主机安全服务

常见问题

文档版本 16

发布日期 2024-01-08

华为云计算技术有限公司

商标声明


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

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品咨询

1.1 什么是主机安全?

主机安全是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

工作原理

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

主机安全的工作原理如图1-1所示。

图 1-1 工作原理

各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：10180。 • 每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。 • 根据您配置的安全策略，阻止攻击者对主机的攻击行为。 **说明** • 如果未安装Agent或Agent状态异常，您将无法使用主机安全服务。 • 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、容器安全与主机安全共用同一个Agent，您只需在同一主机安装一次。

1.2 什么是容器安全?

容器安全能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时提供容器进程白名单、容器文件监控、容器信息收集和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

1.3 什么是网页防篡改?

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

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

网页防篡改的操作流程和主要功能概览。操作流程如图1-2所示，主要功能概览请参考表1-2。

图 1-2 网页防篡改操作流程

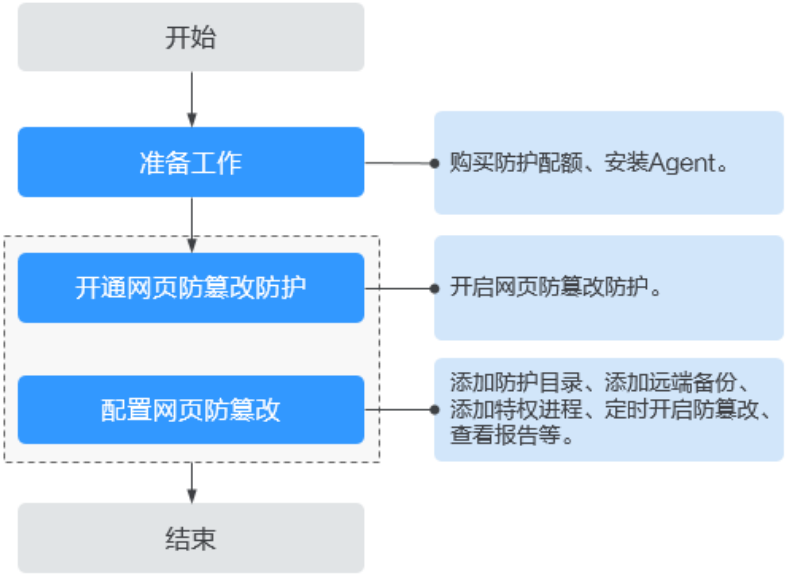


表 1-2 主机安全防篡改操作流程及功能说明

操作类型	操作	描述与参考
准备工作	--	使用主机安全服务前，如果无VDC业务员账号，需要运营管理员创建VDC和VDC管理员，VDC管理员创建VDC业务员。
开通网页防篡改防护	申请防护配额	您需要申请防护配额后，才能开启网页防篡改防护。
	安装Agent	Agent是HSS提供的客户端，用于执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息上报给云端防护中心。 安装Agent后，您才能开启网页防篡改防护。
	设置告警通知	设置告警通知功能后，您能接收到HSS发送的告警通知，及时了解主机/网页内的安全风险。 否则，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警信息。
	开启主机防护	开启主机防护时，您需为指定的主机分配一个配额。
配置网页防篡改防护	添加防护目录	网页防篡改实时监控网站目录，开启网页防篡改前请添加防护目录。

操作类型	操作	描述与参考
	添加远端备份	HSS默认将防护目录下的文件备份在“添加防护目录”时添加的本地备份路径下，为防止备份在本地的文件被攻击者破坏，请您启用远端备份功能。
	添加特权进程	开启网页防篡改防护后，防护目录中的内容是只读状态，如果您需要修改防护目录中的文件或更新网站，可以添加特权进程。
	定时开启网页防篡改	网页防篡改提供的定时开关功能，能够定时开启/关闭静态网页防篡改功能，您可以使用此功能定时更新需要发布的网页。
	开启动态网页防篡改	动态网页防篡改提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为。
	查看网页防篡改报告	开启网页防篡改防护后，HSS将立即对您添加的防护目录执行全面的安全检测。您可以查看主机被非法篡改的详细记录。

1.4 镜像、容器、应用的关系是什么?

- 镜像是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数（如匿名卷、环境变量、用户等）。镜像不包含任何动态数据，其内容在构建之后也不会被改变。
- 容器和镜像的关系，像程序设计中的实例和类一样，镜像是静态的定义，容器是镜像运行时的实体。容器可以被创建、启动、停止、删除、暂停等。
- 一个镜像可以启动多个容器。
- 应用可以包含一个或一组容器。

1.5 如何使用主机安全服务?

如使用主机安全服务请按照如下步骤进行操作：

步骤1 **购买防护配额**。

步骤2 **安装Agent**。

安装Agent后，您才能开启主机安全服务。

步骤3 **设置告警通知**。

开启告警通知功能后，您能接收到主机安全服务发送的告警通知，及时了解主机内的安全风险。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。

- 开启主机安全服务时，您需为指定的主机分配一个配额，关闭主机安全服务或删除主机后，该配额可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

1.6 HSS 是否支持防护本地 IDC 服务器?

支持。

如果您的服务器能连接到公网，就可以使用主机安全服务对其进行防护。

具体实施方案请参见**HSS多云纳管部署**。

1.7 HSS 是否和其他安全软件有冲突?

主机安全服务可能会和“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。

1.8 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
主机安全服务（HSS）	基础安全	提升主机整体安全性。	• 资产管理 • 漏洞管理 • 入侵检测 • 基线检查 • 网页防篡改

服务名称	所属分类	防护对象	功能差异
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 • 准确访问防护

1.9 HSS 支持跨账号使用吗?

HSS不支持跨账号使用，每个账号需要单独购买HSS进行部署。但是支持多个IAM用户共享使用。

多个 IAM 用户共享使用

例如，您通过注册华为云创建了1个账号（“domain1”），且由“domain1”账号在IAM中创建了2个IAM用户（“sub-user1a”和“sub-user1b”），如果您授权了“sub-user1b”用户HSS的权限策略，则“sub-user1b”用户可以使用“sub-user1a”用户的HSS。

1.10 什么是 HSS 的 Agent?

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

Agent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/容器；实时监测主机/容器的安全状态；并将收集的主机/容器信息上报给云端防护中心。
- 根据您配置的安全策略，阻止攻击者对主机/容器的攻击行为。

说明

- 如果未安装Agent或Agent状态异常，您将无法使用主机安全服务。
- 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。

Linux Agent 相关进程

Agent进程运行账号：root。

Agent包含以下进程：

表 1-4 Linux 主机 Agent 运行进程

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

Windows Agent 相关进程

Agent进程运行账号：system。

Agent包含以下进程：

表 1-5 Windows 主机 Agent 运行进程

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

1.11 主机安全服务可以跨云使用吗?

可以。

如果您的业务不在华为云上，可以使用HSS。主机安全服务HSS支持防护华为云ECS服务器、华为云BMS服务器、华为云云耀云服务器、华为云云桌面（Workspace）以及第三方云服务器和线下主机，方便您集中管理同一区域内多样化部署的服务器。

具体实施方案请参见**HSS多云纳管部署**。

1.12 购买什么版本的 HSS 能够满足等保二级的整改要求?

您需要购买企业版、旗舰版、容器版或者网页防篡改版才能满足等保二级及以上的认证，基础版的功能无法满足整改要求。

购买企业版、旗舰版、网页防篡改版、容器版详情请参见**购买主机安全防护配额**。

1.13 主机安全服务支持版本升级吗?

配额版本支持升级。

升级说明

- 网页防篡改版、容器版目前为最高版本，暂无法进行升级。
- 升级的目标规格为企业版或旗舰版时，通过原配额版本直接操作升级即可。升级的目标规格为网页防篡改版时，需单独进行购买，购买后将目标服务器防护配额绑定为网页防篡改版。
- 基础版可升级为企业版或旗舰版或网页防篡改，企业版可升级为旗舰版或网页防篡改，旗舰版可升级为网页防篡改。

升级至企业版/旗舰版操作

主机安全服务的配额版本升级时目标配额版本的“使用状态”必须为“空闲”，因此，升级的操作流程取决于目标配额版本的使用状态。

- **使用状态为空闲**

  可直接在防护配额页面直接进行升级操作，操作详情请参见**配额版本升级**。
- **使用状态为使用中**

  a. 需要对目标配额进行解除绑定操作，操作详情请参见**解绑配额**。

  b. 解除绑定后查看目标配额版本的“使用状态”为“空闲”。

  c. 执行配额升级操作，操作详情请参见**升级至企业版/旗舰版**。

升级至网页防篡改版操作

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

1. 在主机安全服务控制台购买网页防篡改版防护配额，详情请参见**购买防护配额**。
2. 解除目标配额与服务器的绑定，操作详情请参见**解绑配额**。
3. 重新绑定升级的网页防篡改，操作详情请参见**升级至网页防篡改版**。

1.14 HSS 是否支持病毒查杀?

主机安全服务 HSS支持检测恶意程序、勒索病毒等入侵威胁。

- 对于恶意进程和进程异常行为：HSS支持手动隔离查杀，详细操作请参见**处理告警事件**。
- 对于勒索病毒：HSS为您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**勒索病毒防护**。

同时建议您可以安装杀毒软件，作为主机安全的进一步加固。

2 Agent 问题

2.1 购买 HSS 后会自动安装 Agent 吗?

购买HSS后系统不会自动执行安装Agent，但可通过复制命令执行快捷安装Agent。

Agent 安装场景说明

Agent的安装场景可分为如下情况：

- 购买服务器时的自动安装
- 购买服务器后的手动安装

新购服务器时的自动安装

在新购买华为云ECS时，勾选“开通主机安全防护”，HSS会自动为该ECS安装Agent，并开启防护。

- “计费模式”选择的“包年/包月”，您可以选择“基础版”、“企业版”、“旗舰版”和“网页防篡改版”主机安全服务，完成购买后，HSS自动为该ECS开启相应版本的主机防护。
- “计费模式”选择的“按需计费”，您可以选择“企业版”主机安全服务，完成购买后，HSS自动为该ECS开启“企业版”主机防护。

如果您选择的主机安全服务配额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）。各版本主机安全服务配额的差异请参见**版本功能特性**。

购买 HSS 后的手动安装

如果您单独购买HSS，HSS不会为服务器自动安装Agent，需要您在HSS控制台找到目标系统的安装命令，登录服务器安装Agent，操作步骤详情请参见**安装Agent**。

2.2 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：如果登录主机的IP地址被识别为攻击IP，但是无法被“解封”。
- 冲突原因：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，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。
- 操作步骤：
  a. 以**root**用户登录ECS。
  b. 执行以下命令，检查是否安装了DenyHosts。
  ps -ef | grep denyhosts.py
  如果界面回显类似以下信息，则说明安装了DenyHosts。

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

  c. 执行以下命令，停止DenyHosts。
  kill -9 'cat /var/lock/denyhosts'
  d. 执行以下命令，取消DenyHosts的自启动。
  chkconfig --del denyhosts;

2.3 如何安装 Agent?

- 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**。

2.4 如何卸载 Agent?

提供一键卸载和手动本地卸载两种方式。

操作场景

- Agent包选择错误，需要卸载Agent后重新安装。
- 安装命令复制错误（如在32位的主机中安装64位的Agent），需要卸载Agent后重新安装。
- 主机安全服务升级Agent失败，需要排查执行Agent卸载。

前提条件

通过控制台一键卸载Agent时，云服务器的“Agent状态”为“在线”。

控制台一键卸载 Agent

用户可以通过主机安全服务控制台直接卸载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 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航中，选择“安装与配置”，进入“安装与配置”界面。

步骤4 在目标服务器所在行的“操作”列，单击“卸载Agent”。

如果需要批量卸载Agent，您可以批量勾选所有待卸载Agent的服务器，单击列表上方的“批量卸载Agent”。

步骤5 在弹出的卸载Agent对话框中，单击“确认”。

云服务列表“Agent状态”显示为“离线”，卸载Agent成功。

----结束

主机本地卸载

用户在不需要使用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. 登录需要卸载主机安全服务Agent的云服务器，并执行如下命令切换到**root**用户。

     su - root

  b. 在任意目录执行如下命令，卸载Agent。

     说明

     不可以在/usr/local/hostguard/目录下执行卸载命令，可以在其他任意目录下执行卸载命令。

     - 针对EulerOS、CentOS、RedHat等支持rpm安装软件的OS，执行命令：**rpm -e hostguard**
     - 针对Ubuntu、Debian等支持deb安装软件的OS，执行命令：**dpkg -P hostguard**

     当界面回显如下类似信息，则表示卸载Agent完成，无需再执行下一步。如果卸载失败请执行步骤3。

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

  c. （可选）当执行步骤2卸载Agent失败时，可参考如下方式卸载Agent。

     - 针对EulerOS、CentOS、RedHat等支持rpm安装软件的OS。
       1) 执行如下命令，删除安装记录。

          rpm -e --justdb hostguard

       2) 执行如下命令，查询是否有hostguard残留进程。

          ps -ef | grep hostguard

          如果有残留，请执行命令**kill -9“进程pid”**杀死所有残留进程。

       3) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。

ll /usr/local/hostguard

如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。

4) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。

ll /etc/init.d/hostguard

如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。

- 针对Ubuntu、Debian等支持deb安装软件的OS。

1) 执行如下命令，查询是否有hostguard残留进程。

ps -ef | grep hostguard

如果有残留，请执行命令**kill -9“进程pid”**杀死所有残留进程。

2) 执行如下命令，查看“/usr/local/hostguard”目录是否存在。

ll /usr/local/hostguard

如果该目录存在，请执行命令**rm -rf /usr/local/hostguard**删除目录。

3) 执行如下命令，查看“/etc/init.d/hostguard”文件是否存在。

ll /etc/init.d/hostguard

如果该文件存在，请执行命令**rm -f /etc/init.d/hostguard**删除文件。

- **卸载Windows版本Agent**

a. 登录需要卸载主机安全服务Agent的云服务器。

b. 在“控制面板 > 程序和功能”中选中“HostGuard”，然后单击“卸载”。

说明

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

c. 在“HostGuard卸载向导”提示框中，单击“是”，开始卸载。

d. （可选）重启主机。

- 如果您开启了网页防篡改，卸载Agent需要重启主机。在“HostGuard卸载向导”弹窗中，单击“是”，重启主机。
- 如果您未开启网页防篡改，无需重启主机。在“HostGuard卸载向导”弹窗中，单击“否”，不重启主机。

2.5 Agent 安装失败应如何处理?

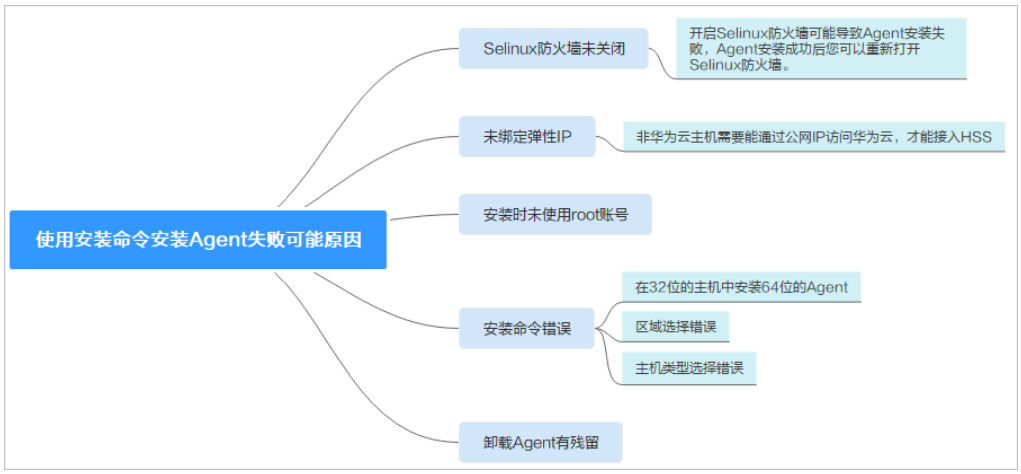
如果您使用过旧版主机安全服务，当前在新版安装Agent后仍然显示未安装请参考**Agent安装成功后显示未安装怎么处理?**。

如果为首次安装Agent出现安装失败，请参考本文排查处理。

问题现象

使用命令安装失败，安装Agent后，控制台防护列表页面仍然显示“未安装”。

可能原因



解决方案

步骤1 确认是否已关闭主机Selinux防火墙。

- 已关闭：请执行下一步骤。
- 未关闭：请关闭Selinux防火墙后重新安装。

步骤2 确认主机是否已绑定弹性IP。

- 是：请执行下一步骤。
- 否：请绑定弹性IP后重新安装。

步骤3 请根据主机所在区域、主机操作系统，确认安装命令是否正确。

1. 正确地选择主机所在的区域，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：请执行下一步骤。
- 否：请使用正确的命令重新安装。

步骤4 确认安装账号是否为**root**账号。

- 是：请执行下一步骤。
- 否：请使用root账号重新安装。

步骤5 确认主机DNS能否正常解析Agent下载域名。

1. 执行如下命令，检查解析情况。
   - Linux主机：**ping -c 1 hss-agent.区域代码.myhuaweicloud.com**
   - Windows主机：**ping -n 1 hss-agent.区域代码.myhuaweicloud.com**

说明

命令中的区域代码，每个区域不同，各区域代码请参见**地区和终端节点**。

以“华北-北京一”为例，完整命令示例：ping -c 1 hss-agent.cn-north-1.myhuaweicloud.com

2. 查看命令执行结果。
   - 解析成功：界面回显解析出的IP，表示DNS解析正常，请执行**6**。
   - 解析失败：界面回显“name or service not known”或未解析出IP，表示DNS解析失败。由于公网无法访问Agent下载地址，请配置正确的华为云内网DNS地址后，重新安装Agent，详细操作请参见**修改云服务器的DNS服务器地址**、**华为云内网DNS地址**。

步骤6 使用root账号**卸载Agent**后强制安装。

- 安装成功：结束操作。
- 安装失败：请联系技术支持。

----结束

2.6 Agent 状态异常应如何处理?

Agent状态主要分为以下三种，如果Agent的运行状态为“未安装”或者“离线”时，表示Agent与服务器间通信异常。

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

可能的原因

- 控制台Agent状态未更新。

  安装Agent后，不会立即生效，需要等待5-10分钟左右控制台才会刷新。
- 操作系统不支持。

  HSS目前支持的操作系统请参见**HSS支持的操作系统及版本**。
- 网络故障。

  主机中的Agent和云端防护中心出现异常，如网卡故障、IP地址异变及带宽较低。
- 主机内存不足。
- Agent进程异常。

处理方法

步骤1 在主机上安装Agent成功已超过10分钟，控制台Agent状态仍显示“离线”。

- 是：请执行**2**。
- 否：请您耐心等待Agent上线，无需执行后续操作。安装Agent成功后，不会立即生效，需要等待5-10分钟左右控制台才会刷新状态。

步骤2 主机的操作系统是否在**HSS支持的操作系统及版本**范围内。

- 是：请执行**3**。
- 否：主机安全服务的Agent无法正常安装和运行在您的主机上，请升级为主机安全服务支持的操作系统后再尝试安装Agent。

步骤3 主机网络是否正常。

- 是：请执行**4**。
- 否：请确保您的主机所属安全组出方向设置允许访问100.125.0.0/16网段的10180端口，且主机能正常访问网络。待主机能正常访问网络后，再查看Agent状态。

步骤4 主机剩余可用内存是否大于300MB。

- 是：请执行**5**。
- 否：主机内存不足将导致Agent离线，请扩充内存容量，容量扩充完成后，Agent将恢复上线。

步骤5 Agent进程异常，需要重启Agent。

- Windows操作系统
  a. 以管理员**administrator**权限登录主机。
  b. 打开“任务管理器”。
  c. 在“服务”页签选中“HostGuard”。
  d. 单击鼠标右键，选择“重新启动”，完成重启Agent。
- Linux操作系统
  请以**root**用户在命令行终端执行以下命令，完成重启Agent。
  service hostguard restart
  如果回显以下信息，则表示重启成功。

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

重启进程后等待2-3分钟：

- 如果Agent状态为“在线”，则故障清除。
- 如果Agent状态仍为“未安装”或者“离线”，请卸载Agent，再重新安装Agent。

----结束

2.7 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2-1**所示。

表 2-1 Agent 的默认安装路径

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

2.8 Agent 检测时占用多少 CPU 和内存资源?

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

具体占用的CPU、内存资源如下：

CPU 占用峰值

Agent运行时，CPU占用控制在**1vCPU**的20%以内。因此，实际占用比例与您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**。

如果CPU占用比例超过1vCPU的20%，Agent会自动降CPU；自动降CPU后，Agent检测主机时间会延长，但不影响服务使用。如果CPU占用比例超过1vCPU的25%，Agent将自动重启。

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。
- 如果Agent正在执行病毒查杀任务，病毒查杀程序会额外占用部分CPU，占用最多不超过多核的30%。关于病毒查杀的详细介绍请参见**病毒查杀**。

内存占用峰值

Agent运行时，内存占用控制在**500 MB**以内。如果Agent内存占用超过最大内存限制**500 MB**，Agent会在5分钟内自动重启。

说明

如果Agent正在执行病毒查杀任务，内存占用控制在**均值800 MB**。关于病毒查杀的详细介绍请参见**病毒查杀**。

如果主机可用内存小于50 MB，Agent会切换为“静默”状态。如果Agent内存占用超限重启，半小时达10次，Agent切换为“空载”状态；1小时达15次，Agent当天切换为“静默”状态。以下是状态说明：

- 空载状态：Agent所有防护功能关闭，可通过控制台执行升级、卸载操作。
- 静默状态：Agent所有防护功能关闭，不可通过控制台执行升级、卸载操作。

Agent后台状态可在Agent安装目录下的conf/framework.conf文件中查看“run_mode”字段。

如果需要将Agent恢复为正常状态，可按以下操作执行：

说明

如果您开启了自保护策略，请先关闭自保护策略再执行以下操作。详细操作参考**关闭自保护**。

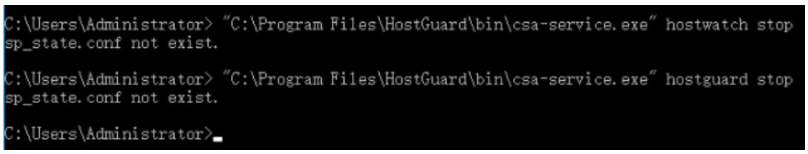
1. （可选）主机扩容。

   主机可用内存小于50 MB才需执行此操作。
2. 修改Agent安装目录下的conf/framework.conf文件，将run_mode冒号后面的模式改为normal。
3. 执行以下操作，删除记录重启次数的文件。

- Linux：执行命令**rm -f /usr/local/hostguard/run/restart.conf**。
- Windows：找到**C:\Program Files\HostGuard\run\restart.conf**并删除。

4. 执行以下操作，重启Agent。
   - Linux：执行命令**service hostguard restart**。
   - Windows：
     - Agent为4.0.17及以下版本：
       1) 以管理员**administrator**权限登录主机。
       2) 打开“任务管理器”，选择“服务”页签。
       3) 选中Hostwatch，单击鼠标右键选择“停止”，等待状态改变为“已停止”后执行步骤4。
       4) 选择中Hostguard，单击鼠标右键选择“停止”。
       5) 选中Hostwatch，单击鼠标右键选择“开始”，完成重启。
          启动Hostwatch后会自动拉起Hostguard。
     - Agent为4.0.18及以上版本：
       1) 以管理员**administrator**权限登录主机。
       2) 打开cmd命令提示符窗口，依次执行以下命令停止服务。
          sc control hostwatch 198
          sc control hostguard 198
          如图 停止服务所示为正常现象，开启自保护的主机上不会生成sp_state.conf文件。

          图 2-1 停止服务

       3) 打开“任务管理器”，选择“服务”页签。
       4) 选中Hostwatch，单击鼠标右键选择“开始”，完成重启。
          启动Hostwatch后会自动拉起Hostguard。

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2-2所示。

表 2-2 Agent 资源占用一览

vCPUs规格	Agent运行占用CPU资源比例（峰值）	执行病毒查杀时，内存占用(峰值)	内存占用（峰值）	执行病毒查杀时，内存占用（均值）
1vCPUs	20%	50%	500 MB	800 MB
2vCPUs	10%	40%	500 MB	800 MB
4vCPUs	5%	35%	500 MB	800 MB

vCPUs规格	Agent运行占用CPU资源比例（峰值）	执行病毒查杀时，内存占用(峰值)	内存占用（峰值）	执行病毒查杀时，内存占用（均值）
8vCPUs	2.5%	32.5%	500 MB	800 MB
12vCPUs	约1.67%	约31.67%	500 MB	800 MB
16vCPUs	约1.25%	约31.25%	500 MB	800 MB
24vCPUs	约0.84%	约30.84%	500 MB	800 MB
32vCPUs	约0.63%	约30.63%	500 MB	800 MB
48vCPUs	约0.42%	约30.42%	500 MB	800 MB
60vCPUs	约0.34%	约30.34%	500 MB	800 MB
64vCPUs	约0.32%	约30.32%	500 MB	800 MB

2.9 网页防篡改、容器安全与主机安全共用 Agent 吗?

是的。

同一服务器安装一次Agent即可满足所有版本的使用。

2.10 如何查看未安装 Agent 的主机?

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“安装与配置”，进入Agent管理页面。

步骤4 单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。

Agent状态，如下所示：

- 未安装：未安装Agent，或Agent已安装但未成功启动。
- 在线：Agent运行正常。
- 离线：Agent与HSS服务器通信异常，HSS无法提供安全防护功能。
  单击“离线原因”，您可以查看导致Agent不在线的可能原因。

----结束

2.11 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，但主机会在两个平台显示，因此Agent状态及防护情况只能在新版或旧版其中一个平台正常显示，Agent在另一版本则显示未安装。

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

解决办法

由于Agent对于主机的唯一性，主机安全服务新版和旧版您只能使用一个平台。

如果您正在使用旧版，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

目前主机安全服务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服务。

2.12 Agent 如何升级?

主机安全服务将Agent1.0升级至Agent2.0需要在主机安全服务（旧版）控制台中操作，升级后您将在主机安全服务（新版）继续查看、管理主机防护状态，主机安全服务（旧版）将停止检测、防护。

如何判断是否已升级

判断服务器是否升级需要在主机安全服务（旧版）控制台查看服务器的“Agent状态”。

步骤1 **登录管理控制台**。

步骤2 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务（旧版）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，进入主机安全服务（旧版）服务器页面。

步骤4 在服务器页面查看所有服务器的“Agent状态”为“升级成功”表示目标主机的Agent已升级成功。

如果为“在线”状态且可进行**升级操作**。

图 2-2 查看 Agent 状态

步骤5 单击“前往查看”，将跳转至主机安全服务（新版）控制台“云服务器”页面查看服务器运行情况。

----结束

升级前提条件

- 升级时目标云服务器的“Agent状态”必须为“在线”。
- 升级Agent需要在旧版主机安全服务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console进行计费，旧版停止计费。
- 升级后需切换至主机安全服务（新版）查看云服务器防护状态，主机安全服务（旧版）将停止防护。

  说明

  - 当前支持切换至主机安全服务的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，在总览页左上角单击“返回旧版”，可切换至主机安全（旧版）。
- 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。

控制台一键升级 Agent2.0

步骤1 登录管理控制台。

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

步骤3 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 2-3 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服务的“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”。
- 如果服务器开启了网页防篡改版防护，请先前往网页防篡改页面，关闭网页防篡改防护后，再进行Agent升级，否则无法选中待升级的服务器。

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3**进入的主机安全服务（旧版）界面查看目标云服务器的“Agent状态”为“升级成功”表示升级成功。

说明

- 升级过程中出现升级失败或完成后仍然显示未安装处理办法可参见**Agent升级失败或安装后仍然显示未安装怎么处理？**。

图 2-4 查看 Agent 状态

----结束

Windows 主机手动升级 Agent2.0

如果您的Windows主机通过控制台一键升级Agent2.0失败可进行手动升级。

步骤1 远程登录待升级Agent2.0的Windows主机。

步骤2 进入Windows主机的C:\Program Files (x86)\HostGuard目录下。

步骤3 删除“PkgConfMgr.exe”文件。

注意

如果您在开启主机安全服务（旧版）防护时授权Agent1.0打开防火墙，Agent1.0在打开防火墙的同时会添加允许全入（hostguard_AllowAnyIn）和全出（hostguard_AllowAnyOut）的规则，防止打开防火墙后对您的业务造成影响。Agent1.0被卸载后，全入全出规则会被删除，您如果没有给自己的业务创建放通规则，业务的网络访问会被阻断。因此您务必要将“PkgConfMgr.exe”文件删除，避免Agent1.0添加的全入全出规则被删除。

步骤4 双击“unins000.exe”文件，卸载Agent1.0。

步骤5 在“HostGuard卸载向导”弹窗中，单击“是”，完全删除HostGuard及其所有组件。

步骤6 （可选）重启主机。

- 如果您开启了网页防篡改，卸载Agent1.0需要重启主机。在“HostGuard卸载向导”弹窗中，单击“是”，重启主机。
- 如果您未开启网页防篡改，无需重启主机。在“HostGuard卸载向导”弹窗中，单击“否”，不重启主机。

步骤7 查看Windows主机的C:\Program Files (x86)\HostGuard目录不存在，表示卸载Agent1.0完成。

步骤8 登录管理控制台。

步骤9 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务（新版）页面。

步骤10 在左侧导航栏选择“安全与配置 > Agent管理”。

步骤11 在Agent管理页面，单击“接入多云资产”。

步骤12 在Agent安装指南弹窗中，根据服务器的系统架构和操作系统，选择“复制”下载Agent的链接。

步骤13 在待安装Agent2.0的Windows主机中，通过IE浏览器访问复制的Agent2.0下载链接，下载Agent安装包并解压。

步骤14 使用管理员权限运行Agent2.0安装程序。

安装Agent2.0时，在主机类型界面，选择主机类型。

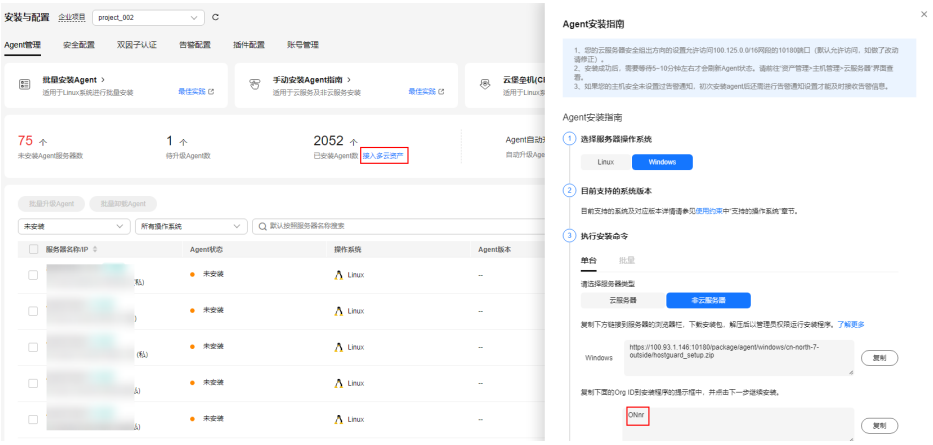
- 华为云主机：请选择“华为云主机”。
- 非华为云主机：请选择“其他云主机”。

  在Agent安装指南中复制Org ID，如图2-5所示，在安装程序提示框中输入Org ID，然后按界面提示完成Agent安装。

须知

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

图 2-5 获取 Org ID（非华为云主机）



步骤15 安装完成后，在“Windows任务管理器”中查看进程“HostGuard.exe”和“HostWatch.exe”。

两个进程皆存在，则表示Agent安装成功。

步骤16 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

Linux 主机手动升级 Agent2.0

如果您的Linux主机通过控制台一键升级Agent2.0失败可进行手动升级。

步骤1 远程登录待升级Agent2.0的Linux主机。

步骤2 执行以下命令，卸载Agent1.0。

说明

不可以在/usr/local/hostguard/目录下执行卸载命令，可以在其他任意目录下执行卸载命令。

- EulerOS、CentOS、SUSE、RedHat等支持rpm安装方式的OS的卸载命令：**rpm -e hostguard;**
- Ubuntu、Debian等支持deb安装方式的OS的卸载命令：**dpkg -P hostguard;**

步骤3 查看Linux主机的/usr/local/hostguard/目录不存在，表示Agent1.0卸载完成。

步骤4 登录管理控制台。

步骤5 在页面左上角选择“区域”，单击 ☰，选择“安全与合规 > 主机安全服务”，进入主机安全服务（新版）页面。

步骤6 在左侧导航栏选择“安全与配置 > Agent管理”。

步骤7 在Agent管理页面，单击“接入多云资产”。

步骤8 在Agent安装指南弹窗中，根据服务器的系统架构和操作系统，选择“复制”安装Agent的命令。

步骤9 在Linux主机中以root权限执行上一步获取的安装命令，安装Agent2.0。

如果界面回显信息如**图 Agent安装成功**所示，表示Agent2.0安装成功。

图 2-6 Agent 安装成功

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

步骤10 使用**service hostguard status**命令，查看Agent的运行状态。

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

图 2-7 Agent 运行正常

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

步骤11 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

2.13 主机安全服务升级失败怎么处理?

Agent 升级说明

- 无论升级前还是升级后同一台主机都会同时在主机安全服务新、旧版呈现，服务器状态以使用的控制台版本为准。
- 整个升级Agent过程均为免费。
- 升级时查看“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服务（新版）继续被防护，主机安全服务（旧版）将停止防护。

升级 Agent 原理

在主机安全服务控制台单击升级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。

- 升级时Agent在旧版控制台反馈的状态：

  - 升级成功：已经升级成功，可切换至主机安全服务（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。
- 升级时Agent在新版控制台反馈的状态：
  - 未安装：目标主机在新版控制台还未进行Agent安装。
  - 在线：Agent运行正常。
  - 离线：Agent通信异常。

失败常见原因

说明

自动执行升级完成后，需要等待5~10分钟左右Agent才会自动刷新Agent状态。

Agent升级失败或超过等待时间仍不显示可能原因如下：

1. DNS无法解析：Agent升级只能通过内网DNS解析，因此需要保证内网DNS地址的正确性。
2. 10180端口被限制访问：Agent升级需要通过端口10180进行访问。
3. 可用内存不足：Agent升级需要占用一定内存，主机剩余内存小于300M会影响正常升级。
4. 无法正常获取metadata：Agent升级需要获取服务器的ID、名称、Region等信息。

原因排查及解决办法

- **DNS无法解析**
  - 排查步骤
    i. 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
    ii. 执行以下命令，查询目标云服务器的内网DNS地址。
    cat /etc/resolv.conf
    iii. 记录目标服务器已查询的DNS地址和所在Region，参照**内网DNS地址**对比，确认是否与标准的Region和DNS地址相匹配。
    iv. 如果排查确认Region和DNS匹配，则非DNS解析问题，排查其他原因。
    如果Region和DNS不匹配，则为内网DNS解析地址有误。
  - 解决办法
    确认Region和DNS不匹配后，需要确认服务器已设置的内网DNS修改后是否影响业务。
    - 如果不影响，可参照**切换服务器的DNS地址**修改服务器的内网DNS，修改后执行升级。
    - 如果会影响业务，内网DNS无法进行修改，您需要建立主机名与IP地址之间的映射关系，添加信息后执行升级，操作步骤如下：
      1) 登录目标云服务器。
      2) 执行以下命令，切换至root权限。
      sudo su -
      3) 执行以下命令，编辑hosts文件。

vi /etc/hosts

4) 键盘键入“i”，进入编辑模式。
5) 按照如下格式添加语句，建议映射关系。

私有IP地址 主机名

【示例】：

192.168.0.1 hostname01

192.168.0.2 hostname02

6) 键盘键入“Esc”退出编辑模式。
7) 执行以下命令，保存并退出。

:wq

- **10180端口被限制访问。**

  待安装或升级Agent的线上主机需要与网段相通，要求您的服务器安全组出方向的设置允许访问100.125.X.X/16网段的10180端口。

  – 排查步骤

    i. 在页面左上角选择“区域”，单击 ☰，选择“计算 > 弹性云服务器”。
    ii. 单击目标服务器名称，进入服务器详情页面，单击“安全组”，查看安全组规则。
    iii. 选择“出方向规则”，查看禁止策略中是否有10180端口。
      1) 如果没有，表示非端口被限制访问问题。
      2) 如果存在，表示端口被限制访问。

  – 解决办法

    端口被限制访问，需要将端口策略修改为允许，操作详情请参见**配置安全组规则**中的步骤8。

- **可用内存不足。**

  – 排查步骤

    ▪ Linux主机

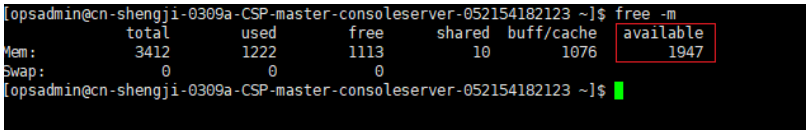
      1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
      2) 执行以下命令，查看目标云服务器的内存使用情况。

         free -m

      3) 执行命令反馈信息如**图2-8**所示，查看free项的数值。

         如果available数值小于300M，则表示内存不足。

         图 2-8 查看内存



    ▪ Windows主机

      1) 通过远程管理工具（如：mstsc、rdp）远程登录目标云服务器。

2) 打开任务管理器。
3) 选择“性能 > 内存”，进入“内存”页面，查看剩余可用内存。
如果可用内存小于300M，则表示内存不足。

- 解决办法
  - 关闭一些高内存占用的应用程序。
  - 扩充内存容量后再进行安装，扩容操作详情请参见**变更服务器规格**。

- **无法正常获取metadata。**
  - 排查步骤
    排查是否能正常获取metadata数据操作详情请参见**查询Metadata元数据**。
  - 处理步骤
    需配置路由与169.254.169.254相同才能正常获取，操作详情请参见**云服务器无法获取元数据怎么办？** 。

2.14 主机安全服务不升级有什么影响?

HSS（旧版）在没有被HSS（新版）完全替换前可继续正常使用。

升级至 HSS（新版）的必要性

- 后续产品演进，HSS（新版）将完全替换HSS（旧版），届时HSS（旧版）将会下线。
- 在HSS（新版）中，新增了部分功能以及对部分功能的能力做了大幅度提升，升级后可提升服务器的安全防护能力，大致如下：

表 2-3 HSS（新版）主要功能迭代情况

功能名称	功能描述	功能形态
未防护资产的免费体检	针对未购买HSS防护配额的服务器进行定期免费扫描检测，并提供报告预览。	新增
资产指纹管理	深度扫描服务器中的资产，将资产划分为账号、端口、进程、Web目录、软件信息等不同维度进行统计展示和管理。	新增
资产重要性	您可对名下所有服务器按照服务器资产绑定资产重要性等级，绑定后可按照不同等级的资产进行批量管理，包括但不限于部署策略、开启/关闭防护、分配组、安装Agent，操作详情请参见**关联资产重要性**。	新增
应用漏洞	漏洞扫描新增对应用漏洞的扫描，包括检测Web服务、Web框架、Web站点、中间件、内核模块等资产信息存在的漏洞，操作详情请参见**查看漏洞详情**。	新增
基线报告导出	您可对基线检查的配置检查和经典弱口令检测的结果进行筛选导出。	新增

功能名称	功能描述	功能形态
应用防护	为运行时的应用提供安全防御，您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。包括但不限于对SQL注入、命令注入、反序列化输入、文件遍历、JSP执行操作系统命令等漏洞的扫描检测，操作详情请参见**开启应用防护**。	新增
Agent安装	支持一键批量安装Agent，操作详情请参见**批量安装Agent**。	新增
防护配额管理	支持防护配额版本有低版本直接升级至高版本，操作详情请参见**防护配额管理**。	新增
基线检查	支持自定义勾选等保合规的基线检测项，生成检测结果，操作详情请参见**管理基线检查策略**。	新增
告警事件管理	支持对勒索软件、反弹Shell告警的隔离查杀处理。 支持对一般漏洞利用、Redis漏洞利用、Hadoop漏洞利用、MySQL漏洞利用的检测告警。 操作详情请参见**告警事件概述**。	新增
安全报告	支持自定义报告周期、报告内容、发送时间，操作详情请参见**订阅安全报告**。	升级
勒索病毒	实时监控全盘新增文件及运行中的进程，动态生成诱饵文件进行主动诱捕，识别勒索软件，同时可自定义策略对服务器进行定期备份，操作详情请参见**开启勒索病毒防护**。	升级
容器安全防护	将原有的容器安全服务合并至HSS（新版），将服务器负载进行统一管理。	合并

2.15 华为云 ECS 在 Agent 安装以后会访问哪些地址?

华为云服务器在安装Agent后通常情况会访问的设备、IP、端口如**表2-4**所示。

表 2-4 新装 Agent 访问情况说明

源设备	源IP	源端口	目的设备	目的IP	目的端口（监听）	协议	访问说明	备注
HSS Agent	Agent管理 IP	随机	HSS服务端	HSS服务端-ip1 HSS服务端-ip2	10180	TCP	HSS Agent访问HSS服务端节点，主要是获取服务器端下发的策略/配置/指令、下载Agent软件包/升级包、下载特征库、上报告警事件/资产指纹数据库/基线检查结果和在用户授权许可下上传可疑的可执行程序文件。	每个Region的HSS服务端IP地址不同，Agent通过域名访问，访问的域名格式为：hss-agent.{{REGION_ID}}.myhuaweicloud.com.REGION_ID，每个Region会有差异，每个Region的具体域名可以通过Agent安装指南中的安装命令看到HSS服务器域名地址。
			元数据服务节点	元数据服务节点IP	80		HSS Agent获取Agent所在服务器的metadata信息，包括获取ECS的uuid、availability_zone、project_id和enterprise_project_id信息。	-

2.16 如何使用镜像批量安装 Agent?

可通过已制作的私有镜像为新创建的服务器进行安装部署。

说明

已有的私有镜像不支持跨Region使用，跨Region使用会导致Agent状态显示未安装。

示例：在A区域制作的私有镜像部署在B区域，部署完成后B区域的Agent状态会显示为未安装，如果在A区进行部署，则Agent状态正常。

如果需跨Region使用，镜像安装完成后，您可先对原**Agent进行卸载**，清除原Agent信息，然后获取目标Region的安装命令执行**Agent安装**即可。

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**安装Windows版本客户端**。

说明

除在主机中安装HSS的Agent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 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**。

步骤5 使用**步骤4**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方式批量安装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**购买弹性云服务器**。

步骤2 在购买的弹性云服务器中安装HSS的Agent，详细操作请参见**安装Linux Agent**。

说明

除在主机中安装HSS的Agent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 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5 使用**步骤4**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

2.17 无法访问 Windows 或 Linux 版本 Agent 下载链接?

问题原因

Agent下载链接为华为云内网地址，因此在下载Agent前，您需要先为主机配置华为云内网DNS地址。如果没有配置华为云内网DNS地址，主机将访问不了下载链接。

解决办法

重新配置正确的内网DNS地址，主机域名使用**华为云提供的内网DNS地址**进行解析后，访问对应系统版本的Agent下载链接，重新安装Agent。

2.18 升级 Agent 失败，提示“替换文件失败”怎么处理?

问题现象

在主机安全服务控制台“安装与配置 > Agent管理”页面，升级Agent后，Agent升级状态显示“升级失败”，鼠标滑动至升级失败文字处查看到提示“替换文件失败”。

解决办法

主机安全服务Agent 3.2.4及以下版本不能平滑升级至新版本，因此您需要手动卸载3.2.4及以下版本Agent，再重新安装新版本Agent，详细操作请参考：

1. **卸载Agent**。
2. **安装Agent**。

2.19 批量安装 Agent 失败，提示“网络不通”怎么处理?

问题现象

在主机安全服务控制台“主机管理 > 云服务器”页面，通过账号密码的方式批量为主机安装Agent失败，失败原因提示“网络不通访问超时”。

解决办法

1. 确认主机状态是否为“运行中”。
   - 是：请执行**2**继续排查问题。
   - 否：主机状态为“运行中”时，才能执行Agent安装，请排查主机状态确认主机恢复运行后重试安装。
2. 确认批量安装Agent的主机是否在同一个VPC下。
   - 是：请执行**3**继续排查问题。
   - 否：通过账号密码一键批量安装Agent的安装方法仅适用于为同一个VPC下的主机进行安装。您可以参考**通过安装命令批量安装Agent**进行批量安装。
3. 确认批量安装Agent的主机账号密码是否相同。
   - 是：请执行**4**继续排查问题。

- 否：通过账号密码一键批量安装Agent的安装方法仅适用于为账号密码相同的主机进行安装。您可以参考**通过安装命令批量安装Agent**进行批量安装。

4. 执行以下命令，确认主机安全组出方向是否放通100.125.0.0/16网段的10180端口。

   curl -kv https://hss-agent.区域代码.myhuaweicloud.com:10180

   命令中的区域代码，每个区域不同，各区域代码请参见**地区和终端节点**。

   以“华北-北京一”为例，完整命令示例：curl -kv https://hss-agent.cn-north-1.myhuaweicloud.com:10180

   - 已放通：ping命令执行正常，表示已放通100.125.0.0/16网段的10180端口，请执行**5**继续排查问题。
   - 未放通：ping命令执行后，界面卡住不动，表示未放通100.125.0.0/16网段的10180端口，请参见**添加安全组规则**放通该端口。

5. 执行以下命令，确认主机DNS能否正常解析下载Agent的域名。

   ping -c 1 hss-agent.区域代码.myhuaweicloud.com

   命令中的区域代码，每个区域不同，各区域代码请参见**地区和终端节点**。

   以“华北-北京一”为例，完整命令示例：ping -c 1 hss-agent.cn-north-1.myhuaweicloud.com

   - 解析成功：界面回显解析出的IP，表示DNS解析正常，请执行**6**继续排查问题。
   - 解析失败：界面回显“name or service not known”或未解析出IP，表示DNS解析失败。请执行以下操作修改DNS服务器。

     i. 执行以下命令打开resolv.conf文件。

     vi /etc/resolv.conf

     ii. 在文件中添加华为云内网DNS地址，DNS地址请参见**华为云的内网DNS**。

     例如，华北-北京一的DNS地址为100.125.1.250和100.125.21.250，则在文件中添加“nameserver 100.125.1.250”和“nameserver 100.125.21.250”。

     iii. 输入**wq**，并按Enter键，保存。

6. 执行以下命令，确认主机能否获取元数据。

   curl http://169.254.169.254/openstack/latest/meta_data.json

   - 如果界面有返回值，表示可获取元数据，请执行**7**继续排查问题。
   - 如果界面无返回值或卡住不动，请参考**Linux服务无法获取元数据怎么办?**解决无法获取元数据问题。

7. 确认主机安全组入方向是否禁用ICPM命令。

   使用另一台主机ping需要安装Agent的主机IP，不能ping通，表示安全组入方向禁用了ICMP命令，请参见**添加安全组规则**放通ICMP命令。

3 账户暴力破解问题

3.1 HSS 如何拦截暴力破解?

可检测的暴力破解攻击类型

HSS可检测到的暴力破解攻击类型如下：

- Windows系统： SqlServer(暂不支持自动拦截) 、Rdp
- Linux系统：MySQL、vfstp、ssh

如果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3-1所示。

图 3-1 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，如果删除iptables规则，HSS将无法防护MySQL/vsftp被暴力破解。

暴力破解拦截原理

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

通过暴力破解检测算法和全网IP黑名单，如果发现暴力破解主机的行为，HSS会对发起攻击的源IP进行拦截，默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。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账号的破解行为。

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）的主机，在遭受SSH账户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警；SSH登录IP白名单功能也对其不生效。

告警策略

- 如果黑客暴力破解密码成功，且成功登录您的服务器，会立即发送实时告警通知用户。
- 如果检测到暴力破解攻击并且评估认为账户存在被破解的风险，会立即发送实时告警通知用户。
- 如果该次暴力破解没有成功，主机上也没有已知风险项（不存在弱口令），评估认为账户没有被破解的风险时，不会发送实时告警。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。您也可以登录主机安全服务控制台“入侵检测 > 安全告警事件”页面实时查看拦截信息。

查看暴力破解检测结果

步骤1 **登录管理控制台**。

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

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

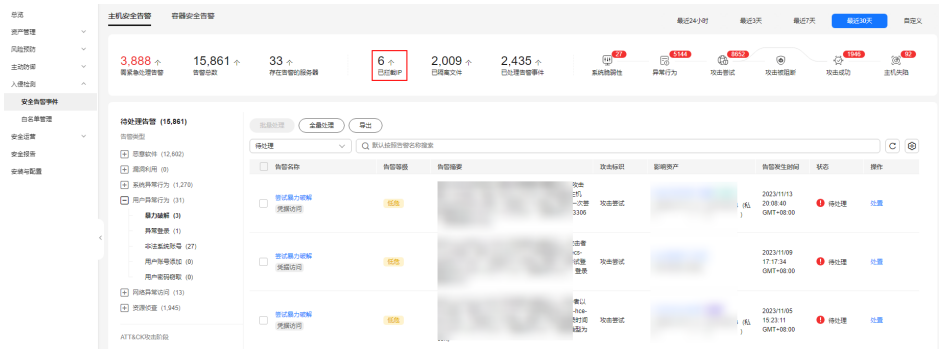
步骤4 选择查看主机或容器的暴力破解检测结果。

- 查看主机的暴力破解检测结果
  a. 选择主机告警事件页签，进入主机告警事件页面。
  b. 在左侧类型栏，选择“用户异常行为 > 暴力破解”，查看防护的主机上的暴力破解告警事件记录。
  c. 单击已拦截IP区域的数值，可查看已拦截的攻击源IP、攻击类型、拦截状态、拦截次数、开始拦截时间和最近拦截时间。
     - 已拦截：表示该暴力破解行为已被HSS成功拦截。
     - 已解除：表示您已解除对该暴力破解行为的拦截。

       说明

       默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。

图 3-2 暴力破解



- 查看容器的暴力破解检测结果
  a. 选择容器告警事件页签，进入容器告警事件页面。
  b. 在左侧类型栏，选择“用户异常行为 > 暴力破解”，查看防护的容器上的暴力破解告警事件记录。

----结束

处理拦截 IP

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

  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

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

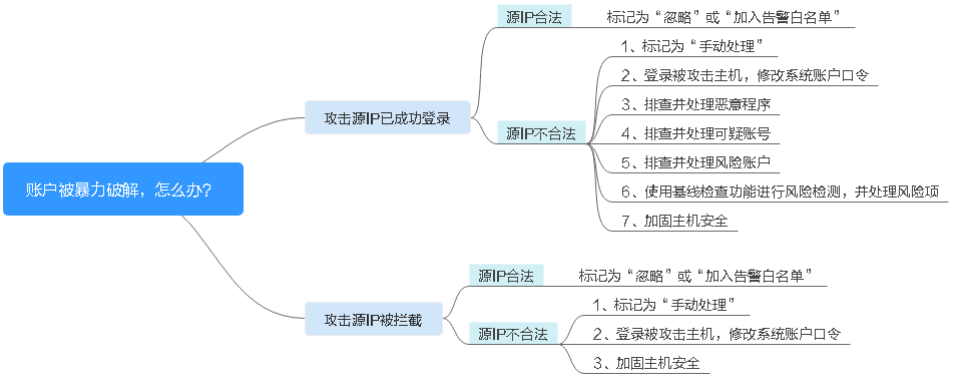
3.2 账户被暴力破解，怎么办？

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

排查思路

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

图 3-3 排查思路



账户被暴力破解，攻击源 IP 已成功登录

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

步骤1 登录管理控制台。

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

步骤3 **判断源IP的合法性。**

1. 在左侧导航栏选择“入侵检测 > 安全告警事件”页面，进入安全告警事件页面。
2. 在事件类型栏选择“用户异常行为 > 异常登录”，筛选异常登录告警事件。
3. 单击告警事件名称，弹出告警事件详情页面，查看成功登录主机的源IP是否为合法IP。
   - 如果源IP合法（多次输错口令，但未达到拦截IP条件，成功登录），您可以单击“处理”，忽略该事件。
   - 如果源IP不合法，是未知IP，那么您主机系统已经被入侵成功。

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

图 3-4 异常登录

步骤4 **排查并处理恶意程序。**

1. 在左侧导航栏选择“入侵检测 > 安全告警事件”页面，进入安全告警事件页面。

2. 在左侧类型栏选择“恶意软件 > 未分类恶意程序”，筛选未分类恶意程序告警事件。
3. 选择查看告警名称为“恶意程序”的告警事件，排查系统是否被植入了恶意程序。

   单击告警名称，可查看告警事件详细信息。

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

     针对恶意程序，在目标恶意程序告警事件所在行的“操作”列，单击“处理”，选择“隔离查杀”，立即终止恶意程序进程。
   - 如果没有被植入恶意程序，请执行**步骤8**。

步骤5 排查账号可疑变动记录。

1. 在左侧导航栏选择“资产管理 > 主机指纹”，进入主机指纹页面。
2. 排查系统中账号的变动记录是否可疑，防止攻击者创建新的账户或更改账户权限（例如：将某个原来不具备登录权限的账户修改为具备登录权限），详细信息请参见**账号信息管理**。

步骤6 排查并处理非法账号。

1. 在左侧导航栏选择“入侵检测 > 安全告警事件”，进入安全告警事件页面。
2. 在左侧类型栏选择“用户异常行为 > 非法系统账号”，查看所有非法账号的告警，对告警信息进行处理，详细信息请参见**处理非法系统账号**。

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**。

----结束

账户被尝试破解，攻击源 IP 被拦截

如果您为主机开启了HSS基础版以上（不含基础版）防护，HSS会为您的主机提供暴力破解防护。

您可以通过配置登录安全检测策略限定暴力破解的判断方式和封禁时间，详细操作请参见**配置登录检测策略**。

如果您未配置过登录安全检测策略，登录安全检测策略默认为：如果30秒内，账户暴力破解次数达到5次及以上，或者3600秒内，账户暴力破解次数达到15次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因账户破解被入侵。

如果您收到了攻击源IP被拦截的告警，请及时确认该源IP是否为可信IP。

约束与限制

- Linux操作系统

  使用鲲鹏计算EulerOS（EulerOS with ARM）的主机，在遭受SSH账户破解攻击时，HSS不会对攻击IP进行拦截，仅支持对攻击行为进行告警。
- Windows操作系统

- 开启主机防护时，需要授权开启Windows防火墙，且使用主机安全服务期间请勿关闭Windows防火墙。如果关闭Windows防火墙，HSS无法拦截账户暴力破解的攻击源IP。
- 通过手动开启Windows防火墙，也可能导致HSS不能拦截账户暴力破解的攻击源IP。

操作步骤

步骤1 登录管理控制台。

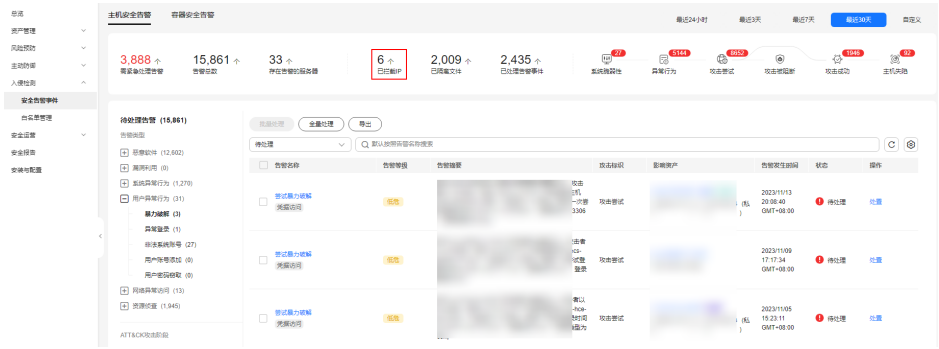
步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。

步骤3 选择“入侵检测 > 安全告警事件”，选择“暴力破解”，查看账户暴力破解事件。

出现账户暴力破解告警事件，说明您的主机可能存在被暴力破解风险。

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

图 3-5 暴力破解



步骤4 建议您立即确认源IP是否是已知的合法IP。

- 如果源IP合法。
  - 选择账户暴力破解事件，单击“处理”，并标记为“忽略””或者“加入登录告警白名单”。

    将该事件“忽略”或者“加入登录告警白名单”，均不会解除拦截的IP。
  - 如果需要解除拦截的IP，请单击“已拦截IP”，立即解除拦截的IP，或者当HSS检测到超过默认拦截时间后，主机不再被暴力破解攻击，将会自动解除拦截。默认拦截时间为12小时。
- 如果源IP不合法，是未知IP。

  请选择发生的账户暴力破解事件，单击“处理”，并标记为“手动处理””。

  立即登录主机系统，修改并设置安全的账户密码，并加固您的主机安全。

----结束

相关问题

- HSS如何拦截暴力破解?
- 如何手动解除误拦截IP?

3.3 如何预防账户暴力破解攻击?

账户破解风险

一旦主机账户被破解，入侵者就拥有了对主机的操作权限，主机上的数据将面临被窃取或被篡改的风险，企业的业务会中断，造成重大损失。

如何预防

- **配置SSH登录白名单**

  SSH登录白名单功能是防护账户破解的一个重要方式，配置后，只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。详细操作请参见**配置SSH登录IP白名单**。

- **开启双因子认证**

  双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次身份认证。

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

- **修改默认端口**

  将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。

- **设置安全组规则，限制攻击源IP访问您的服务端口**

  说明

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

  您可以通过**配置安全组规则**来限制攻击源IP访问您的服务端口。如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。

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

  表 3-1 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账户，您可以在控制台查看并处理主机中的口令风险。

3.4 如何解决部分 Linux 系统的账户破解防护功能未生效的问题?

故障原因

主机系统中SSHD服务没有依赖libwrap.so。

说明

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

解决方法

登录云服务器安装主机安全服务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）

3.5 如何手动解除误拦截 IP?

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

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

说明

- 默认拦截时间为12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 > 主机安全服务”，进入主机安全平台界面。

步骤3 在左侧导航树中，选择“入侵检测 > 安全告警事件 > 主机安全告警”。

步骤4 在安全告警统计栏，单击“已拦截IP”。

图 3-6 已拦截 IP

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

----结束

3.6 频繁收到 HSS 暴力破解告警如何处理?

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

频繁被暴力破解的可能原因

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

处理办法

您可通过以下方式来改善被频繁暴破攻击的情况，降低风险：

- **配置SSH登录白名单**

  SSH登录白名单功能是防护账户破解的一个重要方式，配置后，只允许白名单内的IP登录到服务器，拒绝白名单以外的IP。详细操作请参见**配置SSH登录IP白名单**。

- **开启双因子认证**

  双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次身份认证。

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

- **修改默认端口**

  将默认的远程管理端口“22”、“3389”修改为不易猜测的其他端口。

- **设置安全组规则，限制攻击源IP访问您的服务端口**

  说明

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

  您可以通过**配置安全组规则**来限制攻击源IP访问您的服务端口。如果是远程登录端口，您可以只允许特定的IP地址远程登录到弹性云服务器。

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

表 3-2 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账户，您可以在控制台查看并处理主机中的口令风险。

HSS 如何拦截暴力破解?

HSS支持检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击。

默认情况下，如果30秒内，账户暴力破解次数达到5次及以上，或者3600秒内，账户暴力破解次数达到15次及以上，HSS就会拦截该源IP，禁止其再次登录，防止主机因账户破解被入侵。

如果您为主机开启了HSS基础版以上（不含基础版）防护，您可以通过配置登录安全检测策略限定暴力破解的判断方式和封禁时间，详细操作请参见**配置登录检测策略**。

HSS拦截的IP可在控制台“入侵检测 > 安全告警事件”页面，单击“已拦截IP”上方的数值进行查看。

3.7 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**。

3.8 服务器远程端口已修改，为什么暴力破解记录仍显示旧端口?

问题描述

服务器远程端口已修改，但是暴力破解告警记录中的服务器远程端口仍显示为旧端口。

解决方案

主机安全服务的Agent在启动时才会读取服务器远程端口配置，如果您修改了服务器远程端口，请按如下方式重启Agent。

- Windows：以administrator权限登录主机，在任务管理器中，选中“HostGuard”，单击鼠标右键，选择“重新启动”。
- Linux：以root权限执行**service hostguard restart**命令。

4 弱口令和风险账号问题

4.1 出现弱口令告警，怎么办？

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

出现弱口令告警的原因

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

排查弱口令

步骤1 登录管理控制台。

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

步骤3 选择“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 4-1 经典弱口令

步骤4 根据经典弱口令列表中的“服务器名称/IP地址”、“账号名称”、“账号类型”和“弱口令使用时长（单位：天）”，登录待修改弱口令的主机，修改弱口令。

----结束

修改常见的服务器弱口令

系统名称	修改登录口令	说明
Windows系统	以Windows 10为例说明。 1. 登录Windows主机系统。 2. 单击左下角的  ，然后单击  ，弹出“Windows设置”窗口。 3. 在“Windows设置”窗口中，单击“账户”。 4. 在左侧导航栏中，单击登录选项。 5. 在“登录选项”页面，请根据页面提示信息修改服务器密码。	无
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 **passwd [<user>]**	如果不输入登录用户名，则修改的是当前用户的口令。 命令执行完成后，请根据提示输入新的口令。 **说明** “user”为登录用户名。
MySQL数据库	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 **SELECT user, host, authentication_string From user;** 部分MySQL数据库版本可能不支持以上查询命令。 如果执行以上命令没有获取到用户密码信息，请执行命令。 **SELECT user, host password From user;** 3. 执行以下命令，根据查询结果及弱密码告警信息，修改具体用户的密码。 **SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');** 4. 执行以下命令，刷新修改的密码信息。 **flush privileges;**	无
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 **requirepass <password>;**	● 如果已存在登录口令，则将其修改为复杂口令。 ● 如果不存在登录口令，则添加为新口令。 **说明** “password”为登录口令。

系统名称	修改登录口令	说明
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

4.2 如何设置安全的口令?

请按如下建议设置口令：

- 使用复杂度高的密码。

  建议密码复杂度至少满足如下要求：

  a. 密码长度至少8个字符。

  b. 包含如下至少三种组合：

  i. 大写字母（A~Z）

  ii. 小写字母（a~z）

  iii. 数字（0~9）

  iv. 特殊字符

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

4.3 关闭弱口令策略后，之前扫描的弱口令事件为什么还会重复出现?

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

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

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

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

5 入侵告警问题

5.1 收到 HSS 的告警通知，如何查找到相关信息并处理?

如何查看

主机安全告警查看操作详情请参见**查看主机安全告警**，容器安全告警查看操作详情请参见**查看容器安全告警事件**。

如何处理

主机安全服务提供漏洞修复方法、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**处理主机安全告警**。

容器安全提供对告警的处理，操作详情请参见**处理容器告警事件**。

5.2 主机被挖矿攻击，怎么办?

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

当主机提示有挖矿行为时，请确定并清除挖矿程序，并及时对主机进行安全加固。

排查操作步骤

步骤1 **登录管理控制台**。

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

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

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

图 5-1 处理进程异常行为

步骤4 排查其他自启动项，有的挖矿进程为了实现长期驻留，会向系统中添加自启动项来确保系统重启后仍然能重新启动，因此，需要及时清除可疑的自启动项。

选择“资产管理 > 主机指纹”，单击“自启动项”，选择“历史变动记录”，查看历史变动情况。

----结束

主机安全加固

挖矿程序清除后，为了保障主机安全，请及时对主机进行安全加固。

Linux加固建议

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

- **账户安全加固**

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

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

- **口令安全加固**

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

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

- **授权安全加固**

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

5.3 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”页面中，开启自动隔离查杀。
- 方式二：在“入侵检测 > 安全告警事件 > 主机安全告警 > 事件列表”中，将恶意程序手动隔离查杀。

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

恢复隔离查杀文件

1. 在“入侵检测 > 安全告警事件 > 主机告警事件”页面中，单击“已隔离文件”区域的数值，弹出“已隔离文件”页面。
2. 在目标服务器的所在行的“操作”列，单击“恢复”，弹出恢复确认对话框。
3. 单击“确认”，恢复隔离文件。

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

5.4 提示主机有挖矿行为怎么办?

当主机提示有挖矿行为时：

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

5.5 服务器遭受攻击为什么没有检测出来?

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

5.6 源 IP 被 HSS 拦截后，如何解除?

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

账户暴力破解

- 如果发现暴力破解主机的行为，HSS会对发起攻击的源IP进行拦截，默认拦截时间为12小时。**如果被拦截的IP在默认拦截时间内没有再继续攻击，系统自动解除拦截**。
- 如果您确认源IP是可信的IP（比如运维人员因为记错密码，多次输错密码导致被封禁），可单击“入侵检测 > 安全告警事件”页面下“已拦截IP”的“查看详情”，在弹出的页面，可手动解除被拦截的可信IP。

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

全网 IP 黑名单

不能手动解除拦截。

开启 SSH 登录 IP 白名单

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

5.7 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12小时内没有再继续暴力破解就会自动解除IP。

5.8 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。

5.9 HSS 的病毒库、漏洞库多久更新一次?

更新周期：

- 漏洞库：正常情况下每月更新一次，如果有重大紧急漏洞会立即更新。

- 病毒库：正常情况下每天更新一次。

更新日期：漏洞库和病毒库更新的具体日期，您可以在HSS管理控制台的“总览 > 防护地图”区域查看。

5.10 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。

5.11 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**预防账户暴力破解攻击的措施**，及时对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。

5.12 HSS 由旧版升级为新版后不告警了，怎么办?

新旧版HSS的告警通知功能独立生效，新版HSS的告警通知功能默认为关闭状态，不会继承旧版设置，因此不会向您发送告警通知。您需要在新版HSS控制台重新手动开启告警通知，详细操作请参见**开启告警通知**。

5.13 高危命令执行告警，如何添加白名单?

如果您在服务器上执行了正常业务相关命令，HSS进行“高危命令执行”告警，您可以添加白名单，避免告警。

添加命令告警白名单方式如下：

1. **登录管理控制台**。
2. 在页面左上角选择“区域”，单击，选择“安全与合规 > 主机安全服务”，进入主机安全平台界面。
3. 在左侧导航树中选择“安全运营 > 策略管理”，进入“策略管理”页面。
4. 找到服务器对应防护版本的策略组，单击策略组名称，进入策略组管理页面。
5. 单击“实时进程”策略名称。
6. 添加命令白名单。参数说明如下：
   - 进程全路径或程序名：填写进程的全路径或者程序名称，例如/usr/bin/sleep或sleep。
   - 命令行正则表达式：填写需要加白的命令行的正则表达式，例如^[A-Za-z0-9[:space:]*\\.\\\":_'\\(>=-]+$

图 5-2 添加白名单

7. 单击“确认”，保存修改。

6 异常登录问题

6.1 添加登录白名单后，为什么还有异地登录告警?

HSS提供的“SSH登录IP白名单”、“登录告警白名单”和“异地登录”功能，功能差异如表6-1所示。

表 6-1 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。	-
登录告警白名单	将IP加入登录告警白名单，用于忽略由该IP登录指定主机发生的账户暴力破解告警事件。	在“入侵检测 > 白名单管理 > 登录告警白名单”将IP加入登录告警白名单，HSS将不会对该IP的“账户暴力破解”登录事件进行告警。
异地登录	当不是来自“常用登录地”或者“常用登录IP”的登录行为时，将会进行异地登录告警。 提醒您有新的IP登录您的主机。	在“安装与配置 > 安全配置”中，将登录地与登录IP添加到“常用登录地”与“常用登录IP”，HSS将不会对来自“常用登录地”和“常用登录IP”的登录行为进行异地告警。

6.2 如何查看异地登录的源 IP?

告警策略

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

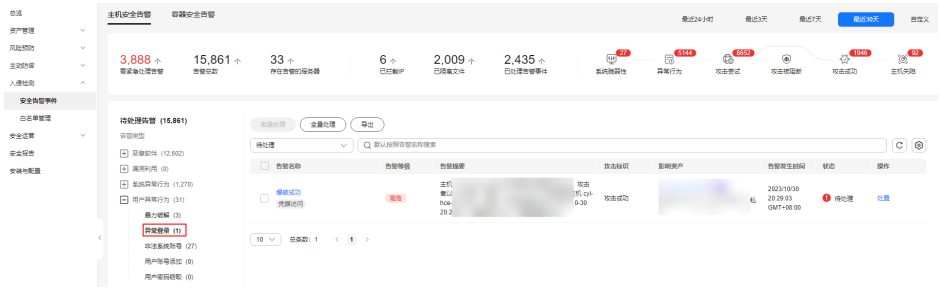
在控制台查看异地登录记录

步骤1 **登录管理控制台**。

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

步骤3 如**图 异常登录**所示查看“异常登录”，单击告警名称“异地登录”查看详情。

图 6-1 异常登录



----结束

本地查看登录记录

- Linux主机

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

- Windows主机

  您可以参考以下步骤查看主机登录日志：

  a. 打开“控制面板”。
  b. 选择“管理工具 > 事件查看器”，进入“事件查看器”页面。
  c. 在左侧导航栏选择“Windows日志 > 安全”，进入“安全”页面。
  d. 在右侧导航栏选择“安全 > 筛选当前日志”，弹出“筛选当前日志”窗口。
  e. 在“筛选器”页签，找到“<所有事件ID>”。
  f. 输入登录事件ID并单击“确认”，筛选需要查看的目标登录事件。

     - 登录成功：4624
     - 登录失败：4625

6.3 收到主机登录成功的告警，怎么处理?

- 如果您在“实时告警通知”项目中勾选了“登录成功通知”选项，则任何账户登录成功的事件都会向您实时发送告警信息。
- 如果您所有ECS上的账户都由个别管理员负责管理，通过该功能可以对系统账户进行严格的监控。
- 如果系统账户由多人管理，或者不同主机由不同管理员负责管理，那么运维人员可能会因为频繁收到不相关的告警而对运维工作造成困扰，此时建议您登录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。

6.4 是否可以关闭异地登录检测?

不可以关闭异地登录检测。

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

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

  图 6-2 添加常用登录地

- 在“安装与配置 > 告警通知”页签，在屏蔽事件中勾选“异常登录”。

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

图 6-3 屏蔽异常登录

6.5 如何确认入侵账号是否登录成功?

- 如果已开启入侵检测告警通知，当有账号被破解，或有账号破解风险时，您会立即收到告警通知。
- 也可以在“入侵检测”页面在线查看攻击IP的拦截情况。
- 如果想进一步确定，请参考如下方式：
  - Linux主机

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

    您可以参考以下步骤查看主机登录日志：

    i. 打开“控制面板”。

    ii. 选择“管理工具 > 事件查看器”，进入“事件查看器”页面。

    iii. 在左侧导航栏选择“Windows日志 > 安全”，进入“安全”页面。

    iv. 在右侧导航栏选择“安全 > 筛选当前日志”，弹出“筛选当前日志”窗口。

    v. 在“筛选器”页签，找到“<所有事件ID>”。

    vi. 输入登录事件ID并单击“确认”，筛选需要查看的目标登录事件。

    - 登录成功：4624
    - 登录失败：4625

7 配置风险问题

7.1 如何在 Linux 主机上安装 PAM 并设置口令复杂度策略?

安装 PAM

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

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

说明

CentOS、Fedora、EulerOS系统默认安装了PAM并默认启动。

设置口令复杂度策略

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

说明

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

- 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统
  man pam_pwquality
- 其他Linux系统
  man pam_cracklib

- CentOS、Fedora、EulerOS操作系统
  a. 执行以下命令，编辑文件“/etc/pam.d/system-auth”。
     vi /etc/pam.d/system-auth
  b. 找到文件中的以下内容。
     - 基于Red Hat 7.0的CentOS、Fedora、EulerOS系统：
       password requisite pam_pwquality.so try_first_pass retry=3 type=

- 其他CentOS、Fedora、EulerOS系统：

  password requisite pam_cracklib.so try_first_pass retry=3 type=

c. 添加参数“minlen”、“dcredit”、“ucredit”、“lcredit”、“ocredit”。如果文件中已有这些参数，直接修改参数值即可，参数说明如表7-1所示。

示例：

password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 type=

说明

“dcredit”、“ucredit”、“lcredit”、“ocredit”中均需要配置为负数。

表 7-1 参数说明

参数	说明	示例
minlen	口令最小长度配置项。 如果需要设置最小口令长度为8，则minlen的值应该设置为8。	minlen=8
dcredit	口令数字要求的配置项。 值为负数N时表示至少有N个数字，值为正数时对数字个数没有限制。	dcredit=-1
ucredit	口令大写字母要求的配置项。 值为负数N时表示至少有N个大写字母，值为正数时对大写字母个数没有限制。	ucredit=-1
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7-1所示。

示例：

password requisite pam_cracklib.so retry=3 minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 difok=3

7.2 如何在 Windows 主机上设置口令复杂度策略?

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

设置本地安全策略中的账户策略步骤如下：

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

说明

- 也可直接在开始菜单栏输入命令**secpol.msc**直接进入本地安全策略控制面板。
- 当策略应用于服务器时，域策略优先生效于服务器上本地定义的策略。

步骤2 选择“账户策略 > 密码策略”后执行以下操作。

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

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

----结束

7.3 如何处理配置风险?

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，选择“基线检查 > 配置检查”。

  b. 单击目标风险项前的 展开检查项，单击目标风险项“操作”列的“忽略”进行单个忽略。也可以勾选多个检测规则单击界面上方的“忽略”进行批量忽略。

图 7-1 忽略配置风险

对于已经忽略的检测规则，单击已忽略页签可“取消忽略”，也可以批量选中想要取消忽略的规则“取消忽略”。

图 7-2 取消忽略

- 修复验证

  完成配置项的修复后，建议您在“风险预防 > 漏洞管理”页面单击“漏洞检测”立即执行手动检测，查看配置项修复结果。

7.4 如何查看配置检查的报告?

支持在线查看配置检查的检测详情。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“风险预防 > 基线检查”，进入“基线检查”页面。

步骤4 在“配置检查”页签，单击配置检查基线名称，进入检测规则详情页面。

步骤5 在目标检查项所在行的“操作”列，单击“检测详情”，查看检查项详细信息和受影响服务器。

图 7-3 检测详情

步骤6 您可以根据检查项的描述信息和修改建议，修复主机中含有风险的配置项或忽略可信任的配置项。

----结束

8 漏洞管理

8.1 如何处理漏洞?

处理方法和步骤

步骤1 查看漏洞检测结果。

步骤2 按照漏洞检测结果给出的漏洞修复紧急度和解决方案逐个进行漏洞修复。

- 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 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验证，核实修复结果。

----结束

相关问题

如何处理配置风险?

8.2 漏洞修复后，为什么仍然提示漏洞存在?

在主机安全服务控制台上使用漏洞管理功能修复系统软件漏洞时，如果提示漏洞修复失败，请参见以下可能原因：

说明

建议您参考漏洞修复与验证章节对您服务器上的漏洞进行修复。

Linux 系统服务器

- **无yum源配置**

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

- **yum源没有相应软件的最新升级包**

切换到有相应软件包的yum源，配置完成后，重新执行漏洞修复操作。

- **内网环境连接不上公网**

  在线修复漏洞时，需要连接Internet，通过外部yum源提供漏洞修复服务。如果服务器无法访问Internet，或者外部yum源提供的服务不稳定时，可以使用华为云提供的**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，您可以在主机安全服务管理控制台的“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 8-1 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**

- **内核漏洞修复后，未重启主机**

  内核漏洞修复完成后，需要重启主机，不重启主机漏洞仍会显示存在。

8.3 漏洞管理显示的主机不存在?

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

8.4 漏洞修复完毕后是否需要重启主机?

“Windows系统漏洞”和“Linux系统Kernel类的漏洞”修复完成后，需要重启服务器，重启服务器后漏洞修复才会生效，否则主机安全服务仍认为您的漏洞未完成修复，将持续为您告警。其他类型的漏洞修复后，则无需重启服务器

8.5 HSS 如何查询漏洞、基线已修复记录?

查看已修复漏洞

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中选择“风险预防 > 漏洞管理”，进入“漏洞管理”页面

步骤4 在各类漏洞页签，筛选查看已修复的漏洞。

须知

漏洞仅在漏洞列表保留展示七天，因此您只能查看最近七天已修复的漏洞。

图 8-1 筛选已修复漏洞

----结束

查看已修复基线

口令复杂度策略、经典弱口令风险项修复后，不支持查看历史修复记录。您可以参考本小节查看已修复的配置检查项。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中选择“风险预防 > 基线检查”，进入“基线检查”页面

步骤4 选择“配置检查”页签。

步骤5 单击基线名称，进入基线详情页。

步骤6 选择“检查项 > 已通过”页签，查看已修复的检查项。

----结束

8.6 漏洞修复失败怎么办?

如果在主机安全服务控制台修复Linux和Windows系统漏洞时失败，请参考本文进行排查处理。

查看漏洞修复失败原因

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

说明

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

步骤4 在“漏洞管理”界面右上角，单击“任务管理”，进入任务管理页面。

步骤5 选择“修复任务”页签，查看漏洞修复结果。

- ：该图标旁显示的数字，表示修复成功的服务器数量。
- ：该图标旁显示的数字，表示修复失败的服务器数量。

步骤6 单击图标，在修复失败详情对话框中，查看修复失败的“失败原因”和“原因说明”。

您可以根据失败原因，参考**Linux漏洞修复失败原因及解决方法**、**Windows漏洞修复失败原因及解决方法**处理漏洞修复失败问题。

----结束

Linux 漏洞修复失败原因及解决方法

须知

- CCE 、MRS、BMS的主机不能修复内核漏洞，贸然修复可能导致功能不可用。
- Kernel类的漏洞修复完成后，需要重启主机，不重启主机漏洞仍会显示存在。
- 失败原因只截取了部分关键字段，具体信息请以主机安全服务控制台显示为准。

失败原因	原因说明	解决办法
timeout	修复超时	请等待1小时后重试修复漏洞。如果仍然修复超时，请您在华为云管理控制台的右上角，单击“工单 > 新建工单”，通过工单向技术人员寻求帮助。
This agent version does not support vulnerability verification	Agent版本太低	服务器安装的Agent版本过低，请**升级Agent**后进行漏洞修复。
Agent status is not normal	Agent状态异常	Agent已离线，无法完成漏洞修复。请参考**Agent状态异常应如何处理?** 使Agent状态恢复正常后，进行漏洞修复。

失败原因	原因说明	解决办法

Error: software have multiple versions	存在漏洞的软件版本未删除	• 如果是普通软件出现此问题，可以删除旧版本包，重新检测漏洞是否存在。
		执行以下命令测试删除旧版本包有无报错。
		`rpm -e --test XXX`
		说明
		“XXX”表示软件带版本号的完整组件名，可通过**rpm -qa**命令查询完整组件名。
		– 删除有报错：表示有软件包依赖，不可删除，建议您忽略该漏洞。
		– 删除无报错：可执行以下命令删除旧版本包。
		`rpm -e XXX`
		• 如果是Kernel、Glibc等内核相关组件出现此问题，删除旧版本包可能会引起操作系统问题，建议您忽略该漏洞。

No package marked for update Error: software info not update Error: kernel is not update is already the newest version Dependencies resolved. Nothing to do. Complete!	未找到新版本升级包	失败原因表示软件已经升级为当前镜像源支持的最高版本，但漏洞仍然存在。 **说明** • CentOS 6和CentOS 8官方已停止维护，HSS使用Redhat的补丁公告替代检测，由于官方不出补丁所以无法修复，建议您切换其他操作系统。 • Ubuntu 18.04及以下版本目前已不支持免费补丁更新，需要购买配置Ubuntu Pro才能安装升级包。 • 可能原因一：镜像源配置错误。 请**配置镜像源**，更新镜像源后，重新修复漏洞。 • 可能原因二：主机禁止内核漏洞修复。 修复内核漏洞可能导致功能不可用，如需修复内核漏洞，请您在华为云管理控制台的右上角，单击“工单 > 新建工单”，通过工单向技术人员寻求帮助，。 **须知** CCE 、MRS、BMS的主机不能修复内核漏洞，贸然修复可能导致功能不可用，请勿升级内核组件。
Error: Failed to download metadata for repo One of the configured repositories failed Errors during downloading metadata for repository	无法连接到yum源	请确认主机所属Region是否在：华北-北京一、华北-北京四、华东-上海一、华东-上海二、华南-广州、中国-香港。 • 是：如果主机因特殊原因无法连接外网，您可以配置华为云提供的镜像源解决问题，详细操作请参见**使用自动化工具配置华为云镜像源**。 • 否：请保证主机可正常访问外网，否则无法连接官方镜像源或其他源。如果主机能正常访问外网，但找不到可用源，您可以配置**华为云的开源镜像源**。

失败原因	原因说明	解决办法
Error: Cannot retrieve repository metadata		
Failed connect to		
E: Failed to fetch		
Error: kernel is not update	内核未更新	• 可能原因一：漏洞修复后未重启。 解决办法：重启主机。kernel漏洞修复后，需要重启主机才会生效，否则下次漏洞扫描时仍判定该漏洞未修复。 • 可能原因二：主机禁止内核漏洞修复。 修复内核漏洞可能导致功能不可用，如需修复内核漏洞，请您在华为云管理控制台的右上角，单击“工单 > 新建工单”，通过工单向技术人员寻求帮助，。
Error: kernel info not update		
Please install a package which provides this module, or verify that the module is installed correctly	yum命令不可用	请根据失败原因中提示的方法，修复命令不可用问题。
command not found		
Error downloading packages	下载升级包失败	请确认主机是否可正常连接外网： • 是：镜像源配置错误，请参考**配置镜像源**，更新镜像源后，重新修复漏洞。 • 否：请保证您的主机可以正常连接外网后，重新修复漏洞。
There are no enabled repositories	未配置可用的源	失败原因表示是镜像源配置错误，请参考**配置镜像源**，更新镜像源后，重新修复漏洞。
Error: Cannot find a valid baseurl for repo		
There are no enabled repos		
dpkg was interrupted	dpkg命令不可用	请根据失败原因中提示的方法，修复命令不可用问题。

Windows 漏洞修复失败原因及解决方法

须知

- Windows补丁安装后，需要重启主机，不重启主机会产生以下影响：
  - 补丁不生效。
  - 在安装其他系统补丁或软件时，可能会导致系统蓝屏、无法启动。
- 失败原因只截取了部分关键字段，具体信息请以主机安全服务控制台显示为准。

失败原因	原因说明	解决办法
timeout	修复超时	请等待1小时后重试修复漏洞。如果仍然修复超时，请您在华为云管理控制台的右上角，单击“工单 > 新建工单”，通过工单向技术人员寻求帮助。
Agent status is not normal	Agent状态异常	Agent已离线，无法完成漏洞修复。请参考**Agent状态异常应如何处理?** 使Agent状态恢复正常后，进行漏洞修复。
This agent version does not support vulnerability verification	Agent版本太低	主机安装的Agent版本过低，请**升级Agent**后进行漏洞修复。

Search patch failed: Search failed, errmsg(Unknown error 0x8024401C)	查找补丁失败	失败原因表示主机上系统的Windows Update组件出现问题。请按以下操作恢复Windows Update组件后，重新修复漏洞：
		1. 打开cmd命令提示符窗口。
		2. 逐一执行以下命令尝试恢复。
		`net stop wuauserv`
		`reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`
		`net start wuauserv`

失败原因	原因说明	解决办法
Search patch failed: Search failed, errmsg(Unknown error 0x8024402C)	查找补丁失败	失败原因表示Windows Update客户端无法连接到Windows更新服务器。请按以下方法尝试恢复Windows Update组件后，重新修复漏洞： 1. 检查主机网络连接是否正常。 请确保您的主机可以连接互联网。 2. 清除Windows Update缓存。 a. 打开控制面板。 b. 进入“系统和安全 > 管理工具 > 服务”。 c. 选中“Windows Update”服务，单击右键，选择“停止”。 d. 打开C:\Windows文件夹，找到并删除“SoftwareDistribution”文件。 e. 选中“Windows Update”服务，单击右键，选择“启动”。 3. 执行以下命令重置Windows Update组件。 net stop wuauserv net stop cryptSvc net stop bits net stop msiserver ren C:\Windows\SoftwareDistribution SoftwareDistribution.old ren C:\Windows\System32\catroot2 catroot2.old net start wuauserv net start cryptSvc net start bits net start msiserver
Search patch failed: Search failed, errmsg(Unknown error 0x80070422)	查找补丁失败	失败原因表示主机上的Windows Update服务被关闭。请按以下操作启动服务后，重新修复漏洞： 1. 打开控制面板。 2. 进入“系统和安全 > 管理工具 > 服务”。 3. 双击“Windows Update”服务。 4. 在“Windows Update的属性”窗口，选择启动类型为“自动”。 5. 单击“确定”。

<table>
<tr><th>失败原因</th><th>原因说明</th><th>解决办法</th></tr>
<tr><td>Search patch failed: Get updates count is 0</td><td>查找补丁失败</td><td rowspan="8">失败原因表示主机的Windows Update故障，请按以下步骤排查问题：
1. 检查主机网络连接是否正常。
● 是：执行步骤2。
● 否：待主机网络连接正常后，重新进行漏洞修复。
2. 打开Windows Update，确认检查更新是否能检查出待安装补丁。
● 是：安装补丁并重启主机。
● 否：
如果修复失败原因中含错误码，请根据错误码在微软官网搜索对应的解决方案。
如果修复失败原因中不含错误码，请参考微软官方提供的重置Windows Update文档，尝试重置Windows Update。</td></tr>
<tr><td>Search patch failed: Search failed,errmsg</td><td>查找补丁失败</td></tr>
<tr><td>Not install security patch</td><td>查找补丁失败</td></tr>
<tr><td>Add patch to update collection failed: Update collection count is 0</td><td>查找补丁失败</td></tr>
<tr><td>Not find patch</td><td>没有找到补丁</td></tr>
<tr><td>Add patch to update collection failed</td><td>安装补丁失败</td></tr>
<tr><td>Com init failed</td><td>调用Windows更新失败</td></tr>
<tr><td>Download patch failed</td><td>下载补丁失败</td><td>● 可能原因一：Windows Update配置问题；仅Windows2008、2012可能会出现此种问题。在主机控制面板中找到“Windows Update > 更改设置”，按如下配置：
– 重要更新：选择下载更新，但是让我选择是否安装更新。
– 推荐更新：勾选。
– Microsoft更新：去勾选。
配置完成后，打开Windows Update，单击“检查更新”，待检查出待安装补丁后，安装补丁并重启主机。
● 可能原因二：主机长时间未打补丁，导致Windows Update异常。
1. 登录主机并打开Windows Update。
2. 单击“检查更新”。
3. 检查出待安装补丁后，安装补丁并重启主机。
说明
此场景漏洞可能一次无法完全修复，请反复检查更新直至安装完所有补丁。</td></tr>
</table>

8.7 手动扫描漏洞或批量修复漏洞时，为什么选不到目标服务器?

问题原因

在手动扫描漏洞或批量修复漏洞时，以下服务器不能被选中执行漏洞扫描或修复操作：

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

解决办法

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“资产管理 > 主机管理”，进入“主机管理”页面。

步骤4 在“云服务器”页签，查看服务器的运行状态、Agent状态以及服务器使用的主机安全服务版本。

图 8-2 查看服务器信息

确认相关信息后，请参考如下方式处理问题：

- 使用主机安全服务“基础版”的服务器。

  主机安全服务基础版不支持手动扫描漏洞和修复漏洞功能，如果您需要使用手动扫描漏洞和修复漏洞功能或更多主机安全服务功能，您可以升级主机安全服务版本，详细操作请参考**升级防护配额版本**。
- 非“运行中”状态的服务器。

  请排查服务器状态，确保服务器状态为“运行中”。
- Agent状态为“离线”的服务器。

  Agent离线后，无法接收控制台下发的指令，请参考**Agent状态异常应如何处理?**，使Agent恢复为“在线”状态。

步骤5 在左侧导航栏选择“风险预防 > 漏洞管理”，进入漏洞管理页面，重新手动扫描漏洞或批量修复漏洞，目标服务器能勾选即表示问题解决。

----结束

9 网页防篡改常见问题

9.1 为什么要添加防护目录?

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

添加防护目录请参见**开启网页防篡改版**的添加防护目录。

9.2 如何修改防护目录?

步骤1 **登录管理控制台**。

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

步骤3 在左侧导航栏中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面。

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

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

说明

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

步骤6 在“编辑防护目录”弹框中进行修改，单击“确认”完成修改。

----结束

9.3 无法开启网页防篡改怎么办?

可能的原因及解决方法如下：

配额不足

- **现象**：
  所选区域内网页防篡改配额不足。

Agent 状态异常

- **现象**
  网页防篡改页面**防护列表**中“Agent状态”为“离线”或者“未安装”。
- **解决方法**
  请参见**Agent状态异常**进行处理，确保主机列表中“Agent状态”为“在线”。

开启了基础版/企业版/旗舰版防护

- **现象**
  主机安全服务页面**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 9-1 添加防护服务器

说明

购买主机安全服务“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。

9.4 开启网页防篡改后，如何修改文件?

开启防护后，防护目录中的内容是只读，如果您需要修改文件或更新网站：

临时关闭网页防篡改

请先临时关闭网页防篡改，完成修改或更新后再开启。

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

设置定时开关

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

定时关闭防护期间，文件存在被篡改的风险，请合理制定定时关闭的时间。

9.5 开启动态网页防篡改后，状态是“已开启未生效”，怎么办?

动态网页防篡改提供tomcat应用运行时的自我保护。

开启动态网页防篡改需要满足以下条件：

- 仅针对Tomcat应用。
- 主机是Linux操作系统。
- 开启动态网页防篡改后，请等待大约20分钟后检查“tomcat/bin”目录下是否已生成“setenv.sh”文件，如果已生成该文件，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。
- 如果“setenv.sh”文件已生成，请检查Tomcat是否重启。

9.6 HSS 与 WAF 的网页防篡改有什么区别?

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

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

网页防篡改的区别

HSS与WAF网页防篡改的区别，如表9-1所示。

表 9-1 HSS 和 WAF 网页防篡改的区别

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

类别	HSS	WAF
动态网页	提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为。	不支持
备份恢复	• 主动备份恢复 如果检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。 • 远端备份恢复 如果本地主机上的文件目录和备份目录失效，可通过远端备份服务恢复被篡改的网页。	不支持
防护对象	网站防护要求高，手动恢复篡改能力差	网站防护要求低，仅需要对应用层进行防护

如何选择网页防篡改

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

10 容器安全常见问题

10.1 如何关闭节点防护?

操作须知

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

操作步骤

步骤1 登录管理控制台。

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

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

说明

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

步骤4 在目标服务器所在行的“操作”列，单击“关闭防护”。

您也可以勾选多个目标服务器，并在列表上方单击“关闭防护”，批量关闭防护。

步骤5 在弹窗中确认关闭服务器的信息，确认无误，单击“确认”，防护关闭。

步骤6 关闭后在“资产管理 > 容器管理 > 容器节点管理”页面查看目标服务器的“容器防护状态”为“未防护”，关闭成功。

⚠ 注意

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

----结束

10.2 容器安全如何切换至主机安全服务控制台?

您可将原容器安全迁移至主机安全服务控制台实现服务器负载的统一管理，同时可享受新增的功能特性。

新版&旧版功能说明

目前容器安全服务已整合至主机安全服务控制台进行统一管理，优化了既有功能的能力，同时新增了部分新功能。

表 10-1 新版&旧版 CGS 功能说明

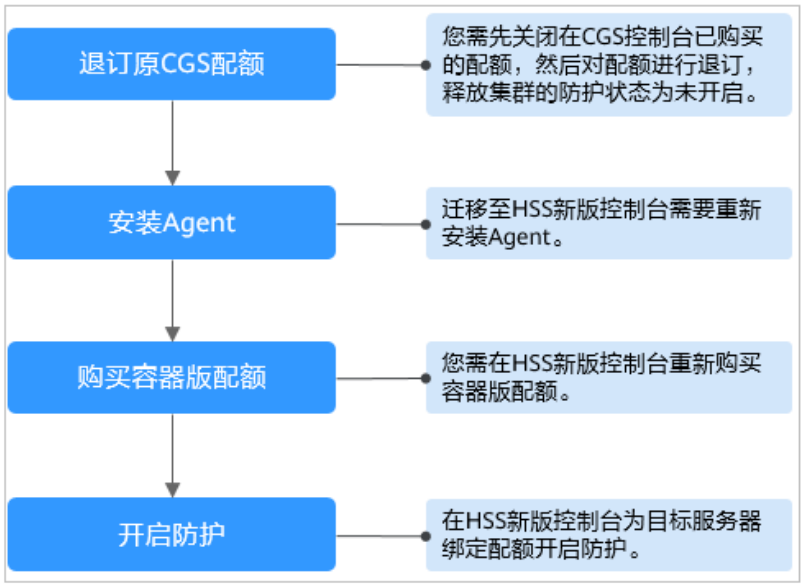
功能项	CGS旧版（原CGS）	CGS新版（HSS新版）
容器资产指纹管理	×	√
容器节点管理	√	√
私有镜像管理	√	√
本地镜像管理	√	√
官方镜像管理	√	×
共享镜像管理	×	√
镜像漏洞检测	√	√
镜像恶意文件检测	√	√
镜像基线检查	√	√
漏洞逃逸攻击	√	√
文件逃逸攻击	√	√
容器进程异常	√	√
容器配置异常	√	√
容器异常启动	√	√
容器恶意程序	√	√
高危系统调用	√	√
敏感文件访问	√	√
容器软件信息	√	√

功能项	CGS旧版（原CGS）	CGS新版（HSS新版）
容器文件信息	√	√
白名单管理	√	√
容器策略管理	√	√

切换流程

将CGS整体切换至HSS的过程需要您先关闭原CGS、再购买HSS容器版本并开启防护即可。

图 10-1 CGS 切换流程



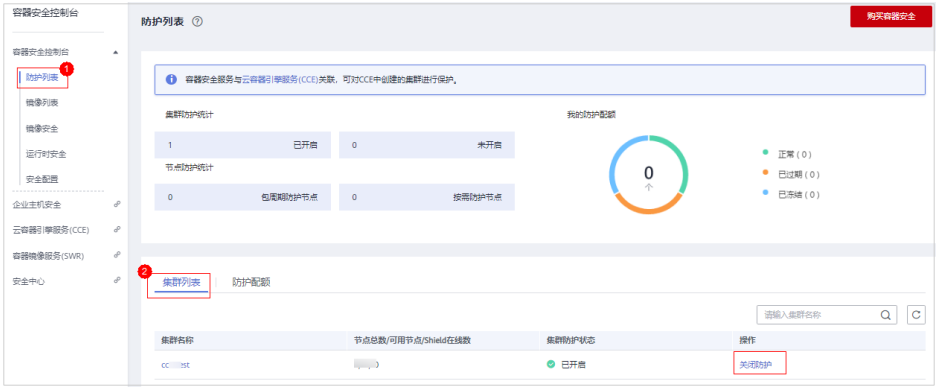
步骤一：关闭原 CGS 防护

步骤1 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 容器安全服务”，进入容器安全服务平台界面。

步骤3 进入容器安全“防护列表”，查看集群防护列表。

图 10-2 查看容器集群防护情况



步骤4 单击目标集群“操作”列的“关闭防护”，释放集群防护状态。

说明

为了方便管理，建议将所有集群的防护都进行关闭。

步骤5 全部关闭完成后，选择“防护配额”页签，在所有配额的“操作”列单击“退订”进行逐一退订。

图 10-3 退订容器版配额

说明

如果原配额计费方式为按需计费，关闭防护时按需划单停止计费。

----结束

步骤二：安装 Agent

旧版CGS与HSS新版是独立存在的，因此在HSS开启容器版防护需要不同的Agent。

步骤1 登录管理控制台。

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

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

步骤4 在“节点列表”中查看已关闭防护的节点是否在列表中存在。

须知

- 如果在HSS新版console查看已有，则无需安装Agent。
- 如果在HSS新版console查看没有，则需要重新在HSS新版控制台**安装Agent**。

----结束

步骤三：在 HSS 控制台购买容器版配额

步骤1 **登录管理控制台**。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入容器管理页面。

步骤4 在页面右上角，单击“购买容器安全”，进入“购买容器安全配额”页面。

步骤5 在购买容器安全配额界面，设置配额的规格。

表 10-2 购买主机安全服务参数说明

参数名称	参数说明	取值样例
计费模式	仅支持包年/包月模式	包年/包月
区域	• 配额的“区域”建议与主机的“区域”相同。 • 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。	华北-北京一
版本选择	选择“容器版”。如果需开启按需计费，你可参照**开启容器节点防护**直接开启防护即可。	容器版
购买节点数	购买的容器版配额数量。	10
购买时长	• 根据您的需求选择时长。 • 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，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。 • 如果未勾选自动“自动续费”，在即将到期时，请**手动续费**。	1年
标签	为同一种类型云资源进行自定义标签，帮助您实现快速查找。	cgs-data

步骤6 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7 确认订单无误后，请阅读《主机安全免责声明》，并**勾选**我已阅读并同意《主机安全免责声明》。

步骤8 单击“去支付”，进入付款页面，单击“确认付款”，完成支付，购买成功。

----结束

步骤四：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 > 主机安全服务”，进入主机安全平台界面。

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

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

图 10-4 开启容器防护

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

- **包年/包月**

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

  “防护配额”分配方式：

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

- **按需计费**

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

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

说明

一个容器安全配额防护一个集群节点。

----结束

10.3 如何开启节点防护?

开启节点防护的同时，系统会自动为该节点安装容器安全插件。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“资产管理 > 容器管理”，进入容器管理界面。

步骤4 在节点列表的“操作”列，单击“开启防护”，为需要开启防护的节点开启防护。

步骤5 在弹出的提示框中，阅读并勾选“我已阅读并同意《 容器安全服务免责声明 》”。

步骤6 单击“确定”，开启节点防护，节点的“防护状态”为“已开启”，说明该节点已开启防护。

说明

- 开启节点防护时，如果已购买的包周期防护配额小于当前已开启防护的节点个数，超出的节点将执行按需计费。主机安全服务按需计费请查看：**什么是容器安全服务的按需计费?**
- 一个主机安全服务配额防护一个集群节点。

----结束

10.4 自建 k8s 容器如何开启 apiserver 审计功能?

适用场景

用户自建k8s容器。

前提条件

- 已开启容器防护，相关操作请参见**开启容器节点防护**。
- 已确认apiserver审计功能未开启，确认步骤如下：
  a. 登录到kube-apiserver所在的节点。
  b. 查看kube-apiserver.yaml文件或者已经启动的kube-apiserver进程。
     - 进入/etc/kubernetes/manifest目录，查看kube-apiserver.yaml中是否存在--audit-log-path和--audit-policy-file，不存在即表示apiserver审计功能未正常开启。
     - 执行**ps**命令，查看kube-apiserver的进程命令行中是否存在--audit-log-path和--audit-policy-file，不存在即表示apiserver审计功能未正常开启。

开启 apiserver 审计功能

步骤1 将以下yaml内容复制并保存至yaml文件，并将yaml文件命名为“audit-policy.yaml”。

该yaml内容为k8s审计功能的配置文件，您可以直接使用或者根据实际业务情况编写。

```
apiVersion: audit.k8s.io/v1 # This is required.
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "RequestReceived"
rules:
```



```
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  # Kube-Proxy running on each node will watch services and endpoint objects in real time
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: "" # core
        resources: ["endpoints", "services"]
  # Some health checks
  - level: None
    users: ["kubelet"] # legacy kubelet identity
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    userGroups: ["system:nodes"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes"]
  - level: None
    users: ["system:apiserver"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["namespaces"]
  # Some system component certificates reuse the master user, which cannot be accurately distinguished
from user behavior,
  # considering that subsequent new functions may continue to add system operations under kube-system,
the cost of targeted configuration is relatively high,
  # in terms of the overall strategy, it is not recommended (allowed) for users to operate under the kube-
system,
  # so overall drop has no direct impact on user experience
  - level: None
    verbs: ["get", "update"]
    namespaces: ["kube-system"]
  # Don't log these read-only URLs.
  - level: None
    nonResourceURLs:
      - /healthz*
      - /version
      - /swagger*
  # Don't log events requests.
  - level: None
    resources:
      - group: "" # core
        resources: ["events"]
  # Don't log leases requests
  - level: None
    verbs: [ "get", "update" ]
    resources:
      - group: "coordination.k8s.io"
        resources: ["leases"]
  # Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
  # so only log at the Metadata level.
  - level: Metadata
    resources:
      - group: "" # core
        resources: ["secrets", "configmaps"]
      - group: authentication.k8s.io
        resources: ["tokenreviews"]
  # Get responses can be large; skip them.
  - level: Request
    verbs: ["get", "list", "watch"]
    resources:
      - group: "" # core
      - group: "admissionregistration.k8s.io"
```

```
    - group: "apps"
    - group: "authentication.k8s.io"
    - group: "authorization.k8s.io"
    - group: "autoscaling"
    - group: "batch"
    - group: "certificates.k8s.io"
    - group: "extensions"
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
 # Default level for known APIs
 - level: RequestResponse
   resources:
    - group: "" # core
    - group: "admissionregistration.k8s.io"
    - group: "apps"
    - group: "authentication.k8s.io"
    - group: "authorization.k8s.io"
    - group: "autoscaling"
    - group: "batch"
    - group: "certificates.k8s.io"
    - group: "extensions"
    - group: "networking.k8s.io"
    - group: "policy"
    - group: "rbac.authorization.k8s.io"
    - group: "settings.k8s.io"
    - group: "storage.k8s.io"
 # Default level for all other requests.
 - level: Metadata
```

步骤2 将audit-policy.yaml文件上传至/etc/kubernetes/路径下。

步骤3 进入/etc/kubernetes/manifests目录，将以下内容填写至配置文件kube-apiserver.yaml中，开启apiserver审计功能。

```
--audit-policy-file=/etc/kubernetes/audit-policy.yaml
--audit-log-path=/var/log/kubernetes/audit/audit.log
--audit-log-maxsize=100
--audit-log-maxage=1
--audit-log-maxbackup=10
```

说明

- --audit-policy-file：指定审计功能所使用的配置文件。
- --audit-log-path：指定用来写入审计事件的日志文件路径。不指定此标志会禁用日志后端。
- --audit-log-maxsize：定义审计日志文件轮转之前的最大大小（兆字节）。
- --audit-log-maxage：定义保留旧审计日志文件的最大天数。
- --audit-log-maxbackup：定义要保留的审计日志文件的最大数量。
- 将上述启动参数填写至配置文件kube-apiserver.yaml时，注意与kube-apiserver.yaml中的启动参数格式保持一致，且不能存在制表符（tab）。

步骤4 （可选）如果您的kube-apiserver是以Pod形式存在，请按如下步骤将审计日志持久化到主机上。

1. 在kube-apiserver.yaml中找到volumeMounts字段，按如下配置挂载数据卷。

```
volumeMounts:
  - mountPath: /etc/kubernetes/audit-policy.yaml
    name: audit
    readOnly: true
  - mountPath: /var/log/kubernetes/audit/
    name: audit-log
    readOnly: false
```


2. 在kube-apiserver.yaml中找到volumes字段，按如下配置挂载。

```
volumes:
- name: audit
  hostPath:
    path: /etc/kubernetes/audit-policy.yaml
    type: File
- name: audit-log
  hostPath:
    path: /var/log/kubernetes/audit/
    type: DirectoryOrCreate
```

----结束

10.5 容器集群防护插件卸载失败怎么办?

故障原因

当集群网络异常或插件正在工作时，通过HSS控制台卸载插件可能会失败。

解决措施

请参考如下步骤手动卸载插件。

步骤1 登录云服务器。

步骤2 在/tmp目录下新建plugin.yaml文件，并将如下脚本内容拷贝至plugin.yaml文件中。

```
apiVersion: v1
kind: Namespace
metadata:
  labels:
    admission.gatekeeper.sh/ignore: no-self-managing
    control-plane: controller-manager
    gatekeeper.sh/system: "yes"
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/audit-version: latest
    pod-security.kubernetes.io/enforce: restricted
    pod-security.kubernetes.io/enforce-version: v1.24
    pod-security.kubernetes.io/warn: restricted
    pod-security.kubernetes.io/warn-version: latest
  name: gatekeeper-system
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assign.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: assignimage.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
```



```
  labels:
    gatekeeper.sh/system: "yes"
  name: assignmetadata.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: configs.config.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constraintpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: constrainttemplates.templates.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplate.expansion.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: expansiontemplatepodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: modifyset.mutations.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
```

```
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.10.0
  labels:
    gatekeeper.sh/system: "yes"
  name: mutatorpodstatuses.status.gatekeeper.sh
---
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.11.3
  labels:
    gatekeeper.sh/system: "yes"
  name: providers.externaldata.gatekeeper.sh
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  creationTimestamp: null
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-role
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
  namespace: gatekeeper-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: gatekeeper-manager-role
subjects:
- kind: ServiceAccount
  name: gatekeeper-admin
  namespace: gatekeeper-system
---
apiVersion: admissionregistration.k8s.io/v1
kind: MutatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
```

```
  name: gatekeeper-mutating-webhook-configuration
---
apiVersion: admissionregistration.k8s.io/v1
kind: ValidatingWebhookConfiguration
metadata:
  labels:
    gatekeeper.sh/system: "yes"
  name: gatekeeper-validating-webhook-configuration
```

步骤3 在/tmp目录下新建uninstall.sh文件，并将如下脚本内容拷贝至uninstall.sh文件中。

```
#!/bin/bash
kubectl delete -f /tmp/plugin.yaml
kubectl delete ns cgs-provider
```

步骤4 执行如下命令卸载容器集群防护插件。

```
bash /tmp/uninstall.sh
```

回显如下图类似信息，表示插件卸载完成。

```
namespace "gatekeeper-system" deleted
resourcequota "gatekeeper-critical-pods" deleted
customresourcedefinition.apiextensions.k8s.io "assign.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignimage.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "assignmetadata.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "configs.config.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constraintpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "constrainttemplates.templates.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplate.expansion.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "expansiontemplatepodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "modifyset.mutations.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "mutatorpodstatuses.status.gatekeeper.sh" deleted
customresourcedefinition.apiextensions.k8s.io "providers.externaldata.gatekeeper.sh" deleted
serviceaccount "gatekeeper-admin" deleted
role.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
clusterrole.rbac.authorization.k8s.io "gatekeeper-manager-role" deleted
rolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "gatekeeper-manager-rolebinding" deleted
secret "gatekeeper-webhook-server-cert" deleted
service "gatekeeper-webhook-service" deleted
deployment.apps "gatekeeper-audit" deleted
deployment.apps "gatekeeper-controller-manager" deleted
poddisruptionbudget.policy "gatekeeper-controller-manager" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-mutating-webhook-configuration" deleted
validatingwebhookconfiguration.admissionregistration.k8s.io "gatekeeper-validating-webhook-configuration" deleted
```

----结束

11 勒索防护问题

11.1 勒索防护的备份与云备份有什么区别?

主机安全服务勒索防护的备份依附于云备份服务，只有购买了云备份服务，勒索备份才能正常使用。

因此，在备份机制、备份管理上两者没有区别，唯一区别是勒索备份会生成勒索专用的备份库。

勒索防护的备份机制继承云备份服务的备份机制，勒索防护的备份文件可在云备份服务统一管理和查看，云备份机制详情请参见**备份机制**。

12 区域和可用区

12.1 什么是区域和可用区?

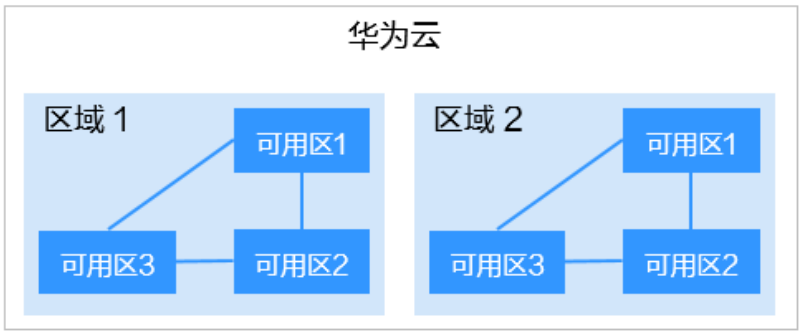
什么是区域、可用区?

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12-1阐明了区域和可用区之间的关系。

图 12-1 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。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

  - 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“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”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**。

12.2 哪些区域支持接入非华为云主机?

目前仅以下区域，可以接入非华为云主机：

- 华北-北京一
- 华北-北京四
- 华东-上海一
- 华东-上海二
- 华南-广州
- 中国-香港
- 亚太-新加坡
- 西南-贵阳一
- 亚太-雅加达

如果您的主机非华为云主机，请在上述区域购买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。

12.3 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。

13 安全配置问题

13.1 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 > 主机安全服务”，进入主机安全服务页面。

步骤3 在左侧导航栏选择“安装与配置”，进入安装与配置页面，选择“安全配置 > SSH登录IP白名单”，进入“SSH登录IP白名单”页签。

步骤4 在目标白名单IP所在行的“操作”列单击“禁用”或者“删除”，清除配置的SSH登录IP白名单。

----结束

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。

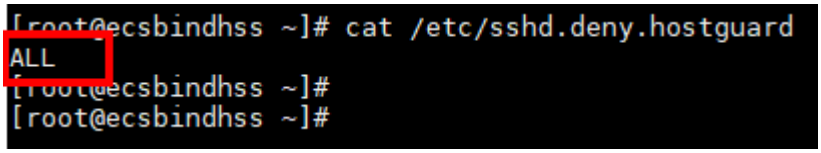
清除配置的SSH登录IP白名单，操作步骤如下所示。

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13-1所示。

cat /etc/sshd.deny.hostguard

图 13-1 查看文件内容



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

13.2 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。

可能原因

- 因账户暴力破解（例如：输入密码错误次数过多，30秒内，错误次数达到5次及以上），导致主机IP被拦截。
- 开启了**SSH登录IP白名单**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 确认是否因为账户暴力破解，导致主机IP被拦截。

- 是，请按如下步骤操作：
  a. 登录主机安全服务控制台。
  b. 在左侧导航树选择“入侵检测 > 安全告警事件”，进入“安全告警事件”页面。
  c. 选择“主机告警事件”页签，单击“已拦截IP”区域的数值，弹出“已拦截IP”页面。
  d. 选中目标攻击源IP，单击列表上方“解除拦截”，解除IP拦截。
- 否，请执行**步骤2**。

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

- 是，将登录主机的IP加入到**SSH登录IP白名单**。
- 否，请联系技术支持工程师。

----结束

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?

13.3 如何使用双因子认证?

本章节指导用户如何使用双因子认证。

如何开启

请参见：开启双因子认证功能。

登录与使用

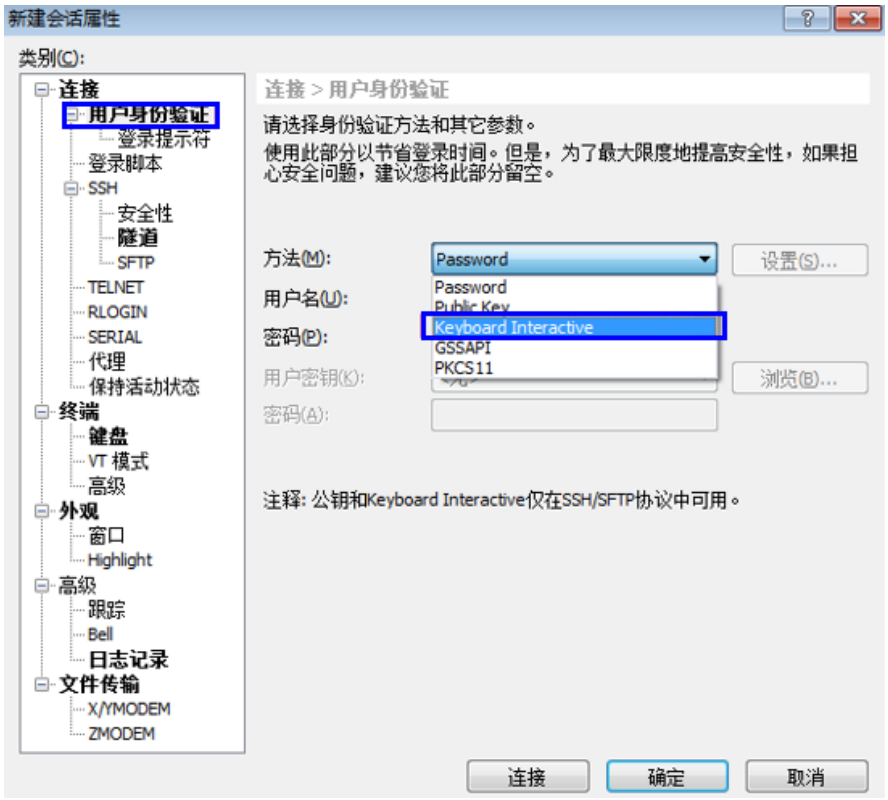
- 登录Linux主机
  a. 使用PuTTY/Xshell登录云主机。
     登录时，请选择“Keyboard Interactive”，输入用户身份验证。
     - PuTTY
       身份验证方法选择“Keyboard Interactive”，并单击“确定”。

       图 13-2 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”。

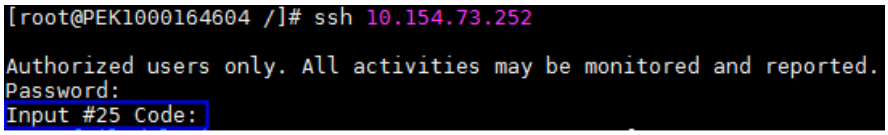
图 13-3 键盘交互模式（二）



b. 输入云主机的账户与密码。

c. 开启双因子认证后，需输入订阅终端接收到的验证码。

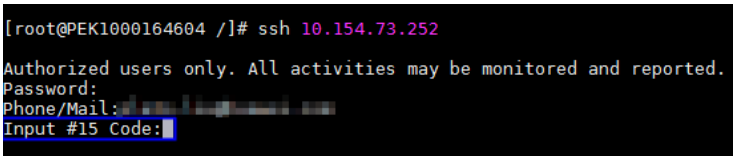
图 13-4 输入验证码



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13-5。

图 13-5 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 13-6 远程桌面连接

c. 如果已开启双因子认证，需要输入预留手机号或邮箱，单击“获取验证码”。

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、云主机账号和密码，单击，登录云主机。

13.4 开启双因子认证失败，怎么办?

问题现象

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

可能原因

- 主机未开启防护。
- 开启双因子认证不会立即生效，需要等大约5分钟才生效。
- Linux主机没有关闭“密钥对”登录方式。
- 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**4**。

步骤4 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。
    setenforce 0 #临时关闭
  - 永久关闭Selinux防火墙。
    vi /etc/selinux config
    selinux=disabled #永久关闭

步骤5 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6**。
- 否：请停止“网防G01”软件和服务器版360安全卫士。

步骤6 请联系技术支持。

----结束

13.5 开启双因子认证后收不到验证码?

- 开启双因子认证功能后，不会立即生效。
  需要等大约5分钟才生效。
- 开启双因子认证需要关闭Selinux防火墙。
  请**关闭Selinux防火墙**后重试。
- Linux主机需要使用“密码”登录方式。
  请按以下步骤切换密钥登录为密码登录：
  a. 使用密钥登录Linux云服务器，设置root密码。
     sudo passwd root
     如果密钥文件丢失或损坏，请重置root密码。
  b. 使用root身份编辑云服务器的ssh登录方式。
     su root
     vi /etc/ssh/sshd_config

修改如下配置项：

- 把PasswordAuthentication no改为PasswordAuthentication yes
  或去掉PasswordAuthentication yes前面的#注释掉。
- 把PermitRootLogin no改为PermitRootLogin yes
  或去掉PermitRootLogin yes前面的#注释掉。

c. 重启sshd使修改生效。

service sshd restart

d. 重启云服务器就可以使用root用户和新设置的密码登录了。

说明

防止非授权用户使用原来的密钥文件访问Linux云服务器，请将/root/.ssh/authorized_keys文件删除或清空authorized_keys文件内容。

13.6 为什么开启双因子认证后登录主机失败?

登录主机失败的原因可能为文件配置错误或登录方式错误导致。

文件配置错误

您可检查配置文件是否正确。

配置文件路径：/etc/ssh/sshd_config

需要确认的配置文件项：

PermitEmptyPasswords no

UsePAM yes

ChallengeResponseAuthentication yes

须知

如果您使用的是root登录，还需要配置文件项为：
PermitRootLogin yes

登录方式错误

失败原因：开启双因子认证后，可能是通过以下方式登录云主机导致登录失败。

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

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

解决办法：您可参照**如何使用双因子认证?** 重新登录认证。

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”。

13.7 开启双因子认证时，如何添加接收验证通知的手机号或邮箱?

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

“选择消息通知服务”下拉列表中，只展示状态已确认的消息通知服务主题。

- 如果没有主题，请单击“查看消息通知服务主题”进行创建。创建完成后，单击“添加订阅”，设置需要接受通知的手机号码或邮箱。
- 如果已有主题，需要添加或者修改手机号码、邮箱：
  - 添加手机号码或邮箱

    单击“查看消息通知服务主题”进入主题页面，单击“添加订阅”，添加需要接受消息通知的手机号码或邮箱。
  - 删除手机号码或邮箱

    单击“查看消息通知服务主题”进入主题页面，单击主题名称，进入主题详情页面，选择订阅总数页签，单独删除或批量删除目标终端即可。

13.8 双因子认证中，验证码是一个固定的验证码吗?

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

图 13-7 验证码验证

13.9 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**。

13.10 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13-8所示。

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

图 13-8 告警方式

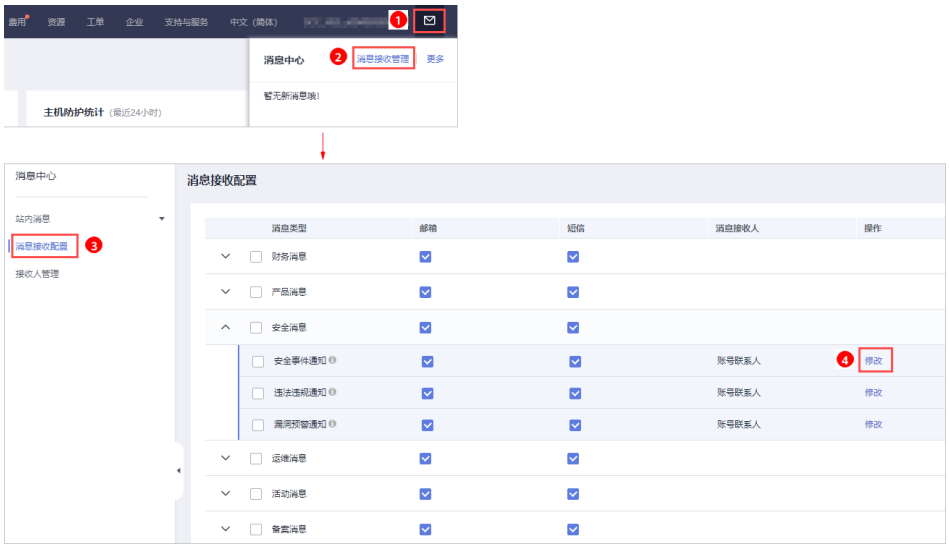
消息中心

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账号联系人，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 13-9 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13-10所示。

图 13-10 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。

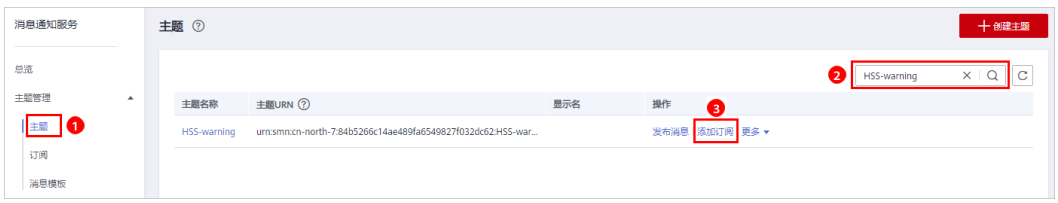
步骤5 单击“删除”，删除订阅。

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 13-11 添加订阅



----结束

13.11 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 13-12 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**。

13.12 是否可以不开启 HSS 告警通知?

可以不开启HSS告警通知。

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

设置告警通知

开启主机安全防护后，如果您想设置告警通知，可以通过以下步骤进行设置：

1. 登录主机安全控制台。
2. 选择“安装与配置 > 告警配置”，进入告警配置页面，设置告警通知。

取消告警通知

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

取消设置HSS告警通知方式，如下所示：

- 方式一：删除消息通知主题
  删除主题后，您配置的告警通知将不会生效。
- 方式二：删除消息通知主题中的订阅
  删除订阅后，您将不会收到告警通知。
- 方式三：取消或关闭消息通知主题中的订阅

取消订阅后，您将不会收到告警通知。

13.13 如何修改告警通知的通知项?

开启主机安全防护后，如果您不想收到HSS的某项告警通知，您可以屏蔽不想接收告警的事件。屏蔽后，无论是否有风险，您都只能登录管理控制台自行查看，无法收到告警短信或邮件。

操作步骤

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“安装与配置”，进入安装与配置界面。

步骤4 选择“告警配置”页签，进入“告警配置”页面。

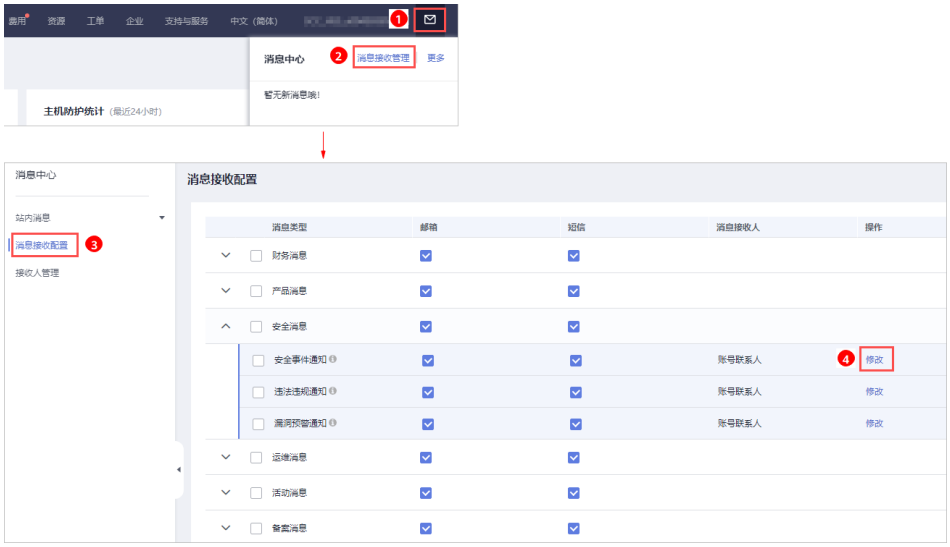
步骤5 选择无需发送告警的屏蔽事件。关于告警通知项详细说明，请参见**告警通知项说明**。

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账号联系人，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 13-13 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。

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

----结束

13.14 如何关闭 SELinux 防火墙?

SELinux(Security Enhanced Linux)安全增强型linux系统，是一个linux内核模块，也是linux的一个安全子系统。

SELinux的主要作用是最大限度地减小系统中服务进程可访问的资源（最小权限原则）。

关闭说明

- SELinux关闭后不会影响业务使用。
- SELinux关闭可根据需求选择临时关闭或永久关闭。

关闭场景

使用HSS的双因子认证功能时，需要将SELinux防火墙进行永久关闭。

关闭操作

步骤1 远程登录目标服务器。

- **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**。
- **非华为云主机**

  请使用远程管理工具（例如：PuTTY、Xshell等）连接您服务器的弹性IP，远程登录到您的服务器。

步骤2 在命令窗口执行关闭命令。

- **临时关闭**

  在命令窗口执行以下命令临时关闭SELinux。

  ```
  setenforce 0
  ```

  说明

  在重启系统后将恢复开启状态。

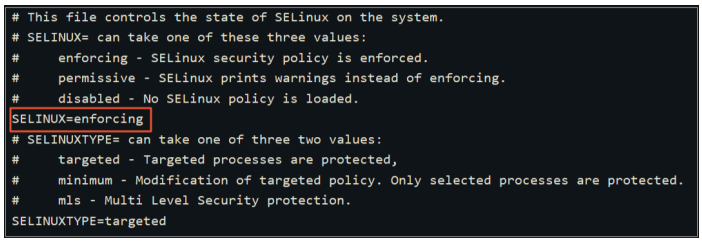
- **永久关闭**

  a. 在目录窗口执行以下命令，编辑SELinux的config文件。

  ```
  vi /etc/selinux/config
  ```

  b. 找到SELINUX=enforcing，按i进入编辑模式，将参数修改为SELINUX=disabled。

  图 13-14 编辑 selinux 状态

c. 修改完成后，按下键盘Esc键，执行以下命令保存文件并退出。

```
:wq
```

步骤3 执行永久关闭命令并保存退出后，执行以下命令立即重启服务器。

```
shutdown -r now
```

说明

执行永久关闭的命令后不会立即生效，重启服务器后才会生效。

步骤4 重启后运行以下命令，验证SELinux的状态为disabled，表明SELinux已关闭。

```
getenforce
```

----结束

14 配额问题

14.1 如何延长 HSS 防护配额有效期?

主机安全服务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，因此无需延长有效期，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**。

14.2 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“安全合规 > 主机安全服务”，进入主机安全服务界面。

步骤3 在左侧导航树中，选择“主机管理”，进入主机管理界面。

步骤4 在“云服务器”页签中，在搜索框筛选“防护状态”为“关闭”的主机，查看未绑定配额的主机。

图 14-1 筛选未绑定配额的主机

----结束

14.3 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：

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

14.4 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

- 如果您购买的是基础版/企业版/旗舰版，请在“主机安全服务 > 主机管理 > 云服务器”页面开启防护。
- 如果您购买的是网页防篡改版，请在“主机安全服务 > 主动防御 > 网页防篡改 > 防护配置”页面开启防护。
- 如果您购买的是容器版，请在“主机安全服务 > 容器管理 > 节点列表”页面开启防护。

企业项目不正确

如果已开通企业项目，请切换到正确的“企业项目”为服务器开启防护。

14.5 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。

14.6 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，以便获得主机安全服务更好的服务体验。

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，以便获得主机安全服务更好的服务体验。

表 14-1 Agent 支持的操作系统

操作系统类型	系统架构	Agent支持的操作系统版本	该操作系统的漏洞扫描支持情况（√表示支持，×表示不支持）
Windows	X86	Windows 10（64位） **说明** 仅支持华为云云桌面使用该操作系统。	×
		Windows 11（64位） **说明** 仅支持华为云云桌面使用该操作系统。	×
		Windows Server 2012 R2 标准版 64位英文(40GB)	√
		Windows Server 2012 R2 标准版 64位简体中文(40GB)	√
		Windows Server 2012 R2 数据中心版 64位英文(40GB)	√
		Windows Server 2012 R2 数据中心版 64位简体中文(40GB)	√
		Windows Server 2016 标准版 64位英文(40GB)	√
		Windows Server 2016 标准版 64位简体中文(40GB)	√
		Windows Server 2016 数据中心版 64位英文(40GB)	√
		Windows Server 2016 数据中心版 64位简体中文(40GB)	√
		Windows Server 2019 数据中心版 64位英文(40GB)	√
		Windows Server 2019 数据中心版 64位简体中文(40GB)	√

操作系统类型	系统架构	Agent支持的操作系统版本	该操作系统的漏洞扫描支持情况（√表示支持，×表示不支持）
Linux	X86	CentOS 7.4（64位）	√
		CentOS 7.5（64位）	√
		CentOS 7.6（64位）	√
		CentOS 7.7（64位）	√
		CentOS 7.8（64位）	√
		CentOS 7.9（64位）	√
		CentOS 8.1（64位）	×
		CentOS 8.2（64位）	×
		CentOS 8（64位）	×
		CentOS 9（64位）	×
		Debian 9（64位）	√
		Debian 10（64位）	√
		Debian 11.0.0（64位）	√
		Debian 11.1.0（64位）	√
		EulerOS 2.2（64位）	√
		EulerOS 2.3（64位）	√
		EulerOS 2.5（64位）	√
		EulerOS 2.7（64位）	×
		EulerOS 2.9（64位）	√
		Fedora 28（64位）	×
		Ubuntu 16.04（64位）	√
		Ubuntu 18.04（64位）	√
		Ubuntu 20.04（64位）	√
		Ubuntu 22.04（64位）	√
		RedHat 7.4（64位）	×
		RedHat 7.6（64位）	×
		RedHat 8.0（64位）	×
		RedHat 8.7（64位）	×

操作系统类型	系统架构	Agent支持的操作系统版本	该操作系统的漏洞扫描支持情况（√表示支持，×表示不支持）
		OpenEuler 20.03 LTS（64位）	×
		OpenEuler 22.03 SP3（64位）	×
		OpenEuler 22.03（64位）	×
		AlmaLinux 8.4（64位）	√
		AlmaLinux 9.0（64位）	×
		RockyLinux 8.4（64位）	×
		RockyLinux 8.5（64位）	×
		RockyLinux 9.0（64位）	×
		HCE 1.1（64位）	√
		HCE 2.0（64位）	√
		SUSE 12 SP5（64位）	√
		SUSE 15（64位）	×
		SUSE 15 SP1（64位）	√
		SUSE 15 SP2（64位）	√
		SUSE 15 SP3（64位）	×
		SUSE 15.5（64位）	×
		Kylin V10（64位）	√
	ARM	CentOS 7.4（64位）	√
		CentOS 7.5（64位）	√
		CentOS 7.6（64位）	√
		CentOS 7.7（64位）	√
		CentOS 7.8（64位）	√
		CentOS 7.9（64位）	√
		CentOS 8.0（64位）	×
		CentOS 8.1（64位）	×
		CentOS 8.2（64位）	×
		CentOS 9（64位）	×
		EulerOS 2.8（64位）	√

操作系统类型	系统架构	Agent支持的操作系统版本	该操作系统的漏洞扫描支持情况（√表示支持，×表示不支持）
		EulerOS 2.9（64位）	√
		Fedora 29（64位）	×
		Ubuntu 18（64位）	×
		Kylin V7（64位）	×
		Kylin V10（64位）	√
		HCE 2.0（64位）	√
		统信UOS V20（64位）	√（统信UOS V20服务器E版、D版）

14.7 购买了主机安全服务版本为什么没有生效?

购买了主机安全服务版本后您还需要做以下操作才可为目标主机开启防护：

1. 安装Agent：为目标主机安装Agent，安装后可实现HSS对数据的监测以及告警的上报，如果已安装可忽略此步骤，安装Agent操作详情请参见**安装Agent**。
2. 绑定配额：将购买的版本配额绑定至需要防护的服务器，绑定后目标服务器才会开启对应版本支持的防护能力，绑定配额开启主机防护操作详情请参见**开启主机安全防护**，开启容器安全防护操作详情请参见**开启器防护**。

开启防护后建议开启告警通知确保在发现告警的第一时间收到通知，同时对服务器进行安全配置，进一步提升服务器的安全性。

14.8 如何切换服务器绑定的防护配额版本?

防护配额切换说明

服务器支持切换绑定的防护配额版本为基础版、专业版、企业版、旗舰版。

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

前提条件

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

操作步骤

步骤1 登录管理控制台。

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

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

说明

云服务器列表仅显示以下主机的防护状态：

- 在所选区域购买的华为云主机
- 已接入所选区域的非华为云主机

步骤4 根据需要可为单台服务器或多服务器切换防护配额版本。

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

表 14-2 切换版本参数配置说明

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

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

表 14-3 切换版本说明

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

c. 阅读并勾选《主机安全免责声明》。

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

步骤5 单击“确定”切换版本。

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

----结束

后续操作

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

15 计费、续费与退订

15.1 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

主机安全服务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，例如一般数据、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。

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**。

15.2 退订后重购 HSS，是否需要重新安装 Agent 与配置主机防护信息?

不需要。

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。

须知

请保证重购防护配额的区域与原购买区域保持一致，HSS不支持跨区域使用。

15.3 如何为主机安全服务续费?

该任务指导您如何在购买的**包年/包月**模式主机安全服务即将到期时进行续费。续费后，您可以继续使用HSS。

- 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，如果您没有及时续费，资源会进入保留期。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。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**。

为了防止造成不必要的损失，请您及时续费。

说明

- 如果在购买主机安全服务时，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，无需手动续费。
- 如果您使用的是子账号，需要主账号对子账号赋予BSS Administrator权限，才可以使用子账号执行续费操作。

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权限的账号，可以对账号中心、费用中心、资源中心的所有菜单项执行任意操作。

手动续费

步骤1 **登录管理控制台**。

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

步骤3 根据不同的配额类型执行续费操作。

- **续费主机配额**：
  a. 在左侧导航栏选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要续费的配额所在行的“操作”列，选择“更多 > 续费”。
  您也可以勾选所有需要续费的配额，在配额列表左上方单击“批量续费”，进行批量续费。
  c. 在续费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**。
- **续费容器配额**：
  a. 在左侧导航栏选择“资产管理 > 容器管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要续费的配额所在行的“操作”列，选择“更多 > 续费”。
  您也可以勾选所有需要续费的配额，在配额列表左上方单击“批量续费”，进行批量续费。
  c. 在续费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

自动续费

如果在购买主机安全服务时，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，无需再次开通自动续费。

如果您在购买主机安全服务时，未勾选并同意“自动续费”，需要开启自动续费，请参照如下步骤进行处理。

步骤1 登录管理控制台。

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

步骤3 为不同的配额类型开通自动续费。

- **自动续费主机配额**：
  a. 在左侧导航栏选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要续费的配额所在行的“操作”列，选择“更多 > 开通自动续费”。
  您也可以勾选所有需要续费的配额，在配额列表左上方单击“开通自动续费”，批量开通自动续费。
  c. 在开通自动续费页面，确认需要开通自动续费的配额名称，选择自动续费时长和自动续费次数。
  d. 单击“确认”，完成自动续费开通。
- **自动续费容器配额**：
  a. 在左侧导航栏选择“资产管理 > 容器管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要续费的配额所在行的“操作”列，选择“更多 > 开通自动续费”。
  您也可以勾选所有需要续费的配额，在配额列表左上方单击“开通自动续费”，批量开通自动续费。
  c. 在开通自动续费页面，确认需要开通自动续费的配额名称，选择自动续费时长和自动续费次数。
  d. 单击“开通”，完成自动续费开通。

----结束

15.4 如何让主机安全服务停止计费?

如果您需要让空闲的主机安全服务配额停止计费，请参照本章节进行处理。

包年/包月计费的主机安全服务配额支持退订，退订后，会退还您未消费的金额，详细操作请参见**退订包年/包月计费模式的主机安全服务配额**。

按需计费的主机安全服务配额按您实际的使用时长收费，关闭防护后就不再计费，详细操作请参见**停用按需计费计费模式的主机安全服务配额**。

说明

如果您使用的是子账号，需要主账号对子账号赋予BSS Administrator操作权限后，才可以使用子账号执行退订操作。

退订“包年/包月”计费模式的主机安全服务配额

包年/包月计费模式的主机安全服务配额支持退订。

- 购买的配额（不包含未生效资源）在开通5天内，且当年已退订资源未超过10个，华为云支持5天无理由全额退款。
- 购买的配额超过5天后退订会收取手续费、已消费金额，不退还已使用代金券和折扣券。

退订规则详细说明请参见**退订规则说明**

步骤1 **登录管理控制台**。

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

步骤3 根据不同的配额类型执行退订操作。

- **退订主机配额**：
  a. 在左侧导航栏选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要退订的配额所在行的“操作”列，选择“更多 > 退订”。
     您也可以勾选所有需要退订的配额，在配额列表左上方单击“批量退订”，进行批量退订。
  c. 在退订资源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**。
- **退订容器配额**：
  a. 在左侧导航栏选择“资产管理 > 容器管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要退订的配额所在行的“操作”列，选择“更多 > 退订”。
     您也可以勾选所有需要退订的配额，在配额列表左上方单击“批量退订”，进行批量退订。
  c. 在退订资源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**。

说明

新购买的主机安全服务配额（不包含未生效资源）在开通5天内，且当年已退订资源未超过10个，华为云支持5天无理由全额退订。具体请参见**可五天无理由退订**。

----结束

停用“按需计费”计费模式的主机安全服务配额

以按需计费方式购买的企业版或容器版防护配额，关闭防护后将不再计费。

步骤1 **登录管理控制台**。

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

步骤3 进入防护列表页面。

- 主机防护列表：在左侧导航栏选择“资产管理 > 主机管理”页面，选择“云服务器”页签，进入主机防护列表页面。
- 容器防护列表：在左侧导航栏选择“资产管理 > 容器管理”页面，选择“容器节点管理 > 节点”页签，进入容器防护列表页面。

步骤4 在需要停止按需计费的防护中的服务器所在行，单击操作列的“关闭防护”。

步骤5 在确认信息窗口中，单击“确认”。

关闭防护成功后，返回防护列表，相应主机或容器防护状态为“未防护”。

----结束

15.5 如何取消自动续费?

您为HSS配额设置自动续费后，还可以取消自动续费。取消自动续费后，为避免配额到期无法使用，您需要为配额**手动续费**。

操作步骤

步骤1 **登录管理控制台**。

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

步骤3 根据不同的配额类型执行取消自动续费操作。

- **主机配额取消自动续费**：
  a. 在左侧导航栏选择“资产管理 > 主机管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要取消自动续费的配额所在行的“操作”列，选择“更多 > 修改自动续费”。
  c. 在“修改自动续费”页面，续费方式选择“手动续费”。
  d. 单击“确定”，取消自动续费。
- **容器配额取消自动续费**：
  a. 在左侧导航栏选择“资产管理 > 容器管理”页面，选择“防护配额”页签，进入防护配额列表页面。
  b. 在需要取消自动续费的配额所在行的“操作”列，单击“更多 > 修改自动续费”。
  c. 在“修改自动续费”页面，续费方式选择“手动续费”。
  d. 单击“确定”，取消自动续费。

----结束

16 其他

16.1 如何使用 Windows 远程桌面连接工具连接主机?

操作步骤

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

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

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

步骤4 在弹出的对话框中，输入主机的用户密码，单击“确定”，连接至主机。

----结束

16.2 如何查看 HSS 的日志文件?

日志路径

您需要根据主机的操作系统，查看日志文件。

操作系统	日志所在路径	日志文件
Linux	/var/log/hostguard/	• hostwatch.log • hostguard.log • upgrade.log • hostguard-service.log • config_tool.log • engine.log

操作系统	日志所在路径	日志文件
Windows	C:\Program Files\HostGuard\log	• hostwatch.log • hostguard.log • upgrade.log

日志保留周期

日志文件	日志描述	文件大小限制	路径下保留的文件	保留周期
hostwatch.log	记录守护进程运行时相关日志。	10 MB	保留8个最新的日志文件。	不超过文件大小限制，只要不卸载HSS Agent，会一直保留日志信息。
hostguard.log	记录工作进程运行时相关日志。	10 MB	保留8个最新的日志文件。	
upgrade.log	记录版本升级时相关日志。	10 MB	保留8个最新的日志文件。	
hostguard-service.log	记录服务启动时相关日志（脚本）。	100 kB	保留2个最新的日志文件。	
config_tool.log	记录服务启动时相关日志（程序）。	10 kB	保留2个最新的日志文件。	
engine.log	记录服务退出时相关日志。	10 kB	保留2个最新的日志文件。	

16.3 如何开启登录失败日志开关?

MySQL

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

步骤1 使用root权限登录主机。

步骤2 查询log_warnings值，命令如下：

show global variables like 'log_warnings'

步骤3 修改log_warnings值，命令如下。

set global log_warnings=2

步骤4 修改配置文件。

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

----结束

vsftp

本节指导用户开启vsftp的登录失败日志开关。

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

vsftpd_log_file=log/file/path

dual_log_enable=YES

步骤2 重启vsftp服务。设置成功后，登录时，会返回如图16-1所示的日志记录。

图 16-1 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

16.4 HSS 有没有服务等级协议?

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**。

16.5 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。

16.6 HSS 是否能以软件形式线下输出?

不支持线下软件的形式。

16.7 企业项目为什么无法查看“所有项目”？

只有具有Tenant Administrator权限或HSS Administrator+Tenant Guest权限的账号可以选择企业项目的“所有项目”进行查看。如果您的子账号没有相应的权限，不支持查看企业项目的“所有项目”内容，您可以参考**给IAM用户授权**给子账号授权。

16.8 如何开启主机安全服务自保护?

主机安全服务自保护提供主机安全的文件、进程和软件的保护功能，防止恶意程序卸载主机安全服务Agent、篡改主机安全服务文件或停止主机安全服务进程。

约束限制

- 仅操作系统为Windows且主机安全服务版本为旗舰版和网页防篡改版时，支持主机安全服务自保护。
- 自保护功能依赖AV检测、HIPS检测或者勒索病毒防护功能使能驱动才能生效，只有这三个功能开启一个以上时，开启自保护才会生效。相关操作请参见：
  - 开启勒索病毒防护。
  - AV检测、HIPS检测默认开启，如果您手动关闭了这两个检测项，可参考查看策略组，重新开启。
- 开启自保护策略后的影响如下：
  - 主机安全服务的Agent不支持通过主机的控制面板卸载，支持通过主机安全服务控制台卸载。
  - 主机安全服务的进程无法被终止。
  - Agent安装路径C:\Program Files\HostGuard下除了log目录、data目录（如果Agent升级过，再加上upgrade目录）外的其他目录无法访问。

操作步骤

步骤1 登录管理控制台。

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

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

步骤4 单击目标旗舰版Windows策略组名称，进入策略组详情页面。

目标策略组指的是您需要开启主机安全服务自保护的服务器所属策略组。

- 如果您未新建新的旗舰版策略组，那您的服务器都以系统默认的旗舰版策略组进行防护，您选择系统默认的旗舰版策略组“tenant_windows_premium_default_policy_group”即可。
- 如果您新建了旗舰版策略组，您要选择您的服务器所属策略组，您可以通过以下方式确认服务器所属策略组：
  a. 在左侧导航栏选择“资产管理 > 主机管理”。
  b. 在云服务器页签，查看服务器所属策略组。

图 16-2 查看服务器所属策略组

步骤5 在自保护策略所在行的“操作”列，单击“开启”。

步骤6 在弹窗中，单击“确认”。

----结束

相关操作

关闭主机安全服务自保护

步骤1 在自保护策略所在行的“操作”列，单击“关闭”。

步骤2 在弹窗中，单击“确认”。

----结束

16.9 主机安全服务自保护无法关闭怎么办?

问题根因

当服务器网络不通时会导致Agent无法通信（Agent接收不到HSS控制台下发的关闭自保护的指令），因此主机安全服务自保护无法关闭。

解决方法

步骤1 登录管理控制台。

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

步骤3 在左侧导航树选择“资产管理 > 主机管理”。

步骤4 在“云服务器”页面，单击服务器防护列表右上角，勾选展示“Agent ID”。

图 16-3 展示 Agent ID

步骤5 在服务器防护列表上方，输入服务器名称或ID，单击查找待关闭HSS自保护的Windows服务器。

步骤6 在目标Windows服务器所在行的Agent ID列，复制Agent ID前八位字符。

步骤7 打开目标Windows服务器的cmd命令行窗口。

步骤8 执行如下命令，关闭HSS自保护。

"C:\Program Files\HostGuard\bin\HssClient.exe"1234abcd

说明

命令中包含的**1234abcd**表示Agent ID前八位字符。以Agent ID的前八位字符作为执行HSSClient.exe时的验证码，是为了防止恶意程序关闭自保护和用户误操作而做的验证防护，只有输入正确的Agent ID前八位字符才能关闭自保护

步骤9 界面回显“Disable self protect succeed.”表示关闭HSS自保护成功。

----结束

16.10 ECS 服务器已经删除，为什么 HSS 的服务器列表仍显示有该服务器?

ECS服务器删除后，HSS不会立即同步相关信息，所以您在HSS的服务器列表可能查看到已经删除的服务器。以下是HSS的服务器列表刷新机制：

- 每日凌晨自动执行一次同步任务，刷新服务器列表。
- 当您进入HSS的“资产管理 > 主机管理”页面后，HSS也会立即启动同步任务，预计十分钟内完成服务器信息同步。十分钟后，您刷新主机管理页面，即可查看最新的服务器列表信息。

A 修订记录

发布日期	修改说明
2024-01-08	第十六次正式发布。 新增： • **批量安装Agent失败，提示“网络不通”怎么处理?** • **高危命令执行告警，如何添加白名单?**
2023-12-21	第十五次正式发布。 • **Agent检测时占用多少CPU和内存资源?** ，增加病毒查杀任务执行时占用说明。 • **如何让主机安全服务停止计费?** ，支持批量退订。
2023-10-27	第十四次正式发布。 新增： • **手动扫描漏洞或批量修复漏洞时，为什么选不到目标服务器?** • **容器集群防护插件卸载失败怎么办?** • **升级Agent失败，提示“替换文件失败”怎么处理?** 修改： 服务中文名称修改为“主机安全服务”
2023-09-27	第十三次正式发布。 新增： • **HSS支持跨账号使用吗?** • **无法访问Windows或Linux版本Agent下载链接?** • **HSS由旧版升级为新版后不告警了，怎么办?** • **漏洞修复失败怎么办?** • **如何切换服务器绑定的防护配额版本?** • **ECS服务器已经删除，为什么HSS的服务器列表仍显示有该服务器?**

发布日期	修改说明
2023-07-25	第十二次正式发布。 新增： • **如何开启主机安全服务自保护？** • **主机安全服务自保护无法关闭怎么办？** • **服务器远程端口已修改，为什么暴力破解记录仍显示旧端口？** • **自建k8s容器如何开启apiserver审计功能？**
2023-07-19	第十一次正式发布。 新增： **如何取消自动续费？** 优化： **Agent如何升级？**，增加手动升级Agent2.0操作。
2023-06-15	第十次正式发布。 新增： • **企业项目为什么无法查看“所有项目”？**

发布日期	修改说明
2023-05-24	第九次正式发布。 新增： • HSS是否支持防护本地IDC服务器? • HSS是否和其他安全软件有冲突? • 购买HSS后会自动安装Agent吗? • 频繁收到HSS暴力破解告警如何处理? • 收到来自华为云IP的暴力破解告警如何处理? • HSS的恶意程序检测周期、隔离查杀是多久一次? • HSS拦截的IP是否需要处理? • 如何防御勒索病毒攻击? • HSS如何查询漏洞、基线已修复记录? • 如何关闭节点防护? • HSS可以跨区域使用吗? • 如何清除HSS中配置的SSH登录IP白名单? • 不能通过SSH远程登录主机，怎么办? • 如何使用双因子认证? • 开启双因子认证失败，怎么办? • 开启双因子认证后收不到验证码? • 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，如何添加接收验证通知的手机号或邮箱? • 双因子认证中，验证码是一个固定的验证码吗? • 如何修改接收告警通知的手机号或邮箱? • 配置告警通知时选不到消息主题? • 是否可以不开启HSS告警通知? • 如何修改告警通知的通知项? • 云服务器列表为什么看不到购买的服务器? • 开启防护时显示没有配额? • HSS到期后不续费，对主机和业务有影响吗? • 退订后重购HSS，是否需要重新安装Agent与配置主机防护信息?
2023-04-27	第八次正式发布。 新增： • 如何为主机安全服务续费? • 如何让主机安全服务停止计费?
2023-03-06	第七次正式发布。 新增FAQ： 如何使用镜像批量安装Agent?

发布日期	修改说明
2023-01-18	第六次正式发布。 新增FAQ： **购买了主机安全服务版本为什么没有生效?** **容器安全如何切换至主机安全服务控制台?**
2022-11-15	第五次正式发布。 新增：**主机安全服务不升级有什么影响?**
2022-11-04	第四次正式发布。 新增：**主机安全服务升级失败怎么处理?**
2022-10-28	第三次正式发布。 新增章节： **Agent如何升级?** **勒索防护的备份与云备份有什么区别?**
2022-10-20	第二次正式发布。 新增Agent问题所有章节。
2022-08-31	第一次正式发布。