主机安全服务

用户指南

文档版本 34

发布日期 2022-05-26

华为技术有限公司

版权所有 © 华为技术有限公司 2023。 保留一切权利。

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

商标声明

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

注意

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

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

目 录

1 开通主机防护 1
1.1 步骤一：购买防护配额 1
1.2 步骤二：安装 Agent 6
1.2.1 Linux 版本 6
1.2.2 Windows 版本 10
1.3 （可选）步骤三：设置告警通知 15
1.3.1 基础版/企业版/旗舰版 15
1.3.2 网页防篡改版 21
1.4 步骤四：开启主机防护 23
1.4.1 基础版/企业版/旗舰版 23
1.4.2 网页防篡改版 30
1.5 （可选）步骤五：切换主机安全版本 34
2 查看主机防护列表 38
3 主机风险总览 41
4 安全配置 46
5 主机管理 52
5.1 创建服务器组 52
5.2 部署策略 54
5.3 升级 Agent 57
6 风险预防 59
6.1 资产管理 59
6.2 漏洞管理 61
6.2.1 查看漏洞详情 61
6.2.2 漏洞修复与验证 65
6.3 基线检查 69
6.3.1 查看基线检查详情 69
6.3.2 基线检查风险项修复建议 70
7 入侵检测 73
7.1 告警事件概述 73
7.2 查看和处理入侵告警事件 79
7.3 管理文件隔离箱 91

7.4 配置告警白名单 93
7.5 配置登录白名单 96
8 高级防御 99
8.1 程序运行认证 99
8.1.1 查看白名单策略列表 99
8.1.2 应用白名单策略 102
8.1.3 查看和处理程序运行事件 106
8.2 文件完整性管理 108
8.2.1 添加管理文件 109
8.2.2 查看变更统计 111
8.3 勒索病毒防护 113
8.3.1 防勒索病毒概述 113
8.3.2 创建防护策略 114
8.3.3 管理防护策略 121
8.3.4 处理防护告警事件 128
9 安全运营 131
9.1 查看和创建策略组 131
9.2 修改策略内容 137
9.3 订阅主机安全报告 150
10 网页防篡改 156
10.1 添加防护目录 156
10.2 添加远端备份服务器 160
10.3 添加特权进程修改防护文件 162
10.4 定时开启网页防篡改 164
10.5 开启动态网页防篡改 165
10.6 查看网页防篡改报告 166
11 管理防护配额 168
11.1 查看配额 168
11.2 绑定主机 171
11.3 升级配额版本 173
11.4 解绑配额 175
12 （可选）管理企业项目 178
12.1 管理项目和企业 178
12.2 管理所有项目 179
13 审计 186
13.1 支持云审计的 HSS 操作列表 186
13.2 查看审计日志 190
14 权限管理 192
14.1 创建用户并授权使用 HSS 192
14.2 HSS 自定义策略 194

14.3 HSS 授权项说明 195

A 修订记录 201

1 开通主机防护

1.1 步骤一：购买防护配额

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

版本推荐说明

HSS提供基础版、企业版、旗舰版和网页防篡改版四种服务版本，各版本适用场景如**表1-1**所示，详细的服务版本功能差异，请参见**服务版本差异**。

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，企业主机安全将停止计费。

版权所有 © 华为技术有限公司

表 1-1 版本推荐说明

版本	计费模式	推荐场景
基础版	• 按需计费 自开启基础版按需防护开始30个自然日内可免费体验使用基础版按需版防护，每台主机均可享受一次免费体验机会。 在购买ECS时您可选择开启赠送的主机安全“基础版”，开启后可免费体验30天的主机安全“基础版”防护。 • 包年/包月 基础版包年/包月无试用期，若有使用需求您需要购买基础版包年/包月版本。	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。 用于测试、个人用户防护主机帐户安全。 基础版仅提供**基线检查**和**入侵检测**的部分功能，呈现一定云上资产安全风险总览。 **说明** • 包周期的基础版到期后，系统将会自动释放目标主机的防护状态，若需继续防护，您需要进行购买目标版本才可继续防护。 • 选择“包年/包月”时，若出现配额不足的提示，你需要进行购买，购买后开启防护即可。
企业版	• 按需计费 • 包年/包月	需要满足**等保合规**基本要求（例如：病毒木马查杀、漏洞一键修复、入侵检测）的主机。
旗舰版	包年/包月	对主机有高安全要求的用户（例如：应对护网行动、业务重要），**推荐使用旗舰版或者网页防篡改版**。 若预算有限，您可以将“旗舰版”或者“网页防篡改版”部署在关键或者高风险主机上，例如：对外暴露EIP的主机、保存关键资产的应用主机、以及数据库主机等。
网页防篡改版	包年/包月	有网站或者关键系统防篡改需求，以及有应用安全防护需求的主机，主要部署在网站或者应用的主机上，**推荐使用网页防篡改版**。 购买网页防篡改，即赠送旗舰版。

约束与限制

- 一个配额只能绑定一个主机，且只能绑定Agent在线的主机。
- **华为云主机：**HSS**不支持**跨区域使用，主机与HSS配额**不在同一区域**时，请退订配额，重新购买主机所在区域的配额。
- **非华为云主机：**仅“中国-香港”区域支持接入非华为云主机，请在该区域内购买防护配额，并使用区域内的安装包或安装命令为非华为云主机安装Agent。

购买防护配额（华为云主机）

步骤1 登录管理控制台。

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

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，设置配额的规格。

1. 选择计费类型，选择“包年/包月”。

   支持“包年/包月”和“按需”。

   说明

   - 选择“按需”时，不需要购买企业主机安全防护配额，直接在当前页面右下角单击“立即开通”，可跳转到云服务器列表页面。
   - 在云服务器列表的“操作列”中，单击“开启防护”，“计费模式”选择“按需计费”，“主机安全版本”选择“基础版”或者“企业版”，可开启“基础版”或者“企业版”防护。

2. 选择区域。

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

3. 选择版本。

   支持“基础版”、“企业版”、“旗舰版”和“网页防篡改版”。版本之间的差异请参见**服务版本差异**。

   - 若您购买的是基础版/企业版/旗舰版配额，请在“企业主机安全 > 主机管理 > 云服务器”页面开启防护。
   - 若您购买的网页防篡改版配额，请在“网页防篡改 > 防护列表”页面开启防护。

   图 1-1 版本选择

版本选择	产品特性	基础版 主机账户安全防护，适用测试、个人用户	企业版 病毒木马查杀，漏洞一键修复，等保必备服务	旗舰版 提供APT攻击检测，勒索病毒专杀等高级功能，应对护网行动等攻防对抗场景	网页防篡改版 网站、关键系统防篡改，政府、教育、国企必备安全服务
	资产管理		支持5类	支持6类	支持6类
	漏洞管理		✓	✓	✓
	基线检查	仅支持口令复杂度和经典弱口令检测	✓	✓	✓
	入侵检测	支持2类，账户暴力破解和异常登录	支持6大类	支持13大类	支持13大类
	高级防御			✓	✓
	策略管理		仅支持默认企业版策略组	✓自定义安全策略	✓自定义安全策略
	安全报告		✓	✓	✓
	安全配置	✓	✓	✓	✓
	网页防篡改				✓

   更多版本对比信息

4. 选择企业项目。

   从下拉列表中选择所在的企业项目。

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

   说明

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

版权所有 © 华为技术有限公司

5. 选择购买时长。

   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，当购买的企业主机安全到期时，如果帐号余额充足，系统将自动为购买的企业主机安全续费，续费周期与购买时长保持一致。

   若未勾选自动“自动续费”，在即将到期时，请手动续费。

6. 设置防护主机数量。

   购买成功后**不支持**增加配额，如需增加配额，请重新购买。无数量限制。

   图 1-2 防护主机数量（企业版）

说明

如果您已开通企业项目，您只需要为您所在的企业项目的主机购买防护配额。

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《企业主机安全免责声明》并勾选“我已阅读并同意《企业主机安全免责声明》”。

步骤7 单击“去支付”，进入“付款”页面，付款后，完成购买防护配额的操作。

----结束

购买防护配额（非华为云主机）

当前仅“中国-香港”区域可接入**非华为云**的主机，请在该区域内购买防护配额，并使用该区域提供的安装命令为非华为云主机安装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 > 企业主机安全”，进入企业主机安全页面。

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，设置配额的规格。

1. 选择计费类型，选择“包年/包月”。

   支持“包年/包月”和“按需”。

   说明

   - 选择“按需”时，不需要购买企业主机安全防护配额，直接在当前页面右下角单击“立即开通”，可跳转到云服务器列表页面。
   - 在云服务器列表的“操作列”中，单击“开启防护”，“计费模式”选择“按需计费”，“主机安全版本”选择“基础版”或者“企业版”，可开启“基础版”或者“企业版”防护。

2. 选择区域。

当前仅“中国-香港”区域可接入**非华为云**的主机，请在该区域内购买防护配额，并使用该区域提供的安装命令为非华为云主机安装Agent。

3. 选择版本。

   支持“基础版”、“企业版”、“旗舰版”和“网页防篡改版”。版本之间的差异请参见**服务版本差异**。

   - 若您购买的是基础版/企业版/旗舰版配额，请在“企业主机安全 > 主机管理 > 云服务器”页面开启防护。
   - 若您购买的网页防篡改版配额，请在“网页防篡改 > 防护列表”页面开启防护。

   图 1-3 版本选择

4. 选择企业项目。

   从下拉列表中选择所在的企业项目。

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

   说明

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

5. 选择购买时长。

   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，当购买的企业主机安全到期时，如果帐号余额充足，系统将自动为购买的企业主机安全续费，续费周期与购买时长保持一致。

   若未勾选自动“自动续费”，在即将到期时，请手动续费。

6. 设置防护主机数量。

   购买成功后**不支持**增加配额，如需增加配额，请重新购买。无数量限制。

   图 1-4 防护主机数量（企业版）

版权所有 © 华为技术有限公司

说明

如果您已开通企业项目，您只需要为您所在的企业项目的主机购买防护配额。

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《企业主机安全免责声明》并勾选“我已阅读并同意《企业主机安全免责声明》”。

----结束

生效条件

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

相关操作

退订

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。

切换主机安全版本

当开启防护的主机版本不满足您当前的防护需求时，您可以重新购买防护配额，切换主机版本。详细操作请参见（可选）步骤五：切换主机安全版本。

1.2 步骤二：安装 Agent

1.2.1 Linux 版本

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

说明

网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

安装成功后，需要等待5~10分钟左右Agent才会自动刷新Agent状态，建议重启服务器后再开启防护。

前提条件

- 待安装Agent所在的线下主机必须绑定弹性IP。
- 待安装Agent所在的线上主机需要与网段相通，要求您的服务器安全组出方向的设置允许访问**100.125.0.0/16**网段的**443**端口。
- 已在本地安装远程管理工具（如：“Xftp”、“SecureFX”、“WinSCP”）。
- 请关闭Selinux防火墙，防止Agent安装失败，安装成功后再打开。

约束与限制

- **华为云主机**

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

- **非华为云主机**
  - 当前仅“中国-香港”区域支持**非华为云主机**的安装方式，其他区域敬请期待。
  - 非**华为云**主机需要能通过**公网IP**访问华为云，才能接入HSS。安装Agent后，在防护列表中，您可以根据主机的IP地址查找该主机。

须知

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

系统影响

安装HSS Agent 对主机没有任何影响。HSS Agent用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。未安装Agent插件的主机将不受HSS保护，控制台页面也不会显示该主机资产的任何系统漏洞、基线风险、入侵事件和安全报告等数据。

默认安装路径

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

“/usr/local/hostguard/”

使用安装命令安装

登录待安装Agent的云主机，使用安装命令在线安装Agent。安装成功后，Agent不会立即生效，需要等待3~5分钟左右控制台才会刷新。

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 > 企业主机安全”，进入企业主机安全页面。

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

图 1-5 复制安装 Agent 的命令

步骤4 远程登录待安装Agent的主机。

- 华为云主机
  - 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**。
  - 若您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：“Xftp”、“SecureFX”、“WinSCP”）登录主机，并使用root帐号在主机中安装Agent。
- 非华为云主机

  请使用远程管理工具（例如：“Xftp”、“SecureFX”、“WinSCP”）登录主机，并使用root帐号在主机中安装Agent。

步骤5 粘贴复制的安装命令，并按“Enter”，在主机中安装Agent。

若界面回显信息与如下信息类似，则表示Agent安装成功。

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

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

若界面回显如下信息，则表示Agent服务运行正常。

```
Hostguard is running
```

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

使用安装包安装（仅华为云主机支持）

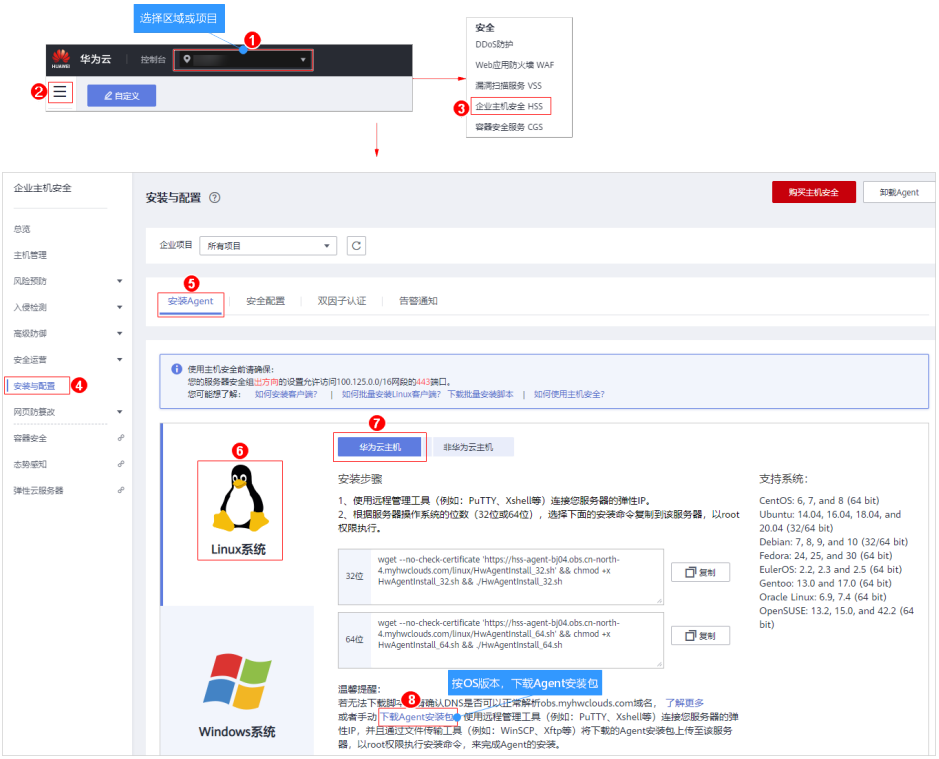
下载企业主机安全服务的Agent软件，上传至待安装Agent的云主机后，在云主机中使用安装命令安装Agent。

版权所有 © 华为技术有限公司

步骤1 登录管理控制台。

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

图 1-6 下载 Agent 安装包



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

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

步骤5 远程登录待安装Agent的主机。

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

步骤6 使用**cd** *安装包所在目录*命令，进入安装包所在目录。

步骤7 使用如下命令，在云主机中安装Agent。

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

  说明

  强制安装请执行命令：**rpm -ivh --force** *安装包名称*

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

  若界面回显信息与如下信息类似，则表示Agent安装成功。

```
Preparing...                ########################### [100%]
1:hostguard                 ########################### [100%]
```


版权所有 © 华为技术有限公司

```
Hostguard is running.
Hostguard installed.
```

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

若界面回显如下信息，则表示Agent服务运行正常。

```
Hostguard is running
```

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

相关操作

- 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?**

1.2.2 Windows 版本

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

说明

网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

安装成功后，需要等待5~10分钟左右Agent才会自动刷新Agent状态，建议重启服务器后再开启防护。

前提条件

- 待安装Agent所在的线下主机必须绑定弹性IP。
- 待安装Agent所在的线上主机需要与网段相通，要求您的服务器安全组出方向的设置允许访问**100.125.0.0/16**网段的**443**端口。
- 已在本地安装远程管理工具（如：“pcAnywhere”、“UltraVNC”）。

约束与限制

- **华为云主机**

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

- **非华为云主机**
  - 当前仅“中国-香港”区域支持**非华为云主机**的安装方式，其他区域敬请期待。
  - 非**华为云**主机需要能通过**公网IP**访问华为云，才能接入HSS。安装Agent后，在防护列表中，您可以根据主机的IP地址查找该主机。

须知

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

系统影响

安装HSS Agent 对主机没有任何影响。HSS Agent用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。未安装Agent插件的主机将不受HSS保护，控制台页面也不会显示该主机资产的任何系统漏洞、基线风险、入侵事件和安全报告等数据。

默认安装路径

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

“C:\Program Files (x86)\HostGuard”

操作步骤

有两种安装方式，以下步骤演示方式二。

- 方式一：复制Agent下载链接，远程登录服务器通过IE浏览器访问该链接，下载并解压Agent安装包。以管理员权限运行Agent安装程序。
- 方式二：下载企业主机安全服务的Agent，上传至待安装Agent的云主机后，在云主机中安装Agent。

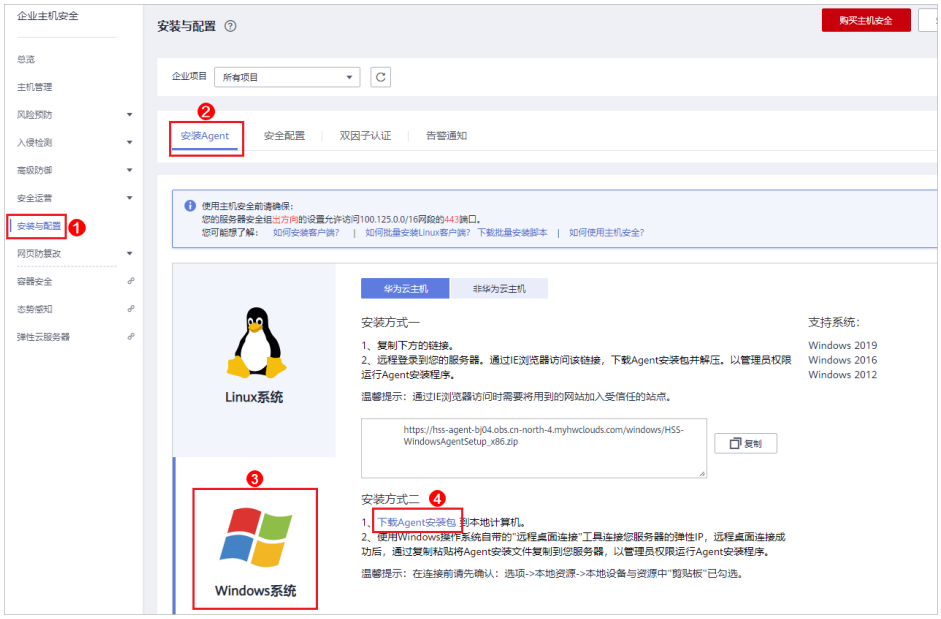
步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，选择“安装与配置”，进入“安装Agent”界面，下载Agent安装包。

版权所有 © 华为技术有限公司

图 1-7 安装 Windows Agent



步骤4 远程登录待安装Agent的主机。

- 华为云主机
  - 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**。
  - 若您的主机已经绑定了弹性IP，您也可以使用Windows系统的“远程桌面连接”工具，或第三方远程管理工具（例如：“pcAnywhere”、“UltraVNC”）登录主机，并使用管理员帐号在主机中安装Agent。
- 非华为云主机

  请使用Windows系统的“远程桌面连接”工具，或第三方远程管理工具（如：“pcAnywhere”、“UltraVNC”）登录主机，并使用管理员帐号在主机中安装Agent。

步骤5 将Agent安装包上传到待安装Agent的主机中。

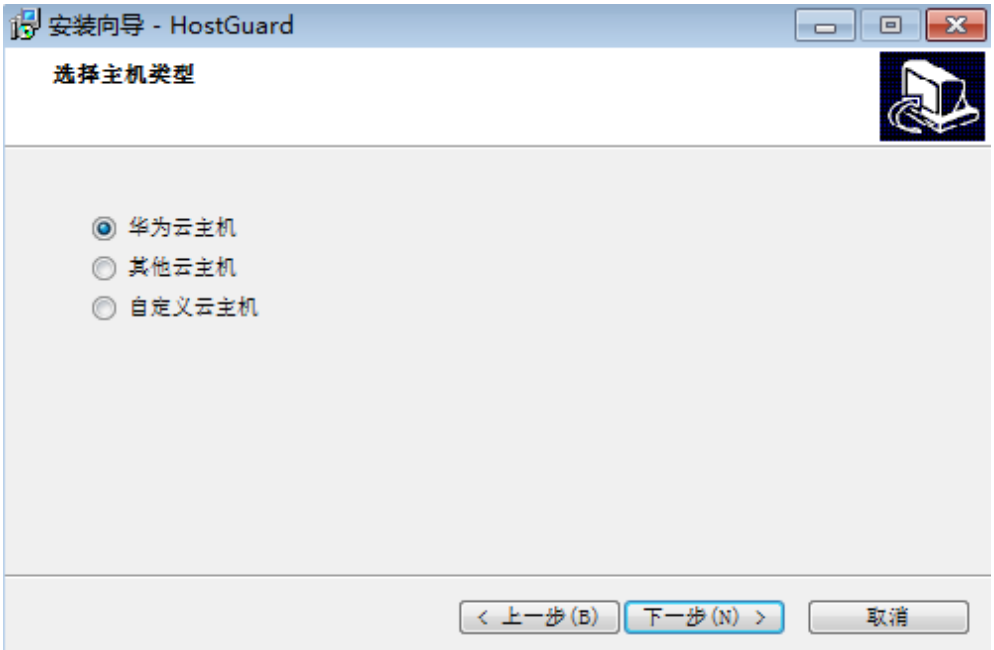
步骤6 使用管理员权限运行Agent安装程序。

安装Agent时，在主机类型界面，选择主机类型。

- 华为云主机：请选择“华为云主机”。

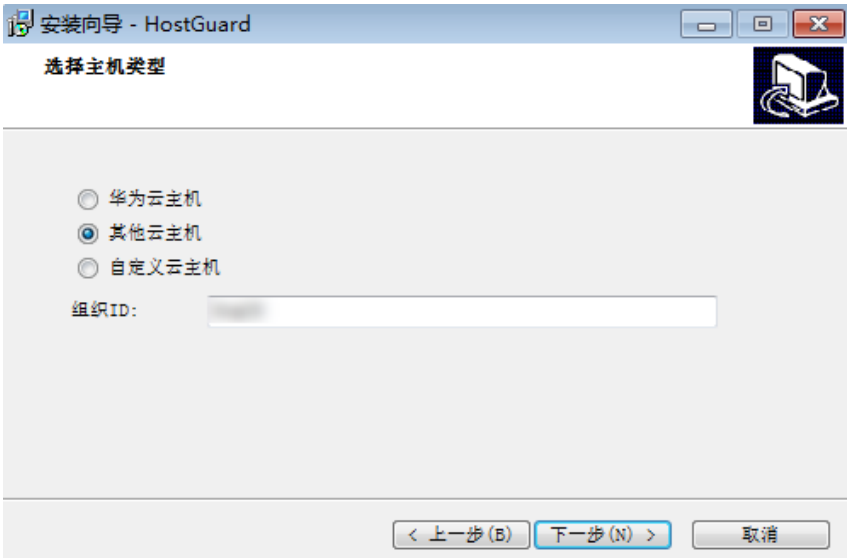
版权所有 © 华为技术有限公司

图 1-8 选择主机类型（华为云主机）



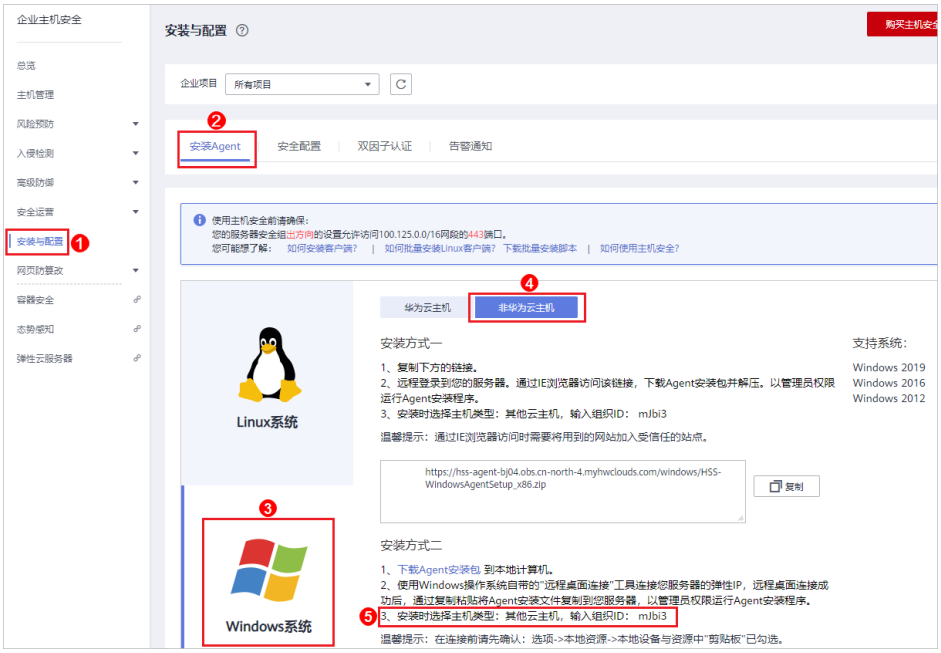
- 非华为云主机：请选择“其他云主机”。请从安装Agent界面复制组织ID，如图1-10所示。

图 1-9 选择主机类型（非华为云主机）



版权所有 © 华为技术有限公司

图 1-10 获取组织 ID（非华为云主机）

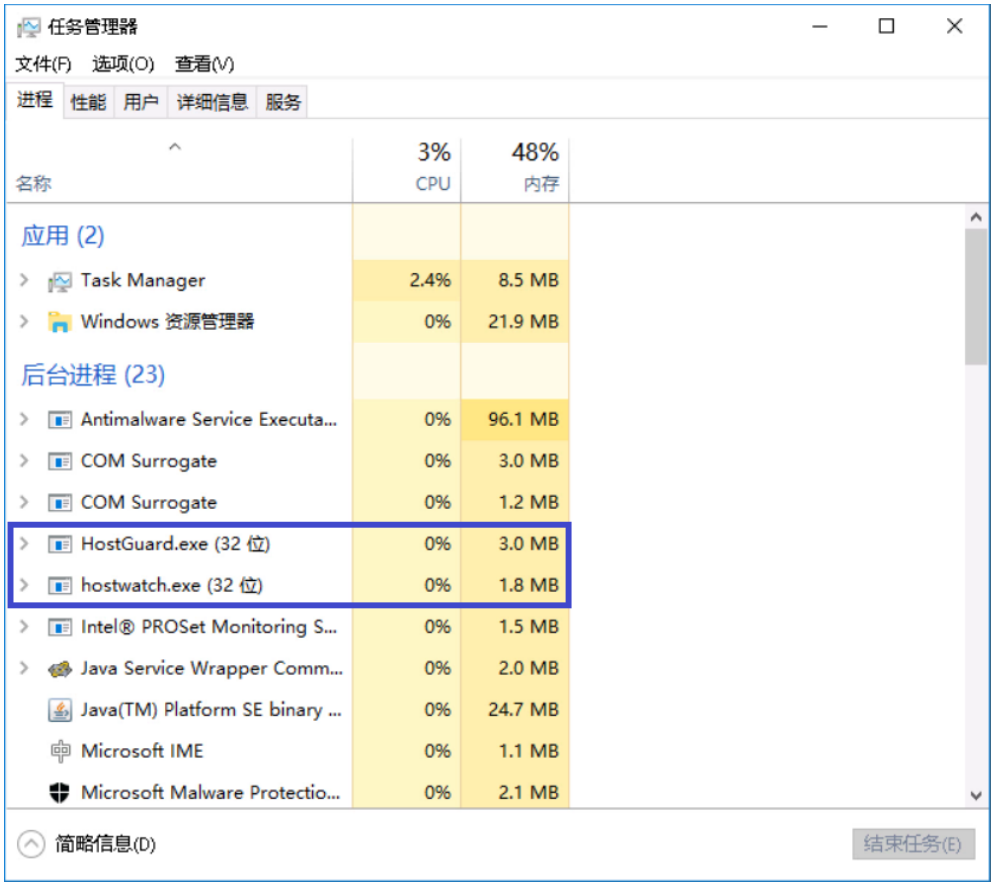


步骤7 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”，如图1-11所示。

若进程不存在，则表示Agent安装失败，请尝试重新安装Agent。

版权所有 © 华为技术有限公司

图 1-11 查看 Agent 运行状态



----结束

相关操作

- 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 （可选）步骤三：设置告警通知

1.3.1 基础版/企业版/旗舰版

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

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

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

- 告警通知设置仅在当前区域生效，若需要接收其他区域的告警通知，请切换到对应区域后进行设置。

- 告警通知信息可能会被误拦截，若您未收到相关告警信息，请在信息拦截中查看。
- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。

开启告警通知的必要性

告警通知开启后，企业主机安全服务一旦检测到有告警（包括但不限于对可疑帐号、未知端口、漏洞、暴力破解、病毒、恶意程序、异常shell、网页篡改、勒索入侵的告警），HSS在第一时间会将告警信息通过短信发送至您配置的移动设备，帮助您随时随地识别告警，及时对服务器采取安全加固、漏洞修复、手动查杀等防护措施，增强服务器防护能力。

前提条件

在设置告警通知前。

- 如果选择“消息中心”，建议您在“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”，新增或修改消息接收人。
- 如果选择“消息主题”，建议您先以管理员身份在“消息通知服务”中创建“消息主题”，详细操作请参见**如何发布主题消息**。

说明

告警通知方式分为“消息中心”和“消息主题”。

消息中心：使用消息中心和其它安全服务共同使用“安全事件通知”的信息接收人。

消息主题：为HSS单独创建的主题，设置告警通知接收人。

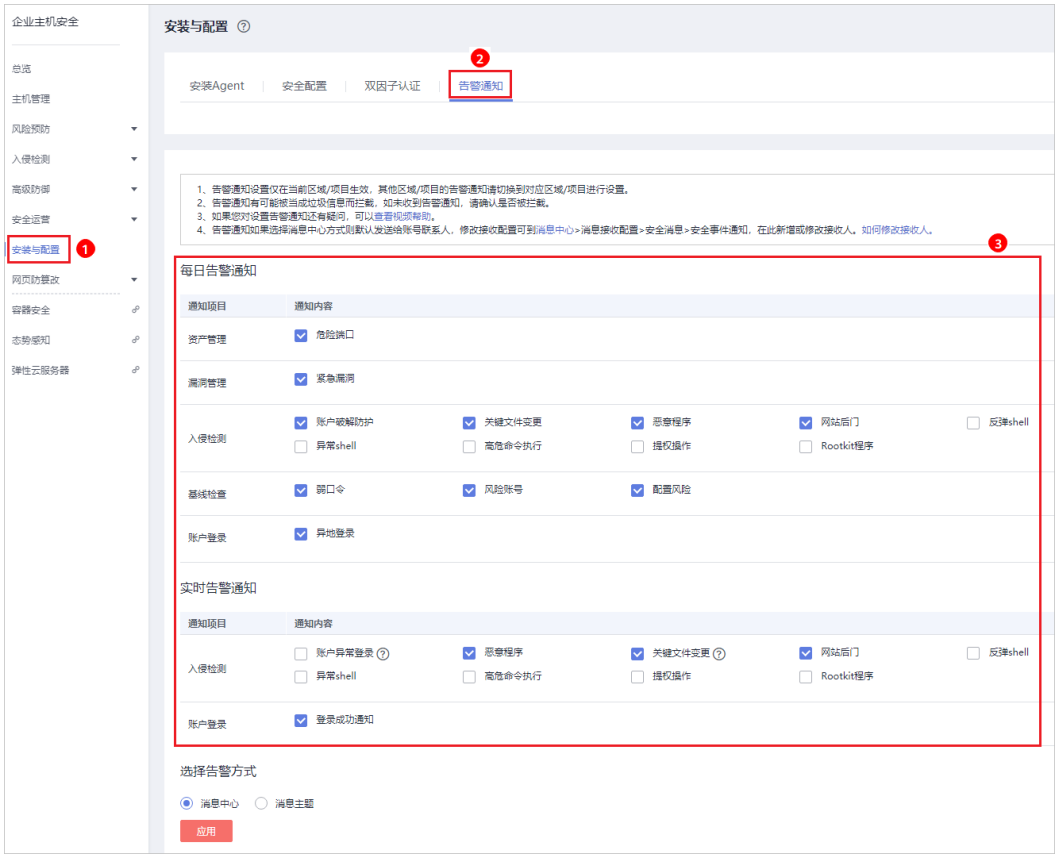
开启基础版/企业版/旗舰版的告警通知

步骤1 **登录管理控制台**。

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

步骤3 选择“告警通知”页签，进入“告警通知”页面，如**图1-12**所示。

图 1-12 基础版/企业版/旗舰版



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

表 1-2 选择通知项

通知项	说明	选择建议
每日告警通知	每日凌晨，企业主机安全服务将主动检测主机系统中的帐号、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。	• 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”。

版权所有 © 华为技术有限公司

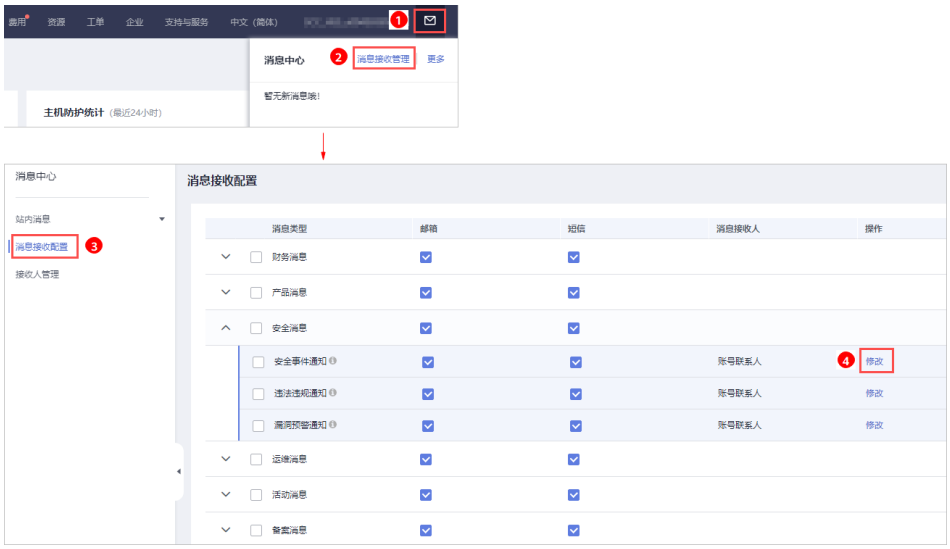
通知项	说明	选择建议
实时告警通知	当攻击者入侵主机时，企业主机安全服务将按照选定的“消息中心”或者“消息通知服务主题”为您告警。	• 建议您接收实时告警通知中所有的内容并及时查看。企业安全服务实时监测主机中的安全情况，能监测到攻击者入侵主机的行为，接收实时告警通知能快速处理攻击者入侵主机的行为。 • 由于实时告警中通知项的内容紧急度较高，如果您使用的“消息通知服务”，接收告警通知，建议您选择“订阅终端”配置为“短信”的“消息通知服务主题”。

步骤5 选择“消息中心”或者“消息主题”告警通知方式，接收告警通知。

- 选择“消息中心”。

  告警通知默认发送给帐号联系人，修改接收配置可到“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”，新增或修改接收人。

  图 1-13 新增或修改接收人



- 选择“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。

版权所有 © 华为技术有限公司

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6 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

通知项	通知内容	通知内容说明
每日告警通知 每日凌晨检测主机中的风险，汇总并统计检测结果后，将检测结果于每日上午10:00发送给你添加的手机号或者邮箱。		
资产管理	危险端口	检测开放了的危险端口或者不必要的端口，通知用户及时排查这些端口是否用于正常业务。
漏洞管理	紧急漏洞	检测系统中的紧急漏洞，通知用户尽快修复，防止攻击者利用该漏洞会对主机造成较大的破坏。
入侵检测	帐户破解防护	检测SSH、RDP、FTP、SQL Server、MySQL等帐户遭受的口令破解攻击。 ● 如果30秒内，帐户暴力破解次数（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，防止主机因帐户破解被入侵。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。 ● 根据帐户暴力破解告警详情，如“攻击源IP”、“攻击类型”和“拦截次数”，您能够快速识别出该源IP是否为可信IP，如果为可信IP，您可以通过手动解除拦截的方式，解除拦截的可信IP。
	关键文件变更	对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。
	恶意程序	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。
	网站后门	检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。

通知项	通知内容	通知内容说明
	高危命令执行	HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	提权操作	HSS检测当前系统的“进程提权”和“文件提权”操作。
	Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。
基线检查	弱口令	检测MySQL、FTP及系统帐号的弱口令。
	风险帐号	检测系统中的可疑帐号、主机中无用的帐号，防止未授权的访问权限和使用操作。
	配置风险	检测系统中的关键应用，如果采用不安全配置，有可能被黑客利用作为入侵主机系统的手段。
帐户登录	异地登录	检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施。 若在非常用登录地登录，则触发安全事件告警。
实时告警通知 事件发生时，及时发送告警通知。		
入侵检测	帐户异常登录	检测“异地登录”和“帐户暴力破解成功”等异常登录。若发生异常登录，则说明您的主机可能被黑客入侵成功。
	恶意程序	通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。
	关键文件变更	对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。
	网站后门	检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。
	反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。
	异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。
	高危命令执行	HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。
	提权操作	HSS检测当前系统的“进程提权”和“文件提权”操作。
	Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。

通知项	通知内容	通知内容说明
帐户登录	登录成功通知	如果在“实时告警通知”项目中勾选了“登录成功通知”选项，则任何帐户登录成功的事件都会向您实时发送告警信息。 如果您所有主机上的帐户都由个别管理员负责管理，通过该功能可以对系统帐户进行严格的监控。 如果系统帐户由多人管理，或者不同主机由不同管理员负责管理，那么运维人员可能会因为频繁收到不相关的告警而对运维工作造成困扰，此时建议您登录企业主机安全服务控制台关闭该告警项。 **说明** 登录成功并不代表发生了攻击，需要您确认登录IP是否是已知的合法IP。

1.3.2 网页防篡改版

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

前提条件

在设置告警通知前。

- 如果选择“消息中心”，建议您在“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”，新增或修改消息接收人。
- 如果选择“消息主题”，建议您先以管理员身份在“消息通知服务”中创建“消息主题”，详细操作请参见如何发布主题消息。

说明

告警通知方式分为“消息中心”和“消息主题”。

消息中心：使用消息中心和其它安全服务共同使用“安全事件通知”的信息接收人。

消息主题：为HSS单独创建的主题，设置告警通知接收人。

开启告警通知的必要性

告警通知开启后，企业主机安全服务一旦检测到有告警（包括但不限于对可疑帐号、未知端口、漏洞、暴力破解、病毒、恶意程序、异常shell、网页篡改、勒索入侵的告警），HSS在第一时间会将告警信息通过短信发送至您配置的移动设备，帮助您随时随地识别告警，及时对服务器采取安全加固、漏洞修复、手动查杀等防护措施，增强服务器防护能力。

开启网页防篡改告警通知

步骤1 登录管理控制台。

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

步骤3 进入“告警通知”页面，选择告警通知时间，如图1-14所示。

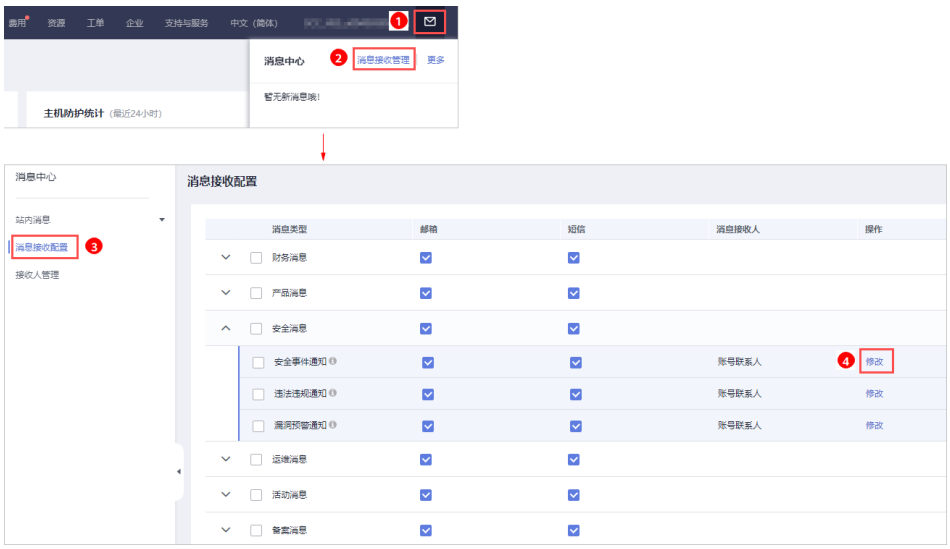
图 1-14 告警通知设置

步骤4 选择“消息中心”或者“消息主题”告警通知方式，接收告警通知。

- 选择“消息中心”。

  告警通知默认发送给帐号联系人，修改接收配置可到“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”，新增或修改接收人。

  图 1-15 新增或修改接收人



- 选择“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：

版权所有 © 华为技术有限公司

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

1.4 步骤四：开启主机防护

1.4.1 基础版/企业版/旗舰版

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

若您购买的是网页防篡改版，请在“网页防篡改 > 防护列表”页面开启防护，具体请参见网页防篡改版。

说明

- 基础版无数量限制，只支持部分功能的检测能力，不支持防护能力，不支持等保认证。

  若需对云服务器进行防护或做等保认证，您需购买企业版及以上（包含企业版、旗舰版、网页防篡改版）版本。
- 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“网页防篡改 > 防护列表”页面开启防护，当开启网页防篡改防护时会自动开启旗舰版防护。

检测周期

主机防护每日凌晨会进行全量检测。

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

前提条件

- “企业主机安全 > 主机管理”页面“云服务器”中“Agent状态”为“在线”。
- 若开启包周期防护，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帐户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警。

- Windows操作系统
  - 开启主机防护时，需要授权开启Windows防火墙，且使用企业主机安全服务期间请勿关闭Windows防火墙。若关闭Windows防火墙，HSS无法拦截帐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不能拦截帐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“安全与合规 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航栏中，选择“主机管理”，进入“云服务器”界面，如图1-16所示。

图 1-16 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“开启防护”。

您可以根据自己的实际场景选择“包年/包月”或者“按需计费”，开启主机防护。

- 包年/包月

  在“开启防护”对话框中，“计费模式”选择“包年/包月”，选择“主机安全版本”、分配“防护配额”，阅读并确认“《企业主机安全免责声明》”如图1-17所示。

版权所有 © 华为技术有限公司

图 1-17 开启包周期主机防护

“防护配额”分配方式：

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

- 按需计费

  在“开启防护”对话框中，“计费模式”选择“按需计费”，选择“主机安全版本”，阅读并确认“《企业主机安全免责声明》”，如图1-18所示。

版权所有 © 华为技术有限公司

图 1-18 开启按需计费主机防护

说明

按需计费：只支持企业版和基础版。基础版可免费体验30天，基础版的包年/包月模式需购买才能使用；企业版和旗舰版出现配额不足则需要**购买主机安全配额**；

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

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

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将根据您购买的服务版本，自动对您的主机执行服务版本对应的安全检测，如**图1-19**所示。

版本之间的差异请参见**服务版本差异**。

版权所有 © 华为技术有限公司

图 1-19 自动执行的安全检测

----结束

查看检测详情

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

在防护列表的“操作”列中单击“查看详情”，统一查看指定主机的检测结果。

版权所有 © 华为技术有限公司

图 1-20 查看详情

在详情界面，能快速查看主机中已被检测出的各项信息和风险。

图 1-21 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，如图1-22所示。

版本之间的功能差异请参见服务版本差异。

版权所有 © 华为技术有限公司

图 1-22 手动配置的检测项

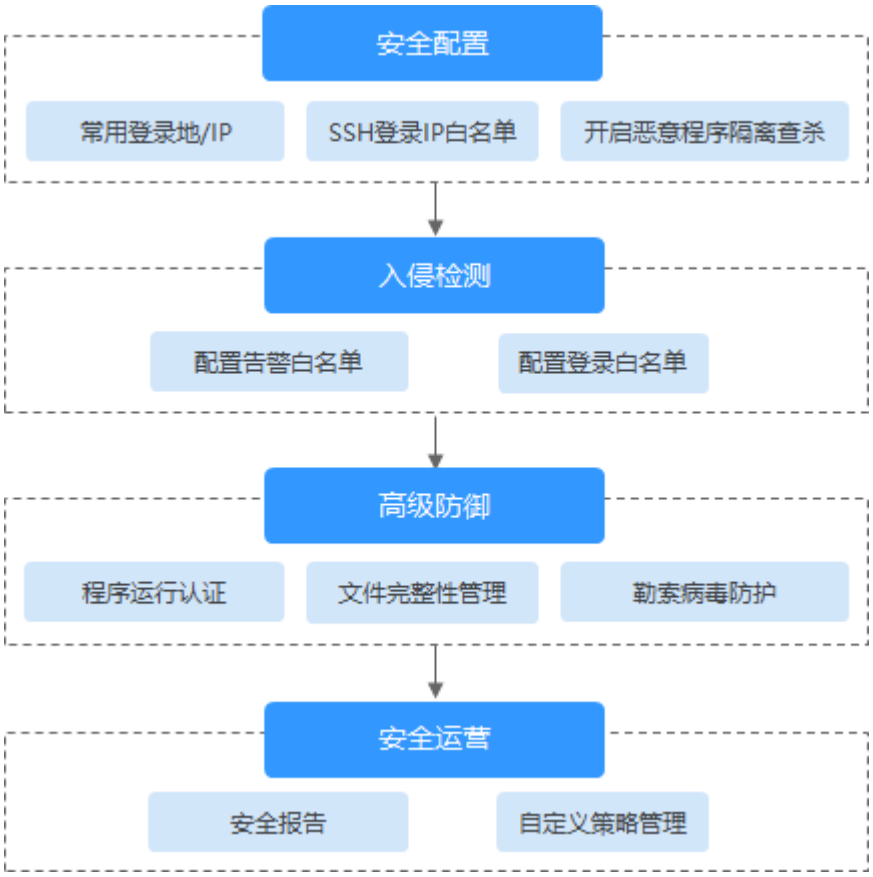


表 1-3 手动配置检测项

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

相关操作

关闭主机防护

版权所有 © 华为技术有限公司

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

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

须知

- 关闭主机防护前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。
- 关闭主机防护后，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。

解绑配额

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

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

说明

当开启了主机防护的云主机被退订，该云主机绑定的配额不会立刻自动释放。您可以通过解绑配额的方式，解除绑定的配额。或者等待Agent离线30天后，自动释放配额。

1.4.2 网页防篡改版

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

开启网页防篡改防护时会同步开启主机安全的旗舰版防护。

网页防篡改原理

表 1-4 网页防篡改原理

防护类型	原理说明
静态网页防护	1. 锁定本地文件目录 驱动级锁定Web文件目录下的文件，禁止攻击者修改，网站管理员可通过特权进程进行更新网站内容。 2. 主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。 3. 远端备份恢复 若本地主机上的文件目录和备份目录失效，还可通过远端备份服务恢复被篡改的网页。

防护类型	原理说明
动态网页防护	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。

约束条件

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

前提条件

- 在“网页防篡改 > 防护列表”页面中“Agent状态”为“在线”、“防护状态”为“关闭”。
- 在“企业主机安全 > 主机管理”页面“云服务器”列表中“Agent状态”为“在线”、“防护状态”为“关闭”。
- 已在所选区域内购买了充足可用的“网页防篡改版”配额。

设置防护目录

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

- 保护指定目录
  您最多可在主机中添加50个防护目录，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“安全与合规 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“网页防篡改”界面，单击“开启防护”。

图 1-23 进入“网页防篡改”界面

版权所有 © 华为技术有限公司

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 在“开启防护”对话框中，为指定的主机分配“防护配额”，单击“确定”，开启防护，如图1-24所示。

说明

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

若您未开启动态网页防篡改，后续您可以在“安装与配置”界面手动开启。

图 1-24 开启网页防篡改

“防护配额”分配方式：

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

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

“网页防篡改版”开启后，旗舰版防护会同步开启。

- 选择“网页防篡改 > 防护列表”，目标主机所在行的“防护状态”为“开启”，且“版本/到期时间”为“网页防篡改版”，则表示网页防篡改版已开启。

版权所有 © 华为技术有限公司

- 选择“企业主机安全 > 主机管理 > 云服务器”，目标主机所在行的“防护状态”为“开启”，且“版本/到期时间”为“旗舰版（网页防篡改赠送）”，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“网页防篡改 > 防护列表 > 配额详情”页面，单击“绑定主机”，为主机绑定防护配额，HSS自动为主机开启网页防篡改防护。
- 一个配额只能绑定一个主机，且只能绑定Agent在线的主机。
- 开启网页防篡改后如果需要更新网站请先临时关闭网页防篡改，完成更新后再开启。否则会造成网站更新失败。
- 关闭网页防篡改期间，您的网站不受保护，更新网页后，请及时开启网页防篡改。

相关操作

关闭网页防篡改

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

关闭网页防篡改后，HSS会自动释放防护配额。您可将空闲的配额分配给其他主机继续使用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，若您的文档不慎被删除，请在主机本地备份或远端主机的备份路径中查找。
- 当用户关闭网页防篡改时会同步关闭旗舰版防护。

解绑配额

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

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

说明

当开启了网页防篡改的云主机被退订，该云主机绑定的配额不会自动释放。您可以通过解绑配额的方式，解除绑定的配额。或者等待Agent离线30天后，自动释放配额。

1.5 （可选）步骤五：切换主机安全版本

您可以根据需要将企业主机安全服务的版本切换为“基础版（按需计费）”、“基础版（包年/包月）”、“企业版（按需计费）”、“企业版（包年/包月）”或者“旗舰版”。

说明

- 主机版本切换不支持批量切换。
- 如果您购买ECS时，勾选了“开通主机安全”，并选择主机安全的“基础版”或者“企业版”，HSS会自动为该ECS安装Agent，并开启“基础版（按需计费）”或者“企业版（按需计费）”防护。此时，若您需要使用购买的包周期配额时，请通过切换版本的方式，开启包周期企业主机安全防护。

注意事项

- 按需变更为包周期。

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

  包周期转按需，需要用户在云服务器列表页面，勾选目标主机，单击“开启防护”，选择按需防护，按需的资费模式才会生效。
- 若企业主机安全服务的版本由高版本版切换为低版本后，主机遭受攻击的可能性将升高。
- 仅支持将主机安全防护的版本切换为“基础版”、“企业版”或者“旗舰版”，如需使用“网页防篡改版”，请先购买“网页防篡改版”的配额，再开启网页防篡改防护。

切换版本前准备

- “企业主机安全 > 主机管理”页面“云服务器”中目标主机的“Agent状态”为“在线”，且已开启主机防护。
- 切换为包周期配额版本时，需重新为主机指定相应的配额，变更版本前请先购买数量充足的配额。
- 切换为低版本前，请对主机执行相应的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。

切换版本

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航栏中，选择“主机管理”，进入“云服务器”界面，如图1-25所示。

图 1-25 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 选择需要切换版本的主机，单击“切换版本”。

说明

- “基础版（按需计费）”与“基础版（包年/包月）”之间和“企业版（按需计费）”和“企业版（包年/包月）”之间不能通过“切换版本”功能直接切换主机安全版本，若需切换，请关闭原版本后重新选择待切换的版本。
- 您也可以通过在云服务器列表页面，勾选目标主机，在列表上方单击“开启防护”，进行直接切换主机安全版本。

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

- 包年/包月

  在“切换版本”对话框中，“计费模式”选择“包年/包月”，选择“主机安全版本”、分配“防护配额”，阅读并确认“《企业主机安全免责声明》”如图1-26所示。

版权所有 © 华为技术有限公司

图 1-26 切换为包周期主机安全版本

“防护配额”分配方式：

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

- 按需计费

  在“切换版本”对话框中，“计费模式”选择“按需计费”，选择“主机安全版本”，阅读并确认“《企业主机安全免责声明》”，如图1-27所示。

版权所有 © 华为技术有限公司

图 1-27 切换为按需计费主机安全版本

步骤5 单击“确定”，切换版本。切换主机安全版本后，请在云服务器列表页面查看主机的“版本/到期时间”。

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

----结束

切换版本后操作

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

版权所有 © 华为技术有限公司

2 查看主机防护列表

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

- 若未找到您的主机，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。

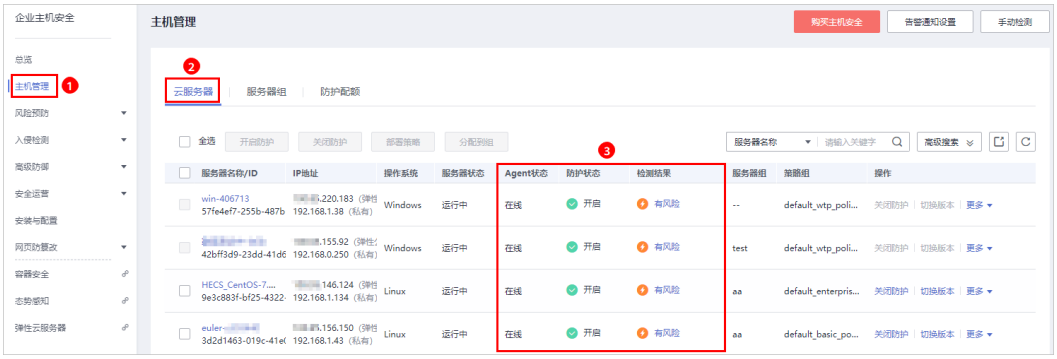
查看基础版/企业版/旗舰版防护列表

步骤1 登录管理控制台。

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

步骤3 在“云服务器”界面，查看服务器的防护状态。

图 2-1 云服务器列表



版权所有 © 华为技术有限公司

说明

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

表 2-1 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。单击“离线”，您可以查看Agent不在线的华为云主机列表，并查看“离线原因”。
防护状态	• 开启：HSS为该服务器提供全面的主机安全防护。 • 关闭：单击“关闭防护”可以暂停HSS对服务器的防护，降低该服务器的资源消耗。
检测结果	• 有风险：主机存在风险。 • 无风险：主机暂未发现风险。 • 未检测：主机未开启防护。

----结束

查看网页防篡改防护列表

步骤1 登录管理控制台。

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

步骤3 在“网页防篡改 > 防护列表”界面，查看服务器的防护状态。

版权所有 © 华为技术有限公司

图 2-2 服务器列表

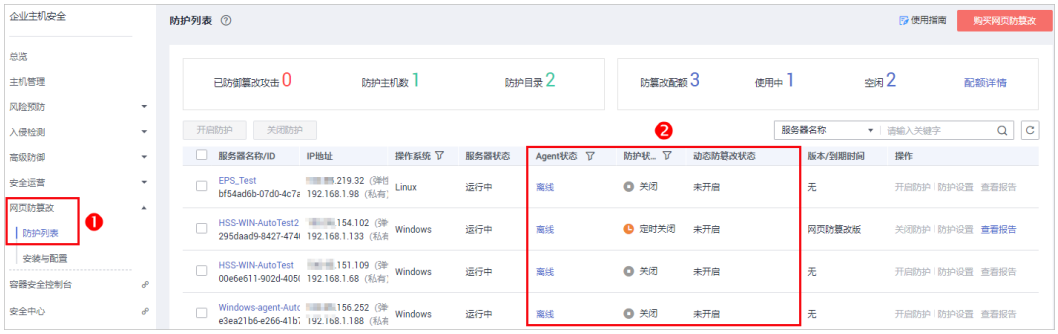


表 2-2 状态说明

参数名称	说明
Agent状态	• 未安装：未安装Agent，或Agent已安装但未成功启动。 单击“未安装”，您可以根据弹出框给出的安装提示，进行Agent的安装，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。 单击“离线”，您可以查看Agent不在线的华为云主机列表，并在该页面查看“离线原因”。
防护状态	静态网页防篡改的状态。 • 开启：HSS为该服务器提供静态网页防篡改防护。 • 定时关闭：在“防护设置 > 定时开关设置”可自定义防护时间段，详细操作请参见**定时开关设置**。 • 关闭：单击“关闭防护”可以暂停静态网页防篡改防护，降低该服务器的资源消耗。
动态防篡改状态	动态网页防篡改的状态。 • 已开启：在“防护设置 > 动态网页防篡改”可开启动态网页防篡改，详细操作请参见**开启动态网页防篡改**。 • 已开启未生效：动态网页防篡改开启后，请重启Tomcat使其生效。 • 未开启：未开启动态网页防篡改。

----结束

相关链接

- **开启基础版/企业版/旗舰版防护**
- **开启网页防篡改版防护**

版权所有 © 华为技术有限公司

3 主机风险总览

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

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，查看您所在企业项目的主机风险总览；或者选择“所有项目”，查看当前区域下所有项目的主机风险总览。

已开启防护的主机风险统计（最近 24 小时）

图 3-1 已开启防护的主机风险统计（最近 24 小时）

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

单击数字，可查看各类风险详情。

版权所有 © 华为技术有限公司

主机防护统计（最近 24 小时）

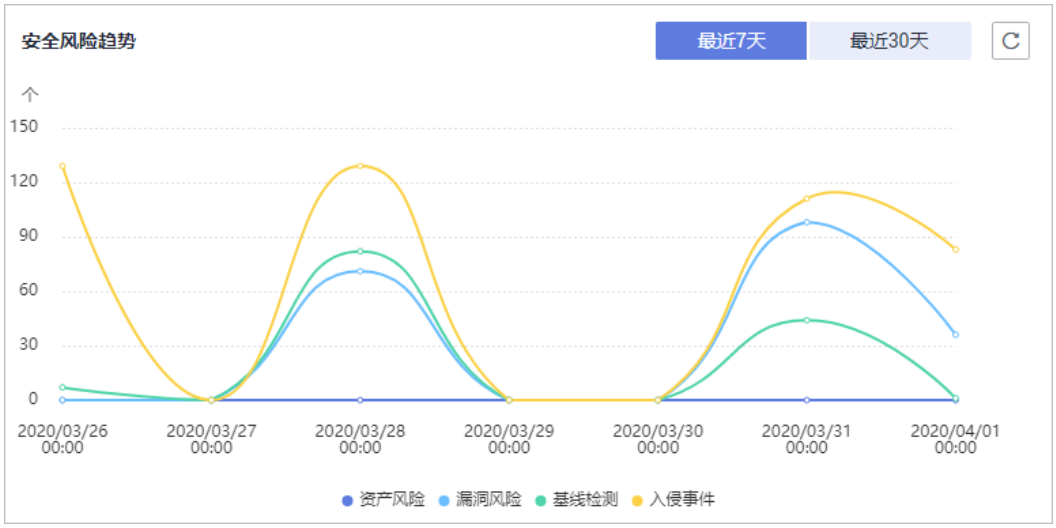
图 3-2 主机防护状态

显示用户开启基础版防护、企业版防护、旗舰版防护和未开启防护的服务器的数量。

单击“全部开启”，可跳转到云服务器列表，对未开启防护的服务器开启防护。

安全风险趋势

图 3-3 安全风险趋势



可显示最近7天、近30天的安全风险趋势。

表 3-1 安全风险趋势说明

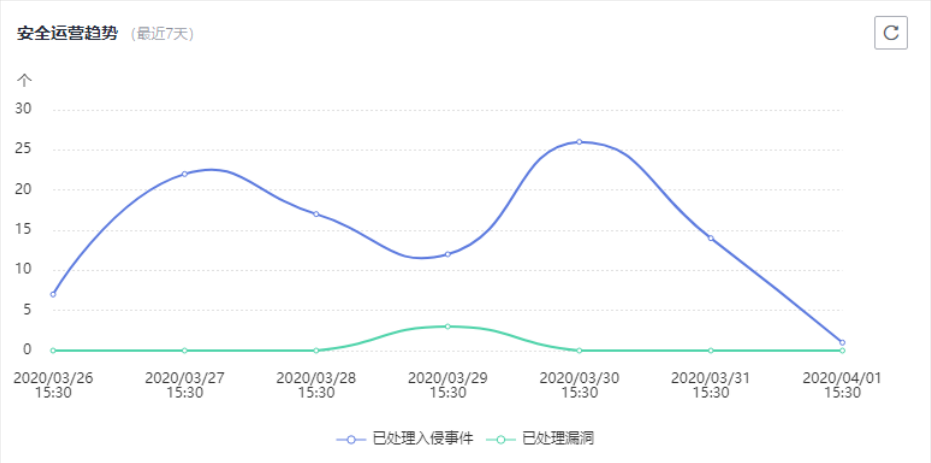
风险分类	风险事件
资产风险	• 帐号信息 • 开放端口 • 进程信息 • Web目录 • 软件信息 • 自启动

版权所有 © 华为技术有限公司

风险分类	风险事件
漏洞风险	• Linux漏洞 • Windows漏洞 • Web-CMS漏洞
基线检测	• 口令复杂度策略检测 • 经典弱口令检测 • 配置检测
入侵事件	• 帐户破解源IP • 异常Shell • 恶意程序 • 高危命令执行 • 进程异常行为 • 自启动检测 • 帐户异常登录 • 提权操作 • 关键文件变更 • 高危恶意程序 • Rootkit程序 • 网站后门 • 风险帐户 • 反弹Shell

安全运营趋势（最近 7 天）

图 3-4 安全运营趋势

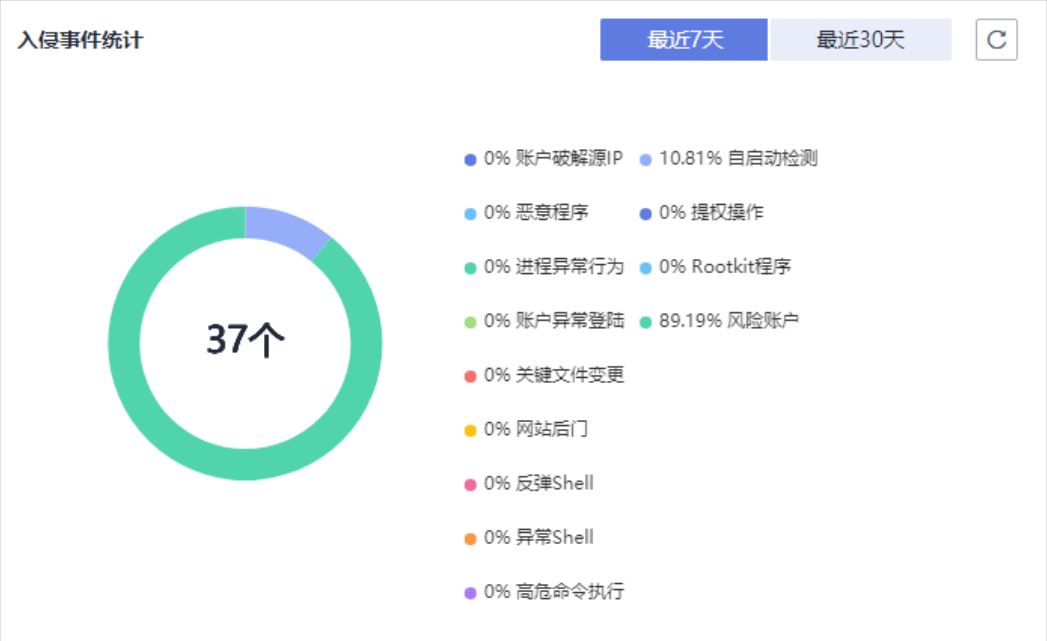


显示最近7天的已处理入侵事件和已处理漏洞。

版权所有 © 华为技术有限公司

入侵事件统计

图 3-5 入侵事件统计



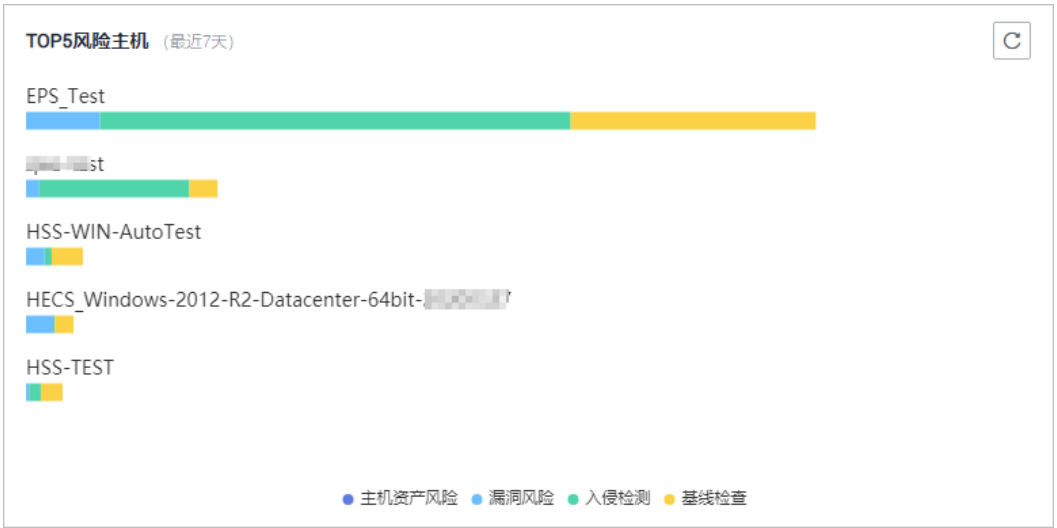
显示最近7天或者最近30天的入侵事件总个数，以及各类入侵事件分类占比。

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

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

TOP5 风险主机（最近 7 天）

图 3-6 TOP5 风险的云服务器（最近 7 天）



版权所有 © 华为技术有限公司

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

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

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

实时入侵事件

图 3-7 实时入侵事件

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

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

版权所有 © 华为技术有限公司

4 安全配置

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

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 > 企业主机安全”，进入企业主机安全页面。

----结束

配置常用登录地

配置常用登录地后，企业主机安全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 在“常用登录地”页面，单击“添加常用地登录”。

图 4-1 添加常用登录地

步骤2 在弹出的对话框中选择“常用登录地”和“可选云服务器”即可完成配置。

----结束

版权所有 © 华为技术有限公司

配置常用登录 IP

配置常用登录IP，企业主机安全服务将对非常用IP登录主机的行为进行告警。

步骤1 在“常用登录IP”页面，单击“添加常用登录IP”。

图 4-2 常用登录 IP

步骤2 在弹出的对话框中输入“常用登录IP”，在“可选云服务器”列表中选择云服务器。

说明

“常用登录IP”必须填写公网IP或者IP段。如果设置的非公网IP地址，您将无法SSH远程登录您的服务器。

----结束

配置 SSH 登录 IP 白名单

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

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

- 启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中，否则您将无法SSH远程登录您的服务器。

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

说明

使用鲲鹏计算EulerOS（EulerOS with ARM）和Centos 8.0及以上版本的主机，SSH登录IP白名单功能对其不生效。

步骤1 在“SSH登录IP白名单”页面，单击“添加白名单IP”。

版权所有 © 华为技术有限公司

图 4-3 SSH 登录 IP 白名单

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

说明

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

----结束

开启恶意程序隔离查杀

开启恶意程序隔离查杀后，HSS对识别出的后门、木马、蠕虫等恶意程序，提供自动隔离查杀功能，帮助用户自动识别处理系统存在的安全风险，更多恶意程序相关内容详情请参见**功能特性**章节中的“入侵检测 > 恶意程序”内容。

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

图 4-4 恶意程序隔离查杀

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

版权所有 © 华为技术有限公司

须知

- 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若隔离查杀有误报，您可以执行取消隔离/忽略操作。
- 在“恶意程序隔离查杀”界面，如果不开启“恶意程序隔离查杀”功能，当HSS检测到恶意程序时，将会触发告警。

  您可以在“入侵检测”的“事件管理”中，查看“恶意程序（云查杀）”中的告警信息，并对恶意程序进行隔离查杀。

开启双因子认证

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

前提条件

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

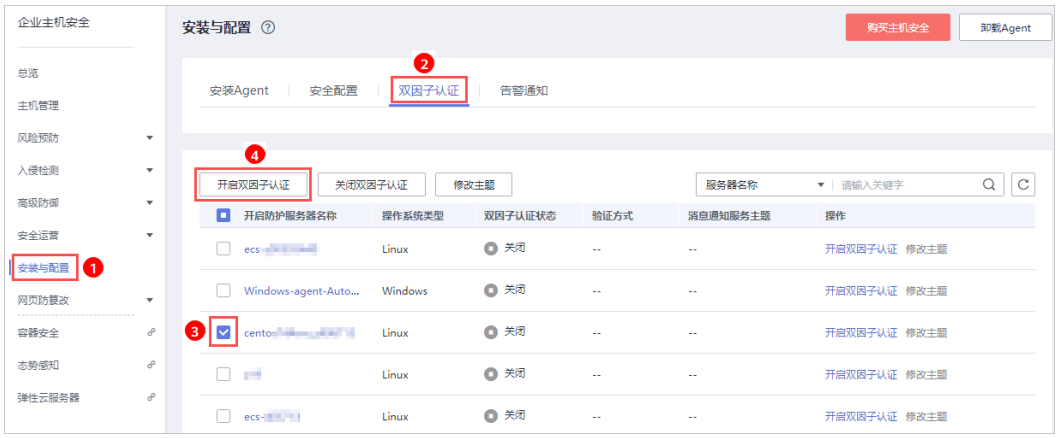
约束与限制

- 开启双因子认证后，不能通过已安装图形化界面的Linux系统登录主机。
- 在Linux主机上，开启双因子认证后，不能通过云堡垒机登录主机。
- 开启双因子认证后，不能通过CloudShell工具登录主机。
- 订阅主题的手机号码或邮箱单次可增加10个，一个主题最多可添加1万个。

操作步骤

步骤1 在“双因子认证”页面，单击“开启双因子认证”。

图 4-5 双因子认证



版权所有 © 华为技术有限公司

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

图 4-6 短信邮件验证

- **验证码验证**

图 4-7 验证码验证

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

须知

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

添加凭证：打开路径“开始菜单 > 控制面板 > 用户帐户 > 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

版权所有 © 华为技术有限公司

5 主机管理

5.1 创建服务器组

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

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航树中，选择“主机管理”，在“服务器组”界面，单击“创建服务器组”，如图5-1所示。

图 5-1 进入服务器组页面

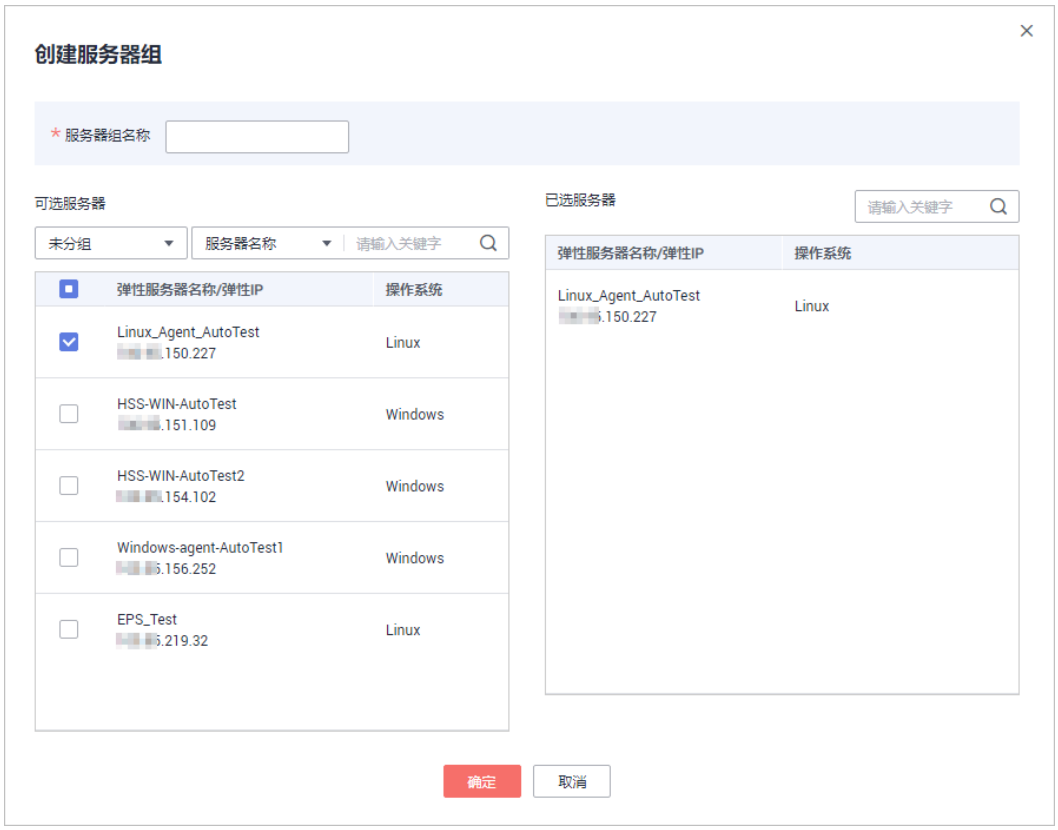
步骤4 在弹出的“创建服务器组”对话框中，输入“服务器组名称”，并设置服务器组中包含的云服务器，如图5-2所示。

说明

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

版权所有 © 华为技术有限公司

图 5-2 创建服务器组



步骤5 设置完成后，单击“确定”，完成服务器组的创建。

----结束

分配服务器到组

若服务器没有被分配到服务器组，您可以将服务器分配到已创建的服务器组。

步骤1 单击“云服务器”，进入云服务器列表界面。

步骤2 选中需要分配到服务器组的一台或多台云服务器，单击“分配到组”，将云服务器分配到服务器组，如图5-3所示。

图 5-3 分配到服务器组

说明

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

版权所有 © 华为技术有限公司

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

说明

一个云服务器只能分配到一个服务器组。

----结束

相关操作

编辑服务器组

步骤1 在待修改的服务器组所在行的操作列，单击“编辑”，修改服务器组。

步骤2 在弹出的对话框中，重新设置分组包含的云服务器。

步骤3 完成修改后，单击“确定”，完成服务器组的修改。

----结束

查看服务器组

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

删除服务器组

在需要删除的服务器组所在行的“操作”列，单击“删除”，删除单个服务器组。

服务器组被删除后，隶属于该服务器组的所有云服务器将被划分到“未分组”中。

5.2 部署策略

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

操作须知

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

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

进入策略管理

步骤1 登录管理控制台。

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

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

----结束

创建策略组

步骤1 选择“default_premium_policy_group（默认旗舰版策略组）”策略组，在该策略组所在行的操作列中，单击“复制”，如图5-4所示。

图 5-4 复制策略组

步骤2 在弹出的对话框中，输入“策略组名称”和“描述”，如图5-5所示。

说明

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

图 5-5 创建策略组

步骤3 单击“确定”，将会创建一个新的策略组。

步骤4 单击已创建的策略组名称，进入策略组的策略页面，如图5-6所示。

版权所有 © 华为技术有限公司

图 5-6 策略组策略

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

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

----结束

部署策略

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

步骤2 选中需要进行策略部署的一台或多台云服务器，单击“部署策略”，如**图5-7**所示。

图 5-7 部署策略

步骤3 在弹出的对话框中，选择策略组后，单击“确定”，完成部署策略操作。

版权所有 © 华为技术有限公司

图 5-8 选择策略组

说明

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

----结束

5.3 升级 Agent

指导您在企业主机安全平台将Agent1.0升级至Agent2.0，升级后您将在主机安全（新版）继续查看、管理主机防护状态，企业主机安全平台将停止检测、防护。

前提条件

- 升级时目标云服务器的“Agent状态”为“在线”才能正常升级。
- 升级Agent需要在旧版主机安全控制台界面进行操作。

升级说明

- 整个升级Agent过程均为免费。
- 升级过程中不影响您在云服务器上业务的正常使用。
- 升级后将在新版conosle进行计费，旧版停止计费。
- 升级后需切换至主机安全（新版）查看云服务器防护状态，企业主机安全平台（HSS）将停止防护。

  说明

  - 当前支持切换至主机安全服务（新版）的Region为华南-广州、中国-香港、亚太-曼谷、亚太-新加坡。
  - 切换至新版后，选择“资产管理 > 主机管理”，单击页面右上角“回到旧版”，可切换至主机安全。

版权所有 © 华为技术有限公司

- 升级后支持开启增强版勒索病毒防护。
- 升级后将提升Agent运行时的安全性、稳定性、可靠性。

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入服务后会弹出新版本上线的公告弹窗，单击弹窗中“云服务器界面”的链接。

图 5-9 进入主机管理进行 Agent 升级

步骤4 自动跳转至旧版主机安全的“云服务器”页面，勾选需要升级的服务器选框，单击上方“升级Agent2.0”。

说明

勾选的目标云服务器“Agent状态”必须为“在线”。

步骤5 在弹框中确认需要升级的云服务器，确认无误，单击“确认”，平台自动执行升级操作。

步骤6 升级时可在步骤5进入的界面查看目标云服务器的Agent状态。

Agent的状态分为升级中、升级成功、升级失败。

----结束

6 风险预防

6.1 资产管理

HSS提供资产管理功能，主动检测主机中的开放端口、系统运行中的进程、主机中的Web目录和自启动项，并对帐号信息和软件信息的变动情况进行记录。关于资产管理的详细说明请参见资产管理功能介绍。

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

资产管理仅提供风险检测功能，若发现有可疑资产信息，请手动处理。

检测周期

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

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

查看主机中的资产信息

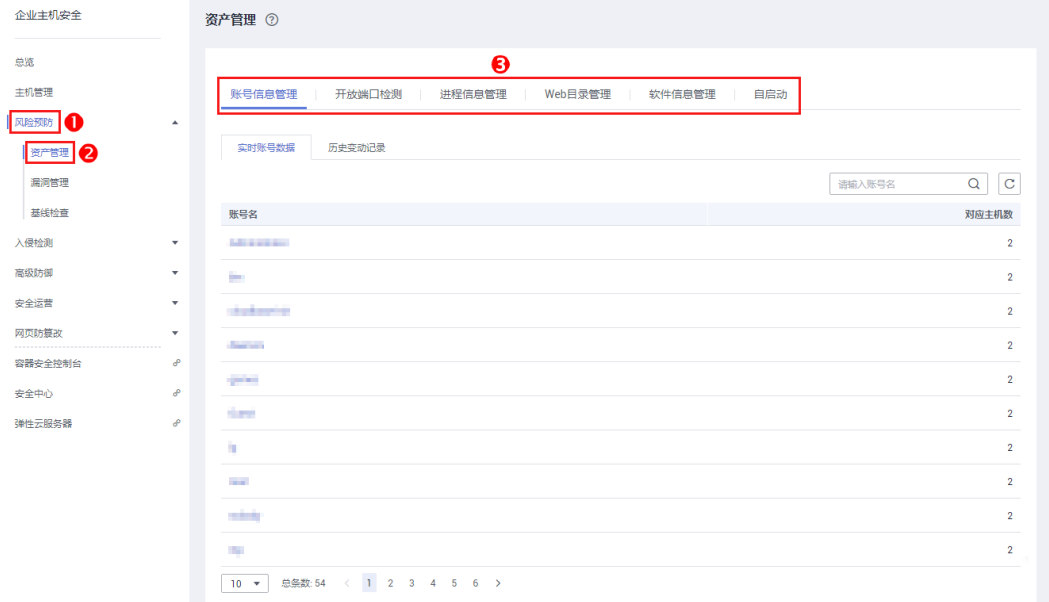
步骤1 登录管理控制台。

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

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

版权所有 © 华为技术有限公司

图 6-1 资产管理



----结束

帐号信息管理

历史变动状态说明：

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

根据实时帐号数据和历史变动记录，您可以统一管理所有主机中的帐号信息。若发现系统中有不必要的多余帐号，或者发现有超级权限的帐号（拥有root权限），需要排查这些帐号是否是正常业务使用，如果不是则建议删除多余帐号或者修改帐号的权限，避免帐号被黑客利用。

开放端口检测

根据开放端口检测结果中的详细信息，您可以统一管理所有主机中的开放端口。

- 手动关闭风险端口

  如果检测到开放了危险端口或者开放了不必要的端口，需要排查这些端口是否是正常业务使用，如果不是正常业务端口，建议关闭端口。对于危险端口建议进一步检查程序文件，如果存在风险建议删除或者隔离源文件。

  建议您及时优先处理危险程度为“危险”的端口，根据业务实际情况处理危险程度为“未知”的端口。
- 忽略风险：如果检测出的危险端口是业务正在使用的正常端口，您可以忽略该条告警。忽略之后将不再作为危险项进行记录，也不再发送告警。

进程信息管理

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

版权所有 © 华为技术有限公司

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

Web 目录管理

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

软件信息管理

历史变动状态说明：

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

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

自启动

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

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

6.2 漏洞管理

6.2.1 查看漏洞详情

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

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

“TOP5服务器”柱状图中，仅展示“修复紧急度”为“需尽快修复”的漏洞。

检测原理

表 6-1 漏洞检测原理

漏洞分类	原理说明
Linux软件漏洞	通过与漏洞库进行比对，检测出系统和软件（例如：SSH、OpenSSL、Apache、MySQL等）是否存在的漏洞，将结果上报至管理控制台，并为您提供漏洞告警。

漏洞分类	原理说明
Windows系统漏洞	通过订阅微软官方更新，判断服务器上的补丁是否已经更新，并推送微软官方补丁，将结果上报至管理控制台，并为您提供漏洞告警。
Web-CMS漏洞	通过对Web目录和文件进行检测，识别出Web-CMS漏洞，将结果上报至管理控制台，并为您提供漏洞告警。 支持检测的软件类型如下： ● wordpress ● Joomla ● drupal ● discuz

说明

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

漏洞库更新周期

HSS实时获取官方发布的漏洞信息，并更新到漏洞库中。

检测周期

企业主机安全服务**每日凌晨**将自动进行一次全面的检测，检测结束后才可导出扫描报告。

前提条件

已开启“企业版”、“旗舰版”或“网页防篡改版”主机防护。

Linux 软件漏洞/Windows 系统漏洞

步骤1 登录管理控制台。

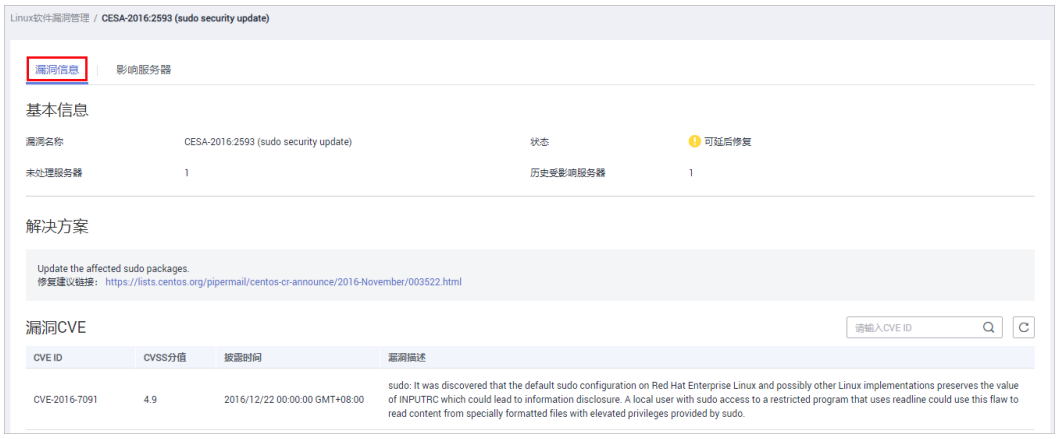
步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 企业主机安全”，进入企业主机安全页面。

步骤3 选择“Linux软件漏洞管理”或“Windows系统漏洞管理”页签，进入相应漏洞管理页面，如图6-2所示。

图 6-2 查看 Linux 软件/Windows 系统漏洞检测结果

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

图 6-3 漏洞信息



步骤5 查看漏洞影响的服务器，在该页面，您可以对漏洞进行处理。

图 6-4 影响服务器

- 单击“修复”，您可一键修复该漏洞。
- 单击“忽略”，您可忽略该漏洞，HSS将不再上报并告警此服务器上的这个漏洞。
- 修复漏洞后，您可以单击“验证”，一键验证该漏洞是否已修复成功。

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

版权所有 © 华为技术有限公司

若您确认已完成漏洞修复，但验证后仍提示未修复，请参考漏洞修复未生效进行排查。

若提示修复失败，可以单击“查看原因”了解具体原因并处理。

----结束

Web-CMS 漏洞

步骤1 登录管理控制台。

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

步骤3 进入“Web-CMS漏洞管理”页面，如图6-5所示。

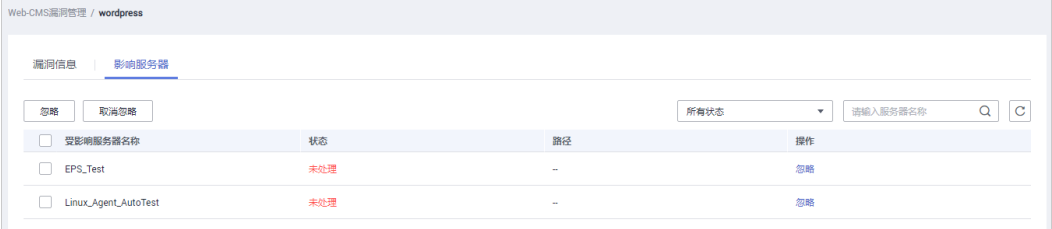
图 6-5 查看 Web-CMS 漏洞检测结果

步骤4 单击“漏洞名称”查看漏洞详情和受影响的服务器。

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

图 6-6 漏洞详细信息

图 6-7 受影响的服务器



----结束

导出漏洞报告

在漏洞列表的右上角，单击 ，导出漏洞报告。

须知

- HSS支持导出5000条漏洞数据，超出的部分数据将无法导出。

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

- 报告是展示了全部主机的安全情况，因此导出的漏洞报告是全部主机的报告，不支持只导出单台主机报告。
- 主机安全服务每日凌晨会自动进行一次全面的扫描检测，扫描结束后可下载漏洞报告，若有手动扫描需求，可**升级至主机安全（新版）**进行手动检测，扫描后可立即导出扫描报告。

6.2.2 漏洞修复与验证

- Linux软件漏洞和Windows系统漏洞：

  您可以使用“一键修复”功能进行修复，也可以根据界面提供的修复建议进行手动修复。

  修复完成后，可通过“验证”功能，快速验证漏洞是否修复成功。

  须知

  Windows漏洞修复需要公网访问权限。

- Web-CMS漏洞：

  请根据界面提供的修复建议进行手动修复。

操作风险

- 执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云服务器备份（CSBS）为ECS创建备份，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。

版权所有 © 华为技术有限公司

- 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。但是，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**。
- 漏洞修复后建议重启服务器，否则可能仍为您推送漏洞信息。

修复紧急度

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

漏洞显示时长

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

控制台一键修复漏洞

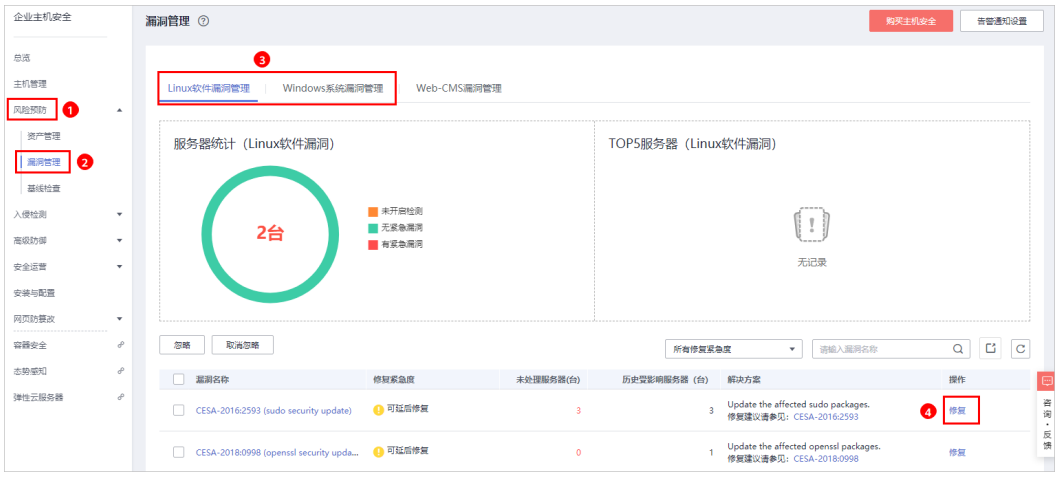
仅Linux软件漏洞和Windows系统漏洞支持控制台一键漏洞修复。

步骤1 **登录管理控制台**。

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

步骤3 进入“漏洞管理”页面，单击“修复”，进入影响服务器页面，如**图6-8**所示。

图 6-8 修复漏洞



步骤4 在影响服务器页面，勾选影响的服务器，单击“一键修复”，修复漏洞，如**图6-9**所示。

图 6-9 一键修复漏洞

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

步骤6 单击“确定”，进行一键修复漏洞，修复状态处于“修复中”。

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

说明

- “Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后需要手动重启，否则HSS仍可能为您推送漏洞消息。
- Windows系统漏洞修复重启后，您还需要在控制台单击已重启，确认主机已重启。

----结束

手动修复系统软件漏洞

根据漏洞列表右侧“解决方案”列中的修复建议修复主机中已经被识别出的漏洞，漏洞修复命令可参见表6-2。

- 不同的漏洞请根据修复建议依次进行修复。
- 若同一主机上的多个软件包存在同一漏洞，您只需修复一次即可。

说明

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

表 6-2 漏洞修复命令

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

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

方案一：创建新的虚拟机执行漏洞修复

版权所有 © 华为技术有限公司

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

方案二：在当前主机执行修复

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

漏洞忽略

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

忽略后，企业主机安全服务将不会对该漏洞告警。

修复验证

漏洞修复后，建议您立即进行验证。

手动验证

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

表 6-3 验证修复命令

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

- 手动执行漏洞检测查看漏洞修复结果。

自动验证

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

6.3 基线检查

6.3.1 查看基线检查详情

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

检测周期

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

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

  各检测项目并行检测，检测时长为30分钟内。
- 在“主机管理”页面，单击“检测结果”中的“有风险”或者“无风险”，进入单主机检测结果页面。

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

告警策略

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

说明

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

检查项列表

表 6-4 检查项列表

检查项	说明
经典弱口令检测	通过与弱口令库对比，检测帐号口令是否属于常用的弱口令。 支持MySQL、FTP及系统帐号的弱口令检测。
口令复杂度策略检测	检测系统帐号的口令复杂度策略。

检查项	说明
配置检测	根据CIS标准并结合多年最佳安全实践进行检测。 目前支持的配置检测类型有：Tomcat、SSH、Nginx、Redis、Apache2、MySQL5、MongoDB、Windows、vsftp、CentOS。

操作步骤

步骤1 登录管理控制台。

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

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

图 6-10 基线检查结果

----结束

导出配置检测报告

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

说明

不支持对单个云服务器执行导出。

6.3.2 基线检查风险项修复建议

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

版权所有 © 华为技术有限公司

存在弱口令

- 为保障您的主机安全，请您及时修改登录主机系统时使用弱口令的帐号，如SSH帐号。
- 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帐号，如MySQL帐号和FTP帐号等。

验证：完成弱口令修复后，建议您（企业版和旗舰版）立即**执行手动检测**，查看弱口令修复结果。如果您未进行手动验证，HSS会在次日凌晨执行自动验证。

增强口令复杂度策略

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

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

存在配置风险

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

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

- 修改有风险的配置项

  您可以根据“审计描述”验证检测结果，根据“修改建议”处理主机中的异常信息。

  建议您及时优先修复“威胁等级”为“高危”的关键配置，根据业务实际情况修复威胁等级为“中危”或“低危”的关键配置。

图 6-11 配置检测报告

- 忽略可信任的配置项

  选中单个存在风险的检测规则，单击操作列的“忽略”进行单个忽略。也可以选中多个检测规则，单击列表左上角的“忽略”批量进行忽略。

  对于已经忽略的检测规则，可以单击操作列的“取消忽略”，单个进行取消忽略，也可以批量选中想要取消忽略的规则撤销忽略。

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

7 入侵检测

7.1 告警事件概述

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

告警事件列表说明

说明

基础版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。

若需对云服务器进行防护或做等保认证，您需购买企业版及以上（包含企业版、旗舰版、网页防篡改版）版本。

版权所有 © 华为技术有限公司

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
帐户暴力破解	黑客通过帐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等帐户遭受的口令破解攻击。 ● 如果30秒内，帐户暴力破解次数（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，防止主机因帐户破解被入侵。 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。 ● 根据帐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。	√	√	√	√
帐户异常登录	检测“异地登录”和“帐户暴力破解成功”等异常登录。若发生异常登录，则说明您的主机可能被黑客入侵成功。 ● 检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。 异地登录检测信息包括被拦截的“登录源IP”、“登录时间”，攻击者尝试登录主机时使用的“用户名”和“云服务器名称”。 若在非常用登录地登录，则触发安全事件告警。 ● 若帐户暴力破解成功，登录到云主机，则触发安全事件告警。	√	√	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
恶意程序（云查杀）	恶意程序可能是黑客入侵成功之后植入的木马、后门等，用于窃取数据或攫取不当利益。 例如：黑客入侵之后植入木马，将受害主机作为挖矿、DDoS肉鸡使用，这类程序会大量占用主机的CPU资源或者网络资源，破坏用户业务的稳定性。 通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识后门、木马、挖矿软件、蠕虫和病毒等恶意程序，也可检测出主机中未知的恶意程序和病毒变种，并提供一键隔离查杀能力。 **说明** 恶意程序（云查杀）检测功能仅支持检测运行中的恶意程序。	×	√（隔离查杀）	√（隔离查杀）	√（隔离查杀）
进程异常行为	检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。	×	√	√	√
关键文件变更	篡改系统关键文件，通常是黑客入侵成功后进行身份隐藏或者发起下一步攻击的准备工作。 ● 对系统关键文件（例如：ls、ps、login、top等）进行监控，一旦文件被修改就进行告警，提醒用户关键文件存在被篡改的可能。监控的关键文件的路径请参见**关键文件变更监控路径**。 ● 关键文件变更信息包括“被更改的关键文件路径”、“文件最后修改时间”以及配置文件所在的“服务器名称”。 ● 添加关键文件指纹库，收集关键文件信息，便于清点合法文件信息，检测异常文件。 对于关键文件变更，HSS只检测目录或文件是否被修改，不关注是人为或者某个进程修改的。	×	√	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
网站后门	以php、jsp等网页文件形式存在的一种命令执行环境。 黑客在入侵了一个网站后，通常会将后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后使用浏览器来访问php或者jsp后门，得到一个命令执行环境，以达到控制网站服务器的目的。 检测云服务器上Web目录中的文件，判断是否为WebShell木马文件，支持检测常见的PHP、JSP等后门文件类型。 ● 网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略被查杀的可信文件。 ● 您可以使用手动检测功能检测主机中的网站后门。	×	√	√	√
反弹Shell	实时监控用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。 您可以在“策略管理”的“反弹/异常Shell检测”中配置反弹Shell检测，HSS会实时检测执行的可疑指令，主机被远程控制执行任意命令等。	×	×	√	√
异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。 您可以在“策略管理”的“反弹/异常Shell检测”中配置异常Shell检测，HSS会实时检测执行的可疑指令，主机被远程控制执行任意命令等。	×	×	√	√
高危命令执行	您可以在“策略管理”的“高危命令检测”中预置高危命令。 HSS实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	×	×	√	√

告警名称	告警说明	基础版	企业版	旗舰版	网页防篡改版
自启动检测	大多数木马通常通过创建自启动服务、定时任务、预加载动态库等方式入侵主机，自启动检测会收集所有云主机自启动的信息，帮助您快速发现主机中可疑的自启动，并清除木马程序问题。 HSS检测并列举当前系统中的自启动服务、定时任务、预加载动态库、Run注册表键和开机启动文件夹，帮助用户及时发现非法自启动。	×	×	√	√
风险帐户	黑客可能通过风险帐号入侵主机，以达到控制主机的目的，需要您及时排查系统中的帐户。 HSS检查系统中存在的可疑隐藏帐号、克隆帐号；若存在可疑帐号、克隆帐号等，则触发告警。	×	√	√	√
提权操作	当黑客成功入侵主机后，会尝试利用漏洞进行root提权或者文件提权，从而达到非法创建和修改系统帐号的权限或者篡改文件的目的。 HSS检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。 ● 对文件的提权。	×	×	√	√
Rootkit程序	HSS检测Rootkit安装的文件和目录，帮助用户及时发现可疑的Rootkit安装。 ● 使用文件特征码检测Rootkit。 ● 对隐藏文件、端口、进程的检测。	×	×	√	√

关键文件变更监控路径

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

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

7.2 查看和处理入侵告警事件

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

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

告警事件处理完成后，告警事件将从“未处理”状态转化为“已处理”。

说明

收到告警事件通知说明您的云服务器被攻击过，不代表已经被破解入侵。
您可在收到告警后，及时对告警进行分析、排查，采取相应的防护措施即可。

约束与限制

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

查看告警事件

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，单击“入侵检测 > 事件管理”，进入“事件管理”页面，如图7-1所示。

图 7-1 事件管理

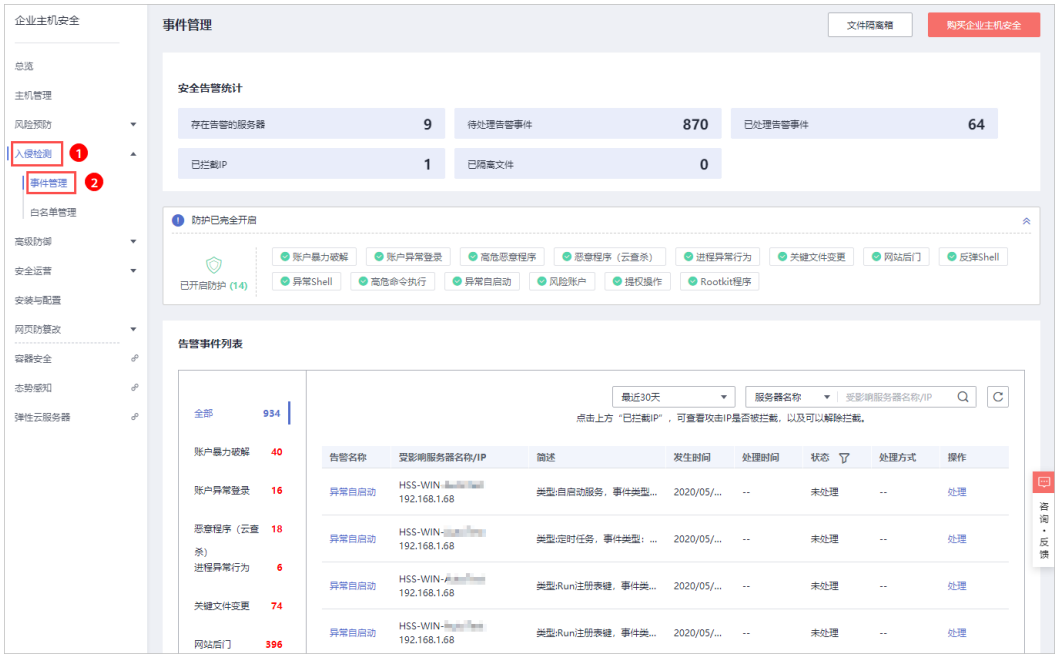


表 7-1 安全告警事件列表说明

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

版权所有 © 华为技术有限公司

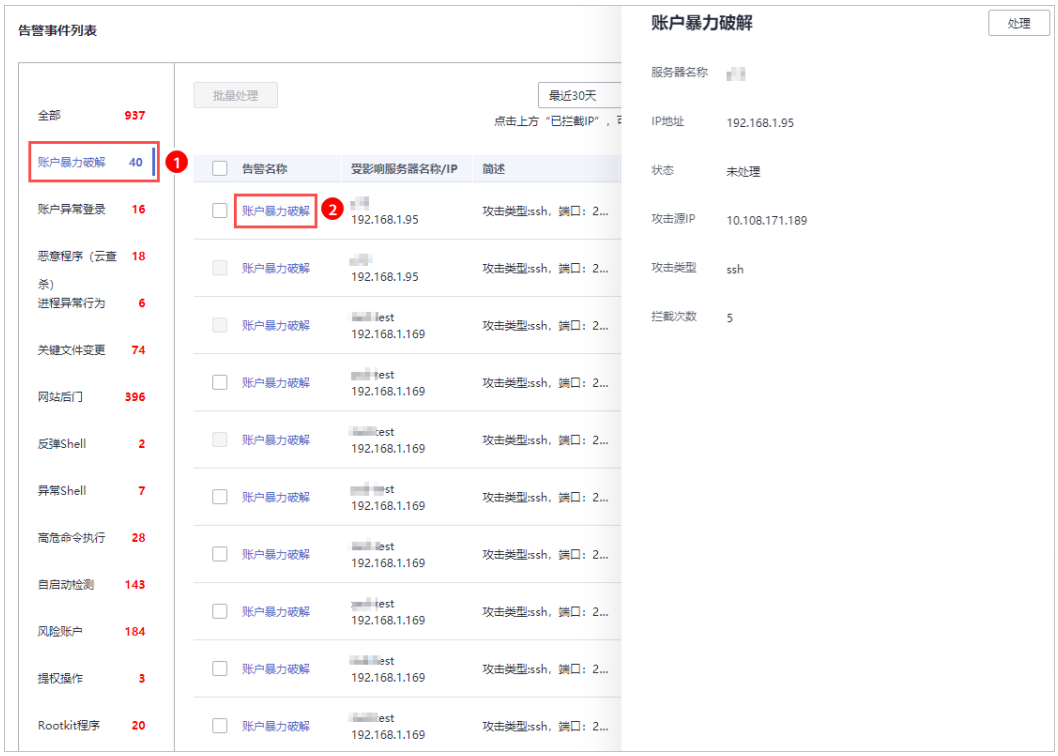
步骤4 单击告警事件列表中的告警事件，可查看告警事件对应的受影响的服务器、发生时间等信息，如图7-2所示。

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

图 7-2 告警事件统计数量

步骤5 单击告警列表中的告警名称，可查看告警的详细信息，如图7-3所示。

图 7-3 告警详细信息



----结束

版权所有 © 华为技术有限公司

处理告警事件

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

说明

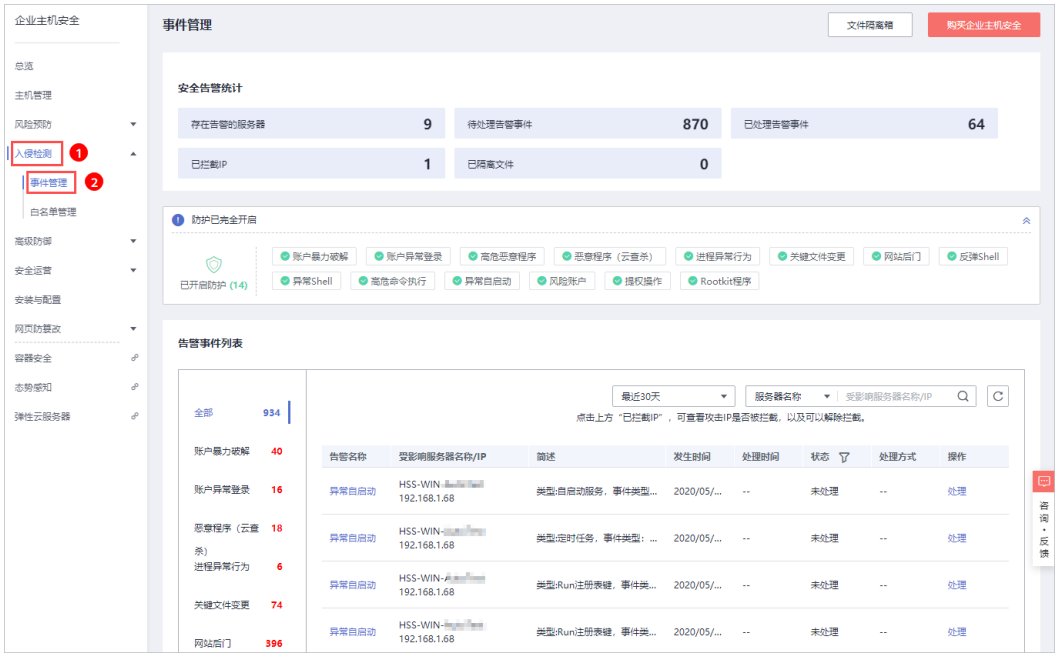
由于网络攻击手段、病毒样本在不断演变，实际的业务环境也有不同差异，因此，无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏，单击“入侵检测 > 事件管理”，进入事件管理页面。

图 7-4 事件管理



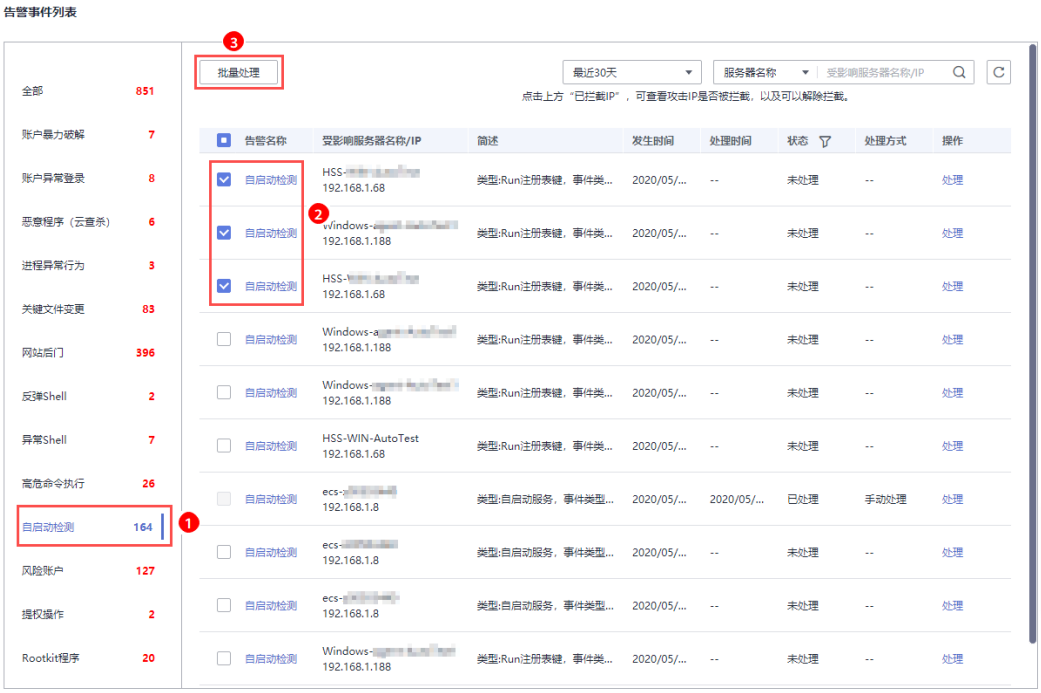
步骤4 单击告警列表中的告警事件，勾选待处理的告警事件，单击“批量处理”，处理告警事件，如图7-5所示，处理方式如表7-2所示。

说明

您也可以单击告警名称所在行的“处理”，处理告警。

版权所有 © 华为技术有限公司

图 7-5 处理告警事件



告警事件展示在“事件管理”页面中，事件管理列表仅展示最近30天的告警事件。

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

表 7-2 处理告警事件

处理方式	处理方式说明
忽略	仅忽略本次告警。若再次出现相同的告警信息，HSS会再次告警。
隔离查杀	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**。 有以下两类告警事件支持线上隔离查杀。 ● 恶意程序（云查杀） ● 进程异常行为 **说明** 程序被隔离查杀时，该程序的进程将被立即终止，为避免影响业务，请及时确认检测结果，若隔离查杀有误报，您可以执行取消隔离/忽略操作。
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。

版权所有 © 华为技术有限公司

处理方式	处理方式说明
加入登录白名单	如果确认“帐号暴力破解”和“帐户异常登录”类型的告警事件是误报，且不希望HSS再上报该告警，您可以将本次登录告警事件加入登录白名单。 HSS不会对登录白名单内的登录事件上报告警。加入登录白名单后，若再次出现该登录事件，则HSS不会告警。
加入告警白名单	如果确认以下类型的告警事件是误报，且不希望HSS再上报该告警，您可以将本次告警事件加入告警白名单。 HSS不会对告警白名单内的告警事件上报告警。加入告警白名单后，若再次出现该告警事件，则HSS不会告警。 ● 反弹Shell ● Webshell检测 ● 进程异常行为检测 ● 进程提权 ● 文件提权 ● 高危命令 ● 恶意程序

----结束

告警处理建议

告警名称	告警参数说明	处理建议
帐户暴力破解	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 攻击源IP：攻击主机的IP地址。 ● 攻击类型：可拦截的攻击类型，包含mysql、mssql、vsftp、filezilla、serv-u、ssh、rdp。 ● 尝试破解次数：被尝试破解的次数。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	**该告警事件需要您高度重视。** 若接收到帐户暴力破解告警通知，说明您的主机可能存在被暴力破解风险，包括但不限于以下这些情况： ● 系统存在弱口令，同时正在遭受暴力破解攻击。 ● 数次口令输错（但未达到封禁源IP条件）后成功登录。 建议您立即确认源IP是否是已知的合法IP。 ● 若源IP合法。 您可以“忽略”该次告警并手工解除IP封禁。或者“加入告警白名单”，该告警将不会再次触发。 ● 若源IP不合法，是未知IP，那么您的主机系统可能已经被黑客入侵成功。 1. 建议您将该事件标记为“手动处理”。 2. 立即登录系统并修改并设置安全的帐户密码。 3. 通过帐号信息管理和风险帐户排查所有系统帐户，对可疑帐户进行处理，防止攻击者创建新的帐户或者更改帐户权限。 4. 通过恶意程序（云查杀）排查系统是否被植入了恶意程序。针对恶意程序，请登录云主机，尽快结束其进程，阻止恶意程序运行。

告警名称	告警参数说明	处理建议
帐户异常登录	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 攻击类型：攻击的类型，包含mysql、mssql、vsftp、filezilla、serv-u、ssh、rdp。 ● 端口：被攻击的端口。 ● 主机：攻击者的IP地址。 ● 用户名：攻击者的用户名。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出帐户异常登录，建议您立即确认该源IP是否是已知的合法IP。 ● 若源IP合法，您可以“忽略”该事件。 如果该登录地是合法的常用登录地，您可以将该地区加入“常用登录地”列表。 ● 若该源IP不合法，是未知IP，那么您的主机系统已经被入侵成功，需要您高度重视。 建议您将该事件标记为“手动处理”，并立即登录系统并修改帐户密码，同时全面排查系统风险，避免系统遭受进一步破坏。
恶意程序（云查杀）	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 恶意程序路径：恶意程序的路径。 ● 哈希值：哈希值。 ● 文件权限：文件的权限。 ● 运行用户：运行该程序的用户。 ● 程序启动时间：程序启动的时间。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出存在恶意程序，建议您立即对该程序进行确认： ● 若该程序属于正常业务，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。 ● 若是未知程序或者经确认是恶意程序，建议立即执行进程查杀并隔离程序源文件。 – 您可以对已检测出的恶意程序或疑似恶意程序，执行一键“隔离查杀”。或者将该事件标记为“手动处理”，立即登录系统终止该进程并全面排查系统风险，避免系统遭受进一步破坏。 – HSS提供恶意程序自动隔离查杀功能，可对目前部分主流勒索病毒、DDOS木马等进行主动防护和主动隔离。 建议您启用该功能，加固主机安全防线。 详细操作请参见**开启恶意程序自动隔离查杀**。 ● 若事后确认该程序是无害程序或者查杀该程序影响了业务，可以“取消隔离查杀”，或者从“文件隔离箱”中还原程序源文件。

版权所有 © 华为技术有限公司

告警名称	告警参数说明	处理建议
进程异常行为	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 疑似恶意程序路径：疑似恶意程序的路径。 ● 文件权限：文件的权限。 ● PID：进程ID。 ● 命令行：启动异常进程的命令行。 ● 父进程PID：父进程的进程ID。 ● 父进程程序路径：父进程的程序路径。 ● 行为：该异常进程的行为，例如：高CPU。 ● 连接数： ● CPU使用频率：CPU的使用频率。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出进程异常行为，建议您立即对该进程进行确认： ● 若该进程属于正常业务，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。 ● 若是未知进程或者经确认是恶意程序，建议立即执行进程查杀并隔离程序源文件。 – 您可以对已检测出的恶意程序或疑似恶意程序，执行一键“隔离查杀”。或者将该事件标记为“手动处理”，立即登录系统终止该进程并全面排查系统风险，避免系统遭受进一步破坏。 – HSS提供恶意程序自动隔离查杀功能，可对目前部分主流勒索病毒、DDOS木马等进行主动防护和主动隔离。 建议您启用该功能，加固主机安全防线。 详细操作请参见**开启恶意程序自动隔离查杀**。 ● 若事后确认该程序是无害程序或者查杀该程序影响了业务，可以“取消隔离查杀”，或者从“文件隔离箱”中还原程序源文件。

版权所有 © 华为技术有限公司

告警名称	告警参数说明	处理建议
关键文件变更	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 操作：对关键文件执行的操作。 ● 文件路径：被操作的关键文件的路径。 ● 移动到：移动到的路径。 ● 是否目录：操作的是否是目录，“true”或者“false”。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出关键文件变更，建议您立即对该变更进行确认： ● 若合法，您可以“忽略”该告警。 ● 若不合法，关键文件被异常的读取、写入、删除等，确认非用户主动行为。 建议您将该事件标记为“手动处理”，立即将该文件替换为操作系统的标准版本。并修改帐户密码，同时全面排查系统风险，避免系统遭受进一步破坏。
网站后门	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 木马文件路径：木马所在的文件路径。 ● 发现时间：发现的时间。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出网站后门，建议您立即确认该文件是否合法。 ● 若合法，您可以“忽略”该告警；或者“加入告警白名单”，该告警将不会再次触发。 ● 若不合法，建议您将该事件标记为“手动处理”，并对该文件立即执行隔离。
反弹/异常Shell	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 文件路径：文件的路径。 ● 详情：详情。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出反弹/异常Shell，建议您立即确认该反弹/异常Shell是否合法。 ● 若合法，您可以“忽略”该事件。 ● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统阻断非法连接或者命令执行，并全面排查系统风险，避免系统遭受进一步破坏。

告警名称	告警参数说明	处理建议
高危命令执行	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 哈希值：哈希值。 ● PID：进程的ID。 ● 进程路径：进程的路径。 ● 进程命令：执行该进程的命令。 ● 父进程PID：父进程的ID。 ● 父进程路径：父进程的路径。 ● 父进程命令：执行父进程的命令。 ● 会话用户名：会话的用户名。 ● 运行用户：运行的用户。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出高危命令执行，建议您立即确认该高危命令执行是否合法。 ● 若合法，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。 ● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统排查该命令所执行的操作，并全面排查系统风险，避免系统遭受进一步破坏。

告警名称	告警参数说明	处理建议
自启动检测	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 服务名：自启动服务的名称。 ● 路径：自启动服务的路径。 ● 类型：自启动的类型。 ● 事件类型：事件的类型。 ● 运行用户：运行的用户。 ● 文件HASH：文件的HASH。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出新增自启动项，需要用户自行判断该自启动是否合法。 ● 若合法，您可以“忽略”该事件；或者“加入告警白名单”，该告警将不会再次触发。 ● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统删除非法自启动项目，并全面排查系统风险，避免系统遭受进一步破坏。
风险帐户	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 帐号名：风险帐号的名称。 ● 用户组：风险帐号所在的用户组。 ● UID/SID：UID/SID。 ● 用户目录：用户的目录。 ● 用户启动Shell：用户启动的Shell。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出风险帐号，建议您立即确认该帐号是否合法。 ● 若合法，您可以“忽略”该事件。 ● 若不合法，请将该事件标记为“手动处理”，建议执行以下操作： – 删除可疑帐号 删除主机中无用的系统登录帐号，如SSH帐号。 删除主机中MySQL、FTP使用的无用的帐号。 – 限制帐号权限 通过限制关键配置项，限制非管理员的文件访问权限和文件修改权限，防止未授权的访问权限和使用操作。

告警名称	告警参数说明	处理建议
提权操作	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● 提权方式：提权的方式。 ● 提权文件路径：提权文件的路径。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出提权操作，建议您立即确认该提权操作是否合法。 ● 若合法，您可以“忽略”该事件。 ● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统阻止非法创建和修改系统帐号或者篡改文件的行为，并全面排查系统风险，避免系统遭受进一步破坏。
Rootkit程序	● 服务器名称：云服务器的名称。 ● IP地址：受影响服务器的IP地址。 ● Rootkit名称：Rootkit的名称。 ● 子模块名称：子模块的名称。 ● 特征：Rootkit程序特征。 ● 状态：处理告警事件的状态，“已处理”或者“未处理”。	若检测出Rootkit程序安装，建议您立即确认该Rootkit安装是否合法。 ● 若合法，您可以“忽略”该事件。 ● 若不合法，请将该事件标记为“手动处理”，建议您立即登录系统终止该Rootkit安装行为，并全面排查系统风险，避免系统遭受进一步破坏。

7.3 管理文件隔离箱

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

对以下两类告警事件支持线上隔离查杀：

- 恶意程序（云查杀）
- 进程异常行为

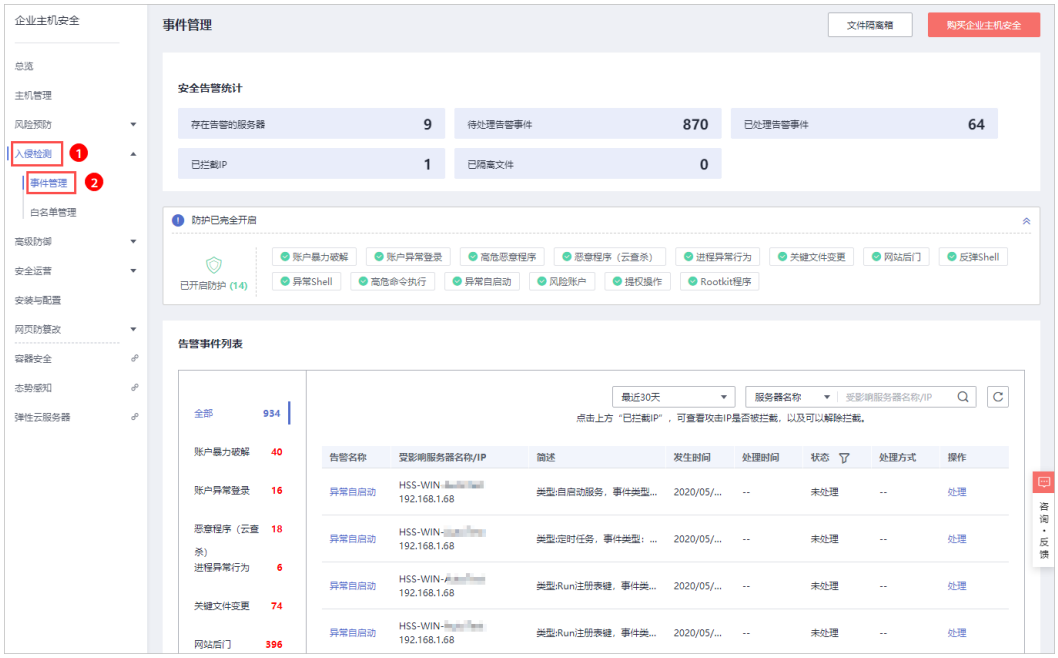
选择隔离查杀

步骤1 登录管理控制台。

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

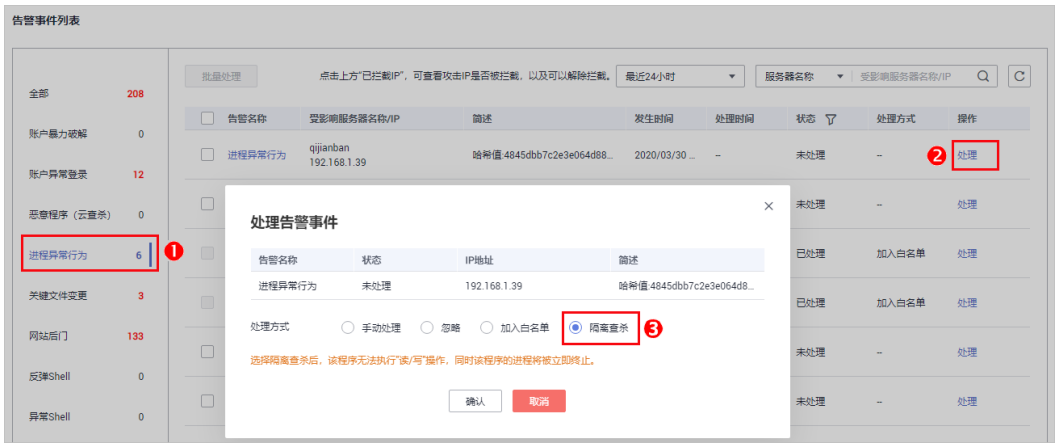
步骤3 在左侧导航栏，单击“入侵检测 > 事件管理”，进入事件管理页面。

图 7-6 事件管理



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

图 7-7 隔离查杀



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

----结束

查看文件隔离箱

步骤1 在“事件管理”页面，单击“文件隔离箱”，弹出文件隔离箱页面。

步骤2 在文件隔离箱列表中，您可以查看被隔离的文件服务器名称、路径和修改时间，如图7-8所示。

图 7-8 文件隔离箱

----结束

一键恢复

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

步骤2 单击“确认”，恢复的文件将重新回到告警事件列表中。

说明

执行恢复操作会将隔离文件查杀恢复，请谨慎操作。

----结束

7.4 配置告警白名单

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

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

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

仅企业版、旗舰版支持白名单管理，网页防篡改版赠送旗舰版，包含旗舰版所有功能。

添加告警白名单

表 7-3 添加告警白名单

添加方式	说明
加入告警白名单	处理告警事件时，将告警事件加入到告警白名单，详细信息请参见查看和处理入侵告警事件。 以下类型的告警事件加入“告警白名单”： ● 反弹Shell ● Webshell检测 ● 进程异常行为检测 ● 进程提权 ● 文件提权 ● 高危命令 ● 恶意程序
导入告警白名单	在“告警白名单”页面，导入告警白名单列表。

查看告警白名单

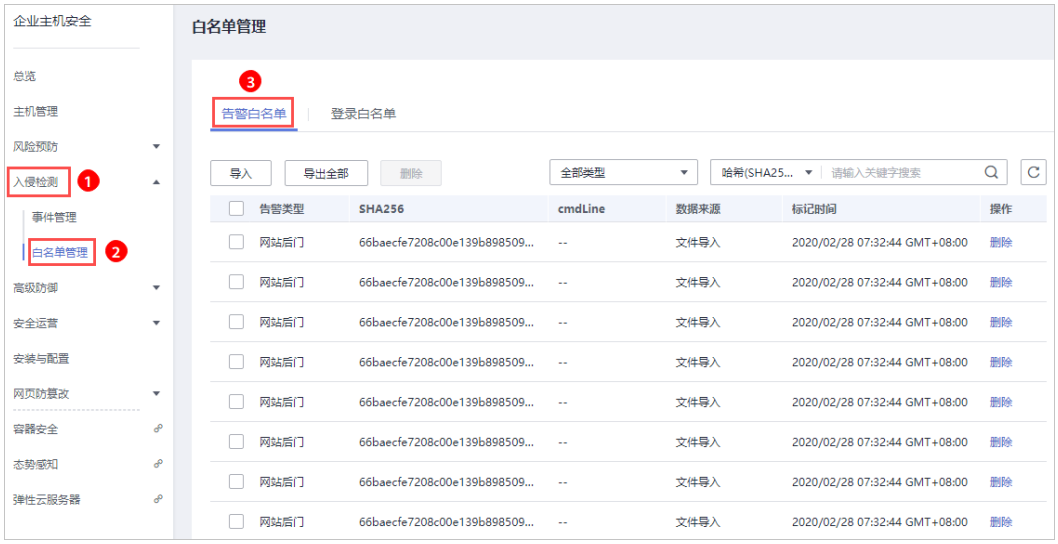
加入告警白名单后，您可以查看已添加的告警白名单，操作步骤如下所示。

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“白名单管理”页面，单击“告警白名单”，查看已添加的告警白名单列表，如图7-9所示。

图 7-9 告警白名单列表



----结束

导入/导出告警白名单

导入和导出告警白名单功能用来备份和恢复告警白名单。

须知

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

  格式要求：

  ```
  告警类型,SHA256,cmdLine,数据来源,标记时间
  "webshell","66baecfe7208c00e139b898509626ee4d2ea81382ef15a4283b95d50f669b121","--","文件导入","2020/02/28 07:32:44 GMT+08:00"
  ```

- 告警白名单支持增量导入，相同的记录多次导入不会增加。

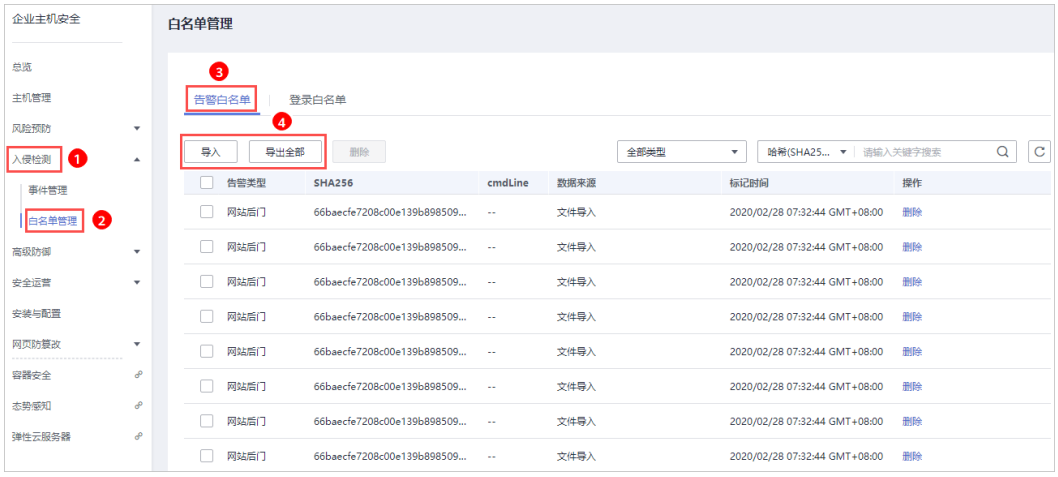
步骤1 登录管理控制台。

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

步骤3 进入“白名单管理”页面，选择“告警白名单”，如图7-10所示。

版权所有 © 华为技术有限公司

图 7-10 选择告警白名单



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

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

  说明

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

----结束

相关操作

删除告警白名单

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

说明

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

7.5 配置登录白名单

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

版权所有 © 华为技术有限公司

说明

- 配置的目标服务器IP、登录端IP以及登录端用户名需同时满足白名单配置的信息，检测时才会忽略。
- 如果将已经产生告警的目标IP通过**添加登录告警白名单**方式加入白名单，加入白名单之后的检测会对目标IP进行忽略，但已经产生的告警不会自动放行，仍需对告警进行处理，处理详情请参见**查看和处理入侵告警事件**。

您可以通过以下两种方式添加登录白名单：

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

仅企业版、旗舰版支持白名单管理，网页防篡改版赠送旗舰版，包含旗舰版所有功能。

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“白名单管理”页面，选择“登录白名单”，单击“添加”，如**图7-11**所示。

图 7-11 登录白名单

步骤4 在“添加登录安全白名单”对话框中，输入“服务器IP”、“登录IP”和“登录用户名”，如**图7-12**所示。

说明

- “服务器IP”和“登录IP”支持IPv4地址。
- “服务器IP”和“登录IP”支持单个IP、IP范围、IP掩码，以英文逗号分隔，例如：192.168.1.1、192.168.2.1-192.168.6.1、192.168.7.0/24。
- “服务器IP”和“登录IP”支持最大长度为128字节。

图 7-12 添加登录安全白名单

步骤5 单击“确认”，完成登录白名单的添加。

----结束

其他操作

删除登录白名单

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

说明

执行删除操作后无法恢复，请谨慎操作。

版权所有 © 华为技术有限公司

8 高级防御

8.1 程序运行认证

8.1.1 查看白名单策略列表

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

背景信息

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

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

说明

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

查看白名单策略列表

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 > 企业主机安全”，进入企业主机安全页面。

版权所有 © 华为技术有限公司

步骤3 进入“程序运行认证”页面，选择“白名单策略”页签，查看白名单策略列表，如图8-1所示。

图 8-1 查看白名单策略列表

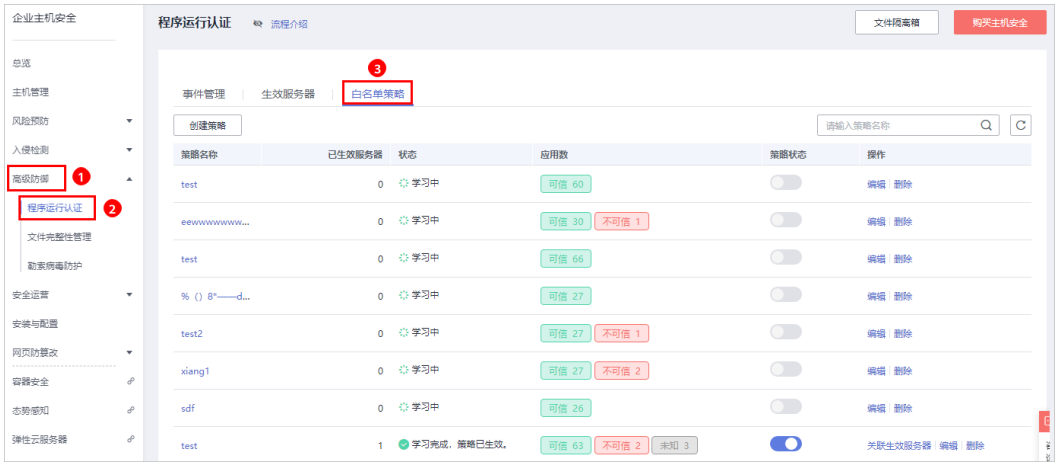


表 8-1 策略列表说明

参数	参数说明
策略名称	创建的白名单策略的策略名称。
已生效服务器	应用白名单策略生效的服务器数量。
状态	策略的生效状态。包含以下状态： ● 学习中 智能学习进行中。 策略创建完成后，自动对学习的服务器执行智能学习。新创建的策略状态都为“学习中”。 ● 学习完成，策略未生效 该策略已完成智能学习，需确认并启用策略。 智能学习完成后，您还需单击该策略状态下的，启用该策略。启用策略后，策略才能生效，HSS会自动识别您服务器中进程的风险类型（可信、不可信和未知）。 ● 学习完成，策略已生效 该策略已完成智能学习，并且已应用到关联生效服务器中。
应用数	HSS自动识别学习服务器中应用进程的风险数量，包含“可信”、“不可信”和“未知”应用进程的数量。
策略状态	策略的状态，白名单策略处于“学习完成，策略未生效”，可单击，开启白名单策略。开启白名单策略后，策略才生效。

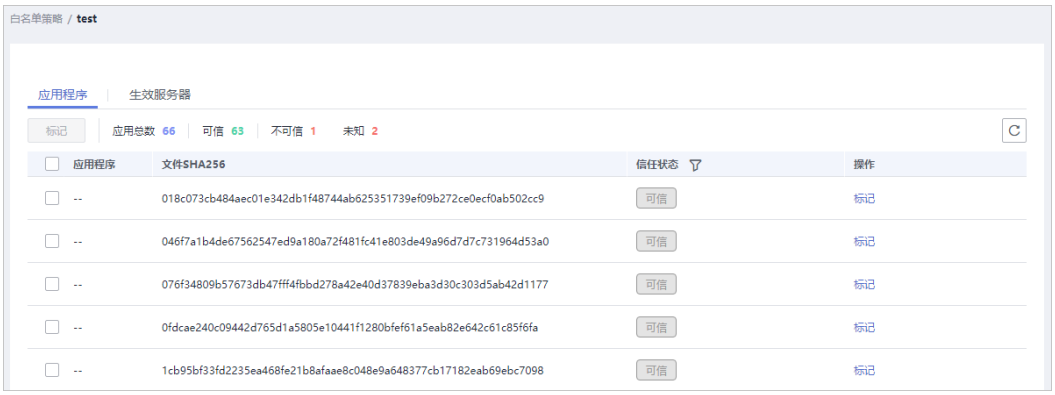
版权所有 © 华为技术有限公司

参数	参数说明
操作	可对该策略执行的操作。支持以下操作： ● 关联生效服务器：单击“关联生效服务器”，打开“关联生效服务器”页面，可增加或删除应用该白名单策略的服务器。 ● 编辑：单击“编辑”打开编辑策略白名单页面，对该策略进行修改。可修改该策略的“智能学习天数”和执行智能学习的服务器。 ● 删除：删除白名单策略。 策略删除后，对应的生效服务器的进程将不再受到该白名单策略的保护。

步骤4 单击策略名称，进入白名单策略详情页面，查看关联服务器的“应用程序”，如图8-2所示。

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

图 8-2 应用程序列表



步骤5 单击“生效服务器”页签，查看应用该白名单策略的生效服务器，如图8-3所示。

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

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

图 8-3 查看生效服务器

版权所有 © 华为技术有限公司

说明

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

----结束

8.1.2 应用白名单策略

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

前提条件

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

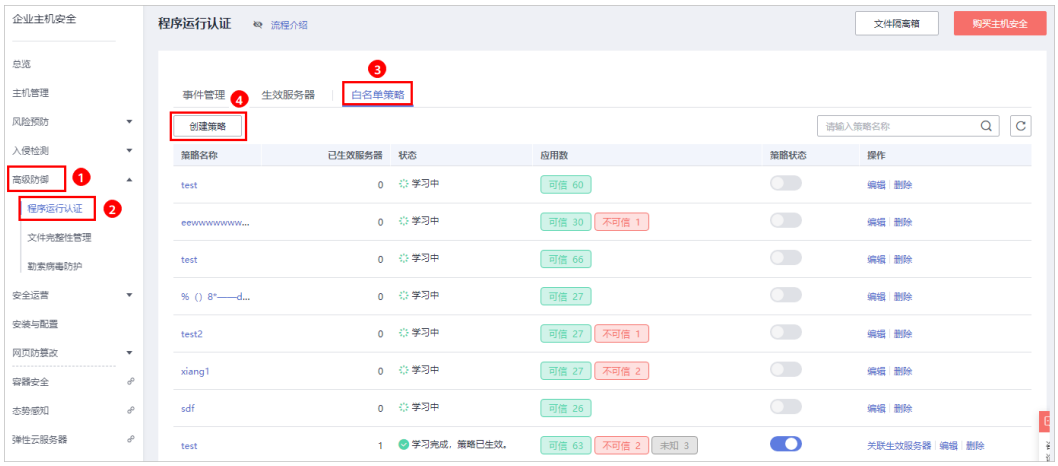
创建白名单策略

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“程序运行认证”页面，选择“白名单策略”，单击“创建策略”，如图8-4所示。

图 8-4 创建白名单策略



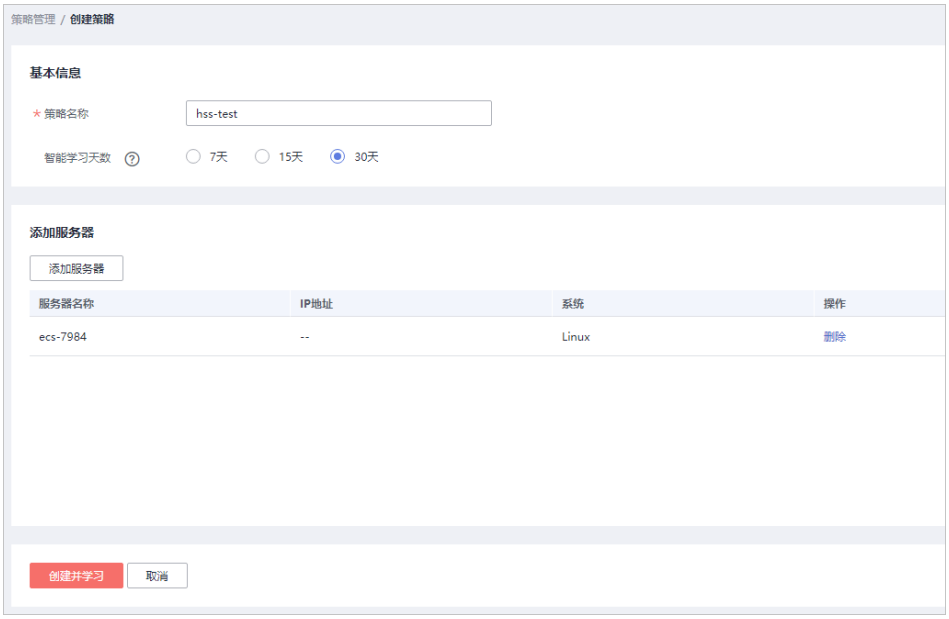
步骤4 在创建策略页面中，配置策略“基本信息”，如图8-5所示。

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

  如果选择的智能学习天数小于实际业务场景操作的天数，会导致智能学习失败。

版权所有 © 华为技术有限公司

图 8-5 配置策略信息



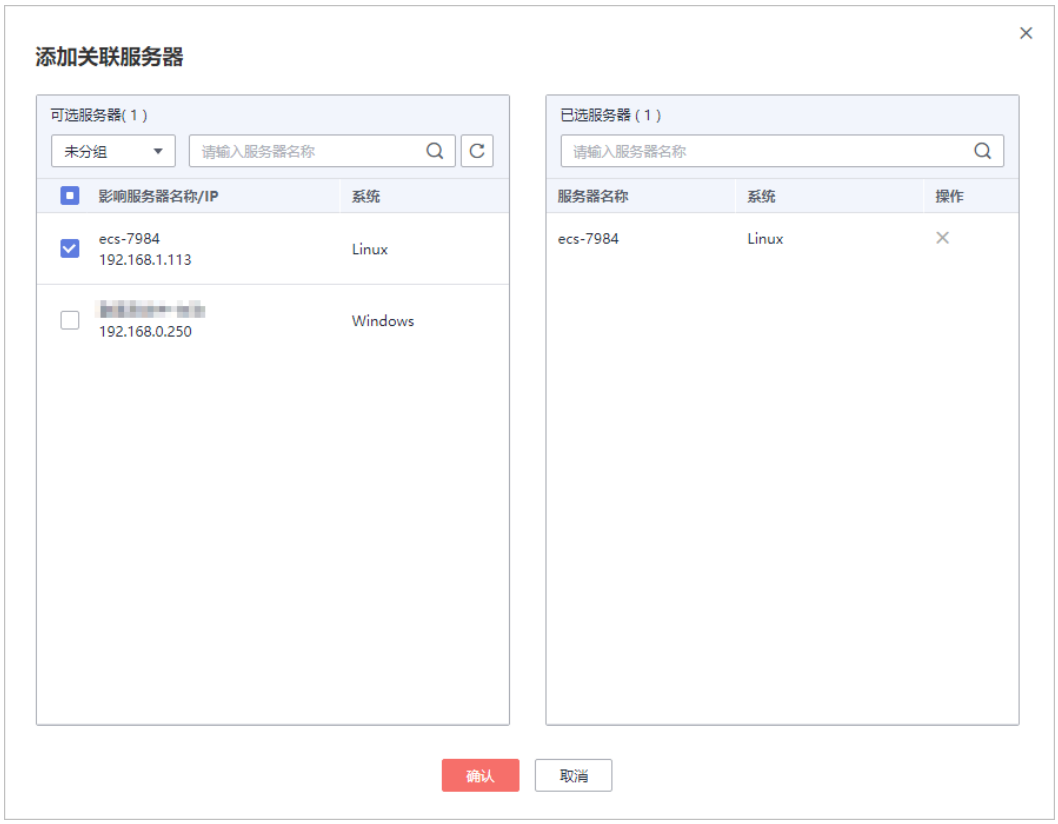
步骤5 单击“添加服务器”，添加智能学习服务器，如图8-6所示。

须知

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

版权所有 © 华为技术有限公司

图 8-6 添加白名单策略学习服务器



步骤6 单击“确认”，完成白名单策略学习服务器的添加。

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

步骤7 单击“创建并学习”，完成白名单策略的创建。

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

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

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

----结束

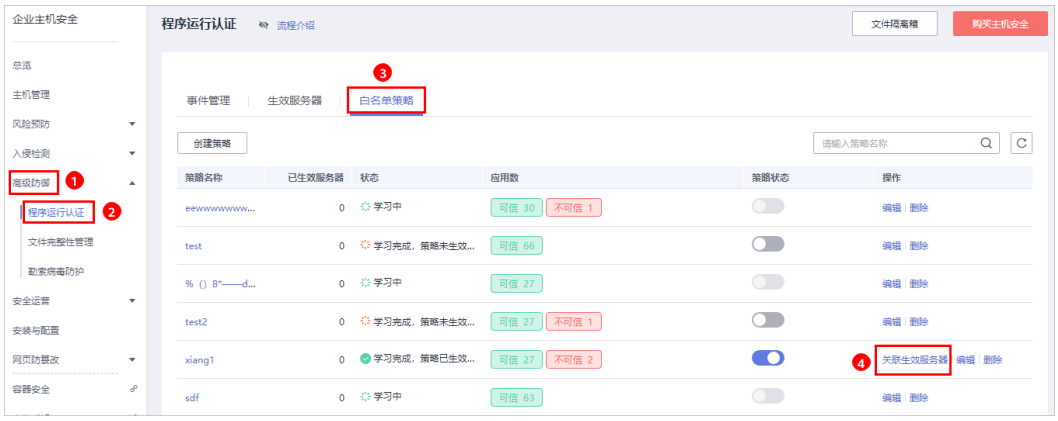
添加生效服务器

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

白名单策略状态处于“学习完成，策略已生效”，才能成功添加生效服务器。

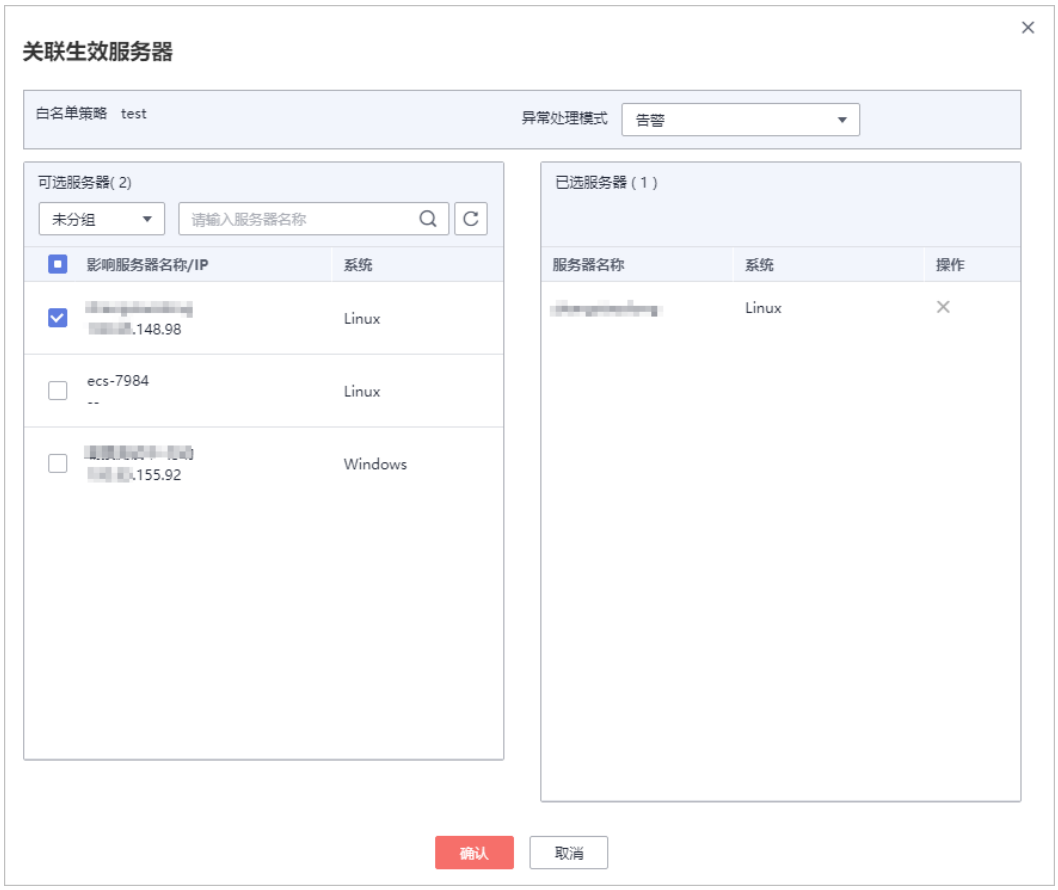
步骤1 单击“关联生效服务器”，为白名单策略添加生效服务器，如图8-7所示。

图 8-7 添加关联生效服务器



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

图 8-8 配置关联生效服务器



步骤3 配置完成后，单击“确认”，完成关联生效服务器的添加。

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

----结束

相关操作

管理生效服务器

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

  您可以查看生效服务器的“服务器名称/IP地址”、“白名单策略”、“异常行为数”和“异常处理模式”。
- 若不需要检测添加的生效服务器，可以在该生效服务器所在行的“操作”列，单击“删除”，删除生效服务器。删除后，该服务器的进程将不再受该白名单策的保护。

编辑白名单策略

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

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

删除白名单策略

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

8.1.3 查看和处理程序运行事件

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

你可以对进程告警事件进行“可信”、“不可信”和“未知”标记。

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

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

说明

建议您对“不可信”、“未知”和不在白名单策略中的进程进行重点排查和处理。

程序运行认证检测功能在当前版本中为测试使用，可能存在无法完全满足对应能力的情况，你可购买升级后的主机安全（新版）进行使用。

查看程序运行事件

步骤1 登录管理控制台。

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

步骤3 进入“程序运行认证”页面，选择“事件管理”，如图8-9所示。

图 8-9 程序运行事件管理页面

表 8-2 程序运行事件管理

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

----结束

处理程序运行事件

步骤1 在事件管理列表的操作列中，单击“处理”，处理进程告警事件，如图8-10所示。

图 8-10 处理应用进程告警事件

步骤2 在弹出的处理事件窗口中，选择处理方式，处理进程告警事件，如图8-11所示。

版权所有 © 华为技术有限公司

图 8-11 处理进程告警事件

表 8-3 处理告警事件

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

步骤3 单击“确定”，完成进程告警事件处理。

----结束

8.2 文件完整性管理

版权所有 © 华为技术有限公司

8.2.1 添加管理文件

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

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

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

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

后续将支持注册表变更统计，敬请期待。

须知

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

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

开启文件完整性管理

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“文件完整性管理”页面，单击 ⬭，开启文件完整性管理，默认 ⬬，如图8-12所示。

图 8-12 开启文件完整性管理

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

----结束

版权所有 © 华为技术有限公司

添加管理文件

若需要添加管理文件，请满足以下条件：

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

添加管理文件的操作步骤，如下所示。

步骤1 登录管理控制台。

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

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

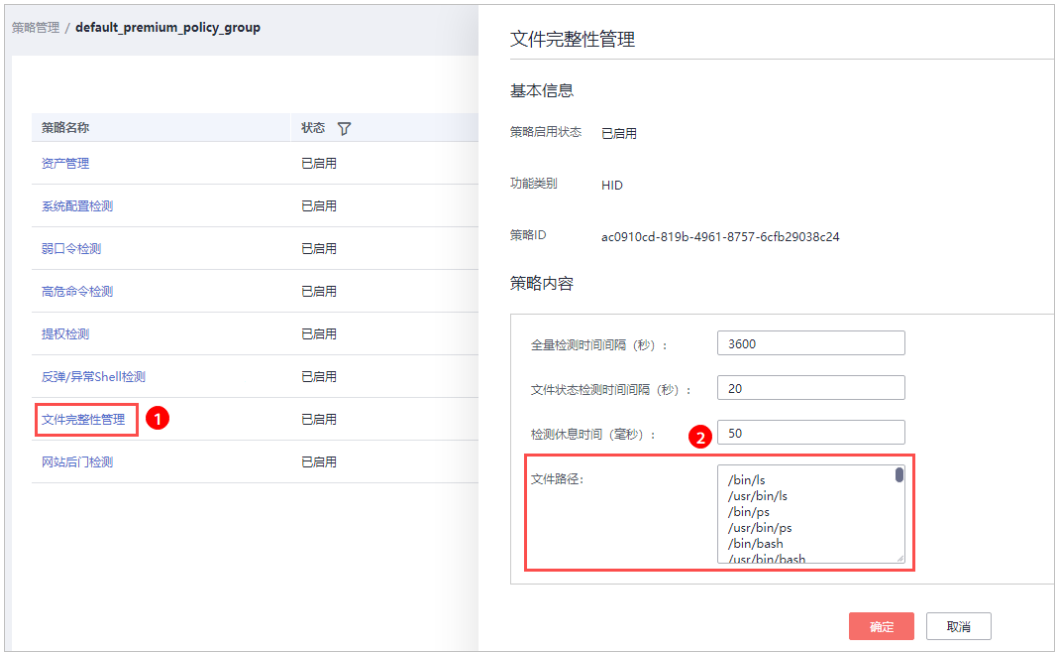
步骤4 在策略管理页面，单击主机应用的策略组的名称，进入策略列表页面，以默认“旗舰版策略组”为例，如图8-13所示。

图 8-13 默认策略组

步骤5 单击“文件完整性管理”，弹出文件完整性管理策略的页面，添加需要管理的文件，如图8-14所示。

关于配置“文件完整性管理”策略，详细操作请参见文件完整性管理。

图 8-14 进入文件完整性管理策略



版权所有 © 华为技术有限公司

步骤6 添加完成后，单击“确定”，完成管理文件的添加。

----结束

相关操作

关闭文件完整性管理

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

8.2.2 查看变更统计

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

查看变更概况

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“文件完整性管理”页面，查看变更概况，如图8-15所示。

图 8-15 查看变更概况

表 8-4 变更概况

类别	说明
服务器总数（台）	所有管理的服务器的总台数。
变更统计	• 变更总数（个）：所有管理的变更的总的数量。 • 文件数：所有管理的文件变更的数量。 • 注册表：所有管理的注册表变更的数量。

版权所有 © 华为技术有限公司

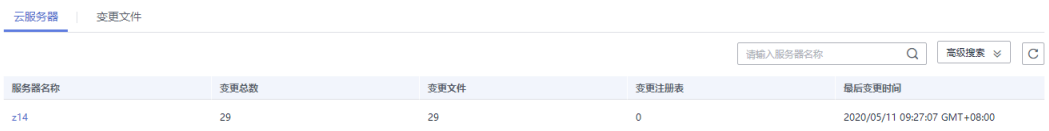
类别	说明
变更类别	• 修改：所有管理的文件和注册表修改的数量 • 新增：所有管理的文件和注册表新增的数量。 • 删除：所有管理的文件和注册表删除的数量。

----结束

查看单个云服务器变更文件

步骤1 在云服务器列表中，查看服务器对应的文件和注册表变更总数、变更文件、变更注册表和最后变更时间，如图8-16所示。

图 8-16 云服务器列表页面



步骤2 单击服务器名称，你可以在列表上方查看该服务器的变更统计总数，包括变更总数、变更文件数量、变更注册表数量，如图8-17所示。

说明

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

图 8-17 服务器变更详情

步骤3 在该服务器的文件列表中，您可以查看该服务器文件和注册表的变更详情。

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

说明

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

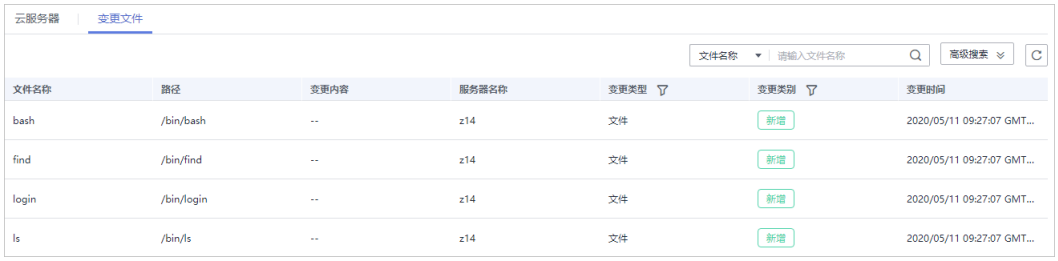
----结束

版权所有 © 华为技术有限公司

查看全量变更文件

在变更文件列表中，查看所有主机的变更文件，包含文件变更的文件名称、路径、变更内容、服务器名称、变更类型、变更类别和变更时间，如图8-18所示。

图 8-18 变更文件列表



说明

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

8.3 勒索病毒防护

8.3.1 防勒索病毒概述

服务器感染勒索病毒越来越普遍，一旦服务器遭受勒索病毒攻击，关键文件会被加密，无法正常使用，企业业务将受到严重影响。HSS针对勒索病毒提供了防勒索解决方案，帮助您从勒索病毒入侵前、入侵时和入侵后全方位应对勒索病毒。

说明

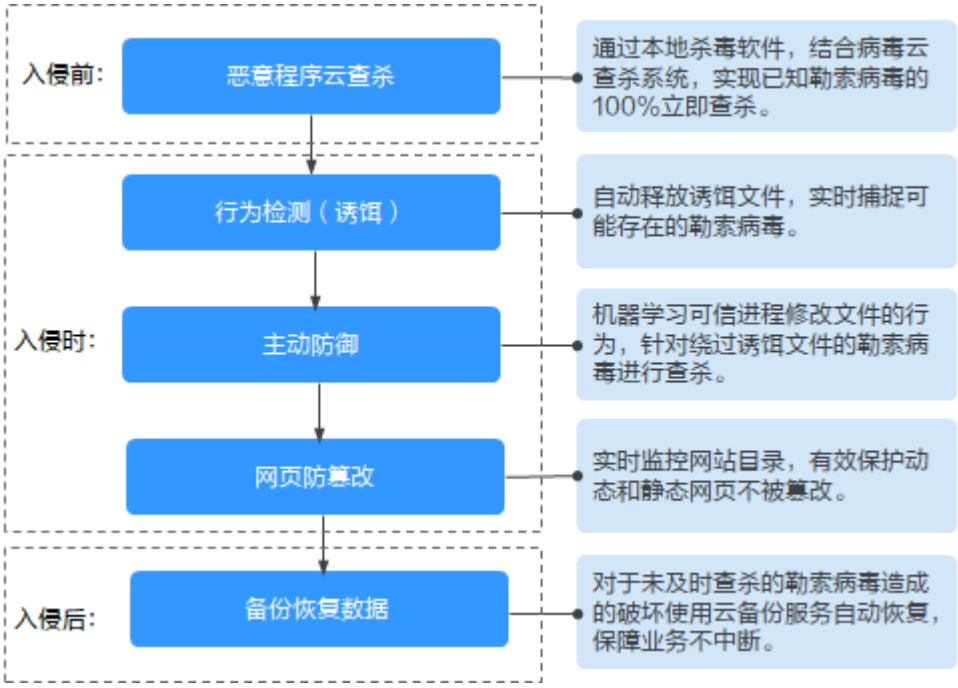
防勒索病毒功能在当前版本中为测试使用，可能存在无法完全满足对应能力的情况，您可购买升级后的主机安全（新版）进行使用。

工作原理

创建防勒索病毒策略后，HSS可有效监控您云主机上存储的重要文件，防止未经过认证或授权的进程文件对监控文件的加密或修改操作，保障您的主机不被勒索病毒侵害。同时，还可以自动释放诱饵文件，诱捕可能存在的勒索病毒。若您的服务器不慎被勒索病毒入侵，您可以使用云备份服务恢复数据，保障业务不中断。

版权所有 © 华为技术有限公司

图 8-19 防勒索病毒工作原理图



功能介绍

创建勒索病毒防护策略后，HSS通过机器学习引擎对服务器运行状态的自动学习和管理端智能分析，完成可信程序的判定。同时，学习服务器上的可信进程修改文件的行为。防护策略学习完成后，自动应用于关联服务器，在防护阶段对非可信程序的操作进行告警。

- Linux防护勒索
  - 创建Linux防护策略时，若开启诱饵防护，HSS将会在关联服务器上预置诱饵文件。若发现未知勒索病毒加密诱饵文件的行为，立即告警。

    说明

    - HSS会对预置诱饵文件进行标识，如果您在服务器中发现可疑文件，请确定是否为HSS预置的诱饵文件。
    - 诱饵文件不会对您的业务产生影响，也不存在任何的恶意行为，若将诱饵文件删除，HSS将无法诱捕新型未知的勒索病毒。
  - 创建Linux防护策略完成后，智能学习策略通过机器学习引擎学习关联服务器上的可信进程修改文件的行为，对绕过诱饵文件的勒索病毒进行告警。
- Windows防护勒索

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

8.3.2 创建防护策略

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

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

说明

防勒索病毒功能在当前版本中为测试使用，可能存在无法完全满足对应能力的情况，您可购买升级后的主机安全（新版）进行使用。

前提条件

- 已开启“旗舰版”或“网页防篡改版”主机安全防护。
- Linux主机的“Agent状态”为“在线”。

创建 Linux 防护策略

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“创建策略”，创建Linux防护策略，如图8-20所示。

图 8-20 Linux 防护策略管理页面

步骤4 配置Linux防护策略基本信息，如图8-21所示。

版权所有 © 华为技术有限公司

图 8-21 配置 Linux 防护策略

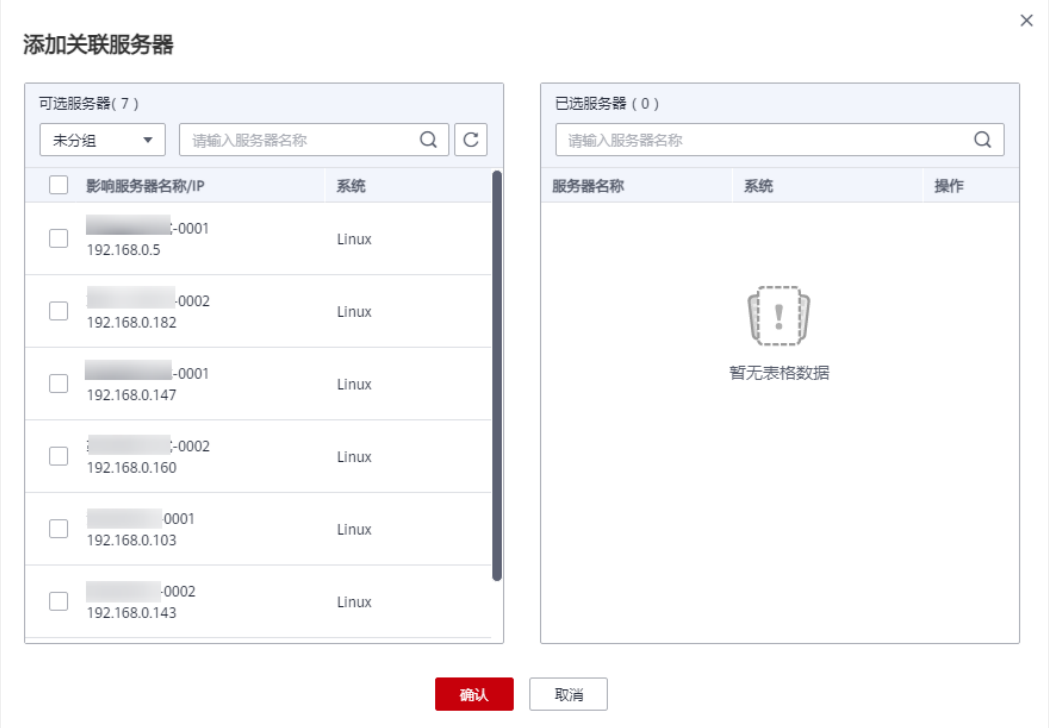
表 8-5 策略基本信息说明

参数	参数说明
策略名称	创建的勒索病毒防护策略的策略名称。
诱饵防护	开启诱饵防护后，HSS将会在关联服务器中预置诱饵文件，帮助您实时诱捕新型未知的勒索病毒。
智能学习天数	请根据您业务的场景选择智能学习的天数，您可以选择“7天”、“15天”或者“30天”。 智能学习功能是通过机器学习引擎学习服务器上的进程修改文件的行为。
防护状态	告警：当检测到对设置的监控路径文件的不可信操作时，触发告警。
监控文件路径	监控的文件的路径，多个文件以分号分隔。监控填写的路径下的文件操作。 例 ： /opt;/opt/sap **说明** 若是防护所有路径，可设置为“--”，但建议配置关键文件的具体路径即可。
扩展名	检测监控路径下包含文件扩展名的所有文件，多个扩展名以分号分隔。 例：sql;txt;sh

步骤5 单击“添加服务器”，在弹出的“添加关联服务器”的窗口中，选择关联服务器，如图8-22所示。

版权所有 © 华为技术有限公司

图 8-22 添加 Linux 关联服务器



步骤6 添加完成关联服务器后，单击“确认”，完成关联服务器的添加。

说明

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

步骤7 完成关联服务器添加后，单击“创建并学习”，完成Linux防护策略的创建。

Linux防护策略创建完成后，该策略的详情将会自动展示在策略管理列表中，如图8-23所示。

图 8-23 Linux 防护策略列表

表 8-6 策略管理列表说明

参数	参数说明
策略名称	创建的智能学习策略的策略名称。
已生效服务器	应用该智能学习策略的服务器数量。

版权所有 © 华为技术有限公司

参数	参数说明
学习中服务器	学习该策略的服务器数量。
可信进程数	智能学习策略生效后，HSS会自动识别您服务器中进程的可信进程，并统计可信进程的数量。
监控文件路径	监控的文件的路径。
扩展名	检测监控路径下包含文件扩展名的所有文件。
防护状态	使用该策略的服务器的防护状态。 告警：当检测到对设置的监控路径文件的不可信操作时，触发告警。
诱饵防护状态	● 开启：诱饵防护为开启状态，HSS在关联服务器中预置诱饵文件，发现未知勒索病毒加密诱饵文件的行为，立即告警。 ● 关闭：诱饵防护为关闭状态。

----结束

创建 Windows 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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“创建策略”，创建Windows防护策略，如图8-24所示。

图 8-24 Windows 防护策略管理页面

步骤4 配置勒索病毒防护策略基本信息，如图8-25所示。

版权所有 © 华为技术有限公司

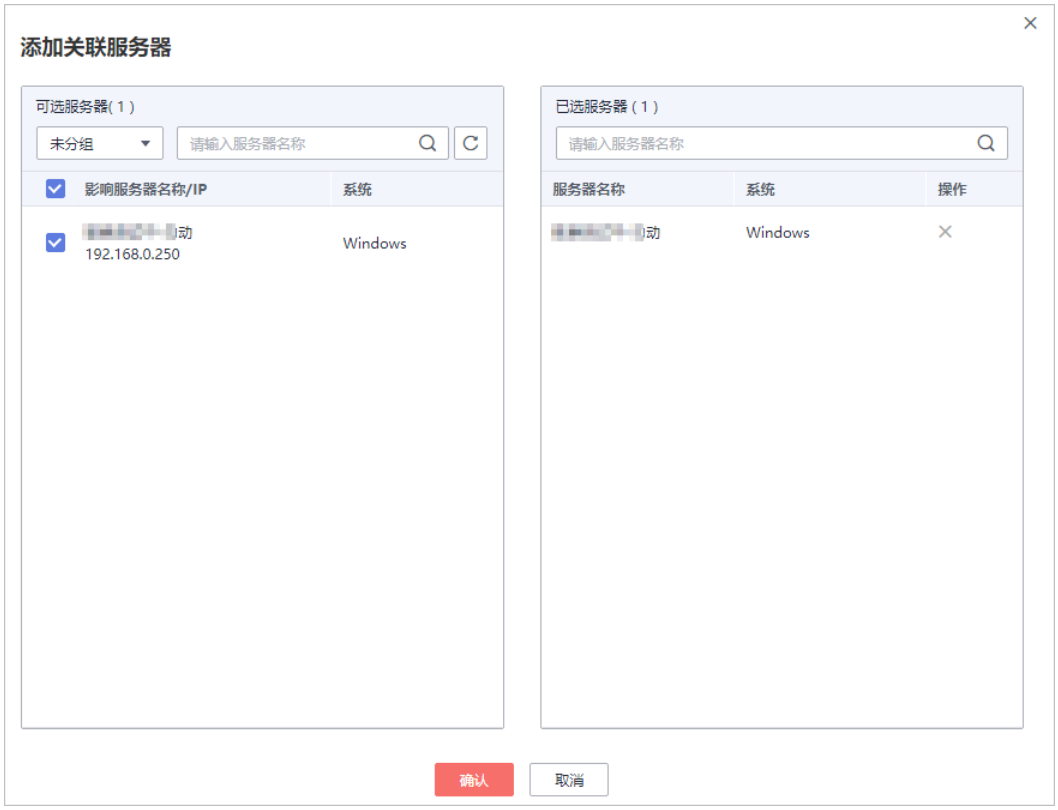
图 8-25 配置 Windows 防护策略

表 8-7 策略基本信息说明

参数	参数说明
策略名称	创建的勒索病毒防护策略的策略名称。
智能学习天数	请根据您业务的场景选择智能学习的天数，您可以选择“7天”、“15天”或者“30天”。 智能学习功能是通过机器学习引擎学习服务器上的进程修改文件的行为。
防护状态	告警：当检测到对设置的监控路径文件的不可信操作时，触发告警。
监控文件路径	监控的文件的路径，多个文件以分号分隔。监控填写的路径下的文件操作。 如果不填写监控文件路径，HSS会监控主机上所有的文件路径。
扩展名	检测监控路径下包含文件扩展名的所有文件，多个扩展名以分号分隔。

步骤5 单击“添加服务器”，在弹出的“添加关联服务器”的窗口中，选择关联服务器，如图8-26所示。

图 8-26 添加 Windows 关联服务器



步骤6 添加完成关联服务器后，单击“确认”，完成关联服务器的添加。

说明

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

步骤7 完成关联服务器添加后，单击“创建并学习”，完成Windows防护策略的创建。

Windows防护策略创建完成后，该策略的详情将会自动展示在策略管理列表中，如图8-27所示。

图 8-27 Windows 防护策略管理列表

版权所有 © 华为技术有限公司

表 8-8 策略管理列表说明

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

----结束

8.3.3 管理防护策略

防护策略创建完成后，通过机器学习引擎学习服务器上的进程修改文件的行为。策略学习完成后，自动应用于关联服务器。

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

说明

防勒索病毒功能在当前版本中为测试使用，可能存在无法完全满足对应能力的情况，您可购买升级后的主机安全（新版）进行使用。

前提条件

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

查看防护策略列表

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“策略管理”，进入防护策略管理列表页面，如图8-28所示。

图 8-28 策略管理列表

表 8-9 防护策略列表说明

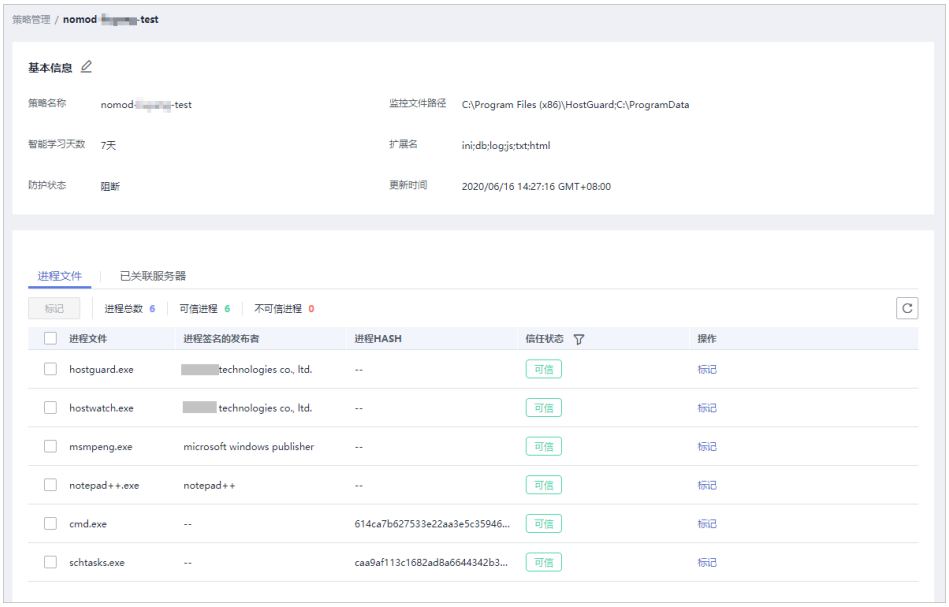
参数	参数说明
策略名称	创建的防护策略的策略名称。
已生效服务器	应用防护策略生效的服务器数量。
学习中服务器	智能学习进行中，自动对关联服务器执行智能学习。新创建的策略状态都为“学习中”。
可信进程数	HSS自动识别关联服务器中的可信进程的数量。
监控文件路径	监控的文件的路径，多个文件以分号分隔。监控该路径下的文件操作。 如果监控文件路径为“--”，表示HSS会监控主机上所有的文件路径。
扩展名	检测监控路径下包含文件扩展名的所有文件。
防护状态	检测到进程文件对监控路径文件扩展名的文件的不可信操作，触发进行告警。
诱饵防护状态	仅Linux防护列表中，包含诱饵防护状态。 ● 开启：诱饵防护为开启状态，HSS在关联服务器中预置诱饵文件，发现未知勒索病毒加密诱饵文件的行为，立即告警。 ● 关闭：诱饵防护为关闭状态。

步骤4 单击策略名称，进入策略详细信息页面，您可以查看策略的“基本信息”和“进程文件”信息，如图8-29所示。

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

版权所有 © 华为技术有限公司

图 8-29 防护策略详情



步骤5 单击“已关联服务器”，查看关联服务器，如图8-30所示。

图 8-30 查看关联服务器

表 8-10 已关联服务器列表

参数	参数说明
服务器名称	服务器的名称。
IP地址	服务器的IP地址。
系统	服务器的操作系统，仅支持防护Windows操作系统。

版权所有 © 华为技术有限公司

参数	参数说明
策略状态	策略的生效状态。包含以下状态： ● 学习中 智能学习进行中。 策略创建完成后，自动对关联服务器执行智能学习。新创建的策略状态都为“学习中”。 ● 学习完成，策略已生效 该策略已完成智能学习，并且已应用到关联服务器中。
操作	可对该策略执行的操作。支持以下操作： ● 重新学习 – 若软件出现重大改版，需要对关联服务器进行重新学习。 请单击“重新学习”，重新对关联服务器进行智能学习。 – 若设置的智能学习天数不够，不能完成机器的智能学习，或者策略学习的时间已超过设置的“智能学习天数”，仍然处于“学习中”状态。 请根据业务场景重新设置“智能学习天数”后，单击“重新学习”，重新对关联服务器进行智能学习。 – 若学习过程中，服务器处于“关机”或者“故障”状态、Agent处于“离线”状态、或者服务器关闭旗舰版防护，学习将会已中断，但策略仍然处于“学习中”，单击“重新学习”，无法对Agent下发任务。 请检查并恢复以上场景，满足服务器“运行中”、Agent“在线”和开启旗舰版防护后，单击“重新学习”，重新对关联服务器进行学习。 ● 删除 删除关联服务器，关联服务器删除后，关联服务器的文件将不再受到该策略的保护。

----结束

编辑防护策略

编辑防护策略后，防护策略需要重新开始学习。

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

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“策略管理”，进入防护策略管理列表页面，如图8-28所示。

图 8-31 策略管理列表

步骤4 单击“编辑”打开“编辑策略”页面，对该策略进行修改。

可修改该策略的策略名称、诱饵防护、智能学习天数、防护状态、监控文件路径和扩展名。

图 8-32 编辑策略

步骤5 单击“确认”，完成策略编辑。

----结束

版权所有 © 华为技术有限公司

管理策略中的关联服务器

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

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“策略管理”，进入防护策略管理列表页面，如图8-28所示。

图 8-33 策略管理列表

步骤4 单击已创建策略的策略名称，进入详情页面，以Linux防护为例，如图8-34所示。

图 8-34 进入策略详情页面

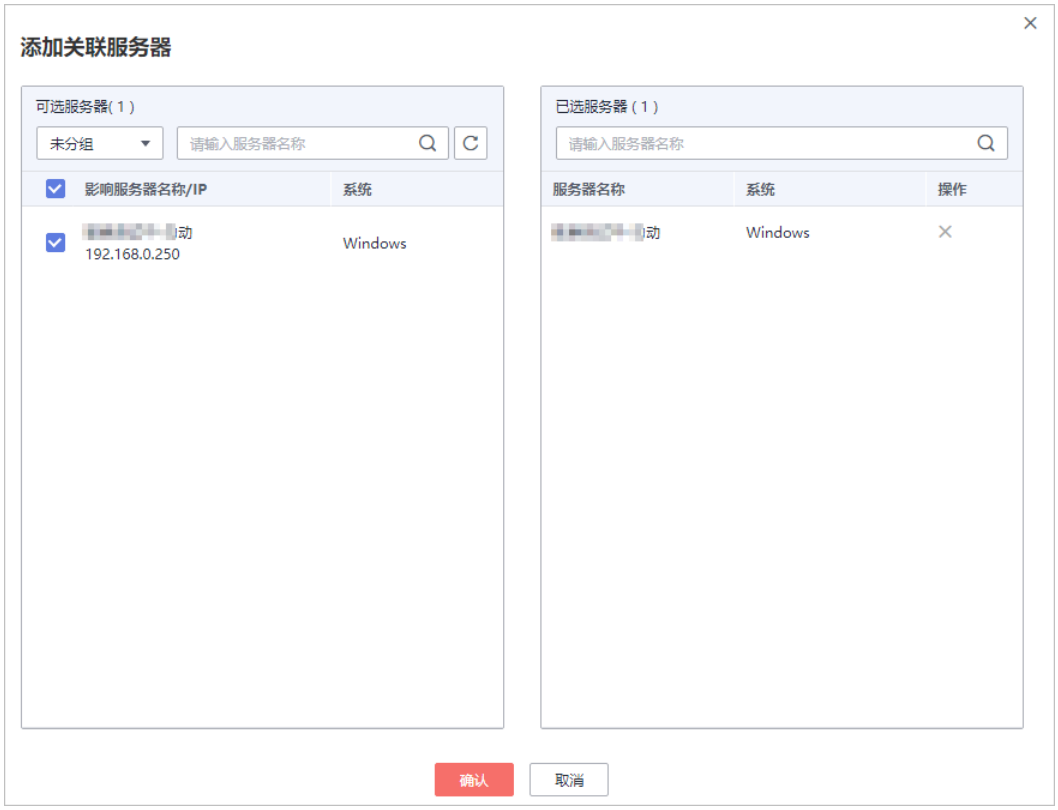
步骤5 选择“关联服务器”，单击“添加服务器”，添加关联的服务器，如图8-35所示。

版权所有 © 华为技术有限公司

图 8-35 添加关联的服务器

步骤6 在弹出的添加服务器窗口中，选择关联的服务器，如图8-36所示。

图 8-36 添加 Windows 关联服务器



步骤7 单击“确认”，完成关联服务器添加。

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

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

----结束

版权所有 © 华为技术有限公司

删除防护策略

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 进入“勒索病毒防护”页面，单击“策略管理”，进入防护策略管理列表页面，如图8-28所示。

图 8-37 策略管理列表

步骤4 单击“删除”，弹出删除策略窗口。

步骤5 单击“确定”，完成策略删除。策略删除后，对应的关联服务器进程将不再受到该策略的保护。

----结束

8.3.4 处理防护告警事件

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

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

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

说明

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

防勒索病毒功能在当前版本中为测试使用，可能存在无法完全满足对应能力的情况，你可购买升级后的主机安全（新版）进行使用。

查看防护告警事件列表

步骤1 登录管理控制台。

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

步骤3 进入“勒索病毒防护”页面，选择“事件管理”页签，查看勒索病毒防护事件列表，如图8-38所示。

图 8-38 勒索病毒防护列表

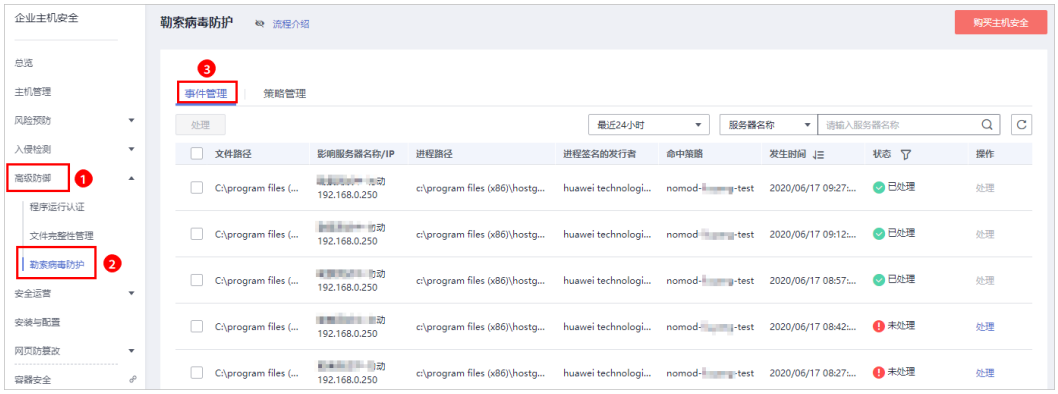


表 8-11 勒索病毒防护列表说明

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

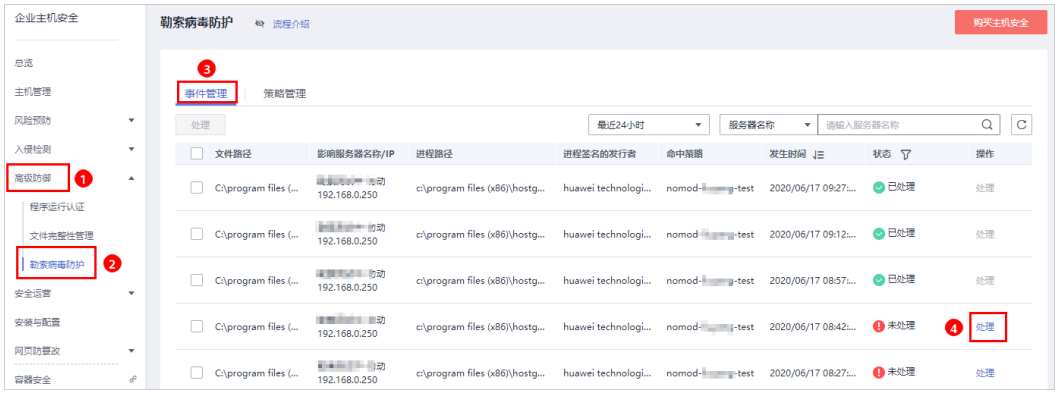
----结束

处理防护告警事件

步骤1 在“事件管理”列表的“操作”列中，单击“处理”，处理勒索病毒防护告警事件，如图8-39所示。

版权所有 © 华为技术有限公司

图 8-39 处理勒索病毒防护告警事件



步骤2 在弹出的处理事件窗口中，选择信任状态“可信”或者“不可信”，处理进程文件操作告警事件，如图8-40所示。

图 8-40 处理勒索病毒防护事件

表 8-12 处理告警事件

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

步骤3 单击“确定”，完成勒索病毒防护告警事件标记处理。

----结束

版权所有 © 华为技术有限公司

9 安全运营

9.1 查看和创建策略组

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

操作须知

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

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

策略列表

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

版权所有 © 华为技术有限公司

策略名称	策略说明	支持的操作系统	企业版	旗舰版	网页防篡改版
资产管理	检测系统中的软件信息，包含软件名称、软件路径、主要应用等，帮助用户识别异常资产。	Linux，Windows	×	√	√
系统配置检测	对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项。	Linux，Windows	×	√	√
高危命令检测	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。	Linux	×	√	√
提权检测	检测当前系统的“进程提权”和“文件提权”操作。 检测以下异常提权操作： ● 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。	Linux	×	√	√
异常/反弹Shell检测	检测系统中异常/反弹Shell的获取行为，包括对shell文件的修改、删除、移动、拷贝、硬链接、访问权限变化。	Linux	×	√	√
文件完整性管理	检测操作系统、应用程序软件和其他组件的文件，确定文件是否发生了可能遭受攻击的更改。	Linux	×	√	√

进入策略管理

步骤1 登录管理控制台。

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

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

----结束

查看策略组列表

步骤1 在“策略管理”界面，查看显示的策略组。如图9-1所示，字段说明如表9-1所示。

说明

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

图 9-1 策略组列表

表 9-1 策略组列表字段说明

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

步骤2 单击策略组名称，进入查看策略组详情界面，可以查看该策略组的策略列表，包括策略名称、状态、功能类别和支持的操作系统，如图9-2所示。

说明

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

版权所有 © 华为技术有限公司

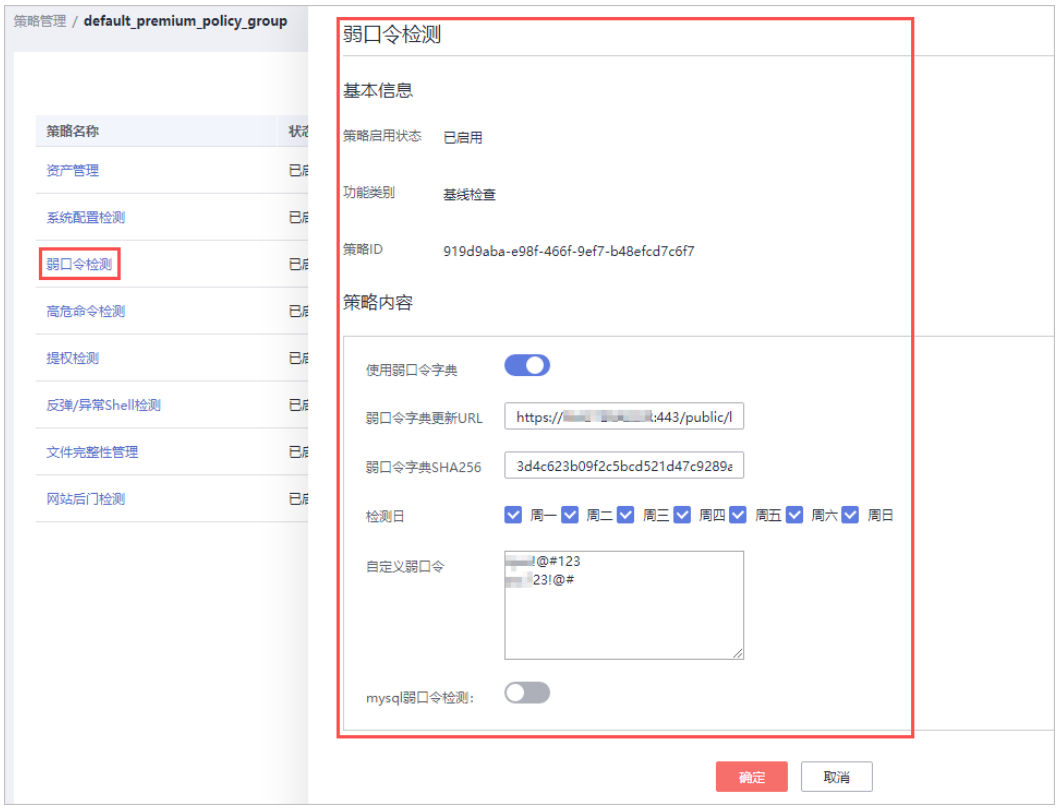
图 9-2 策略组详情

步骤3 单击策略名称，可以查看策略的详情，以弱口令为例，如图9-3所示。

说明

若需要修改策略，请参见修改策略内容。

图 9-3 策略详情

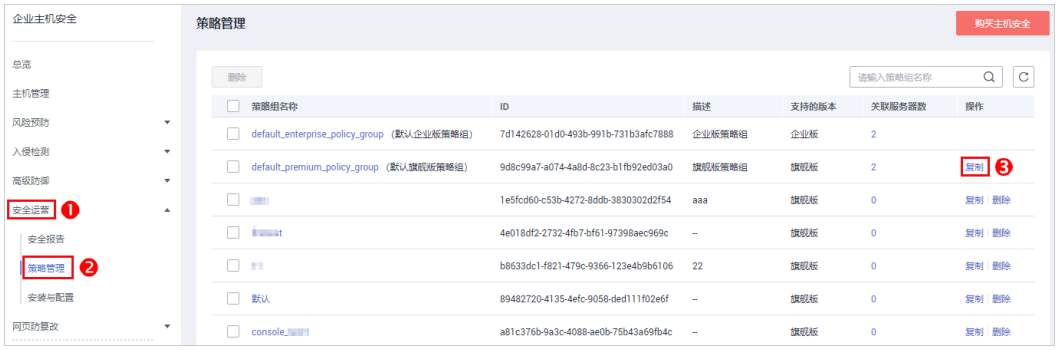


----结束

创建策略组

步骤1 选择“default_premium_policy_group（默认旗舰版策略组）”策略组，在该策略组所在行的操作列中，单击“复制”，如图9-4所示。

图 9-4 复制策略组



步骤2 在弹出的对话框中，输入“策略组名称”和“描述”，如图9-5所示。

说明

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

图 9-5 创建策略组

步骤3 单击“确定”，将会创建一个新的策略组。

步骤4 单击已创建的策略组名称，进入策略组的策略页面，如图9-6所示。

版权所有 © 华为技术有限公司

图 9-6 策略组策略

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

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

----结束

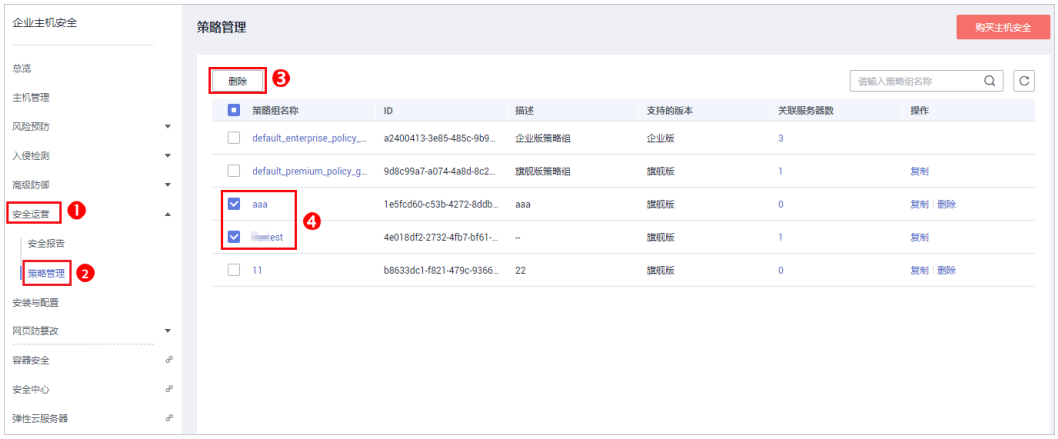
相关操作

删除策略组

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

步骤1 选中需要删除的一个或多个策略组，单击“删除”，如**图9-7**所示。

图 9-7 删除策略组列表



说明

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

步骤2 在弹出对话框中，单击“确定”，完成策略组的删除。

----结束

9.2 修改策略内容

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

须知

策略内容的修改，只在当前所修改的策略组生效。

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 > 企业主机安全”，进入企业主机安全页面。

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

----结束

资产管理

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“资产管理”，弹出资产管理界面。

步骤3 在弹出的资产管理界面中，修改“策略内容”，如图9-8所示，参数说明如表9-2所示。

版权所有 © 华为技术有限公司

图 9-8 资产管理策略

表 9-2 资产管理策略内容参数说明

参数	说明
检测时间	检测的时间，可具体到每一天的每一分钟。
检测日	检测日期，勾选周一到周日的任意日期。
需要获取信息的软件名称	• 软件名称中不能包含空格且内容长度不得超过5000字符，多个软件名称用逗号分隔。 • 如果不配置，则获取所有已安装软件信息。
软件搜索路径	软件搜索的路径。Windows主机不需要添加。

参数	说明
主要应用/组件	● 软件名：软件名称。 ● 软件主程序 ： 软件的主程序。 ● 执行命令 ： 执行的命令。 ● 操作：单击“添加”可以将软件添加到此列表；单击“删除”可以将软件从该列表移除。
获取UDP端口	获取UDP端口信息，检测WEB的目录。 ● ：开启。 ● ：关闭。
检测端口信息的时间间隔（秒）	进程文件检测端口信息的时间间隔，可配置范围为“30秒~86400秒”。

步骤4 单击“确定”，完成修改。

----结束

系统配置检测

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 在策略组列表中，单击“系统配置检测”，弹出系统配置检测界面。

步骤3 在“系统配置检测”界面，修改“修改策略内容”，如图9-9所示，参数说明如表9-3所示。

图 9-9 系统配置检测

表 9-3 系统配置检测策略内容参数说明

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

步骤4 勾选需要检测的操作系统。

步骤5 单击“确定”，完成修改。

----结束

弱口令检测

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

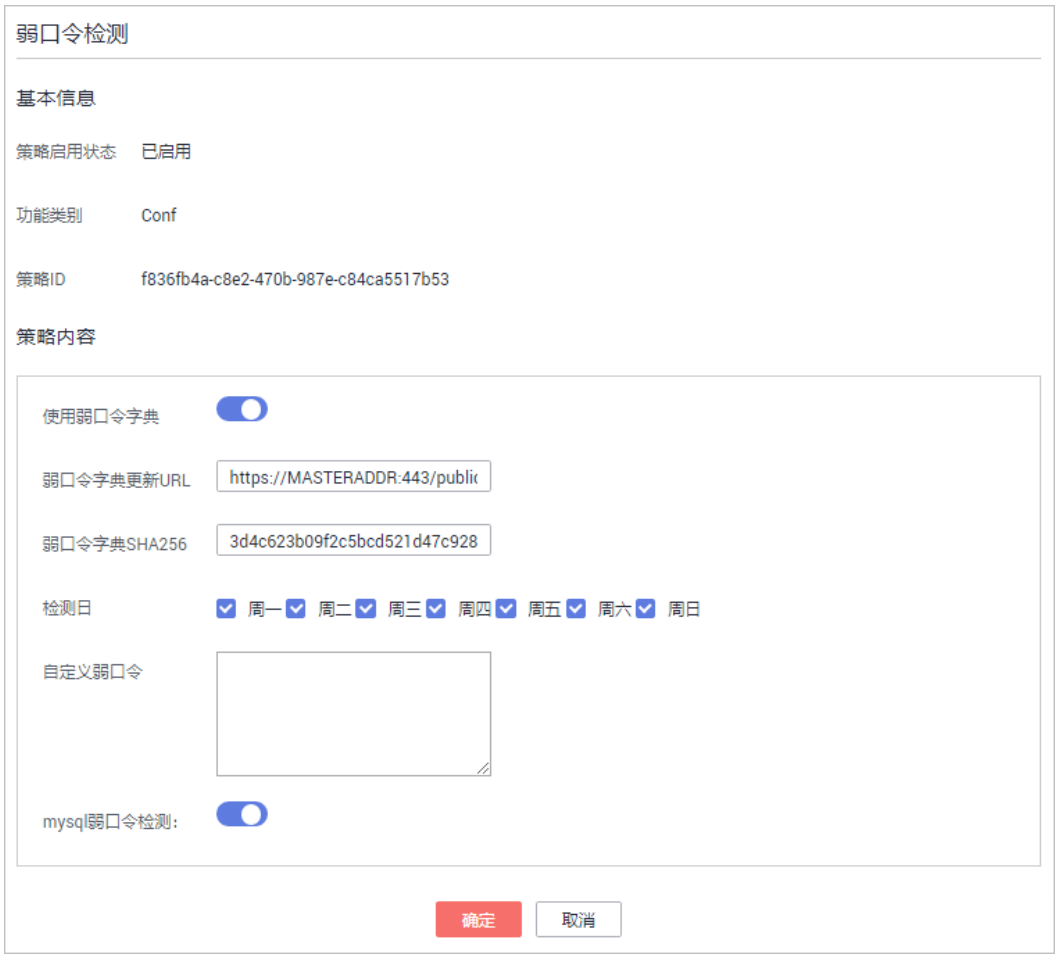
企业主机安全服务会对使用经典弱口令的用户帐号告警，主动检测出主机中使用经典弱口令的帐号。您也可以将疑似被泄露的口令添加在自定义弱口令列表中，防止主机中的帐户使用该弱口令，给主机带来危险。

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

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

步骤3 在弹出的“策略内容”界面中，修改“策略内容”，如图9-10所示，参数说明如表9-4所示。

图 9-10 弱口令检测



版权所有 © 华为技术有限公司

表 9-4 弱口令检测策略内容参数说明

参数	说明
使用弱口令字典	选择是否开启使用弱口令字典。 ● ：开启。 ● ：关闭。
弱口令字典更新URL	弱口令字典更新的网页地址。
弱口令字典SHA256	弱口令字典的SHA256值。
检测日	弱口令检测日期。勾选周一到周日检测弱口令的时间。
自定义弱口令	您可以将疑似被泄露的口令添加在自定义弱口令文本框中，防止主机中的帐户使用该弱口令，给主机带来危险。
MySQL弱口令检测	对登录MySQL的口令进行弱口令检测，您可以选择开启或者关闭MySQL弱口令检测。

步骤4 单击“确定”，完成修改。

----结束

高危命令检测

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“高危命令检测”，弹出高危命令检测界面。

步骤3 在弹出的高危命令检测界面中，修改“策略内容”，如图9-11所示，参数说明如表9-5所示。

图 9-11 高危命令检测内容

表 9-5 高危命令检测策略内容参数说明

参数	说明
上报或记录进程消亡消息	是否开启上报或记录进程消亡消息。 • ：开启。 • ：关闭。

版权所有 © 华为技术有限公司

参数	说明
使用消息通道去重上报	是否开启使用消息通道去重上报。 ● ：开启。 ● ：关闭。
进程统计信息上报间隔（分钟）	开启消息通道去重上报后有效。 配置进程统计信息上报间隔，配置为有效数字。
独立进程最大CPU使用率（%）	开启消息通道去重上报后有效。 配置独立进程最大CPU使用率，可配置范围为“5~99”。
独立进程最大内存使用（MB）	开启消息通道去重上报后有效。 配置独立进程最大内存使用，可配置范围为“50~1024”。
独立进程数据接收方IP和端口	开启消息通道去重上报后有效。 配置独立进程数据接收方IP和端口。
独立进程数据发送限速（KB/S）	开启消息通道去重上报后有效。 独立进程数据发送限速，可配置范围为“1~100”。
精简日志模式	是否开启使用精简日志模式。 ● ：开启。 ● ：关闭。
收集进程网络连接信息	是否开启收集进程网络连接信息。 ● ：开启。 ● ：关闭。
记录日志	是否开启记录日志。 ● ：开启。 ● ：关闭。
日志记录路径	日志记录的路径。
日志记录最大文件大小（MB）	日志记录最大文件的大小，可配置范围“10~1024”。 ● 若日志超过配置的最大文件大小，系统会自动将“.log”文件重命名为“.log.0”，并新建“.log”日志文件，将日志继续写入“.log”文件。 ● 最多存在2个日志文件，若日志再次超过配置的最大文件大小，系统会删除“.log.0”的日志文件，将“.log”日志文件重命名为“.log.0”，并新建“.log”日志文件，将日志继续写入“.log”文件。
高危命令	设置高危命令，一行一个高危命令。

版权所有 © 华为技术有限公司

参数	说明
白名单（不记录/不上报）	● 进程全路径或程序名：进程的完整路径或者程序的名称。 ● 命令行正则表达式 ： 命令行的正则表达式。 ● 操作：单击“添加”可以将进程或者程序添加到此列表；单击“删除”可以将进程或者程序从该列表移除。

步骤4 单击“确定”，完成修改。

----结束

提权检测

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“提权检测”，弹出提权检测界面。

步骤3 在弹出的“提权检测”策略内容中，修改“策略内容”，如图9-12所示，参数说明如表9-6所示。

图 9-12 提权检测

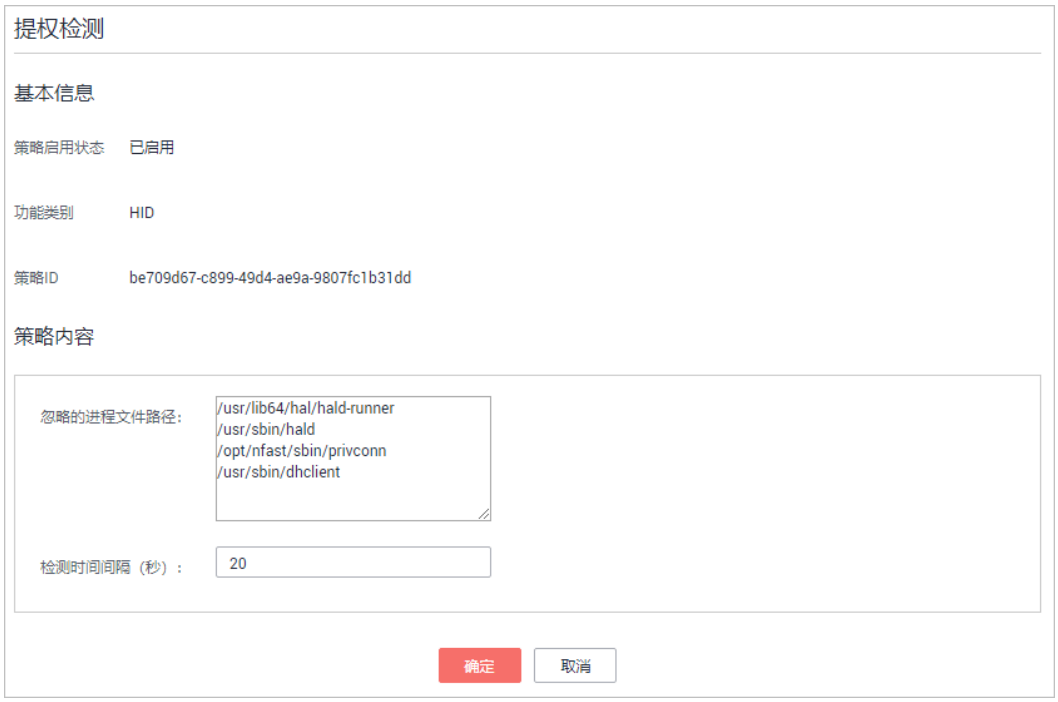


表 9-6 提权检测策略内容参数说明

参数	说明
忽略的进程文件路径	忽略的进程文件的路径。

版权所有 © 华为技术有限公司

参数	说明
检测时间间隔（秒）	进程文件检测时间间隔，可配置范围为“5~3600”。

步骤4 单击“确定”，完成修改。

----结束

异常/反弹 Shell 检测

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“异常/反弹Shell检测”，弹出异常/反弹Shell检测界面。

步骤3 在弹出的异常/反弹Shell检测界面中，修改“策略内容”，如图9-13所示，参数说明如图9-13所示。

图 9-13 异常/反弹 shell 检测

表 9-7 反弹/异常 shell 检测策略内容参数说明

参数	说明
反弹shell忽略的进程文件路径	反弹shell忽略的进程文件的路径。

参数	说明
反弹shell扫描周期（秒）	反弹shell扫描的周期，可配置范围为“30-86400”。
异常shell检测	选择是否开启异常shell检测，建议开启。 • ：开启。 • ：关闭。
进程打开文件上限	进程打开文件的上限数，可配置范围为“10-300000”。

步骤4 单击“确定”，完成修改。

----结束

文件完整性管理

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“文件完整性管理”，弹出关键文件完整性管理界面。

步骤3 在弹出的文件完整性管理界面中，修改“策略内容”，如图9-14所示，参数说明如表9-8所示。

版权所有 © 华为技术有限公司

图 9-14 文件完整性管理

表 9-8 文件完整性管理策略内容参数说明

参数	说明
全量检测时间间隔（秒）	检测配置的所有文件的时间间隔，可配置范围为“3600-100000”。 例如：配置为“3600”，就是间隔一个小时检测一次所有文件。
文件状态检测时间间隔（秒）	文件状态检测周期。可配置范围为“10-600”。
检测休息时间（毫秒）	检测配置的单个文件的时间间隔，可配置范围为“0-1000”。 例如：配置为“50”，检测“/bin/ls”后，等待“50”毫秒再检测“/usr/bin/ls”。

版权所有 © 华为技术有限公司

参数	说明
监控文件	需要检测的文件。 **说明** ● 策略默认添加的文件是非常关键的文件，请谨慎删除！ ● 若删除默认添加的文件，HSS将不会再对该文件发生的变更进行统计。

步骤4 单击“确定”，完成修改。

----结束

网站后门检测

网站后门检测功能只有在设置Web路径之后才会生效。

步骤1 在策略管理列表中，单击待修改的策略组名称，进入策略组界面。

步骤2 单击“网站后门检测”，弹出网站后门检测界面。

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

图 9-15 网站后门检测

版权所有 © 华为技术有限公司

说明

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

表 9-9 网站后门检测策略内容参数说明

参数	说明
自动识别Web目录	请根据需要开启或关闭自动识别Web路径，若缺少目录请进行手动添加。 ● ：开启。 ● ：关闭。
手动添加Web目录	手动添加需要检测的Web目录。 ● 文件路径以“/”开头，不能以“/”结尾。 ● 结尾必须有端口号。 ● 多个路径通过回车换行分隔且名称中不能包含空格。
检查文件后缀	检查文件的后缀，可以检测“jsp”、“jspx”、“jspf”、“php”、“php5”和“php4”。
监测文件修改	是否开启监测文件修改功能。

步骤4 单击“确定”，完成修改。

----结束

9.3 订阅主机安全报告

企业主机安全支持订阅周报和月报，展现每周或每月的主机安全趋势以及关键安全事件与风险。企业主机安全仅保留6个月的安全报告，建议您定期下载，以满足等保测评以及审计的需要。

说明

- 支持Region：香港、曼谷、新加坡。不支持Region：约翰内斯堡、墨西哥城一、圣保罗一、圣地亚哥。
- 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。
- 完成报告订阅后，第二天08：00系统会基于当前订阅时间的周期生成上一个周期的报告，生成后可对上一周期的报告进行查看、下载。

下载主机安全报告

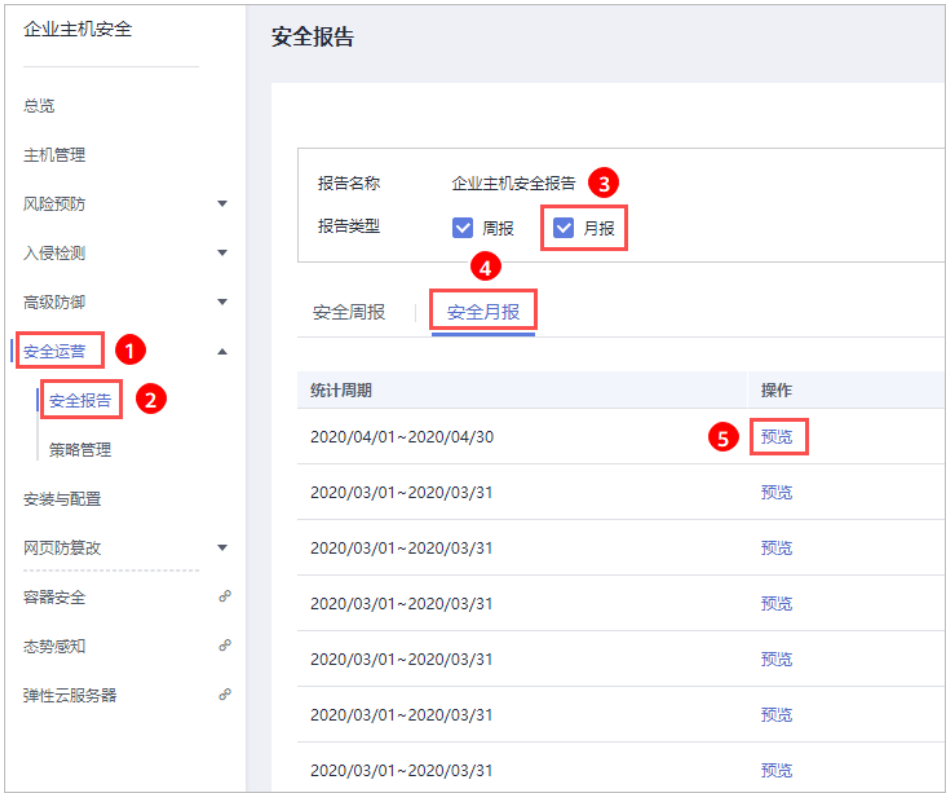
步骤1 登录管理控制台。

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

步骤3 选择“安全报告”页面，单击操作列的“预览”，预览安全周报或月报。

图 9-16 安全周报

图 9-17 安全月报



版权所有 © 华为技术有限公司

步骤4 单击预览页面右侧的“下载”，可下载安全报告到本地。

图 9-18 下载安全报告

----结束

主机安全报告模板说明

企业主机安全支持订阅周报和月报，您可以根据需要下载主机安全的周报或者月报；下载安全报告后，您可以根据HSS的检测结果，了解主机风险状态，并及时对主机风险进行处理。

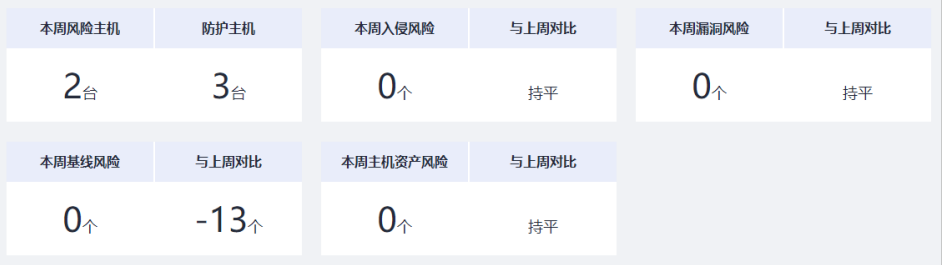
报告模板主要内容包含：风险总览、风险趋势、风险分布、TOP5主机、TOP5暴力破解攻击来源、漏洞统计、资产帐号变动记录、危险开放端口、弱口令、风险帐号、异地登录、恶意程序、网站后门、帐号破解以及关键文件变更。

如下以周报的报告模板为例进行说明。

- 风险总览

  查看本周的风险信息与上周对比的风险情况。

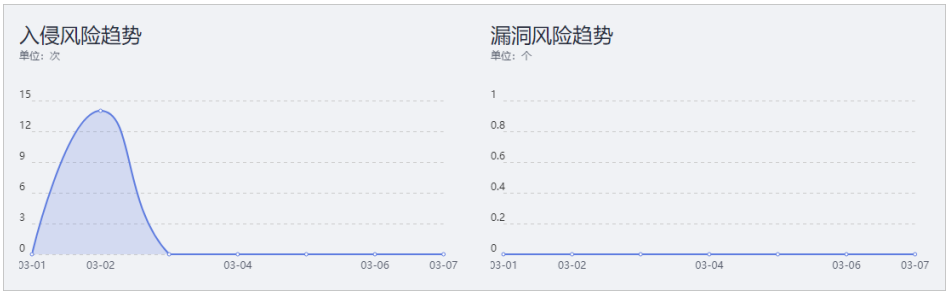
  图 9-19 风险总览信息



- 风险趋势

  查看本周的入侵风险趋势和漏洞风险趋势。

  图 9-20 风险趋势



版权所有 © 华为技术有限公司

- TOP5风险主机和TOP5暴力破解攻击来源

  查看本周的TOP5风险主机和TOP5暴力破解攻击来源。

图 9-21 TOP5 风险主机和 TOP5 暴力破解攻击来源

- 漏洞统计

  查看本周检测出的漏洞统计信息。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-22 漏洞统计信息

漏洞统计

漏洞名称	漏洞类型	修复紧急度	受影响服务器数	最后发现时间	解决方案
2021年2月9日-KB4601318（操作系统内部版本14393.4225）	Windows漏洞	需尽快修复漏洞	1	2021/03/03 14:57:00 GMT+08:00	--
CESA-2020:0540 (sudo security update)	Linux漏洞	可延后修复漏洞	2	2021/03/03 14:56:22 GMT+08:00	Update the affected sudo packages.
CESA-2019:1587 (python security update)	Linux漏洞	可延后修复漏洞	2	2021/03/03 14:56:22 GMT+08:00	Update the affected python packages.
CESA-2020:0375 (kernel security update)	Linux漏洞	可延后修复漏洞	2	2021/03/03 14:56:22 GMT+08:00	Update the affected kernel packages.
CESA-2019:1481 (kernel security update)	Linux漏洞	可延后修复漏洞	2	2021/03/03 14:56:22 GMT+08:00	Update the affected kernel packages.
CESA-2019:1294 (bind security update)	Linux漏洞	可延后修复漏洞	2	2021/03/03 14:56:22 GMT+08:00	Update the affected bind packages.

- 资产帐号变动记录

  查看本周检测出的资产变动记录。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-23 资产帐号变动记录

资产账号变动记录

账号名称	关联服务器	变动状态	管理员权限	发生变动时间
[illegible]	[illegible]	新建	否	2021/03/03 14:55:02 GMT+08:00
zxd	[illegible]	新建	是	2021/03/02 17:54:37 GMT+08:00
zxd2	[illegible]	新建	否	2021/03/02 17:54:37 GMT+08:00

- 危险开放端口

  查看本周检测出的开放的危险端口。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

版权所有 © 华为技术有限公司

图 9-24 开放的危险端口

危险开放端口

本地端口	端口类型	对应主机数	危险程度	状态	端口描述
3388	UDP	1	未知	未处理	非常用端口，请确认
3388	TCP	1	未知	未处理	非常用端口，请确认
3390	TCP	1	未知	未处理	非常用端口，请确认
3390	UDP	1	未知	未处理	非常用端口，请确认
3391	UDP	1	未知	未处理	非常用端口，请确认
3391	TCP	1	未知	未处理	非常用端口，请确认
5050	UDP	1	未知	未处理	非常用端口，请确认
5353	UDP	1	未知	未处理	非常用端口，请确认

- 弱口令

  查看本周检测出的弱口令。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-25 弱口令

弱口令

服务器名称	账号名称	账号类型	弱口令使用时长（单位：天）
[illegible]	[illegible]	系统账号	0

- 风险帐号

  查看本周检测出的风险帐号。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-26 风险帐号

风险账号

账号名称	关联服务器	异常说明	用户组	用户目录	UID/SID	用户启动Shell
[illegible]	[illegible]	该账号的UID为0，但是用户名不是root。	root	/ home/ [illegible]	0	/ bin/ bash

- 异地登录

  查看本周检测出的异地登录。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-27 异地登录

异地登录

服务器名称	登录源IP	登录用户名	登录时间
rasp	[illegible]i([illegible].184.191)	root	2021/03/03 16:31:33 GMT+08:00
rasp	[illegible]([illegible].184.191)	root	2021/03/03 16:31:33 GMT+08:00

- 恶意程序

  查看本周检测出的恶意程序。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

版权所有 © 华为技术有限公司

图 9-28 恶意程序

恶意程序

服务器名称	恶意程序路径	状态	文件权限	运行用户	程序启动时间	隔离查杀时间	描述
rasp	/ root/ inotify_x64	未处理	--	--	--	--	test

- 网站后门

  查看本周检测出的网站后门。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-29 网站后门

网站后门

服务器名称	木马文件路径	状态	发现时间
[illegible]	/ root/ InsightOpsHandler.php	未处理	2021/03/03 15:00:27 GMT+08:00

- 帐号破解

  查看本周检测出的帐号破解。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-30 帐号破解

账号破解

服务器名称	攻击源IP	攻击类型	拦截次数	拦截状态	开始拦截时间	最近拦截时间
[illegible]	10.108.171.189	ssh	12	已解除	2021/01/26 10:31:55 GMT+08:00	2021/03/03 11:41:03 GMT+08:00

- 关键文件变更

  查看本周检测出的关键文件变更。

  最多仅列举20条风险项，详情请登录企业主机安全控制台查看。

图 9-31 关键文件变更

关键文件变更

服务器名称	被更改的关键文件路径	文件修改时间
[illegible]	/etc/passwd	2021/03/03 14:55:01 GMT+08:00
[illegible]	/etc/passwd	2021/03/03 14:55:01 GMT+08:00
rasp	/usr/bin/du	2021/03/02 20:42:03 GMT+08:00
rasp	/usr/bin/du	2021/03/02 20:41:17 GMT+08:00
rasp	/usr/bin/du	2021/03/02 20:41:11 GMT+08:00
rasp	/usr/bin/du	2021/03/02 20:36:43 GMT+08:00

版权所有 © 华为技术有限公司

10 网页防篡改

10.1 添加防护目录

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

约束与限制

- 网页防篡改仅防护“防护目录”下的文件，不防护文件中链接指向的文件。
- 设置本地备份路径时，请设置合法的备份目录，若设置的备份目录不存在，则防篡改不生效。
- 本地备份路径与添加的防护目录不能重叠，否则会导致本地备份失败。
- 备份目录所在磁盘需要有足够的磁盘空间，若备份目录所在磁盘空间不足，会导致防篡改失败。

保护指定目录

步骤1 登录管理控制台。

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

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

步骤4 若主机为Linux系统，“防护模式”选择“保护指定目录”，如图10-1所示。

若主机为Windows系统，不需要选择“防护模式”，请跳过此步骤。

版权所有 © 华为技术有限公司

图 10-1 保护指定目录

步骤5 添加防护目录，您最多可在主机中添加50个防护目录。

1. 单击“添加防护目录”，在弹出的“添加防护目录”对话框中添加防护目录，有关防护规则的详细内容请参见**表10-1**。

图 10-2 添加防护目录

表 10-1 防护规则

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

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

2. 添加完成后，单击“确定”，完成添加防护目录的操作。

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

步骤6 启用远端备份。

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

有关添加远端备份服务器的详细操作，请参见**添加远端备份服务器**。

1. 单击“启动远端备份”。

版权所有 © 华为技术有限公司

图 10-3 开启远端备份

2. 通过下拉框选择备份服务器。

图 10-4 启动远端备份

3. 单击“确定”，启动远端备份。

----结束

相关操作

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

须知

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

版权所有 © 华为技术有限公司

10.2 添加远端备份服务器

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

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

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。

设置远端备份服务器

步骤1 登录管理控制台。

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

步骤3 在“远端备份服务器”页面，单击“添加远端备份服务器”。

图 10-5 远端备份服务器

步骤4 在弹出的对话框中，添加远端备份服务器，相关参数说明请参见表10-2。

版权所有 © 华为技术有限公司

图 10-6 添加远端备份服务器

表 10-2 添加远端备份服务器参数说明

参数名称	说明
地址	该地址为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。 ● 若多个主机的防护目录同时备份在同一远端备份服务器时，备份路径下生成以“Agentid”为目录的文件夹，存放各主机的防护文件，以便用户手动恢复被篡改的网页。 例如：两台主机的防护目录分别为“/hss01”和“hss02”，主机Agentid分别为“f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“f2ddbabc-6cdc-43af-abcd-e4e6f086626f”，设置远端备份路径为“/hss01”。 备份后路径为“/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f”。 ● 若设置为远端备份服务器的主机开启了“网页放篡改”防护，那么该备份路径与自身的“防护目录”不能重叠，否则会导致远端备份失败。

步骤5 单击“确定”，完成添加备份服务器的操作。

----结束

版权所有 © 华为技术有限公司

启动远端备份

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

步骤2 “防护模式”选择“保护指定目录”，单击“启动远端备份”，如图10-7所示。

图 10-7 开启远端备份

步骤3 在“远端备份服务器”下拉框中，选择远端备份服务器。

图 10-8 启动远端备份

步骤4 单击“确定”，启动远端备份。

----结束

相关操作

关闭远端备份

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

10.3 添加特权进程修改防护文件

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

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

版权所有 © 华为技术有限公司

特权进程可以访问被防护的目录，请确保特权进程安全可靠。

每个主机中最多可以添加10个特权进程的路径。

前提条件

- 在“网页防篡改 > 防护列表”页面中“Agent状态”为“在线”、“防护状态”为“开启”。
- 仅Windows系统支持特权进程。

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 > 企业主机安全”，进入企业主机安全页面。

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

步骤4 在“特权进程设置”页面，单击“添加特权进程”。

图 10-9 添加特权进程

步骤5 在弹出的“添加特权进程”对话框中，添加特权进程文件所在的路径。

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

步骤6 特权进程添加完成后，单击“确定”，完成添加特权进程的操作。

说明

若HSS的Agent是2018年8月3日前安装的，请在特权进程添加完成后重启操作系统。

----结束

相关操作

修改或删除已添加的特权进程

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

说明

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

10.4 定时开启网页防篡改

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

说明

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

操作步骤

步骤1 登录管理控制台。

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

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

步骤4 在“定时开关设置”页面，开启定时开关。

图 10-10 定时开关

步骤5 在弹出的对话框中，单击“确定”。

步骤6 设置“关闭防护时间段”和“定时关闭防护频率”。

图 10-11 设置定时防护参数

----结束

版权所有 © 华为技术有限公司

关闭防护时段设置规则

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

10.5 开启动态网页防篡改

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

前提条件

主机为Linux操作系统。

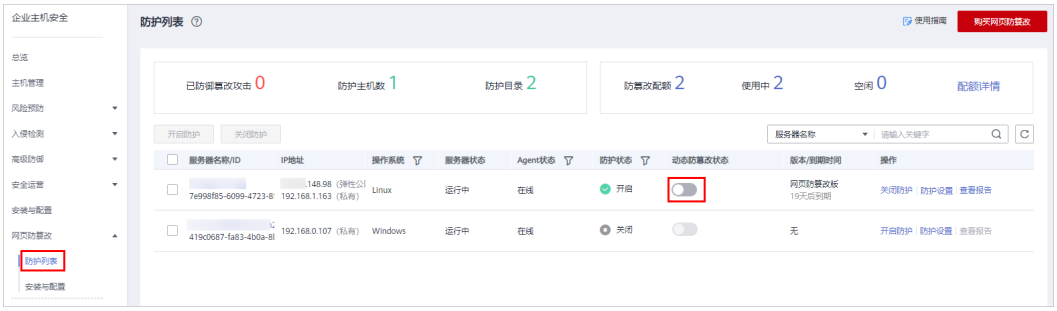
操作步骤

步骤1 登录管理控制台。

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

步骤3 在“网页防篡改 > 防护列表”页面，单击目标主机所在行的“动态防篡改状态”列的 。

图 10-12 开启动态网页防篡改



说明

您也可以单击“防护设置 > 动态网页防篡改”，进入动态网页防篡改页签；在动态网页防篡改页签，单击 ，开启动态网页防篡改。

步骤4 在弹出“开启动态网页防篡改”窗口中，单击“确定”，开启动态网页防篡改。

步骤5 动态网页防篡改开启后，还需重启Tomcat才能使其生效。

版权所有 © 华为技术有限公司

当您关闭动态网页防篡改，再重新开启后，仍需要重启Tomcat才能使其生效。

----结束

10.6 查看网页防篡改报告

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

前提条件

云服务器的“Agent状态”为“在线”且“防护状态”为“开启”。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在“网页防篡改 > 防护列表”页面，单击“查看报告”。

图 10-13 查看防护记录

步骤4 在防护记录界面，查看防护记录详情。

图 10-14 静态网页防篡改防护记录

版权所有 © 华为技术有限公司

图 10-15 动态网页防篡改防护记录

----结束

版权所有 © 华为技术有限公司

11 管理防护配额

11.1 查看配额

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

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

企业版/旗舰版配额

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在“主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。

图 11-1 查看主机安全防护配额

版权所有 © 华为技术有限公司

步骤4 在防护配额页面，查看主机安全防护配额，以及使用该配额的服务器名称。

表 11-1 参数说明

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

说明

- 绑定主机

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

  一个配额只能绑定一个主机，且只能绑定agent在线的主机。

- 续费

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

- 解绑配额

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

----结束

网页防篡改配额

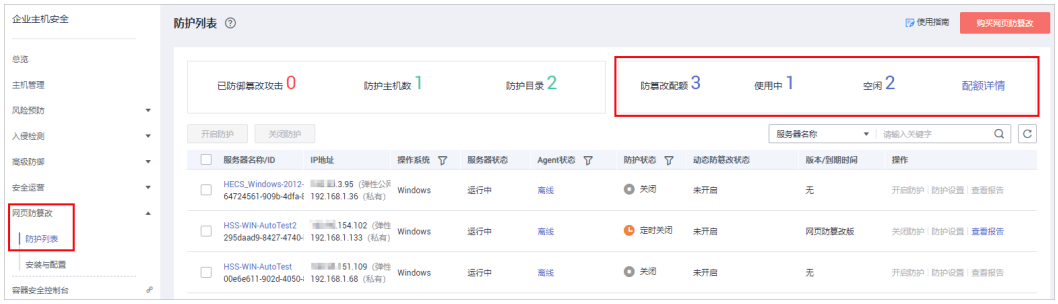
步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“网页防篡改”，进入网页防篡改的防护列表界面。

版权所有 © 华为技术有限公司

图 11-2 查看企业主机安全“网页防篡改版”防护配额



步骤4 单击“配额详情”，进入网页防篡改防护配额详细信息页面。

图 11-3 配额详情

步骤5 在网页防篡改防护配额页面，查看防护配额详细信息。

表 11-2 参数说明

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

版权所有 © 华为技术有限公司

说明

- 绑定主机

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

  一个配额只能绑定一个主机，且只能绑定Agent在线的主机。

- 续费

  您可以在需要续费的网页防篡改配额所在行的操作列，单击“续费”，为购买的网页防篡改续费。详细操作请参见如何续费。

- 退订

  您可以在需要退订的网页防篡改配额所在行的操作列，单击“退订”，退订购买的网页防篡改。详细操作请参见如何退订。

- 解绑配额

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

----结束

11.2 绑定主机

一个配额只绑定一个主机，且只能绑定agent在线的主机。

前提条件

- 主机已安装agent。
- 购买的防护配额的“配额状态”为“正常”，“使用状态”为“空闲”。

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在“主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。

版权所有 © 华为技术有限公司

图 11-4 查看主机安全防护配额

步骤4 在防护配额列表页面，单击“绑定主机”，为空闲配额绑定主机。

说明

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

图 11-5 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。

版权所有 © 华为技术有限公司

图 11-6 选择绑定的主机

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

11.3 升级配额版本

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

若您有网页防篡改版的业务需求，您需要参照购买防护配额重新购买。

前提条件

- 已购买“基础版”或者“企业版”防护配额。
- 待升级的防护配额的“配额状态”为“正常”，“使用状态”为“空闲”。
- 多个防护配额同时升级时，请确保待升级的防护配额为相同的版本。

升级版本

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航栏中，选择“主机管理 > 防护配额”，勾选待升级的配额，单击“升级规格”，如图11-7所示。

图 11-7 升级规格

步骤4 在“主机安全配额升级规格”页面，设置升级后的规格。

1. 选择升级后的规格

   支持升级为“企业版”、“旗舰版”。版本之间的差异请参见**服务版本差异**。

   请根据您已购买的版本，选择升级后的规格。

   - “基础版”

     可以升级为“企业版”、“旗舰版”。
   - “企业版”

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

       请先进行移除或者续订。
     - 若主机安全配额处于“使用中”状态，无法进行升级操作。

       在不影响业务场景的情况下，您可以选择“允许升级时了关闭防护”，或者移除。

       说明

       升级规格时关闭防护可能会造成当前云服务器业务中断，请谨慎操作。

步骤5 在页面右下角，单击“立即购买”，进入“详情”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，请阅读并勾选“我已阅读并同意《企业主机安全免责声明》”。

步骤7 单击“去支付”，进入“付款”页面，付款后，完成主机安全配额的升级规格操作。

----结束

版权所有 © 华为技术有限公司

11.4 解绑配额

解绑配额后，HSS会关闭主机防护，无法检测主机存在的潜在风险，请谨慎操作。

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

解绑机制

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

前提条件

主机已绑定配额。

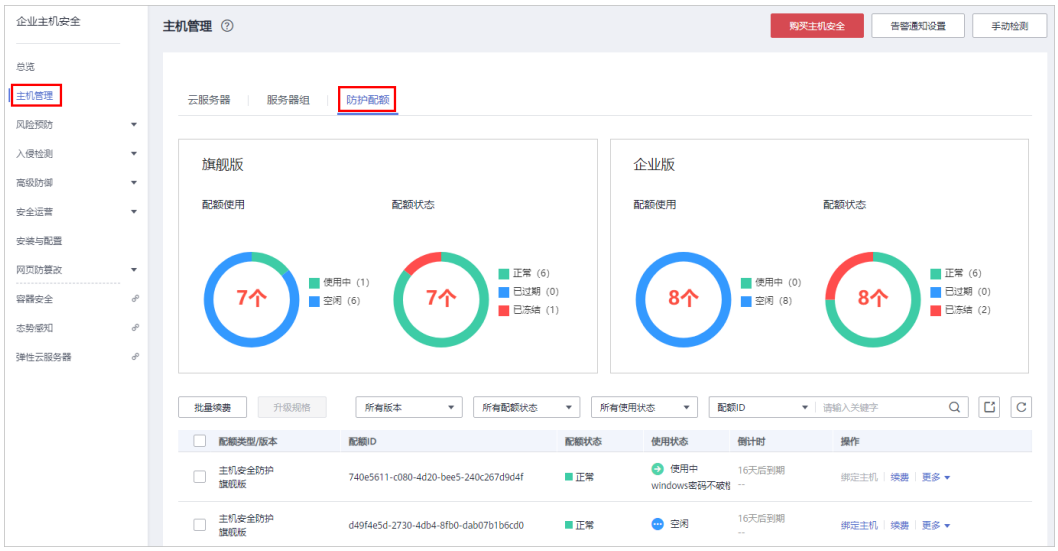
解绑基础版/企业版/旗舰版配额

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在“主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。

图 11-8 查看主机安全防护配额



步骤4 在防护配额列表页面，选择“更多”，单击“解绑配额”，解除绑定的配额，如图11-9所示。

版权所有 © 华为技术有限公司

图 11-9 解绑配额

说明

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

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

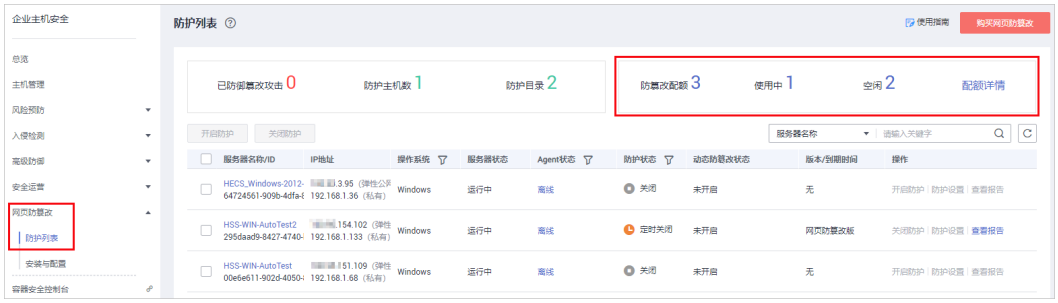
解绑网页防篡改配额

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 在左侧导航树中，选择“网页防篡改”，进入网页防篡改的防护列表界面。

图 11-10 查看企业主机安全“网页防篡改版”防护配额



步骤4 单击“配额详情”，进入网页防篡改防护配额详细信息页面。

图 11-11 配额详情

版权所有 © 华为技术有限公司

步骤5 在防护配额列表页面，选择“更多”，单击“解绑配额”，解除绑定的配额，如图11-12所示。

图 11-12 解绑网页防篡改配额

说明

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

步骤6 在弹出的解绑配额对话框中，单击“确定”，解除绑定。

----结束

版权所有 © 华为技术有限公司

12 （可选）管理企业项目

12.1 管理项目和企业

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

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

- 授权

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

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。

  – 购买企业主机安全时选择企业项目

    在购买页面，“企业项目”下拉列表中选择目标企业项目，实现资源与企业项目关联。

  – 资源迁入

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

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

  更多信息，请参阅《企业管理用户指南》。

12.2 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、登录白名单、恶意程序自动隔离查杀和告警通知等。

- 部署策略组

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

  “所有项目”中的策略组独立于其他每一个企业项目的策略组，与其他企业项目的策略组互不干扰。

- 订阅所有项目安全报告

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

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

前提条件

拥有Tenant Administrator权限，或者HSS Administrator+Tenant Guest权限。

绑定主机配额

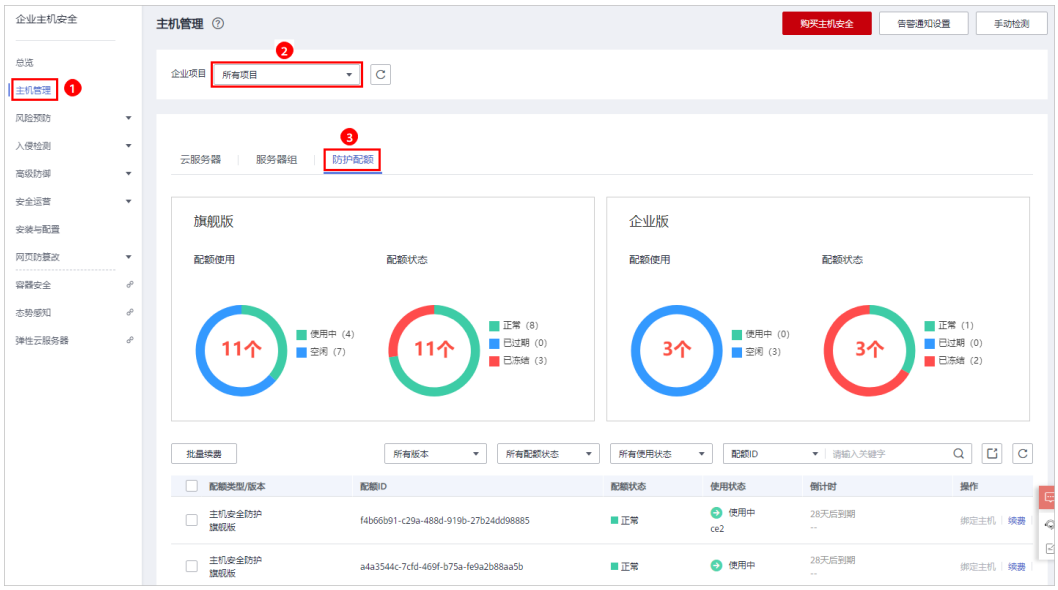
如下，以在“所有项目”中为任意一个企业项目的主机绑定“主机安全旗舰版配额”为例说明。

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 > 企业主机安全”，进入企业主机安全页面。

步骤3 选择“主机管理 > 所有项目 > 防护配额”，进入“防护配额”页面，在防护配额页面，您可以查看到所有项目的防护配额，如图12-1所示。

图 12-1 防护配额页面



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。

图 12-2 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。

版权所有 © 华为技术有限公司

图 12-3 绑定配额

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

批量安全配置

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

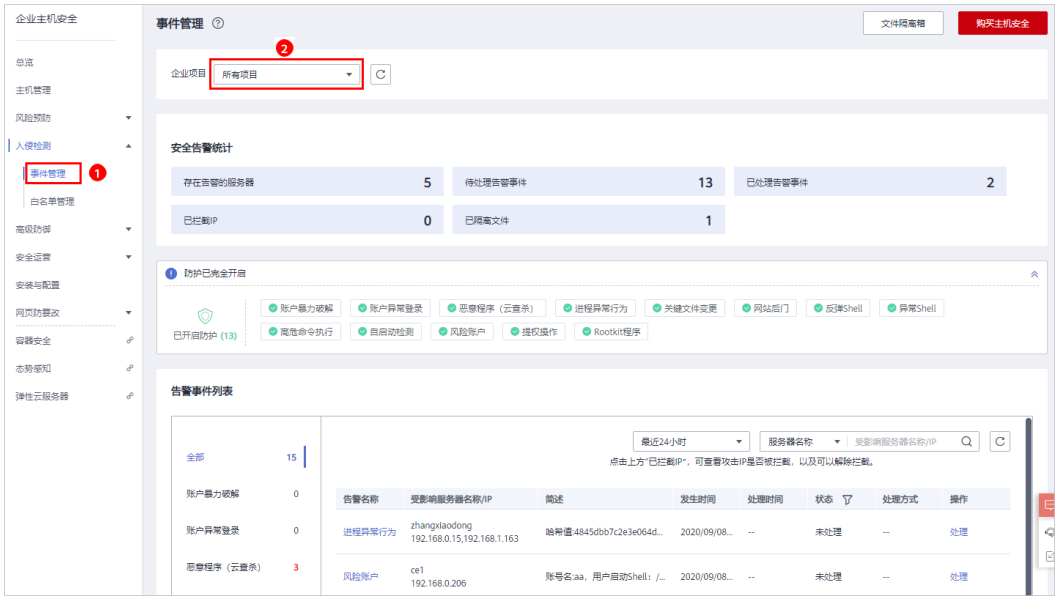
须知

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

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

步骤1 选择“入侵检测 > 事件管理”，进入事件管理页面。

图 12-4 事件管理页面



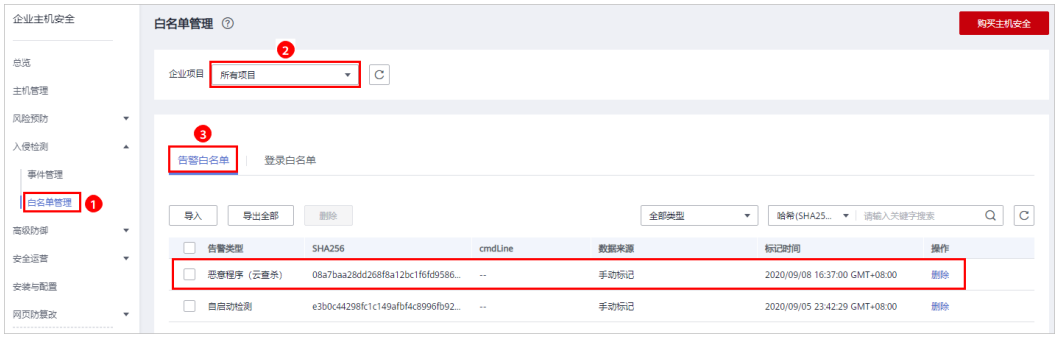
步骤2 在“企业项目”下拉列表中，选择“所有项目”。

步骤3 在告警事件列表中，以“恶意程序（云查杀）”为例，将“恶意程序（云查杀）”加入告警白名单，如图12-5所示。

图 12-5 加入告警白名单

步骤4 选择“白名单管理 > 所有项目 > 告警白名单”，进入告警白名单页面。

图 12-6 告警白名单页面



步骤5 在“企业项目”下拉列表中，分别选择“企业项目一”和“企业项目二”，查看“恶意程序（云查杀）”均已分别添加到“企业项目一”和“企业项目二”下的告警白名单中。

图 12-7 企业项目一告警白名单

步骤6 若“企业项目二”中需要HSS对添加的“恶意程序（云查杀）”事件进行告警，您可以在“企业项目二”中将添加的告警白名单删除。

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

----结束

部署策略组

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

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

步骤1 选择“安全运营 > 策略管理 > 所有项目”，单击“复制”，在所有项目中，创建策略组。

图 12-8 复制默认策略组

步骤2 在弹出的窗口中，输入策略组名称，例如“hss_test”，如图12-9所示。

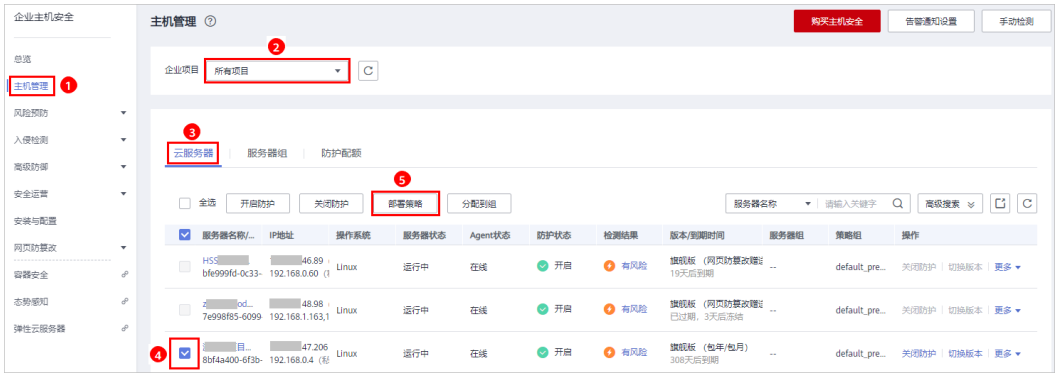
图 12-9 配置策略组

步骤3 单击“确定”，完成策略组的创建。

您可以根据您的需要单击策略组的名称，配置策略组。

步骤4 选择“主机管理 > 所有项目”，选择任意一台开启旗舰版防护的主机，单击“部署策略”，为主机部署创建的“hss_test”策略组。

图 12-10 部署自定义策略



步骤5 在弹出的窗口中，选择策略组，如图12-11所示。

图 12-11 选择待部署的策略组

步骤6 单击“确定”，完成策略组的部署。

----结束

订阅所有项目的安全报告

选择“安全报告 > 所有项目”，勾选“周报”、“月报”，订阅周报和月报。

图 12-12 订阅所有项目安全报告

版权所有 © 华为技术有限公司

13 审计

13.1 支持云审计的 HSS 操作列表

企业主机安全通过云审计服务（Cloud Trace Service，CTS）为用户提供云服务资源的操作记录，记录内容包括用户从管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果，供用户查询、审计和回溯使用。

云审计服务支持的HSS操作列表如表13-1所示。

表 13-1 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
开启主机安全防护	hss	openHssProtect
关闭主机安全防护	hss	closeHssProtect
手动检测	hss	manualDetection
解除封禁IP	hss	unblockIp
设置常用登录地	hss	setCommonLocation
设置登录IP白名单	hss	setWhiteIpList
启用或停用登录IP白名单	hss	switchWhiteIpList
忽略端口	hss	ignorePort
取消忽略端口	hss	noIgnorePort
忽略配置风险	hss	ignoreConfigRisky
取消忽略配置风险	hss	notIgnoreConfigRisky
一键修复漏洞	hss	repairVul
验证漏洞	hss	verifyVul
一键修复待重启确认	hss	confirmVul

版权所有 © 华为技术有限公司

操作名称	资源类型	事件名称
忽略软件漏洞	hss	ignoreVul
取消忽略软件漏洞	hss	notIgnoreVul
开启防火墙	HSS	turnonFirewall
网页防篡改开启防护	HSS	openWtp
网页防篡改关闭防护	hss	stopWtp
网页防篡改添加防护目录	hss	addWtpDir
网页防篡改删除防护目录	hss	deleteWtpDir
网页防篡改修改防护目录	hss	modifyWtpDir
网页防篡改暂停防护目录	hss	suspendWtpDir
网页防篡改恢复防护目录	hss	resumeWtpDir
网页防篡改设置备份服务器	hss	setWtpBackupHost
网页防篡改设置远端备份	hss	setWtpRemoteBackup
网页防篡改添加特权进程	hss	addWtpPrivilegedProcess
网页防篡改删除特权进程	hss	deleteWtpPrivilegedProcess
网页防篡改修改特权进程	hss	modifyWtpPrivilegedProcess
开启双因子认证	hss	turnOnTwoFactor
关闭双因子认证	hss	turnOffTwoFactor
修改双因子认证主题	hss	modifyTwoFactorTopic
忽略网站后门	hss	ignoreWebShell
取消忽略网站后门	hss	notIgnoreWebShell
卸载客户端	hss	unInstall
网页防篡改设置保护模式	hss	setProtectMode
网页防篡改添加被保护文件系统	hss	addFileSystem

操作名称	资源类型	事件名称
网页防篡改删除被保护文件系统	hss	delFileSystem
网页防篡改修改被保护文件系统	hss	modifyFileSystem
网页防篡改暂停被保护文件系统	hss	suspendFileSystem
网页防篡改恢复被保护文件系统	hss	resumeFileSystem
网页防篡改开启定时停止防护功能	hss	turnonTimedStopProtect
网页防篡改关闭定时停止防护功能	hss	turnoffTimedStopProtect
网页防篡改设置定时停止防护执行周期	hss	setTimedStopDate
网页防篡改添加停止防护时间段	hss	addTimerRange
网页防篡改修改停止防护时间段	hss	modifyTimerRange
网页防篡改删除停止防护时间段	hss	delTimerRange
设置网页防篡改告警	hss	setWtpAlertConfig
开启动态网页防篡改	hss	turnonRasp
关闭动态网页防篡改	hss	turnoffRasp
订阅安全报告	hss	subSafetyReport
开启恶意程序自动隔离查杀	hss	turnOnMPAutomatic
关闭恶意程序自动隔离查杀	hss	turnOffMPAutomatic
导入告警白名单	hss	importAlarmWhitelist
删除告警白名单	hss	deleteAlarmWhitelist
导出告警白名单	hss	exportAlarmWhitelist
操作登录白名单	hss	operateLoginWhitelist
事件管理操作	hss	operateEventStatus
文件隔离箱中恢复	hss	deleteProcessIsolationRule
修改策略组	hss	modifyPolicyGroup

操作名称	资源类型	事件名称
删除策略组	hss	deletePolicyGroup
复制策略组	hss	copyPolicyGroup
修改策略组内容	hss	modifyPolicyContent
部署策略	hss	deployPolicyGroup
添加服务器组	hss	addHostGroup
删除服务器组	hss	deleteHostGroup
修改服务器组	hss	modifyHostGroup
加入服务器组	hss	insertHostGroup
开启或关闭文件文整性管理	hss	switchKeyfiles
程序运行认证事件操作	hss	operateAppWhiteListEvent
创建白名单策略	hss	replaceAppWhiteListPolicy
开启或关闭白名单策略	hss	switchAppWhiteListPolicy
删除白名单策略	hss	deleteAppWhiteListPolicy
白名单策略标记应用程序	hss	operateAppWhiteListPolicyApp
删除生效服务器	hss	deleteAppWhiteListHostInfo
关联生效服务器	hss	addAppWhiteListHostInfo
勒索病毒防护事件操作	hss	operateAppRansomEventInfo
勒索病毒防护创建、编辑策略	hss	replaceAppRansomPolicyInfo
勒索病毒防护删除策略	hss	deleteAppRansomPolicyInfo
勒索病毒防护标记进程状态	hss	operateAppRansomHashInfo
勒索病毒防护删除服务器	hss	deleteAppRansomHostInfo
勒索病毒防护添加服务器	hss	addAppRansomHostInfo
勒索病毒防护已关联服务器重新学习	hss	relearnAppRansomHostInfo

13.2 查看审计日志

开启了云审计服务后，系统开始记录HSS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 HSS 的云审计日志

步骤1 登录管理控制台。

步骤2 单击页面上方的☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。

  在下拉框中选择查询条件。
  - “事件类型”选择“管理事件”。
  - “事件来源”选择“HSS”。
  - “筛选类型”选择“事件名称”时，还需选择某个具体的事件名称；选择“资源ID”时，还需选择或者手动输入某个具体的资源ID；选择“资源名称”时，还需选择或手动输入某个具体的资源名称。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- “事件级别”：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- “时间范围”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

步骤5 单击“查询”，查看对应的操作事件。

步骤6 在需要查看的记录左侧，单击∨展开该记录的详细信息，展开记录如图13-1所示。

图 13-1 展开记录

步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图13-2所示，显示了该操作事件结构的详细信息。

图 13-2 查看事件

查看事件


```
{
    "project_id": "63661f4fa990431eb79a308709b5d660",
    "context": {
        "request": "{\"X-Auth-Token\":\"MIIakAYJKoZIhvcNAQcCoIIagTCCGn0CAQExDTALBglghkgBZQMEAgEwghiiBgkqhkiG9w0BBwG
        "code": "200",
        "source_ip": "[redacted]",
        "trace_type": "ConsoleAction",
        "event_type": "system",
        "project_id": "63661f4fa990431eb79a308709b5d660",
        "trace_id": "8235bfe1-1759-11ea-9718-891dd39b46ec",
        "trace_name": "manualDetection",
        "resource_type": "hss",
        "trace_rating": "warning",
        "api_version": "v1",
        "service_type": "HSS",
        "response": "{}",
        "tracker_name": "system",
        "time": "1575548378373",
        "record_time": "1575548379231",
        "request_id": "d1a98cd8-ff03-4d90-b283-b14e5fe9ed08",
        "user": {
            "name": "[redacted]",
            "id": "06a022904380105f1fb6c010bf36c684",
            "domain": {
                "name": "[redacted]",
                "id": "0c264ba0cefb48c0a9674fee0c6e144f"
```


----结束

14 权限管理

14.1 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，在您的华为云帐号中，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、高效的其他华为云帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果华为云帐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14-1**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14-1**所示。

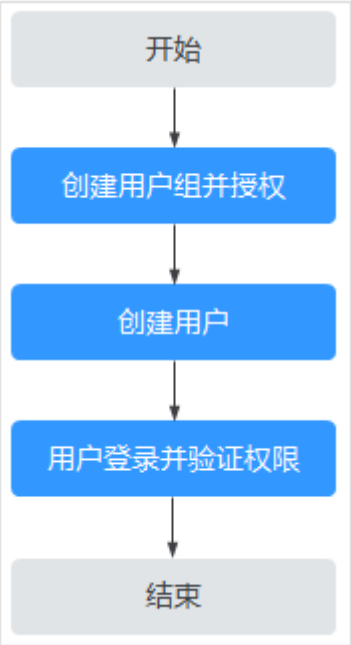
版权所有 © 华为技术有限公司

表 14-1 HSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
HSS Administrator	企业主机安全服务（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和BSS Administrator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。
HSS FullAccess	企业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。
HSS ReadOnlyAccess	企业主机安全服务的只读访问权限。	系统策略	无

示例流程

图 14-1 给用户授权服务权限流程



版权所有 © 华为技术有限公司

1. 创建用户组并授权。

   在IAM控制台创建用户组，并授予HSS服务的管理员权限“HSS Administrator”。

2. 创建用户并加入用户组。

   在IAM控制台创建用户，并将其加入1中创建的用户组。

3. 用户登录并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在“服务列表”中选择除企业主机安全外（假设当前策略仅包含“HSS Administrator”）的任一服务，若提示权限不足，表示“HSS Administrator”已生效。

14.2 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"
            ]
        }
    ]
}
```

14.3 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），如果华为云帐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。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如

果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

说明

“√”表示支持，“x”表示暂不支持。

企业主机安全服务（HSS）支持的自定义策略授权项如下所示：

授权列表

权限	授权项	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
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	-	√	√
查询帐户破解防护报告	hss:accountCracks:list	-	√	√
帐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	IAM项目(Project)	企业项目(Enterprise Project)
批量操作漏洞	hss:vuls:operate	-	√	√
查询帐号信息列表	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	-	√	√
查询风险帐号检测报告	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	-	√	√

版权所有 © 华为技术有限公司

权限	授权项	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
设置登录IP白名单	hss:whiteIps:set	-	√	√
查询登录IP白名单	hss:whiteIps:list	-	√	√
设置自定义弱口令	hss:weakPwds:set	-	√	√
查询自定义弱口令	hss:weakPwds:get	-	√	√
设置Web路径	hss:webDirs:set	-	√	√
查询Web路径	hss:webDirs:get	-	√	√
查询双因子认证服务器列表	hss:twofactorAuth:list	-	√	√
设置双因子认证	hss:twofactorAuth:set	-	√	√
开启或关闭恶意程序自动隔离查杀	hss:automaticKillMp:set	-	√	√
查询恶意程序自动隔离查杀	hss:automaticKillMp:get	-	√	√
订阅安全报告	hss:safetyReport:set	-	√	√
查询安全报告	hss:safetyReport:list	-	√	√
查询包周期配额	hss:quotas:get	-	√	√
购买配额	hss:quotas:set	-	√	√
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	-	√	√

版权所有 © 华为技术有限公司

权限	授权项	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
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	-	√	√

版权所有 © 华为技术有限公司

权限	授权项	依赖的授权项	IAM项目(Project)	企业项目(Enterprise Project)
设置网页防篡改告警	hss:wtpAlertConfig:set	-	√	√
查询网页防篡改告警	hss:wtpAlertConfig:get	-	√	√
查询网页防篡改统计信息	hss:wtpDashboard:get	-	√	√
查询策略组信息	hss:policy:get	-	√	√
设置策略组信息	hss:policy:set	-	√	√
查询程序运行认证	hss:ars:get	-	√	√
设置程序运行认证	hss:ars:set	-	√	√
查询入侵检测事件列表	hss:event:get	-	√	√
入侵检测事件操作	hss:event:set	-	√	√
查询服务器分组信息	hss:hostGroup:get	-	√	√
设置服务器组	hss:hostGroup:set	-	√	√
文件完整性管理	hss:keyfiles:set	-	√	√
查询关键文件变更报告	hss:keyfiles:list	-	√	√
查询自启动列表	hss:launch:list	-	√	√

版权所有 © 华为技术有限公司

A 修订记录

发布日期	修改说明
2022-05-26	第三十四次正式发布。 新增Agent升级操作指导。
2022-04-25	第三十三次正式发布。 优化、新增内容如下： ● 基础版使用及能力的说明。 ● 配置白名单的场景说明。 ● 收到告警信息不代表已被破解入侵的说明。
2022-01-27	第三十二次正式发布。 新增审计内容章节如下： **支持云审计的HSS操作列表** **查看审计日志**
2021-12-30	第三十一次正式发布。 修改内容如下： **（可选）步骤三：设置告警通知**，新增消息中心和消息主题的说明。 **安全配置**，新增主题设置的手机号码或邮箱个数限制的说明。 **步骤一：购买防护配额**，新增基础版本的场景说明。 **升级配额版本**：配额升级不支持升级至网页防篡改版。
2021-08-03	第三十次正式发布。 ● **步骤一：购买防护配额**，优化相关内容描述。 ● **安全配置**，新增配置SSH登录白名单说明和双因子认证使用约束条件。
2021-07-14	第二十九次正式发布。 ● **步骤一：购买防护配额**，优化相关内容描述。 ● **基础版/企业版/旗舰版**，优化相关内容描述。

版权所有 © 华为技术有限公司

发布日期	修改说明
2021-06-08	第二十八次正式发布。 ● 资产管理，新增开放端口检测时间。 ● 查看漏洞详情，新增漏洞更新时间。
2021-05-08	第二十七次正式发布。 Windows版本，console新增Agent安装包下载链接，可直接复制页面下载链接，登录服务器后通过IE浏览器访问下载。
2021-02-25	第二十六次正式发布。 （可选）步骤三：设置告警通知，修改设置告警通知，可以不开启告警通知，直接开启主机安全防护。
2021-01-26	第二十五次正式发布。 新增（可选）步骤五：切换主机安全版本。
2020-12-29	第二十四次正式发布。 勒索病毒防护，增加Linux系统勒索病毒防护。
2020-12-24	第二十三次正式发布。 查看主机防护列表，云服务器列表“高级搜索”中增加通过“防护计费模式”和“服务器计费模式”搜索符合条件的主机。
2020-12-08	第二十二次正式发布。 新增管理防护配额。
2020-11-16	第二十一次正式发布。 Linux版本和Windows版本，将“支持跨区域使用”修改为“不支持跨区域使用”。
2020-10-15	第二十次正式发布。 ● 基础版/企业版/旗舰版，新增告警通知项说明。 ● 告警事件概述，新增关键文件监控路径。 ● 查看和处理入侵告警事件，新增告警处理建议。
2020-09-21	第十九次正式发布。 新增管理所有项目。
2020-06-19	第十八次正式发布。 ● 新增程序运行认证。 ● 新增勒索病毒防护。 ● 新增管理项目和企业。 ● 步骤一：购买防护配额，增加“企业项目”选项说明。 ● 查看主机防护列表，“高级搜索”增加可以通过“服务器状态”进行搜索主机。

版权所有 © 华为技术有限公司

发布日期	修改说明
2020-06-05	第十七次正式发布。 ● 步骤四：开启主机防护，新增绑定主机防护配额自动开启防护，以及解绑主机防护配额。 ● 基础版/企业版/旗舰版，新增“消息中心”发送消息。 ● 漏洞修复与验证，新增一键修复、验证功能。
2020-05-18	第十六次正式发布。 ● 查看主机防护列表，新增支持高级搜索功能。 ● 配置告警白名单，新增导入/导出告警白名单。 ● 文件完整性管理，关键文件校验功能变更为文件完整性管理。 ● 购买网页防篡改版赠送旗舰版。
2020-04-09	第十五次正式发布。 新增以下章节： ● 创建服务器组 ● 部署策略 ● 查看和处理入侵告警事件 ● 管理文件隔离箱 ● 配置告警白名单 ● 配置登录白名单 ● 程序运行认证 ● 关键文件校验 ● 查看和创建策略组 ● 修改策略内容 ● HSS自定义策略 ● HSS授权项说明
2019-12-18	第十四次正式发布。 ● 安全配置，新增SSH登录IP白名单支持IPv6地址。 ● 新增订阅主机安全报告。
2019-09-04	第十三次正式发布。 优化目录结构。
2019-08-09	第十二次正式发布。 支持非华为云主机。
2019-07-19	第十一次正式发布。 优化产品介绍目录结构，方便用户查阅。
2019-07-03	第十次正式发布。 根据界面变化更新截图。

版权所有 © 华为技术有限公司

发布日期	修改说明
2019-03-28	第九次正式发布。 **添加防护目录**，更新了截图和相关描述。
2019-02-28	第八次正式发布。 根据界面变化更新截图。
2019-01-17	第七次正式发布。 根据界面变化更新截图。
2018-11-29	第六次正式发布。 ● **设置告警通知**，更新了截图及描述。 ● **安全配置**，更新了截图及描述。
2018-10-25	第五次正式发布。 **主机风险总览**，更新了截图及描述。
2018-09-27	第四次正式发布。 ● **漏洞管理**，更新了截图及描述。 ● **资产管理**，更新了截图及描述。
2018-09-15	第三次正式发布。 ● **入侵检测**，更新了截图及描述。 ● **资产管理**，更新了截图及描述。 ● **基线检查**，更新了截图及描述。
2018-08-30	第二次正式发布。 增加“恶意程序检测”。
2018-08-16	第一次正式发布。

版权所有 © 华为技术有限公司