主机安全服务

常见问题

文档版本 49

发布日期 2022-08-30

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 产品咨询

1.1 什么是企业主机安全?

企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过资产管理、漏洞管理、基线检查、入侵检测、程序运行认证、文件完整性校验、安全运营、网页防篡改等功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

工作原理

在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

企业主机安全服务的工作原理如图1-1所示。

图 1-1 工作原理

企业主机安全服务的组件功能及工作流程说明如下：

表 1-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	● 使用AI、机器学习和深度算法等技术分析主机中的各项安全风险。 ● 集成多种杀毒引擎，深度查杀主机中的恶意程序。 ● 接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。 ● 接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面。
Agent	● Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：**443**。 ● 每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。 ● 根据您配置的安全策略，阻止攻击者对主机的攻击行为。 **说明** ● 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。 ● Agent可安装在华为云弹性云服务器（Elastic Cloud Server，ECS）/裸金属服务器（Bare Metal Server，BMS）、线下主机以及第三方云主机中。 ● 根据操作系统版本选择对应的安装命令/安装包进行安装。 ● 网页防篡改与主机安全共用同一个Agent，您只需在同一主机安装一次。

1.2 哪些区域可以使用 HSS?

以下区域支持HSS服务：

- 华北-北京一
- 华北-北京四
- 华东-上海一
- 华东-上海二
- 华南-广州
- 西南-贵阳一

仅在以下区域，您才可以接入非华为云主机：

- 华北-北京一
- 华东-上海二

- 华南-广州
- 华北-北京四

表 1-2 配额购买场景

主机类型	如何购买配额
华为云弹性云服务器ECS 华为云裸金属服务器BMS 华为云云耀云服务器	请在ECS/BMS/HECS所在区域购买HSS配额。
第三方云主机	请在“华北-北京一”、“华东-上海二”、“华南-广州”、“华北-北京四”这四个区域购买HSS配额，然后使用非华为云主机的安装方式，将主机接入配额所在区域。
线下主机	

1.3 如何使用企业主机安全服务?

如使用企业主机安全请按照如下步骤进行操作：

步骤1 购买防护配额。

请购买对应版本的防护配额。

步骤2 安装Agent。

- 安装Agent后，您才能开启企业主机安全服务。
- 基础版、企业版和网页防篡改版共用一个Agent。

步骤3 （可选）设置告警通知。

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。

步骤4 开启主机防护。

- Agent安装成功后，您可以为主机开启安全防护。
- 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，该配额可被分配给其他的主机使用。

步骤5 查看检测结果并处理相关风险。

----结束

1.4 企业主机安全支持版本升级吗?

企业主机安全支持版本升级。

升级版本

如果您已购买“基础版”或者“企业版”防护配额，且您当前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”或者“网页防篡改版”。

详细信息请参见**升级版本规格**。

切换版本

基础版、企业版、旗舰版和网页防篡改版是独立的版本，如果各版本有充足的配额，你可以通过“切换版本”的方式切换使用的防护配额。

- 如果购买了充足的基础版、企业版、旗舰版配额。可以通过“切换版本”的方式在版本间轻松切换。

  您可以在“管理控制台 > 主机管理 > 云服务器”页面，在“操作”列中，单击“开启防护”，为主机切换为基础版、企业版或者旗舰版主机安全防护。

  详情请参见**开启基础版/企业版/旗舰版防护**章节的版本切换。
- 如果没有基础版、企业版或者旗舰版对应的配额，请根据需要**购买配额**。
- 如果待开启“网页防篡改”防护的主机已开启基础版/企业版/旗舰版主机安全防护，如需使用“网页防篡改版”，请先关闭基础版/企业版/旗舰版主机安全防护，购买“网页防篡改版”主机安全配额后，选择并**开启网页防篡改版**主机安全防护。

  购买网页防篡改版时赠送旗舰版，开启网页防篡改防护时会同步开启旗舰版防护。

1.5 HSS 是否支持防护本地 IDC 服务器?

支持。

若您的本地服务器能连接到公网，就可以使用企业主机安全对其进行防护。

1.6 HSS 是否和其他安全软件有冲突?

企业主机安全可能会和“DenyHosts”、“网防G01”或“360安全卫士服务器版”冲突。

Agent 软件可能与“DenyHosts”有冲突

详情请参见：**Agent是否和其他安全软件有冲突?**

双因子认证功能可能与“网防 G01”或“360 安全卫士服务器版”冲突

开启企业主机安全服务的Windows主机，在使用双因子认证功能时，可能会和“网防G01”软件或360安全卫士服务器版的登录认证功能产生冲突，您可以根据实际情况，选择使用华为云企业主机安全服务的双因子认证功能、“网防G01”或“360安全卫士服务器版”的登录认证功能。

1.7 HSS 与 CodeArts Inspector、WAF 有什么区别?

华为云提供的HSS、CodeArts Inspector、WAF服务，帮助您全面从主机、网站、Web应用等层面防御风险和威胁，提升系统安全指数。建议三个服务搭配使用。

表 1-3 HSS、CodeArts Inspector、WAF 的区别

服务名称	所属分类	防护对象	功能差异
企业主机安全（HSS）	主机安全	提升主机整体安全性。	● 资产管理 ● 漏洞管理 ● 入侵检测 ● 基线检查 ● 网页防篡改
漏洞管理服务（CodeArts Inspector）	应用安全	提升网站整体安全性。	● 多元漏洞检测 ● 网页内容检测 ● 网站健康检测 ● 基线合规检测
Web应用防火墙（WAF）	应用安全	保护Web应用程序的可用性、安全性。	● Web基础防护 ● CC攻击防护 ● 精准访问防护

1.8 HSS 可以跨帐号使用吗?

不支持帐号与帐号之间共享使用。

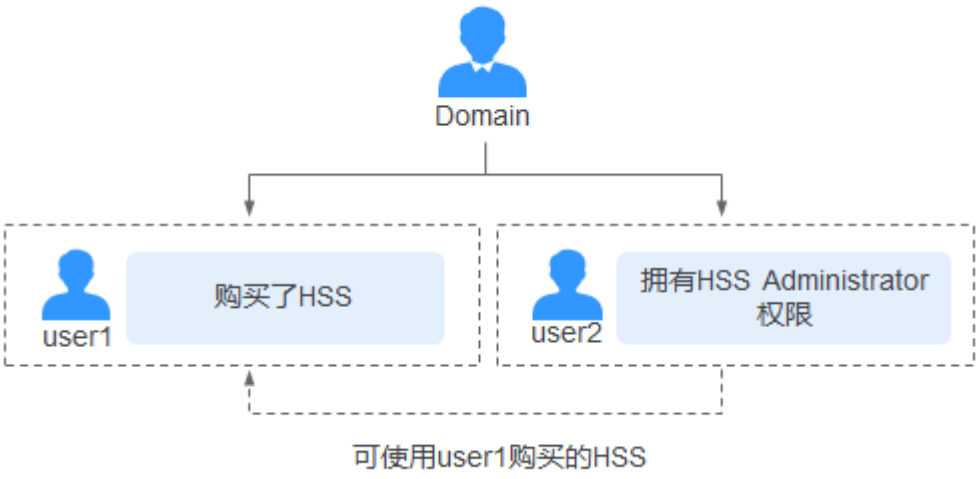
若您未开通企业项目，支持同一帐号下多个IAM用户、及帐号与该帐号下IAM用户共享使用。

同一帐号下多个 IAM 用户共享使用

例如：您创建了1个帐号（“Domain”），“Domain”下有2个IAM用户（“user1”和“user2”）。

当“user1”购买了HSS，如果“user2”授权了HSS Administrator权限，则“user2”也可以使用HSS。

图 1-2 同一帐号下多个 IAM 用户共享使用



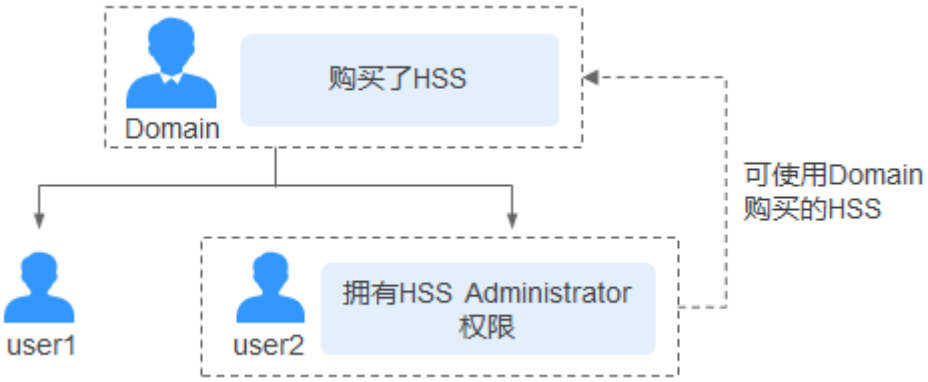
有关HSS权限管理的详细操作，请参见**创建用户并授权使用HSS**。

帐号与该帐号下的 IAM 用户共享使用

例如：您创建了1个帐号（“Domain”），“domain”帐号下有1个IAM用户（“user2”）。

- 当“Domain”购买了HSS，如果“user2”授权了HSS Administrator权限，则“user2”也可以使用HSS。

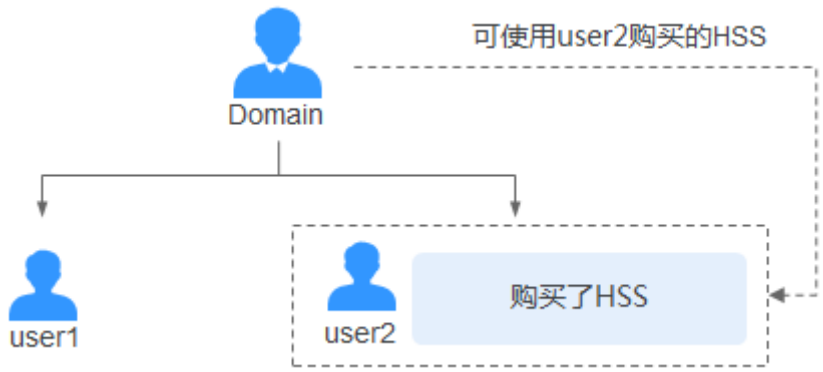
  图 1-3 帐号与该帐号下的 IAM 用户共享使用（1）

  有关HSS权限管理的详细操作，请参见**创建用户并授权使用HSS**。

- 当“user2”购买了HSS，则“Domain”也可以使用HSS。

图 1-4 帐号与该帐号下的 IAM 用户共享使用（2）



1.9 什么是 HSS 的 Agent?

Agent是企业主机安全服务（Host Security Service，HSS）提供的Agent，用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。

Agent分为Linux版本和Windows版本，您需要根据主机的OS版本，选择对应版本进行安装。主机上**安装Agent**，并**开启HSS防护**后，即可获得HSS提供的主机防护功能。

Agent 的作用

- 每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息上报给云端防护中心。
- 根据您配置的安全策略，阻止攻击者对主机的攻击行为。

说明

- 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。
- Agent可安装在华为云弹性云服务器（Elastic Cloud Server，ECS）/裸金属服务器（Bare Metal Server，BMS）/云耀云服务器（Hyper Elastic Cloud Server，HECS）、线下主机以及第三方云主机中。
- 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。

Linux Agent 相关进程

Agent进程运行帐号：root。

Agent包含以下进程：

表 1-4 Linux Agent 包含以下进程

Agent进程名称	进程功能	进程所在路径
hostguard	该进程用于系统的各项安全检测与防护、Agent进程的守护和监控。	/usr/local/hostguard/bin/hostguard
upgrade	该进程用于Agent版本的升级。	/usr/local/hostguard/bin/upgrade

Windows Agent 相关进程

Agent进程运行帐号：system。

Agent包含以下进程：

表 1-5 Windows Agent 包含以下进程

Agent进程名称	进程功能	进程所在路径
HostGuard.exe	该进程用于系统的各项安全检测与防护。	C:\Program Files (x86)\HostGuard \HostGuard.exe
HostWatch.exe	该进程用于Agent进程的守护和监控。	C:\Program Files (x86)\HostGuard \HostWatch.exe
upgrade.exe	该进程用于Agent升级。	C:\Program Files (x86)\HostGuard\upgrade.exe

1.10 HSS 可以跨区域使用吗?

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。

1.11 业务不在华为云上，是否可以使用 HSS?

支持将HSS的Agent安装在华为云ECS服务器、BMS服务器、线下主机以及第三方主机中，您可以集中管理同一区域内多样化部署的主机。

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。

非华为云主机需要能通过公网IP访问华为云，才能接入HSS。请根据您的操作系统安装Agent，并接入HSS。

安装 Linux Agent

登录待安装Agent非华为云主机，使用安装命令在线安装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。

图 1-5 企业主机安全

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 1-6 复制安装 Agent 的命令

步骤4 远程登录待安装Agent的非华为云主机。

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
```

----结束

安装 Windows Agent

有两种安装方式，以下步骤演示方式一。

- 方式一：下载企业主机安全服务的Agent，上传至待安装Agent的云主机后，在云主机中安装Agent。
- 方式二：登录待安装Agent的云主机，在云主机中登录华为云管理控制台，下载并安装Agent。

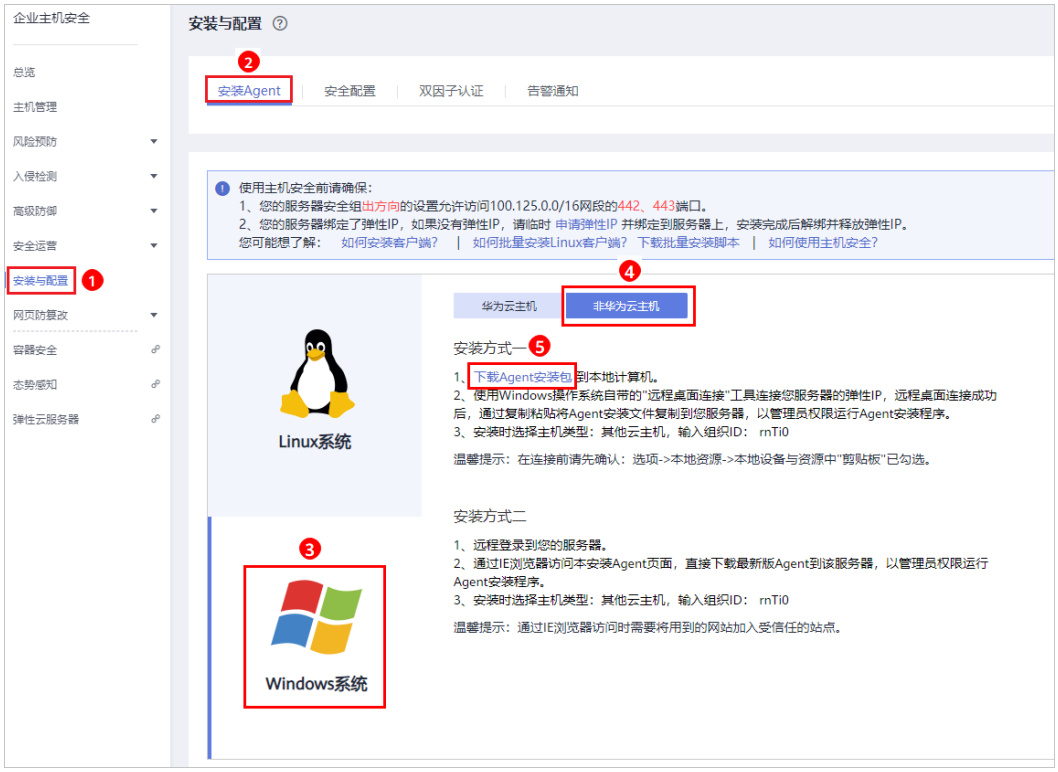
步骤1 登录管理控制台。

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。

图 1-7 企业主机安全

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。

图 1-8 安装 Windows Agent



步骤4 远程登录待安装Agent的非华为云主机。

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。

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1-9所示。

图 1-9 选择主机类型（非华为云主机）

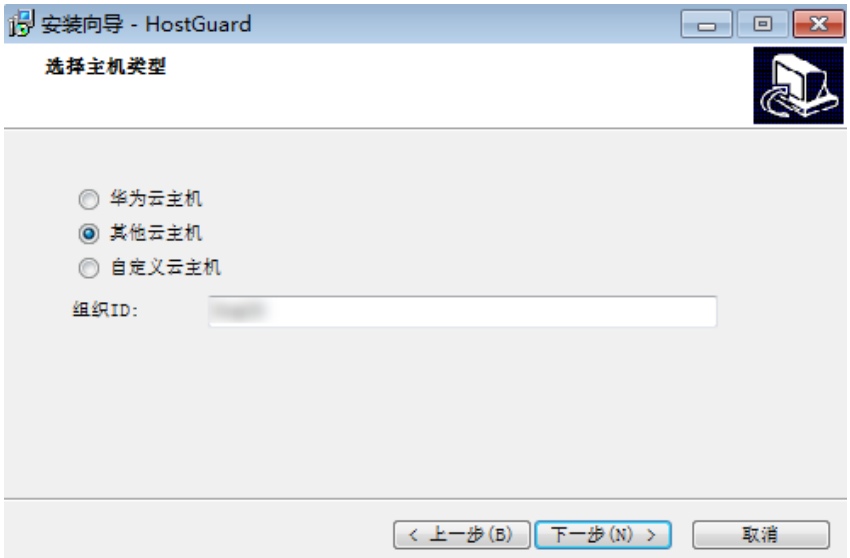
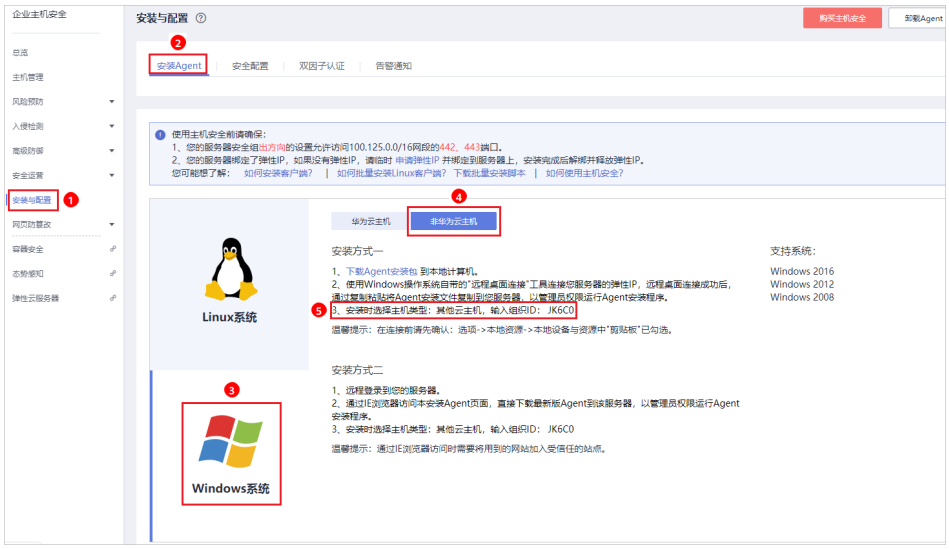


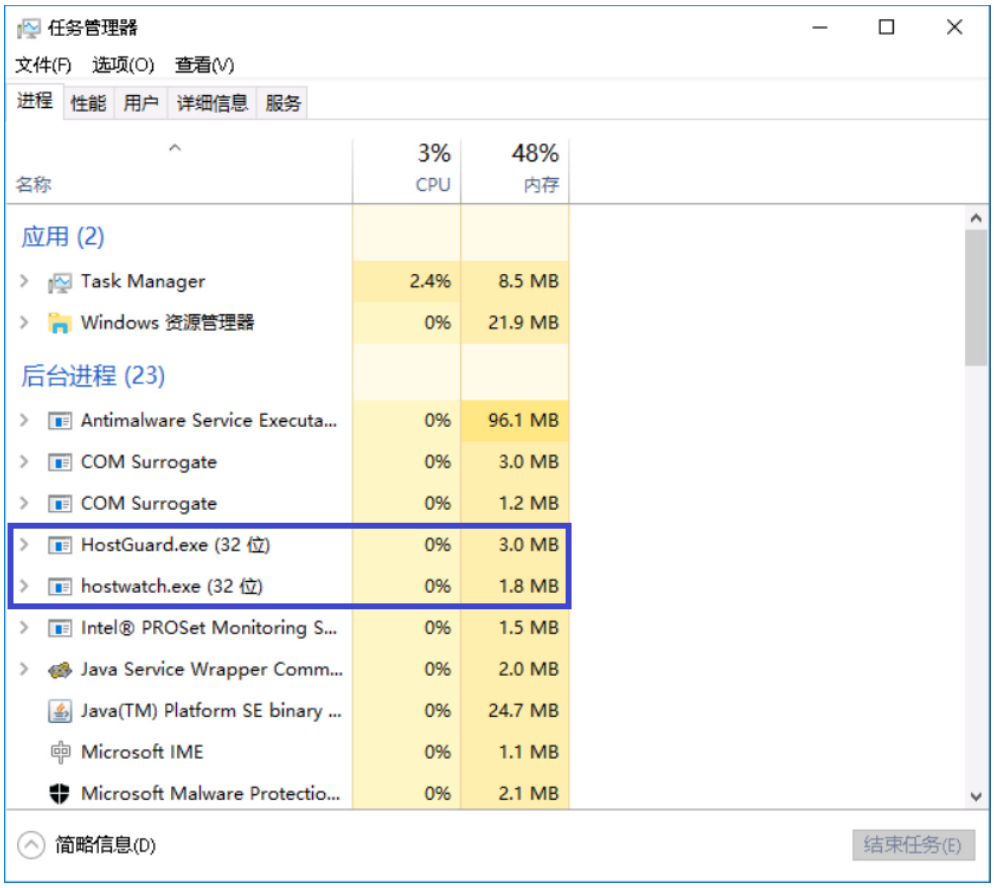
图 1-10 获取组织 ID（非华为云主机）



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。

图 1-11 查看 Agent 运行状态



----结束

1.12 HSS 是否支持线下多台服务器共用一个公网 IP?

HSS不支持线下多台服务器共用一个公网IP地址的情况。与HSS绑定的每一个服务器均需要一个公网IP地址。

1.13 购买什么版本的 HSS 能够满足等保认证?

您需要买企业版、旗舰版或者网页防篡改版才能满足等保等级的认证，基础版的功能无法满足等保认证。

1.14 HSS 是否支持病毒查杀?

主机安全服务支持检测恶意程序、勒索病毒等入侵威胁，暂不支持病毒自动查杀。

当前可对检测到的恶意程序和进程异常行为进行手动隔离查杀，处理告警事件详情请参见**处理告警事件**。

主机安全服务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，详情请参见**防勒索病毒概述**。

你可通过**创建防护策略**来防止您的主机被勒索病毒侵害。

同时您可以安装杀毒软件，作为主机安全的进一步加固。

1.15 HSS 与 SA 的基线检查有什么区别?

HSS基线检查主动检测**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，降低入侵风险并满足安全合规要求。

SA基线检查支持对**华为云的云服务**关键配置项进行检测，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

表 1-6 HSS 与 SA 基线检查的区别

类别	HSS	SA
检测对象	• 华为云弹性云服务器（Elastic Cloud Server，ECS） • 华为云裸金属服务器（Bare Metal Server，BMS） • 华为云云耀云服务器（Hyper Elastic Cloud Server，HECS） • 第三方云主机 • 线下主机	• 统一身份认证（Identity and Access Management，IAM） • 弹性负载均衡（Elastic Load Balance，ELB） • 云审计服务（Cloud Trace Service，CTS） • 弹性云服务器（Elastic Cloud Server，ECS）
功能	• 口令复杂度策略检测 检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性。 • 经典弱口令检测 检测系统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。 • 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。	• 身份与访问管理 检测是否启用IAM用户、检测IAM用户是否启用AK/SK认证，检测IAM用户是否开启登录保护，检测IAM用户是否开启操作保护、检查IAM密码策略和IAM登录验证策略配置，以及检查IAM用户会话超时策略和帐号停用策略的配置。 • 检测 检测ELB健康状态以及是否启用CTS。 • 基础设施防护 检测安全组入方向规则和高危端口、远程管理端口暴露配置，检测是否启用秘钥对登录ECS，以及检测日志指标过滤和告警事件配置。 • 数据保护 检测ELB证书有效性。

1.16 HSS 可以添加黑名单 IP 吗?

HSS暂不支持手动添加黑名单IP，HSS的帐户暴力破解防护功能已具备全网IP黑名单功能。

当发现暴力破解主机的行为，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。若被拦截的IP在超过默认拦截时间后，没有再被继续攻击，系统自动解除拦截。

1.17 主机重装系统后，HSS 防护功能是否需要手动开启?

购买主机时，若勾选了主机安全服务，主机重装系统后，HSS的Agent会自动安装并开启防护。

购买主机时，若未勾选主机安全服务，主机重装系统后，需要您为主机**安装Agent**并在HSS管理控制台上**开启防护**。

更多主机安全防护配置，请参见**安全配置**、**高级防御**。

1.18 HSS 的恶意程序检测周期、隔离查杀是多久一次?

检测周期：实时检测。

隔离查杀周期：

- 已开启自动隔离查杀：系统实时查杀（出现告警，立刻自动查杀）。
- 未开启自动隔离查杀：需人工查杀，逐一处理。

须知

1. HSS的隔离查杀支持对“恶意程序（云查杀）”和“进程异常行为”实时检测的告警进行查杀，检测能力详情请参见**服务版本差异**。
2. HSS隔离查杀分为自动隔离查杀和人工隔离查杀。
   - 开启自动隔离查杀：详情请参见**安全配置**中的“开启恶意程序隔离查杀”章节。
   - 人工隔离查杀：操作详情请参见**管理文件隔离箱**中的“选择隔离查杀”章节。

1.19 HSS 的病毒库、漏洞库多久更新一次?

更新周期：即时发现，即时更新。

漏洞库：当Windows或Linux官网有补丁发布时，企业主机安全服务产品的相关负责人会在第一时间同步更新企业主机安全服务的漏洞库。

病毒库：当后台发现新型病毒后，企业主机安全服务产品的相关负责人会在第一时间同步更新企业主机安全服务的病毒库。

1.20 每台云服务器都需要配置部署主机安全服务吗?

存在场景

购买云服务器后，使用场景可能存在以下情况：

- 场景一：云服务器所属集群节点未绑定EIP。
- 场景二：云服务器所属集群绑定EIP。

解决办法

场景一：未绑定EIP，通常情况集群及云服务器是相对安全的。

场景二：集群已绑定EIP时，集群存在对外暴露的风险，遭受攻击的几率会成倍增加，此时建议您的云上主机全量部署主机安全服务。

全量部署后可有效防止未防护主机感染的勒索、挖矿等病毒传染给其他主机，导致企业网整体沦陷。

企业主机安全服务不同版本的区别及防护能力详情请参见服务版本差异。

购买防护配额的约束限制和操作详情请参见购买防护配额。

1.21 开启 HSS 基础版防护及说明

开启 HSS 基础版防护

场景定位	开启渠道	开启方式	开启步骤	校验开启状态
对即将需要购买的ECS或HECS开启防护	在ECS或HECS控制台购买时开启（建议方案）	自动配置执行开启	• 在您购买ECS时，勾选“开通主机安全”，并选择主机安全的“基础版”，HSS会自动为该ECS安装Agent并开启“基础版（按需计费）”防护。 购买配置详情请参见购买参数配置，开启主机安全请参见开启主机安全。 • 在您购买HECS时，勾选“主机安全基础班”，HSS会自动为该HECS安装Agent并开启“基础版（按需计费）”防护。 购买配置详情请参见购买参数配置，开启主机安全请参见开启主机安全。	开启后可在开启防护列表查看防护情况。

场景定位	开启渠道	开启方式	开启步骤	校验开启状态
对已经购买的服务器进行开启（购买时或购买后未开启主机安全防护）	在HSS控制台开启	手动配置执行开启	在HSS控制台进行手动安装Agent后开启基础版防护。 1. 安装**Linux版本**/**Windows版本**的Agent。 2. Agent安装完成后**开启主机防护**。 若需开启告警通知，详情请参见**设置告警通知**。	

1.22 HSS 的数据传输实现原理是什么？

端口使用：HSS采用企业主机安全服务端的443端口，Agent使用的是随机端口通信，Agent可以通过任意端口将数据传输到HSS的443端口。

传输方式：HSS是通过IP的方式进行传输，监控的Agent是通过DNS的方式传输，传输过程不会产生数据丢失的情况。

2 购买 HSS

2.1 ECS 如何享受免费的 HSS 防护?

新购买 ECS

- 在新购买华为云ECS时，勾选“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”或者“企业版”防护。

  购买ECS时，参数选择说明如表2-1所示。

  表 2-1 参数选择说明

ECS计费模式	选择HSS	自动开启HSS防护	HSS计费
包年/包月	基础版	基础版（按需）	免费体验
按需计费	“基础版”或者“企业版”	“基础版（按需）”或者“企业版（按需）”	• 基础版（按需）：免费体验30天。 • 企业版（按需）：按实际使用的时长收费。

  目前，仅支持“华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”区域，其他区域敬请期待。

- 若“基础版”或者“企业版”不满足您的业务需求，您也可以购买其他版本配额。关闭“基础版（按需）”或者“企业版本（按需）”防护后，开启更高级的防护。

已购买 ECS

- 若已购买ECS，且购买时没有“开通主机安全”，您需要在ECS上手动安装Agent，并手动开启“基础版（按需）”防护。

图 2-1 开启基础版（按需）防护

- 若“基础版（按需）”不满足您的业务需求，您也可以购买其他版本配额。关闭“基础版（按需）”防护后，开启更高级的防护。

2.2 购买云服务器时，为什么无法选择免费的企业主机安全防护?

开启防护场景

购买云服务器时，您可以通过勾选“开通主机安全”自动开启企业主机安全服务HSS，提升云服务器安全性。勾选后，系统会自动为您购买的云服务器安装Agent，开启免费版企业主机安全防护。

问题现象及解决方法

如果您在购买云服务器时系统未显示“开通主机安全”选项，原因可能如下：

- 选择的云服务器镜像版本不支持开启HSS。仅当选择HSS支持的操作系统版本时，才能勾选HSS免费版对云服务器进行安全防护，HSS支持的操作系统版本详情请参见企业主机安全使用约束中的“支持的操作系统”。
- 部分规格的云服务器暂不支持开启HSS，系统会自动隐藏“主机安全”入口，具体以控制台显示为准。

2.3 如何扩充 HSS 防护配额?

企业主机安全的防护配额计费模式分为“按需计费”和“包年/包月”。

- 按需计费：根据当前使用情况进行实时计费，可持续不限时长使用，无配额限制，因此无需扩充，正常使用即可。

- 包年/包月：防护配额为固定的使用周期，仅限购买周期内使用，到期前可申请**续费**，如需扩充配额，重新**购买防护配额**即可。

3 开通与配置

3.1 Agent

3.1.1 购买 HSS 后会自动安装 Agent 吗?

取决于开通主机安全方式。

除了在购买ECS时勾选“开通主机安全”会自动安装Agent外，其他方式均不支持自动安装。

新购 ECS 时，勾选“开通主机安全”

在新购买华为云ECS时，勾选“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”或者“企业版”防护。

- “计费模式”选择的“包年/包月”，您只能选择主机安全“基础版”，并开启“基础版”防护。
- “计费模式”选择的“按需计费”，您可以选择“基础版”或者“企业版”，HSS自动为该ECS开启“基础版”或者“企业版”防护。

目前，仅支持“华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”区域，其他区域敬请期待。

若基础版或者企业版不满足您的业务需求，您可以**购买其他版本配额**，获取更高级的防护（不需要重新安装Agent）。各版本的差异请参见**服务版本**。

其他情况

不会自动安装Agent，需要**手动安装Agent**、**手动开启防护**。

3.1.2 如何安装 Agent?

- 华为云主机
  - Linux客户端，请参见**安装Linux版本Agent**。
  - Windows客户端，请参见**安装Windows版本Agent**。

- 非华为云主机
  - Linux客户端，请参见安装Linux版本Agent。
  - Windows客户端，请参见安装Windows版本Agent。

相关问题

- Agent安装失败应如何处理?
- Agent状态异常应如何处理?
- 如何卸载Agent?

3.1.3 如何批量安装 Agent?

本节介绍了不同操作系统下，批量安装Agent的方法。Agent支持运行的操作系统，请参见使用约束。

Windows 操作系统

windows操作系统可以使用镜像的方式批量安装Agent，操作步骤如下：

步骤1 购买华为云弹性云服务器，选定所需使用的Windows系统镜像，详细操作请参见购买华为云弹性云服务器。

步骤2 在购买的弹性云服务器中安装HSS Agent，详细操作请参见在华为云主机中安装Windows版本客户端。

说明

除在主机中安装HSSAgent外，请勿开启其他服务或执行相关配置操作。

步骤3 在任务管理器中关闭HostGuard进程。

步骤4 删除“C:\Program Files(x86)\HostGuard\config\agentinfo”下的文件。

步骤5 关闭弹性云服务器，使用该弹性云服务器制作镜像，详细操作请参见创建镜像。

说明

关闭弹性云服务器后，在制作镜像前，请勿重启弹性云服务器，否则您需重新执行步骤3和步骤4。

步骤6 使用步骤5制作的镜像为Windows弹性云服务器批量安装Agent。

说明

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。

----结束

Linux 操作系统

Linux操作系统可以通过如下两种方式批量安装Agent：

方法一：使用脚本批量安装Agent

前提条件

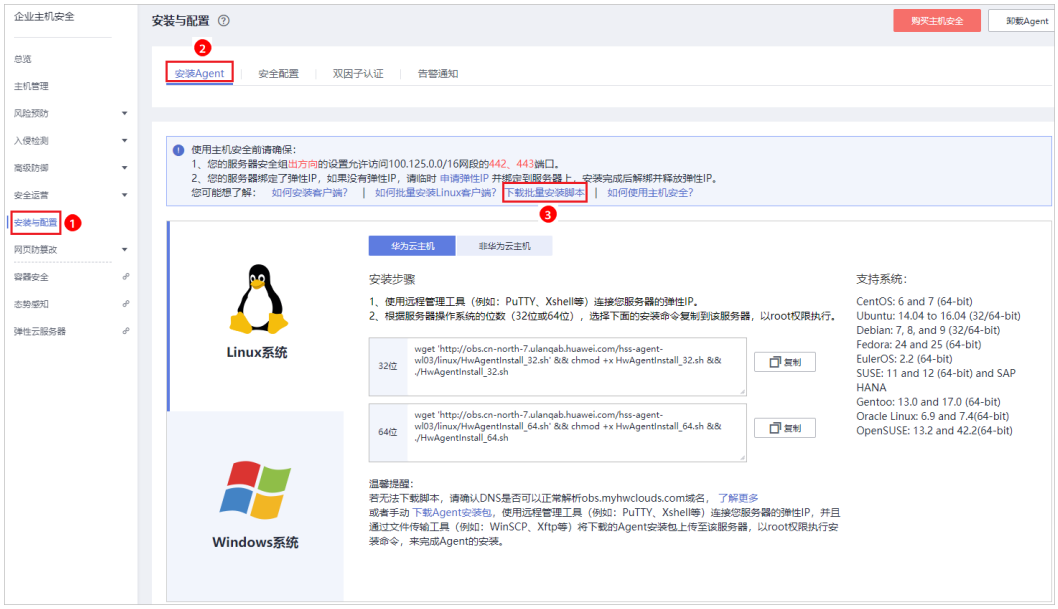
批量安装脚本需要使用ansible工具，需要被控端满足以下条件：

- 被控端当前用户与主控端用户一致。
- 被控端和主控端做过ssh免密交换。
- ansible主控端配置有忽略ssh登录验证。

操作步骤

步骤1 下载批量安装脚本，如图3-1所示。

图 3-1 下载批量安装脚本



步骤2 收集待安装主机（被控端）的IP、ssh用户名、ssh密码、root密码。

步骤3 把主机IP、ssh用户名、密码、root密码按顺序保存在一个文本文件中（utf-8编码），文档格式unix格式，空格分隔，每行一个记录，最后一行以换行结尾，如“hostinfo.txt”，格式参考如下：

例：现在有两台待安装主机，主机A：192.168.1.101，ssh登录用户名为**root**，root密码为“123456”，另一台主机B：192.168.1.102，ssh登录用户名为**test**，test的密码为“test123”，root的密码为“123456”，则文件的内容如图3-2所示：

图 3-2 示例

```
192.168.1.101 root 123456 123456
192.168.1.102 test test123 123456
```

步骤4 找一台linux机器作为执行机（主控端：建议4U8G），该机器可以通过ssh（22端口）连接待安装主机。

步骤5 在执行机上执行ansible，检查是否已安装ansible，如果没有请安装ansible。

步骤6 把主机信息配置文件hostinfo.txt和Agent安装脚本（deploy-ansible-expect）上传到执行机（放在同一个目录下）。

步骤7 执行**sh config.sh hostinfo.txt**命令，生成ansible需要的配置信息文件hosts。

步骤8 执行**chmod u+x install.sh; ./install.sh**完成批量安装。

----结束

说明

1. ansible脚本是默认使用su来切换root，但是有些机器su无法切换成root。如果执行结果有因为权限失败的，可以尝试修改安装脚本里面的hosts文件，将ansible_become_method=su改为ansible_become_method=sudo，保存后重新执行install.sh。
2. 部分机器在使用ansible安装的时候可能出现如下图的错误提示（在ubuntu16上发现过该错误），原因是目标机器上没有默认的python。可以选择以下两种方法进行规避。

```
TASK [copy to remote host] ****************************************************************
fatal: [[redacted]]: FAILED! => {"msg": "Failed to get information on remote file (/tmp/ho
stguard_install.sh): Shared connection to [redacted] closed.\r\n"}
```

   1. 可以参照**如何安装Agent?** 手动安装。
   2. 登录目标机器设置默认python。

      可以执行**sudo update-alternatives --install /usr/bin/python python /usr/bin/python3 10**

      也可以执行**ln -s /usr/bin/python3 /usr/bin/python(ln -s /usr/bin/python2 /usr/bin/python)**
3. 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。

方法二：使用镜像批量安装Agent

步骤1 购买华为云弹性云服务器，选定所需使用的Linux系统镜像，详细操作请参见**购买华为云弹性云服务器**。

步骤2 在购买的弹性云服务器中安装HSSAgent，详细操作请参见**在华为云主机中安装Linux Agent**。

说明

除在主机中安装HSSAgent外，请勿开启其他服务或执行相关配置操作。

步骤3 在服务器中关闭HSS进程。

使用**ps -ef**命令确定HSS的PID，使用**kill -pid**命令关闭Linux系统中的hostguard进程。

步骤4 删除配置文件。

使用**rm -rf**命令，删除linux系统中“/usr/local/hostguard/conf/agentinfo”下的文件。

步骤5 关闭弹性云服务器，使用该弹性云服务器制作镜像，详细操作请参见**创建镜像**。

说明

关闭弹性云服务器后，在制作镜像前，请勿重启弹性云服务器，否则您需重新执行步骤3和步骤4。

步骤6 使用**步骤5**制作的镜像为Linux弹性云服务器批量安装Agent。

说明

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。

----结束

3.1.4 如何使用命令行方式安装 Agent（Windows 操作系统）？

前提条件

- 待安装Agent所在的线上主机需要与网段相通，服务器安全组出方向需设置允许访问**100.125.0.0/16**网段的**443**端口。

操作步骤

步骤1 使用具有“管理员”权限的帐号（例如，administrator）登录Windows弹性云服务器。

步骤2 在浏览器地址栏输入Agent安装包地址，下载并解压缩安装包。

表 3-1 安装包下载路径

名称	格式	下载路径
Windows Agent安装包	zip	华北-北京一：**https://hostguard-agent.obs.cn-north-1.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip** 华北-北京四：**https://hss-agent-bj04.obs.cn-north-4.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip** 华东-上海一：**https://obs.cn-east-3.myhuaweicloud.com/hss-agent-sh01/windows/HSS-WindowsAgentSetup_x86.zip** 华东-上海二：**https://hss-agent-sh02.obs.cn-east-2.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip** 华南-广州：**https://hss-agent-gz01.obs.cn-south-1.myhuaweicloud.com/windows/HSS-WindowsAgentSetup_x86.zip** 西南-贵阳一：**https://obs.cn-southwest-2.myhuaweicloud.com/hss-agent-gy01/windows/HSS-WindowsAgentSetup_x86.zip**

步骤3 运行“CMD命令提示符”，找到安装包所在路径。

步骤4 执行**.\hostguard_setup.exe /silent**命令，完成安装Agent。

安装Agent成功后，建议删除Agent的安装包。

说明

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。

----结束

3.1.5 Agent 是否和其他安全软件有冲突?

Agent可能会和DenyHosts这款软件产生冲突。

- 冲突表现：若登录主机的IP地址被识别为攻击IP，但是无法被“解封”。
- 冲突原因：企业主机安全服务和DenyHosts会同时封禁可能为攻击IP的登录IP地址，企业主机安全服务无法解封DenyHosts中封禁的IP地址。
- 处理方法：建议停止DenyHosts。

1. 以**root**用户登录ECS。
2. 执行以下命令，检查是否安装了DenyHosts。

   ps -ef | grep denyhosts.py

   若界面回显类似以下信息，则说明安装了DenyHosts。

```
[root@hss-test ~]# ps -ef | grep denyhosts.py
root      64498      1  0 17:48 ?        00:00:00 python denyhosts.py --daemon
```

3. 执行以下命令，停止DenyHosts。

   kill -9 'cat /var/lock/denyhosts'

4. 执行以下命令，取消DenyHosts的自启动。

   chkconfig --del denyhosts;

3.1.6 Agent 的默认安装路径是什么？

在Linux/Windows操作系统的主机中安装Agent时，安装过程中不提供安装路径的选择，默认安装在以下路径中，如表3-2所示。

表 3-2 Agent 的默认安装路径

操作系统	默认安装路径
Linux	/usr/local/hostguard/
Windows	C:\Program Files (x86)\HostGuard

3.1.7 如何筛选未安装 Agent 的主机？

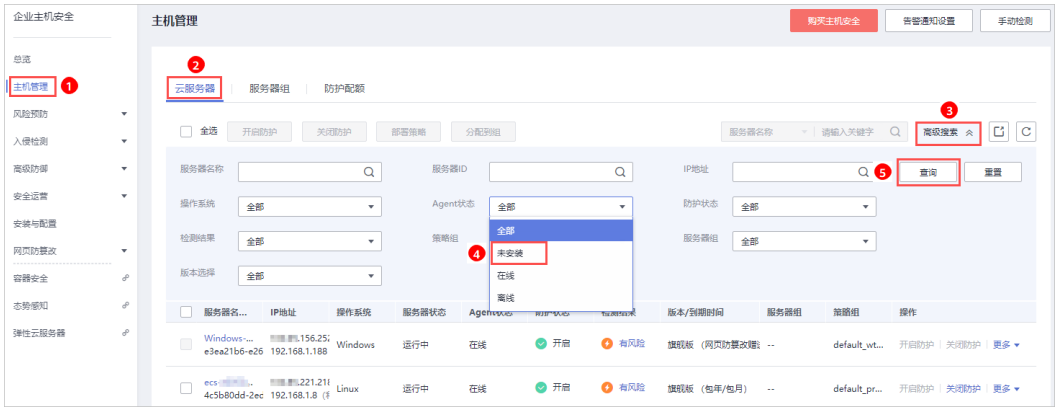
步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 3-3 企业主机安全

步骤3 在主机管理页面，筛选未安装Agent的云服务器，如图3-4所示。

图 3-4 筛选未安装 Agent 的主机



Agent状态，如下所示：

- 未安装：未安装Agent，或Agent已安装但未成功启动。
- 在线：Agent运行正常。
- 离线：Agent与HSS服务器通信异常，HSS无法提供安全防护功能。
  单击“离线”，您可以查看Agent不在线的华为云主机列表，并查看“离线原因”。

----结束

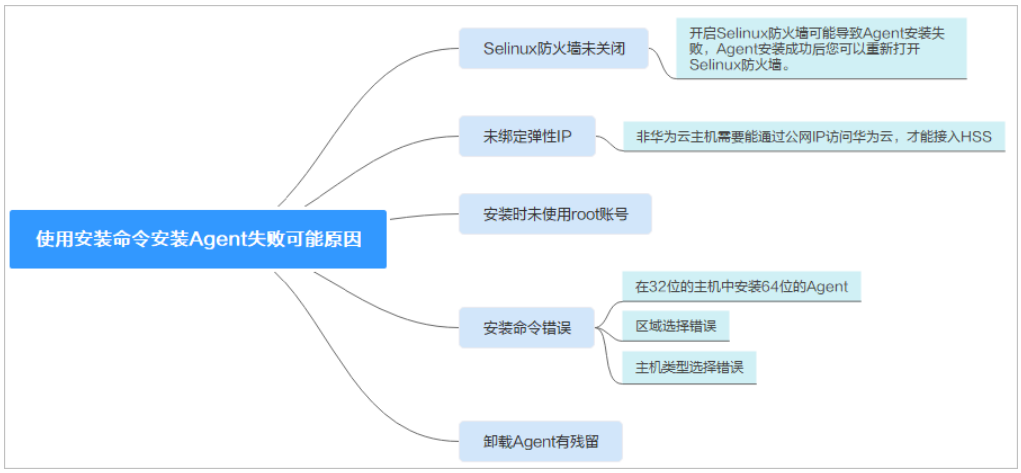
3.1.8 Agent 安装失败应如何处理?

使用安装命令安装 Agent 失败

问题现象

使用命令安装失败，安装Agent后，控制台防护列表页面仍然显示“未安装”。

可能原因



解决方案

步骤1 确认是否已关闭主机Selinux防火墙。

- 已关闭：请执行**步骤2**。
- 未关闭：请关闭Selinux防火墙后重新安装。

步骤2 确认主机是否已绑定弹性IP。

- 是：请执行**步骤3**。
- 否：请绑定弹性IP后重新安装。

步骤3 请根据主机所在区域、主机操作系统，确认安装命令是否正确。

1. 正确地选择主机所在的区域，详细操作请参见“**如何切换可用区域？**”。
2. 根据主机操作系统复制正确的安装命令。
   - 主机中32位的系统，只能使用32位系统对应的操作命令。
   - 主机中64位的系统，只能使用64位系统对应的操作命令。

- 是：请执行**步骤4**。
- 否：请使用正确的命令重新安装。

步骤4 确认安装帐号是否为**root**帐号。

- 是：请执行**步骤5**。
- 否：请使用root帐号重新安装。

步骤5 使用root帐号**卸载Agent**后强制安装。

- 安装成功：结束操作。
- 安装失败：请联系技术支持。

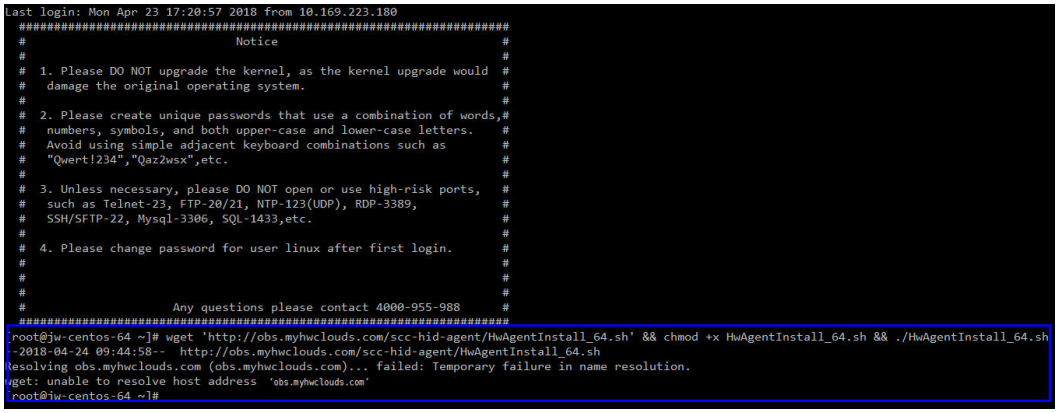
----结束

使用脚本安装 Agent 失败

问题现象

安装Agent时报错，使用脚本安装Agent提示如下报错信息。

图 3-5 报错信息



可能原因

DNS地址配置错误，DNS无法解析域名obs.myhuaweicloud.com。

解决方案

配置DNS完成后，重新执行安装脚本。操作步骤如下所示：

步骤1 执行以下命令，查看“resolv.conf”文件。

cat /etc/resolv.conf

步骤2 执行以下命令，ping域名，若回显如图3-6所示，请进行步骤3。

ping obs.myhuaweicloud.com

图 3-6 域名无法 ping 通

```
[root@jw-centos-64 ~]# cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search openstacklocal
nameserver [redacted]
nameserver [redacted]
[root@jw-centos-64 ~]# ping  obs.myhuaweicloud.com
ping: unknown host obs.myhuaweicloud.com
[root@jw-centos-64 ~]#
```

步骤3 执行以下命令，打开“resolv.conf”文件。

vi /etc/resolv.conf

将如图3-7所示的部分替换成公共域名解析服务DNS常用的IP，如下所示：

```
nameserver DNS常用IP1
nameserver DNS常用IP2
```

图 3-7 替换内容

```
[root@jw-centos-64 ~]# cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search openstacklocal
nameserver [redacted]
nameserver [redacted]
[root@jw-centos-64 ~]# ping  obs.myhuaweicloud.com
ping: unknown host obs.myhuaweicloud.com
[root@jw-centos-64 ~]#
```

步骤4 修改完成后，再次执行命令**ping obs.myhuaweicloud.com**，若回显信息类似如下，说明域名已经ping通。

图 3-8 域名 ping 通信息

```
PING obs.cgl.[redacted].myhuaweicloud.com([redacted]) 56(84) bytes of data.
64 bytes from ecs-[redacted]-24-11.compute.huaweicloud-dns.com ([redacted]): icmp_seq
=1 ttl=42 time=29.0 ms
64 bytes from ecs-[redacted]-24-11.compute.huaweicloud-dns.com ([redacted]): icmp_seq
=2 ttl=42 time=28.8 ms
64 bytes from ecs-[redacted]-24-11.compute.huaweicloud-dns.com ([redacted]): icmp_seq
=3 ttl=42 time=28.7 ms
^C
--- obs.cgl.[redacted].myhuaweicloud.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 28.770/28.878/29.063/0.190 ms
```

步骤5 配置DNS完成后，请重新执行安装脚本。

----结束

Agent 安装失败案例

- **安装失败信息**：install rpm package failed。

  原因分析：安装包错误，需确认安装环境对应的安装包、参照的安装流程是否正确。

  解决办法：

  a. 参照**如何卸载Agent?** 将已安装的Agent进行卸载。

  b. 卸载后参照**Linux版本**或**Windows版本**重新安装Agent。

3.1.9 Agent 状态异常应如何处理?

Agent状态主要分为以下三种，若Agent的运行状态为“未安装”或者“离线”时，可能是Agent与服务器间通信异常。请参见本文进行排查。

- 未安装：主机从未安装Agent，或Agent已安装但未成功启动。
- 离线：Agent与服务器通信异常，主机中的Agent已被删除，或非华为云主机离线。
- 在线：主机内的Agent运行正常。

可能的原因

- 网络故障。

  主机中的Agent和云端防护中心出现异常，如网卡故障、IP地址异变及带宽较低。
- Agent进程异常。
- 安装Agent后，不会立即生效，需要等待3~5分钟左右控制台才会刷新。

处理方法

步骤1 排查网络故障。

请确保您的云服务器所属安全组出方向设置允许访问**100.125.0.0/16**网段的**443**端口，确保云服务器能正常访问网络。

待网络恢复正常后：

- 若Agent状态为“在线”，则故障清除。
- 若Agent状态仍为“未安装”或者“离线”，请执行**步骤2**。

步骤2 若长时间Agent状态仍为“未安装”或者“离线”，可能是Agent进程异常，需要登录主机，重启Agent进程。

- Windows操作系统

  以管理员**administrator**权限登录主机，完成重启Agent。

图 3-9 重启 Windows Agent

- Linux操作系统

  请以**root**用户在命令行终端执行以下命令，完成重启Agent。

  service hostguard restart

  若回显以下信息，则表示重启成功。若无回显信息，请**卸载Agent**，重新**安装Agent**。

```
root@HSS-Ubuntu32:~#service hostguard restart
Stopping Hostguard...
Hostguard stopped
Hostguard restarting...
Hostguard is running
```

重启进程后等待约2分钟：

- 若Agent状态为“在线”，则故障清除。
- 若Agent状态仍为“未安装”或者“离线”，请**卸载Agent**，重新**安装Agent**。

----结束

3.1.10 Agent 运行时占用多少 CPU 和内存资源?

HSS服务采用轻量级Agent，占用资源极少，不会影响主机系统的正常业务运行。

具体占用的CPU、内存资源如下：

CPU 占用峰值

Agent运行时，CPU占用比例控制在**1vCPU**的10%。因此，实际占用比例与您购买的云服务器规格有关，详见**不同规格主机Agent资源占用一览**。

若占用比例达到1vCPU的10%，Agent会自动降CPU；自动降CPU后，Agent检测主机时间会延长，但不影响服务使用。

说明

Agent定时检测任务会基于使用地时间在每日00：00-04：00执行，全量扫描主机，不会影响主机系统的正常运行。

内存占用峰值

Agent运行时，内存占用控制在**150MB**以内。

若内存占用达到200MB，Agent会在5分钟内自动重启。

不同规格主机 Agent 资源占用一览

Agent运行时，不同规格的云服务器CPU、内存占用情况如**表3-3**所示。

表 3-3 Agent 资源占用一览

vCPUs规格	Agent运行占用CPU资源比例（峰值）	内存占用（峰值）
1vCPUs	10%	150MB
2vCPUs	5%	150MB
4vCPUs	2.5%	150MB
8vCPUs	1.25%	150MB
12vCPUs	约0.83%	150MB
16vCPUs	约0.63%	150MB
24vCPUs	约0.42%	150MB
32vCPUs	约0.31%	150MB
48vCPUs	约0.21%	150MB
60vCPUs	约0.17%	150MB
64vCPUs	约0.16%	150MB

3.1.11 安装 HSS Agent 有什么影响?

安装HSS Agent不影响在线业务，也不会影响服务器的运行状态。

企业主机安全服务（HSS）提供的Agent，用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。

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

3.1.12 网页防篡改与主机安全共用 Agent 吗?

是的。

网页防篡改与主机安全共用同一个Agent，同一主机只需安装一次。

3.1.13 如何卸载 Agent?

操作场景

- Agent包选择错误，需要卸载Agent后重新安装。
- 安装命令复制错误（如在32位的主机中安装64位的Agent），需要卸载Agent后重新安装。

前提条件

云服务器的“Agent状态”为“在线”。

控制台一键卸载 Agent

用户可以通过企业主机安全控制台直接卸载Agent，方便用户操作。

说明

卸载Agent后主机安全服务将无法为该服务器提供任何防护。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 3-10 企业主机安全

步骤3 在左侧导航中选择“安装与配置”，进入“安装与配置”界面，单击右上角“卸载Agent”。

步骤4 在弹出的“卸载Agent”界面中，如图3-11所示，选择需要卸载Agent的云服务器。

图 3-11 卸载 Agent

步骤5 单击“确定”。

云服务列表“Agent状态”显示为“离线”，卸载Agent成功。

----结束

主机本地卸载

用户在不需要使用企业主机安全服务或需要重新安装Agent时，可从本地卸载版本Agent。

说明

卸载Agent后主机安全服务将无法为该服务器提供任何防护。

- **卸载Linux版本Agent**
  a. 登录需要卸载企业主机安全服务Agent的云服务器，并执行**su - root**命令切换到**root**用户。
  b. 在任意目录执行以下命令，卸载Agent。
     i. 针对“.rpm”格式的安装包，执行命令：**rpm -e --nodeps hostguard**
     ii. 针对“.deb”格式的安装包，执行命令：**dpkg -P hostguard**

     若界面回显如下信息，则表示卸载完成。

```
Stopping Hostguard...
Hostguard stopped
Hostguard uninstalled.
```

- **卸载Windows版本Agent**
  a. 登录需要卸载主机安全服务Agent的云服务器。
  b. 在“控制面板 > 程序和功能”中选中“HostGuard”，然后单击“卸载”。

说明

- 用户也可以进入安装目录，双击“unins000.exe”，启动卸载程序。
- 若安装Agent时创建了开始菜单下存放Agent快捷方式的文件夹，用户还可以在“开始 > HostGuard”中选择“卸载HostGuard”进行卸载。

c. 在“HostGuard卸载”提示框中，单击“是”，开始卸载。

d. 卸载完成后单击“确定”。

3.1.14 Agent 升级失败如何处理?

Agent 升级说明

- 整个升级Agent过程均为免费。
- 升级时查看“Agent状态”为“在线”才能正常升级。
- 升级过程中不影响您在云服务器上业务的正常使用。
- 升级后将在新版conosle进行计费，旧版停止计费。
- 升级后云服务器在主机安全（新版）继续被防护，主机安全（旧版）将停止防护。
- 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。

升级 Agent 原理

在企业主机安全控制台单击升级Agent后，系统将自动按照先卸载Agent1.0，然后安装Agent2.0的顺序执行，无需人为操作。

升级后Agent反馈的状态为：

- 升级成功：已经升级成功，可切换至主机安全（新版）查看防护情况。
- 升级中：Agent正在升级。
- 升级失败：Agent升级失败。

升级失败原因

升级失败可能因为卸载Agent1.0失败或安装Agent2.0失败。

解决办法

需要清除在执行升级Agent过程中残留在云服务器的信息，然后再重新手动安装Agent。

操作步骤：

步骤1 按照**卸载Agent**的操作流程执行卸载。

- 出现如**图3-12**所示，表示Agent在升级过程中卸载失败，现已卸载成功。

图 3-12 卸载成功

```
Hostguard uninstalled.
[root@ecs-test0426 ~]# service hostguard status
Redirecting to /bin/systemctl status hostguard.service
Unit hostguard.service could not be found.
[root@ecs-test0426 ~]#
[root@ecs-test0426 ~]#
[root@ecs-test0426 ~]#
```

- 出现如图3-13所示，表示Agent在升级过程中已卸载成功。

图 3-13 已被卸载

```
[root@ecs-test0426 ~]#
[root@ecs-test0426 ~]#
[root@ecs-test0426 ~]# rpm -e hostguard
error: package hostguard is not installed
[root@ecs-test0426 ~]#
```

步骤2 将平台切换至主机安全（新版）（主机安全+容器安全）进行手动安装Agent，安装操作详情请参见**安装Agent**。

说明

- 当前支持切换至主机安全服务（新版）的Region为华北-乌兰察布二零一、华北-乌兰察布二零二、西南-贵阳一、华南-深圳、华南-广州-友好用户环境、华东-上海一、华东-上海二、华北-北京一、华北-北京四。
- 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。

----结束

3.1.15 Agent 安装后控制台不显示怎么处理?

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。

Agent安装后超过等待时间仍不显示可能原因如下：

- 安装的Agent包与云服务器系统及版本不匹配
- 安装时云服务器剩余内存不足
- 100.125.X.X:443端口被限制

解决办法

- **Agent包不匹配**
  a. 需要您**卸载已安装的Agent包**。
  b. 重新获取与目标云服务器系统及版本匹配的包链接进行**重新安装**。
- **内存不足**
  a. 通过远程管理工具（如：Xftp、SecureFX、WinSCP）远程登录目标云服务器。
  b. 执行以下命令，查看目标云服务器的内存使用情况。
     free -m
  c. 执行命令反馈信息如图3-14所示，查看free项的数值。

图 3-14 查看内存

```
[root@cn-north-6a-HSS-master-msghandler-010061009125 opsadmin]# free -m
              total        used        free      shared  buff/cache   available
Mem:           7796        1144        3068          19        3582        6339
Swap:             0           0           0
[root@cn-north-6a-HSS-master-msghandler-010061009125 opsadmin]#
```

若小于500M，则说明内存不足，需要关闭一些应用或扩容才能正常安装Agent。

- **443端口被限制**

  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.X.X/16网段的443端口。

3.1.16 Agent 安装成功后显示未安装怎么处理?

Agent 使用说明

同一主机Agent成功安装一次即可。

安装成功后，建议重启主机后再执行开启防护及绑定配额操作。

显示未安装原因

目前主机安全服务新版和旧版共存使用，由于一台主机只能安装单一Agent，但主机会在新、旧版两个平台同时显示，因此Agent状态及防护情况只能在新版或旧版其中一个平台正常显示。

示例：若A主机已经在旧版console正常安装了Agent，那么在新版console中Agent状态为未安装，此时在新版console安装Agent会显示安装成功，但安装后仍会显示未安装。

解决办法

由于Agent对于主机的唯一性，主机安全新版和旧版您只能使用一个平台。

若您正在使用旧版，您可通过**升级Agent**使用新版主机安全服务，整个升级过程均为免费，且不影响业务使用。

说明

目前主机安全新版相对于旧版提升了勒索防护、新增了应用防护等能力，建议您使用新版主机安全。

若安装Agent后控制台没有任何显示，解决方案可参见**Agent安装后控制台不显示怎么处理?** 。

在升级过程中若出现升级失败，解决方案可参见**Agent升级失败如何处理?**

3.2 安全配置

3.2.1 如何清除 HSS 中配置的 SSH 登录 IP 白名单?

防护配额在不同状态下，清除HSS中配置的SSH登录IP白名单的方式不同。请根据配额的状态，选择清除SSH登录IP白名单的方式。

正常/已过期

配额状态为“正常”和“已过期”时，您可以正常使用配额，通过管理控制台“禁用”或者“删除”配置的SSH登录IP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。

图 3-15 企业主机安全

步骤3 在“安装与配置”界面，选择“安全配置 > SSH登录IP白名单”，进入SSH登录IP白名单页面。

图 3-16 SSH 登录 IP 白名单

步骤4 单击“禁用”或者“删除”，清除配置的SSH登录IP白名单。

----结束

已冻结/冻结期满，配额被删除

当配额状态为“已冻结”时，或者冻结期满，配额被彻底删除后，HSS均不会再防护您的主机，您无法通过管理控制台清除SSH登录IP白名单。

清除配置的SSH登录IP白名单，操作步骤如下所示。

步骤1 登录需要清除SSH登录IP白名单的云主机。

步骤2 执行以下命令，查看“/etc/sshd.deny.hostguard”文件，如图3-17所示。

cat /etc/sshd.deny.hostguard

图 3-17 查看文件内容

```
[root@ecsbindhss ~]# cat /etc/sshd.deny.hostguard
ALL
[root@ecsbindhss ~]#
[root@ecsbindhss ~]#
```

步骤3 执行以下命令，打开“/etc/sshd.deny.hostguard”文件。

vim /etc/sshd.deny.hostguard

步骤4 按“**i**”进入编辑模式，删除“ALL”。

步骤5 按“Esc”退出编辑，输入“:wq”保存并退出。

----结束

3.2.2 不能通过 SSH 远程登录主机，怎么办?

问题现象

可以通过华为云管理控制台登录到主机，但是无法通过SSH远程登录主机，为什么?

可能原因

- 因帐户暴力破解（例如：输入密码错误次数过多，30秒内，错误次数达到5次及以上），导致主机IP被拦截。
- 开启了**SSH登录IP白名单**功能，但需要通过SSH登录主机的IP没有添加到IP白名单。

  开启SSH登录IP白名单后，只允许白名单内的IP通过SSH登录到服务器，拒绝白名单以外的IP。

解决方案

步骤1 确认是否因为帐户暴力破解，导致主机IP被拦截。

- 是，请按如下步骤操作：
  a. 登录企业主机安全控制台。
  b. 在左侧导航树选择“入侵检测 > 事件管理”，进入“事件管理”页面。
  c. 单击“已拦截IP”，弹出“已拦截IP”页面。
  d. 选中目标攻击源IP，单击列表上方“解除拦截”，解除IP拦截。
- 否，请执行**步骤2**。

步骤2 确认是否已开启SSH登录白名单，且登录主机的IP没有添加到IP白名单。

- 是，将登录主机的IP加入到IP白名单，详细操作请参见**配置SSH登录IP白名单**。
- 否，请联系技术支持工程师。

----结束

相关操作

- **无法登录到Linux云服务器怎么办?**

- 无法登录到Windows云服务器怎么办?

3.3 双因子认证

3.3.1 如何使用双因子认证?

本章节指导用户如何使用双因子认证。

如何开启

请参见：开启双因子认证功能。

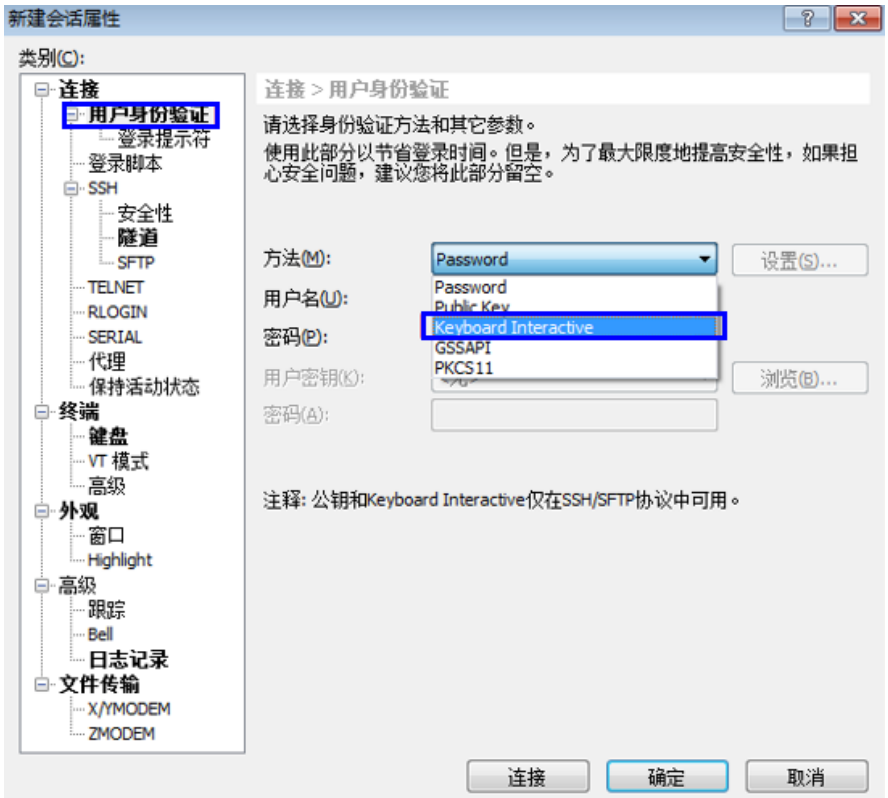
登录与使用

- 登录Linux主机
  a. 使用PuTTY/Xshell登录云主机。
     登录时，请选择“Keyboard Interactive”，输入用户身份验证。
     - PuTTY
       请参见图3-18选择“Keyboard Interactive”，并单击“确定”。

       图 3-18 键盘交互模式（一）

     - Xshell
       在会话属性框中，选择“连接 > 用户身份验证 > 方法”，单击“方法”下拉选项，选择“Keyboard Interactive”，单击“确定”。

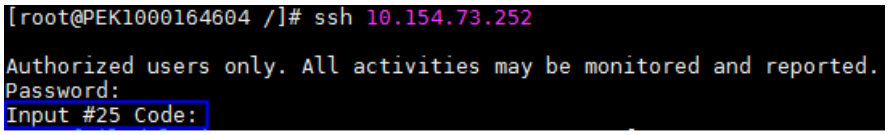
图 3-19 键盘交互模式（二）



b. 输入云主机的帐户与密码。

c. 开启双因子认证后，需输入订阅终端接收到的验证码，如图3-20所示。

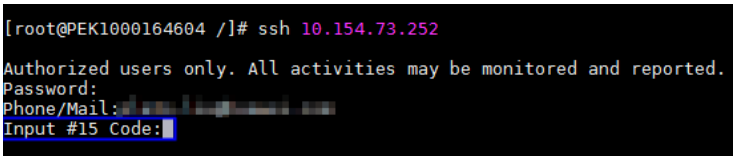
图 3-20 输入验证码



说明

- 订阅主题的手机或邮箱会收到信息：【华为云】您的云服务器（xxxx-yyyy）第XX号登录验证码为：XXXXXX。
- 如果未收到验证码，请检查Selinux防火墙是否关闭，关闭后重试。
- 当企业主机安全服务检测到主机可能遭受到暴力破解时，需先输入订阅终端的详细信息（如手机号码或邮箱），输入正确后，系统才会发出验证码。如图3-21。

  图 3-21 输入手机号码/邮箱

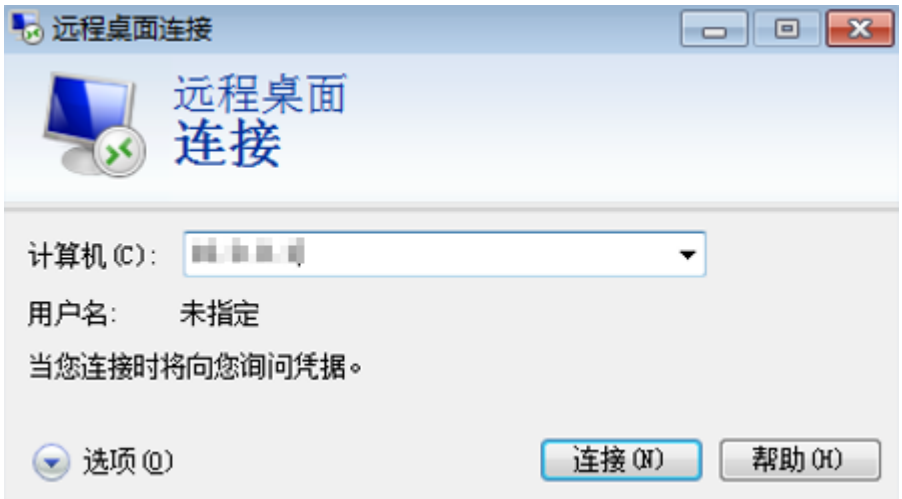
- 订阅主题的手机号码或邮箱单次可增加10个，一个主题最多可添加1万个。

- 登录Windows主机

a. 单击“开始”菜单，在搜索栏中输入“远程桌面连接”，按“Enter”，打开远程桌面连接。

b. 在“计算机”栏输入云主机的IP地址，并单击“连接”。

图 3-22 远程桌面连接



c. 若已开启双因子认证，需要输入预留手机号或邮箱，单击“获取验证码”。

图 3-23 输入手机号或邮箱

说明

订阅主题的手机或邮箱会收到信息：【华为云】您的云服务器（xxxx-yyyy）第XX号登录验证码为：XXXXXX。

d. 获取验证码后，在登录界面输入验证码、云主机帐号和密码，单击  ，登录云主机。

3.3.2 开启双因子认证失败，怎么办?

问题现象

- 在双因子认证列表下，没有待开启双因子认证的主机，怎么办?
- 开启双因子认证后，不生效，怎么办?
- 开启双因子认证失败，怎么办?

可能原因

- 主机未开启防护。
- 开启双因子认证不会立即生效，需要等大约5分钟才生效。
- Linux主机没有关闭“密钥对”登录方式。
- 与“网防G01”软件、服务器版360安全卫士存在冲突。
- 没有关闭Selinux防火墙。

解决方案

步骤1 确认待开启双因子认证的主机，是否已开启主机安全防护。

- 是：请执行**步骤2**。
- 否：请将待开启双因子认证的主机开启主机安全防护。

步骤2 确认开启双因子认证后，是否已等待5分钟。

- 是：请执行**步骤3**。
- 否：请等待5分钟后，再确认开启的双因子认证是否生效。

步骤3 确认是否为Linux主机，且使用“密钥对”方式登录。

- 是：请关闭“密钥对”登录方式，开启“密码”登录方式。详细操作请参见**Linux云服务器怎样切换密钥登录为密码登录?**
- 否：请执行**步骤4**。

步骤4 确认主机是否已停止“网防G01”软件、服务器版360安全卫士。

- 是：请执行**步骤5**。
- 否：请停止“网防G01”软件和服务器版360安全卫士。

步骤5 确认主机是否已关闭Selinux防火墙。

- 是：请执行**步骤6**。
- 否：请执行以下命令，关闭Selinux防火墙。
  - 临时关闭Selinux防火墙。
    setenfore 0 #临时关闭
  - 永久关闭Selinux防火墙。
    vi /etc/selinux config
    selinux=disabled #永久关闭

步骤6 请联系技术支持。

----结束

3.3.3 开启双因子认证后收不到验证码?

- 开启双因子认证功能后，不会立即生效。
  需要等大约5分钟才生效。
- 开启双因子认证需要关闭Selinux防火墙。
  请关闭Selinux防火墙后重试。
- Linux主机需要使用“密码”登录方式。

请关闭“密钥对”登录方式。

3.3.4 为什么开启双因子认证后登录主机失败?

登录主机失败的原因可能为文件配置错误或登录方式错误导致。

文件配置错误

您可检查配置文件是否正确。

配置文件路径：/etc/ssh/sshd_config

需要确认的配置文件项：

PermitEmptyPasswords no

UsePAM yes

ChallengeResponseAuthentication yes

须知

如果您使用的是root登录，还需要配置文件项为：

PermitRootLogin yes

登录方式错误

失败原因：开启双因子认证后，可能是通过以下方式登录云主机导致登录失败。

- 通过CloudShell工具登录云主机。
- Linux主机中，通过云堡垒机登录云主机。

根本原因：双因子的验证实现是通过内置模块进行验证，由于以上登录方式无法弹出交互页面，导致验证失败。

解决办法：您可参照如何使用双因子认证? 重新登录认证。

说明

开启双因子的前提条件、约束与限制更多详情请参见安全配置章节中的“开启双因子认证”。

3.3.5 开启双因子认证时，如何添加手机号?

当您开启双因子认证，选择“短信邮件验证”，才可以在消息通知服务主题中添加手机号/邮箱接收验证码。

“选择消息通知服务”下拉列表中，只展示状态已确认的消息通知服务主题。

- 如果没有主题，请单击“查看消息通知服务主题”进行创建。具体操作请参见创建主题。
- 如果已有主题，添加或者修改手机号码/邮箱收到验证码，请修改对应主题，具体操作请参见订阅主题。

图 3-24 短信邮件验证

3.3.6 双因子认证中，验证码是一个固定的验证码吗?

当您开启双因子认证无法用手机/邮箱接收验证码时，您可以选择“验证码验证”。当您每次登录云主机时，HSS均会生成一个随机验证码发送到您的登录界面，您直接输入随机验证码即可登录该云主机。

图 3-25 验证码验证

3.4 主机配额

3.4.1 如何查看配额?

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

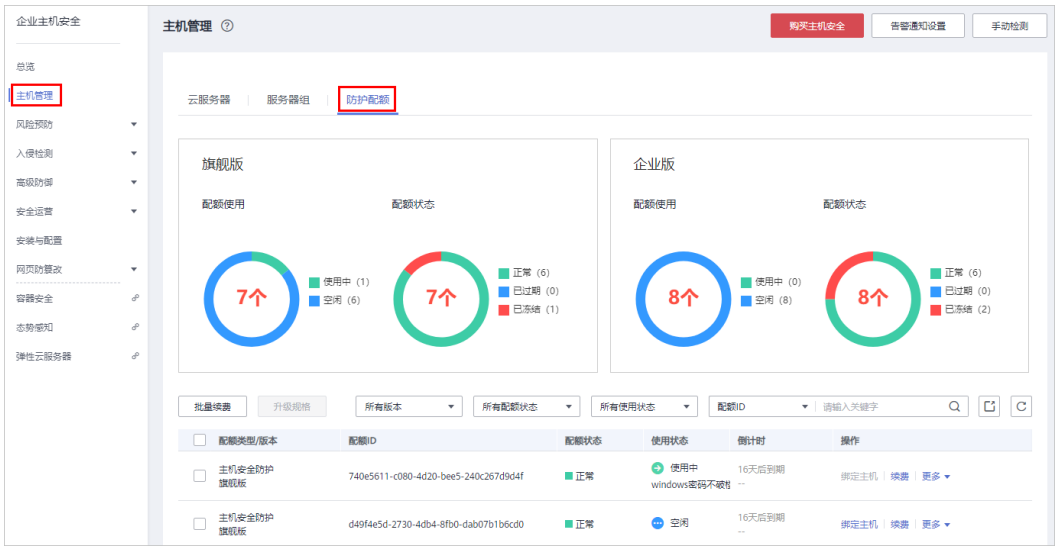
步骤1 登录管理控制台。

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。

图 3-26 企业主机安全

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 3-27 查看主机安全防护配额



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 3-4 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。

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

说明

- 绑定主机

  您也可以通过在“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

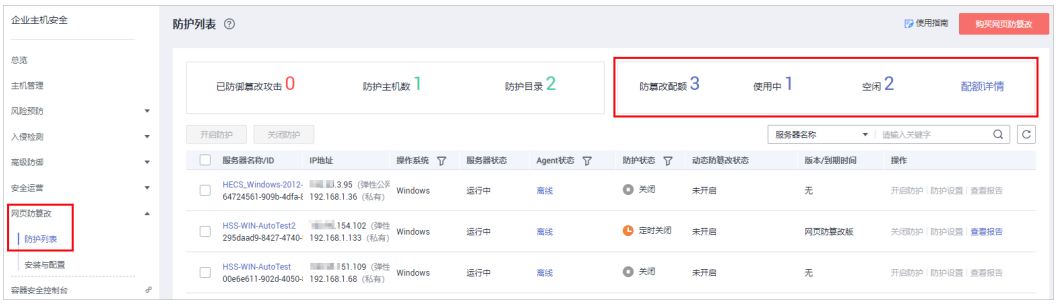
步骤1 **登录管理控制台**。

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。

图 3-28 企业主机安全

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 3-29 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 3-30 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 3-5 参数说明

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

说明

- 绑定主机

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

  一个配额只能绑定一个主机，且只能绑定Agent在线的主机。

- 续费

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

3.4.2 如何筛选未绑定配额的主机?

步骤1 **登录管理控制台**。

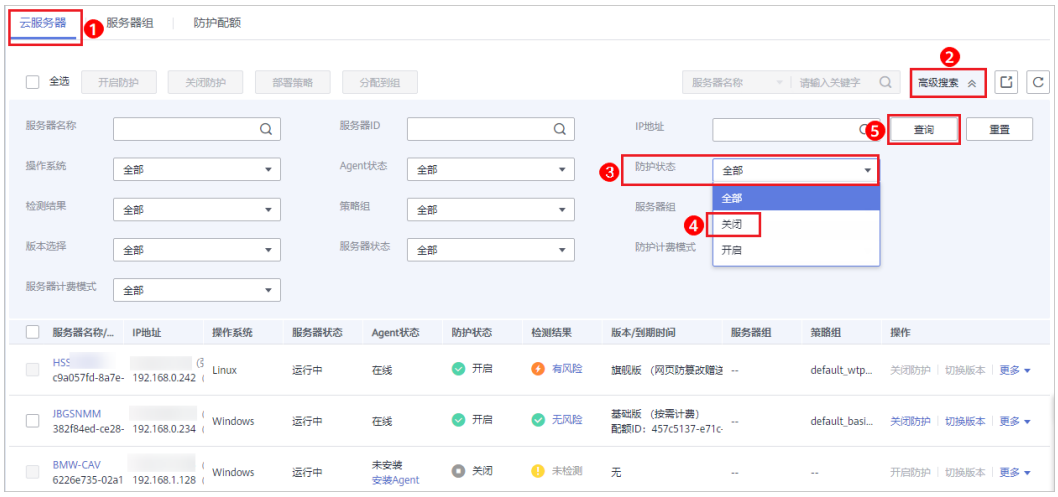
步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 企业主机安全”，进入企业主机安全页面。

图 3-31 企业主机安全

步骤3 在左侧导航树中，选择“主机管理”，进入主机管理界面。

步骤4 在“云服务器”页签中，筛选未绑定配额的主机。

图 3-32 筛选未绑定配额的主机



步骤5 查看未绑定配额的主机。

图 3-33 未绑定配额的主机

----结束

3.4.3 云服务器列表为什么看不到购买的服务器?

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

解决方法：

若未找到您的主机，请切换到正确的区域后再进行查找。若已开通企业项目，请切换到正确区域及企业项目后再进行查找。

3.4.4 开启防护时显示没有配额?

未购买配额

请先在服务器所在区域购买充足的配额，具体操作请参见**购买主机安全配额**。

区域不正确

购买配额后，请切换到配额所在区域对服务器开启防护。

位置不正确

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

企业项目不正确

若已开通企业项目，请切换到正确的“企业项目”为服务器开启防护。

3.4.5 防护配额如何分配?

“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。

说明

一般情况下，采用随机分配的方式。

3.4.6 防护的主机切换操作系统，HSS 配额会发生变化吗?

不会变化。在切换主机操作系统前，请您先确认企业主机安全服务的Agent是否支持待切换的操作系统。不支持的操作系统，与Agent可能存在兼容性问题，建议您重装或者选择为Agent支持的操作系统版本，以便获得企业主机安全更好的服务体验。

企业主机安全服务的Agent可运行在CentOS、EulerOS等Linux系统以及Windows 2012、Windows 2016等Windows系统的主机上。

须知

已停止服务的Linux系统版本或者Windows系统版本，与Agent可能存在兼容性问题，建议重装或者升级为Agent支持的操作系统版本，以便获得企业主机安全更好的服务体验。

- 企业主机安全服务支持的华为云主机Linux系统版本如表3-6和表3-7所示。

表 3-6 Linux 系统版本（X86 计算）

序号	支持的OS类型
1	CentOS：7，8 (64 bit)
2	Debian：7，8，9 and 10 (32/64 bit)
3	EulerOS：2.2，2.3 and 2.5 (64 bit)
4	Fedora：24，25，and 30 (64 bit)
5	OpenSUSE：13.2，15.0 and 42.2 (64bit)

序号	支持的OS类型
6	Ubuntu：14.04，16.04，18.04 and 20.04 (32/64 bit)
7	Gentoo：13.0 and 17.0 (64 bit)
8	Oracle Linux：6.9 and 7.4 (64bit)

表 3-7 Linux 系统版本（鲲鹏计算）

序号	支持的OS类型
1	CentOS：7.4，7.5，7.6，8.0 64bit with ARM(40GB)
2	EulerOS：2.8 64bit with ARM(40GB)
3	Fedora：29 64bit with ARM(40GB)
4	OpenSUSE：15.0 64bit with ARM(40GB)
5	Ubuntu：18.04 64bit with ARM(40GB)

- 企业主机安全服务支持的华为云主机Windows系统版本如**表3-8**所示。

表 3-8 Windows 系统版本

序号	支持的OS类型	使用限制说明
1	Windows Server 2019 数据中心版 64位英文(40GB)	若服务器安装了McAfee软件、360安全卫士、腾讯管家等第三方安全防护软件，请先停止第三方安全防护软件的防护功能，待Agent安装完成后再开启。
2	Windows Server 2019 数据中心版 64位简体中文(40GB)	
3	Windows Server 2016 标准版 64位英文(40GB)	
4	Windows Server 2016 标准版 64位简体中文(40GB)	
5	Windows Server 2016 数据中心版 64位英文(40GB)	
6	Windows Server 2016 数据中心版 64位简体中文(40GB)	
7	Windows Server 2012 R2 标准版 64位英文(40GB)	
8	Windows Server 2012 R2 标准版 64位简体中文(40GB)	
9	Windows Server 2012 R2 数据中心版 64位英文(40GB)	

序号	支持的OS类型	使用限制说明
10	Windows Server 2012 R2 数据中心版 64位简体中文(40GB)	

3.5 告警通知配置

3.5.1 告警通知短信是否收费?

消息通知服务为付费服务，价格详情请参见SMN价格详情。

3.5.2 如何修改接收告警通知的手机号或邮箱?

开启告警通知功能后，HSS通过您设置的手机号或邮箱向您发送告警通知，帮助您及时了解主机/网页内的安全风险。

设置HSS告警通知时，您可以选择“消息中心”或者“消息主题”，如图3-34所示。

- 若选择的是“消息中心”，则参照消息中心修改手机号或邮箱。
- 若选择的是“消息主题”，则参照消息主题修改手机号或邮箱。

图 3-34 告警方式

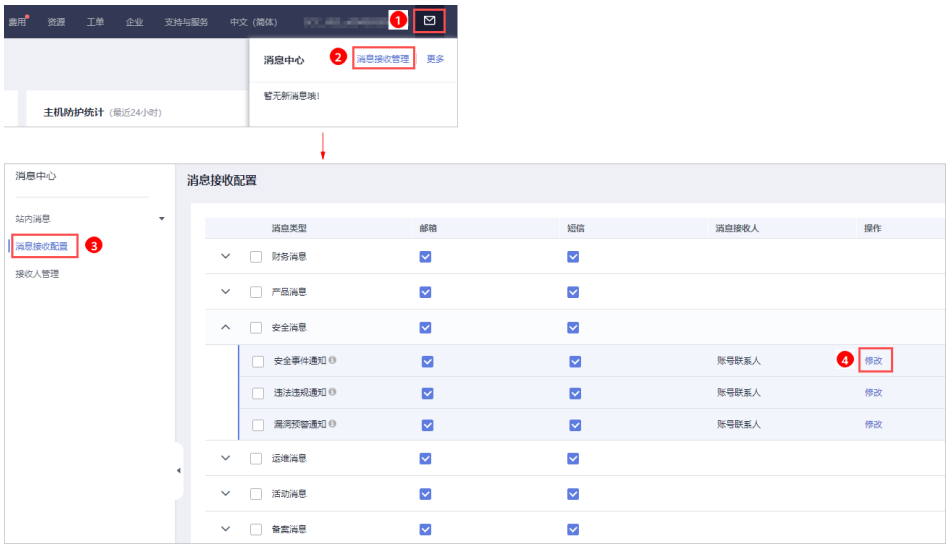
消息中心

步骤1 登录管理控制台。

步骤2 进入消息中心，新增或修改“消息中心”中接收告警通知的邮箱、手机号。

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，具体操作请参见修改指定消息接收人。

图 3-35 新增或修改告警通知接收人



步骤3 在弹出的“修改消息接收人”窗口中，勾选或取消勾选待修改的联系人，单击“确定”，完成修改操作。

----结束

消息主题

如果接收告警通知的订阅终端（手机号或邮箱）变更，需要删除订阅后，重新添加接收告警通知的手机号或邮箱。

例如：需要删除HSS告警通知的消息主题名称是“HSS-warning”，消息订阅终端是“test@example.com”。

前提条件

拥有SMN administrator权限。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择区域后，单击 ☰ ，选择“应用服务 > 消息通知服务”。

步骤3 单击“订阅”，进入订阅页面，搜索待删除订阅终端（手机号或者邮箱），如图3-36所示。

图 3-36 搜索符合条件的订阅终端

步骤4 请根据“订阅终端”和“主题名称”，确认该订阅终端接收的是HSS的告警通知。

步骤5 单击“删除”，删除订阅。

说明

删除订阅后，消息订阅者将无法接收HSS推送的消息，请谨慎操作。

步骤6 删除订阅后，选择“主题”，查询到指定主题，为主题添加新的订阅，详细操作请参见添加订阅和请求订阅。

图 3-37 添加订阅

----结束

3.5.3 配置告警通知时选不到消息主题?

未创建主题

在“告警通知”页面，单击“查看消息通知服务主题”，进入SMN服务。创建新的主题，具体操作请参见创建主题。

图 3-38 查看消息通知服务主题

主题未订阅

创建主题后，您需要为该主题添加一个或多个订阅，并按接收到的消息提示确认订阅，否则将无法选到该主题，确认订阅请参见添加订阅。

3.5.4 是否可以不开启 HSS 告警通知?

可以不开启HSS告警通知。

若您开启了主机防护，没有设置告警通知，您将无法接收到HSS发送的告警通知，及时了解主机/网页的安全风险。若需要了解主机的安全风险，您只能登录管理控制台自行查看。

设置告警通知

开启主机安全防护后，若您想设置告警通知，可以通过以下两种方式进行设置。

- 基础版/企业版/旗舰版
  - 选择“主机管理”页面，在“使用指引”的“设置告警通知”中，单击“告警通知设置”，设置告警通知。

图 3-39 设置告警通知

– 选择“安装与配置 > 告警通知”，设置告警通知。

- 网页防篡改版

  选择“网页防篡改 > 安装与配置 > 告警通知”，设置告警通知。

取消告警通知

开启主机安全防护后，若您不想收到HSS的告警通知，您可以取消设置HSS告警通知。取消告警通知后，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警短信或邮件。

取消设置HSS告警通知方式，如下所示：

- 方式一：删除消息通知主题

  删除主题后，您配置的告警通知将不会生效。
- 方式二：删除消息通知主题中的订阅

  删除订阅后，您将不会收到告警通知。
- 方式三：取消或关闭消息通知主题中的订阅

  取消订阅后，您将不会收到告警通知。

3.5.5 如何修改告警通知的通知项?

开启主机安全防护后，若您不想收到HSS的某项告警通知，您可以取消设置的HSS告警通知项。取消某项告警通知后，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警短信或邮件。

基础版/企业版/旗舰版

步骤1 登录管理控制台。

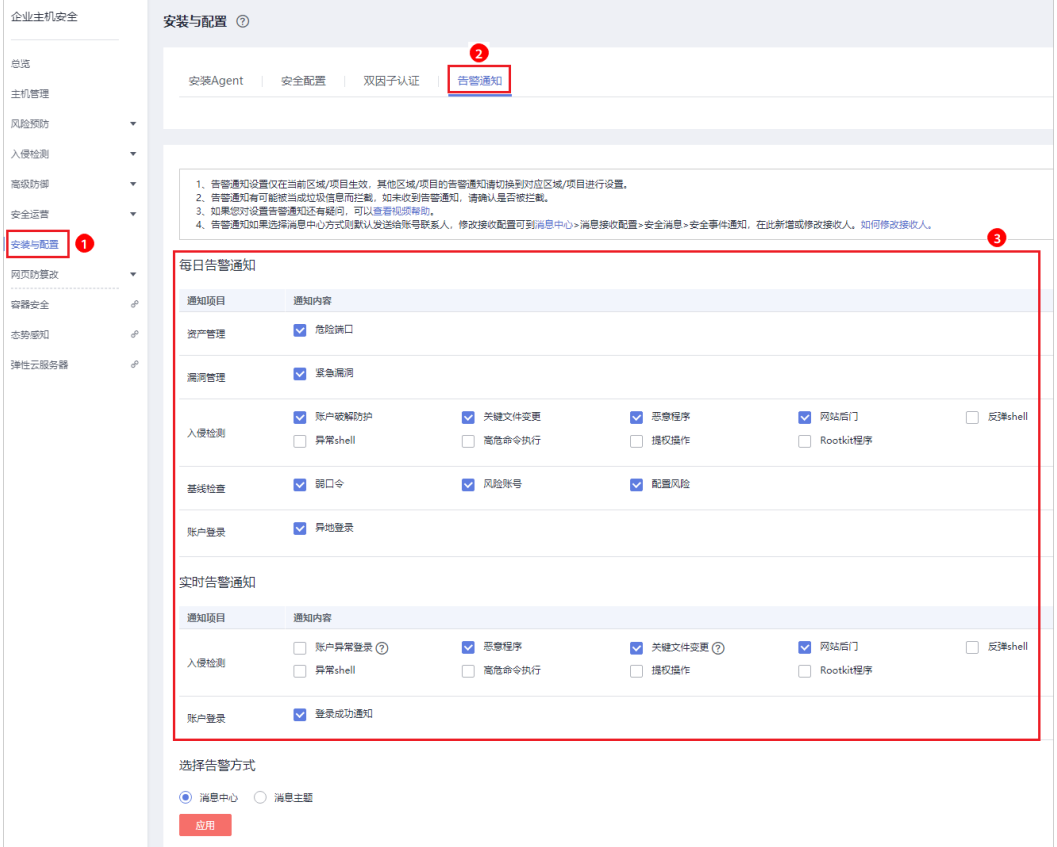
步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 企业主机安全”，进入企业主机安全页面。

图 3-40 企业主机安全

步骤3 在左侧导航树中，选择“安装与配置”，进入安装与配置界面。

步骤4 选择“告警通知”页签，进入“告警通知”页面，如图3-41所示。

图 3-41 基础版/企业版/旗舰版



步骤5 修改勾选“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 3-9 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”。

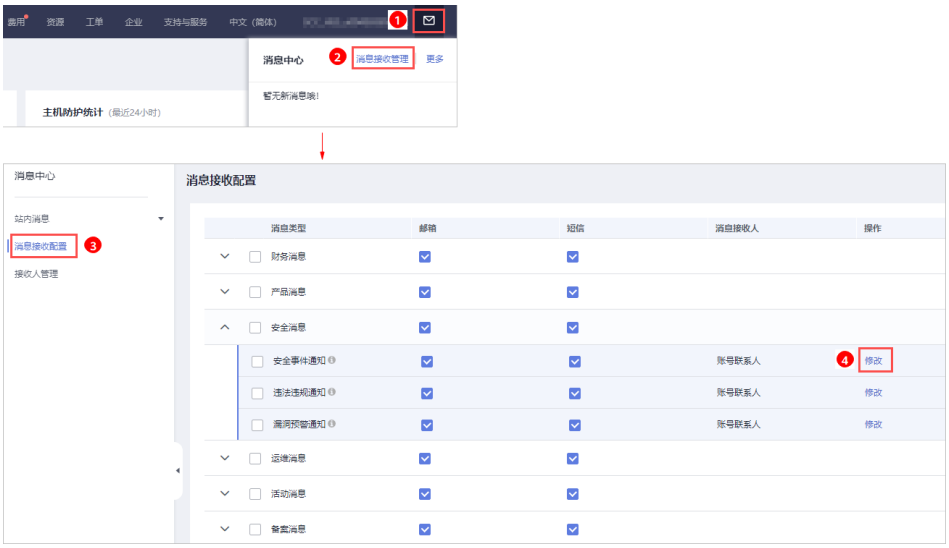
通知项	说明	选择建议
实时告警通知	当攻击者入侵主机时，企业主机安全服务将按照选定的“消息中心”或者“消息通知服务主题”为您告警。	• 建议您接收实时告警通知中所有的内容并及时查看。企业安全服务实时监测主机中的安全情况，能监测到攻击者入侵主机的行为，接收实时告警通知能快速处理攻击者入侵主机的行为。 • 由于实时告警中通知项的内容紧急度较高，如果您使用的“消息通知服务”，接收告警通知，建议您选择“订阅终端”配置为“短信”的“消息通知服务主题”。

步骤6 选择设置的告警方式，“消息中心”或者“消息主题”告警通知方式。

- 选择“消息中心”。

  告警通知默认发送给帐号联系人，新增或修改接收人，请前往“消息中心 > 消息接收配置 > 安全消息 > 安全事件通知”进行修改，具体操作请参见**修改指定消息接收人**。

  图 3-42 新增或修改接收人



- 选择“消息主题”。单击下拉列表选择需要更改接收**消息通知类型**的**消息通知主题**。

步骤7 单击“应用”，完成修改主机安全告警通知的操作。界面弹出“告警通知设置成功”提示信息，则说明告警通知设置成功。

若涉及多个**消息通知主题**更改，请重复**步骤5**~**步骤7**操作。

----结束

4 告警事件处理

4.1 收到 HSS 的告警通知，如何查找到相关信息并处理?

如何查看

企业主机安全发出的告警，在安全控制台上可以查看到详细信息。

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。

如何处理

企业主机安全提供漏洞修复方法、入侵事件排查/处理方法、风险配置修复建议，详细操作请参见快速提升主机安全性。

告警处理建议

- 漏洞告警，请根据HSS提供的修复紧急度结合业务进行修复漏洞，详细操作请参见漏洞修复与验证。
- 入侵检测告警处理建议，请参见入侵检测告警处理建议。
- 基线检查告警，详细操作请参见基线检查风险项修复建议。

4.2 帐户暴力破解问题

4.2.1 HSS 如何拦截帐户暴力破解?

拦截范围

HSS可拦截的攻击类型包括：mysql、sqlsever 2012、vsftp、ssh、rdp。

若您的服务器上安装了MySQL或者vsftp，开启主机安全防护之后，Agent会在iptables里面新增一些规则，用于mysql/vsftp爆破防护。当检测到爆破行为后会将爆破IP加入到阻断列表里面，新增的规则如图4-1所示。

图 4-1 新增规则

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
IN_HIDS_MYSQLD_BIP_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3306
IN_HIDS_MYSQLD_DENY_DROP  tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3306

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_BIP_DROP (1 references)
target     prot opt source               destination

Chain IN_HIDS_MYSQLD_DENY_DROP (1 references)
target     prot opt source               destination
```

须知

不建议删除已添加的iptables规则，若删除iptables规则，HSS将无法防护mysql/vsftp被暴力破解。

帐户破解拦截原理

暴力破解是一种常见的入侵攻击行为，通过暴力破解或猜解主机密码，从而获得主机的控制权限，会严重危害主机的安全。

通过暴力破解检测算法和全网IP黑名单，若发现暴力破解主机的行为，HSS会对发起攻击的源IP进行拦截，SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。**若被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。同时HSS支持**双因子认证**功能，双重认证用户身份，有效阻止攻击者对主机帐号的破解行为。

您可以**配置常用登录IP**、**配置SSH登录IP白名单**，常用登录IP、SSH登录IP白名单中的IP登录行为不会被拦截。

说明

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

告警策略

- 如果黑客暴力破解密码成功，且成功登录您的服务器，会立即发送实时告警通知用户。
- 如果检测到暴力破解攻击并且评估认为帐户存在被破解的风险，会立即发送实时告警通知用户。
- 如果该次暴力破解没有成功，主机上也没有已知风险项（不存在弱口令），评估认为帐户没有被破解的风险时，不会发送实时告警。企业主机安全服务会在每天发送一次的每日告警信息中通告当日攻击事件数量。您也可以登录企业主机安全控制台入侵检测页面实时查看拦截信息。

查看帐户破解检测结果

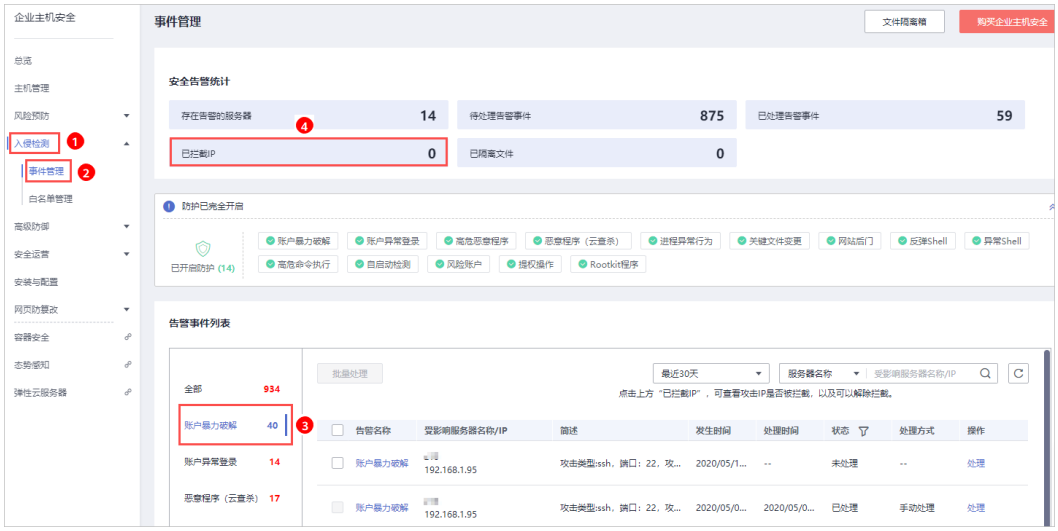
步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 4-2 企业主机安全

步骤3 进入“帐户暴力破解”页面，查看已防护的服务器上的暴力破解拦截记录，如图4-3所示。

图 4-3 帐户破解防护



步骤4 单击“已拦截IP”，可查看已拦截的攻击源IP、攻击类型、拦截次数、开始拦截时间和最近拦截时间，以及拦截状态。

- 已拦截：表示该暴力破解行为已被HSS成功拦截。
- 已解除：表示您已解除对该暴力破解行为的拦截。

说明

SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。**若被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截。**

----结束

处理拦截 IP

- 如果发现某个主机被频繁攻击，需要引起重视，建议及时修补漏洞，处理风险项。

  建议开启**双因子认证**功能，并**配置常用登录IP**、**配置SSH登录IP白名单**。
- 如果发现有合法IP被误封禁（比如运维人员因为记错密码，多次输错密码导致被封禁），可以**手动解除拦截IP**。

须知

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

4.2.2 帐户被暴力破解，怎么办?

- 若您的主机被暴力破解成功，攻击者很可能已经入侵并登录您的主机，窃取用户数据、勒索加密、植入挖矿程序、DDoS木马攻击等恶意操作。
- 若您的主机被尝试暴力破解，攻击源IP被HSS拦截，请及时采取有效的措施预防帐户暴力破解事件。

排查思路

以下排查思路按照收到帐户暴力破解告警通知的状态进行逐层细化，您可以根据帐户暴力破解的实际情况选择对应的分支进行排查。

图 4-4 排查思路

帐户被暴力破解，攻击源 IP 已成功登录

若您收到帐户暴力破解成功的告警信息，例如“**【帐户被爆破告警】企业主机安全服务当前检测到您XX区域的云服务器XX的帐户被破解，已成功登录：攻击源IP：10.108.1.1，攻击类型：ssh**”，则说明您的主机被暴力破解成功，建议您尽快加固您的主机安全。

步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 4-5 企业主机安全

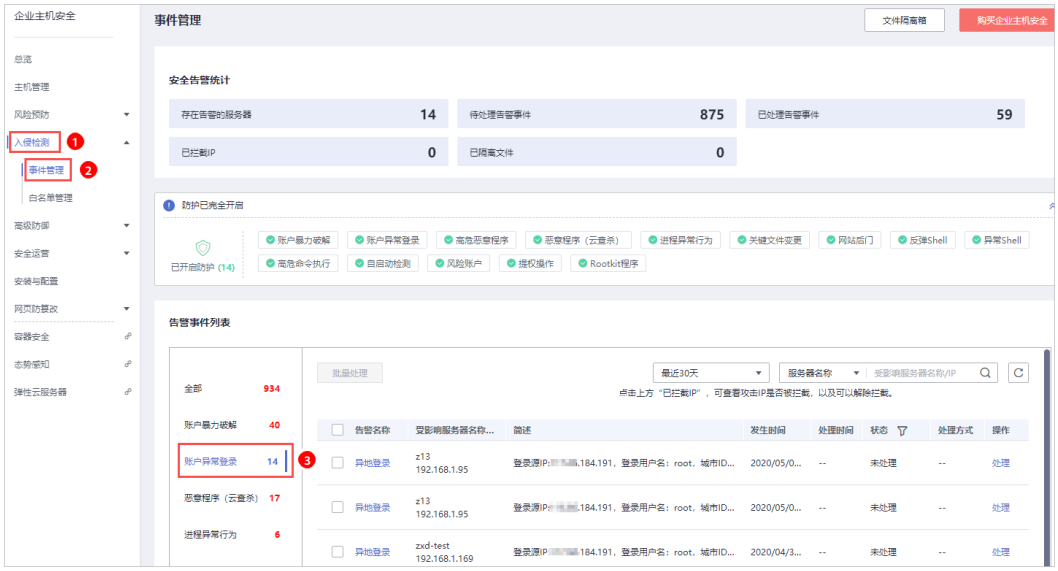
步骤3 **判断源IP的合法性。**

选择“入侵检测 > 事件管理”页面，进入“帐户异常登录”页面，查看成功登录主机的源IP是否为合法IP。

- 若源IP合法（多次输错口令，但未达到拦截IP条件，成功登录），您可以单击“处理”，忽略该事件。
- 若源IP不合法，是未知IP，那么您主机系统已经被入侵成功。

  请单击该事件并标记为“手动处理”，并登录被攻击的主机，尽快修改该主机的系统帐户口令，口令设置方法请参见**如何设置安全的口令?**

图 4-6 帐户异常登录



步骤4 **排查并处理恶意程序。**

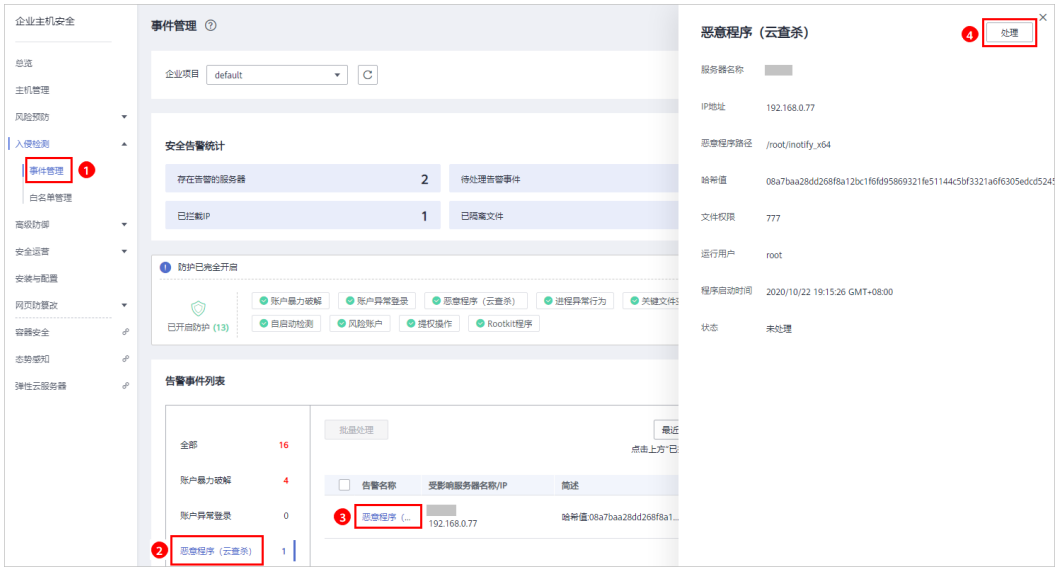
选择“恶意程序（云查杀）”排查系统是否被植入了恶意程序。

- 若被植入了恶意程序，请根据检测结果中提示的“恶意程序路径”、“运行用户”、“程序启动时间”等信息，分析、判断哪些确实是恶意程序。

  针对恶意程序，单击恶意程序告警事件，并单击“处理”，选择“隔离查杀”，立即终止恶意程序进程。

- 若没有被植入恶意程序，请执行**步骤5**。

图 4-7 恶意程序（云查杀）



步骤5 排查并处理可疑帐号。

选择“风险预防 > 帐号信息管理”，排查并处理系统中的可疑帐号，防止攻击者创建新的帐户或更改帐户权限（例如：将某个原来不具备登录权限的帐户修改为具备登录权限），详细信息请参见**帐号信息管理**。

步骤6 排查并处理风险帐户。

选择“入侵检测 > 事件管理”中的“风险帐户”排查所有系统帐户，对风险帐户进行处理，详细信息请参见**处理风险帐号**。

步骤7 使用基线检查功能进行风险检测，并根据建议处理风险项。

检测主机中的口令复杂度策略，关键软件中含有风险的配置信息，详细信息请参见**基线检查**。

步骤8 加固您的服务器安全。

- Linux主机SSH登录的安全加固，详细信息请参见**Linux云服务器SSH登录的安全加固**。
- 您也可以根据**如何预防帐户暴力破解攻击？**章节，加强主机帐户暴力破解防护。

----结束

帐户被尝试破解，攻击源 IP 被拦截

若30秒内，帐户暴力破解次数达到5次及以上，或者3600秒内，帐户暴力破解次数达到15次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因帐户破解被入侵，请及时确认该源IP是否为可信IP。

约束与限制

- Linux操作系统

  使用鲲鹏计算EulerOS（EulerOS with ARM）和Centos 8.0及以上版本的主机，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。

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。

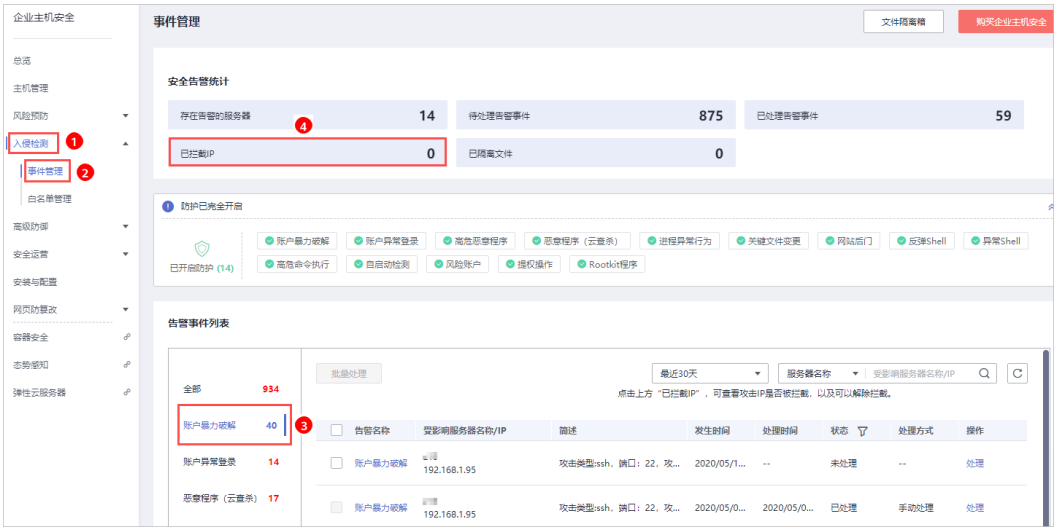
图 4-8 企业主机安全

步骤3 选择“入侵检测 > 事件管理”，选择“帐户暴力破解”，查看帐户暴力破解事件。

出现帐户暴力破解告警事件，说明您的主机可能存在被暴力破解风险。

- 系统存在弱口令，同时正在遭受暴力破解攻击，攻击IP被拦截。
- 数次口令输错后，源IP被拦截。

图 4-9 帐户暴力破解事件



步骤4 建议您立即确认源IP是否是已知的合法IP。

- 若源IP合法。

- 选择帐户暴力破解事件，单击“处理”，并标记为“忽略”或者“加入告警白名单”。

  将该事件“忽略”或者“加入告警白名单”，均不会解除拦截的IP。
- 若需要解除拦截的IP，请单击“已拦截IP”，立即解除拦截的IP，或者当HSS检测到超过默认拦截时间后，主机不再被暴力破解攻击，将会自动解除拦截。

  SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。

- 若源IP不合法，是未知IP。

  请选择发生的帐户暴力破解事件，单击“处理”，并标记为“手动处理”。

  立即登录主机系统，修改并设置安全的帐户密码，并加固您的主机安全。您也可以参照如何预防帐户暴力破解攻击？章节，加强主机帐户暴力破解防护。

----结束

相关问题

- HSS如何拦截帐户暴力破解？
- 如何手动解除误拦截IP？

4.2.3 如何预防帐户暴力破解攻击？

暴力破解来源

攻击源可分为华为云攻击源和非华为云攻击源。

华为云攻击源：被攻击原因及处理办法详情请参见收到来自华为云IP的暴力破解告警如何处理？，日常预防措施请参见预防措施。

非华为云攻击源：被尝试破解或已被破解告警信息处理办法详情请参见帐户被暴力破解，怎么办？，日常预防措施详情请参见预防措施。

预防措施

在企业主机安全已有的防护能力基础之上，可以从安全产品、应用、网络防护层面出发，做到全方位预防暴力破解。

- **安全产品层面**
  - **开启云堡垒机**

    可对主机资源、应用服务器进行统一纳管，提供登录认证、资源管理、会话审计等功能。云堡垒机功能特性详情请参见功能特性。快速使用详情请参见快速入门。

    开启云堡垒机后，入侵、破解将优先被云堡垒机监测拦截告警，与HSS形成双重防护。
- **应用层面**
  - **使用SSH KEY登录**

    为主机资源、应用服务器开启SSH KEY密钥登录，在每次登录时要求公钥和私钥必须相匹配才可登录成功。创建密钥对详情请参见创建密钥对。
  - **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、登录验证码，对云服务器登录行为进行二次身份认证。

在“双因子认证”页面，勾选需要开启双因子的主机，单击“开启双因子认证”，开启双因子认证。详细操作请参见双因子认证。

- **网络层面**
  - **配置SSH登录白名单**

    SSH登录白名单功能是防护帐户破解的一个重要方式，配置后，在开启密钥登录的基础之上只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。详细操作请参见配置SSH登录IP白名单。
  - **修改默认端口**

    将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。详细操作请参见怎样修改远程登录的端口？。
  - **设置安全组规则，限制攻击源IP访问您的服务端口**

    说明

    建议设置对外开放的远程管理端口（如SSH、远程桌面登录），只允许固定的来源IP进行连接。

    账户破解防护可实时检测攻击者对主机中帐户的暴力破解攻击，拦截攻击源IP。您可以通过配置安全组规则来限制攻击源IP访问您的服务端口。

    如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。

    例：仅允许特定IP地址（例如，192.168.20.2）通过SSH协议访问Linux操作系统的弹性云服务器的22端口，安全组规则如下所示：

    表 4-1 仅允许特定 IP 地址远程连接云服务器

方向	协议应用	端口	源地址
入方向	SSH（22）	22	例如：192.168.20.2/32

  - **设置安全强度高的口令**

    口令复杂度策略检测和弱口令检测可检测出主机系统中使用弱口令的帐户，您可以在控制台查看并处理主机中的口令风险。

    口令的设置方法请参见如何设置安全的口令复杂度策略、如何设置安全的口令。

4.2.4 如何解决部分 Linux 系统的帐户破解防护功能未生效的问题？

故障原因

主机系统中SSHD服务没有依赖libwrap.so。

说明

libwrap是一个免费的软件程序库，实现了通用的TCP Wrapper功能。任何包含了libwrap.so的daemon程序可以使用/etc/hosts.allow和/etc/hosts.deny文件中的规则对主机进行简单的访问控制。

解决方法

登录云服务器安装企业主机安全Agent，详细操作请参见安装Agent章节（云服务器需要绑定弹性IP），然后执行下面的命令：

sh /usr/local/hostguard/conf/config_ssh_xinetd.sh。

存在问题的镜像版本

- Gentoo的镜像存在该问题的版本如下：
  - Gentoo Linux 17.0 64bit（40GB）
  - Gentoo Linux 13.0 64bit（40GB）
- OpenSUSE的镜像存在该问题的版本如下：
  - OpenSUSE 42.2 64bit（40GB）
  - OpenSUSE 13.2 64bit（40GB）

4.2.5 如何手动解除误拦截 IP?

在30秒内，帐户暴力破解次数达到5次及以上，或者3600秒内，帐户暴力破解次数达到15次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因帐户破解被入。若已拦截IP为合法IP被误封禁（比如运维人员因为记错密码，多次输错密码导致被封禁），您可以参照本章节手动解除拦截IP。

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

说明

- SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。
- 当HSS检测到拦截IP超过默认拦截时间后，主机不再被暴力破解攻击，将会自动解除拦截。

手动解除拦截 IP

步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 4-10 企业主机安全

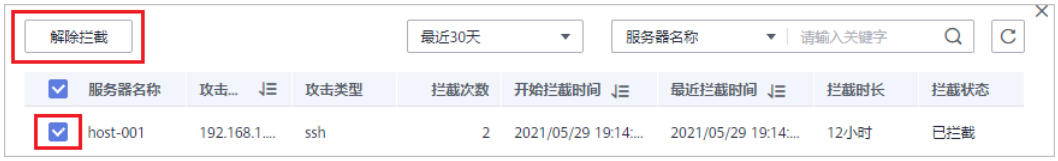
步骤3 在左侧导航树中，选择“入侵检测 > 事件管理”。

步骤4 在安全告警统计区域中，单击“已拦截IP”。

图 4-11 已拦截 IP

步骤5 在弹出的“已拦截IP”页面，勾选误禁IP后，单击列表上方的“解除拦截”，解除拦截IP。

图 4-12 解除拦截 IP



----结束

4.2.6 频繁收到 HSS 暴力破解告警如何处理?

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。

可能原因：由于您服务器的远程连接端口没做访问控制，导致网络上的病毒频繁攻击您服务器端口。

解决方案：您可通过以下方式来改善被频繁暴破攻击的情况，降低风险：

1. 配置白名单
2. 修改端口
3. 设置安全组规则
4. 开启双因子认证
5. 设置高强度口令

操作详情请参见**如何预防账户暴力破解攻击?**

4.2.7 收到来自华为云 IP 的暴力破解告警如何处理?

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。

被攻击原因

使用华为云服务器的用户中，有少部分用户存在口令设置简单、端口易被猜测、未使用安全防护产品等情况，导致被暴破攻击，攻击者利用被暴破攻击的用户服务器作为攻击源，对其他用户发起二次攻击，因此会受到来自华为云IP的攻击。

处理办法

- 发现此类告警，建议第一时间在安全组中对告警的IP进行限制，操作详情请参见**添加安全组规则**。
- 出现此类告警的第一时间，华为云的安全防护就会进行拦截，随后会对这些用户进行告警，并要求在7个自然日内整改完成，超过7个自然日未完成整改，将直接冻结该用户的eip，直到整改完成才能恢复正常使用。

说明

- 您可以通过设置高强度口令、修改端口等方法来改善服务的安全状况，更多方法和具体操作详情请参见**如何预防账户暴力破解攻击?** 。
- 您可以通过购买防护配额对主机进行防护，增强安全能力，购买详情请参见**购买防护配额**，版本差异详情请参见**服务版本差异**。

4.3 弱口令和风险帐号问题

4.3.1 出现弱口令告警，怎么办?

若您收到弱口令告警，则说明您的主机存在被入侵的风险。数据、程序都存储在系统中，若密码被破解，系统中的数据和程序将毫无安全可言，请及时修改弱口令。

出现弱口令告警的原因

- 设置的自动生成密码的方式过于简单，与弱口令检测的密码库相重合。
- 将同一密码用于多个子账号，会被系统判定为弱密码。

排查弱口令

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“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。

图 4-13 企业主机安全

步骤3 选择“风险预防 > 基线检查”，单击“经典弱口令检测”，查看存在的弱口令。

图 4-14 经典弱口令

步骤4 根据经典弱口令列表中的“弹性云服务器名称”、“账号名”、“账号类型”和“弱口令使用时长”，登录待修改弱口令的主机，修改弱口令。

----结束

修改常见的服务器弱口令

系统名称	修改登录口令	说明
Windows系统	以Windows 10为例说明。 1. 登录Windows主机系统。 2. 单击左下角的，然后单击，弹出“Windows设置”窗口。 3. 在“Windows设置”窗口中，单击“账户”。 4. 在左侧导航栏中，单击登录选项。 5. 在“登录选项”页面，请根据页面提示信息修改服务器密码。	无
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 **passswd [<user>]**	若不输入登录用户名，则修改的是当前用户的口令。 命令执行完成后，请根据提示输入新的口令。 **说明** “user”为登录用户名。

系统名称	修改登录口令	说明
MySQL数据库	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 **SELECT user, host, authentication_string From user;** 部分MySQL数据库版本可能不支持以上查询命令。 若执行以上命令没有获取到用户密码信息，请执行命令。 **SELECT user, host password From user;** 3. 执行以下命令，根据查询结果及弱密码告警信息，修改具体用户的密码。 **SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');** 4. 执行以下命令，刷新修改的密码信息。 **flush privileges;**	无
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 **requirepass <password>;**	● 若已存在登录口令，则将其修改为复杂口令。 ● 若不存在登录口令，则添加为新口令。 **说明** “password”为登录口令。
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

4.3.2 如何设置安全的口令?

请按如下建议设置口令：

- 使用复杂度高的密码。

  建议密码复杂度至少满足如下要求：

  a. 密码长度至少8个字符。

  b. 包含如下至少三种组合：

     i. 大写字母（A~Z）

     ii. 小写字母（a~z）

     iii. 数字（0~9）

iv. 特殊字符

c. 密码不为用户名或用户名的倒序。

- 不使用有一定特征和规律容易被破解的常用弱口令。
  - 生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份
  - 数字或字母连排或混排，常用彩虹表中的密码、滚键盘密码。
  - 短语密码
  - 公司名称、admin、root等常用词汇
- 不使用空密码或系统的缺省密码。
- 不要重复使用最近5次（含5次）内已使用的密码。
- 不同网站/账号使用不同的密码。
- 根据不同应用设置不同的账号密码，不建议多个应用使用同一套账户/密码。
- 定期修改密码，建议至少每90天更改一次密码。
- 账号管理人员初次发放或者初始化密码给用户时，如果知道密码内容，建议强制用户首次使用修改密码，若不能强制用户修改密码，则为密码设置过期的期限（用户必须及时修改密码，否则密码应被强制失效）。
- 建议为所有账户配置设置连续认证失败次数超过5次（不含5次），锁定账号策略和30分钟自动解除锁定策略。
- 建议对所有账户设置不活动时间超过10分钟自动退出或锁定策略。
- 新建系统中的账号缺省密码在首次使用前，建议强制用户更改。
- 建议开启账户登录记录日志功能，登录日志最少保存180天，登录日志中不能保存用户的密码。

4.3.3 关闭弱口令策略后，之前扫描的弱口令事件为什么还会重复出现?

若您在关闭弱口令策略前，已经修改弱口令事件，进行重新检测并符合弱口令检测要求，该弱口令事件不会在重复出现。

若您在关闭弱口令策略前，未修改弱口令事件，已经检测出来的结果不会改变，系统也将不再进行新的检测且历史检测结果会保留30天。

- 为保障您的主机安全，请您及时修改登录主机系统时使用弱口令的帐号，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，建议您立即执行手动检测，查看弱口令修复结果。如果您未进行手动验证且未关闭弱口令检测，HSS会在次日凌晨执行自动验证。

4.4 入侵告警问题

4.4.1 主机被挖矿攻击，怎么办？

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。

黑客入侵主机后植入挖矿程序，挖矿程序会占用CPU进行超高运算，导致CPU严重损耗，并且影响主机上其他应用的运行。当您的主机被挖矿程序入侵，挖矿程序可能进行内网渗透，并在被入侵的主机上持久化驻留，从而获取最大收益。

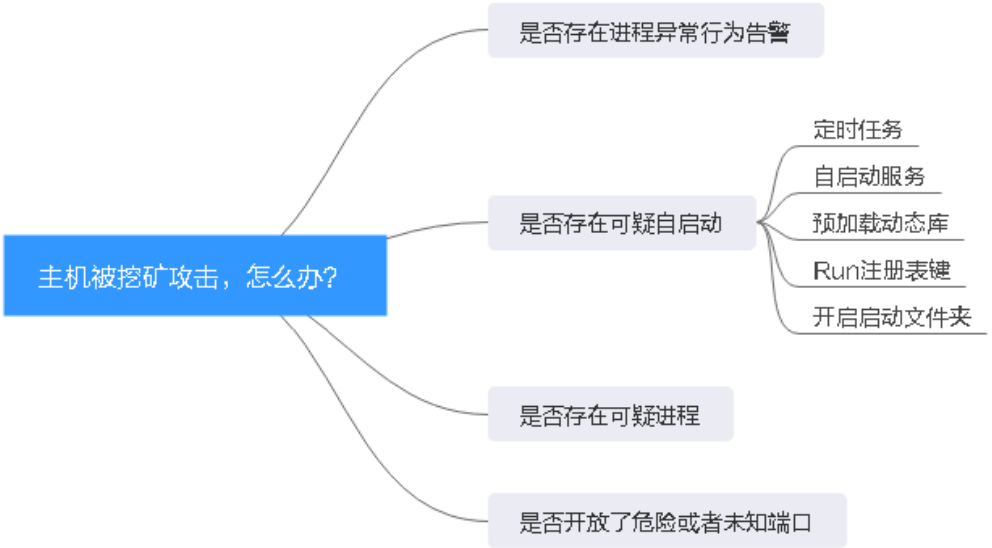
当主机提示有挖矿行为时，请确定并清除挖矿程序，并及时对主机进行安全加固。

确定并清除挖矿程序

排查思路

以下排查思路按照“挖矿程序”入侵并驻留的地方进行逐层排查，您可以根据被挖矿攻击的实际情况选择对应的分支进行排查。

图 4-15 排查思路



操作步骤

步骤1 登录管理控制台。

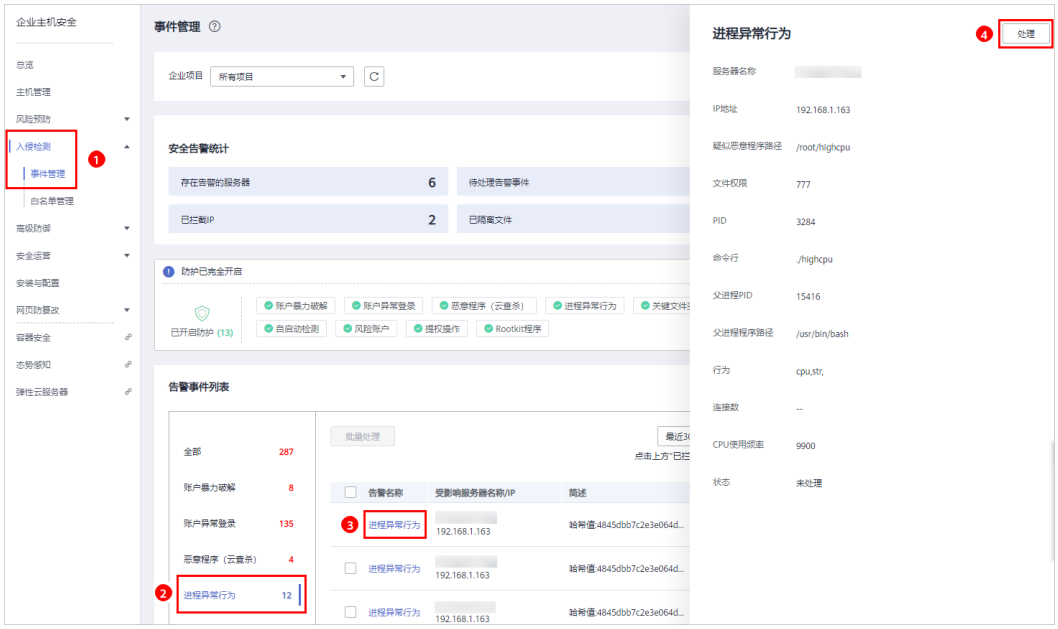
步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 企业主机安全”，进入企业主机安全页面。

图 4-16 企业主机安全

步骤3 排查进程异常行为，若出现主机挖矿行为，会触发HSS发送“进程异常行为”告警。

选择“入侵检测 > 事件管理”，选择“进程异常行为”，查看并处理发生的异常进程行为告警。您可以单击“处理”，对挖矿程序进行隔离查杀。

图 4-17 处理进程异常行为



步骤4 排查定时任务，大部分挖矿程序会在受感染的主机中写入定时任务，完成程序的驻留，当您只清除挖矿程序时，定时任务会再次从主机下载挖矿进程或者直接执行挖矿脚本，导致挖矿进程清除失败。

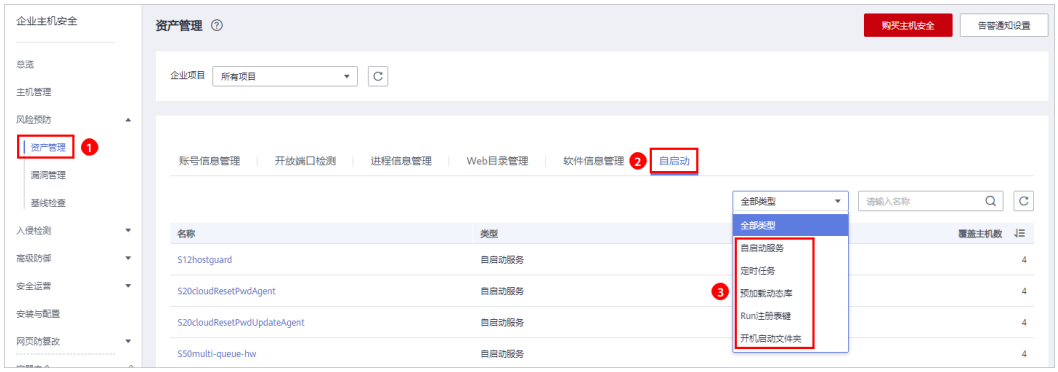
选择“风险预防 > 资产管理”，单击“自启动”，选择“定时任务”，查看异常定时任务。

图 4-18 排查定时任务

步骤5 排查其他自启动项，有的挖矿进程为了实现长期驻留，会向系统中添加自启动项来确保系统重启后仍然能重新启动，因此，需要及时清除可疑的自启动项。

选择“风险预防 > 资产管理”，单击“自启动”，分别选择“自启动服务”、“预加载动态库”、“Run注册表键”、“开启启动文件夹”，逐个排查自启动项。

图 4-19 排查自启动项

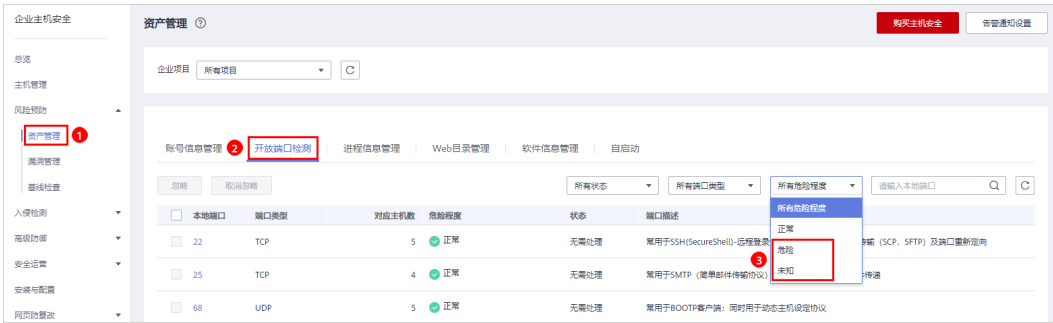


步骤6 排查可疑进程信息，快速查看主机中存在的可疑应用进程，并及时终止可疑的应用进程。

图 4-20 排查可疑进程

步骤7 排查是否开放了危险或者未知端口，及时关闭危险或者未知端口。

图 4-21 排查开放端口



步骤8 若通过以上手段均无法删除挖矿程序，请重装系统。

----结束

主机安全加固

挖矿程序清除后，为了保障主机安全，请及时对主机进行安全加固。

Linux加固建议

1. 使用HSS**每日凌晨**自动进行一次全面的检测，帮助您深度防御主机和应用方面潜在的安全风险。详细信息请参见**快速掌握主机安全态势**。
2. 修改系统所有帐号口令（包括系统帐户和应用帐户）为符合规范的强口令，或将主机登录方式改为密钥登录彻底规避风险。
   a. 设置安全口令，详细操作请参见**如何设置安全的口令？**。
   b. 使用密钥登录主机，详细操作请参见**使用私钥登录Linux主机**。
3. 严格控制系统管理员帐户的使用范围，为应用和中间件配置各自的权限和并严格控制使用范围。
4. 使用安全组定义访问规则，根据业务需求对外开放端口，对于特殊业务端口，建议设置固定的来源IP（如：远程登录）或使用VPN、堡垒机建立自己的运维通道，详细操作请参见**安全组规则**。

Windows加固建议

使用HSS全面体检并深度防御主机和应用方面潜在的安全风险，同时您还可以对您的Windows系统进行帐户安全加固、口令安全加固和授权安全加固。

- **帐户安全加固**

帐户	说明	操作步骤
默认帐户安全	• 禁用Guest用户 • 禁用或删除其他无用帐户（建议先禁用帐户三个月，待确认没有问题后删除）	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组 > 用户”。 4. 双击**Guest**用户，在弹出的Guest属性窗口中，勾选“帐户已禁用”。 5. 单击“确定”，完成Guest用户禁用。

帐户	说明	操作步骤
按照用户分配帐户	根据业务要求，设定不同的用户和用户组。 例如，管理员用户，数据库用户，审计用户等。	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组”，根据业务要求，设定不同的用户和用户组，包括管理员用户，数据库用户，审计用户等。
定期检查并删除无关帐户	定期删除或锁定与设备运行、维护等与工作无关的帐户。	1. 打开控制面板。 2. 选择“管理工具 > 计算机管理”。 3. 选择“系统工具 > 本地用户和组”。 4. 单击“用户”或者“用户组”，在用户或者用户组页面，删除或锁定与设备运行、维护等与工作无关的帐户。
不显示最后的用户名	配置登录登出后，不显示用户名称。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 安全选项”。 4. 双击“交互式登录：不显示最后的用户名”。 5. 在弹出的“交互式登录：不显示最后的用户名”属性窗口中，选择“启用”，并单击确定。

- **口令安全加固**

口令	说明	操作步骤
复杂度	必须满足**如何设置安全的口令？**的要求。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“帐户策略 > 密码策略”。 4. 确认“密码必须符合复杂性要求”已启用。
密码最长留存期	对于采用静态口令认证技术的设备，帐户口令的留存期不应长于90天。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“帐户策略 > 密码策略”。 4. 配置“密码最长使用期限”不大于90天。

口令	说明	操作步骤
帐户锁定策略	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次后，锁定该用户使用的帐户。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“帐户策略 > 帐户锁定策略”。 4. 配置“帐户锁定阈值”不大于10次。

- **授权安全加固**

授权	说明	操作步骤
远程关机	在本地安全设置中，从远端系统强制关机权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“从远端系统强制关机”，权限只分配给Administrators组。
本地关机	在本地安全设置中关闭系统权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“关闭系统”，权限只分配给Administrators组。
用户权限指派	在本地安全设置中，取得文件或其它对象的所有权的权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“取得文件或其他对象的所有权”，权限只分配给Administrators组。
授权帐户登录	在本地安全设置中，配置指定授权用户允许本地登录此计算机。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“允许本地登录”，权限给指定授权用户。
授权帐户从网络访问	在本地安全设置中，只允许授权帐号从网络访问（包括网络共享等，但不包括终端服务）此计算机。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“从网络访问此计算机”，权限给指定授权用户。

4.4.2 添加告警白名单后，为什么进程还是被隔离?

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

隔离查杀恶意程序

- 方式一：在“安装与配置 > 安全配置 > 恶意程序隔离查杀”中，开启自动隔离查杀。
- 方式二：在“入侵检测 > 事件管理 > 告警事件列表”中，将恶意程序手动隔离查杀。

隔离查杀后，该程序无法执行“读/写”操作，同时该程序的进程将被立即终止。HSS将程序或者进程的源文件加入文件隔离箱，被隔离的文件不会对主机造成威胁。

恢复隔离查杀文件

- 方式一：在“入侵检测 > 事件管理 > 已隔离文件”中，单击“恢复”，恢复隔离文件。
- 方式二：在“入侵检测 > 事件管理 > 告警事件列表”中，取消隔离查杀。

被隔离查杀的程序恢复隔离后，文件的“读/写”权限将会恢复，但被终止的进程不会再自动启动起来。

4.4.3 提示主机有挖矿行为怎么办?

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。

当主机提示有挖矿行为时：

1. 建议备份数据，关闭不必要的端口。
2. 增强主机密码。
3. 使用企业主机安全服务（HSS），HSS提供帐户破解防护、异地登录检测恶意程序检测、网站后门检测等入侵检测功能，以及软件漏洞、一键查杀恶意程序或修复系统漏洞等功能。

4.4.4 主机对外攻击预警，怎么处理?

你好，您的主机可能中了木马病毒，建议您重装系统，并设置强口令加固服务器及phpstudy、Redis等应用。

- 设置系统所有帐号为符合规范的强密码，不要使用默认密码，或存在键盘特征的密码。
- 根据业务配置安全组策略，非公开的业务端口建议设置固定的来源IP，避免不必要的端口暴露在公网。
- 及时升级系统及应用的最新补丁。
- 定期备份数据。

- 删除或重命名phpmyadmin文件夹。

4.4.5 服务器遭受攻击为什么没有检测出来?

- 若您的主机在开启HSS之前已被入侵，HSS可能无法检测出来。
- 若您购买了主机安全配额但是没有开启防护，HSS无法检测出来。
- HSS主要是防护主机层面的攻击，若攻击为web层面攻击，无法检测出来。建议咨询安全SA提供安全解决方案，或者推荐使用安全的其他产品（WAF，DDOS等）。

4.4.6 源 IP 被 HSS 拦截后，如何解除?

源IP被帐户暴力破解、源IP隶属于全网IP黑名单，以及开启IP白名单后，源IP不在IP白名单中时，均会被拦截，请根据具体场景解除拦截。

帐户暴力破解

- 若发现暴力破解主机的行为，HSS会对发起攻击的源IP进行拦截，SSH类型攻击默认拦截12小时，其他类型攻击默认拦截24小时。**若被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。
- 若您确认源IP是可信的IP（比如运维人员因为记错密码，多次输错密码导致被封禁），可单击“入侵检测 > 事件管理”页面下的“已拦截IP”，在弹出的“已拦截IP”页面，可手动解除被拦截的可信IP。

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

全网 IP 黑名单

不能手动解除拦截。

开启 SSH 登录 IP 白名单

若在HSS中**配置SSH登录白名单**，只允许白名单内的IP登录到主机。若需要登录主机，请添加到“SSH登录IP白名单”中。

4.4.7 没有手动解除的 IP 拦截记录为什么会显示已解除?

如果被拦截的IP在24小时内没有再继续暴力破解就会自动解除IP。

4.4.8 HSS 拦截的 IP 是否需要处理?

在收到有拦截IP的告警时，需要您对拦截的IP进行判断，被拦截IP是否为正常业务所使用。

- 如果是您正在使用的业务所属IP，您需将拦截IP**添加至白名单**。
- 如果是非正常业务所使用，则无需处理。

4.4.9 如何防御勒索病毒攻击?

勒索病毒一般通过挂马、邮件、文件、漏洞、捆绑、存储介质进行传播。

因此在云服务器使用期间，可通过**预防帐户暴力破解的措施**来降低风险，及时对企业主机安全服务检测发现的告警进行处理，通常可以达到防止勒索病毒入侵的。

4.5 异常登录问题

4.5.1 添加登录白名单后，为什么还有异地登录告警?

HSS提供的“SSH登录IP白名单”、“登录白名单”和“异地登录”功能，功能差异如表4-2所示。

表 4-2 功能差异

功能名称	实现机制	屏蔽告警
SSH登录IP白名单	将IP加入SSH登录IP白名单，只允许白名单内的IP通过SSH登录指定服务器。 **须知** 启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中。	-
登录白名单	将IP加入登录白名单，用于忽略由该IP登录指定主机发生的帐户暴力破解告警事件。	登录管理控制台。在“入侵检测 > 白名单管理 > 登录白名单”将IP加入登录白名单，HSS将不会对该IP的“帐户暴力破解”登录事件进行告警。
异地登录	当不是来自“常用登录地”或者“常用登录IP”的登录行为时，将会进行异地登录告警。 提醒您有新的IP登录您的主机。	登录管理控制台。在“安装与配置 > 安全配置”中，将“登录地”与“登录IP”添加到“常用登录地”与“常用登录IP”，HSS将不会对来自“常用登录地”和“常用登录IP”的登录行为进行异地告警。

4.5.2 如何查看异地登录的源 IP?

告警策略

异地登录检测功能**实时检测**您服务器上的异地登录行为，您配置常用登录地后，对于在非常用登录地的登录行为HSS会立即进行告警。

在控制台查看异地登录记录

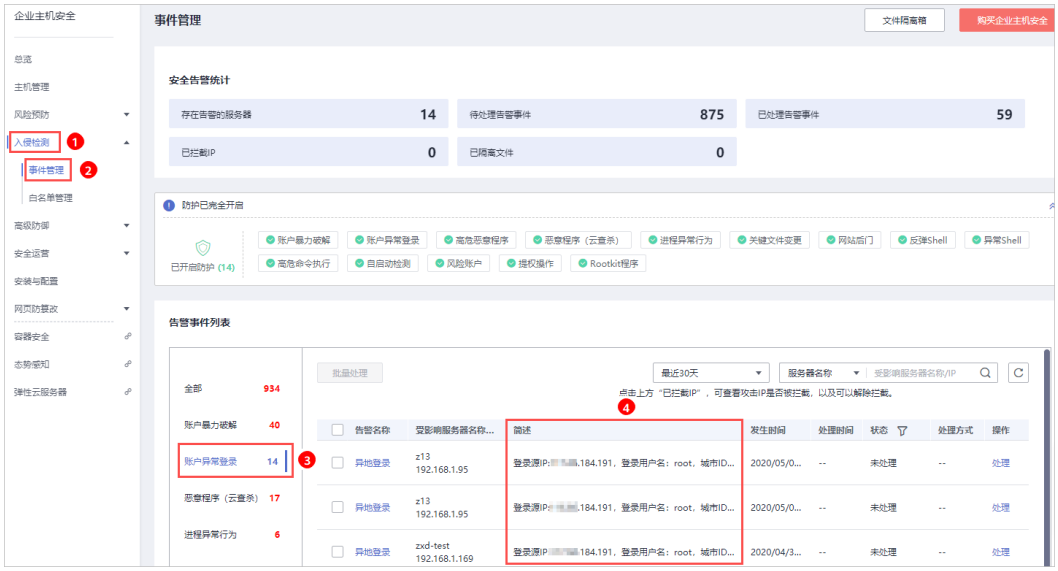
步骤1 登录管理控制台。

步骤2 在页面左上角选择“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。

图 4-22 企业主机安全

步骤3 单击“帐户异常登录”，如图4-23所示。

图 4-23 异地登录



----结束

本地查看登录记录

对于linux主机，您可以在“/var/log/secure”和“/var/log/message”路径下查看日志，或使用**last**命令查看登录记录中是否有异常登录。

4.5.3 收到主机登录成功的告警，怎么处理?

- 若您在“实时告警通知”项目中勾选了“登录成功通知”选项，则任何帐户登录成功的事件都会向您实时发送告警信息。
- 若您所有ECS上的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。
- 若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。
- 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。

4.5.4 是否可以关闭异地登录检测?

不可以关闭异地登录检测。

如果不想接收异地登录的告警通知，您可以将登录地点添加到常用登录地，或者取消勾选告警通知，操作步骤如下所示。

步骤1 登录管理控制台。

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

步骤3 添加常用登录地。

在“常用登录地”页面，单击“添加常用地登录”，将登录地点添加到常用登录地。添加到常用登录地的登录行为，HSS不会进行异地登录告警。

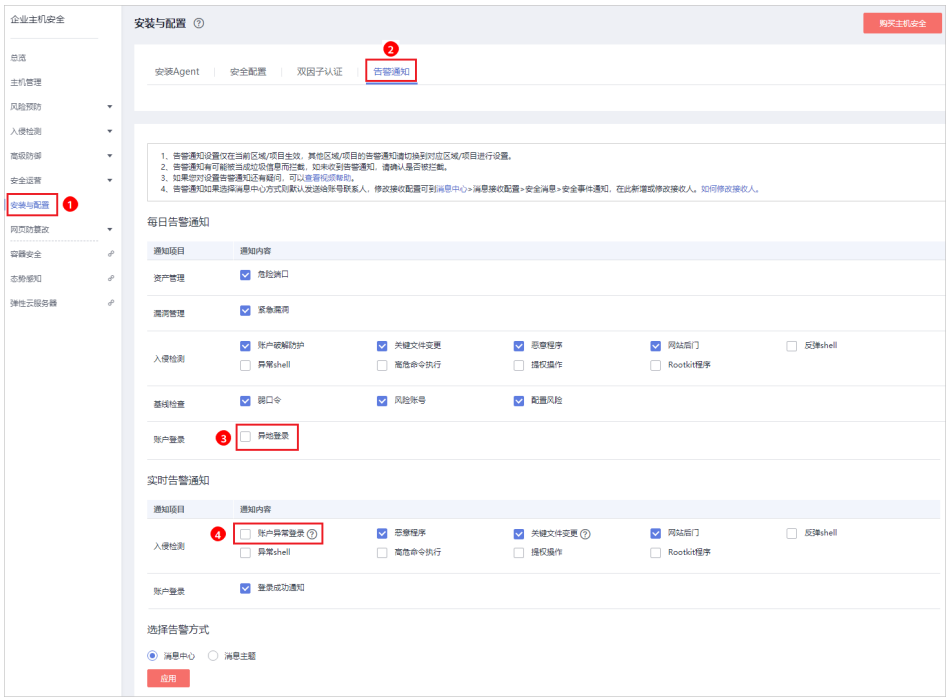
图 4-24 添加常用登录地

步骤4 取消异地登录告警。

在“安装与配置 > 告警通知”页签，取消勾选“每日告警通知”中的“异地登录”和“实时告警通知”中的“帐户异常登录”，如图4-25所示。

帐户异常登录包含异地登录、发生帐户被黑客破解并登录成功事件。如果取消勾选“帐户异常登录”告警通知的选项，当发生帐户被黑客暴力破解时，您将不能实时接收到帐户破解的告警通知，请谨慎操作。

图 4-25 取消勾选异地登录告警通知



----结束

4.5.5 如何确认入侵帐号是否登录成功?

- 若已开启入侵检测告警通知，当有帐号被破解，或有帐号破解风险时，您会立即收到告警通知。
- 也可以在“入侵检测”页面在线查看攻击IP的拦截情况。
- 若想进一步确定，可以在Linux主机上的“/var/log/secure”和“/var/log/message”查看日志，或使用**last**命令查看是否有异常登录记录。

4.6 配置风险问题

4.6.1 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略?

安装 PAM

如果当前系统中未安装PAM（Pluggable Authentication Modules），就无法为系统提供口令复杂度策略检测功能。

若云服务器的操作系统为Debian或Ubuntu，请以管理员用户在命令行终端执行命令**apt-get install libpam-cracklib**进行安装。

说明

CentOS、Fedora、EulerOS系统默认安装了PAM并默认启动。

设置口令复杂度策略

为了确保系统的安全性，建议设置的口令复杂度策略为：口令最小长度不小于8，至少包含大写字母、小写字母、数字和特殊字符中的三种。

说明

以下配置为基础的安全要求，如需其他更多的安全配置，请执行以下命令获取Linux帮助信息。

- 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统

  man pam_pwquality

- 其他Linux系统

  man pam_cracklib

- CentOS、Fedora、EulerOS操作系统

  a. 执行以下命令，编辑文件“/etc/pam.d/system-auth”。

     vi /etc/pam.d/system-auth

  b. 找到文件中的以下内容。

     - 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统：

       password requisite pam_pwquality.so try_first_pass retry=3 type=

     - 其他CentOS、Fedora、EulerOS系统：

       password requisite pam_cracklib.so try_first_pass retry=3 type=

  c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表4-3所示。

     示例：

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

     说明

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

表 4-3 参数说明

参数	说明	示例
minlen	口令最小长度配置项。 PAM默认使用了“credits”，因此最小口令长度需要加1，若需要设置最小口令长度为8，则minlen的值应该设置为9。	minlen=9
dcredit	口令数字要求的配置项。 值为负数N时表示至少有N个数字，值为正数时对数字个数没有限制。	dcredit=-1

参数	说明	示例
ucredit	口令大写字母要求的配置项。 值为负数N时表示至少有N个大写字母，值为正数时对大写字母个数没有限制。	ucredit=-1
lcredit	口令小写字母要求的配置项。 值为负数N时表示至少有N个小写字母，值为正数时对小写字母个数没有限制。	lcredit=-1
ocredit	特殊字符要求的配置项。 值为负数N时表示至少有N个特殊字符，值为正数时对特殊字符个数没有限制。	ocredit=-1

- Debian、Ubuntu操作系统
  a. 执行以下命令，编辑文件“/etc/pam.d/common-password”。
     vi /etc/pam.d/common-password
  b. 找到文件中的以下内容：
     password requisite pam_cracklib.so retry=3 minlen=8 difok=3
  c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表4-3所示。
     示例：
     password requisite pam_cracklib.so retry=3 minlen=9 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

4.6.2 如何在 Windows 主机上设置口令复杂度策略?

为了确保系统的安全性，建议设置的口令复杂度策略为：口令最小长度不小于8位，至少包含大写字母、小写字母、数字和特殊字符中的三种。

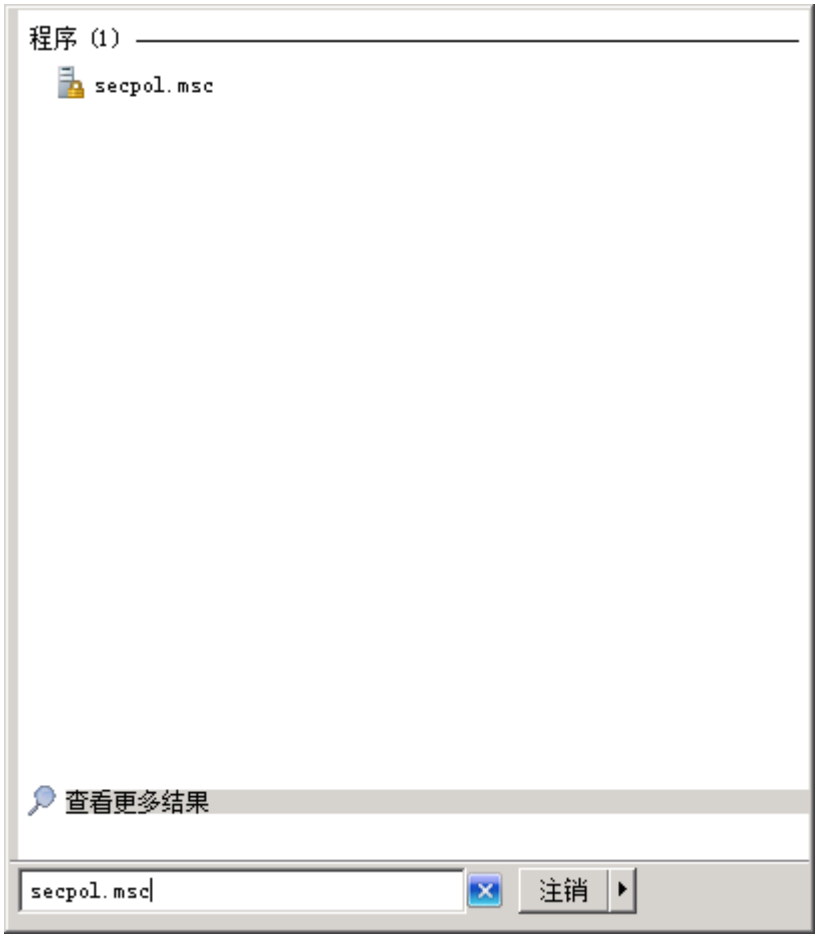
设置本地安全策略中的帐户策略步骤如下：

步骤1 以管理员帐户**Administrator**登录。单击“开始 > 控制面板 > 系统和安全 > 管理工具”，进入管理工具文件夹，双击“本地安全策略”，打开“本地安全策略”控制面板。

说明

也可直接在开始菜单栏输入命令**secpol.msc**直接进入本地安全策略控制面板，如图4-26所示。

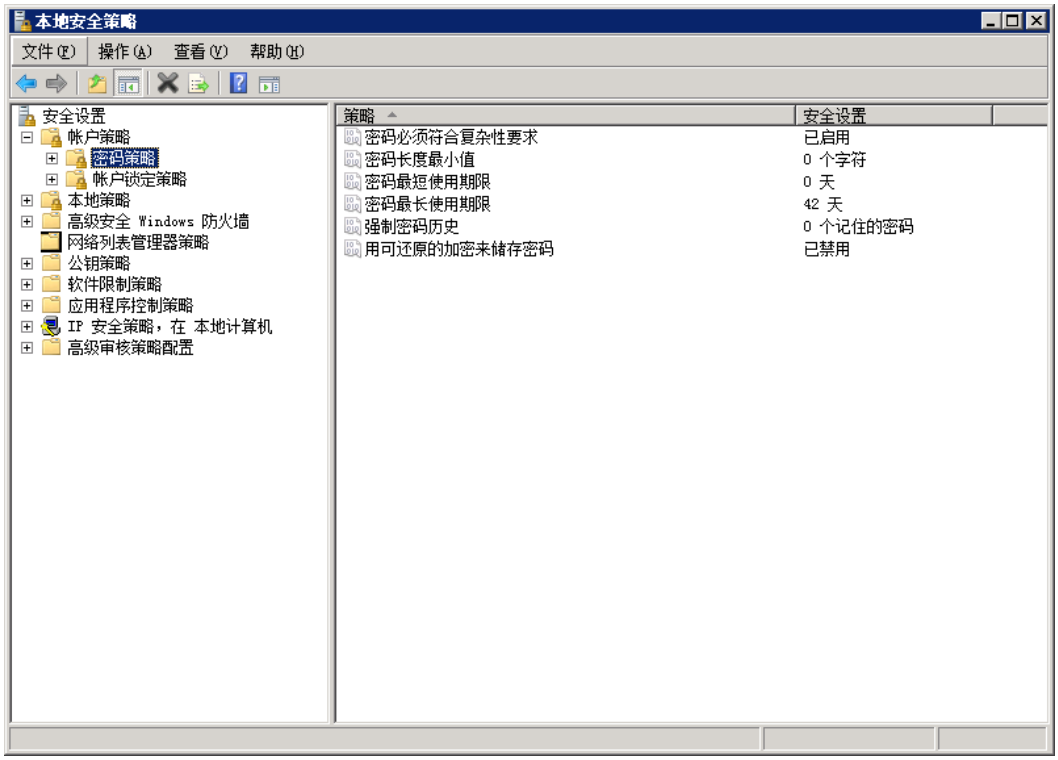
图 4-26 输入命令



步骤2 选择“帐户策略 > 密码策略”后执行以下操作，如图4-27所示。

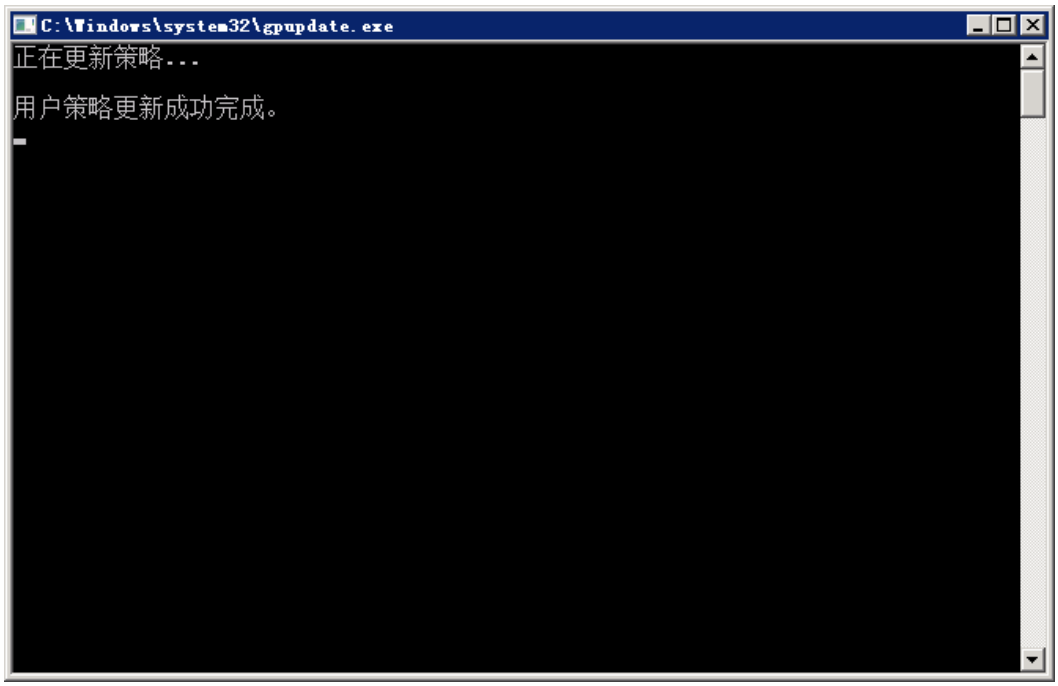
- 双击“密码必须符合复杂性要求”，勾选“已启用”选项，单击“确定”，启用“密码必须符合复杂性要求”策略。
- 双击“密码长度最小值”，填入长度（建议大于等于8），单击“确定”，设置“密码长度最小值”策略。

图 4-27 本地安全策略配置项



步骤3 运行**gpupdate**命令刷新策略，刷新成功后，如图4-28所示，以上设置被应用与系统中。

图 4-28 执行结果



----结束

4.6.3 如何处理配置风险?

企业主机安全服务对主机执行配置检测后，您可以根据检测结果中的相关信息，修复主机中含有风险的配置项或忽略可信任的配置项。

- 修改有风险的配置项

  查看检测规则对应的详情信息，您可以根据审计描述验证检测结果，根据修改建议处理主机中的异常信息。

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

- 忽略可信任的配置项

  a. 单击云服务器名称，查看服务器的详细信息。

  b. 选中单个“存在风险的检测规则”，单击操作列的“忽略”或者列表左上角的“忽略”进行单个忽略。也可以选中多个检测规则单击界面左上角的“忽略”批量进行忽略，如图4-29所示。

  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。

  图 4-29 批量忽略

- 修复验证

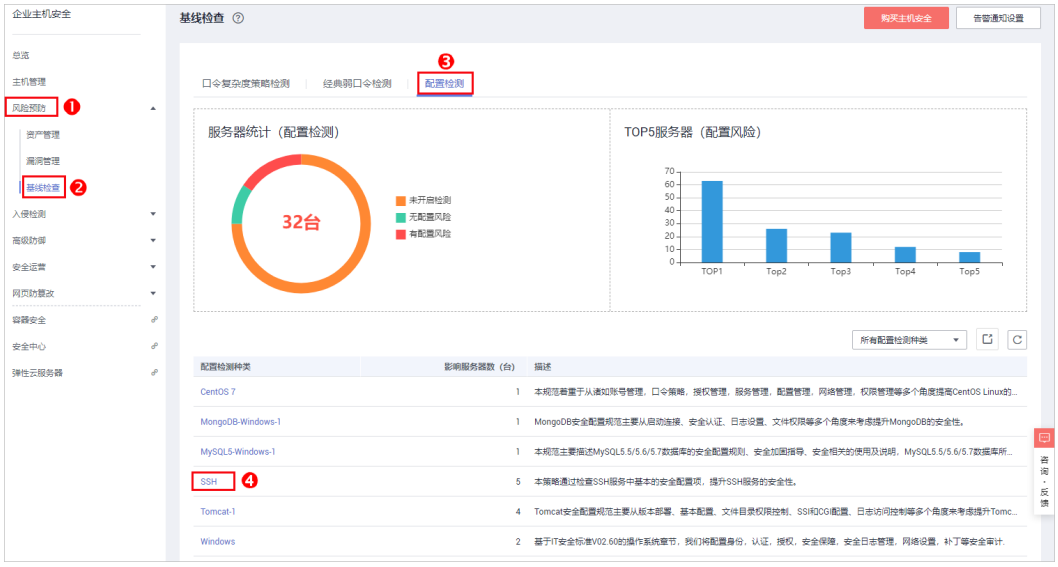
  完成配置项的修复后，建议您立即手动执行配置检测，查看配置项修复结果。

4.6.4 如何查看配置检测报告?

操作步骤

步骤1 在“配置检测”页面，单击配置检测种类名称，以下以“SSH”为例。

图 4-30 配置检测种类



步骤2 在检测规则详情页面，单击“检测详情”。

图 4-31 检测详情

步骤3 您可以根据配置检测报告中的描述信息和修改建议，修复主机中含有风险的配置项或忽略可信任的配置项。

图 4-32 配置检测报告

----结束

5 漏洞管理

5.1 如何处理漏洞?

处理方法和步骤

步骤1 查看漏洞检测结果。

步骤2 按照漏洞检测结果给出的漏洞修复紧急度和解决方案逐个进行漏洞修复。

- windows系统漏洞修复完成后需要重启。
- Linux系统Kernel类的漏洞修复完成后需要重启。

步骤3 企业主机安全服务每日凌晨将全面检测Linux主机和Windows主机，以及主机Web-CMS的漏洞，漏洞修复完成后建议立即执行一次检测，核实修复结果，请参见手动执行软件漏洞检测。

----结束

相关问题

如何处理配置风险?

5.2 漏洞修复后，为什么仍然提示漏洞存在?

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。

漏洞存在原因

漏洞修复后仍然在控制台存在，进入漏洞管理页面查看漏洞状态，漏洞的“状态”可能存在“修复失败”或“修复成功”两种状态。

- 目标漏洞“状态”为“修复成功”

  修复成功的漏洞仍然会在控制台显示30个自然日，到期后才会自动清除。
- 目标漏洞“状态”为“修复失败”

说明

修复漏洞流程建议您参考漏洞修复与验证您服务器上的漏洞进行修复。

在企业主机安全控制台上使用漏洞管理功能修复系统软件漏洞时，如果提示漏洞修复失败，根据Windows和Linux不同系统出现的可能原因排查如下：

Windows 系统服务器

- **补丁安装包下载不成功**

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

- **补丁安装包不匹配**

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

- **另一个补丁正在安装**

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

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

须知

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

Linux 系统服务器

- **无yum源配置**

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

- **yum源没有相应软件的最新升级包**

  切换到有相应软件包的yum源，配置完成后，重新执行漏洞修复操作。

- **内网环境连接不上公网**

  在线修复漏洞时，需要连接Internet，通过外部yum源提供漏洞修复服务。如果服务器无法访问Internet，或者外部yum源提供的服务不稳定时，可以使用华为云提供的镜像源进行漏洞修复。

- **内核老版本存留**

  由于内核升级比较特殊，一般都会有老版本存留的问题。您可通过执行修复命令查看当前使用的内核版本是否已符合漏洞要求的版本。确认无误后，对于该漏洞

告警，您可以在企业主机安全管理控制台的“漏洞管理 > Linux软件漏洞管理”页面进行**忽略**。同时，不建议您删除老版本内核。

表 5-1 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*

说明

软件名称是指需要修复的目标软件名称。可在资产指纹页面选择“软件”查看所有软件信息。

后续操作

漏洞修复后，建议立即执行一次检测，核实修复效果，详情请参见手动执行软件漏洞检测。

说明

- 若未进行手动验证，主机防护每日凌晨进行全量检测，修复后需要等到次日凌晨检测后才能查看检测结果。
- Windows系统漏洞和Linux系统Kernel类的漏洞修复完成后需要手动重启主机，否则HSS仍可能为您推送漏洞消息。

5.3 漏洞管理显示的主机不存在?

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

5.4 漏洞修复完毕后是否需要重启主机?

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

5.5 HSS 怎么区分高危漏洞和低危漏洞?

您可通过漏洞管理页的“修复紧急度”来区分高危漏洞和低危漏洞。

“修复紧急度”分为如下三种类型：

- 需尽快修复：属高危漏洞，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：属中危漏洞，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：属低危漏洞，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。

说明

您可在漏洞管理页面**查看漏洞详情**，参照**漏洞修复与验证**对漏洞进行修复和验证。

5.6 HSS 如何查询漏洞、基线已修复记录?

已修复的漏洞记录目前控制台还不支持查询。

若需要查看当前漏洞的详细信息或导出漏洞报告，详情请参见**查看漏洞详情**。

若需要查看当前基线检查的详细信息或导出配置检测报告，详情请参见**查看基线检查详情**。

5.7 修复漏洞时服务器内容被清空是否可以恢复?

可以。

但是通过恢复操作只能将服务器数据恢复至最后一次备份时的状态，未备份的无法恢复。

5.8 漏洞修复失败如何处理?

问题描述

在按照**漏洞修复与验证**修复漏洞后，漏洞修复“状态”为“修复失败”。

可能原因

1. 漏洞修复超时。
2. 漏洞修复状态冲突。
3. yum源不存在漏洞补丁升级包。

解决方案

上述问题已在主机安全（新版）中得到解决，请升级当前版本。升级操作，请参见**升级Agent**。

说明

Agent升级成功后，您将切换使用新版HSS：**登录主机安全（新版）控制台**

6 网页防篡改

6.1 为什么要添加防护目录?

网页防篡改是对目录中的文件进行防篡改防护，所以，开启网页防篡改后，需要添加防护目录才能起到防护作用。

添加防护目录请参见**开启网页防篡改版**的添加防护目录。

6.2 如何修改防护目录?

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“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。

图 6-1 企业主机安全

步骤3 在左侧导航栏中，选择“网页防篡改”，进入“网页防篡改”界面。

步骤4 选择所需开启“网页防篡改”防护的主机，在主机列表右侧的“操作”列中，单击“防护设置”，进入防护设置页面。

步骤5 选择所需修改的防护目录，在防护目录列表右侧操作列中，单击“编辑”修改。

说明

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

图 6-2 防护设置

步骤6 在“编辑防护目录”弹框中进行修改，单击“确定”完成修改。

图 6-3 编辑防护目录

----结束

6.3 无法开启网页防篡改怎么办?

可能的原因及解决方法如下:

配额不足

- **现象**:
  所选区域内网页防篡改配额不足，如图6-4所示。

  图 6-4 配额不足

- **解决方法**
  请在所选区域内购买网页防篡改配额。

Agent 状态异常

- **现象**
  网页防篡改页面防护列表中“Agent状态”为“离线”或者“未安装”，如图6-5所示。

  图 6-5 Agent 状态

- **解决方法**
  请参见Agent状态异常进行处理，确保主机列表中“Agent状态”为“在线”。

开启了基础版/企业版/旗舰版防护

- **现象**

企业主机安全页面主机列表中“防护状态”为“开启”。

- **解决方法**

  请先关闭主机防护，再开启网页防篡改。

  说明

  主机防护包含基础版、企业版、旗舰版以及网页防篡改版防护。如果已开启基础版、企业版或者旗舰版防护，需要先关闭主机防护，才能开启网页防篡改。

位置选择错误

请在“网页防篡改 > 防护列表”页面开启防护。

图 6-6 进入“网页防篡改”界面

说明

购买企业主机安全服务“网页防篡改版”后，您可以使用“旗舰版”中的所有功能，此时您只能通过“网页防篡改”页面开启防护，当开启网页防篡改防护时会同步开启旗舰版防护。

6.4 开启网页防篡改后，如何修改文件?

开启防护后，防护目录中的内容是只读，如果您需要修改文件或更新网站：

指定特权进程

特权进程有权修改文件，具体操作请参见设置特权进程。

- 特权进程可以访问被防护的目录，请确保特权进程安全可靠。
- 仅Windows系统支持特权进程。

临时关闭网页防篡改

请先临时关闭网页防篡改，完成修改或更新后再开启。

关闭网页防篡改期间，文件存在被篡改的风险，更新网页后，请及时开启网页防篡改。

设置定时开关

定时开关可以定时关闭**静态网页防篡改**，您可以使用此功能定时更新需要发布的网页。

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

6.5 开启动态网页防篡改后，状态是“已开启未生效”，怎么办?

动态网页防篡改提供tomcat应用运行时的自我保护。

开启动态网页防篡改需要满足以下条件：

- 仅针对Tomcat应用。
- 主机是Linux操作系统。
- 开启动态网页防篡改后，请等待大约20分钟后检查“tomcat/bin”目录下是否已生成“setenv.sh”文件，若已生成该文件，则重启Tomcat即可成功开启动态网页放篡改。

如果您开启网页防篡改后，状态是“已开启未生效”：

- 请检查您的“tomcat/bin”目录下的“setenv.sh”文件是否生成。
- 若“setenv.sh”文件已生成，请检查Tomcat是否重启。

6.6 HSS 与 WAF 的网页防篡改有什么区别?

HSS网页防篡改版是专业的锁定文件不被修改，实时监控网站目录，并可以通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，是政府、院校及企业等组织必备的安全服务。

WAF网页防篡改为用户提供应用层的防护，对网站的静态网页进行缓存，当用户访问网站时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网页防篡改的区别

HSS与WAF网页防篡改的区别，如表6-1所示。

表 6-1 HSS 和 WAF 网页防篡改的区别

类别	HSS	WAF
静态网页	锁定驱动级文件目录、Web文件目录下的文件，禁止攻击者修改。	缓存服务端静态网页
动态网页	• 动态数据防篡改 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。 • 特权进程管理 配置特权进程白名单后，网页防篡改功能将主动放行可信任的进程，确保正常业务进程的运行。	不支持

类别	HSS	WAF
备份恢复	● 主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。 ● 远端备份恢复 若本地主机上的文件目录和备份目录失效，可通过远端备份服务恢复被篡改的网页。	不支持
防护对象	网站防护要求高，手动恢复篡改能力差	网站防护要求低，仅需要对应用层进行防护

如何选择网页防篡改

防护对象	选择网页防篡改
普通网站	WAF网页防篡改+HSS企业版
网站防护+高要求网页防篡改	WAF网页防篡改+HSS网页防篡改

7 企业项目

7.1 HSS 支持企业项目后，如何同步配置数据?

HSS目前已支持企业项目。

如果您的帐号在HSS未支持企业项目时已经使用企业项目，ECS分布在不同的企业项目中，HSS默认将ECS全量集中在“default”中。

HSS支持企业项目后，HSS会根据您设置的企业项目，自动将ECS迁移到对应的企业项目下，并展示在HSS界面中；迁移后，“default”项目中的HSS相关配置在非“default”项目中不生效，需要您重新配置，或者联系技术支持将“default”项目下的配置数据同步迁移到非“default”项目下。

须知

- 必配：告警通知，支持企业项目后，请在非“default”项目下务必配置“告警通知”，否则，您将不能收到非“default”项目下的告警信息。
- 可选配置：安全配置、服务器组、白名单管理、文件完整性管理、订阅安全报告、远端备份服务器、迁移配额等，您可以根据自己的实际情况，选择配置。

以下操作步骤中，以默认项目为“default”，非“default”项目为“企业项目一”为例进行说明。

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。

图 7-1 企业主机安全

步骤3 进入“主机管理”页面，在“企业项目”下拉列表中，选择“企业项目一”，刷新云服务器列表，如图7-2所示。

图 7-2 刷新主机列表

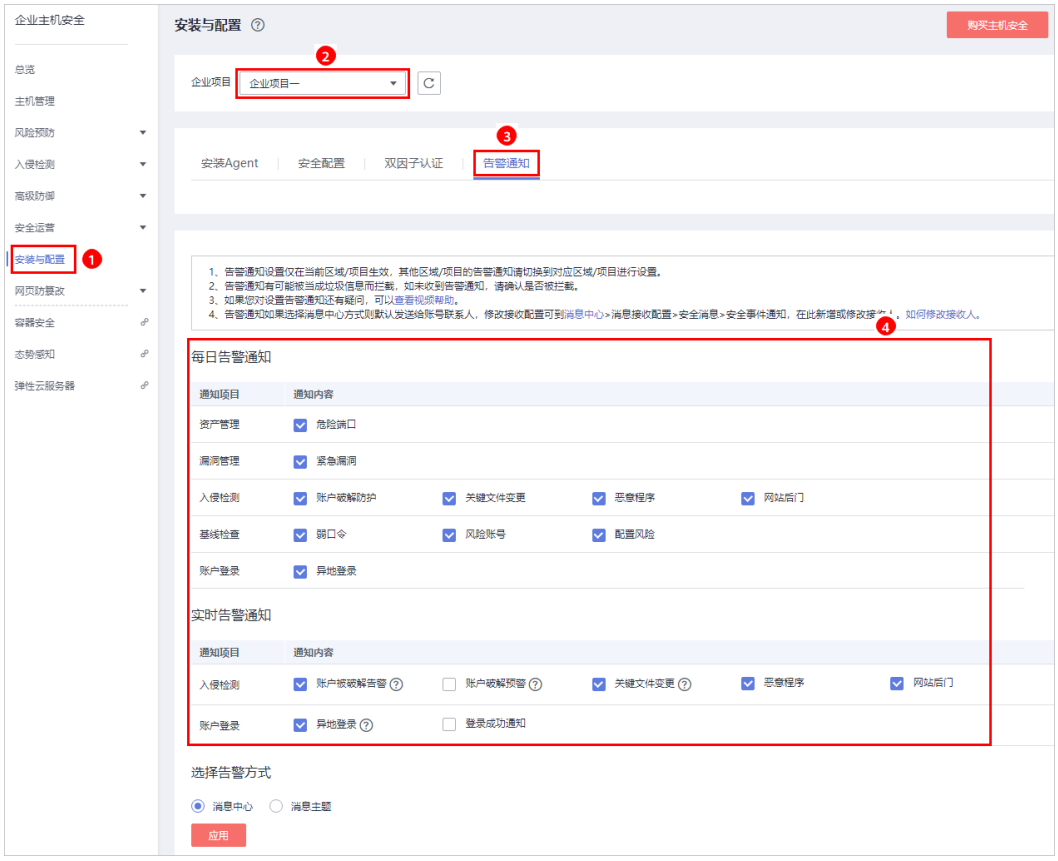
----结束

（必配）重新配置告警通知

- **配置基础版/企业版/旗舰版告警通知**

步骤1 选择“告警通知”页签，进入“告警通知”页面，如图7-3所示。

图 7-3 基础版/专业版/旗舰版



步骤2 根据需要勾选“每日告警通知”和“实时告警通知”中的通知项。

步骤3 选择“消息中心”或者“消息主题”告警通知方式，接收告警通知。

步骤4 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

- **配置网页防篡改告警通知**

步骤1 进入“告警通知”页面，选择告警通知时间，如图7-4所示。

图 7-4 告警通知设置

步骤2 根据需要勾选“每日告警通知”和“实时告警通知”中的通知项。

步骤3 选择“消息中心”或者“消息主题”告警通知方式，接收告警通知。

步骤4 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

（可选）迁移安全配置数据

您需要对企业项目重新进行安全配置。包括配置常用登录地、常用登录IP，开启恶意程序自动隔离查杀功能。

支持企业项目后，SSH登录IP白名单已配置的数据，会自动从“default”项目同步迁移到“企业项目一”。

选择“安装与配置”页面，在“安全配置”下，配置常用登录地、常用登录IP和开启恶意程序自动隔离查杀，如图7-5所示。

图 7-5 配置安全配置

（可选）重新创建服务器组

若在支持企业项目前，已为主机创建服务器组，你需要在企业项目下创建新的服务器组。

步骤1 选择“主机管理”，在“服务器组”界面，单击“创建服务器组”，如图7-6所示。

图 7-6 进入服务器组页面

步骤2 在弹出的创建服务器组窗口中，设置服务器组名称，并将主机分配给该服务器组，如图7-7所示。

图 7-7 分配主机

步骤3 单击“确定”，完成服务器组创建。

----结束

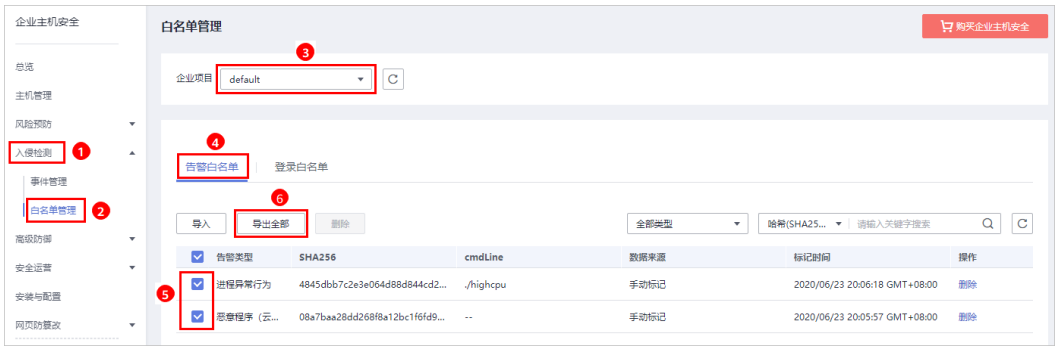
（可选）迁移白名单数据

支持多项目后，配置的告警白名单和登录白名单不会自动同步到对应的企业项目。

- 告警白名单：您需要手动将“default”项目下的告警白名单导出后，再导入到对应“企业项目一”下。
- 登录白名单：您需要到对应“企业项目一”下，逐一进行手动配置。

步骤1 选择“白名单管理”页面，选择“default”项目，导出告警白名单，如图7-8所示。

图 7-8 导出告警白名单



步骤2 在“企业项目”下拉列表中，选择企业项目，例如“企业项目一”，导入告警白名单，如图7-9所示。

图 7-9 导入告警白名单

步骤3 在登录白名单页面，手动添加登录白名单，如图7-10所示。

图 7-10 添加登录白名单

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7-11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 7-11 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

（可选）开启文件完整性管理

支持企业项目后，文件完整性管理不会自动开启，旗舰版用户，请进入文件完整性管理页面，重新开启文件完整性管理。

进入“文件完整性管理”页面，单击，开启文件完整性管理，如图7-12所示。

图 7-12 开启文件完整性管理

（可选）订阅安全报告

选择“安全报告”页面，勾选“周报”和“月报”，如图7-13所示。

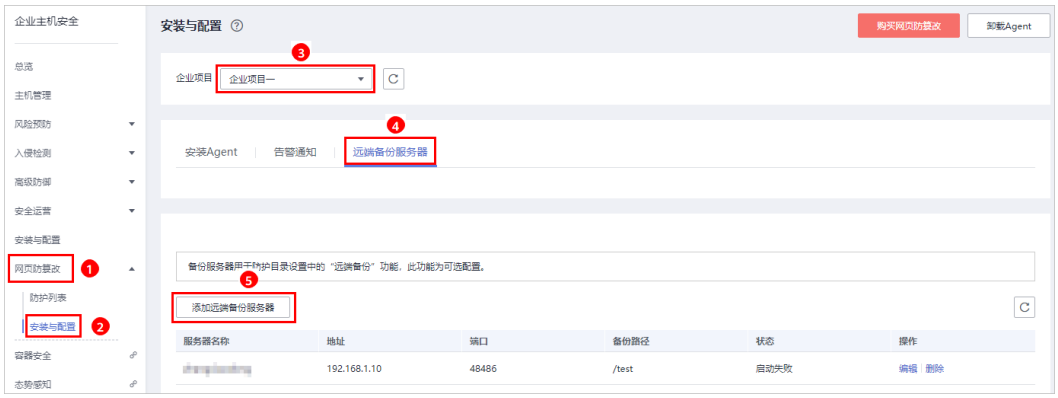
图 7-13 订阅安全报告

（可选）网页防篡改-配置远端备份服务器

“default”项目下配置的远端备份服务器不会自动添加到“企业项目一”，需要您手动在“企业项目一”下添加远端备份服务器，并启动远端备份。

步骤1 选择“网页防篡改 > 安装与配置”，添加远端备份服务器，如图7-14所示。

图 7-14 添加远端备份服务器



步骤2 选择“防护列表”页面，单击“防护配置”，进入防护配置页面，如图7-15所示。

图 7-15 进入防护设置页面

步骤3 在防护设置页面，启动远端备份，如图7-16所示。

图 7-16 启动远端备份

步骤4 在弹出的启动远端备份窗口中，在远端备份服务器下拉列表中，选择远端备份服务器，单击“确定”，启动远端备份。

----结束

（可选）迁移配额

支持企业项目后，“企业项目一”下的主机使用的是“default”项目下的配额，如果在“企业项目一”下将主机关闭防护，那么“企业项目一”下的主机将不能再使用包周期的防护配额开启主机防护。如果需要使用包周期的防护配额开启防护，您可以将“default”项目下的配额迁移到“企业项目一”中，操作步骤如下所示。

步骤1 选择“主机管理”页面，在企业项目下拉列表中选择“企业项目一”，在云服务器列表中，查看非“default”项目下的ECS，如图7-17所示。

图 7-17 查看主机名称

步骤2 获取主机防护配额。

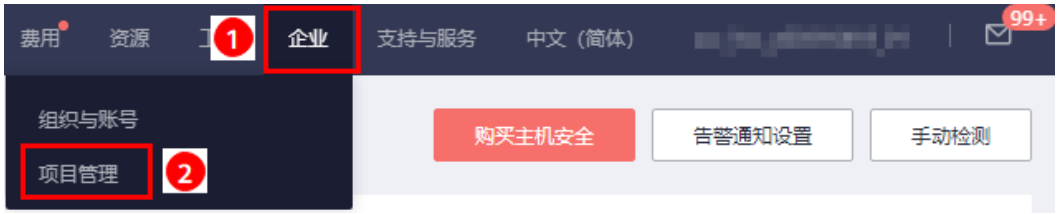
- 若迁移到“企业项目一”下的主机处于“开启防护”状态，选择“防护配额”页签，获取“配额ID”，如图7-18所示。

- 若迁移到“企业项目一”下的主机没有开启主机防护，则在“default”项目下，获取处于“空闲”状态的“配额ID”。

图 7-18 获取配额 ID

步骤3 在控制台右上角单击“企业”，选择“项目管理”，如图7-19所示。

图 7-19 选择项目管理

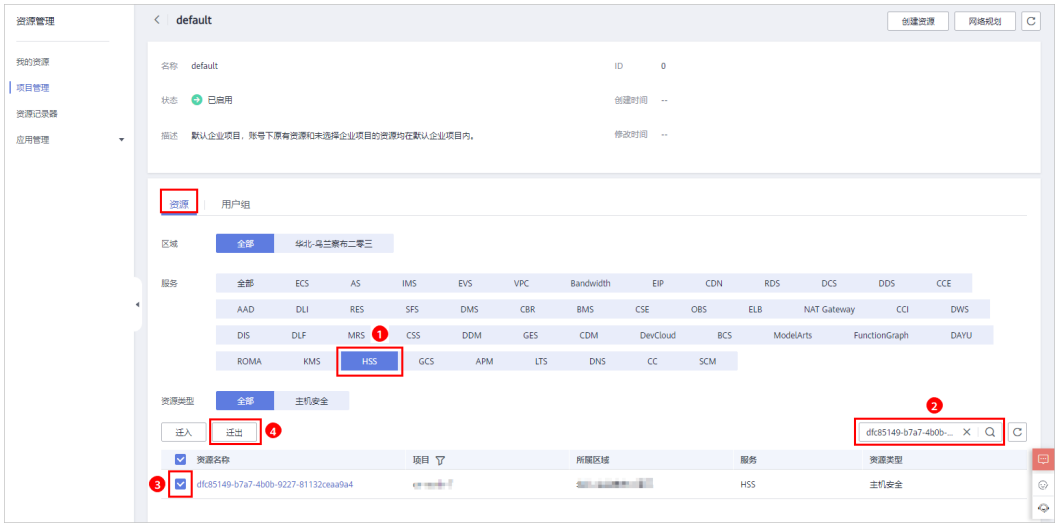


步骤4 在项目管理页面，单击“default”，进入“default”项目，如图7-20所示。

图 7-20 进入 default 项目

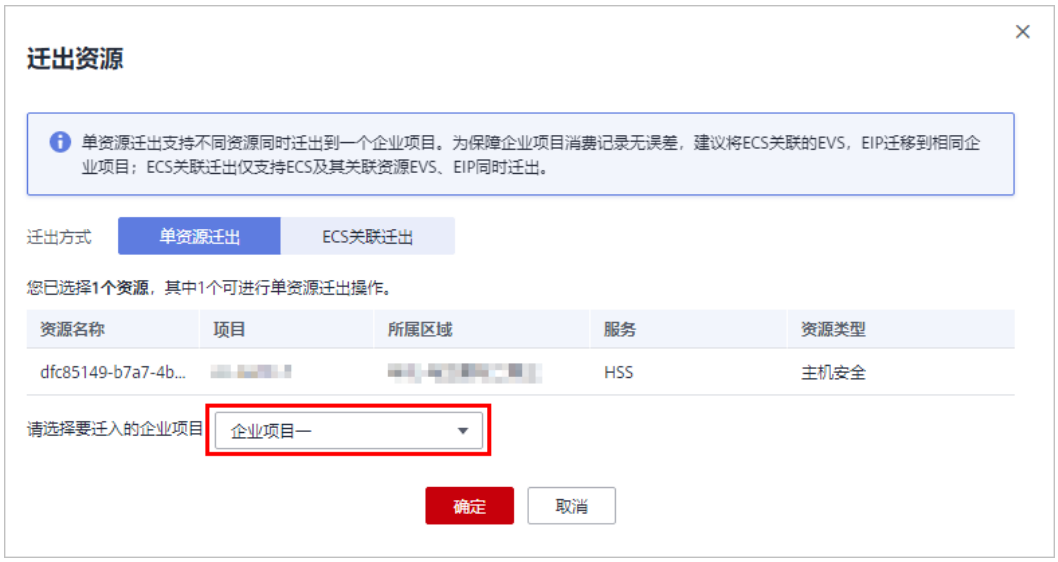
步骤5 在“资源”页签下，选择“HSS”，根据步骤2获取的配额ID，搜索主机配额，并迁出配额，如图7-21所示。

图 7-21 迁出配额



步骤6 在弹出的“迁出资源”窗口中，选择要迁入的项目，例如：企业项目一，如图7-22所示。

图 7-22 迁入企业项目



步骤7 单击“确定”，完成防护配额的迁入，您可以在对应企业项目下，正常使用迁入的防护配额。

您可以返回企业主机安全管理控制台，选择“主机管理”，在“企业项目”下拉列表中，选择“企业项目一”，在“防护配额”页签，查看迁入的防护配额。

----结束

7.2 防护配额与主机不在同一企业项目，是否可以相互绑定?

可以相互绑定，但为了方便您的管理，请在购买防护配额时，分企业项目购买。

您可以通过以下两种方式实现防护配额与主机的绑定。

- 所有项目

  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。

- 迁移配额

  您可以通过迁移配额的方式，将配额迁移到指定企业项目中，实现配额与主机的绑定。

所有项目

前提条件

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

操作步骤

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。

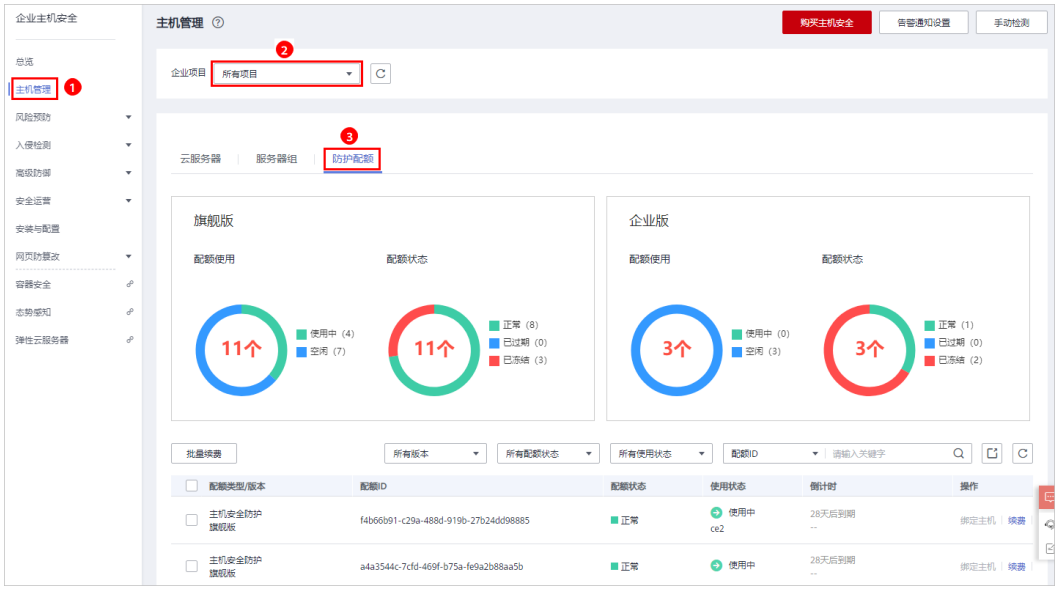
步骤1 登录管理控制台。

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。

图 7-23 企业主机安全

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7-24所示。

图 7-24 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 7-25 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。

图 7-26 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

迁移配额

例如：购买的所有防护配额均在“default”项目中，需要将“default”项目中的防护配额迁移到“企业项目一”中，然后在“企业项目一”为主机开启HSS防护。

步骤1 选择“主机管理”页面，在企业项目下拉列表中选择“企业项目一”，在云服务器列表中，查看非“default”项目下的ECS，如图7-27所示。

图 7-27 查看主机名称

步骤2 获取主机防护配额。

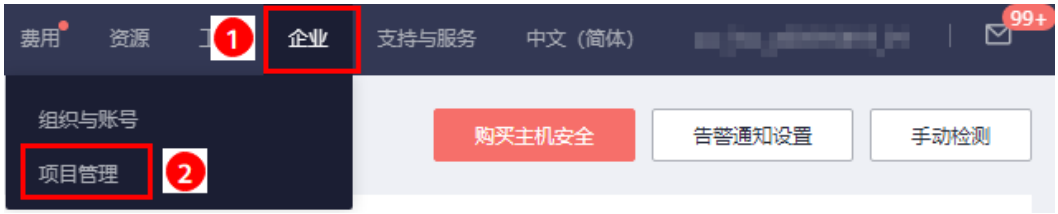
- 若迁移到“企业项目一”下的主机处于“开启防护”状态，选择“防护配额”页签，获取“配额ID”，如图7-28所示。

- 若迁移到“企业项目一”下的主机没有开启主机防护，则在“default”项目下，获取处于“空闲”状态的“配额ID”。

图 7-28 获取配额 ID

步骤3 在控制台右上角单击“企业”，选择“项目管理”，如图7-29所示。

图 7-29 选择项目管理



步骤4 在项目管理页面，单击“default”，进入“default”项目，如图7-30所示。

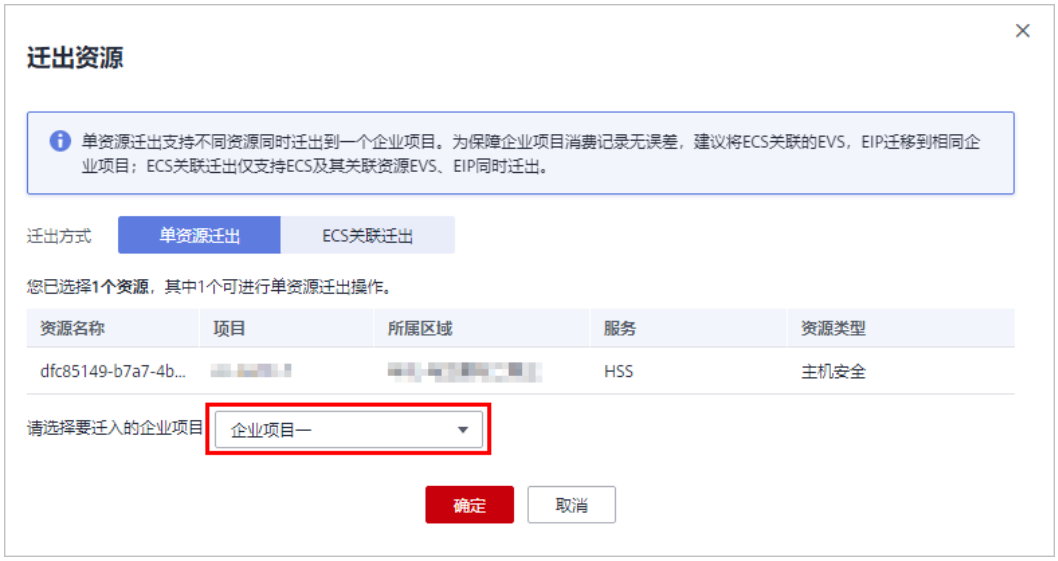
图 7-30 进入 default 项目

步骤5 在“资源”页签下，选择“HSS”，根据步骤2获取的配额ID，搜索主机配额，并迁出配额，如图7-31所示。

图 7-31 迁出配额

步骤6 在弹出的“迁出资源”窗口中，选择要迁入的项目，例如：企业项目一，如图7-32所示。

图 7-32 迁入企业项目



步骤7 单击“确定”，完成防护配额的迁入，您可以在对应企业项目下，正常使用迁入的防护配额。

您可以返回企业主机安全管理控制台，选择“主机管理”，在“企业项目”下拉列表中，选择“企业项目一”，在“防护配额”页签，查看迁入的防护配额。

----结束

8 区域和可用区

8.1 什么是区域和可用区?

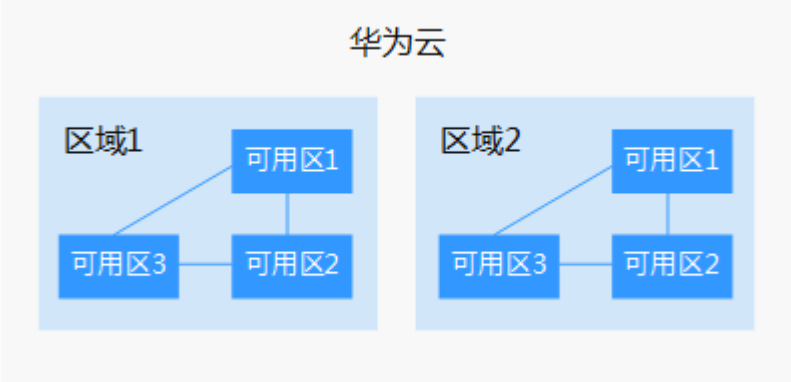
什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图8-1阐明了区域和可用区之间的关系。

图 8-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见华为云服务价格详情。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅地区和终端节点。

9 费用

9.1 价格体系

目前支持通过“包年/包月”和“按需计费”的方式购买。

详细的服务资费费率标准请参见产品价格详情。

9.2 HSS 到期后不续费，对主机和业务有影响吗?

不会产生直接影响。

停止续费说明

企业主机安全是提升主机整体安全性的服务，到期后不续费会自动停止防护。

停止续费风险

不续费会降低服务器的防护能力，遭受破解、入侵的风险会增加，会有很大的安全隐患，例如我们的数据、程序都是运行在云服务器上，一旦系统被入侵成功，数据将面临被窃取或被篡改的风险，企业的业务将面临中断，造成重大损失。

企业主机安全服务提供事前预防、事中防护、实时/每日告警的全方位保护措施，提高主机的安全性，保护企业的业务安全。更多详细信息请参见产品介绍。

相关操作

- 购买企业主机安全配额
- 续费

9.3 退订重购 HSS 后，是否需要重新安装 Agent 与配置主机防护信息?

退订HSS时，退订的是防护配额。

HSS不会自动卸载主机上已安装的Agent，也不会修改或者删除已配置的主机防护信息。

重购的 HSS 配额与原配额在同一区域

不需要重新安装Agent，也不需要重新配置主机防护信息。

重购的 HSS 配额与原配额不在同一区域

HSS不支持跨区域使用，请退订配额后重新购买主机所在区域的配额。重新购买后不需要重新配置主机防护信息。

9.4 如何续费?

该任务指导您如何在企业主机安全即将到期时进行续费。续费后，您可以继续使用。

- 自动续费

  如果在购买配额时，您已勾选并同意“自动续费”，则在服务到期前，系统会自动按照购买周期生成续费订单并进行续费。

- 手动续费

  服务到期前，系统会以短信或邮件的形式提醒您服务即将到期，并提醒您续费。

  服务到期后，若您没有及时续费，资源会进入保留期。

  保留期时长根据用户等级来定，具体请参见保留期时长限制。

  进入保留期，HSS将不再防护您的主机，但与HSS相关的配置信息会被系统保留。保留期满，HSS相关的配置信息也将被释放。

  为了主机的整体安全性，请您及时续费。

前提条件

已获取BSS Administrator权限和HSS Administrator权限与密码。

说明

拥有BSS Administrator权限的帐号，可以对帐号中心、费用中心、资源中心的所有菜单项执行任意操作。

操作步骤

步骤1 查看防护配额，找到需要续费的配额。

步骤2 在需要续费的配额所在行的操作列，单击“续费”。

步骤3 在对应页面根据页面提示完成续费。

详细续费操作请参见续费管理。

----结束

9.5 如何申请退订配额及退款?

- 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。
- 为避免浪费配额资源，您可以退订“空闲”状态的配额。

说明

退订配额时，不支持配额的批量退定。

前提条件

如果您退订的配额资源正在使用中，请先关闭防护，然后再执行退订操作。

操作步骤

步骤1 查看防护配额，找到需要退订的配额。

步骤2 在需要退订的配额所在行的操作列，单击“退订”。

步骤3 在对应页面根据页面提示完成退订。

详细退订操作请参见退订管理。

----结束

批量退款

步骤1 登录管理控制台。

步骤2 单击界面右上方的“费用与成本”，进入“费用中心”界面，如图9-1所示。

图 9-1 费用中心入口

步骤3 在左侧导航树上，选择“订单管理 > 退订与退换货”。

步骤4 在对应页面根据页面提示完成退订。

详细退订操作请参见退订管理。

----结束

10 其他

10.1 在 Windows 中文系统中输入数字卡顿或需要数字连输怎么办?

登录界面输入帐号、密码时选用英文输入法。

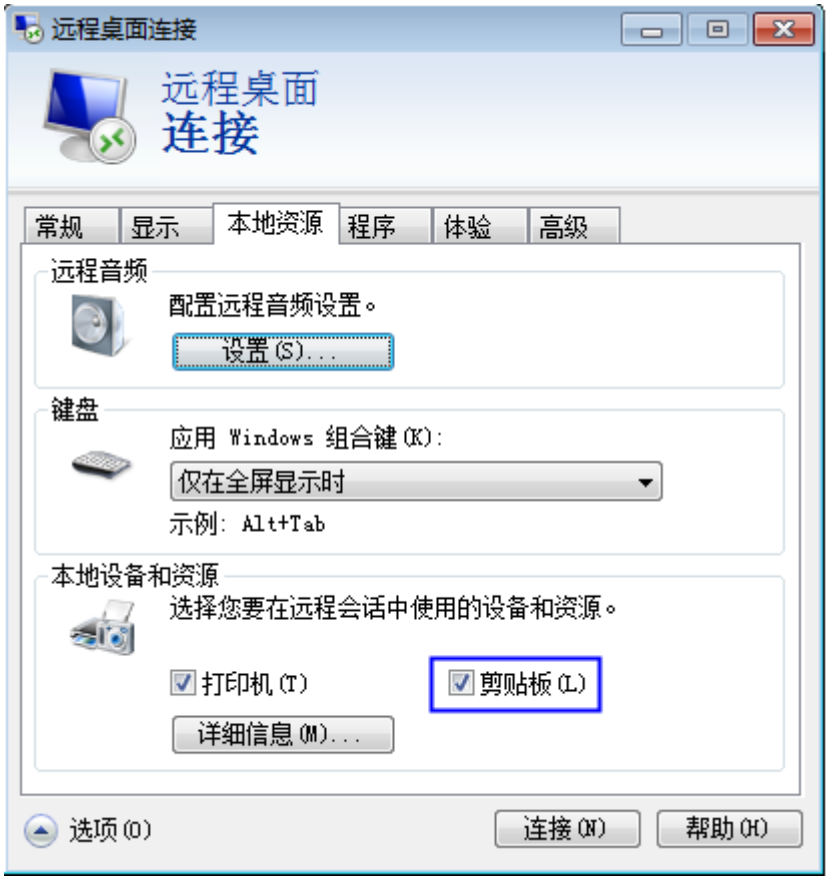
10.2 如何使用 Windows 远程桌面连接工具连接主机?

操作步骤

步骤1 在本地主机上选择“开始 > 运行”，输入命令**mstsc**，打开Windows“远程桌面连接”工具。

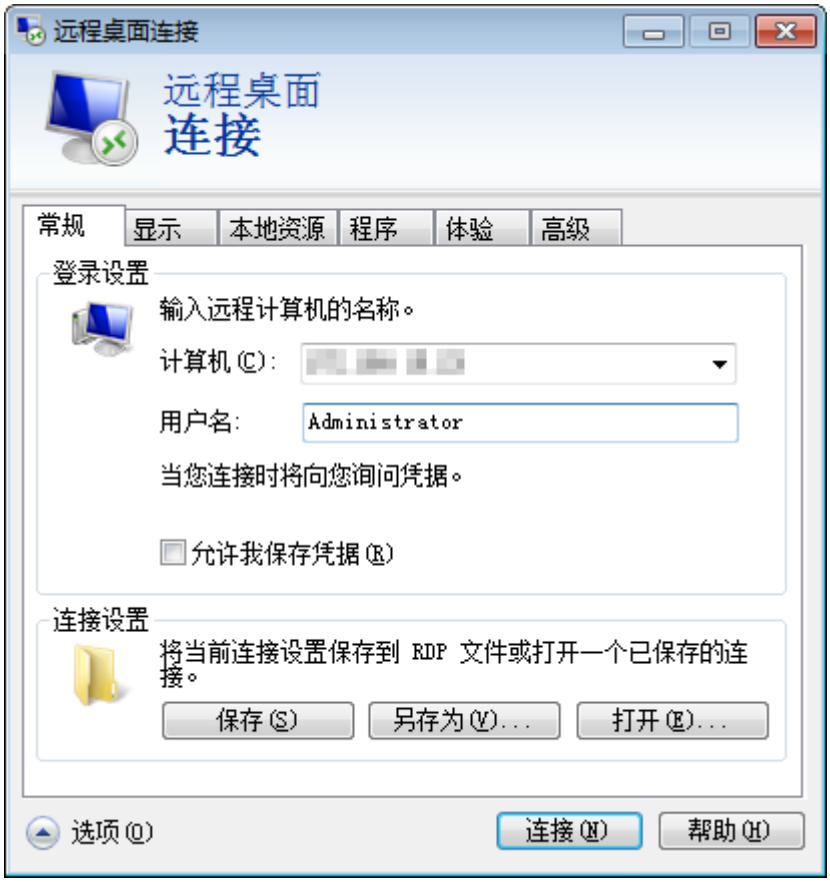
步骤2 单击“选项”，选择“本地资源”页签，在“本地设备和资源”区域中，勾选“剪贴板”，如图10-1所示。

图 10-1 远程桌面连接



步骤3 选择“常规”页签，在“计算机”中输入云服务器的弹性IP，在“用户名”中输入“Administrator”，单击“连接”，如图10-2所示。

图 10-2 设置常规信息



步骤4 在弹出的对话框中，输入主机的用户密码，单击“确定”，连接至主机。

----结束

10.3 如何查看 HSS 的日志文件?

日志路径

您需要根据主机的操作系统，查看日志文件。

操作系统	日志所在路径	日志文件
Linux	/usr/local/hostguard/log/	• daemon.log：记录守护进程运行时相关日志。 • hostguard.log：记录监控进程运行时相关日志。 • hostguard_procmon.log：记录进程创建的信息。 • urlconfig.log：只在安装时，记录识别region信息。 • upgrade.log：记录升级时相关日志。 • hostguard_rsync.log：记录网页防篡改备份服务器的运行日志。
Windows	C:\Program Files (x86)\HostGuard\log\	

日志保留周期

日志文件	文件大小限制	路径下保留的文件	保留周期
daemon.log	10M	保留5个最新的“daemon.log”日志文件。	不超过文件大小限制，只要不卸载HSS Agent，会一直保留日志信息。
hostguard.log	10M	保留5个最新的“hostguard.log”日志文件。	
hostguard_procmon.log	20M	保留2个最新的“hostguard_procmon.log”日志文件。	
urlconfig.log	不限制	保留1个“urlconfig.log”日志文件。	
upgrade.log	不限制	保留1个“upgrade.log”日志文件。	
hostguard_rsync.log	不限制	保留1个“hostguard_rsync.log”日志文件。	

10.4 如何开启登录失败日志开关?

MySQL

在帐户破解防护功能中，Windows和Linux系统都支持MySQL软件的5.6和5.7版本，开启登录失败日志开关的具体的操作步骤如下：

步骤1 使用root权限登录主机。

步骤2 查询log_warnings值，命令如下：

show global variables like 'log_warnings'

步骤3 修改log_warnings值，命令如下。

set global log_warnings=2

步骤4 修改配置文件。

- Windows系统，修改配置文件my.ini，在[mysqld]中增加log_warnings=2。
- Linux系统中，修改配置文件my.conf，在[mysqld]中增加log_warnings=2。

----结束

Filezilla

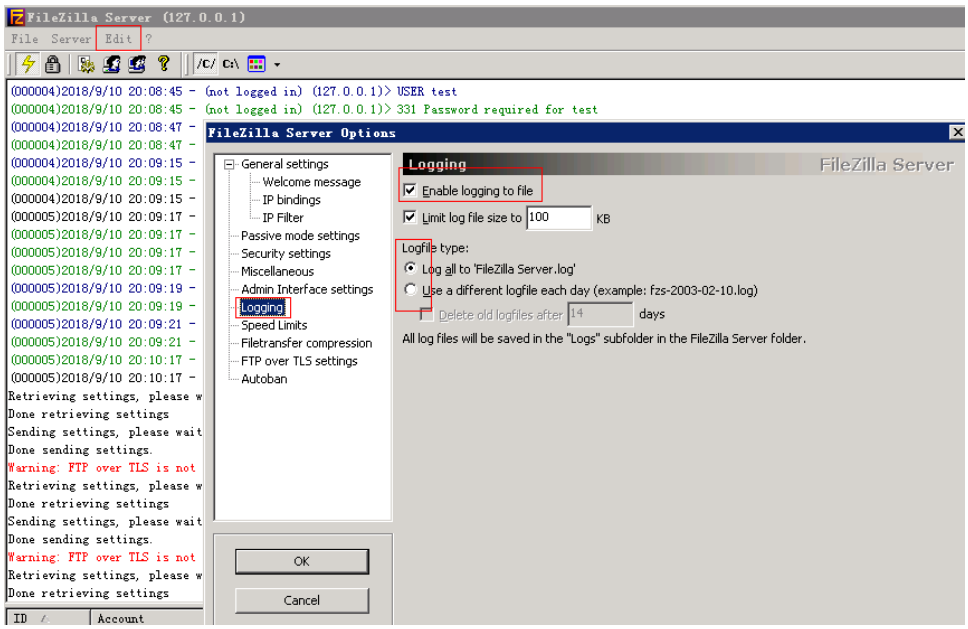
在帐户破解防护功能中，仅Windows系统支持filezilla软件的0.9.60版本。filezilla默认不开启日志，需要在设置中开启日志开关。

开户日志开关的操作步骤如下：

步骤1 打开filezilla软件。

步骤2 选择“Edit > Settings > Logging”，勾选“Enable logging to file”，如图10-3所示。

图 10-3 filezilla 配置



----结束

vsftp

本节指导用户开启vsftp的登录失败日志开关。

步骤1 修改配置文件（比如：/etc/vsftpd.conf），设置以下两项：

vsftpd_log_file=log/file/path

dual_log_enable=YES

步骤2 重启vsftp服务。设置成功后，登录时，会返回如图10-4所示的日志记录。

图 10-4 日志记录

```
Wed Aug 29 14:53:05 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Aug 29 14:53:11 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:14 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:18 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
Wed Aug 29 14:55:26 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 11:50:16 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Sep  5 11:50:23 2018 [pid 1] [ftp_test] OK LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 13:59:53 2018 [pid 2] CONNECT: Client "::ffff:10.130.153.31"
Wed Sep  5 13:59:59 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
Wed Sep  5 14:00:08 2018 [pid 1] [ftp_test] FAIL LOGIN: Client "::ffff:10.130.153.31"
```

----结束

10.5 如何立即执行手动检测?

企业主机安全服务将实时检测主机中的风险和异常操作，在每日凌晨将对主机执行全面扫描，此外，您也可以使用手动检测功能全面检测主机中关键的配置信息。

须知

手动检测完成后，需至少间隔三分钟，才能再次对同一个项目执行手动检测。

前提条件

服务器的“Agent状态”为“在线”、“防护状态”为“开启”、“版本”为“企业版”或者“旗舰版”。

检测项目

软件信息、Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、网站后门检测、口令风险和配置风险。

检测时长

- 检测单个检测项目（例如：口令风险）的检测时长为30分钟内。
- 一键手动检测，检测多个检测项目时，各个检测项目并行检测，检测时长为30分钟内。

一键手动检测

一键执行手动检测能同时检测主机中的**软件信息、漏洞、网站后门、关键配置信息、较弱的口令复杂度策略、使用弱口令的用户帐号**。检测完成后，可在企业主机安全服务控制台查看各项风险统计或指定查看单个服务器的安全详情。

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。

图 10-5 企业主机安全

步骤3 在“主机管理”页面的右上角，单击“手动检测”，执行手动检测，如图10-6所示。

图 10-6 一键执行手动检测

步骤4 在弹出的“手动检测”对话框中，选择所需检测的主机，单击“确定”，完成一键手动检测的操作。

图 10-7 手动检测

步骤5 在安全控制台“企业主机安全”菜单或主机列表“操作”列的“查看详情”中查看各项手动检测结果并对检测结果执行相应的操作。

----结束

单点执行手动检测

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。

图 10-8 企业主机安全

步骤3 在左侧导航栏中，选择“主机管理”，在云服务器列表的“操作”列中，单击“查看详情”，进入指定主机的详情页面。

图 10-9 查看详情

- **手动收集软件信息**

  选择“资产管理”页签，在页面下侧“软件信息”中，手动检测主机中的软件信息。

图 10-10 收集软件信息

- **手动执行漏洞检测**

  选择“漏洞管理”页签，在“Linux软件漏洞管理”和“Web-CMS漏洞管理”中，手动检测主机中的软件漏洞和Web-CMS漏洞。

说明

软件漏洞检测和软件信息管理任意一个手动检测都会触发收集服务器上的软件信息。

– 选择“漏洞管理”页签，选择系统软件漏洞，单击“手动检测”，系统将立即执行一次系统软件漏洞检测。

图 10-11 系统软件漏洞检测

– 选择“漏洞管理”页签，选择Web-CMS漏洞，单击“手动检测”，系统将立即执行一次Web-CMS漏洞检测。

图 10-12 Web-CMS 漏洞检测

- **手动执行口令风险检测**

  选择“基线检查”页签，在“口令风险”中，手动检测主机中较弱的口令复杂度策略、弱口令以及风险配置项。

图 10-13 弱口令风险检测

- **手动执行配置检测**

  选择“基线检查”页签，在“配置检测”中，手动检测主机中不安全的配置项。

图 10-14 配置检测

步骤4 当“手动检测状态”为“检测完成”时，单击 ，查看最新检测结果。

----结束

10.6 手动检测为什么会失败?

手动检测完成后，需至少间隔三分钟，才能再次对同一个项目执行手动检测。

10.7 HSS 有没有服务等级协议?

企业主机安全没有单独的服务等级协议，服务等级协议请参见：**https://www.huaweicloud.com/declaration/sla.html**。

10.8 怎么去除由于修复软件漏洞造成的关键文件变更告警?

告警通知检测到关键文件变更，如果您确认是正常操作可以不用关注，7天后自动消除。

10.9 HSS 是否能以软件形式线下输出?

不支持线下软件的形式。

10.10 HSS 中安装 Agent 必须要绑定公网 IP 吗?

安装Agent时，需要连接公网才能下载安装包。

若是华为云的主机，安装完成后可以解绑公网IP。

10.11 HSS 是否能通过 API 方式使用?

可以，HSS支持“华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”区域通过API方式“查询弹性云服务器状态列表”“查询入侵事件列表”。其他区域和更多的开放接口，敬请期待。

10.12 HSS 支持告警日志转存 OBS 吗?

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

10.13 如何切换主机之间已绑定的防护配额?

需要先解绑配额，重新绑定即可。详细步骤如下：

1. 参照**解绑配额**对不同版本的目标主机和配额进行解绑。
2. 参照**绑定主机**将目标主机和配额进行绑定。
3. 重新绑定后可**查看配额**的重新绑定情况。

说明

为了能更全面、更彻底的对主机进行防护，建议**升级配额版本**。

A 修订记录

发布日期	修改说明
2022-08-30	第四十九次正式发布。 新增常见问题：**Agent安装成功后显示未安装怎么处理？** 。 修改内容：**如何批量安装Agent？** ，补充Agent支持的操作系统描述。
2022-08-10	第四十八次正式发布。 新增常见问题：**漏洞修复失败如何处理?**
2022-07-30	第四十七次正式发布。 补充说明升级Agent全过程均为免费。 补充说明退订配额不支持批量退定。
2022-07-15	第四十六次正式发布。 下线支持centos 6系统版本的说明。
2022-06-30	第四十五次正式发布。 修改基础版免费使用的说明。
2022-05-31	第四十四次正式发布。 新增常见问题如下： **Agent安装后控制台不显示怎么处理?** **如何防御勒索病毒攻击?**
2022-05-26	第四十三次正式发布。 新增**Agent升级失败如何处理?**
2022-04-25	第四十二次正式发布。 优化、新增内容如下： ● 基础版使用及能力的说明。 ● 收到告警信息不代表已被破解入侵的说明。

发布日期	修改说明
2022-04-20	第四十一次正式发布 新增常见问题如下： **HSS拦截的IP是否需要处理？** 修改常见问题如下： **每台云服务器都需要配置部署主机安全服务吗？**
2022-04-11	第四十次正式发布。 新增常见问题如下： **修复漏洞时服务器内容被清空是否可以恢复？**
2022-03-18	第三十九次正式发布。 完善优化章节如下： **购买云服务器时，为什么无法选择免费的企业主机安全防护？** **如何扩充HSS防护配额？**
2022-01-29	第三十八次正式发布。 新增如下常见问题： **开启HSS基础版防护及说明** **HSS的数据传输实现原理是什么？**
2022-01-13	第三十七次正式发布。 完善优化章节如下： **如何预防帐户暴力破解攻击？** **收到来自华为云IP的暴力破解告警如何处理？**
2021-10-22	第三十六次正式发布。 新增如下常见问题： **收到来自华为云IP的暴力破解告警如何处理？** **HSS如何查询漏洞、基线已修复记录？**
2021-10-18	第三十五次正式发布。 新增如下常见问题： ● **如何切换主机之间已绑定的防护配额？** ● **HSS的恶意程序检测周期、隔离查杀是多久一次？** ● **HSS的病毒库、漏洞库多久更新一次？** ● **每台云服务器都需要配置部署主机安全服务吗？** ● **频繁收到HSS暴力破解告警如何处理？** ● **HSS怎么区分高危漏洞和低危漏洞？** 优化如下常见问题： ● **Agent安装失败应如何处理？**

发布日期	修改说明
2021-08-03	第三十四次正式发布。 新增如下常见问题： ● **主机重装系统后，HSS防护功能是否需要手动开启？** 修改如下常见问题： ● **Agent状态异常应如何处理？** ● **如何扩充HSS防护配额？**
2021-07-14	第三十三次正式发布。 新增如下常见问题： ● **如何修改告警通知的通知项？** ● **防护的主机切换操作系统，HSS配额会发生变化吗？** ● **如何筛选未绑定配额的主机？** ● **HSS可以添加黑名单IP吗？** ● **HSS与SA的基线检查有什么区别？** ● **如何扩充HSS防护配额？** 修改如下常见问题： ● **Agent安装失败应如何处理？** ● **漏洞修复后，为什么仍然提示漏洞存在？**
2021-07-08	第三十二次正式发布。 **Agent状态异常应如何处理？**，增加“卸载Agent”和“安装Agent”链接。
2021-06-08	第三十一次正式发布。 新增如下常见问题： ● **安装HSS Agent有什么影响？** ● **如何手动解除误拦截IP？** ● “内核漏洞升级修复后，为什么仍然提示漏洞存在？” ● **漏洞修复后，为什么仍然提示漏洞存在？** ● **HSS支持告警日志转存OBS吗？** 修改如下常见问题： ● **HSS如何拦截帐户暴力破解？** ● **帐户被暴力破解，怎么办？** ● **如何预防帐户暴力破解攻击？** ● **漏洞修复完毕后是否需要重启主机？**

发布日期	修改说明
2021-04-28	第三十次正式发布。 ● 新增如下常见问题： – **如何使用命令行方式安装Agent（Windows操作系统）？** – **关闭弱口令策略后，之前扫描的弱口令事件为什么还会重复出现？**。 ● 修改如下常见问题： – **Agent状态异常应如何处理？** – **添加登录白名单后，为什么还有异地登录告警？**
2021-02-25	第二十九次正式发布。 **是否可以不开启HSS告警通知？** 修改问题内容，可以不设置告警通知，开启主机安全防护。
2021-02-01	第二十八次正式发布。 新增如下常见问题： ● **HSS是否支持线下多台服务器共用一个公网IP？** ● **防护配额与主机不在同一企业项目，是否可以相互绑定？** ● **购买云服务器时，为什么无法选择免费的企业主机安全防护？**
2020-11-16	第二十七次正式发布。 **HSS可以跨区域使用吗？** 将支持跨区域使用修改为“不支持跨区域使用”。
2020-11-10	第二十六次正式发布。 新增如下常见问题： ● **帐户被暴力破解，怎么办？** ● **出现弱口令告警，怎么办？** ● **主机被挖矿攻击，怎么办？** ● **添加告警白名单后，为什么进程还是被隔离？** ● **添加登录白名单后，为什么还有异地登录告警？** ● **如何修改接收告警通知的手机号或邮箱？**
2020-06-20	第二十五次正式发布。 新增**HSS支持企业项目后，如何同步配置数据？**。
2020-05-18	第二十四次正式发布。 新增如下常见问题： ● **HSS与WAF的网页防篡改有什么区别？** ● **如何查看HSS的日志文件？**

发布日期	修改说明
2020-03-09	第二十三次正式发布。 新增如下常见问题： ● **如何筛选未安装Agent的主机？** ● **为什么开启双因子认证后登录主机失败？** ● **开启双因子认证时，如何添加手机号？** ● **双因子认证中，验证码是一个固定的验证码吗？** ● **开启动态网页防篡改后，状态是“已开启未生效”，怎么办？** ● **如何清除HSS中配置的SSH登录IP白名单？**
2020-01-14	第二十二次正式发布。 新增如下常见问题： ● **什么是HSS的Agent？** ● **是否可以不开启HSS告警通知？**
2019-12-26	第二十一次正式发布。 新增如下常见问题： ● **HSS可以跨账号使用吗？** ● **购买HSS后会自动安装Agent吗？**
2019-12-18	第二十次正式发布。 删除以下常见问题： 华为云主机安全是否支持订阅周报功能？
2019-11-27	第十九次正式发布。 新增如下常见问题： ● **HSS到期后不续费，对主机和业务有影响吗？** ● **开启网页防篡改后，如何修改文件？** ● **配置告警通知时选不到消息主题？** ● **如何避免账户破解攻击？** ● **开启防护时显示没有配额？**
2019-10-12	第十八次正式发布。 新增以下常见问题： **如何处理漏洞？**
2019-09-23	第十七次正式发布。 新增以下常见问题： ● **基础版能够升级为企业版吗？** ● **没有手动解除的IP拦截记录为什么会显示已解除？** ● 主机安全基线检测检查出配置风险项怎么办？ ● **为什么要添加防护目录？** ● **无法开启网页防篡改怎么办？**

发布日期	修改说明
2019-04-25	第十三次正式发布。 新增以下常见问题： 企业版能升级为网页防篡改版吗？
2019-04-08	第十六次正式发布。 **如何使用双因子认证？** 更新了截图和相关描述。
2019-03-18	第十五次正式发布。 新增以下常见问题： 企业主机安全是否支持对裸金属机器提供防护？
2018-11-06	第十四次正式发布。 新增以下常见问题： ● **在Windows中文系统中输入数字卡顿或需要数字连输怎么办？** ● **如何批量安装Agent？**
2018-10-25	第十三次正式发布。 修改以下常见问题： **如何批量安装Agent？**
2018-09-15	第十二次正式发布。 新增以下常见问题： ● **如何开启登录失败日志开关？** ● 如何开启filezilla的登录失败日志开关？ ● 如何开启vsftp的登录失败日志开关？
2018-08-02	第十一次正式发布。 修改以下常见问题： **如何解决Linux系统的账户破解防护功能未生效的问题？**
2018-07-19	第十次正式发布。 新增以下常见问题： 如何解决SUSE12 SP2（包含SAP）、Gentoo系统设置帐户破解防护拦截IP后未生效？
2018-06-28	第九次正式发布。 新增以下常见问题： Windows系统如何设置安全的口令复杂度策略？
2018-06-13	第八次正式发布。 新增以下常见问题： 如何批量安装Agent？
2018-05-17	第七次正式发布。 优化常见问题标题。

发布日期	修改说明
2018-05-07	第六次正式发布。 修改以下常见问题： 企业主机安全是否收费?
2018-04-19	第五次正式发布。 修改以下常见问题： 更新“如何安装Agent? ”的截图。
2018-03-15	第四次正式发布。 删除以下常见问题： 安装Windows版本Agent报错应该如何处理?
2018-01-09	第三次正式发布。 新增以下常见问题： 如何安装Agent?
2017-11-17	第二次正式发布。 新增以下常见问题： 如何安装PAM并设置安全的口令复杂度策略?
2017-09-30	第一次正式发布。