗中，选择“处理方式”。

可选择“加入进程白名单”或“隔离查杀”。

步骤8 单击“确认”，完成处理。

----结束

5.4.6 扩展进程白名单

对于策略关联的服务器，如果您认为HSS学习到的应用进程比HSS扫描到的进程指纹少且可疑进程告警事件较多，您可以配置HSS扩展进程白名单，通过比对HSS已学习的应用进程和资产指纹功能扫描到的对应服务器的资产指纹，进一步扩展HSS应用进程情报库，补充可信进程白名单。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签。

步骤5 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤6 选择“关联服务器”页签。

步骤7 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8 单击“开始匹配”，比对服务器进程指纹和HSS学习到的应用进程。

步骤9 将比对出的可信进程选中，并单击“确认”，完成进程白名单扩展。

----结束

5.4.7 重新学习服务器

如果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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签。

步骤5 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤6 选择“关联服务器”页签。

步骤7 勾选需要目标服务器，并单击列表左上方的“重新学习”。

步骤8 在弹窗中单击“确认”，开始重新学习。

----结束

5.4.8 关闭应用进程控制防护

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签。

步骤5 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6 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 应用进程控制”，进入“应用进程控制”界面。

步骤4 选择“白名单策略”页签。

步骤5 单击目标服务器关联的策略名称，进入“策略详情”界面。

步骤6 选择“关联服务器”页签。

步骤7 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8 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

5.5 文件完整性管理

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

5.5.1 查看云服务器文件变更详情

约束限制

仅旗舰版、网页防篡改版、容器版支持文件完整性相关操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

可选择目标企业项目进行筛选。

步骤4 选择“云服务器”和“变更文件”页签可查看对应的变更详情。

步骤5 单击服务器名称进入服务器变更详情页，可查看服务器的文件变更记录。

表 5-23 变更参数说明

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

----结束

5.5.2 查看历史变更文件

约束限制

仅旗舰版、网页防篡改版、容器版支持文件完整性相关操作。

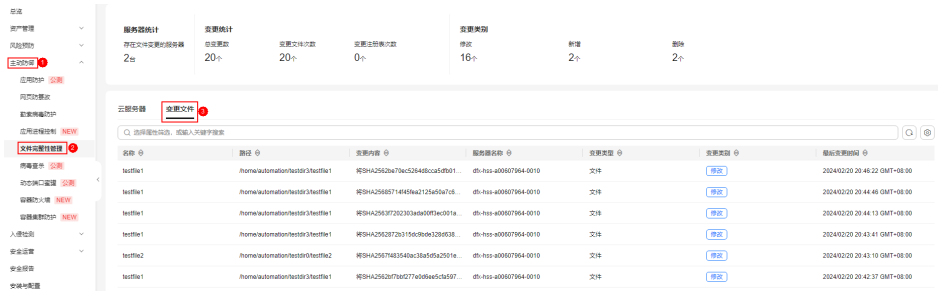
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 左侧选择“主动防御 > 文件完整性管理 > 变更文件”，进入变更文件页面，查看所有文件变更记录，企业项目可默认，参数可参见查看云服务器文件变更详情章节中的表5-23。

图 5-43 查看变更文件



----结束

5.6 病毒查杀

5.6.1 病毒查杀概述

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。

使用约束

使用病毒查杀功能须满足以下条件：

- 服务器已开启HSS专业版、企业版、旗舰版、网页防篡改版或容器版防护，购买和升级HSS的操作，请参见购买主机安全防护配额和配额版本升级。
  - 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。
- 服务器已安装Agent的版本为以下版本，升级Agent的操作，请参见Agent升级。
  - Linux：3.2.9及以上版本。
  - Windows：4.0.20及以上版本。
- 服务器已开启AV检测策略，详细操作请参见策略管理概述。

病毒查杀使用流程

1. 扫描病毒

2. 查看并处理病毒

5.6.2 扫描病毒

静态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，因此提前查杀静态病毒文件是防护服务器安全的关键之一。HSS的病毒查杀功能，支持扫描服务器上的病毒文件，并提供以下三种病毒扫描方式供您扫描病毒：

- 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。
- 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。
- 自定义查杀：您可以根据自身需求自定义病毒扫描任务。

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。资源占用情况请参见Agent检测时资源占用情况。

快速查杀

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 单击“快速查杀”，弹出“快速查杀”对话框。

步骤5 根据界面提示，填写“快速查杀”任务相关参数。

- 任务名称：您可自定义一个任务名称。
- 选择服务器：选择需要进行快速查杀的服务器。

  说明

  服务器处于查杀状态中时，不能被选择。
- 处置策略：选择针对检测到的病毒文件的处理方式。
  - 自动处置：经过云病毒检测中心进一步确认为病毒的病毒文件系统自动进行隔离；未被确认为病毒的可疑文件会被打上“可疑”标签，需人工确认后进行处置。
  - 人工处置：仅对检测到的病毒文件展示告警不自动隔离，需人工确认后进行处置。

步骤6 单击“开始扫描”，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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 单击“全盘查杀”，弹出“全盘查杀”对话框。

步骤5 根据界面提示，填写“全盘查杀”任务相关参数。

- 任务名称：您可自定义一个任务名称。
- 选择服务器：选择需要进行全盘查杀的服务器。

  说明

  - 服务器处于查杀状态时，不能被选择。
  - 全盘扫描，不扫描网络目录。
- 处置策略：选择针对检测到的病毒文件的处理方式。
  - 自动处置：经过云病毒检测中心进一步确认为病毒的病毒文件系统自动进行隔离；未被确认为病毒的可疑文件会被打上“可疑”标签，需人工确认后进行处置。
  - 人工处置：仅对检测到的病毒文件展示告警不自动隔离，需人工确认后进行处置。

步骤6 单击“开始扫描”，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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 单击“自定义查杀”，弹出“自定义查杀”对话框。

步骤5 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 5-24 自定义查杀策略参数说明

参数名称	参数说明
任务名称	自定义查杀任务名称。
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。 ● 音频文件：音频文件，常见的mp3、mp4、flv等

参数名称	参数说明
扫描目录	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。
排除目录	无需扫描病毒文件的目录。
选择服务器	选择需要扫描的服务器。处于查杀状态的服务器不支持选择。
处置策略	选择针对检测到的病毒文件的处理方式。 • 自动处置：经过云病毒检测中心进一步确认为病毒的病毒文件系统自动进行隔离；未被确认为病毒的可疑文件会被打上“可疑”标签，需人工确认后进行处置。 • 人工处置：仅对检测到的病毒文件展示告警不自动隔离，需人工确认后进行处置。

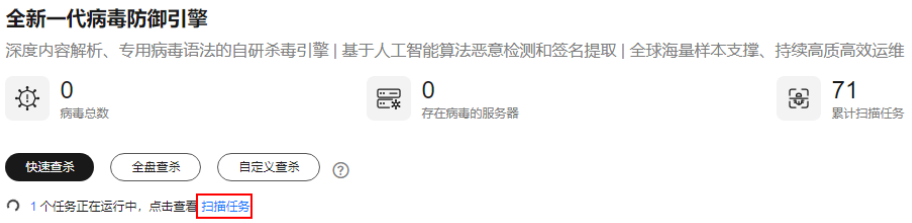
步骤6 单击“开始扫描”，启动查杀任务。

----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”。

     图 5-44 查看扫描任务

  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**。

5.6.3 查看并处理病毒

病毒扫描任务执行完成后，系统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：经过云病毒检测中心进一步确认为病毒的病毒文件系统自动进行隔离；未被确认为病毒的可疑文件会被打上“可疑”标签，需人工确认后进行处置。
- 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。

本章节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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 查看扫描到的病毒文件。

步骤5 在目标病毒文件所在行的操作列，单击“处置”。

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6 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 5-25 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，如果再次出现该病毒文件告警事件，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，该病毒文件不能执行“读/写”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7 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”；针对病毒文件告警事件的处置记录，您可以前往历史处置记录页面查看，详细操作请参考**历史处置记录**。

----结束

导出病毒文件告警事件

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 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5 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。

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

5.6.4 管理文件隔离箱

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

如果您需要将已隔离文件解除隔离，您可以执行恢复操作。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 单击界面右上角“文件隔离箱”，弹出“文件隔离箱”弹窗。

步骤5 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6 单击“确认”，恢复的文件将重新回到病毒事件列表中。

说明

执行恢复操作会将恢复隔离文件，请谨慎操作。

----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 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 病毒查杀”，进入“病毒查杀”界面。

步骤4 单击界面右上角“文件隔离箱”，弹出“文件隔离箱”弹窗。

步骤5 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6 单击“确认”，完成删除。

说明

执行删除操作会将隔离文件彻底删除，请谨慎操作。

----结束

5.7 动态端口蜜罐

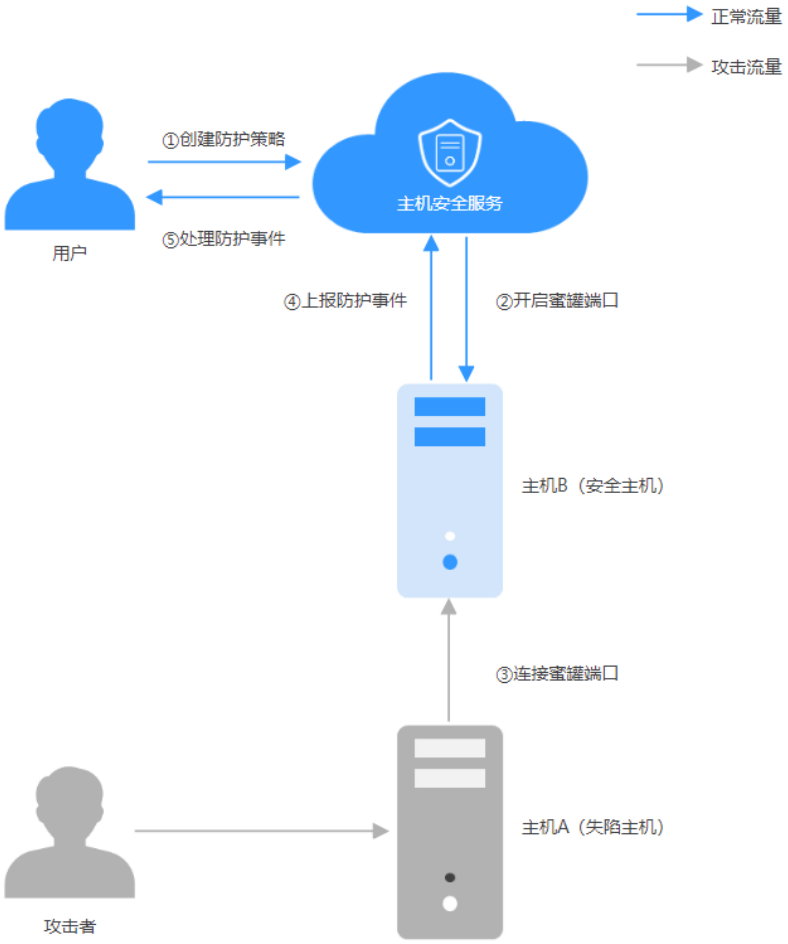
5.7.1 动态端口蜜罐概述

什么是动态端口蜜罐?

动态端口蜜罐功能是一个攻击诱捕陷阱，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。

图 5-45 动态端口蜜罐防护原理图



如何使用动态端口蜜罐?

动态端口蜜罐使用流程如**图 动态端口蜜罐使用流程**所示

图 5-46 动态端口蜜罐使用流程

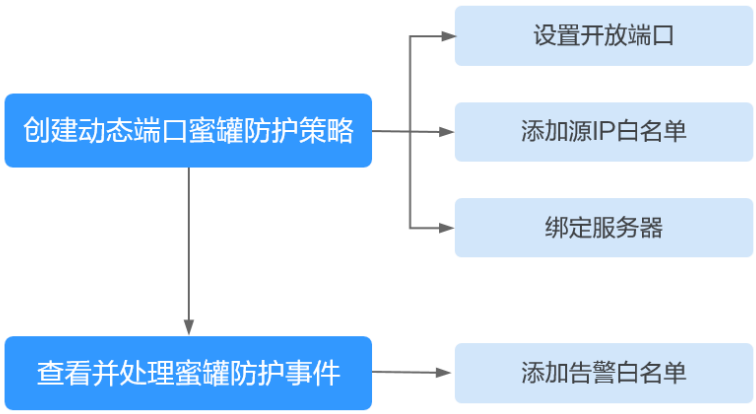


表 5-26 动态端口蜜罐使用流程说明

操作项	说明
创建动态端口蜜罐防护策略	设置需要开启动态端口蜜罐功能的服务器端口，添加源IP白名单以及绑定防护服务器等。
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

- 服务器已开启HSS旗舰版、网页防篡改版或容器版防护，购买和升级HSS的操作，请参见购买主机安全防护配额和配额版本升级。
- 服务器已安装Agent的版本为以下版本，升级Agent的操作，请参见Agent升级。
  - Linux：3.2.10及以上版本。
  - Windows：4.0.22及以上版本。
- 一台服务器最多支持添加10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。

5.7.2 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并绑定服务器开启防护。

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10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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 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**。

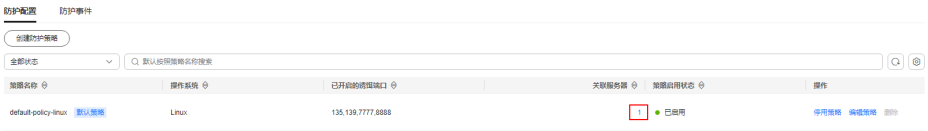
表 5-27 创建动态端口蜜罐防护策略参数说明

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	选择要添加动态端口蜜罐功能的服务器操作系统类型。
防护端口	选择实现动态端口蜜罐功能的服务器端口。 – 推荐端口：主机安全服务提供的交叉端口推荐，Linux系统推荐使用Windows常用端口，Windows系统推荐使用Linux常用端口，供您参考。 – 自定义端口：您可根据自身需求添加自定义端口或者删除一些推荐端口。 **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产生连接蜜罐端口的行为，建议您将该主机的IP加到源IP白名单。

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。

步骤7 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。

图 5-47 关联服务器



步骤8 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**。

5.7.3 查看并处理蜜罐防护事件

操作场景

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，一旦发现可疑的连接行为将会上报告警。

本章节介绍如何查看并处理这些防护告警事件。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

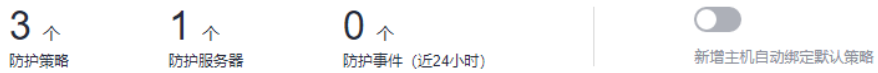
步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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。

图 5-48 防护信息概览



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 5-28 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。
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可能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	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。

参数名称	参数说明
状态	告警处理状态，分为“已处理”和“待处理”。
操作	您可以对告警事件进行“处置”操作。

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“处置”，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 5-29 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，可作补充描述。

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 5-30 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。

参数名称	参数说明
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。
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。

筛选不同处置状态的防护事件

在防护事件列表左上方的状态下拉框中，选择目标处置状态的防护事件进行查看。

图 5-49 筛选防护事件

5.7.4 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**：将停用的动态端口蜜罐动能启用。
- **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 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 配置策略。

可修改策略名称、防护端口、源IP白名单。

步骤7 单击“下一步”。

步骤8 选择绑定服务器。

步骤9 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 确认信息无误后，单击“确认”，完成删除。

----结束

5.7.5 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 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7 根据界面提示，选择防护策略。

步骤8 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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“主动防御 > 动态端口蜜罐”，进入“动态端口蜜罐”界面。

步骤4 （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5 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6 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7 确认信息无误后，单击“确认”，解除绑定。

----结束

5.8 容器防火墙

5.8.1 容器防火墙概述

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

约束与限制

- 仅HSS容器版支持该功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 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。权限配置详细操作请参见**配置命名空间权限**。

容器防火墙原理

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

防护集群类型

用户在云容器引擎（Cloud Container Engine，简称CCE）服务中购买的集群，简称CCE集群。

相关操作

- **创建网络策略（容器隧道网络模型集群）**
- **创建安全组规则（VPC网络模型集群）**
- **创建安全组策略（云原生网络2.0模型集群）**

5.8.2 创建网络策略（容器隧道网络模型集群）

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

本章节介绍如何为容器隧道网络模型的集群创建网络策略。

约束与限制

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

通过 YAML 创建网络策略

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 在集群列表上方，单击“手动同步”，同步所有集群在CCE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6 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7 单击策略列表上方“YAML创建”。

步骤8 在YAML创建界面输入或单击“导入”数据。

以下为一个YAML创建的网络策略示例：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:                    #规则对具有role=db标签的Pod生效
    matchLabels:
      role: db
  policyTypes:
    - Ingress
    - Egress
  ingress:                        #表示入规则
    - from:
        - namespaceSelector:      #只允许具有project=myproject的命名空间访问
            matchLabels:
              project: myproject
        - podSelector:            #只允许具有role=frontend标签的Pod访问
            matchLabels:
              role: frontend
      ports                       #只允许使用TCP协议访问6379端口
```

```
    - protocol: TCP
      port: 6379
egress:                    #表示出规则
  - to:
    - ipBlock:              #只允许访问目的对象的10.0.0.0/24网段。
        cidr: 10.0.0.0/24
    ports:                  #只允许使用TCP协议访问目的对象的6379端口
    - protocol: TCP
      port: 6379
```

步骤9 输入完成后，单击“确认”。

----结束

通过可视化界面创建网络策略

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 在集群列表上方，单击“手动同步”，同步所有集群在CCE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6 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7 单击网络策略列表上方“创建网络策略”。

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

表 5-31 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 5-32 添加出方向规则

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

步骤8 设置完成后，单击“确定”。

----结束

5.8.3 创建安全组规则（VPC 网络模型集群）

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

本章节介绍如何为VPC网络模型的集群创建安全组规则。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 在集群列表上方，单击“手动同步”，同步所有集群在CCE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6 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7 在目标节点所在行的“操作”列，单击“配置策略”。

步骤8 在弹出的对话框中单击“确认”，跳转到ECS服务器详情页面。

步骤9 选择“安全组”页签，查看安全组规则。

步骤10 单击“配置规则”，系统自动跳转到安全组页面。

步骤11 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**添加安全组规则**。

----结束

5.8.4 创建安全组策略（云原生网络 2.0 模型集群）

云原生网络2.0模型的集群支持通过配置安全组策略的方式限制访问容器宿主服务器的流量；当未配置安全组策略时，默认所有进出容器宿主服务器的流量都被允许。

本章节介绍如何为云原生网络2.0模型的集群创建安全组策略。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 在集群列表上方，单击“手动同步”，同步所有集群在CCE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6 在目标云原生网络2.0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7 单击策略列表上方“创建”，弹出“创建安全组策略”对话框。

步骤8 根据界面提示，填写策略信息。相关参数说明请参见**表 创建安全组策略参数说明**。

表 5-33 创建安全组策略参数说明

参数名称	参数说明
策略名称	自定义输入一个策略名称。
命名空间	选择命名空间。

参数名称	参数说明
负载类型	选择负载类型。支持以下三种类型： • 无状态负载 • 有状态负载 • 守护进程集
工作负载	选择目标工作负载。
关联安全组	选择需要关联的安全组。一个策略最多只能关联五个安全组。 列表中的已有的安全组为您在VPC服务中创建的安全组；如果您需要创建新的安全组，您可以单击“创建安全组”，跳转至VPC控制台进行创建，创建详细操作请参见**创建安全组**。

步骤9 策略信息填写完成后，单击“确认”，完成创建。

----结束

5.8.5 管理网络策略（容器隧道网络模型集群）

容器隧道网络模型的集群网络策略创建完成后，您可以参考本章节修改策略或删除不需要的策略。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 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6 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7 定位目标网络策略，选择执行管理操作。

- 修改网络策略
  - 在目标策略所在行的“操作”列，单击“编辑YAML”，进入YAML界面，修改YAML信息后，单击“确认”。
  - 在目标策略所在行的“操作”列，单击“更新”，进入更新网络策略界面，修改网络策略信息后，单击“确认”。
- 删除网络策略

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

----结束

5.8.6 管理安全组规则（VPC 网络模型集群）

VPC网络模型的集群安全组规则创建完成后，您可以参考本章节修改规则或删除不需要的规则。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 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6 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7 在目标节点所在行的“操作”列，单击“配置策略”。

步骤8 在弹出的对话框中单击“确认”，跳转到ECS服务器详情页面。

步骤9 选择“安全组”页签，查看安全组规则。

步骤10 单击“配置规则”，系统自动跳转到安全组页面。

步骤11 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

5.8.7 管理安全组策略（云原生网络 2.0 模型集群）

云原生网络2.0的集群安全组策略创建完成后，您可以参考本章节修改策略或删除不需要的策略。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏选择“主动防御 > 容器防火墙”，进入“容器防火墙”页面。

步骤4 （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5 在目标云原生网络2.0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6 单击策略列表上方“手动同步”，同步集群策略信息。

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7 选择需要对策略实施的操作。

- 查看策略内容

  在目标策略所在行的“操作”列，单击“查看YAML”，弹出“查看YAML”弹窗，您可以选择YAML或JSON视图查看策略详细内容。如需下载到本地查看，可单击弹窗左上角“下载”。

- 更新策略内容

  a. 在目标策略所在行的“操作”列，单击“更新”，弹出“更新安全组策略”对话框。

  b. 添加或删除关联安全组。

  c. 单击“确认”，完成更新。

- 删除策略

  a. 在目标策略所在行的“操作”列，单击“删除”，弹出“删除策略”对话框。

  b. 确认信息无误，单击“确认”，完成删除。

----结束

5.9 容器集群防护

5.9.1 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。

使用约束

使用容器集群防护功能须满足以下条件：

- 容器集群为云容器引擎（Cloud Container Engine，简称CCE）服务中购买的集群，且集群版本为1.20及以上版本。
- 容器节点服务器已开启HSS容器版防护，购买HSS的操作，请参见**购买主机安全防护配额**。
- 服务器已安装Agent的版本为以下版本，升级Agent的操作，请参见**Agent升级**。
  - Linux：3.2.7及以上版本。
  - Windows：4.0.19及以上版本。
- 操作集群内的资源对象需要获取对应的操作权限，因此使用容器集群防护功能时，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。权限配置详细操作请参见**配置命名空间权限**。

容器集群防护使用流程

图 5-50 使用流程图

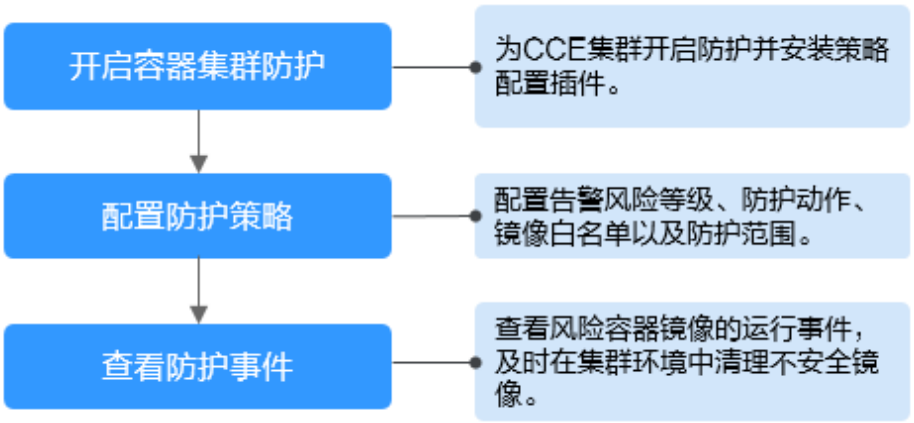


表 5-34 容器集群防护使用流程说明

操作项	描述
开启容器集群防护	为CCE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。
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。

5.9.2 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**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 容器集群防护”，进入“容器集群防护”界面。

步骤4 选择“防护集群”页签。

步骤5 单击“手动同步”，同步CCE集群。

步骤6 在目标集群所在行的操作列，单击“开启防护”。

您也可以勾选所有目标集群，并在集群列表左上方单击“开启防护”，批量为集群开启防护。

须知

- 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7 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

5.9.3 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。

新建防护策略

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 容器集群防护”，进入“容器集群防护”界面。

步骤4 选择“防护策略”页签，单击“新建策略”。

步骤5 在新建策略弹窗中，配置策略参数。

1. 确定防护策略，相关参数说明请参见**表 配置容器集群防护策略参数说明**。

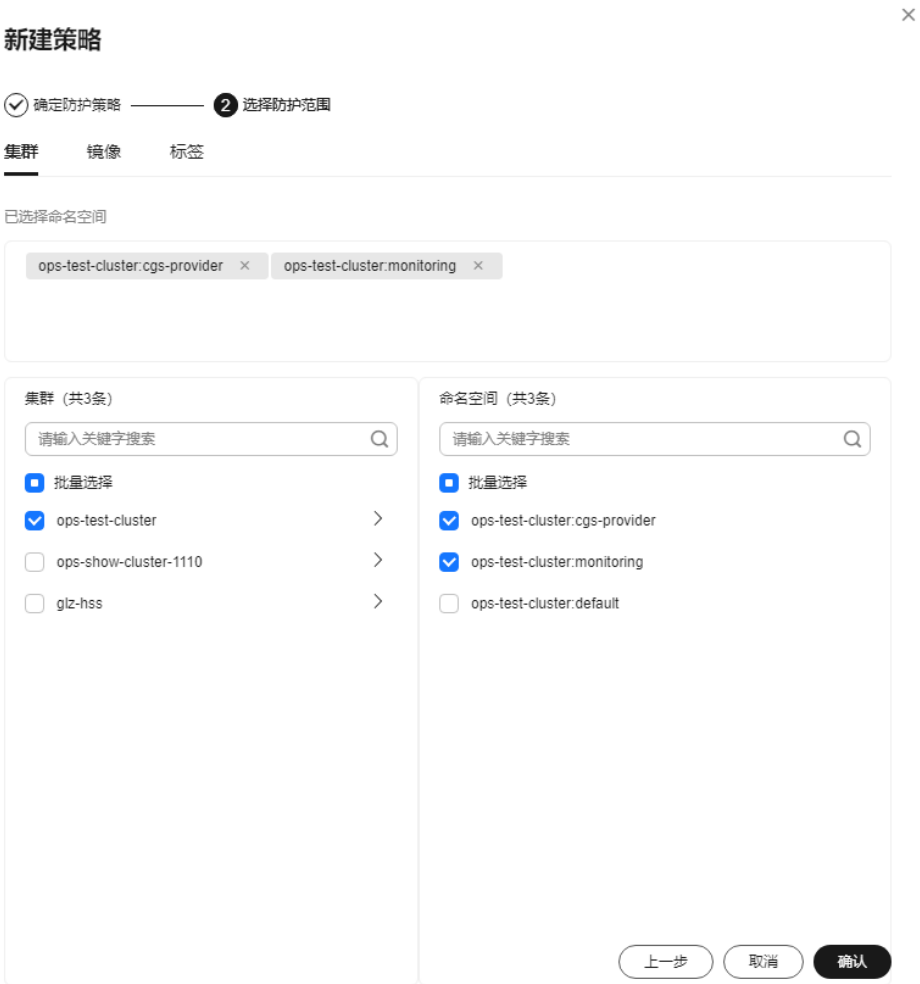
表 5-35 配置容器集群防护策略参数说明

参数名称	参数说明
策略模板	选择策略默认模板。
策略名称	策略名称，需自定义。
策略描述	自定义策略用途等，作策略区分。
拦截未扫描镜像	是否拦截未使用HSS的容器镜像安全扫描功能扫描过的镜像。 -  ：关闭 -  ：开启
告警策略	选择告警策略类型。 - 基线 - 漏洞 - 恶意脚本
风险等级	选择触发告警的风险等级。 - 高危 - 中危 - 低危
基线项目	选择高危基线风险项，如果启动的镜像中包含这些高危基线风险项，HSS会立即执行防护动作。
漏洞项目	选择高危漏洞，如果启动的镜像中包含这些高危漏洞，HSS会立即执行防护动作。
恶意样本	选择高危恶意样本，如果启动的镜像中包含这些高危恶意样本，HSS会立即执行防护动作。
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。

参数名称	参数说明
加白名单	填写需要加入白名单的镜像名称。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 **须知** 加入白名单的镜像启动时，HSS将不会进行安全检测，请谨慎操作！

2. 单击“下一步”。
3. 选择防护范围。
   选择集群、镜像和标签的防护范围。

图 5-51 选择防护范围



步骤6 单击“确认”，完成策略创建。

您可以在防护策略列表中查看新建的防护策略。

----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。

- 编辑：修改防护策略信息。
- 删除：删除不需要的防护策略。

须知

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

5.9.4 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 容器集群防护”，进入“容器集群防护”界面。

步骤4 选择“防护事件”页签，查看集群中发现的风险事件。

步骤5 单击告警名称，查看告警事件影响的资源详细信息。

----结束

5.9.5 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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航栏，选择“主动防御 > 容器集群防护”，进入“容器集群防护”界面。

步骤4 选择“防护集群”页签。

步骤5 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6 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7 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？**。

6 入侵检测

6.1 安全告警事件

6.1.1 主机安全告警

6.1.1.1 主机安全告警事件概述

主机安全服务支持账户暴力破解、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	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
恶意软件	未分类恶意软件	恶意程序可能是黑客入侵成功之后植入的木马、后门等，用于窃取数据或攫取不当利益。 例如：黑客入侵之后植入木马，将受害主机作为挖矿、DDoS肉鸡使用，这类程序会大量占用主机的CPU资源或者网络资源，破坏用户业务的稳定性。 通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。	×	√	√	√	√	Linux、Windows	√	√	√
	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。	×	√	√	√	√	Linux、Windows	√	√	√
	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。	×	√	√	√	√	Linux、Windows	√	√	√
	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。	×	√	√	√	√	Linux、Windows	√	√	√

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	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。	×	√	√	√	√	Linux、Windows	√	√	√
	后门	检测服务器中存在的后门，并进行告警上报。	×	√	√	√	√	Linux、Windows	√	√	×
	Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。	×	√	√	√	√	Linux	√	×	×
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。	×	×	×	√	√	Linux、Windows	√	√（部分支持）	√（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。	×	×	√	√	√	Linux、Windows	√	√	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	Webshell	检测云服务器上web目录中的文件，判断是否为Webshell木马文件，支持检测常见的PHP、JSP等后门文件类型。 您可以在“策略管理”的“Webshell检测”中配置Webshell检测，HSS会实时检测执行的可疑指令、主机被远程控制执行任意命令等。 该告警需要您在策略管理中添加防护目录，添加详情请参见**Webshell检测**。	×	√	√	√	√	Linux、Windows	√	√	×
	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。	×	√	√	√	√	Linux、Windows	√	√	√
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。	×	×	√	√	√	Linux、Windows	√	×	×
	Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	√	Linux	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	√	Linux	√	×	×
	MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。	×	√	√	√	√	Linux	√	×	×
系统异常行为	反弹Shell	实时监控用户的进程行为，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。	×	√	√	√	√	Linux	√	×	×
	文件提权	检测当前系统对文件的提权行为并进行告警。	×	√	√	√	√	Linux	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	进程提权	检测以下进程提权操作并进行告警： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。	×	√	√	√	√	Linux	√	×	×
	关键文件变更	实时监控系统关键文件（例如：ls、ps、login、top等），对修改文件内容的操作进行告警，提醒用户关键文件可能被篡改。监控的关键文件的路径请参见**关键文件变更监控路径**。 对于关键文件变更，HSS只检测文件内容是否被修改，不关注是人为还是进程进行的修改。	×	√	√	√	√	Linux	√	×	×
	文件/目录变更	实时监控系统文件/目录，对创建、删除、移动、修改属性或修改内容的操作进行告警，提醒用户文件/目录可能被篡改。	×	√	√	√	√	Linux、Windows	√	×	×
	进程异常行为	检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。	×	×	√	√	√	Linux、Windows	√	√（部分支持）	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	高危命令执行	您可以在“策略管理 > 实时进程”的“高危命令检测”中预置高危命令。 HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	×	√	√	√	√	Linux、Windows	√	×	×
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、复制、硬链接、访问权限变化。 您可以在“策略管理”的“恶意文件检测”中配置异常Shell检测，HSS会实时检测执行的可疑指令、主机被远程控制执行任意命令等。	×	√	√	√	√	Linux	√	×	×
	Crontab可疑任务	检测并列出当前所有主机系统中自启动服务、定时任务、预加载动态库、Run注册表键或者开机启动文件夹的汇总信息。 帮助用户通过自启动变更情况，及时发现异常自启动项，快速定位木马程序的问题。	×	×	×	√	√	Linux、Windows	√	×	×
	系统安全防护被禁用	检测勒索软件加密前准备动作：通过注册表关闭 Windows Defender 实时保护功能，一旦发现立即上报告警。	×	×	√	√	√	Windows	√	×	×
	备份删除	检测勒索软件加密前准备动作：删除备份格式文件或Backup文件夹下的文件，一旦发现立即上报告警。	×	×	√	√	√	Windows	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	异常注册表操作	检测通过注册表关闭系统防火墙、勒索病毒Stop修改注册表并写入特定字符串等操作，一旦发现立即上报告警。	×	×	√	√	√	Windows	√	×	×
	系统日志删除	检测到通过命令或工具清除系统日志的操作时进行告警。	×	×	√	√	√	Windows	√	×	×
	可疑命令执行	• 检测通过命令或工具创建、删除计划任务或自启动任务。 • 检测远程执行命令的可疑行为。	×	×	√	√	√	Windows	√	×	×
	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。	×	×	√	√	√	Linux、Windows	√	×	×
	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。	×	×	√	√	√	Linux、Windows	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
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。	√	√	√	√	√	Linux、Windows	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	异常登录	检测“异地登录”和“账户暴力破解成功”等异常登录。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。	√	√	√	√	√	Linux、Windows	√	×	×
	非法系统账号	黑客可能通过风险账号入侵主机，以达到控制主机的目的，需要您及时排查系统中的账户。 HSS检查系统中存在的可疑隐藏账号、克隆账号；如果存在可疑账号、克隆账号等，则触发告警。	×	√	√	√	√	Linux、Windows	√	×	×
	用户账号添加	检测使用命令创建隐藏账户，一旦创建成功后用户交互界面和命令查询均不可见。	×	×	√	√	√	Windows	√	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	用户密码窃取	检测主机中的系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。	×	×	√	√	√	Windows	√	×	×
网络异常访问	可疑的下载请求	检测到利用系统工具下载程序的可疑HTTP请求时进行告警。	×	×	√	√	√	Windows	√	×	×
	可疑的HTTP请求	检测到利用系统工具或进程执行远程托管脚本的可疑HTTP请求时进行告警。	×	×	√	√	√	Windows	√	×	×
	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。	×	√	√	√	√	Linux	√	×	×
	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。	×	√	√	√	√	Linux	√	×	×
资源侦查	端口扫描	检测用户指定的端口存在被扫描或者嗅探的行为，一旦发现进行告警上报。	×	×	×	√	√	Linux	×	×	×

事件类型	告警名称	告警说明	基础版	专业版	企业版	旗舰版	网页防篡改版	支持的操作系统	加入告警白名单	手动隔离查杀	自动隔离查杀
	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。	×	×	×	√	√	Linux	√	×	×

关键文件变更监控路径

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

6.1.1.2 查看主机告警事件

主机安全服务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，详细信息请参见**查看和创建策略组**。
- 其他检测项不允许手动关闭检测。
- 未开启防护的服务器不支持告警事件相关操作。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

表 6-1 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。

参数名称	告警事件状态说明
已处理告警事件	展示您资产中所有已处理的告警事件数量。
已拦截IP	展示已拦截的IP。单击“已拦截IP”，可查看已拦截的IP地址列表。 已拦截IP列表展示“服务器名称”、“攻击源IP”、“登录类型”、“拦截状态”、“拦截次数”、“开始拦截时间”、“最近拦截时间”。 如果您发现有合法IP被误封禁（比如运维人员因为记错密码，多次输错密码导致被封禁），可以手工解除拦截。如果发现某个主机被频繁攻击，需要引起重视，建议及时修补漏洞，处理风险项。 **须知** • 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**。

步骤4 查看资产中存在的告警。

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。

告警名称处也会展示ATT&CK攻击阶段标签，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 6-2 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	攻击者尝试保持住他们入侵的进攻点。

ATT&CK攻击阶段	说明
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。
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。

步骤5 单击事件类型的告警名称，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

对于部分恶意软件，HSS支持告警源文件下载，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”。

图 6-1 告警详细信息

表 6-3 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**。

参数名称	参数说明
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。
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。

----结束

6.1.1.3 处理主机告警事件

主机安全服务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，详细信息请参见**查看和创建策略组**。
- 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 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

表 6-4 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。

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

步骤4 单击告警名称，查看告警信息和处理建议。

步骤5 处理告警事件。

说明

告警事件展示在“主机安全告警”页面中，事件列表仅展示最近30天的告警事件。

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

- 处理单个告警事件

  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”。

图 6-2 全量处理告警事件

步骤6 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 6-5 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，请及时确认如果测结果，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。

处理方式	处理方式说明
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。加入告警如果名单后，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7 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“处置”。

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

6.1.1.4 导出主机告警事件

本章节为您介绍如何将主机安全告警事件导出到本地进行查看。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 选择“主机安全告警”页签。

步骤5 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

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6 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

6.1.1.5 管理文件隔离箱

主机安全服务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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

表 6-6 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。

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

步骤4 单击支持隔离查杀的告警事件“操作”列的“处理”，选择“隔离查杀”。

说明

对应告警事件支持隔离查杀的情况详情请参见**主机安全告警事件概述**。

步骤5 单击“确认”，对目标告警事件进行隔离查杀。

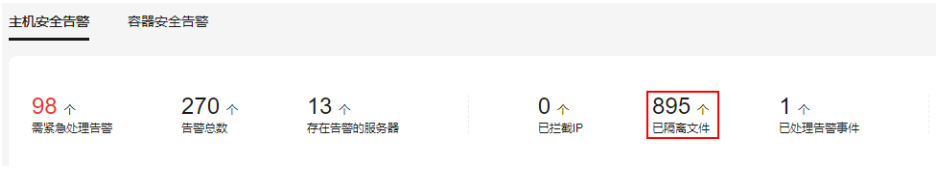
被成功隔离的文件会添加到“主机安全告警”的“文件隔离箱”中，无法对主机造成威胁。

----结束

查看文件隔离箱

步骤1 在“主机安全告警”页面的“安全告警统计”中，单击“已隔离文件”上方的数值，进入“文件隔离箱”页面。

图 6-3 安全告警统计



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。

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。

说明

执行恢复操作会将隔离文件查杀恢复，请谨慎操作。

----结束

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。

说明

执行删除操作会将隔离文件彻底删除，请谨慎操作。

----结束

6.1.2 容器安全告警

6.1.2.1 容器安全告警事件概述

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

约束限制

- 仅HSS容器版支持容器安全告警功能，购买和升级HSS的操作，请参见**购买主机安全防护配额**和**配额版本升级**。
- 容器安全告警功能支持对Linux容器以下运行时进行入侵检测告警：
  - Containerd
  - Docker

告警事件列表说明

事件类型	告警名称	原理说明
恶意软件	未分类恶意软件	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出容器中未知的恶意程序和病毒变种。
	勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。
	Webshell	检测容器中Web目录中的文件，判断是否为Webshell木马文件，支持检测常见的PHP、JSP等后门文件类型。
	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
	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。

事件类型	告警名称	原理说明
	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。CGS监控容器进程，如果发现进程使用了危险系统调用（例如：“open_by_handle_at”、“ptrace”、“setns”、“reboot”等），触发高危系统调用告警。
	高危命令执行	实时检测容器系统中执行的高危命令，当发生高危命令执行时触发告警。
	容器进程异常	● 容器恶意程序 HSS监控容器内启动的容器进程的行为特征和进程文件指纹，如果特征与已定义的恶意程序吻合则触发容器恶意程序告警。 ● 容器异常进程 容器业务通常比较单一。如果用户能够确定容器内只会运行某些特定进程，可以在“策略管理”设置“容器进程白名单”并将策略关联容器镜像。 对于已关联的容器镜像启动的容器，HSS只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。

事件类型	告警名称	原理说明
	敏感文件访问	HSS监控容器内已配置文件保护策略的容器镜像文件状态。如果发生文件修改事件则触发文件异常告警。

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

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

事件类型	告警名称	原理说明
	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，一旦发现进行警上报。

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

6.1.2.2 查看容器告警事件

主机安全服务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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

- 查看容器告警事件概览。
  - 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。

  告警名称处也会展示ATT&CK攻击阶段标签，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 6-7 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	攻击者尝试保持住他们入侵的进攻点。
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。
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

  对于部分恶意软件，HSS支持告警源文件下载，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”。

  表 6-8 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。

- 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

6.1.2.3 处理容器告警事件

主机安全服务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。

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

表 6-9 安全告警统计说明

告警事件状态	告警事件状态说明
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。
存在告警的容器	展示存在告警的容器数量。
已处理告警事件	展示您资产中所有已处理的告警事件数量。

步骤4 单击告警名称，查看告警信息和处理建议。

步骤5 处理告警事件。

说明

告警事件展示在“容器安全告警”页面中，事件列表仅展示最近30天的告警事件。

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

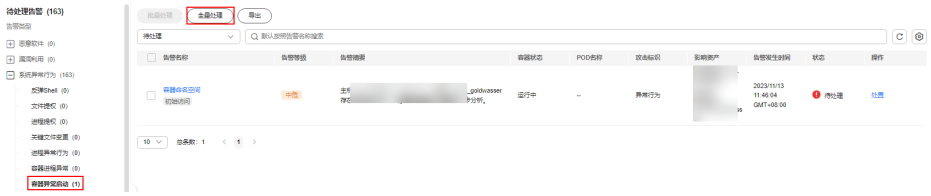
- 处理单个告警事件

  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”。

图 6-4 全量处理告警事件



步骤6 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 6-10 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。 如果登录IP已被拦截，将登录告警事件加入登录告警白名单的同时会解除对登录IP的拦截。 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。

处理方式	处理方式说明
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**容器安全告警事件概述**。

步骤7 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“处置”。

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

6.1.2.4 导出容器告警事件

本章节为您介绍如何将容器安全告警事件导出到本地进行查看。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 选择“容器安全告警”页签。

步骤5 在告警事件列表上方，单击“导出”，导出所有安全告警事件。

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6 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

6.2 白名单管理

6.2.1 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。

说明

- 配置的目标服务器IP、登录端IP以及登录端用户名需同时满足白名单配置的信息，检测时才会忽略。
- 如果将已经产生告警的目标IP通过**添加登录告警白名单**方式加入白名单，加入白名单之后的检测会对目标IP进行忽略不再告警，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**。

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。

添加登录告警白名单

步骤1 **登录管理控制台**。

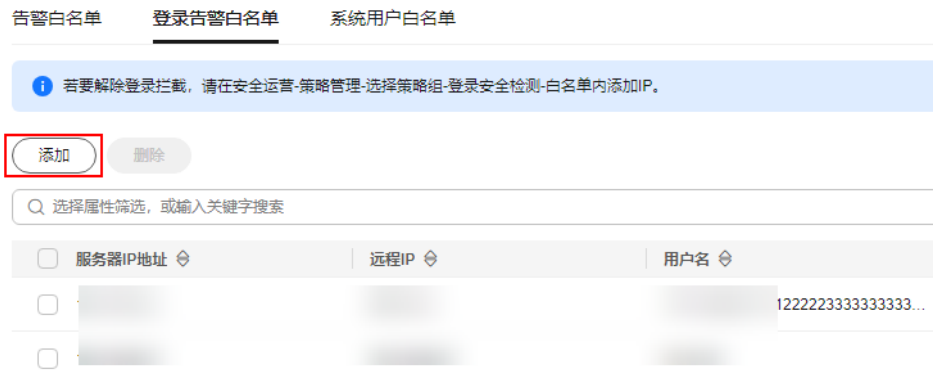
步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

图 6-5 添加登录告警白名单



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

表 6-11 登录安全白名单参数说明

参数名称	参数说明	取值样例
服务器IP 登录IP	• 支持IPv4地址。 • 支持单个IP、IP范围、IP掩码，以英文逗号分隔。	• 192.168.1.1 • 192.168.2.1-192.168.6.1 • 192.168.7.0/24
登录用户名	当前登录用户名。	hss_test
备注	可自定义目标白名单说明。	测试

步骤5 单击“确认”，完成登录告警白名单的添加。

----结束

其他操作

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。

说明

执行删除操作后无法恢复，请谨慎操作。

6.2.2 管理告警白名单

白名单管理提供告警白名单的展示与删除功能，用户可以通过配置告警白名单避免大量告警误报的发生，提升安全事件告警质量。

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

在“安全告警事件”页面处理告警事件时，如果告警为误报，您可以将告警加入告警白名单。告警加入白名单后，后续主机安全平台不会再对该事件进行告警和统计。

添加告警白名单

表 6-12 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 • Redis漏洞利用 • Hadoop漏洞利用 • MySQL漏洞利用

查看告警白名单

加入告警白名单后，您可以查看已添加的告警白名单，操作步骤如下所示。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 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6-13所示。

图 6-6 告警白名单列表

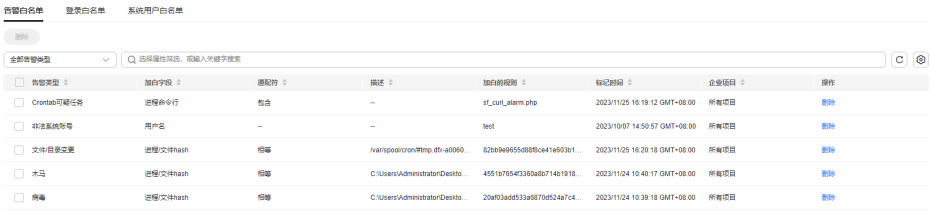


表 6-13 告警白名单列表参数说明

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。
加白的规则	加白规则ID。
描述	目标白名单的说明。
数据来源	目标白名单的来源方式。
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。

----结束

相关操作

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“入侵检测 > 安全告警事件”页面，在告警事件所在行的操作列单击“处置”，选择“删除告警白名单”。

6.2.3 管理系统用户白名单

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

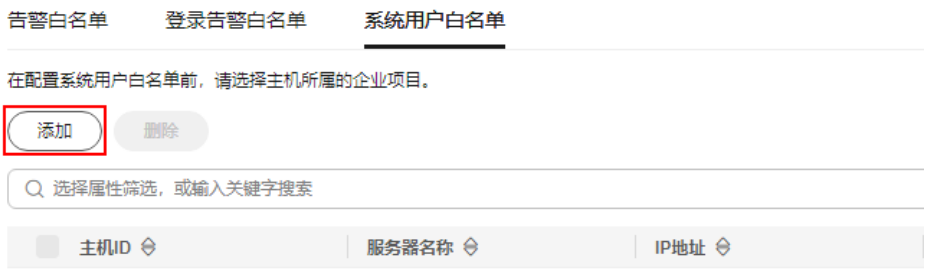
步骤3 在左侧导航栏，选择“入侵检测 > 白名单管理”，进入“白名单管理”页面。

步骤4 （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5 选择“系统用户白名单”页签，单击“添加”。

图 6-7 配置系统用户白名单



步骤6 在“添加系统用户白名单”弹窗中填写主机ID、系统用户名以及备注信息。

步骤7 单击“确认”，添加完成。

----结束

相关操作

修改系统用户白名单

步骤1 （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

7 安全运营

7.1 策略管理

7.1.1 策略管理概述

当资产采集、基线检查或入侵检测等策略不满足您的主机防护需求时，您可以管理这些策略。

HSS各版本支持管理的策略如**表 策略列表**所示，策略配置详细操作请参见**配置策略**。

如果您拥有多个旗舰版、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，详细操作请参见**创建策略组**。

表 7-1 策略列表

功能类型	策略名称	策略说明	支持的操作系统	专业版	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	×	×	√	√	√
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	√	√	√	√	√
	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	×	×	×	×	√

功能类型	策略名称	策略说明	支持的操作系统	专业版	企业版	旗舰版	网页防篡改版	容器版
	配置检测	对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项。	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“入侵检测 > 安全告警事件 > 主机安全告警 > 事件类型 > 恶意软件”下的子类别中分别呈现。 开启AV检测后资源占用情况如下： CPU资源占用不超过单vCPUs的40%，实际占用情况需根据主机情况而定，参照详情请参见**检测资源占用一览表**。	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	√	√	√	√	√
	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	×	×	×	×	√

功能类型	策略名称	策略说明	支持的操作系统	专业版	企业版	旗舰版	网页防篡改版	容器版
	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	×	×	×	×	√
	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	√	√	√	√	√
	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	专业版	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，全局检测各个主机的运行信息，保障云主机的安全性。您可以建立自己的进程白名单，对于进程的非法行为、黑客入侵过程进行告警。	Linux	√	√	√	√	√
	root提权	检测当前系统文件路径的root提权行为。	Linux	√	√	√	√	√
	实时进程	检测进程中高危命令的执行行为，发生高危命令执行时，触发告警。	Linux，Windows	√	√	√	√	√
	rootkit检测	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。	Linux	√	√	√	√	√

功能类型	策略名称	策略说明	支持的操作系统	专业版	企业版	旗舰版	网页防篡改版	容器版
自保护	自保护	保护主机安全服务的文件、进程、软件，防止恶意程序卸载主机安全服务Agent、篡改主机安全服务文件或停止主机安全服务进程。 • 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： – 主机安全服务的Agent不支持通过主机的控制面板卸载，支持通过主机安全服务控制台卸载。 – 主机安全服务的进程无法被终止。 – 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	×	×	√	√	×

7.1.2 创建策略组

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。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

表 7-2 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_advanced_default_policy_group：专业版linux系统预置策略，仅可被查看，不可复制和删除。 • tenant_windows_advanced_default_policy_group：专业版windows系统预置策略，仅可被查看，不可被复制和删除。 • 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。 • wtp_主机名称：网页防篡改版策略，每台主机开启网页防篡改防护时都会默认生成对应的网页防篡改策略组。
ID	策略组的ID号，对策略组的唯一标识。
描述	对策略组的描述。
支持的版本	策略组支持的主机安全服务的版本。
支持的操作系统	策略支持的操作系统类型。
关联服务器数	策略关联的服务器数。单击数值，可查看策略组关联的服务器。

步骤4 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5 在弹出的对话框中，输入“策略组名称”和“描述”。

说明

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

步骤6 单击“确认”，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**。

7.1.3 配置策略

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

- 已开启专业版、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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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。

表 7-3 策略组列表字段说明

字段	说明
策略组名称	策略组的名称。系统预置策略组名称如下： ● tenant_linux_advanced_default_policy_group：专业版linux系统预置策略，仅可被查看，不可复制和删除。 ● tenant_windows_advanced_default_policy_group：专业版windows系统预置策略，仅可被查看，不可被复制和删除。 ● 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。 ● wtp_主机名称：网页防篡改版策略，每台主机开启网页防篡改防护时都会默认生成对应的网页防篡改策略组。
ID	策略组的ID号，对策略组的唯一标识。
描述	对策略组的描述。
支持的版本	策略组支持的主机安全服务的版本。
支持的操作系统	策略支持的操作系统类型。
关联服务器数	策略关联的服务器数。单击数值，可查看策略组关联的服务器。

步骤4 单击目标策略组名称，进入策略详情列表。

说明

您可以根据需要在策略所在行的操作列执行“开启”或“关闭”操作。策略关闭后，将不再执行对应策略的检测。

步骤5 单击目标策略名称对不同策略进行修改。

----结束

资产发现

步骤1 单击“资产发现”，弹出“资产发现”策略详情界面。

步骤2 在弹出的资产管理界面中，修改“策略内容”，参数说明如表7-4所示。

表 7-4 资产管理策略内容参数说明

参数名称	参数说明
检测时间	针对不同资产自动执行检测的固定时间点，其中中间件、Web框架、内核模块、Web应用、Web站点、Web服务、数据库可进行自定义检测时间。 偏移时间指在设置的目标时间向前或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。

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。

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

步骤1 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7-5所示。

图 7-1 修改弱口令检测

表 7-5 弱口令检测策略内容参数说明

参数	说明
检测时间	配置弱口令检测的时间，可具体到每一天的每一分钟。
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”。

图 7-2 修改配置检测

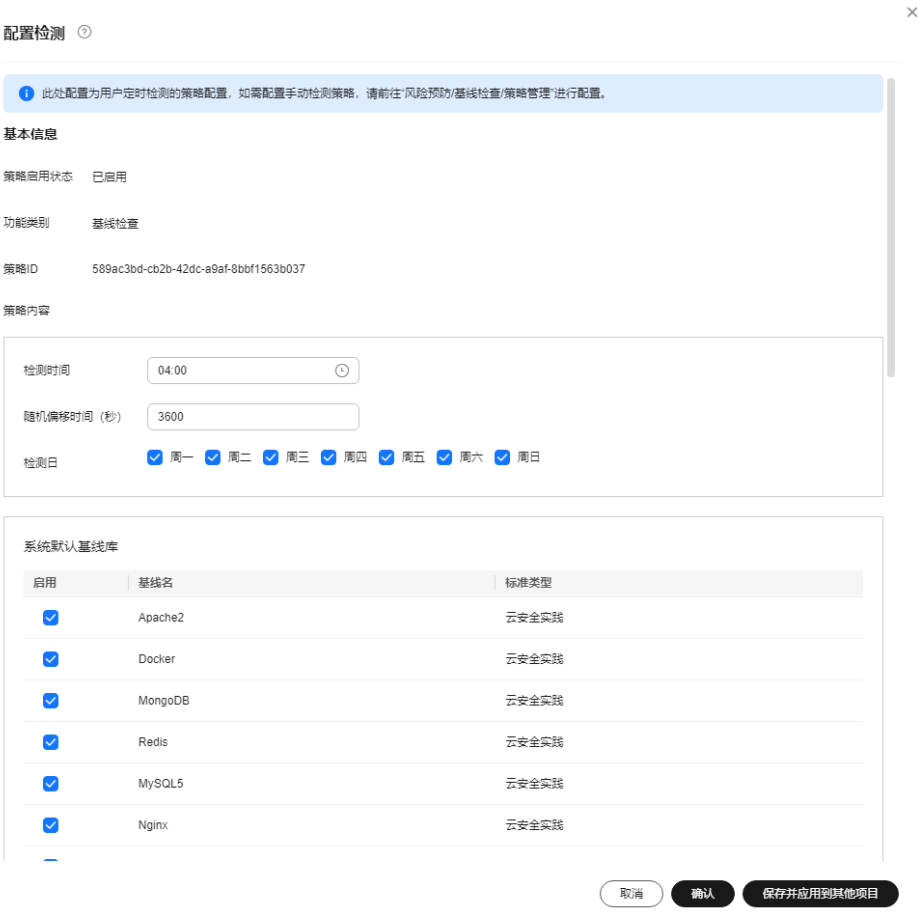


表 7-6 系统配置检测策略内容参数说明

参数	说明
检测时间	配置系统检测的时间，可具体到每一天的每一分钟。
随机偏移时间（秒）	配置系统检测的随机偏移时间，可配置范围为“0~7200秒”。
检测日	系统配置检测日期，勾选周一到周日的检测系统配置的时间。
系统默认基线库	系统已经配置好的检测基线，只需要勾选需要扫描检测的基线即可，所有值均为默认，不可修改。

步骤3 勾选需要检测的基线或自定义基线。

说明

如果有等保合规的需求，可按需勾选“标准类型”为“等保合规”的基线项。

步骤4 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

Webshell 检测

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

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

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

图 7-3 修改 Webshell 检测策略

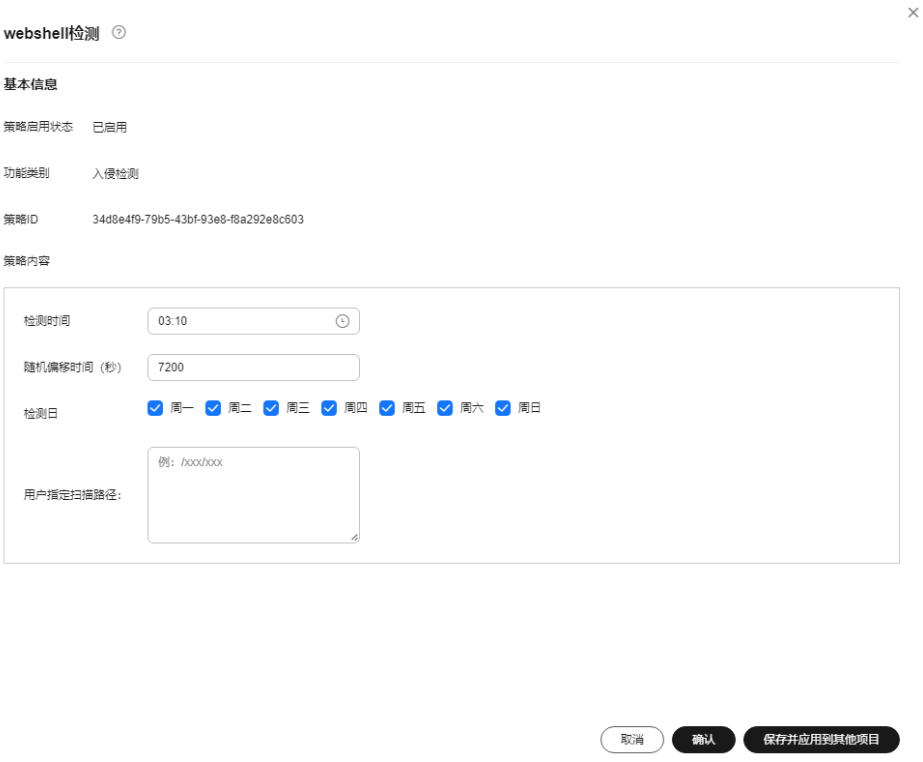


表 7-7 Webshell 检测策略内容参数说明

参数	说明
检测时间	配置Webshell检测的时间，可具体到每一天的每一分钟。

参数	说明
随机偏移时间（秒）	配置随机偏移时间，可配置范围为“0~7200秒”。
检测日	Webshell检测日期，勾选周一到周日的检测Webshell的时间。
用户指定扫描路径	手动添加需要检测的Web目录。 • 文件路径以“/”开头，不能以“/”结尾。 • 多个路径通过回车换行分隔且名称中不能包含空格。

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7-8所示。

图 7-4 修改文件保护策略

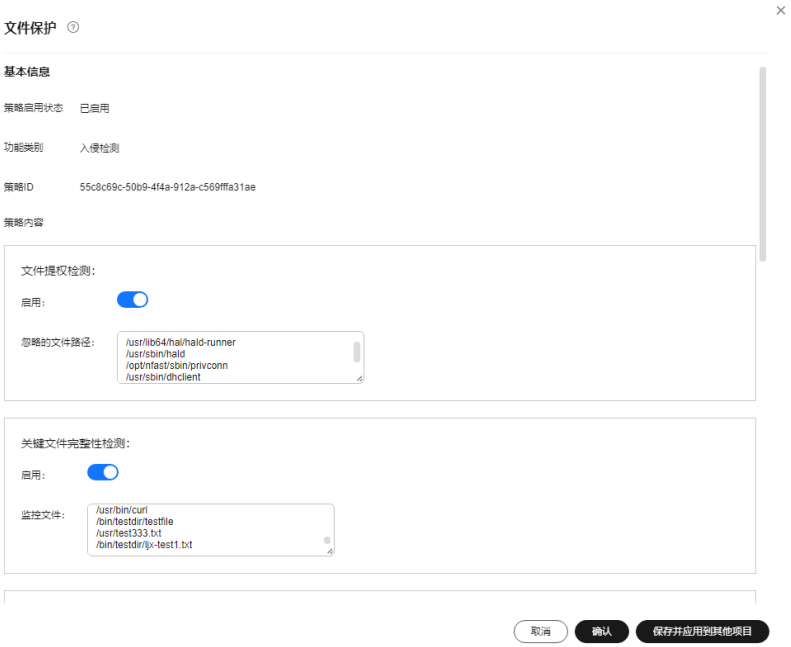


表 7-8 文件保护策略内容参数说明

参数	说明
文件提权检测	• 启用：是否开启文件提权检测。 –  ：开启。 –  ：关闭。 • 忽略的文件路径：填写需要忽略的文件路径。文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。
关键文件完整性检测	• 启用：是否开启关键文件完整性检测。 –  ：开启。 –  ：关闭。 • 监控文件：配置监控文件。
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。 • 会话IP白名单：如果操作文件的进程属于以上IP的会话，则不予审计。 • 忽略监控文件类型后缀：忽略监控的文件类型的后缀。 • 忽略监控的文件路径：配置忽略监控文件的路径。 • 监控登录密钥：是否开启监控登录密钥。 –  ：开启。 –  ：关闭。
文件目录监控	• 监控模式：监控文件或目录路径的模式。 • 文件或目录路径：系统预置了部分文件或目录监控路径，您可以自行修改需要检测的文件更改类型以及添加需要监控的文件或目录路径。

步骤3 确认无误，单击“确认”，完成修改。

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。

图 7-5 修改 HIPS 检测策略

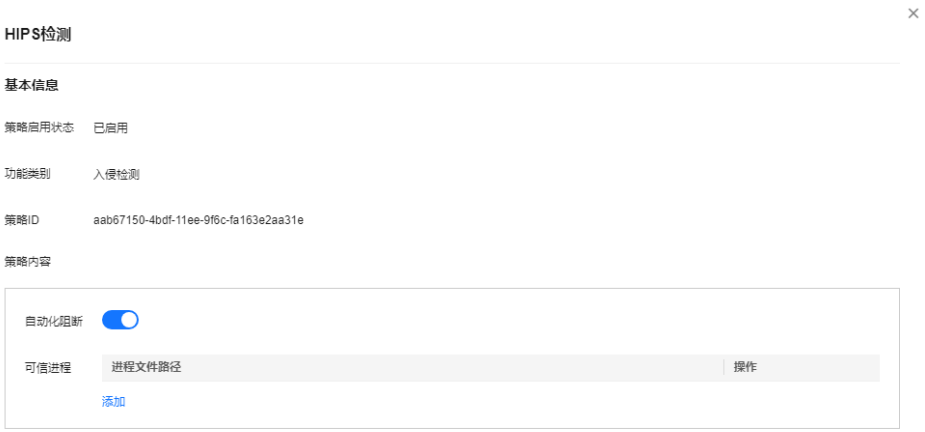


表 7-9 HIPS 检测策略内容参数说明

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。

图 7-6 修改安全检测策略

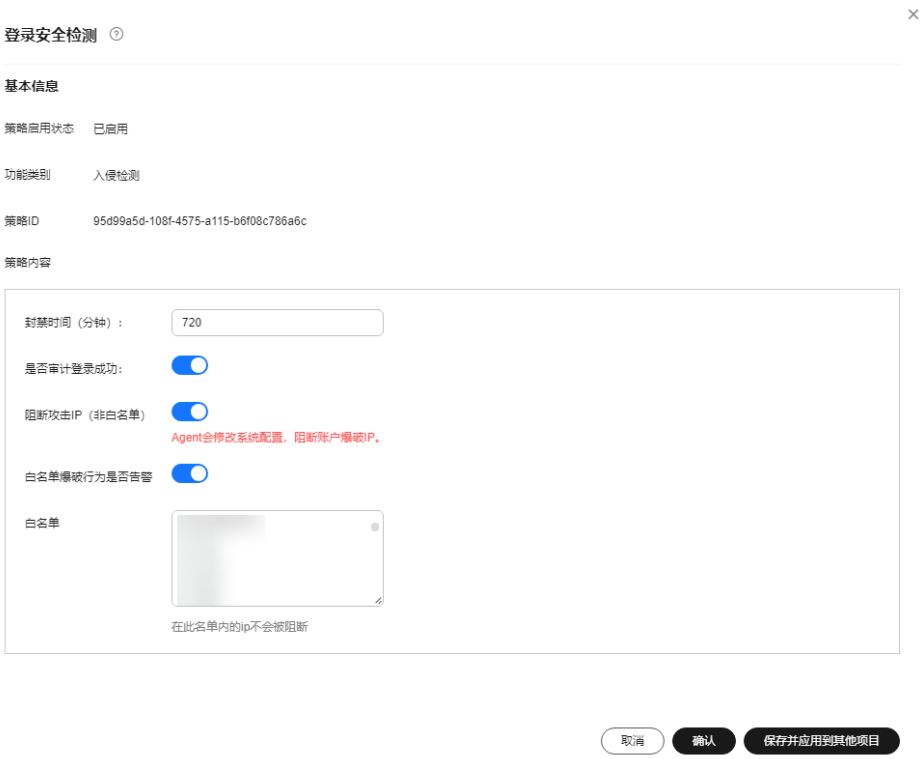


表 7-10 登录安全检测策略内容参数说明

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。
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7-11所示。

图 7-7 修改恶意文件检测策略

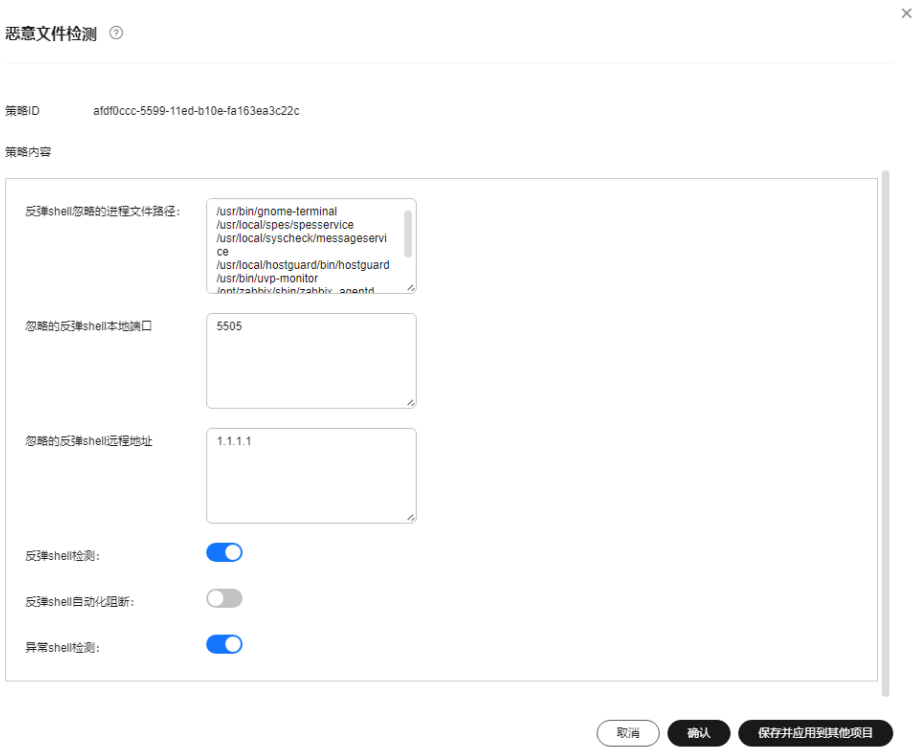


表 7-11 恶意文件检测策略内容参数说明

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	• 选择是否开启反弹shell检测，建议开启。 –  ：开启。 –  ：关闭。

参数	说明
反弹Shell自动化阻断	选择是否开启反弹Shell自动阻断，建议开启。 ●  ：开启。 ●  ：关闭。 **说明** 在**开启恶意程序隔离查杀**后生效。
异常shell检测	● 选择是否开启异常shell检测，建议开启。 –  ：开启。 –  ：关闭。

步骤3 确认无误，单击“确认”，完成修改。

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7-12**所示。

表 7-12 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7-13所示。

图 7-8 修改 root 提权策略

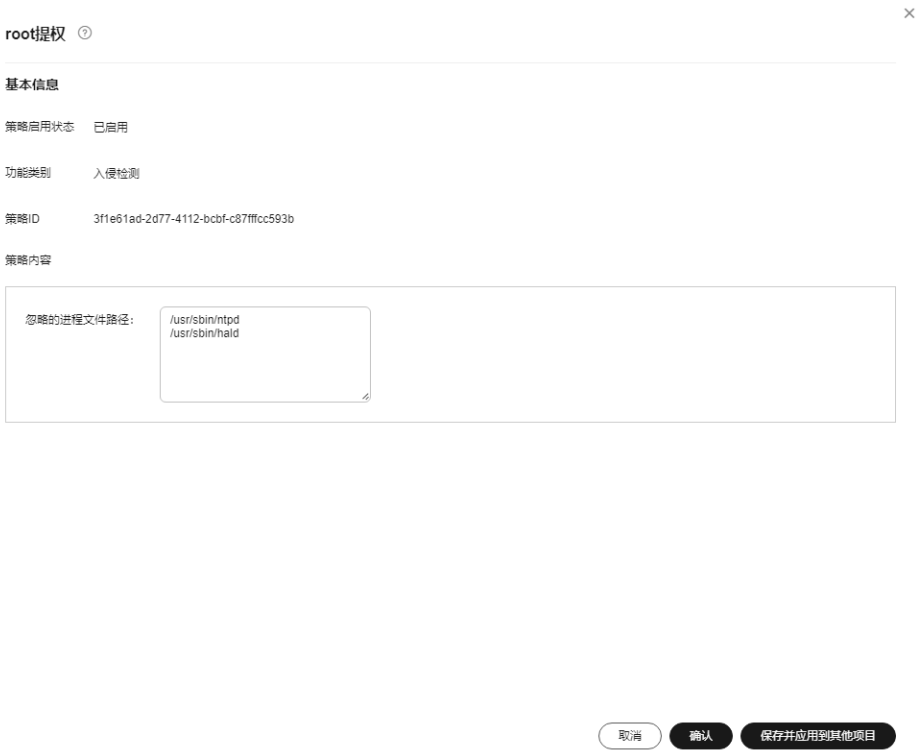


表 7-13 root 提权策略内容参数说明

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7-14所示。

图 7-9 修改实时进程策略

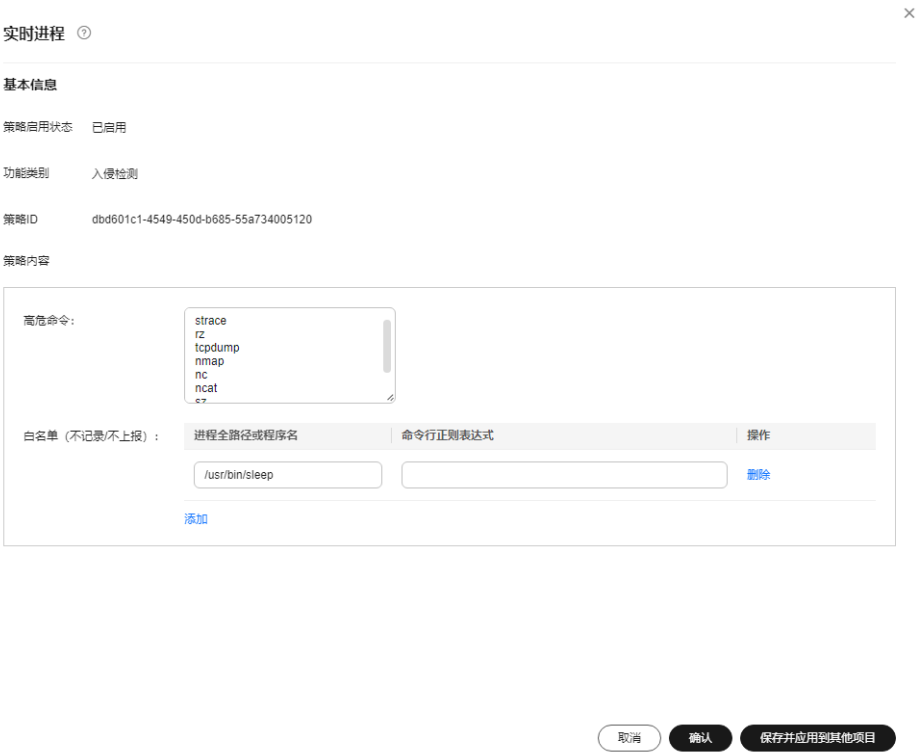


表 7-14 实时进程策略内容参数说明

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（ /*\=>. : ' " +- ）。 **说明** 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”。

图 7-10 修改 rootkit 检测策略

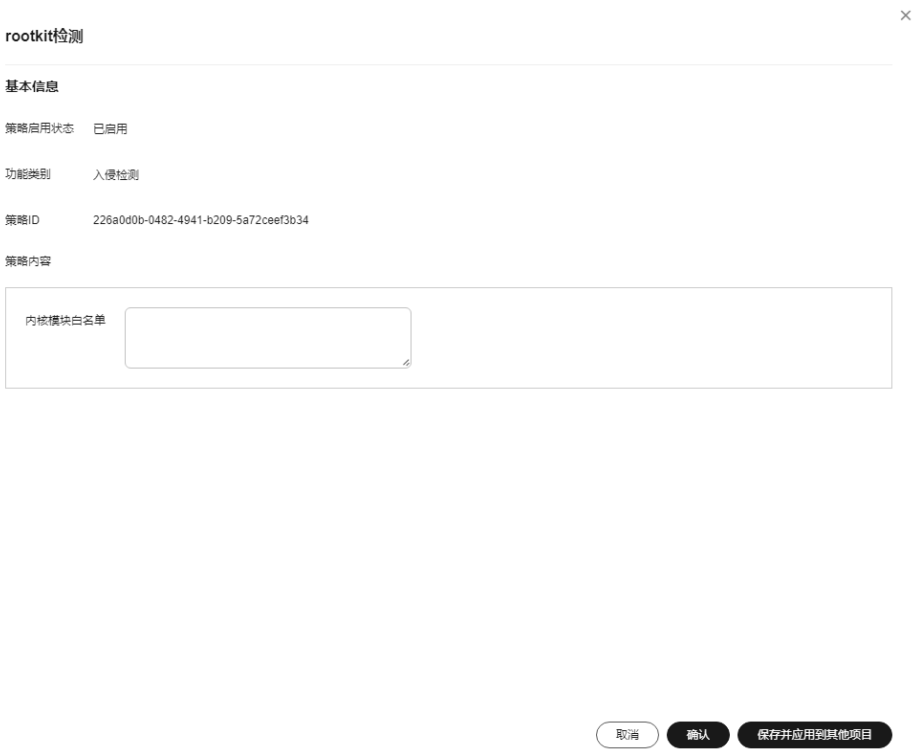


表 7-15 rootkit 检测策略内容参数说明

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7-16所示。

表 7-16 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：检测为高危等级病毒文件将自动执行隔离，其余风险等级病毒不自动隔离。 • 人工处置：检测的病毒无论是什么风险等级，都不会自动隔离，需手动处理。	自动处置

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7-17所示。

说明

白名单优先级更高，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。

表 7-17 容器信息收集策略参数说明

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

步骤3 确认无误，单击“确认”，完成修改。

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7-18所示。

表 7-18 集群入侵检测策略参数说明

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

说明

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

步骤3 确认无误，单击“确认”，完成修改。

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 7-19 容器逃逸策略参数说明

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

步骤3 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 7-20 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。 • 多个镜像白名单以换行符相隔，最多可添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。 多个组织白名单以换行符相隔，最多可添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

须知

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

步骤1 单击“容器文件监控”，滑出“容器文件监控”策略详情界面。

步骤2 在弹出的容器文件监控界面中，修改“策略内容”，参数说明如**表7-21**所示。

表 7-21 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
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7-22所示。

表 7-22 容器进程白名单策略参数说明

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

步骤3 确认无误，单击“确认”，完成修改。

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7-23所示。

表 7-23 镜像异常行为策略参数说明

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

参数名称	参数说明	取值样例
规则模板	• 选择不同的规则进行配置，支持的规则项如下： – 镜像白名单 – 镜像黑名单 – 镜像标签白名单 – 镜像标签黑名单 – 创建容器白名单 – 创建容器黑名单 – 容器mount proc白名单 – 容器seccomp unconfined – 容器特权白名单 – 容器capabilities白名单 • 规则填写参数说明如下： – 精准匹配：通过目标镜像名称来检测，填写目标镜像名称匹配镜像，多个名称以英文分号隔开，最多填写20个。 – 正则匹配：通过正则来检测，填写正则表达式匹配镜像，多个表达式以英文分号隔开，最多填写20个。 – 前缀匹配：通过前缀名称来检测，填写前缀名称匹配镜像，多个前缀以英文分号隔开，最多填写20个。 – 标签名称：通过标签及标签值来筛选检测，最多可添加20个标签项。 – 权限类型：通过选择权限进行指定检测或忽略检测，权限说明详情请参见**表7-24**。	-

表 7-24 镜像异常行为权限说明

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

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

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

步骤3 确认无误，单击“确认”，完成修改。

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7-25所示。

表 7-25 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	填写IP白名单，多个用英文分号隔开。	test_bj4
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

自保护

自保护策略是保护主机安全服务的软件、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。

7.1.4 删除策略组

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。

约束限制

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。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 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5 单击“确认”，完成删除。

----结束

7.2 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。

约束限制

HSS基础版不支持该功能，购买和升级HSS的操作请参见**购买主机安全防护配额**和**配额版本升级**。

查看所有漏洞的历史处置记录

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 选择“漏洞管理”页签，查看所有漏洞的历史处置记录。

- 查看指定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，输入漏洞类型、漏洞名称、服务器IP等并单击，可查看指定属性的漏洞处置记录。

----结束

查看安全告警事件的历史处置记录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 选择“安全告警事件”页签，查看安全告警事件的历史处置记录。

- 查看指定企业项目的安全告警事件处置记录

  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安全告警事件的处置记录。

- 查看指定属性的安全告警事件处置记录

  在安全告警事件列表上方搜索框中，输入告警名称、告警等级、攻击标识等并单击，可查看指定属性的安全告警事件处置记录。

----结束

查看病毒查杀的历史处置记录

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

步骤4 选择“病毒查杀”页签，查看病毒查杀告警事件的历史处置记录。

- 查看指定企业项目的病毒查杀事件处置记录

  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病毒查杀告警事件的处置记录。

- 查看指定属性的病毒查杀事件处置记录

  在病毒查杀事件列表上方搜索框中，输入病毒名称、病毒文件路径、病毒等级、病毒类型等并单击，可查看指定属性的病毒查杀告警事件处置记录。

----结束

8 安全报告

8.1 安全报告

8.1.1 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，您可通过该章节创建需要生成报告的周期和内容。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

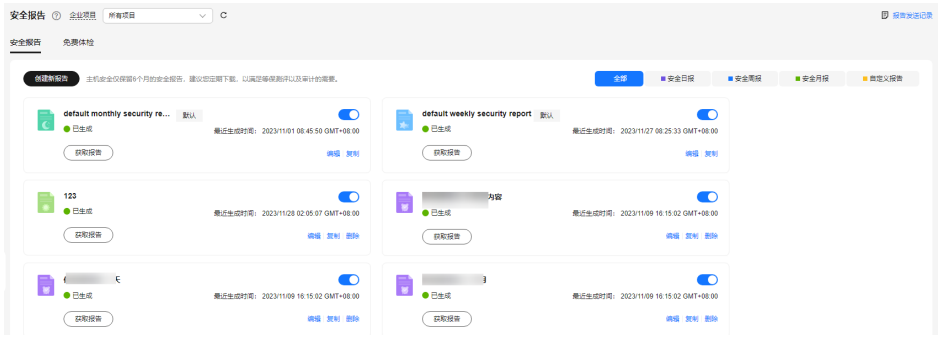
步骤3 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-1 查看安全报告



步骤4 创建新报告

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

步骤5 对报告基本信息进行配置，参数说明如表8-1所示。

表 8-1 报告基本信息参数说明

参数名称	参数说明	取值样例
报告名称	默认的报告名称。	ecs security report
报告类型	报告的统计周期类型名称。 ● 安全日报（统计周期为每天00:00-24:00） ● 安全周报（统计周期为周一00:00-周日24:00） ● 安全月报（统计周期为每月1号00:00-月度最后一天24:00） ● 自定义报告（自定义统计周期，周期范围应介于1天（包含）至3个月（包含）之间）。 ● 所有类型报告将在生成后的次日自动发送至您设置的报告接收人。	安全月报
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。 ● 消息中心：使用消息中心和其它安全服务共同使用“安全事件通知”的信息接收人。需登录控制台，在右上角信箱查看。 ● 消息主题：为HSS单独创建的主题，设置告警通知接收人。可选择短信或邮件接收通知。 ● 无需发送到邮箱：不发送报告至邮箱。	消息主题

步骤6 确认信息无误，单击页面右下角“下一步”，配置报告内容。

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

----结束

8.1.2 订阅安全报告

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

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

订阅说明

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

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

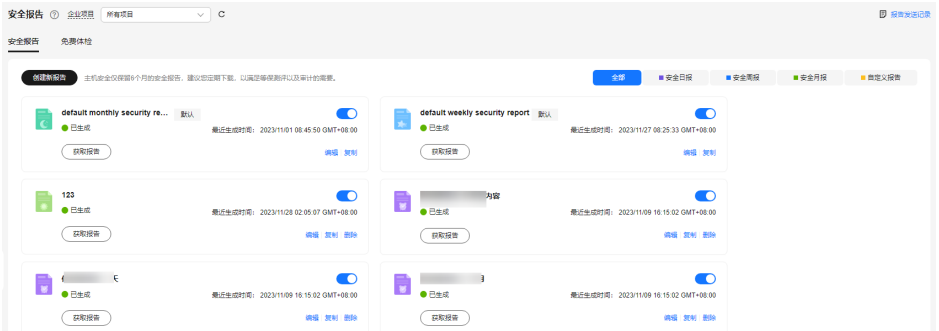
步骤3 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-2 查看安全报告



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

图 8-3 开启安全报告

----结束

8.1.3 查看安全报告

主机安全服务支持订阅日报、周报、月报和自定义，展现不同周期主机安全趋势以及关键安全事件与风险，订阅报告将为您保存6个月，以满足等保测评以及审计的需要。

说明

- 如果您已开通企业项目，您可以在“企业项目”下拉列表中，选择您所在的企业项目，订阅您所在企业项目的主机安全报告；或者选择“所有项目”，订阅当前区域下所有项目的主机安全报告。
- 勾选订阅报告后，第二天即可查看、下载。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

安全报告概览

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

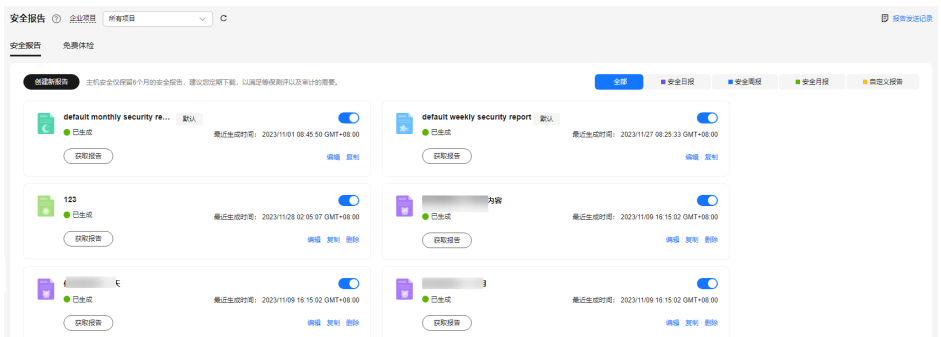
步骤3 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-4 查看安全报告



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

----结束

查看报告发送记录

发送记录存储了邮件发送报告的发送详情。

步骤1 单击安全报告概览页右上角的“报告发送记录”查看报告发送记录。

步骤2 在弹窗中查看报告发送记录，参数说明如表8-2所示。

表 8-2 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

8.1.4 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，该章节将指导您完成相关操作。

约束限制

需开启企业版、旗舰版、网页防篡改版及容器版任一版本。

编辑安全报告

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

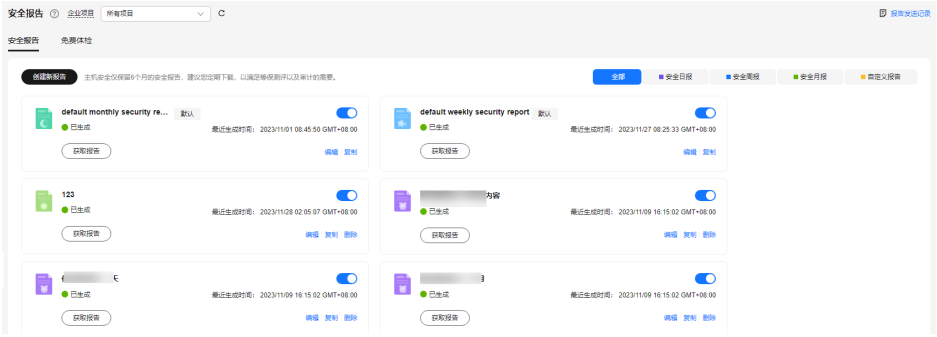
步骤3 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-5 查看安全报告



步骤4 单击目标报告的“编辑”按钮，对报告进行编辑。

步骤5 对报告基本信息进行编辑，参数说明如表8-3所示。

表 8-3 报告基本信息参数说明

参数名称	参数说明	取值样例
报告名称	默认的报告名称。	default monthly security report
报告类型	报告的统计周期类型名称，不可编辑。	安全月报
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。 • 消息中心：使用消息中心和其它安全服务共同使用“安全事件通知”的信息接收人。需登录控制台，在右上角信箱查看。 • 消息主题：为HSS单独创建的主题，设置告警通知接收人。可选择短信或邮件接收通知。 • 无需发送到邮箱：不发送报告至邮箱。	消息主题

步骤6 确认信息无误，单击页面右下角“下一步”，编辑报告内容。

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

----结束

关闭订阅

步骤1 登录管理控制台，进主机安全服务页面。

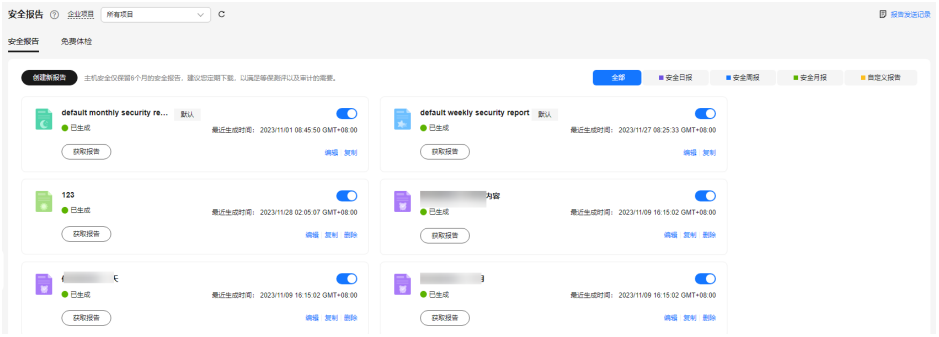
步骤2 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-6 查看安全报告



步骤3 单击目标报告的开关，使其状态为  ，表示目标报告订阅已关闭。

----结束

删除报告

说明

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

步骤1 登录管理控制台，进主机安全服务页面。

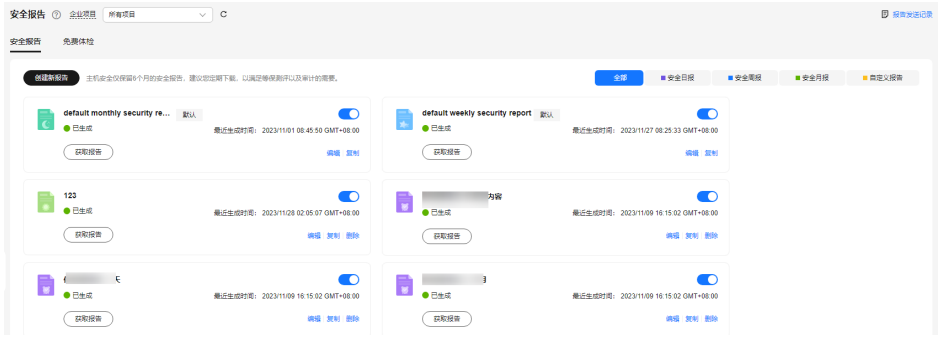
步骤2 左侧选择“安全报告”进入安全报告概览页面。

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

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。

图 8-7 查看安全报告



步骤3 单击目标报告的“删除”，对目标报告进行删除。

----结束

8.2 免费体检

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。

如果有基线检查、应用防护、网页防篡改、勒索防护、入侵检测、策略管理、文件完整性检测、隔离查杀等检测或防护需求，您可**开启主机安全防护**。

免费体检说明

- 针对未开启防护的服务器每周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周一凌晨。
- 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。
- 在报告中单一体检项仅支持展示总结果数的一半，且最多仅展示5条体检结果。
- 如果有实时防护、报告下载、漏洞在线修复、等保认证等需求，您可通过购买主机安全服务的不同版本来满足。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“安全报告 > 免费体检”查看未开启防护资产的体检情况。

说明

该页面免费体检的服务器均为未开启防护的服务器。

图 8-8 免费体检

步骤4 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

9 安装与配置

9.1 Agent 管理

9.1.1 查看 Agent 状态

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

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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 查看Agent状态。

步骤5 单击“接入多云资产”，可查看Agent安装快速指导。

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

----结束

9.1.2 升级 Agent

主机安全服务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主机安全服务。

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 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置”，进入Agent管理页面。

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“待升级Agent数”区域的数值，筛选待升级Agent的服务器。

步骤5 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6 在弹窗中确认即将升级Agent的服务器，确认无误，单击“确认”，开始执行自动升级。

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

----结束

Agent 自动升级

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置”，进入Agent管理页面。

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。

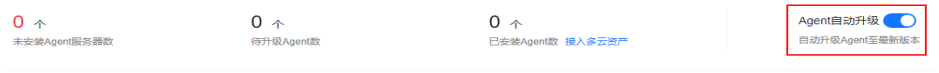
步骤4 单击  ，开启Agent自动升级。

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。

说明

只有Agent状态为“在线”时，才能执行自动升级。

图 9-1 开启 Agent 自动升级



----结束

相关操作

安装Agent

9.1.3 卸载 Agent

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

卸载方式说明

卸载方式	说明
Agent在线卸载	如果主机上的Agent状态为“在线”，可采用**Agent在线卸载**方式。
Agent离线卸载	如果主机上的Agent状态为“离线”，可采用**Agent离线卸载**方式。

Agent 在线卸载

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

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

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“已安装Agent数”区域的数值，查看Agent已安装的服务器列表，详情请参见**表Agent在线服务器列表参数说明**。

图 9-2 查看 Agent 在线列表

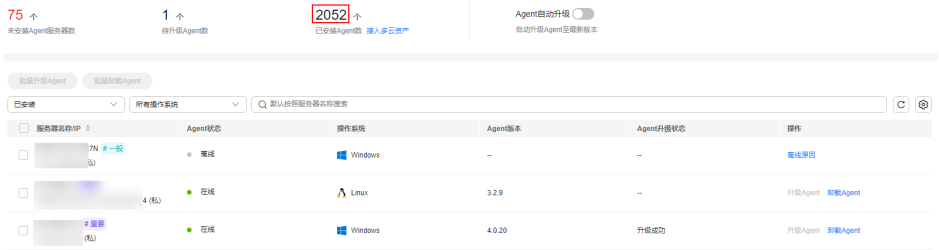


表 9-1 Agent 在线服务器列表参数说明

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

步骤5 单击目标服务器“操作”列的“卸载Agent”，在弹窗中确认卸载信息无误，单击“确认”，完成卸载。

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。

----结束

Agent 离线卸载

- **卸载Linux版本Agent**
  a. 登录需要卸载主机安全服务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。

     说明

     不可以在/usr/local/hostguard/目录下执行卸载命令，可以在其他任意目录下执行卸载命令。

     - 针对EulerOS、CentOS、RedHat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。如果卸载失败请执行步骤3。

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


c. （可选）当执行步骤2卸载Agent失败时，可参考如下方式卸载Agent。

- 针对EulerOS、CentOS、RedHat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”**杀死所有残留进程。
  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”**杀死所有残留进程。
  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. 登录需要卸载主机安全服务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 File\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。

相关操作

安装Agent

9.2 账号管理

9.2.1 账号管理概述

主机安全服务具备安全可靠的跨账号数据汇聚和资源访问能力，如果您的账号由组织管理，您可以对组织内所有成员账号进行统一的工作负载安全防护：

- 统一对组织内所有成员账号的主机进行安全防护，包括资产管理、漏洞检测和修复、基线检查以及入侵检测等。
- 统一对组织内所有成员账号的容器进行安全防护。

通过HSS对组织成员账号进行工作负载安全防护需要执行以下操作：

1. 添加组织成员账号
2. 查看账号管理

有关组织的详细说明请参见《组织用户指南》。

9.2.2 添加组织成员账号

如果您需要对组织成员账号进行工作负载安全防护，您可以参考本章节添加账号。

前提条件

- 已创建组织，相关操作详情请参见创建组织。
- 已设置HSS为可信服务，操作详情请参考启用、禁用可信服务。
- 当前操作的账号为组织管理账号或委托管理员账号。

约束限制

账号管理功能仅部分region支持，支持的region请参见功能总览。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 账号管理”，进入账号管理页面，单击“添加账号”，

步骤4 在弹出页面通过树状展开勾选目标账号，自动添加至右侧“已选账号”，确认无误，单击“确认”。

说明

添加的账号为同一个组织内的账号，有关组织账号的详细说明请参见《组织账号概述》

步骤5 添加成功，在账号列表可查看添加的账号。

----结束

9.2.3 查看组织成员账号安全风险

添加组织成员账号后，您可以在账号管理页面，查看已添加到HSS进行工作负载防护的组织成员账号及相应账号的工作负载安全防护详情。

查看账号管理

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 账号管理”，进入账号管理页面，查看全部账号列表信息。账号列表信息参数说明请参见**表 账号列表参数说明**。

表 9-2 账号列表参数说明

参数名称	参数说明
账号名	账号名称。
项目名称	账号所属Region。
主机数量	账号下的主机数量。
漏洞管理（最近24小时）	最近24小时主机存在的漏洞数量。
基线检查（最近24小时）	最近24小时主机存在的基线风险数量。
安全告警（最近24小时）	最近24小时主机存在的安全告警数量。

----结束

删除账号

步骤1 单击目标账号“操作”列的“删除”。

步骤2 在弹窗中确认信息无误，单击“确认”，完成删除。

----结束

9.3 插件配置

9.3.1 插件配置概述

插件管理功能支持对多种插件进行管理，您可根据需求按照插件指导安装和管理需要的插件。

插件类型

当前仅支持Docker插件的管理。

Docker 插件应用场景

开通容器安全防护后，如果您需要使用镜像阻断功能，您需要**安装Docker插件**。

Docker插件是实现镜像阻断能力的一个插件。镜像阻断是一种容器安全防御功能， 它可以在Docker环境中容器启动前阻断具有高危漏洞或不符合安全标准的容器镜像的运行。

镜像阻断的应用场景如下：

- 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。

9.3.2 查看插件详情

呈现所使用的服务器使用插件详情。

可自定义对插件进行安装、升级、卸载操作。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 插件配置”，进入插件配置页面，查看插件列表详情。插件列表参数说明请参见**表 Docker插件列表参数说明**。

插件列表默认展示所有服务器，如果服务器安装了插件，插件列表会展示插件的详细信息，如果服务器未安装插件，插件信息为空。

表 9-3 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

9.3.3 安装插件

开通容器安全防护后，如果您需要使用镜像阻断功能，请参照本章节安装Docker插件。

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启主机安全服务容器版本。
- 目前仅支持华为云线上服务器。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件安装指南”，在滑出面板的“安装步骤”中获取安装命令，单击“复制”。

步骤4 以root权限远程登录待安装插件的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见在云服务器控制台上登录主机。

- 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5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量安装的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

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

步骤8 将批量安装的命令复制粘贴至命令框，键入回车，开始自动执行安装。

说明

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9 反馈“remote_install finished. [OK]”则安装成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

----结束

9.3.4 插件升级

可自行对目标服务器的插件进行升级。

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启主机安全服务容器版本。
- 目前仅支持华为云线上服务器。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件升级指南”，在滑出面板的“升级步骤”中获取升级命令，单击“复制”。

步骤4 以root权限远程登录待升级插件的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见**在云服务器控制台上登录主机**。
- 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账号在主机中升级插件。

步骤5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量升级的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

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

步骤8 将批量升级的命令复制粘贴至命令框，键入回车，开始自动执行升级。

说明

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9 反馈“remote_upgrade finished. [OK]”则升级成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

```
remote_upgrade finished. [OK]
```

----结束

9.3.5 卸载插件

约束限制

- 仅支持Docker类容器，暂不支持containerd的容器。
- Docker Engine版本在18.06.0以及以上。
- Docker API版本在1.38以及以上。
- 仅支持Linux操作系统。
- 仅支持X86和ARM硬件架构。
- 已开启主机安全服务容器版本。
- 目前仅支持华为云线上服务器。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树选择“安装与配置 > 插件配置 > Docker插件”，单击“插件卸载指南”，在滑出面板的“卸载步骤”中获取卸载命令，单击“复制”。

步骤4 以root权限远程登录待卸载插件的主机。

- 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见在云服务器控制台上登录主机。
- 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5 执行以下命令进入tmp目录。

```
cd /tmp/
```

步骤6 执行以下命令，创建文件linux-host-list.txt并将需要批量卸载的节点私有ip添加至文件中。

命令格式：

```
echo 127.8.8.8 22 root rootPassword >> linux-host-list.txt
或echo 127.8.8.8 22 user userPassword rootPassword >> linux-host-list.txt
```

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

步骤8 将批量卸载的命令复制粘贴至命令框，键入回车，开始自动执行卸载。

步骤9 反馈“remote_uninstall finished. [OK]”则卸载成功，等待3-5分钟可在“安装与配置 > 插件配置”查看面板服务器的Docker插件状态。

```
remote_uninstall finished. [OK]
```

----结束

10 审计

10.1 支持云审计的 HSS 操作列表

主机安全服务通过云审计服务（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10-1**所示。

表 10-1 云审计服务支持的 HSS 操作列表

操作名称	资源类型	事件名称
取消忽略端口	hss	notIgnorePortStatus
忽略端口	hss	ignorePortStatus
取消忽略配置检测项	hss	notIgnoreCheckRuleStat
忽略配置检测项	hss	ignoreCheckRuleStat
重新进行基线检测	hss	runBaselineDetect
解绑配额	hss	cancelHostsQuota
关闭容器防护	hss	closeContainerProtectStatus
开启容器防护	hss	openContainerProtectStatus
解除已拦截IP	hss	changeBlockedIp
处理事件状态	hss	changeEvent
恢复已隔离文件	hss	changeIsolatedFile
删除告警白名单	hss	removeAlarmWhiteList
添加登录告警白名单	hss	addLoginWhiteList
删除登录告警白名单	hss	removeLoginWhiteList

操作名称	资源类型	事件名称
新增服务器组	hss	addHostsGroup
分配到服务器组	hss	associateHostsGroup
修改服务器组	hss	changeHostsGroup
删除服务器组	hss	deleteHostsGroup
关闭主机防护	hss	closeHostsProtectStatus
开启主机防护	hss	openHostsProtectStatus
卸载agent	hss	uninstallAgents
运行镜像扫描	hss	runImageScan
从SWR服务同步镜像列表	hss	runImageSynchronizeTask
更新并扫描SWR镜像	hss	runSwrImageScan
重新体检	hss	resetRiskScore
添加策略组	hss	addPolicyGroup
删除策略组	hss	deletePolicyGroup
部署策略组	hss	deployPolicyGroup
修改策略内容	hss	modifyPolicyDetail
修改策略组	hss	modifyPolicyGroup
关闭自动隔离查杀	hss	closeAutoKillVirusStatus
开启自动隔离查杀	hss	openAutoKillVirusStatus
设置常用登录IP	hss	modifyLoginCommonIp
设置常用登录地	hss	modifyLoginCommonLocation
设置SSH登录白名单	hss	modifyLoginWhiteIp
修复漏洞	hss	changeVulStatus
添加防护目录	hss	addHostProtectDirInfo
添加特权进程	hss	addPrivilegedProcessInfo
添加定时关闭防护配置	hss	addTimingOffConfigInfo
删除远端备份服务器	hss	deleteBackupHostInfo
删除防护目录	hss	deleteHostProtectDirInfo
删除特权进程	hss	deletePrivilegedProcessInfo
删除定时关闭防护配置	hss	deleteTimingOffConfigInfo

操作名称	资源类型	事件名称
设置定时关闭防护周期	hss	setDateOffConfigInfo
修改防护目录开启状态	hss	setProtectDirSwitchInfo
修改动态网页防篡改状态	hss	setRaspSwitch
设置远端备份服务器	hss	setRemoteBackupInfo
修改定时关闭防护状态	hss	setTimingOffSwitchInfo
关闭网页防篡改防护	hss	closeWtpProtectionStatus
开启网页防篡改防护	hss	openWtpProtectionStatus
修改远端备份服务器	hss	updateBackupHostInfo
修改防护目录	hss	updateHostProtectDirInfo
修改特权进程	hss	updatePrivilegedProcessInfo
修改Tomcat bin目录	hss	updateRaspPathInfo
修改定时关闭防护时间段	hss	updateTimingOffConfigInfo

10.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

在新版事件列表查看审计事件

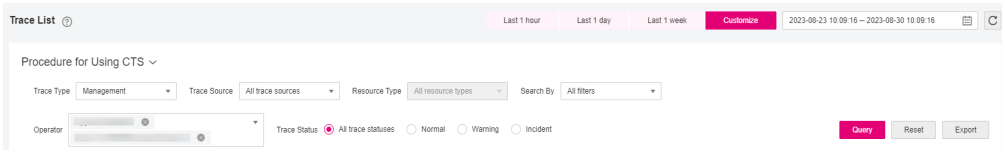
1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
   - 单击 按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。

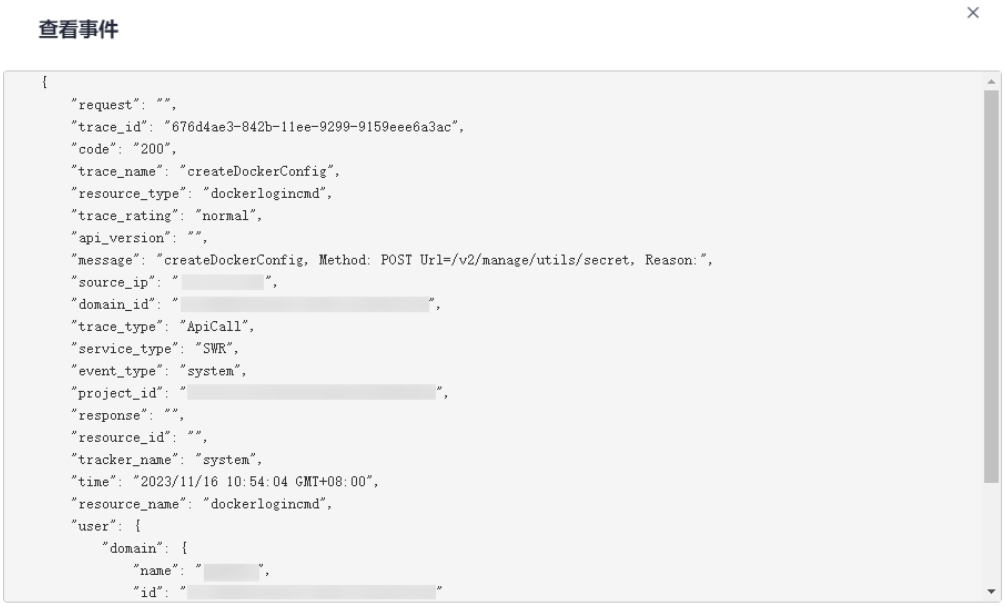
2. 单击左上角 ☰，选择“管理与监管管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件，如图10-1所示。当前事件列表支持四个维度的组合查询，详细信息如下：

图 10-1 筛选框



   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询最近7天内任意时间段的操作事件。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 ↻ 按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 ⌄ 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**“云审计服务事件参考 > 事件结构”章节和**事件样例**“云审计服务事件参考 > 事件样例”章节。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

11 监控

11.1 HSS 监控指标说明

功能说明

本节定义了主机安全服务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定义，用户可以通过云监控服务提供管理控制台或API接口来检索主机安全服务产生的监控指标和告警信息。

命名空间

SYS.HSS

监控指标

表 11-1 主机安全服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	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个	服务器	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个	服务器	300秒
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个	服务器	300秒

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
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个	服务器	300秒

维度

表 11-2 维度列表

key	Value
hss_enterprise_project_id	企业项目，取值为企业项目ID。

11.2 设置监控告警规则

通过设置HSS告警规则，用户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、监控指标、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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“管理与监管 > 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”页面。

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 根据界面提示配置参数。

关键参数如下，更多配置参数信息，请参见**创建告警规则和通知**：

- 告警名称：系统会生成一个名称，也可以进行修改。
- 资源类型：主机安全服务
- 维度：主机安全
- 监控范围：告警规则适用的资源范围，可选全部资源或指定资源。
- 触发规则：选择需要可选择关联模板、导入模板或自定义模板。

说明

选择关联模板后，所关联模板内容修改后，该告警规则中说包含策略也会跟随修改。

- 告警策略：触发告警规则的告警策略。

步骤7 根据界面提示，配置告警通知参数

如果要配置通过邮件、短信、HTTP和HTTPS向用户发送告警通知，则设置“发送通知”为开启 。

更多配置参数信息，请参见**创建告警规则和通知**。

步骤8 配置完成后，单击“立即创建”，完成告警规则的创建。

----结束

11.3 查看监控指标

云平台提供的云监控服务，可以对主机安全服务防护的服务器情况进行监控。您可以通过管理控制台，查看主机安全服务的各项监控指标。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“管理与监管 > 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 权限管理

12.1 创建用户并授权使用 HSS

如果您需要对您所拥有的HSS进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，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、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用HSS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图12-1**所示。

前提条件

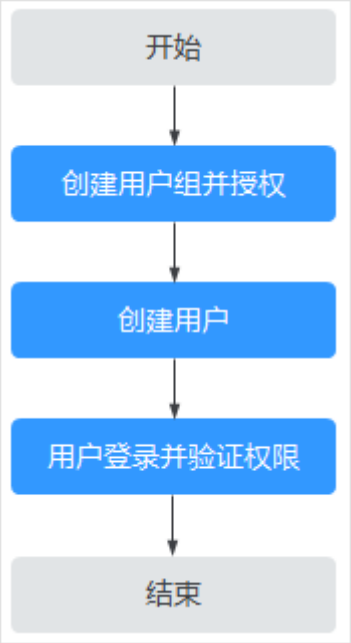
给用户组授权之前，请您了解用户组可以添加的HSS权限，并结合实际需求进行选择，HSS系统策略如**表12-1**所示。

表 12-1 HSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
HSS Administrator	主机安全服务（HSS）管理员，拥有该服务下的所有权限。	系统角色	• 依赖Tenant Guest角色。 Tenant Guest：全局级角色，在全局项目中勾选。 • 购买HSS防护配额需要同时具有ECS ReadOnlyAccess、BSS Administrator和TMS ReadOnlyAccess角色。 – ECS ReadOnlyAccess：系统策略，弹性云服务器的只读访问权限。 – BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 – TMS ReadOnlyAccess：系统策略，标签管理服务的只读访问权限。
HSS FullAccess	主机安全服务所有权限。	系统策略	购买HSS防护配额需要具有BSS Administrator角色。 BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 SMN ReadOnlyAccess：系统策略，消息通知服务的只读访问权限。
HSS ReadOnlyAccess	主机安全服务的只读访问权限。	系统策略	SMN ReadOnlyAccess：系统策略，消息通知服务的只读访问权限。

示例流程

图 12-1 给用户授权服务权限流程



1. **创建用户组并授权**。在IAM控制台创建用户组，并授予HSS服务的管理员权限“HSS Administrator”。
2. **创建用户并加入用户组**。在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在“服务列表”中选择除主机安全服务外（假设当前策略仅包含“HSS Administrator”）的任一服务，如果提示权限不足，表示“HSS Administrator”已生效。

12.2 HSS 自定义策略

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

目前华为云支持以下两种方式创建自定义策略：

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

具体创建步骤请参见：**创建自定义策略**。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"
            ]
        }
    ]
}
```

12.3 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），如果华为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。

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。

主机安全服务（HSS）支持的自定义策略授权项如下所示：

授权列表，包含HSS对应的授权项，如查询主机安全防护列表、云服务器开启或关闭防护、手动检测等。

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	-

权限	授权项	依赖的授权项
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	-
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	-

权限	授权项	依赖的授权项
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	-
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	-

权限	授权项	依赖的授权项
查询入侵检测事件列表	hss:event:get	-
入侵检测事件操作	hss:event:set	-
查询服务器分组信息	hss:hostGroup:get	-
设置服务器组	hss:hostGroup:set	-
文件完整性管理	hss:keyfiles:set	-
查询关键文件变更报告	hss:keyfiles:list	-
查询自启动列表	hss:launch:list	-

13 （可选）管理企业项目

13.1 管理项目和企业

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

创建项目并授权

- 创建项目

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

- 授权

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

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

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

创建企业项目并授权

- 创建企业项目

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

  说明

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

- 授权

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

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

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

- 关联资源与企业项目

  企业项目可以将云资源按企业项目统一管理。

  – 购买主机安全服务时选择企业项目

    在购买页面，“企业项目”下拉列表中选择目标企业项目，实现资源与企业项目关联。

  – 资源迁入

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

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

  更多信息，请参阅**《企业管理用户指南》**。

13.2 管理所有项目

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

- 绑定主机配额

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

- 批量安全配置

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

- 部署策略组

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

  “所有项目”中的策略组独立于其他每一个企业项目的策略组，与其他企业项目的策略组互不干扰。

- 订阅所有项目安全报告

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

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

前提条件

拥有Tenant Administrator权限，或者HSS Administrator+Tenant Guest权限。

绑定主机配额

如下，以在“所有项目”中为任意一个企业项目的主机绑定“主机安全服务网页防篡改版配额”为例说明。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务页面。

步骤3 选择“资产管理 > 主机管理 > 防护配额”，进入“防护配额”页面，在防护配额页面，您可以查看主机防护的防护配额。

步骤4 在配额列表中，选择“使用状态”为“空闲”的配额，单击“绑定主机”，为主机绑定配额。

步骤5 在弹出的配额详情对话框中，选择待绑定配额的主机。

步骤6 单击“确定”，完成配额绑定。绑定配额后，您可以在云服务器列表中，查看到该主机已开启防护。

----结束

绑定容器配额

如下，以在“所有项目”中为任意一个企业项目的节点绑定“容器版配额”为例说明。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务页面。

步骤3 选择“资产管理 > 容器管理 > 防护配额”，进入“防护配额”页面，在防护配额页面，您可以查看容器防护的防护配额。

步骤4 在配额列表中，查看“使用状态”为“空闲”的配额，即可以绑定主机的配额单。

步骤5 选择“节点列表”页签，在目标“未防护”的服务器“操作”列单击“开启防护”。

说明

开启防护的主机“服务器状态”须为“正常”，“Agent状态”须为“在线”。

步骤6 在弹出的配额详情对话框中，选择待绑定配额的主机。

在“您确定要对以下集群开启防护吗？”对话框中，“计费模式”选择“包年/包月”，阅读并确认“《容器安全服务免责声明》”。

“防护配额”分配方式：

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

- 指定分配：下拉框选择具体配额ID，您可以为主机分配指定的配额。

步骤7 单击“确定”，完成配额绑定。绑定配额后，您可以在云服务器列表中，查看到该主机已开启防护。

----结束

A 修订记录

发布日期	修改说明
2024-03-25	第二十一次正式发布。 新增： • **接入指引** • **动态端口蜜罐** • **创建安全组策略（云原生网络2.0模型集群）** • **管理安全组策略（云原生网络2.0模型集群）** • **管理文件隔离箱** 优化： • **导出基线检查报告**，口令复杂度策略检测结果支持导出。 • **新建防护策略**，增加动态诱饵开关说明。 • **扫描病毒**，病毒查杀支持自动隔离。 • **主机安全告警事件概述**，Webshell支持手动隔离查杀；增加自动隔离查杀说明。 • **管理登录告警白名单**，登录白名单更名为“登录告警白名单”。 • **配置策略**，优化Webshell检测、文件保护、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、资产发现、配置检测、端口扫描检测策略；新增容器信息模块策略；新增企业项目选择“所有项目”时的策略修改可应用到其他项目。
2024-02-02	第二十次正式发布。 优化： • **总览**，安全评分模块介绍增加操作说明，各评分模块扣分标准表格拆分。 • **扫描漏洞**，修改扫描方式说明。 • **基线检查**，调整文档结构。 • **策略管理**，调整文档结构。

发布日期	修改说明
2023-12-21	第十九次正式发布。 新增： • **采集主机资产指纹** • **采集容器资产指纹** • **忽略服务器** • **SWR企业版镜像** • **导出容器节点列表** • **导出防护配额列表** • **网页防篡改概述** • **病毒查杀** • **导出主机告警事件** • **导出容器告警事件** 优化： • **安装Agent**，增加Agent概述；整合Agent安装操作。 • **告警通知项说明**，优化告警通知项表格。 • **常用安全配置**，主机登录保护、恶意程序隔离查杀、双因子认证独立为章节。 • **部署防护策略**，容器版策略支持部署。 • **本地镜像**，修改本地镜像关联服务器信息，全量扫描支持查看进度。 • **SWR私有镜像管理**，全量扫描支持查看进度、基线检查结果支持导出。 • **SWR共享镜像管理**，全量扫描支持查看进度、基线检查结果支持导出。 • **绑定防护配额**，配额支持自动绑定。 • **漏洞管理**，支持扫描应急漏洞。 • **基线检查概述**，弱口令检测支持Windows系统口令。 • **处理主机告警事件**，告警白名单规则支持远程IP和用户名。 • **配置策略**，弱口令检测策略内容删除检测休息时间，恶意文件检测策略新增可忽略信息。 • **升级Agent**，支持自动升级。 • **SWR镜像仓库漏洞**，支持扫描应用漏洞、优化漏洞列表信息。

发布日期	修改说明
2023-10-27	第十八次正式发布。 新增： • **集群Agent管理** • **应用进程控制** • **容器集群防护** • **监控** • **导出主机告警事件** • **导出容器告警事件** • **查看安全告警事件的历史处置记录** 优化： • **总览**，改版。 • **主机安全告警事件概述**，新增可疑进程运行、可疑进程文件访问、异常行为外联、端口转发检测告警类型。 • **容器安全告警事件概述**，新增黑客工具、文件提权、关键文件变更、进程异常行为、可疑命令执行、用户密码窃取、异常外联行为、端口转发检测告警类型。 • **勒索病毒防护**，支持单独开启勒索病毒防护、勒索备份。 • **处理主机告警事件**，添加告警白名单支持添加自定义规则；支持同时处理重复告警。 • **处理容器告警事件**，添加告警白名单支持添加自定义规则；支持同时处理重复告警。 • **处理漏洞**，支持漏洞修复前执行备份。 • 服务中文名称修改为“主机安全服务”。

发布日期	修改说明
2023-07-25	第十七次正式发布。 新增： • **容器防火墙** • **管理系统用户白名单** • **查看容器信息** • **处置风险容器** • **查看漏洞历史处置记录** 优化： • **登录安全检测**，支持设置暴力破解白名单。 • **查看防护配额**，支持查看容器配额关联的服务器。 • **查看并处理基线检查结果**，增加MySQL版本差异说明。 • **添加防护目录**，增加排除子目录限制、导出防护目录说明 • **绑定防护配额**，支持容器配额绑定。 • **解绑防护配额**，支持容器配额解绑。 • **查看并处理基线检查结果**，增加选择不同策略，可查看相应检测结果说明。 • **本地镜像**，支持漏洞报告导出。 • **SWR私有镜像管理**，支持漏洞报告导出、软件合规和基础镜像信息检测。 • **SWR共享镜像管理**，支持漏洞报告导出和安全扫描。 • **容器安全告警事件概述**，支持检测并告警进程提权、暴力破解、非法系统用户账号、高危命令执行。 • **恶意文件检测**，支持设置反弹Shell自动化阻断。 • **策略管理概述**，新增自动自保护。 • **开启告警通知**，每日告警通知增加“未安装Agent”告警通知项。 • **恢复服务器数据**，增加备份标识说明。 • **漏洞管理**，优化操作流程，支持漏洞加白。 • **主机指纹**，中间件、Web应用、数据库支持Windows系统。 • **容器指纹**，支持账号、数据库、集群、服务、工作负载、容器。 • 实时更新容器资产信息（手动），支持集群、服务、工作负载、容器。
2023-06-15	第十六次正式发布。 优化： • **扫描漏洞**，增加单台服务器漏洞检测操作。 • **查看漏洞详情**，增加查看单台服务器漏洞操作。
2023-06-01	第十五次正式发布。 主机安全服务高级版更名为专业版上线。

发布日期	修改说明
2023-05-24	第十四次正式发布。 优化： • **管理服务器重要性**，优化内容。 • **容器镜像**，优化约束与限制。 • **查看插件详情**，优化内容。
2023-04-27	第十三次正式发布。 新增： • 2.4.3.2-漏洞检测（自动） • **购买备份存储库** 优化： **开启勒索病毒防护**，优化前提条件
2023-03-31	第十一次正式发布。 新增内容如下： • 补充高级版支持的功能及策略说明。 • 策略组支持AV检测、HIPS检测等检测能力。 • 入侵检测主机告警类型新增木马、病毒、蠕虫等类别。 • Windows新增支持诱饵检测能力。 • 支持手动更新主机资产。 • 支持账号统一管理。 • 资产策略新增自定义时间周期。 • 新增插件安装。
2023-01-18	第十次正式发布。 新增章节如下： • **本地镜像** • **SWR共享镜像管理** • **查看容器资产指纹** • **管理应用防护策略** • **添加特权进程** • **批量Linux服务器安装Agent（控制台一键方式）** • **升级Agent** 新增内容如下： • 企业版恶意文件策略支持反弹shell检测。 • 漏洞支持程序列表和包名的查看。 • 资产发现策略支持自定义检测时间和周期。 • 新增Rookits告警。 • 基线配置的风险支持一键修复。

发布日期	修改说明
2022-12-10	第九次正式发布。 修改如下章节： • **查看并处理勒索病毒防护事件** • **开启勒索病毒防护** • **管理勒索病毒防护策略** • **关闭勒索病毒防护**
2022-11-10	第八次正式发布。 新增章节如下： **免费体检**。 **扫描漏洞**
2022-10-11	第七次正式发布。 新增章节：**升级防护配额**。
2022-09-30	第六次正式发布。 新增章节如下： 开启防护 **关闭防护** **批量Linux服务器安装Agent（控制台一键方式）**
2022-09-20	第五次正式发布。 购买页面新增基础版（包年/包月）的购买。
2022-08-31	第四次正式发布。 修改基础版使用模式，限期免费使用。
2022-07-28	第三次正式发布。 新增支持应用防护功能。 新增支持的Region：中国-香港、亚太-曼谷、亚太-新加坡。 新增勒索病毒防护能力支持windows系统。
2022-07-05	第二次正式发布。 新增服务器关联资产重要性功能。 新增基线检查项支持导出功能。 新增支持对应用漏洞的检测功能。
2022-05-30	第一次正式发布。