企业主机安全

最佳实践

文档版本 12

发布日期 2025-01-07

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 HSS 最佳实践汇总

本文汇总了企业主机安全（HSS）服务的常见应用场景的操作实践，并为每个场景提供详细的方案描述和操作指南，以帮助您使用HSS提升主机和容器的安全性。

HSS 最佳实践

表 1-1 HSS 最佳实践

分类	相关文档
接入HSS	第三方主机通过专线和VPC终端节点接入HSS
	第三方主机通过专线和代理服务器接入HSS
	通过CBH安装HSS的Agent
主机登录保护	使用HSS增强主机登录安全
漏洞修复	Git用户凭证泄露漏洞（CVE-2020-5260）
	SaltStack远程命令执行漏洞（CVE-2020-11651/CVE-2020-11652）
	OpenSSL高危漏洞（CVE-2020-1967）
	Adobe Font Manager库远程代码执行漏洞（CVE-2020-1020/CVE-2020-0938）
	Windows内核特权提升漏洞（CVE-2020-1027）
	Windows CryptoAPI欺骗漏洞（CVE-2020-0601）
	使用HSS扫描和修复漏洞
弱口令防御	使用HSS防御弱口令风险
勒索病毒防护	使用HSS和CBR防御勒索病毒
入侵检测	使用HSS查杀系统木马
	使用HSS应对挖矿攻击

分类	相关文档
	利用白名单机制避免告警误报
文件保护	使用HSS监控Linux主机文件完整性
护网或重保	护网或重保场景下HSS的应用实践

Solution as Code 一键式部署类最佳实践

为帮助企业高效上云，华为云Solution as Code萃取丰富上云成功实践，提供一系列基于华为云可快速部署的解决方案，帮助用户降低上云门槛。同时开放完整源码，支持个性化配置，解决方案开箱即用，所见即所得。

表 1-2 Solution as Code 一键式部署类最佳实践汇总

场景类型	一键式部署方案	说明	相关服务
网站防护	防勒索病毒安全解决方案	该解决方案能帮您为华为云上部署的服务器提供事前安全加固、事中主动防御、事后备份恢复的防勒索病毒方案，抵御勒索软件入侵，营造主机资产安全运行环境。	WAF、HSS、SMN
等保	等保二级解决方案	该解决方案能帮您在华为云上快速部署等保二级合规解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。	WAF、CFW、HSS、SCM、SA、MTD
	等保三级解决方案	该解决方案依托华为云自身安全能力与安全合规生态，为用户提供一站式的等保三级安全解决方案	WAF、HSS、SCM、SA、MTD、CFW、CBH、DBS、CodeArts Inspector

2 HSS 针对官方披露漏洞的修复建议

2.1 Git 用户凭证泄露漏洞（CVE-2020-5260）

2020年4月15日，Git发布安全通告公布了一个导致Git用户凭证泄露的漏洞（CVE-2020-5260）。Git使用凭证助手(credential helper)来帮助用户存储和检索凭证。

当URL中包含经过编码的换行符（%0a）时，可能将非预期的值注入到credential helper的协议流中。受影响Git版本对恶意URL执行git clone命令时，会触发此漏洞，攻击者可利用恶意URL欺骗Git客户端发送主机凭据。

漏洞编号

CVE-2020-5260

漏洞名称

Git用户凭证泄露漏洞

影响范围

影响版本

- Git 2.17.x <= 2.17.3
- Git 2.18.x <= 2.18.2
- Git 2.19.x <= 2.19.3
- Git 2.20.x <= 2.20.2
- Git 2.21.x <= 2.21.1
- Git 2.22.x <= 2.22.2
- Git 2.23.x <= 2.23.1
- Git 2.24.x <= 2.24.1
- Git 2.25.x <= 2.25.2
- Git 2.26.x <= 2.26.0

安全版本

- Git 2.17.4
- Git 2.18.3
- Git 2.19.4
- Git 2.20.3
- Git 2.21.2
- Git 2.22.3
- Git 2.23.2
- Git 2.24.2
- Git 2.25.3
- Git 2.26.1

官网解决方案

目前官方已在最新版本中修复了该漏洞，请受影响的用户及时升级到安全版本。

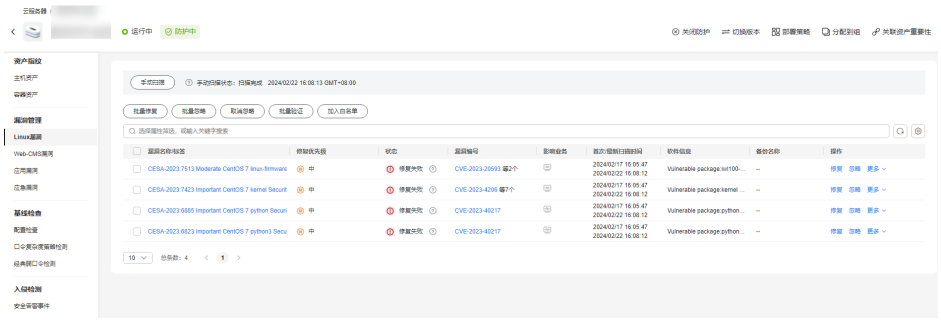
官方下载链接：**https://github.com/git/git/releases**

检测与修复建议

华为云企业主机安全对该漏洞的便捷检测与修复。

步骤1 检测并查看漏洞详情，如**图 手动检测漏洞**所示，详细的操作步骤请参见**查看漏洞详情**。

图 2-1 手动检测漏洞



步骤2 进行漏洞的修复与验证，详细的操作步骤请参见**漏洞修复与验证**。

----结束

其他防护建议

若您暂时无法进行升级操作，也可以采用以下方式进行防护：

- 方式一：使用以下命令禁用credential helper
  git config --unset credential.helper
  git config --global --unset credential.helper
  git config --system --unset credential.helper

- 方式二：提高警惕避免恶意URL
  a. 使用git clone时，检查URL的主机名和用户名中是否存在编码的换行符（%0a）或者凭据协议注入的证据（例如：host=github.com）。
  b. 避免将子模块与不受信任的仓库一起使用（不使用clone --recurse-submodules；只有在检查gitmodules中找到url之后，才使用git submodule update）。
  c. 请勿对不受信任的URL执行git clone。

2.2 SaltStack 远程命令执行漏洞（CVE-2020-11651/CVE-2020-11652）

近日，华为云关注到国外安全研究人员披露SaltStack存在两个严重的安全漏洞。Saltstack是基于python开发的一套C/S自动化运维工具，此次被爆当中存在身份验证绕过漏洞（CVE-2020-11651）和目录遍历漏洞（CVE-2020-11652），攻击者利用漏洞可实现远程命令执行、读取服务器上任意文件、获取敏感信息等。

华为云提醒使用SaltStack的用户尽快安排自检并做好安全加固。

漏洞编号

- CVE-2020-11651
- CVE-2020-11652

漏洞名称

SaltStack远程命令执行漏洞

影响范围

影响版本：

- 低于SaltStack 2019.2.4的版本
- 低于SaltStack 3000.2的版本

安全版本：

- SaltStack 2019.2.4
- SaltStack 3000.2

官网解决方案

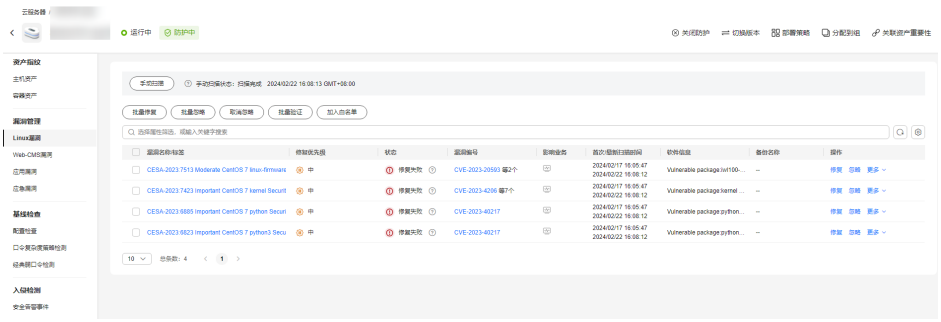
- 目前官方已在最新版本中修复了这两处漏洞，请受影响的用户及时升级到安全版本。
  下载地址：**https://repo.saltstack.com**。
- Salt Master默认监听端口为“4505”和“4506”，用户可通过配置安全组，禁止将其对公网开放，或仅对可信对象开放。

检测与修复建议

华为云企业主机安全对该漏洞的便捷检测与修复。

- 检测相关系统的漏洞，并查看漏洞详情，详细的操作步骤请参见**查看漏洞详情**。
  漏洞修复与验证，详细的操作步骤请参见**漏洞修复与验证**。

图 2-2 手动检测漏洞



- 检测主机是否开放了“4505”和“4506”端口。
  如果检测到开放了“4505”和“4506”端口，建议关闭该端口，或者仅对可信对象开放，详细的操作步骤请参见**查看主机资产指纹**。

图 2-3 主机指纹

- 检测利用此漏洞的挖矿木马，并通过控制台隔离查杀挖矿木马。
  隔离查杀挖矿木马，详细操作步骤请参见**隔离查杀**。

图 2-4 隔离查杀

2.3 OpenSSL 高危漏洞（CVE-2020-1967）

OpenSSL安全公告称存在一个影响OpenSSL 1.1.1d、OpenSSL 1.1.1e、OpenSSL 1.1.1f的高危漏洞（CVE-2020-1967），该漏洞可被用于发起DDoS攻击。

漏洞编号

CVE-2020-1967

漏洞名称

OpenSSL高危漏洞

影响范围

- OpenSSL 1.1.1d
- OpenSSL 1.1.1e
- OpenSSL 1.1.1f

官网解决方案

官方建议受影响的用户尽快安装最新的漏洞补丁。

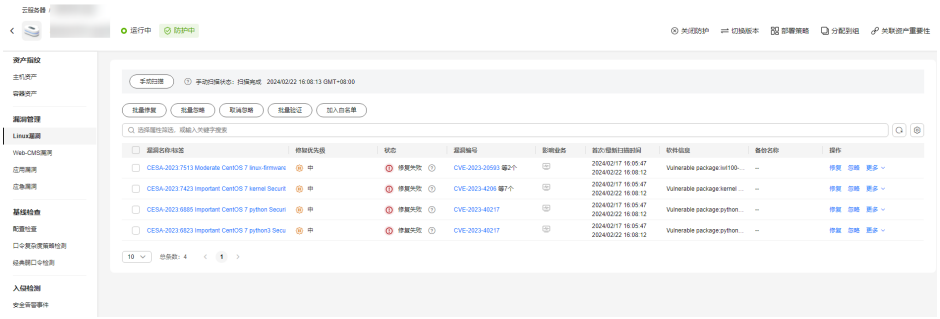
- https://www.debian.org/security/2020/dsa-4661
- https://security.gentoo.org/glsa/202004-10
- https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html

检测与修复建议

华为云企业主机安全支持对该漏洞的便捷检测与修复。

步骤1 检测并查看漏洞详情，如图 手动检测漏洞所示，详细的操作步骤请参见查看漏洞详情。

图 2-5 手动检测漏洞



步骤2 漏洞修复与验证，详细的操作步骤请参见漏洞修复与验证。

----结束

2.4 Adobe Font Manager 库远程代码执行漏洞（CVE-2020-1020/CVE-2020-0938）

当Windows Adobe Type Manager库未正确处理经特殊设计的多主机Adobe Type 1 PostScript格式字体时，Microsoft Windows中存在远程代码执行漏洞。

对于除Windows 10之外的所有系统，成功利用此漏洞的攻击者可以远程执行代码。对于运行Windows 10的系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在AppContainer沙盒上下文中执行代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新账户。

攻击者可通过多种方式利用此漏洞，包括诱导用户打开经特殊设计文档或在Windows预览窗格中查看。

漏洞编号

- CVE-2020-1020
- CVE-2020-0938

漏洞名称

Adobe Font Manager库远程代码执行漏洞

漏洞描述

- 对于除Windows 10之外的所有系统，成功利用远程代码执行漏洞的攻击者可以远程执行代码。
- 对于运行Windows 10的系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在AppContainer沙盒上下文中执行代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新账户。

影响范围

所有Windows系统

官方解决方案

官方建议受影响的用户尽快安装最新的漏洞补丁。

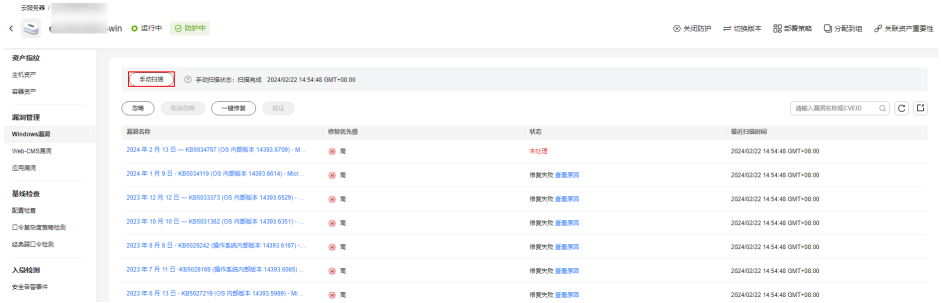
详情请参见**https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1020**。

检测与修复建议

华为云企业主机安全支持对该漏洞的便捷检测与修复。

步骤1 检测并查看漏洞详情，详细的操作步骤请参见**查看漏洞详情**。

图 2-6 手动检测漏洞



步骤2 漏洞修复与验证，详细的操作步骤请参见**漏洞修复与验证**。

----结束

2.5 Windows 内核特权提升漏洞（CVE-2020-1027）

Windows内核处理内存中对象的方式中存在特权提升漏洞，成功利用此漏洞的攻击者可能会利用提升的特权执行代码。

为了利用此漏洞，在本地经过身份验证的攻击者可能会运行经特殊设计应用程序。

漏洞编号

CVE-2020-1027

漏洞名称

Windows内核特权提升漏洞

漏洞描述

Windows内核处理内存中对象的方式中存在特权提升漏洞，成功利用此漏洞的攻击者可能会利用提升的特权执行代码。

影响范围

所有Windows系统

官方解决方案

官方建议受影响的用户尽快安装最新的漏洞补丁。

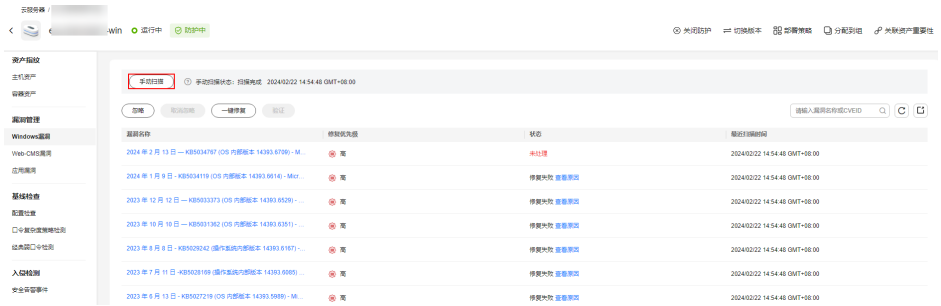
详情请参见**https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1027**。

检测与修复建议

华为云企业主机安全支持对该漏洞的便捷检测与修复。

步骤1 检测并查看漏洞详情，详细的操作步骤请参见**查看漏洞详情**。

图 2-7 手动检测漏洞



步骤2 漏洞修复与验证，详细的操作步骤请参见**漏洞修复与验证**。

----结束

2.6 Windows CryptoAPI 欺骗漏洞（CVE-2020-0601）

2020年1月15日，微软公布了1月的补丁更新列表，其中存在一个由NSA发现的、影响Microsoft Windows加密功能的高危漏洞（CVE-2020-0601）。该漏洞影响CryptoAPI椭圆曲线密码（ECC）证书检测机制，致使攻击者可以破坏Windows验证加密信任的过程，并可以导致远程代码执行。

漏洞编号

CVE-2020-0601

漏洞名称

Windows CryptoAPI欺骗漏洞（CVE-2020-0601）

漏洞描述

Windows CryptoAPI (Crypt32.dll) 验证椭圆曲线加密 (ECC) 证书的方式中存在欺骗漏洞。

攻击者可以通过使用欺骗性的代码签名证书，对恶意可执行文件进行签名来利用此漏洞，从而使该文件看似来自受信任的合法来源，用户将无法知道该文件是恶意文件。例如，攻击者可以通过该漏洞，让勒索木马等软件拥有看似“可信”的签名证书，从而绕过Windows的信任检测机制，误导用户安装。

攻击者还可以利用该漏洞进行中间人攻击，并对有关用户与受影响软件的连接的机密信息进行解密。影响Windows信任关系的一些实例，如用户常见的HTTPS连接、文件签名和电子邮件签名等。

影响范围

- Windows 10
- Windows Server 2016和Windows Server 2019版本
- 依赖于Windows CryptoAPI的应用程序。

官方解决方案

官方建议受影响的用户尽快安装最新的漏洞补丁。

详情请参见**https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0601**。

检测与修复建议

华为云企业主机安全提供了对该漏洞的便捷检测与修复。

在需要检测与修复的云主机上，已安装企业主机安全客户端（Agent），并开启防护。

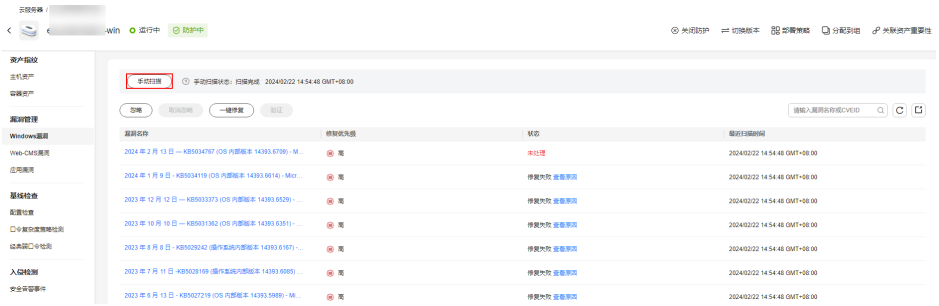
步骤1 登录管理控制台。

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

步骤3 单击左侧“主机管理”，在云服务器列表中，单击Windows操作系统主机的名称，查看主机详情。

步骤4 在详情页面，单击“漏洞管理 > Windows系统漏洞 > 手动检测”检测主机存在的漏洞。

图 2-8 手动检测漏洞



步骤5 检测完成后，可查看“解决方案”所在列的修复建议，根据修复建议修复漏洞。

步骤6 修复过程需要花费一段时间，修复完成后，请重启云主机使补丁生效。

步骤7 重启云主机后，再次单击“手动检测”，验证该漏洞是否修复成功。

说明

您也可以通过在企业主机安全中，选择“漏洞管理 > Windows系统漏洞管理”页签，进入漏洞管理页面，在漏洞列表右上角，输入漏洞名称。查看并修复该漏洞。

- Windows Server 2019：KB4534273
- Windows Server 2016：KB4534271

----结束

3 第三方主机通过专线和代理服务器接入 HSS

3.1 方案概述

应用场景

随着混合云的发展，用户对于云上云下或多云资源实现统一安全管理的需求也越发强烈。企业主机安全支持第三方云主机以及线下IDC接入纳管，用户可以通过一个控制台实现一致的主机安全防护策略，避免因为不同平台安全水位不一致导致的攻击风险。

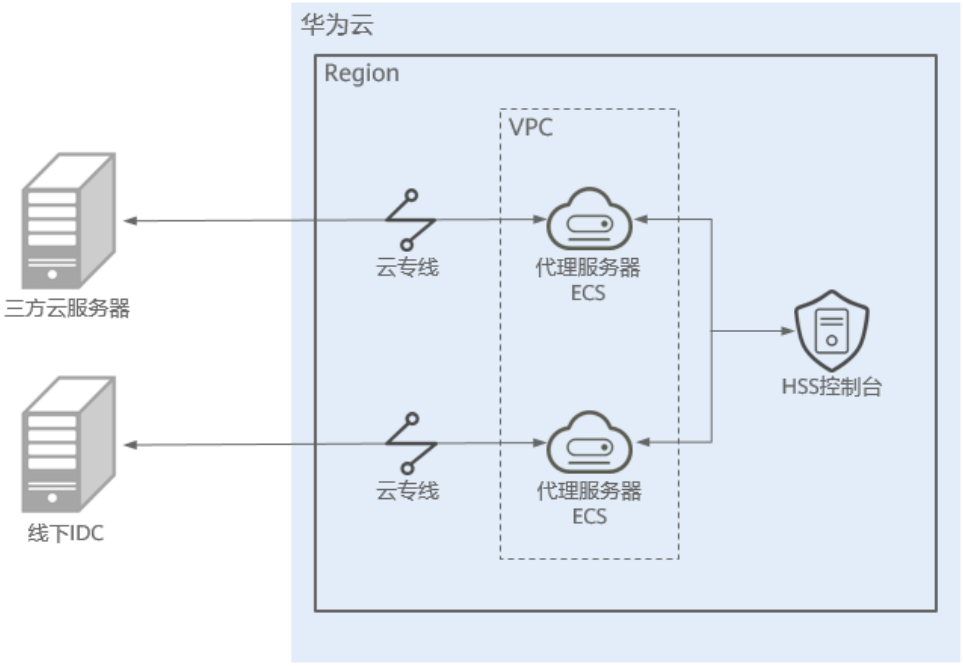
对于不能访问公网的第三方云主机、线下IDC，可以参考本方案通过“专线+代理”的方式接入HSS进行防护管理。如果您的主机能够访问公网，请参考**为第三方主机安装Agent**将主机接入HSS。

方案架构

第三方服务器通过云专线服务与云上VPC实现网络互通，再通过云上弹性云服务器代理接入HSS，如**图 第三方主机通过专线和代理服务器接入HSS**所示。

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

图 3-1 第三方主机通过专线和代理服务器接入 HSS



方案优势

本方案无区域限制，第三方主机可通过本方案接入任意区域。

3.2 资源和成本规划

本方案示例中涉及的资源如下：

表 3-1 资源说明

资源	资源说明	数量	成本说明
云专线（Direct Connect）	DC，作为连接第三方主机和云上资源的专属通道。	2	DC具体的计费方式及标准请参考**DC计费说明**。
弹性云服务器（Elastic Cloud Server）	ECS，作为代理服务器，将第三方服务器的请求转发至HSS后台。	2	ECS具体的计费方式及标准请参考**ECS计费说明**。

3.3 操作流程

第三方云主机、线下IDC通过专线和代理服务器接入HSS的流程如下：

1. **创建专线连接**
   第三方服务器如果不能访问公网，需要创建专线连接云上VPC，实现网络互通。

2. **创建代理服务器**
   需要创建一台云上服务器，作为代理服务器，连接第三方服务器。
3. **为代理服务器安装Agent**
   为代理服务器安装Agent，确保网络的畅通，辅助配置nginx的参数。
4. **为代理服务器安装配置nginx**
   nginx负责将第三方服务器的请求转发至HSS后台管理后台。
5. **通过代理服务器制作Agent安装包或安装命令**
   根据第三方服务器操作系统类型制作对应的安装命令（Linux）或安装包（Windows）。
6. **为第三方服务器安装Agent**
   为第三方服务器安装Agent，将第三方服务器接入HSS实现统一管理。

3.4 实施步骤

3.4.1 创建专线连接

在不使用公网的情况下，第三方云主机、线下IDC可以借助云专线服务，实现访问云上VPC内的服务器。

关于云专线服务的详细介绍请参见**云专线产品介绍**。

创建专线连接

详细的操作指导请参见**通过云专线实现云下IDC访问云上VPC（虚拟网关VGW）**。

步骤1 创建物理连接。

1. 登录管理控制台。
2. 单击管理控制台左上角的  ，选择区域和项目。
3. 单击页面左上方的  ，选择“网络 > 云专线”，进入“物理连接”页面。
4. 在物理连接页面，单击“创建物理连接”，在物理连接页面单击 “自建专线接入”，进入物理连接的端口购买页面。
5. 根据界面提示，在物理连接购买页面配置机房地址、华为云接入点、物理连接端口等信息，可参考**表3-2**输入相关参数。

图 3-2 购买物理连接

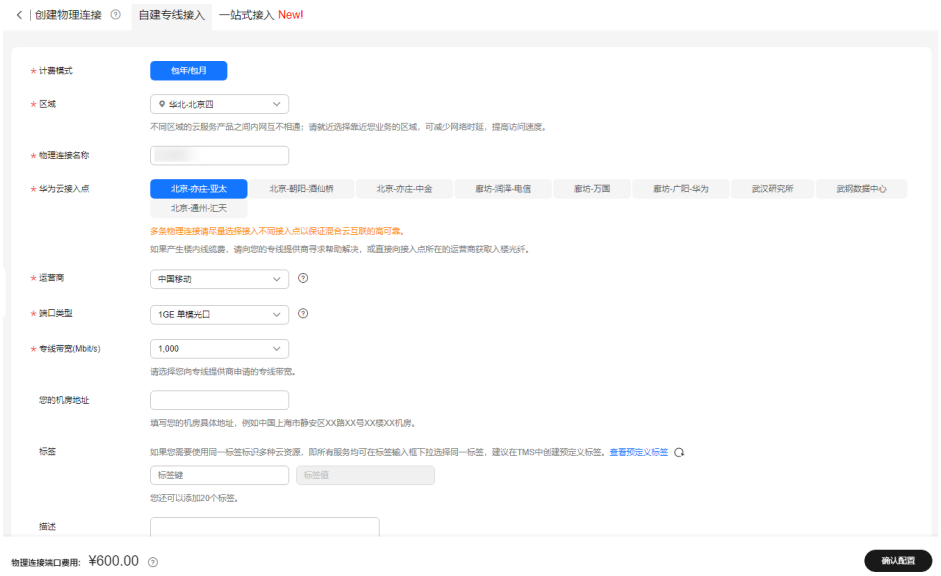


表 3-2 购买物理连接参数

参数	说明
计费模式	专线服务付费方式，目前仅支持包年/包月方式付费。
区域	物理连接开通的区域。用户可以在管理控制台左上角或购买页面切换区域。
物理连接名称	用户将要创建的物理连接的名称（可自定义）。
华为云接入点	物理连接接入点的位置。
运营商	提供物理连接的运营商。
端口类型	物理连接接入端口的类型：1GE，10GE、40GE、100GE。
专线带宽	物理连接的带宽大小，请在下拉框中选择对应的带宽。仅作为运营商接入带宽描述。
您的机房地址	用户填写机房地址，可精确到楼层。 例如上海市浦东新区华京路xx号xx楼xx机房。
标签	云专线服务的标识，包括键和值。可以为云专线服务创建10个标签。 **说明** 如果已经通过TMS的预定义标签功能预先创建了标签，则可以直接选择对应的标签键和值。 预定义标签的详细内容，请参见**预定义标签简介**。
描述	用户可以对物理连接添加备注信息。
联系人姓名/手机/Email	用户可以在此提供用户侧专线负责人信息。 注意：如不提供负责人信息，将只能通过账号信息查询，会增加需求确认时长。

参数	说明
购买时长	购买服务的时长。
自动续费	自动续费时长与购买时长相同。 例如：用户购买时长为三个月，当勾选该项后，将自动续费三个月，以此类推。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

6. 单击“确认配置”。
7. 确认配置信息，单击“提交需求”。
   用户提交需求后请联系专线经理与华为云侧确认专线需求。
8. 系统审核通过需求后，请用户自行联系运营商施工。
   运营商施工完成后，在控制台物理连接列表页，选择物理连接并单击“操作”列的“确认施工完成”。
9. 在确认运营商施工完成的弹窗中，单击“确认”。
10. 在物理连接列表页，选择物理连接并单击“操作”列的“确认配置”。
11. 确认物理连接配置信息，单击“立即支付”。
12. 确认订单信息，选择支付方式，单击“确认”。
13. 支付完成后，等待华为云施工。
    预计两个工作日内，华为驻场工程师会根据客户信息将专线对接到华为云的网关端口。
14. 施工完成后，物理连接接入状态显示为“正常”时，表示完成物理连接接入，同时开始计费。

步骤2 创建虚拟网关。

1. 在左侧导航栏，选择“云专线 > 虚拟网关”。
2. 在虚拟网关页面，单击右上角“创建虚拟网关”。
3. 根据界面提示，配置相关参数。

图 3-3 创建虚拟网关

表 3-3 虚拟网关参数

参数	说明
名称	虚拟网关名称。 字符长度为1~64。
企业项目	将虚拟网关加入已有的企业项目内，支持按企业项目维度管理资源。
虚拟私有云	虚拟网关所关联的虚拟私有云。
本端子网	云专线允许访问的VPC子网。 用户可以添加多个网段，以“,”隔开，使用一条专线访问多个VPC子网。
BGP ASN	虚拟网关的BGP AS号。
标签	为虚拟网关绑定标签，用来标识资源，支持修改。
描述	虚拟网关描述。

4. 单击“确定”。

步骤3 创建虚拟接口。

1. 在左侧导航栏，选择“云专线 > 虚拟接口”。
2. 在虚拟接口页面，单击右上角“创建虚拟接口”。
3. 根据界面提示，配置相关参数。

图 3-4 创建虚拟接口

表 3-4 创建虚拟接口参数

参数	说明
区域	物理连接开通的区域。用户可以在管理控制台左上角或购买页面切换区域。
名称	虚拟接口名称。 字符长度为1~64。
虚拟接口优先级	虚拟接口的优先级。支持选择“优先”或“普通”。 多个虚拟接口关联同一个专线设备，接口优先级相同时表示负载关系，接口优先级不同时表示主备关系。
物理连接	选择可用的物理连接。
网关	虚拟接口关联的网关。 支持选择虚拟网关或全域接入网关。
虚拟网关	当“网关”选择“虚拟网关”时需要配置该参数。 选择虚拟接口关联的虚拟网关。

参数	说明
全域接入网关	当“网关”选择“全域接入网关”时需要配置该参数。 选择虚拟接口关联的全域接入网关。
VLAN	虚拟接口的VLAN。 标准专线的虚拟接口的VLAN由用户配置 。 托管专线的虚拟接口的VLAN会使用运营商或合作伙伴为托管专线分配的VLAN，用户无需配置。
带宽	虚拟接口带宽，单位为Mbit/s。虚拟接口带宽不可以超过物理连接带宽。
企业项目	将虚拟接口加入已有的企业项目内，支持按企业项目维度管理资源。
标签	为虚拟接口绑定标签，用来标识资源，支持修改。
本端网关（华为云侧	华为云侧网络接口互联的IP地址，即华为云和客户线下机房对接时华为云侧设备接口的对接地址，配置后会自动下发到华为云侧网关设备。
远端网关（用户侧）	客户本地数据中心侧网络互联的IP地址，即华为云和客户线下机房对接时客户线下设备接口的对接地址，配置后需要客户自己配置在客户线下设备的接口上。
远端子网	用户数据中心的子网和子网掩码。多个远端子网时，请以逗号隔开。
路由模式	路由模式：静态路由/BGP 双线或者后期有冗余专线接入请选择BGP模式。
BGP邻居ASN	BGP邻居自治系统的标识。 当路由模式为BGP时，需要设置此参数。
BGP MD5认证密码	BGP邻居的MD5值即BGP密码。 当路由模式为BGP时，可设置此参数，两侧网关参数需保持一致。 字符长度为8~255，至少包含以下字符的两种： – 大写字母 – 小写字母 – 数字 – 特殊字符（ ~!,.:;-_"(){}[]/@#$%^&*+|= ）
描述	可自定义虚拟接口的相关描述。

4. 单击“立即创建”。

   当所创建的虚拟接口状态列为“正常”时，完成虚拟接口的创建。

步骤4 配置本地路由。

专线开通后，您需要配置本地数据中心路由：

- 静态路由详细请参考**用户单专线静态路由访问VPC**。
- BGP协议详细请参考**用户单专线BGP协议访问VPC**。

----结束

3.4.2 创建代理服务器

创建1台云上服务器，作为第三方服务器的代理服务器。

登录华为云控制台购买弹性云服务器，关于购买弹性服务器的详细介绍请参见**自定义购买弹性云服务器**。

须知

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

创建代理服务器

步骤1 登录控制台，进入**购买弹性云服务器**页面。

步骤2 在购买弹性云服务页面，设置购买参数。

- CPU架构：此处示例选择“x86计算”。
- 实例：此处示例选择“c6.xlarge.2”。
- 镜像：此处示例选择“公共镜像 > Huawei Cloud EulerOS 2.0 标准版 64位(40 GiB)”。
- 其他参数：根据界面提示，并结合实际情况设置。

步骤3 确认所有信息无误后，单击“立即购买”，在提示框中单击“同意并立即购买”，支付完成后，云服务器将自动创建，并默认开机。

----结束

3.4.3 为代理服务器安装 Agent

为代理服务器安装Agent，确保网络的畅通，辅助配置nginx的参数。

为代理服务器安装 Agent

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的  ，选择区域和项目。

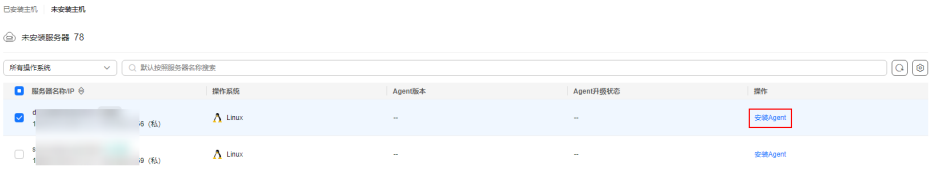
步骤3 单击页面左上方的  ，选择“安全与合规 > 企业主机安全”，进入“企业主机安全”页面。

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

步骤5 选择“Agent管理 > 未安装主机”，进入“未安装主机”页面。

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

图 3-5 安装 Agent



步骤7 选择并填写服务器验证信息。

- 选择服务器验证模式：根据服务器验证方式进行选择，此处示例选择“账号密码方式”。
- 允许以root权限直连：根据服务器是否允许以root直连决定是否勾选。此处示例“勾选”。
  - 服务器root密码：根据服务器实际信息进行填写。
  - 服务器登录端口：根据服务器实际登录端口进行填写。此处示例“22”端口。

图 3-6 填写服务器验证信息。

步骤8 单击“确定”，Agent开始安装。

步骤9 选择“已安装主机”页面，筛选查看目标服务器Agent状态。

Agent状态显示在线，表示Agent安装成功。

----结束

3.4.4 为代理服务器安装配置 nginx

nginx负责将第三方服务器的请求转发至HSS后台管理后台。

为代理服务器安装配置 nginx

步骤1 登录代理服务器

步骤2 检查yum源

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

远程登录代理服务器，执行以下命令检查yum源中是否存在nginx包。

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

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

图 3-7 nginx 包存在（rpm）

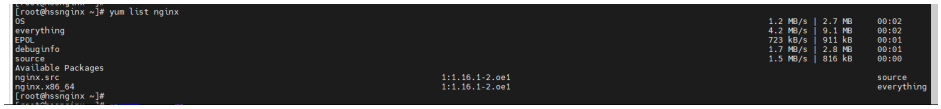
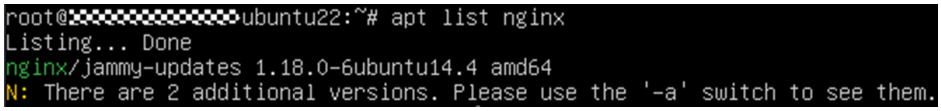


图 3-8 nginx 包存在（deb）



步骤3 安装nginx

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

   图 3-9 安装 nginx（yum）

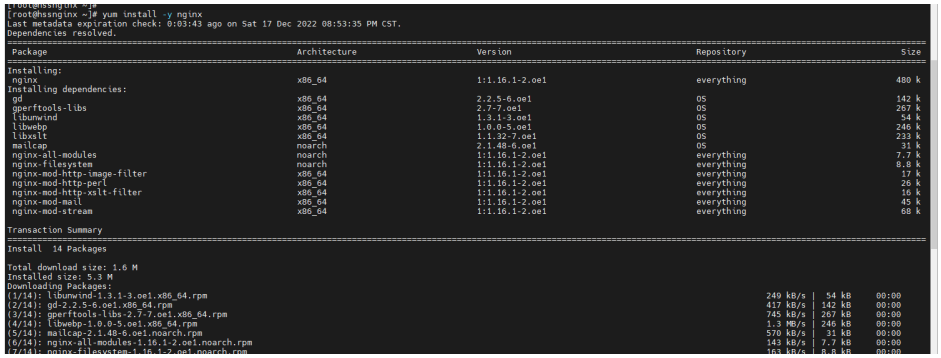
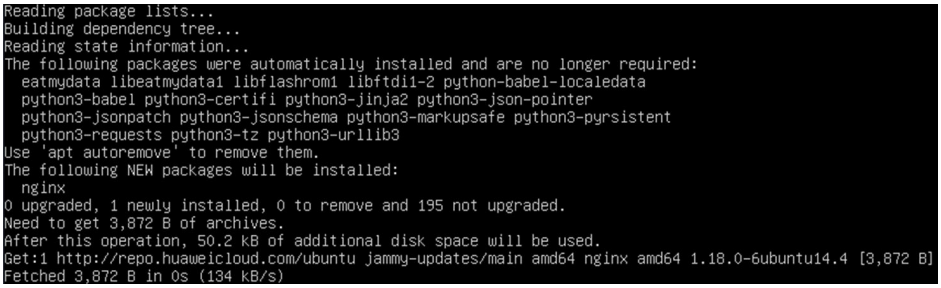
   

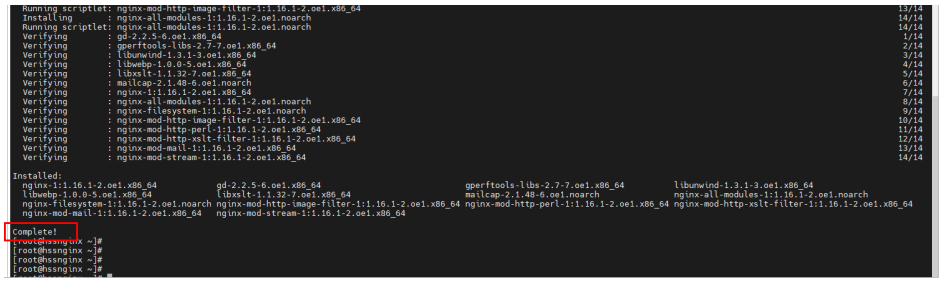
   图 3-10 安装 nginx（apt）

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

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

图 3-11 nginx 安装成功（rpm）



– Ubuntu、Debian等支持deb安装软件的OS：

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

图 3-12 nginx 安装成功（deb）

步骤4 配置Nginx

1. 执行以下命令进入nginx目录。

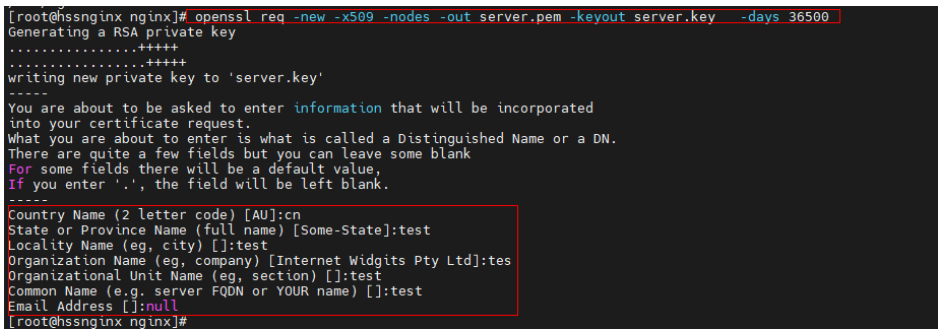
   cd /etc/nginx/

2. 执行以下命令完成证书自签。

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

   命令执行后需填写证书相关信息，自定义填写即可。

图 3-13 自签证书



说明

第一项Country Name受长度限制，只能填写两个字符。

3. 执行以下操作修改nginx.conf。

   a. 依次执行以下命令修改nginx.conf。

      rm -f nginx.conf

      vi nginx.conf

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


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

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

events {
    worker_connections 1024;
}

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

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

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

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

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

    upstream backend_hss {
        server ADDR:10180;
    }

    server {
        listen  10180;

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

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

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

        location / {

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

            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";

       }

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

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

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

:wq!

d. 执行以下命令自动替换nginx.conf中的地址。

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

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

a. 依次执行以下命令，创建nginx的监控脚本。

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

vi /etc/nginx/nginx_monitor.sh

图 3-14 创建 nginx 监控脚本

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

b. 将以下内容复制粘贴到nginx_monitor.sh中。

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

图 3-15 配置 nginx_monitor.sh

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

c. 粘贴完成后，按Esc键，输入以下命令，按回车键退出，完成配置。

:wq!

5. 等待1分钟后，执行以下命令查看nginx进程是否已经启动。

ps -ef | grep nginx

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

图 3-16 nginx 进程启动成功

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

----结束

3.4.5 通过代理服务器制作 Agent 安装包或安装命令

根据第三方服务器操作系统类型，通过代理服务器制作对应的Agent安装命令（Linux）或Agent安装包（Windows）。

通过代理服务器制作 Agent 安装命令（Linux）

步骤1 登录代理服务器

步骤2 执行以下命令进入tmp目录。

cd /tmp

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

echo `hostname -I` > private_ip.conf

cat private_ip.conf

图 3-17 查看 IP

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

须知

- 查看private_ip.conf中的IP是否为代理服务器实际可用IP，即第三方服务器需可以正常连接该IP。
- 如果该IP不是实际可用IP，需手动将该IP修改为实际可用IP。

步骤4 确认IP可用后，依次执行以下操作制作安装命令。

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

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

- x86 deb软件包镜像的命令：

  echo -e "# for Liunx x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh

- Arm rpm软件包镜像的命令：

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

- Arm deb软件包镜像的命令：

  echo -e "# for Liunx ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh

2. 执行以下命令，替换可用IP。

   无需修改，执行即可。

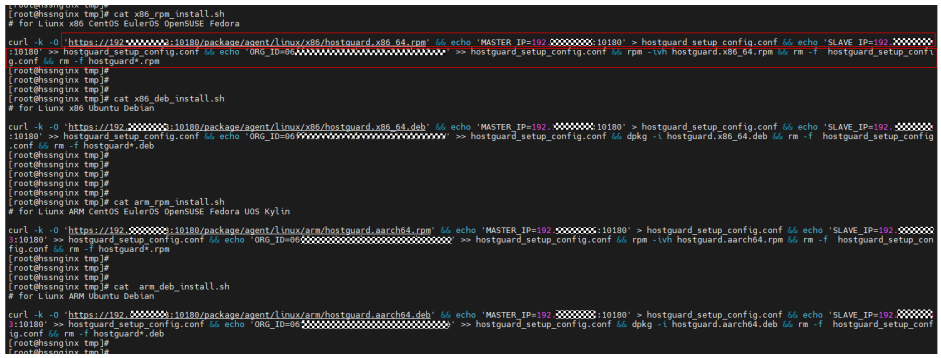
   sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat /usr/local/hostguard/run/metadata.conf | grep -v enterprise_project_id | grep project_id | cut -d ":" -f 2 | cut -d " " -f 2`#g" *install.sh

说明

- 上述5条命令需全部执行完成，最后一条“替换为可用IP”的命令必须执行且必须最后执行。
- x86_rpm_install.sh中的安装命令适用于x86架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora。
- x86_deb_install.sh中的安装命令适用于x86架构，deb软件包管理的镜像，如Ubuntu、Debian。
- arm_rpm_install.sh中的安装命令适用于arm架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora、UOS、Kylin。
- arm_deb_install.sh中的安装命令适用于arm架构，deb软件包管理的镜像，如Ubuntu、Debian。

步骤5 查看生成的命令，生成的目标命令将用于第三方Linux服务器Agent的安装使用。

图 3-18 Linux 安装命令



----结束

通过代理服务器制作 Agent 安装包（Windows）

步骤1 执行以下命令进入tmp目录。

```
cd /tmp
```

步骤2 依次执行以下命令，制作Windows的Agent安装压缩包。

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

```
zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini
```

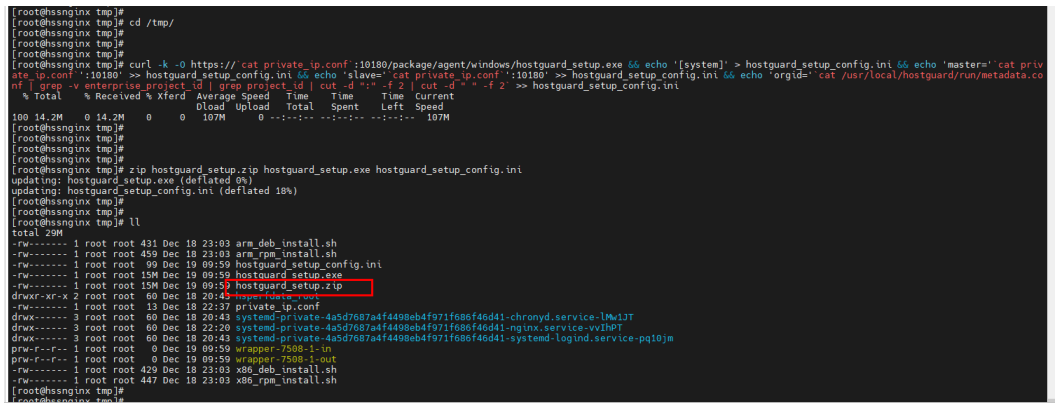
说明

如果代理服务器没有zip命令，需先执行以下命令安装zip插件。

```
yum install -y zip
```

步骤3 查看生成的安装包，将用于第三方Windows服务器Agent的安装使用。

图 3-19 Windows 安装包



----结束

3.4.6 为第三方服务器安装 Agent

为第三方服务器安装Agent，完成后可在HSS实现对服务器的统一管理。

为三方 Linux 服务器安装 Agent

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

步骤2 使用Root账号登录目标第三方Linux服务器，粘贴并执行Linux安装命令。

界面回显如**图 Agent安装完成**所示，表示Agent安装完成。

图 3-20 Agent 安装完成

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

步骤4 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

为三方 Windows 服务器安装 Agent

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

步骤2 将安装包上传到需要安装Agent的目标第三方Windows服务器。

步骤3 使用Administrator账号登录第三方服务器。

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

须知

生成的zip安装包拷贝到本地后一定要进行解压后再执行安装，否则将无法安装。

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

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

步骤7 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

4 第三方主机通过专线和 VPC 终端节点接入 HSS

4.1 方案概述

应用场景

随着混合云的发展，用户对于云上云下或多云资源实现统一安全管理的需求也越发强烈。企业主机安全支持第三方云主机以及线下IDC接入纳管，用户可以通过一个控制台实现一致的主机安全防护策略，避免因为不同平台安全水位不一致导致的攻击风险。

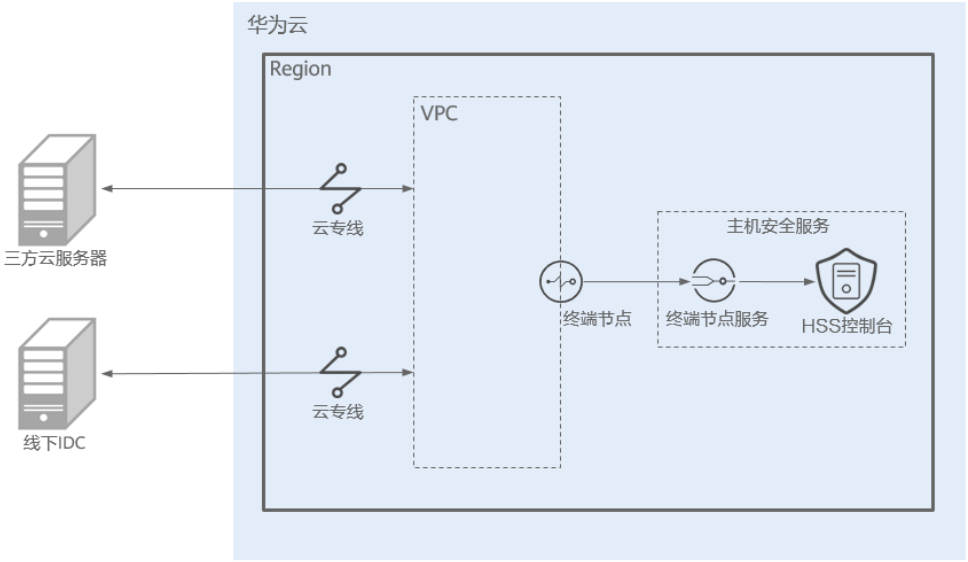
如果您的主机不能访问公网，可以参考本方案通过“专线+VPC终端节点”的方式接入HSS进行防护管理。如果您的主机能够访问公网，请参考**为第三方主机安装Agent**将主机接入HSS。

方案架构

第三方服务器通过云专线服务与云上VPC实现网络互通，再通过VPC终端节点接入HSS，如**图 第三方主机通过专线和VPC终端节点接入HSS**所示。

- **云专线**（Direct Connect），用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。
- **VPC终端节点**（VPC Endpoint），可以在VPC内提供便捷、安全、私密的通道与终端节点服务（华为云服务、用户私有服务）进行连接，该服务使用华为云内部网络，无需弹性公网IP。

图 4-1 第三方主机通过专线和 VPC 终端节点接入 HSS



方案优势

相较于**第三方主机通过专线和代理服务器接入HSS**方案，本方案无需创建代理服务器和配置nginx，操作更简单，成本更低。

约束与限制

目前暂仅“华东二”、“西南-贵阳一”区域，支持第三方主机通过专线和VPC终端节点接入HSS。

4.2 资源和成本规划

本方案示例中涉及的资源如下：

表 4-1 资源说明

资源	资源说明	数量	成本说明
云专线（Direct Connect）	DC，作为连接第三方主机和云上资源的专属通道。	2	DC具体的计费方式及标准请参考**DC计费说明**。
VPC终端节点（VPC Endpoint）	VPCEP，在VPC内提供通道与终端节点服务进行连接，实现第三主机可通过华为云内网访问HSS。	1	免费。

4.3 操作流程

第三方云主机、线下IDC通过专线和VPC终端节点接入HSS的流程如下：

1. **创建专线连接**
   第三方服务器如果不能访问公网，需要创建专线连接云上VPC，实现网络互通。
2. **创建VPC终端节点**
   创建VPC终端节点，用于实现第三方服务器通过华为云内网访问HSS。
3. **获取项目ID**
   获取VPC终端节点所在的项目ID，用于制作安装命令。
4. **制作Agent安装包或安装命令**
   根据第三方服务器操作系统类型制作对应的安装命令（Linux）或安装包（Windows）。
5. **为第三方服务器安装Agent**
   为第三方服务器安装Agent，将第三方服务器接入HSS实现统一管理。

4.4 实施步骤

4.4.1 创建专线连接

在不使用公网的情况下，第三方云主机、线下IDC可以借助云专线服务，实现访问云上VPC内的服务器。

关于云专线服务的详细介绍请参见**云专线产品介绍**。

创建专线连接

详细的操作指导请参见**通过云专线实现云下IDC访问云上VPC（虚拟网关VGW）**。

步骤1 创建物理连接。

1. 登录管理控制台。
2. 单击管理控制台左上角的  ，选择区域和项目。
3. 单击页面左上方的  ，选择“网络 > 云专线”，进入“物理连接”页面。
4. 在物理连接页面，单击“创建物理连接”，在物理连接页面单击 “自建专线接入”，进入物理连接的端口购买页面。
5. 根据界面提示，在物理连接购买页面配置机房地址、华为云接入点、物理连接端口等信息，可参考**表4-2**输入相关参数。

图 4-2 购买物理连接

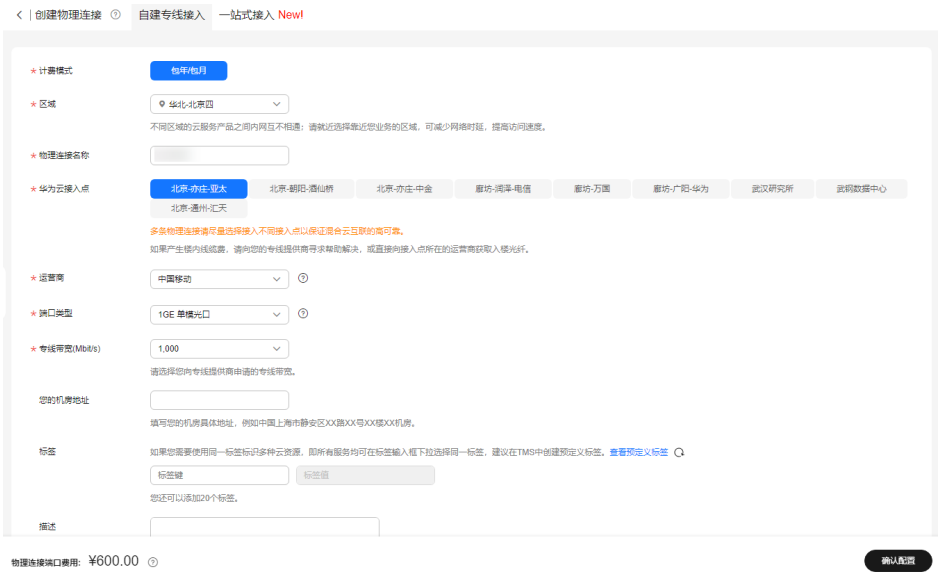


表 4-2 购买物理连接参数

参数	说明
计费模式	专线服务付费方式，目前仅支持包年/包月方式付费。
区域	物理连接开通的区域。用户可以在管理控制台左上角或购买页面切换区域。
物理连接名称	用户将要创建的物理连接的名称（可自定义）。
华为云接入点	物理连接接入点的位置。
运营商	提供物理连接的运营商。
端口类型	物理连接接入端口的类型：1GE，10GE、40GE、100GE。
专线带宽	物理连接的带宽大小，请在下拉框中选择对应的带宽。仅作为运营商接入带宽描述。
您的机房地址	用户填写机房地址，可精确到楼层。 例如上海市浦东新区华京路xx号xx楼xx机房。
标签	云专线服务的标识，包括键和值。可以为云专线服务创建10个标签。 **说明** 如果已经通过TMS的预定义标签功能预先创建了标签，则可以直接选择对应的标签键和值。 预定义标签的详细内容，请参见**预定义标签简介**。
描述	用户可以对物理连接添加备注信息。
联系人姓名/手机/Email	用户可以在此提供用户侧专线负责人信息。 注意：如不提供负责人信息，将只能通过账号信息查询，会增加需求确认时长。

参数	说明
购买时长	购买服务的时长。
自动续费	自动续费时长与购买时长相同。 例如：用户购买时长为三个月，当勾选该项后，将自动续费三个月，以此类推。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

6. 单击“确认配置”。
7. 确认配置信息，单击“提交需求”。
   用户提交需求后请联系专线经理与华为云侧确认专线需求。
8. 系统审核通过需求后，请用户自行联系运营商施工。
   运营商施工完成后，在控制台物理连接列表页，选择物理连接并单击“操作”列的“确认施工完成”。
9. 在确认运营商施工完成的弹窗中，单击“确认”。
10. 在物理连接列表页，选择物理连接并单击“操作”列的“确认配置”。
11. 确认物理连接配置信息，单击“立即支付”。
12. 确认订单信息，选择支付方式，单击“确认”。
13. 支付完成后，等待华为云施工。
    预计两个工作日内，华为驻场工程师会根据客户信息将专线对接到华为云的网关端口。
14. 施工完成后，物理连接接入状态显示为“正常”时，表示完成物理连接接入，同时开始计费。

步骤2 创建虚拟网关。

1. 在左侧导航栏，选择“云专线 > 虚拟网关”。
2. 在虚拟网关页面，单击右上角“创建虚拟网关”。
3. 根据界面提示，配置相关参数。

图 4-3 创建虚拟网关

表 4-3 虚拟网关参数

参数	说明
名称	虚拟网关名称。 字符长度为1~64。
企业项目	将虚拟网关加入已有的企业项目内，支持按企业项目维度管理资源。
虚拟私有云	虚拟网关所关联的虚拟私有云。
本端子网	云专线允许访问的VPC子网。 用户可以添加多个网段，以“,”隔开，使用一条专线访问多个VPC子网。
BGP ASN	虚拟网关的BGP AS号。
标签	为虚拟网关绑定标签，用来标识资源，支持修改。
描述	虚拟网关描述。

4. 单击“确定”。

步骤3 创建虚拟接口。

1. 在左侧导航栏，选择“云专线 > 虚拟接口”。
2. 在虚拟接口页面，单击右上角“创建虚拟接口”。
3. 根据界面提示，配置相关参数。

图 4-4 创建虚拟接口

表 4-4 创建虚拟接口参数

参数	说明
区域	物理连接开通的区域。用户可以在管理控制台左上角或购买页面切换区域。
名称	虚拟接口名称。 字符长度为1~64。
虚拟接口优先级	虚拟接口的优先级。支持选择“优先”或“普通”。 多个虚拟接口关联同一个专线设备，接口优先级相同时表示负载关系，接口优先级不同时表示主备关系。
物理连接	选择可用的物理连接。
网关	虚拟接口关联的网关。 支持选择虚拟网关或全域接入网关。
虚拟网关	当“网关”选择“虚拟网关”时需要配置该参数。 选择虚拟接口关联的虚拟网关。

参数	说明
全域接入网关	当“网关”选择“全域接入网关”时需要配置该参数。 选择虚拟接口关联的全域接入网关。
VLAN	虚拟接口的VLAN。 标准专线的虚拟接口的VLAN由用户配置 。 托管专线的虚拟接口的VLAN会使用运营商或合作伙伴为托管专线分配的VLAN，用户无需配置。
带宽	虚拟接口带宽，单位为Mbit/s。虚拟接口带宽不可以超过物理连接带宽。
企业项目	将虚拟接口加入已有的企业项目内，支持按企业项目维度管理资源。
标签	为虚拟接口绑定标签，用来标识资源，支持修改。
本端网关（华为云侧	华为云侧网络接口互联的IP地址，即华为云和客户线下机房对接时华为云侧设备接口的对接地址，配置后会自动下发到华为云侧网关设备。
远端网关（用户侧）	客户本地数据中心侧网络互联的IP地址，即华为云和客户线下机房对接时客户线下设备接口的对接地址，配置后需要客户自己配置在客户线下设备的接口上。
远端子网	用户数据中心的子网和子网掩码。多个远端子网时，请以逗号隔开。
路由模式	路由模式：静态路由/BGP 双线或者后期有冗余专线接入请选择BGP模式。
BGP邻居ASN	BGP邻居自治系统的标识。 当路由模式为BGP时，需要设置此参数。
BGP MD5认证密码	BGP邻居的MD5值即BGP密码。 当路由模式为BGP时，可设置此参数，两侧网关参数需保持一致。 字符长度为8~255，至少包含以下字符的两种： – 大写字母 – 小写字母 – 数字 – 特殊字符（ ~!,.:;-_"(){}[]/@#$%^&*+|= ）
描述	可自定义虚拟接口的相关描述。

4. 单击“立即创建”。
   当所创建的虚拟接口状态列为“正常”时，完成虚拟接口的创建。

步骤4 配置本地路由。

专线开通后，您需要配置本地数据中心路由：

- 静态路由详细请参考**用户单专线静态路由访问VPC**。
- BGP协议详细请参考**用户单专线BGP协议访问VPC**。

----结束

4.4.2 创建 VPC 终端节点

创建VPC终端节点，用于实现第三方服务器通过华为云内网访问HSS。创建一个VPC终端节点，将占用一个虚拟私有云子网IP。每个虚拟私有云仅需创建一个终端节点。

创建 VPC 终端节点

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域和项目。

步骤3 单击页面左上方的，选择“网络 > VPC终端节点”，进入“终端节点”页面。

步骤4 在页面右上方，单击“购买终端节点”，进入购买“终端节点”页面。

步骤5 根据页面信息，配置购买参数。

1. 区域：选择“华东二”或“西南-贵阳一”。请根据主机要接入的区域选择。
2. 服务类别：选择“云服务”。
3. 选择服务：
   - 选择“com.myhuaweicloud.xxx.hss-agent”，其中“xxx”表示Region ID，例如华东二的Region ID为cn-east-4。
   - 勾选“创建内网域名”。
4. 虚拟私有云：选择与您主机网络互通的私有云。
5. 子网：选择或创建一个子网。
6. IPv4：选择“自动分配IPv4”。
7. 其他参数：根据界面提示按需配置。

步骤6 单击“立即购买”，完成订单提交。

步骤7 返回“终端节点”页面，确认终端节点创建完成，获取并记录服务地址（即IP）。

服务地址在后续制作安装包或安装命令时，需要使用。

----结束

4.4.3 获取项目 ID

步骤1 登录管理控制台。

步骤2 鼠标悬停在右上角的用户名，选择下拉列表中的“我的凭证”。

步骤3 在“API凭证”页面的项目列表中获取项目ID。

您创建的VPC终端节点所属哪个区域，就获取对应区域的项目ID。

图 4-5 获取项目 ID

----结束

4.4.4 制作 Agent 安装包或安装命令

使用1台Linux服务器，制作Agent安装命令（Linux）或Agent安装包（Windows）。

制作 Agent 安装命令（Linux）

步骤1 登录任一Linux服务器。

步骤2 执行以下命令进入tmp目录。

cd /tmp

步骤3 依次执行以下命令，将VPC终端节点IP写入private_ip.conf文件，将项目ID写入project_id.conf文件。

echo "{VPC终端节点ip}" > private_ip.conf

cat private_ip.conf

echo "{项目ID}" > project_id.conf

cat project_id.conf

须知

上述命令中的“终端节点IP”和“项目ID”，请根据实际情况改写。

- VPC终端节点IP即执行**创建VPC终端节点**操作时，您获取的服务地址。
- 项目ID即执行**获取项目ID**操作时，您获取的项目ID。

步骤4 依次执行以下操作制作安装命令。

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

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

echo -e "# for Liunx x86 Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/x86/hostguard.x86_64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > x86_deb_install.sh

- Arm rpm软件包镜像的命令：

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

- Arm deb软件包镜像的命令：

  echo -e "# for Liunx ARM Ubuntu Debian\n\ncurl -k -O 'https://private_ip:10180/package/agent/linux/arm/hostguard.aarch64.deb' && echo 'MASTER_IP=private_ip:10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=private_ip:10180' >> hostguard_setup_config.conf && echo 'ORG_ID=project_id' >> hostguard_setup_config.conf && dpkg -i hostguard.aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb" > arm_deb_install.sh

2. 执行以下命令，替换VPC终端节点IP和项目ID。

   无需修改，执行即可。

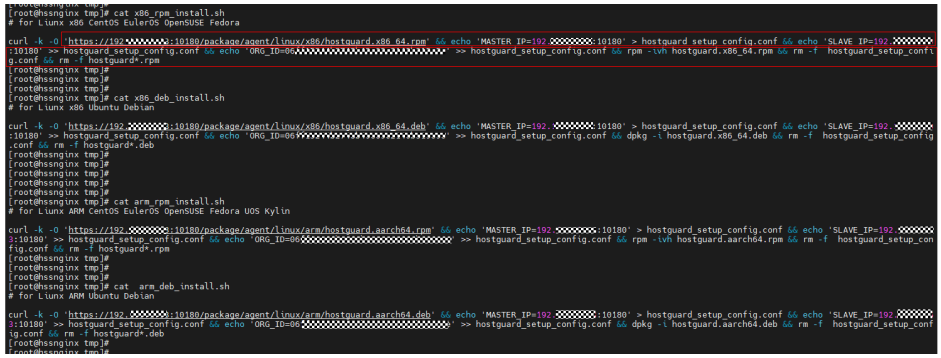
   sed -i "s#private_ip#`cat private_ip.conf`#g" *install.sh && sed -i "s#project_id#`cat project_id.conf`#g" *install.sh

说明

- 上述5条命令需全部执行完成，最后一条“替换VPC终端节点IP和项目”的命令必须执行且必须最后执行。
- x86_rpm_install.sh中的安装命令适用于x86架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora。
- x86_deb_install.sh中的安装命令适用于x86架构，deb软件包管理的镜像，如Ubuntu、Debian。
- arm_rpm_install.sh中的安装命令适用于arm架构，rpm软件包管理的镜像，如CentOS、EulerOS、OpenSUSE、Fedora、UOS、Kylin。
- arm_deb_install.sh中的安装命令适用于arm架构，deb软件包管理的镜像，如Ubuntu、Debian。

步骤5 查看生成的命令，生成的目标命令将用于第三方Linux服务器Agent的安装使用。

图 4-6 Linux 安装命令



----结束

制作 Agent 安装包（Windows）

步骤1 登录任一Linux服务器

步骤2 执行以下命令进入tmp目录。

cd /tmp

步骤3 依次执行以下命令，制作Windows的Agent安装压缩包。

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

zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini

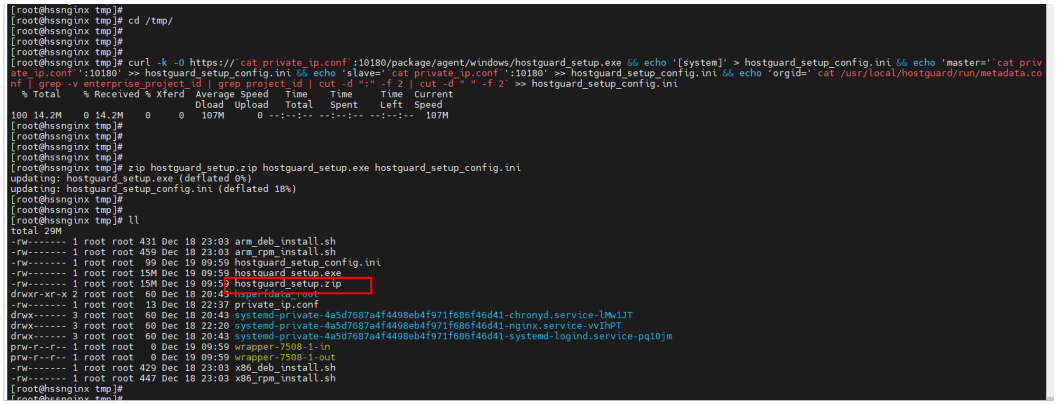
说明

如果代理服务器没有zip命令，需先执行以下命令安装zip插件。

yum install -y zip

步骤4 查看生成的安装包，将用于第三方Windows服务器Agent的安装使用。

图 4-7 Windows 安装包



----结束

4.4.5 为第三方服务器安装 Agent

为第三方服务器安装Agent，完成后可在HSS实现对服务器的统一管理。

为三方 Linux 服务器安装 Agent

步骤1 复制**制作Agent安装命令（Linux）**制作的Linux安装命令。

步骤2 使用Root账号登录目标第三方Linux服务器，粘贴并执行Linux安装命令。

界面回显如**图 Agent安装完成**所示，表示Agent安装完成。

图 4-8 Agent 安装完成

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

步骤4 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

为三方 Windows 服务器安装 Agent

步骤1 将**制作Agent安装包（Windows）**制作的Windows安装包，拷贝到本地PC机。

步骤2 将安装包上传到需要安装Agent的目标第三方Windows服务器。

步骤3 使用Administrator账号登录第三方服务器。

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

须知

生成的zip安装包拷贝到本地后一定要进行解压后再执行安装，否则将无法安装。

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

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

步骤7 查看目标服务器已显示在服务器列表中，表示接入成功。

----结束

5 通过 CBH 安装 HSS 的 Agent

应用场景

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

前提条件

- 已购买云堡垒机（Cloud Bastion Host，CBH）**专业版，**并通过云堡垒机纳管主机资源。

  具体操作请参见**购买云堡垒机**和**通过云堡垒机纳管主机资源**。
- 待安装Agent的主机为SSH协议类型的Linux主机，且主机网络连接正常。
- 已获取云堡垒机的系统管理员账号。

操作步骤

步骤1 使用系统管理员账号**登录云堡垒机系统**。

步骤2 在左侧导航栏，选择“运维 > 快速运维”，进入“快速运维”界面。

步骤3 选择“脚本控制台”页签。

图 5-1 进入脚本控制台

步骤4 配置脚本运维信息。相关参数说明请参见**表 脚本运维参数说明**。

图 5-2 配置脚本运维信息

表 5-1 脚本运维参数说明

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

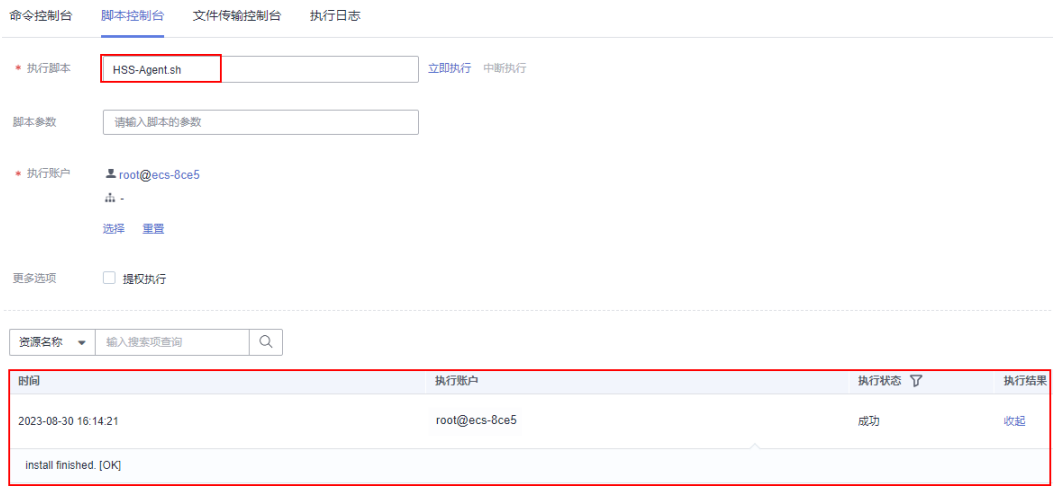
步骤5 单击“立即执行”，执行脚本任务。

图 5-3 执行脚本任务

步骤6 脚本任务执行成功后，在执行结果列单击“展开”，展开执行结果。

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

图 5-4 脚本任务执行成功



步骤7 在企业主机安全控制台，确认Agent安装结果。

1. 登录企业主机安全控制台。
2. 在左侧导航栏，选择“资产管理 > 主机管理”，进入“主机管理”界面。
3. 在“云服务器”页签，查看目标主机的Agent状态。如**图 查看Agent状态**所示。Agent状态为“在线”，表示Agent安装成功。

图 5-5 查看 Agent 状态

----结束

6 使用 HSS 增强主机登录安全

应用场景

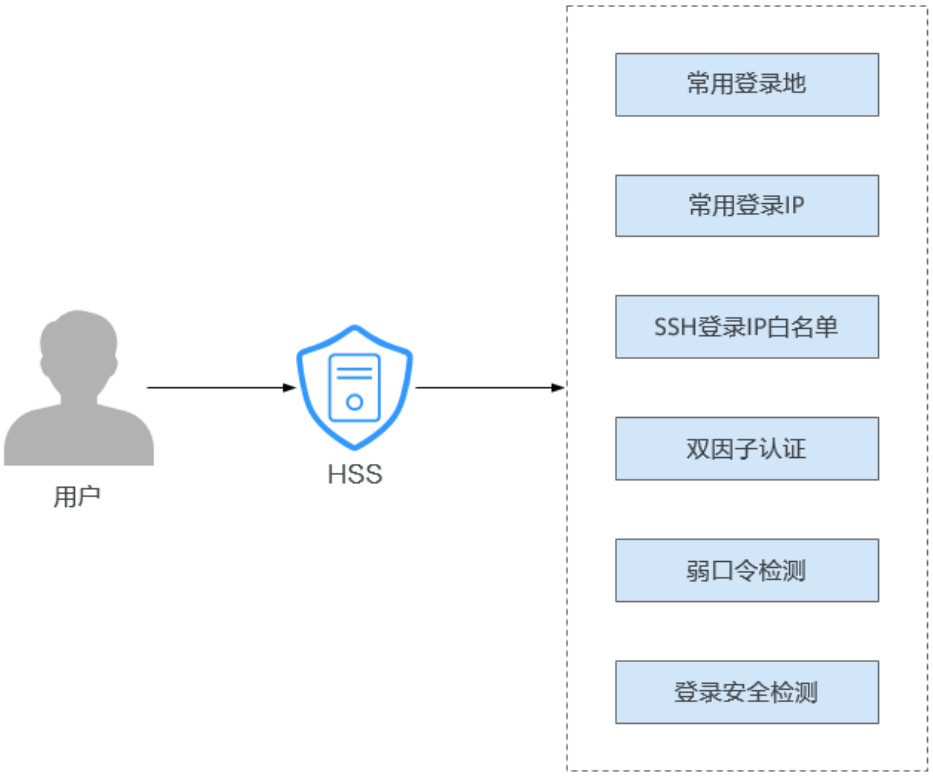
在主机被入侵、破解成功前，通常攻击者是以账号、密码为首要目标进行攻击，因此，增强主机登录时的安全性成为了防护主机安全、保证业务正常运行的第一道安全门。

本方案为您介绍如何通过HSS增强主机登录安全。

方案架构及优势

您可在企业主机安全通过配置常用登录地、常用登录IP、SSH登录IP白名单、双因子认证、弱口令检测、登录安全检测来增强服务器登录时的安全性。

图 6-1 主机登录安全加固



- 常用登录地

  配置常用登录地后，企业主机安全将对非常用登录地登录云服务器的行为进行告警。

- 常用登录IP

  配置常用登录IP后，企业主机安全将对非常用IP登录服务器的行为进行告警。

- SSH登录IP白名单

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

- 双因子认证

  双因子认证功能是一种双因素身份验证机制，结合短信/邮箱验证码，对云服务器登录行为进行二次认证，极大地增强云服务器账户安全性。

- 弱口令检测

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

  企业主机安全默认会对使用经典弱口令的用户账号告警，主动检测出主机中使用经典弱口令的账号。您也可以将疑似被泄露的口令自行添加在自定义弱口令列表中，防止主机中的账户使用该弱口令，给主机带来危险。

- 登录安全检测

  配置登录安全检测策略后，可为目标服务器开启登录安全检测，可有效检测暴破攻击，自动阻断暴破IP，触发告警并上报。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护。详细操作请参见**HSS接入概述**。

约束与限制

- 开启双因子认证后，仅以下登录方式支持双因子认证：
  - Linux：使用SSH密码方式登录云服务器，且OpenSSH版本小于8。
  - Windows：使用RDP文件登录Windows云服务器。
- Windows主机使用双因子认证功能时，不支持使用Windows系统的“用户每次登录时须更改密码”功能，如果您需要正常使用该功能，须关闭双因子认证。
- 在Windows主机上，双因子认证功能可能会和“网防G01”软件、服务器版360安全卫士存在冲突，建议停止“网防G01”软件和服务器版360安全卫士。

实施步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的  ，选择区域和项目。

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

步骤4 配置常用登录地

单一账号最多可添加10个常用登录地。

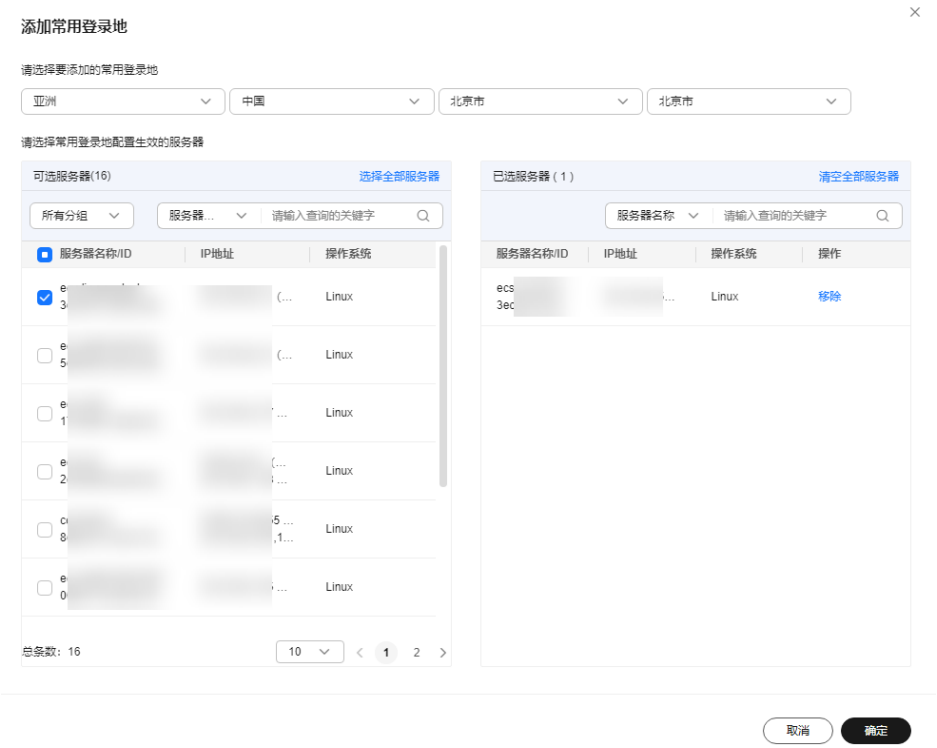
1. 在左侧导航栏，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”页面。
2. 选择“安全配置 > 常用登录地”，进入“常用登录地”页面。
3. 单击“添加常用登录地”，弹出“添加常用登录地”对话框。

图 6-2 添加常用登录地

4. 在对话框中，选择要添加的常用登录地和常用登录地生效的服务器，确认无误后单击“确定”，添加完成。

   常用登录地生效的服务器可选择多个。

图 6-3 填写常用登录地信息



5. 返回“常用登录地”页面，查看到新增的常用登录地，表示添加成功。

步骤5 配置常用登录IP

单一账号最多可添加20个常用登录IP。

1. 选择“安全配置 > 常用登录IP”，进入“常用登录IP”页面。
2. 单击“添加常用登录IP”，弹出“添加常用登录IP”对话框。

图 6-4 添加常用登录 IP

3. 在对话框中，输入“常用登录IP”，勾选需要生效的云服务器，确认无误后单击“确定”，添加完成。

说明

- “常用登录IP”必须填写公网IP或者IP段。
- 生效服务器可选择多个。
- 单次只能添加一个IP，若需添加多个IP，需重复操作添加动作，直至全部IP添加完成。

图 6-5 填写常用登录 IP

4. 返回“常用登录IP”页面，查看到新增的常用登录IP，表示添加成功。

步骤6 配置SSH登录IP白名单

说明

- 单一账号最多可添加10个SSH登录IP白名单。
- 使用鲲鹏计算EulerOS（EulerOS with Arm）的主机，SSH登录IP白名单功能对其不生效。
- 配置了白名单的服务器，只允许白名单内的IP通过SSH登录到服务器，拒绝白名单以外的IP：
  - 启用该功能时请确保将所有需要发起SSH登录的IP地址都加入白名单中，否则您将无法SSH远程登录您的服务器。

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

1. 选择“安全配置 > SSH登录IP白名单”，进入“SSH登录IP白名单”页面。
2. 单击“添加白名单IP”，弹出“添加白名单IP”对话框。

图 6-6 添加 IP 白名单

3. 在对话框中，输入“白名单IP”，勾选需要生效的云服务器，确认无误后单击“确定”，添加完成。

说明

- “常用登录IP”必须填写公网IP或者IP段。
- 生效服务器可选择多个。
- 单次只能添加一个IP，若需添加多个IP，需重复操作添加动作，直至全部IP添加完成。

图 6-7 填写白名单 IP 信息

4. 返回“SSH登录IP白名单”页面，查看到新增的白名单IP，表示添加成功。

步骤7 配置双因子认证

1. 选择“双因子认证”，进入“双因子认证”页面。
2. 在目标服务器所在行的“操作”列，单击“开启双因子认证”，弹出“开启双因子认证”对话框。

   您也可以勾选多台目标服务器，单击列表上方“开启双因子认证”，批量开启多台服务器双因子认证。

图 6-8 开启双因子认证

3. 在对话框中，选择“验证方式”。
   - **短信邮件验证**

     短信邮件验证需要选择消息通知服务主题。

     - 下拉框只展示状态已确认的消息通知服务主题。
     - 如果没有主题，请单击“查看消息通知服务主题”进行创建。具体操作请参见**创建主题**。
     - 如果您的主题中包含多个手机号码/邮箱，在双因子认证过程中：
       - 填写手机号码进行验证时，该主题内的所有订阅终端（手机号、邮箱）都会收到系统发出的验证码消息。

- 填写邮箱进行验证时，仅该验证邮箱会收到系统发出的验证码邮件。

如果您只希望一个手机号码收到验证码，请修改对应主题，仅在主题中保留您希望收到验证码的手机号码。

图 6-9 短信邮件验证

- **验证码验证**

  选择验证码验证，仅通过实时收到的验证码进行验证。

图 6-10 验证码验证

4. 单击“确定”，完成开启双因子认证的操作。
5. 返回“双因子认证”页面，查看目标服务器“双因子认证状态”变更为“开启”，表示开启成功。

   开启双因子认证成功后，需要等大约5分钟才生效。

须知

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

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

步骤8 配置弱口令检测

1. 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”页面。
2. 单击目标策略组名称，进入策略列表页面。

   可根据默认“策略组描述”及“支持的版本”判断目标策略适配的操作系统及防护版本。

   说明

   若有特殊需求需要新建策略组，您可在**创建策略组**后按照此步骤进行操作配置。
3. 单击“策略名称”为“弱口令检测”的名称，弹出“弱口令检测”对话框。
4. 根据业务实际情况修改“策略内容”中的参数，参数说明如**表6-1**所示。

图 6-11 修改弱口令检测

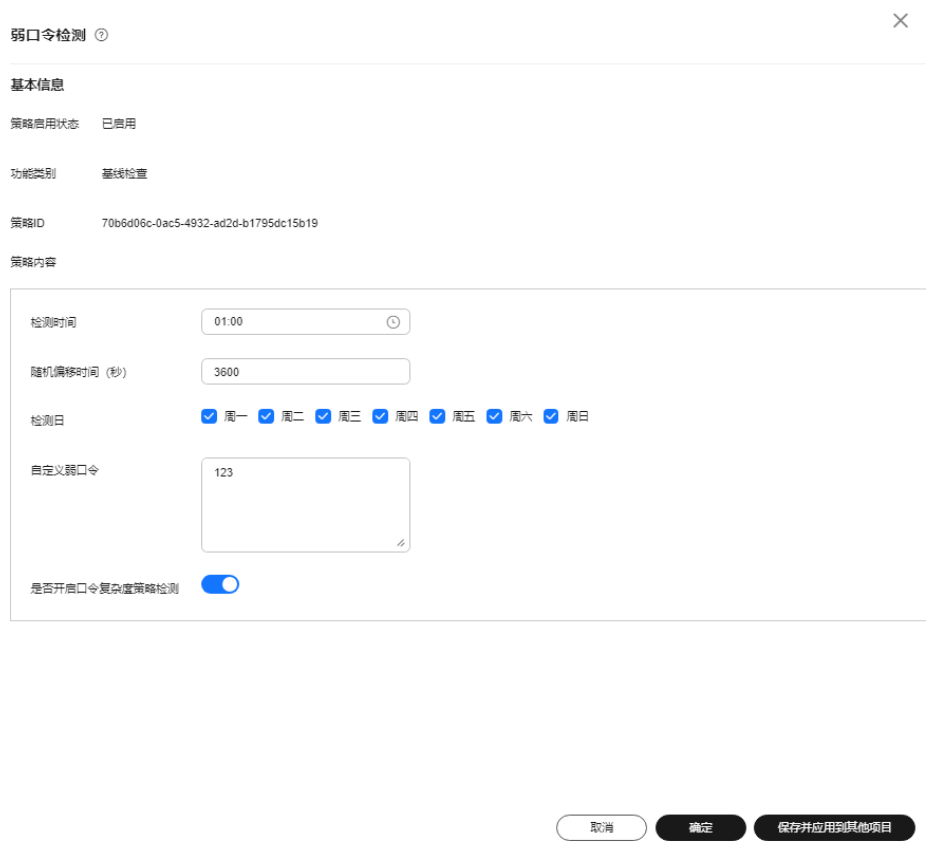


表 6-1 弱口令检测策略内容参数说明

参数	说明	取值样例
检测时间	配置弱口令检测的时间，可具体到每一天的每一分钟。	01:00
随机偏移时间（秒）	检测配置的弱口令时间的随机偏移时间，在“检测时间”的基础上偏移，可配置范围为“0~7200秒”。	3600
检测日	弱口令检测日期。勾选周一到周日检测弱口令的时间。	全选
自定义弱口令	您可以将疑似被泄露的口令添加在自定义弱口令文本框中，防止主机中的账户使用该弱口令，给主机带来危险。 填写多个弱口令时，每个弱口令之间需换行填写，最多可添加300条。	test123*
是否开启口令复杂度策略检测	口令复杂度策略是指服务器设置的口令规则和标准。开启“口令复杂度策略”检测，企业主机安全会在用户手动执行基线检查时，对服务器设置的口令复杂度策略进行检测。	

5. 确认无误后，单击“确定”，完成修改。
   后续HSS将按照您配置的弱口令检测策略，对服务器执行弱口令检测。

步骤9 配置登录安全检测

1. 单击“策略名称”为“登录安全检测”的名称，弹出“登录安全检测”对话框。
2. 根据业务实际情况修改“策略内容”中的参数，参数说明如表6-2所示。

图 6-12 修改安全检测策略

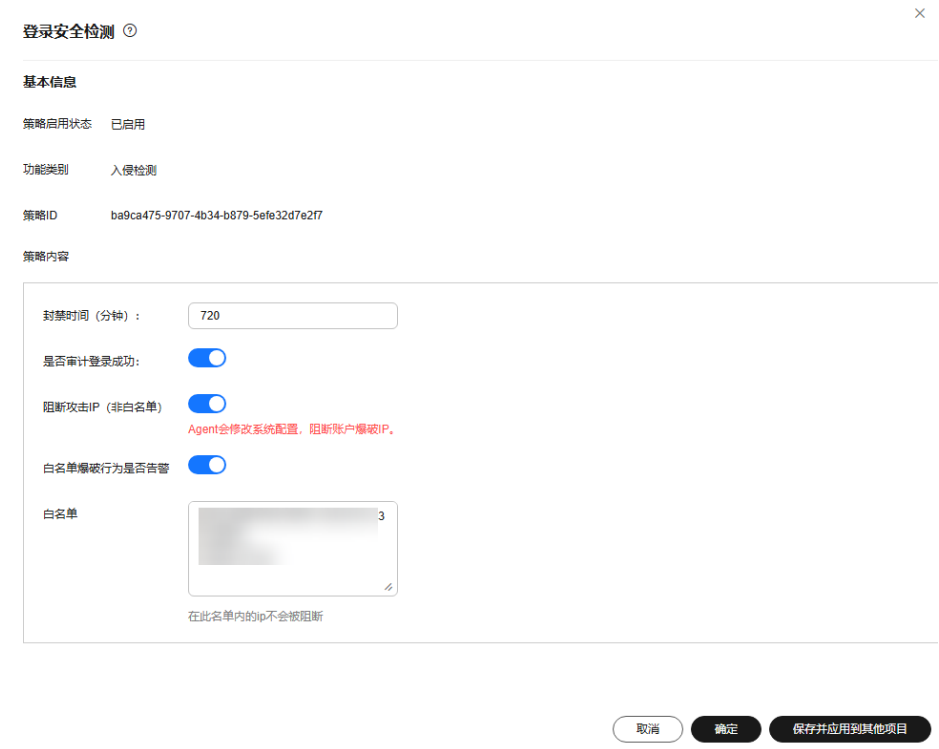


表 6-2 登录安全检测策略内容参数说明

参数	说明
封禁时间（分钟）	可设置被阻断攻击IP的封禁时间，封禁时间内不可登录，封禁时间结束后自动解封，可配置范围为“1~43200”。
是否审计登录成功	- 开启此功能后，HSS将上报登录成功的事件。 ■  ：开启。 ■  ：关闭。
阻断攻击IP（非白名单）	开启阻断攻击IP后，HSS将阻断爆破行为的IP（非白名单）登录。
白名单爆破行为是否告警	- 开启后，HSS将对白名单IP产生的爆破行为进行告警。 ■  ：开启。 ■  ：关闭。
白名单	将IP添加到白名单后，HSS不会阻断白名单内IP的爆破行为。最多可添加50个IP或网段到白名单，且同时支持IPV4和IPV6。

3. 确认无误后，单击“确定”，完成修改。
   后续HSS将按照您配置的登录安全检测策略，对服务器执行登录安全检测。

----结束

7 使用 HSS 和 CBR 防御勒索病毒

7.1 方案概述

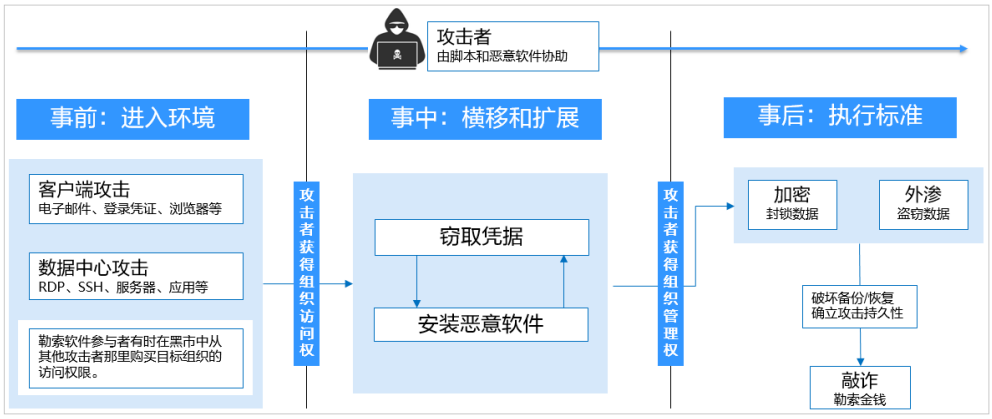
应用场景

勒索软件攻击已成为当今企业面临的最大安全挑战之一。勒索软件可以锁定受害者的数据或资产设备，攻击者会要求在支付赎金后才能赎回数据，防止数据被盗，也存在即使支付赎金也无法赎回数据情况。一旦被勒索软件攻击成功，可能导致您的业务中断、数据泄露、数据丢失等严重问题，从而可能对企业的运转、经济、形象、信誉造成重大损失和不良影响，出现的安全问题可能对企业发展产生重大阻碍，出现一蹶不振的现象。

在攻击云基础设施时，攻击者通常会攻击多个资源以试图获取对客户数据或公司机密的访问权限。在勒索攻击链中，攻击者通过事前侦查探测、事中攻击入侵及横向扩散、事后勒索三个步骤实现对企业的资源勒索：

- **事前侦查探测阶段：**收集基础信息、寻找攻击入口，进入环境并建立内部立足点。
- **事中攻击入侵及横向扩散阶段：**部署攻击资源、侦查网络资产并提升访问权限，窃取凭据、植入勒索软件，破坏检测防御机制并扩展感染范围。
- **事后勒索阶段：**窃取机密数据、加密关键数据后加载勒索信息，基于文件重要等级索要赎金。

图 7-1 被勒索过程



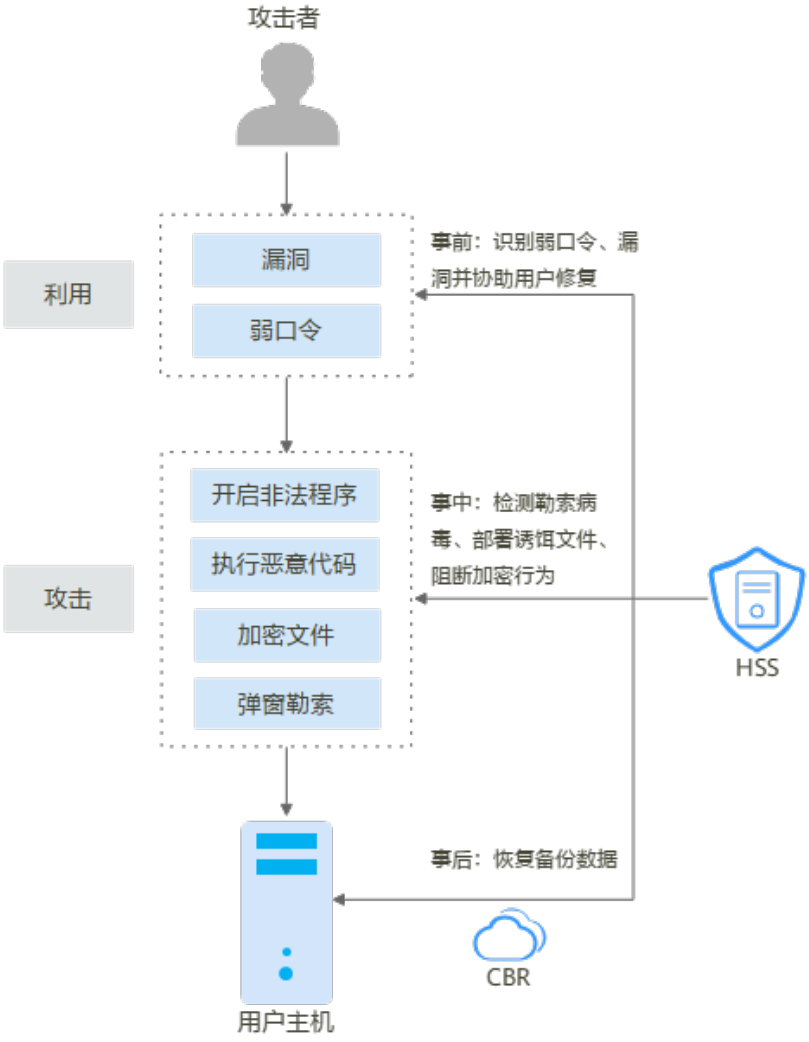
本方案介绍如何通过HSS和CBR为主机进行事前预防、事中检测并及时阻断、事后备份恢复的三阶段防护。

方案架构

企业或个人在进行勒索病毒防护时，可利用HSS检测勒索病毒、识别系统风险项，并通过CBR为业务数据进行备份，此外再合理规划管控账号权限、组织架构等，从而达到最佳的勒索病毒防护效果。

HSS+CBR防护原理示意图如**图 HSS+CBR勒索病毒防护示意图**所示。

图 7-2 HSS+CBR 勒索病毒防护示意图



示意图中实施的各防御措施详情请参见：

- 勒索事前：识别弱口令、漏洞并协助用户修复。
  详细操作请参见**识别并修复勒索风险入口**。
- 勒索事中：检测勒索病毒、部署诱饵文件并阻断加密行为。
  详细操作请参见**开启勒索病毒防护和备份**。

- 勒索事后：恢复备份数据。
  详细操作请参见**恢复备份数据**。

方案优势

- 减少系统风险入口
  用户可以通过HSS定期检测系统存在的漏洞和风险项，第一时间修复漏洞及风险项，减小系统风险等级。
- 实时检测、阻断勒索攻击
  开启勒索病毒防护后，HSS将实时检测并告警勒索病毒攻击，并支持隔离勒索程序。
- 备份业务数据，增加抗风险能力
  服务器被勒索攻击后，可通过CBR恢复备份数据，及时恢复业务，减少损失。

7.2 资源和成本规划

本章节介绍最佳实践中资源规划情况，包含以下内容：

表 7-1 资源说明

资源	资源说明	成本说明
企业主机安全（Host Security Service）	1个HSS旗舰版。防护1台服务器，需要1个HSS旗舰版配额。	HSS具体的计费方式及标准请参考**HSS计费说明**。
云备份（Cloud Backup and Recovery）	1个云服务器备份存储库。	CBR具体的计费方式及标准请参考**CBR计费说明**。

7.3 防御措施

7.3.1 识别并修复勒索风险入口

根据华为云安全历史入侵事件数据表明，90%的勒索攻击入口集中在**弱口令、漏洞利用、基线风险**配置，提前识别风险并修复可显著提升系统防御能力。华为云企业主机安全能帮助您快速识别风险入口，提供便捷一键修复功能降低企业运维成本。

加固弱密码

HSS每日凌晨自动检测主机中使用的经典弱口令和您添加的**自定义弱口令**，您可以根据检测出的弱口令对应的账号信息，加固弱密码。HSS支持检测SSH、FTP、MYSQL类型的弱口令。

步骤1 **登录管理控制台**。

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

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 选择“经典弱口令”页签，查看主机中当前存在的弱口令。

图 7-3 查看经典弱口令检测

步骤5 根据检测出的弱口令对应的主机名称、账号名和账号类型等信息，登录主机加固所有弱口令。

弱口令加固完成后，建议您立即**手动检测**验证加固结果。

----结束

加固基线配置

HSS每日凌晨自动检测系统中关键软件的配置风险并给出详细的加固方法。您可以根据给出的加固建议，正确处理主机内的各种风险配置信息。

步骤1 **登录管理控制台**。

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

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。

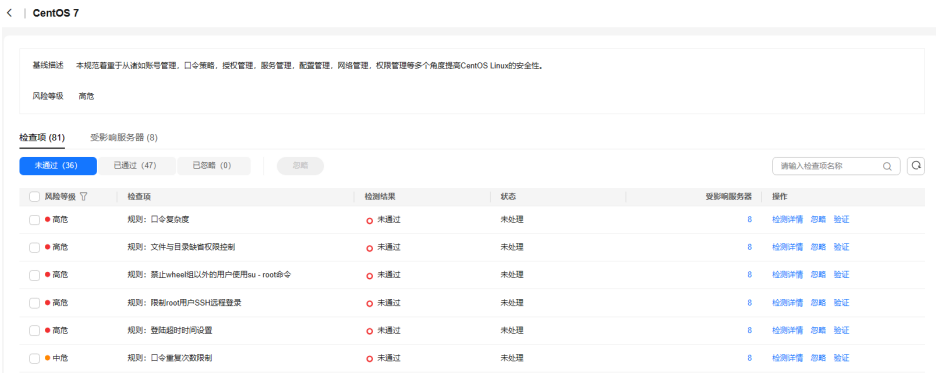
步骤4 选择“配置检查”页签，查看主机中当前存在的基线风险。

图 7-4 查看配置检查统计

步骤5 单击目标基线名称，进入基线详情页面。

步骤6 选择“检查项 > 未通过”页签，查看基线风险项。

图 7-5 查看基线检查详情



步骤7 单击“操作”列的“检测详情”，查看修改建议和受影响的服务器。

步骤8 登录受影响的服务器，根据修改建议加固配置。

步骤9 加固完成后，单击“操作”列的“验证”，验证加固配置结果。

说明

建议重复以上步骤修复所有高风险基线。

----结束

修复漏洞

HSS默认每周自动进行一次全面的漏洞检测并给出修复建议，您可以根据检测漏洞修复建议，修复主机内存在的漏洞威胁。漏洞自动检测周期也可以自行配置，详细操作请参见**自动扫描漏洞**。

说明

漏洞修复优先级分为紧急、高、中、低，建议您优先修复紧急、高优先级的漏洞，根据实际业务情况修复中、低优先级的漏洞。

步骤1 **登录管理控制台**。

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

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

步骤4 选择“Linux漏洞”、“Windows漏洞”、“Web-CMS漏洞”、“应用漏洞”以及“应急漏洞”页签，查看主机当前存在的各类漏洞。

步骤5 根据不同的漏洞类型，进行漏洞修复。

- Linux漏洞、Windows漏洞

  单击待修复的漏洞所在行“操作”列的“修复”，修复漏洞。

  或勾选所有待修复漏洞，单击漏洞列表左上角的“批量修复”，批量修复漏洞。

- Web-CMS漏洞、应用漏洞、应急漏洞

  a. 单击漏洞名称，查看漏洞修复建议。

  b. 登录漏洞影响的主机，手动修复漏洞。

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

  - 方案一：创建新的虚拟机执行漏洞修复

    1) 为需要修复漏洞的ECS主机创建镜像。

    详细操作请参见**通过云服务器创建整机镜像**。

    2) 使用该镜像创建新的ECS主机

    详细操作请参见**通过镜像创建云服务器**。

    3) 在新启动的主机上执行漏洞修复并验证修复结果。

    4) 确认修复完成之后将业务切换到新主机。

    5) 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。

如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。

- 方案二：在当前主机执行修复
  1) 为需要修复漏洞的ECS主机创建备份。
     详细操作请参见**创建云服务器备份**。
  2) 在当前主机上直接进行漏洞修复。
  3) 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态。
     详细操作请参见**使用备份恢复服务器**。

  说明

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

c. 漏洞修复完成后，单击漏洞名称，进入漏洞详情页面。

d. 选择“受影响服务器”页签，单击“操作”列的“更多 > 验证”，验证漏洞修复结果。

----结束

7.3.2 开启勒索病毒防护和备份

在应对勒索攻击时，及时识别并隔离勒索攻击和备份、恢复业务数据的重要性进一步凸显。华为云企业主机安全首创防入侵、防加密、防扩散的三防勒索检测引擎和动态诱饵欺骗技术，实现勒索病毒秒级查杀，业务数据分钟级备份和恢复，勒索防治竞争力业界领先。

开启勒索防护和勒索备份，增强服务器勒索防护力，抵御勒索攻击，降低业务受损风险。

步骤一：创建勒索病毒防护策略

根据自身业务需求，创建勒索防护策略，配置诱饵防护目录、排除目录、防护文件类型等。

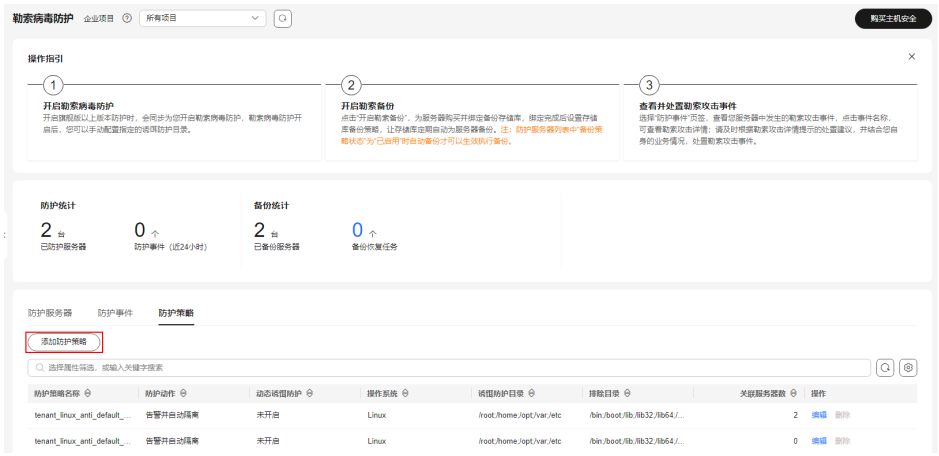
步骤1 **登录管理控制台**。

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

步骤3 选择“主机防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

步骤4 选择“防护策略”页签，单击“添加防护策略”，弹出“添加防护策略”对话框。

图 7-6 添加防护策略



步骤5 配置策略信息，参数说明如**表 防护策略参数说明**所示。

图 7-7 设置防护策略参数

表 7-2 防护策略参数说明

参数名称	参数说明	取值样例
服务器操作系统	选择服务器操作系统类型。	Linux
防护策略名称	设置防护策略的名称。	test
防护动作	发现勒索病毒事件后的处理方式。 • 告警并自动隔离 • 告警	告警并自动隔离
动态诱饵防护	开启动态诱饵防护后，系统会在防护目录和其他随机位置（不包括排除目录）中部署诱饵文件，在随机位置部署的诱饵文件每12小时会自动删除再重新随机部署。诱饵文件会占用小部分服务器资源，请将不希望部署诱饵文件的目录配置在排除目录内。 **说明** 当前仅Linux系统支持动态生成和部署诱饵文件，Windows系统仅支持静态部署诱饵文件。	开启
诱饵防护目录	需要部署静态诱饵进行防护的目录（不包括子目录），建议配置为重要业务目录或数据目录。 多个目录请用英文分号隔开，最多支持填写20个防护目录。 Linux系统必填，Windows系统可选填。	Linux：/etc Windows：C:\Test
排除目录（选填）	无需部署诱饵文件进行防护的目录。 多个目录请用英文分号隔开，最多支持填写20个排除目录。	Linux：/etc/lesuo Windows：C:\Test\ProData
防护文件类型	需要防护的服务器文件类型或格式，自定义勾选即可。 涵盖数据库、容器、代码、证书密匙、备份等9大文件类型，共70+种文件格式。 仅Linux系统时，需要设置此项。	全选
进程白名单（选填）	添加自动忽略检测的进程文件路径，可在告警中获取。 仅Windows系统，需要设置此项。	-

步骤6 确认信息无误，单击“确定”，完成防护策略创建。

----结束

步骤二：开启勒索病毒防护

如果Linux主机安装的Agent版本为3.2.8及以上版本或Windows主机安装的Agent版本为4.0.16及以上版本，开启企业主机安全旗舰版、网页防篡改版或容器安全版防护时，

系统会同步**为您开启勒索病毒防护**；如果Agent版本不满足自动开启条件，您可以手动开启防护。

步骤1 登录管理控制台。

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

步骤3 选择“主机防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

步骤4 选择“防护服务器”页签。

步骤5 选中目标服务器，并单击列表上方的“开启勒索病毒防护”。

步骤6 在“开启勒索病毒防护”弹窗中，确认服务器信息，并选择步骤一创建的防护策略。

步骤7 单击“确定”，开启防护。

服务器勒索防护状态显示已开启，表示开启勒索病毒防护成功。

----结束

步骤三：开启勒索备份

为了预防服务器被勒索后无法挽回业务损失，请为服务器开启勒索备份，定期备份业务数据。

说明

如果您未购买存储库，请参考**购买云服务器备份存储库**购买存储库后，再执行开启勒索备份操作。

步骤1 登录管理控制台。

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

步骤3 选择“主机防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

步骤4 选择“防护服务器”页签。

步骤5 选中目标服务器，并在服务器列表上方单击“开启勒索备份”。

图 7-8 开启勒索备份

步骤6 在“开启备份”弹窗中，选择需要为服务器绑定的存储库。

说明

同时满足以下条件的存储库支持绑定：

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

步骤7 单击“确定”，开启备份。

----结束

步骤四：处理告警并隔离感染设备

当一个入侵者绕过防御机制时，如果您能及时发现并阻断，便可避免灾难的发生。因此在开启勒索病毒防护后，您需要及时处置入侵告警事件，隔离阻断勒索病毒运行、扩散。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“主机防御 > 勒索病毒防护 ”，进入勒索病毒防护界面。

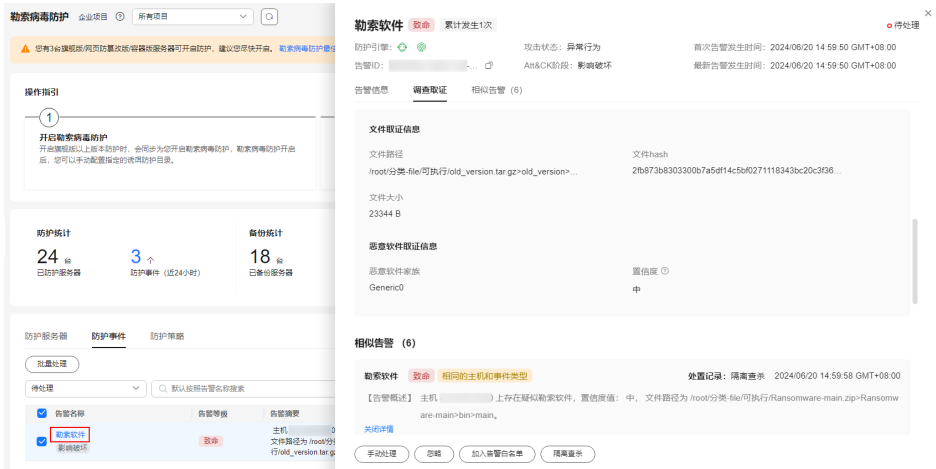
步骤4 选择“防护事件”页签，查看勒索攻击告警事件。

图 7-9 防护事件

步骤5 单击告警名称，查看告警详细信息。

您可以根据告警信息、调查取证等信息排查主机上是否存在勒索软件。

图 7-10 查看告警详细信息



步骤6 在页面下方，选择告警处置方式。

图 7-11 选择告警处置方式

- 手动处理：如果您已手动处理了该事件，可选择“手动处理”。
- 忽略：如果告警暂时无需处理，您可以选择“忽略”，忽略后，告警状态将变为已处理，后续企业主机安全将不会对该事件进行统计。
- 加入告警白名单：如果告警为误报，您可以选择“加入告警白名单”，后续企业主机安全将不再告警。
- 隔离查杀：如果确认是勒索程序引起的告警，您可以选择“隔离查杀”，隔离后，该程序将无法执行“读/写”操作，同时该程序的进程将被立即终止。

⚠ 注意

确认服务器遭受勒索攻击后，请立即采取断网、断电等方式切断勒索病毒外联扩散行为，并及时修改感染设备的密码及同一局域网其他设备密码。

步骤7 在“处理告警事件”对话框中，单击“确定”，处置告警完成。

----结束

相关操作

在使用HSS+CBR之外，建议按照如下方式从其他方面提升自身“免疫力”：

- **收敛互联网暴露面：**定期扫描外部端口，保证公开范围最小化。
- **加强网络访问控制：**各企业应具有明确的网络安全区域划分、访问限制规则，最小化开放访问权限，及时更新访问控制规则。

- **加强账号权限管控：**通过身份管理、细粒度权限控制等访问控制规则为企业不同角色分配账号并授权，同时应提升特权账户的安全性。在另一方面，企业关键业务资产，需要妥善设置并保存账号及口令信息。关键资产上，配置双因素认证鉴别登录人员身份，可有效防范系统爆破风险。
- **搭建高可靠业务架构：**采用集群模式的云服务部署模式。当某一个节点发生紧急问题，业务切换至备用节点，提升业务系统可靠性能力，也可防止数据丢失。在资源允许的条件下，企业或组织可以搭建同城或异地容灾备份系统，当主系统出现发生勒索事件后，可以快速切换到备份系统，从而保证业务的连续性。
- **制定安全事件应急预案：**建立应对勒索病毒攻击等网络安全突发事件的应急组织体系和管理机制，明确工作原则、职责分工、应急流程、关键措施等。一旦发生勒索病毒攻击事件，立即启动内部网络安全应急预案，标准化开展应急处置工作来减轻、消除勒索病毒攻击影响。
- **加强企业员工安全意识：**通过培训、演练等方式提高员工网络安全意识，明确国家网络安全法令及公司网络安全规范，能够识别网络钓鱼等常见的网络安全攻击，具备一定的事件处理能力，知晓安全事件带来的后果和影响。

7.3.3 恢复备份数据

目前由于勒索攻击发展迅速，任何工具都无法提供100%防护；如果服务器不幸失陷，备份恢复能够将损失最小化；您在开启勒索备份后，可以通过华为云云备份服务快速恢复业务，保障业务安全运行。

恢复备份数据

通过备份数据恢复服务器业务数据时，请在还原之前验证备份是否正常，验证无误后，首先还原业务关键型系统。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏选择“主机防御 > 勒索病毒防护 ”，进入勒索病毒防护界面。

步骤4 选择“防护服务器”页签。

步骤5 在目标服务器所在行的“操作”列，选择“更多 > 恢复数据”。

步骤6 在弹窗中选择需要恢复的备份数据源。

步骤7 在目标备份数据源所在行的“操作”列，单击“恢复数据”。

步骤8 在弹窗中确认服务器信息并配置数据存放磁盘等参数。

- 服务器重启：勾选后表示同意数据恢复后重启服务器。
- 高级选项：单击 展开。选择备份数据恢复位置。

图 7-12 恢复服务器

步骤9 单击“确定”，执行备份恢复。

----结束

相关操作

建议您根据勒索攻击路径识别系统薄弱点，重点排查并修复系统薄弱项。

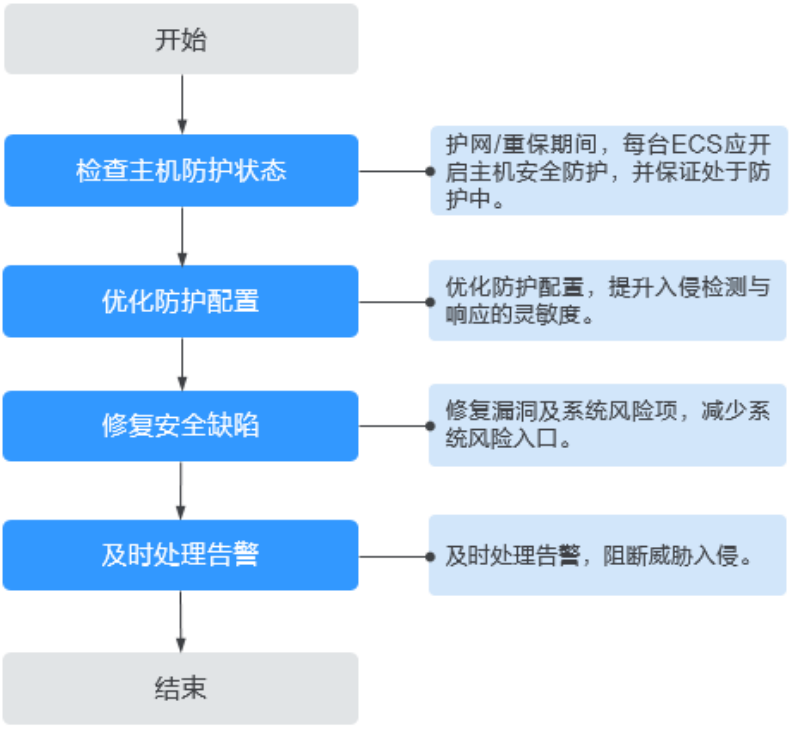
8 护网或重保场景下 HSS 的应用实践

8.1 方案概述

企业主机安全（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。HSS不受地理位置影响，为主机、容器等提供统一的可视化和控制能力。HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

本方案介绍在护网、重保期间，通过检查主机防护状态、优化防护配置、修复安全缺陷、及时处理告警四个方面的操作，有效使用企业主机安全，提升主机防护能力。具体流程如下图所示：

图 8-1 使用流程



8.2 步骤一：检查主机防护状态

护网/重保期间需要保证所有ECS主机均接入企业主机安全，并处于防护中，以提高主机安全风险防御能力。

检查主机防护状态

步骤1 登录管理控制台。

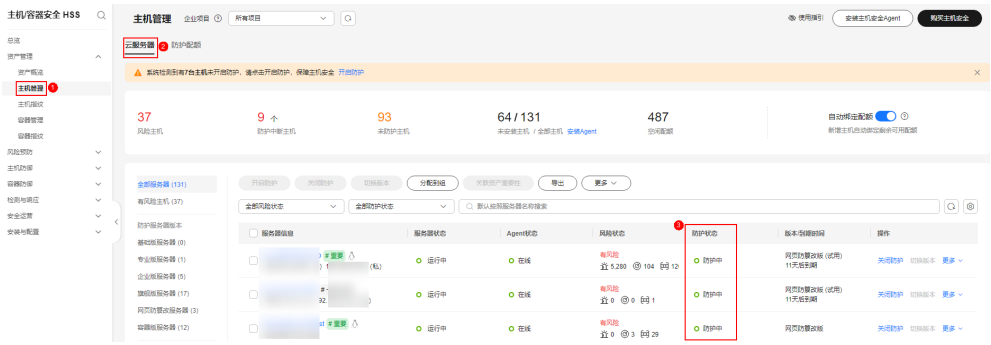
步骤2 单击管理控制台左上角的，选择区域和项目。

步骤3 单击页面左上方的，选择“安全与合规 > 企业主机安全”，进入“企业主机安全”页面。

步骤4 在左侧导航栏，选择“资产管理 > 主机管理”，进入主机管理页面。

步骤5 选择“云服务器”页签，确认服务器防护状态。

图 8-2 查看主机防护状态



步骤6 根据不同防护状态，执行以下操作。

- **未防护**

  服务器未开启防护，被威胁入侵的风险较高，建议您尽快为服务器开启防护。

  开启防护步骤如下：

  a. **购买防护配额**。

  b. **安装Agent**。

  c. **开启防护**。

  说明

  建议普通服务器开启企业版及以上防护，容器节点服务器开启容器版防护。

- **防护中**

  主机已开启防护。企业主机安全会持续优化迭代Agent版本，以便为您提供更好的服务器。请您参考以下操作检查Agent版本。

  a. 在左侧导航栏，选择“安装与配置 > 主机安装与配置”，进入“主机安装与配置”页面。

  b. 在“Agent管理”页签，查看服务器的“Agent升级状态”。

如果“Agent升级状态”为“未升级”，请单击“升级Agent”，将Agent升级为最新版，如图 升级Agent所示。

您也可以批量勾选需升级Agent的主机，单击列表左上角的“批量升级Agent”，批量升级Agent。

图 8-3 升级 Agent

- **防护中断**

  请确认服务器是否关机，Agent是否离线，企业主机安全无法正常为服务器提供防护。

  如果Agent离线，请参考**Agent状态异常应如何处理?**，尽快让Agent恢复为“在线”状态。

----结束

8.3 步骤二：优化防护配置

在护网/重保场景下，建议通过开启恶意软件云查、配置告警通知以及优化防护策略等系列优化防护配置的操作，提高入侵检测与响应的灵敏度。

开启恶意软件云查

HW场景攻击者一般会对攻击中使用的黑客工具、恶意软件等进行修改，改变文件Hash。这类文件无法通过病毒库检出，只能通过恶意软件云查功能的AV恶意文件检测引擎进行识别。

步骤1 **登录管理控制台**。

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

步骤3 在左侧导航树中，选择“安全与配置 > 主机安装与配置”，进入“主机安装与配置”页面。

步骤4 选择“安全配置 > 恶意程序隔离查杀”，进入“恶意程序隔离查杀”页面。

步骤5 在“恶意软件云查”功能所在行，单击开启该功能。

图 8-4 开启恶意软件云查

步骤6 在“开启恶意软件云查”弹窗中，单击“ ”。

按钮显示 ，表示“恶意软件云查”已开启。

----结束

配置告警通知

开启告警通知后，HSS可以通过短信或邮件的形式向您发送风险告警，方便您及时了解主机或容器存在的安全风险。不开启告警通知，您只能自行登录HSS管理控制台查看告警信息。

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“安全与配置 > 告警配置”，进入“告警配置”页面。

步骤4 在“告警配置”页面，配置告警事件、告警方式等信息。相关参数配置请参见**表 配置告警信息**。

图 8-5 告警配置

表 8-1 配置告警信息

参数名称	参数说明	取值样例
实时告警通知	实时告警通知会在事件发生时，及时发送告警通知至您添加的手机号或者邮箱。每小时每类安全事件的告警通知发送上限为10条。  ：表示开启状态。  ：表示关闭状态	
告警等级	告警通知事件的威胁等级，勾选后，系统才会发送对应等级告警。 ● 必选：致命、高危。 ● 可选：中危、低危。	致命、高危、中危
屏蔽事件	需要屏蔽无需发送告警通知的事件。 为了避免大量低危告警掩盖入侵告警，建议屏蔽“文件/目录变更”、“登录成功”和“Crontab可疑任务”事件。	文件/目录变更、登录成功、Crontab可疑任务

参数名称	参数说明	取值样例
选择告警方式	• 消息中心 告警通知默认发送给账号联系人的消息中心，如需修改接收人请参见**修改指定消息接收人**。 • 消息主题 单击下拉列表选择已创建的主题，或者单击“查看消息通知服务主题”创建新的主题。创建新的主题，即配置接收告警通知的手机号码或邮箱地址，具体操作如下： 1. **创建主题**。 定制一个HSS消息事件类型。 2. **添加订阅**。 为创建的主题添加加一个或多个订阅，即配置接收告警通知的手机号码或邮箱地址。 3. 确认订阅。 添加订阅后，按接收到的短信或邮件提示，完成订阅确认。主题订阅确认的信息可能被当成垃圾短信拦截，如未收到，请查看是否设置了垃圾短信拦截。	消息主题

步骤5 单击“应用”，完成配置主机安全告警通知的操作。

界面弹出“告警通知设置成功”提示信息，则说明告警通知设置成功。

----结束

优化防护策略

通过精细化策略配置，可提升主机防护能力。

步骤1 **登录管理控制台**。

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

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 在目标策略组所在行的操作列，单击“编辑防护模式”，系统弹出“编辑防护模式”对话框。

步骤5 在对话框中，选择“高检出”，并单击“ ”。

须知

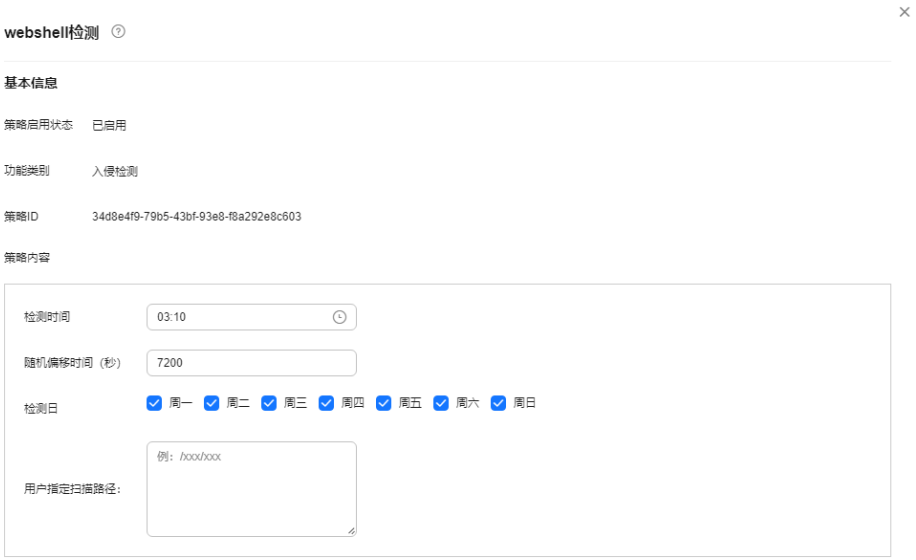
高检出模式下的进程异常行为告警可能存在误报情况。

步骤6 单击目标策略组名称，进入策略列表页面。

步骤7 单击“webshell检测”名称，进入策略详情页面，编辑策略。

在“用户指定扫描路路径”中添加您的Web目录，防止因HSS未能自动识别Web目录，导致漏报告警。

图 8-6 编辑 webshell 检测策略



步骤8 策略修改完成，单击“ ”，修改完成。

----结束

8.4 步骤三：修复安全缺陷

8.4.1 修复漏洞

HSS默认每周自动进行一次全面的漏洞扫描，如果您需要立即扫描主机漏洞也可以**手动扫描**，待漏洞扫描完成后，可查看并修复漏洞。

前提条件

请确保修复漏洞时，您的业务处于低峰期或特定的变更时间窗。

修复说明

- **Linux、Windows漏洞**
  - 如下是近两年在攻防演练中被红队利用最频繁且对企业危害较高的系统漏洞，HSS漏洞库支持扫描该漏洞，如果使用HSS扫描时发现该漏洞，请优先排查修复。
    - Linux DirtyPipe权限提升漏洞（CVE-2022-0847）
  - 如果漏洞影响的软件未启动或启动后无对外开放端口，则实际风险较低，可滞后修复。
- **应用漏洞**
  - HSS不支持扫描如用友、金蝶等商用软件的漏洞，因此商用软件漏洞您需要自行排查。

- 如果Web服务器的应用漏洞无法修复，您可以通过配置安全组规则，限制只可内网访问，或使用WAF防护（只能降低风险，通过内网渗透或规则绕过依然有被入侵的风险）。
- 如下是近两年在攻防演练中被红队利用最频繁且对企业危害较高的应用漏洞，HSS漏洞库支持扫描这些漏洞，如果使用HSS扫描时发现这些漏洞，请优先排查修复。
  - nginxWebUI远程命令执行漏洞
  - Nacos反序列化漏洞
  - Apache RocketMQ命令注入漏洞（CVE-2023-33246）
  - Apache Kafka远程代码执行漏洞（CVE-2023-25194）
  - Weblogic远程代码执行漏洞（CVE-2023-21839）
  - Atlassian Bitbucker Data Center远程代码执行漏洞（CVE-2022-26133）
  - Apache CouchDB远程代码执行漏洞（CVE-2022-24706）
  - F5 BIG-IP命令执行漏洞（CVE-2022-1388）
  - Fastjson 1.2.8反序列化漏洞（CVE-2022-25845）
  - Atlasssian Confluence OGNL注入漏洞（CVE-2022-26134）
  - Apache Log4j2远程代码执行漏洞（CVE-2021-44228）

修复漏洞

步骤1 登录管理控制台。

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

步骤3 在左侧导航树中，选择“风险预防 > 漏洞管理”，进入漏洞管理界面。

步骤4 在漏洞管理界面右上角，选择“主机视图”。

步骤5 查看当前存在漏洞风险的服务器。

图 8-7 查看风险服务器

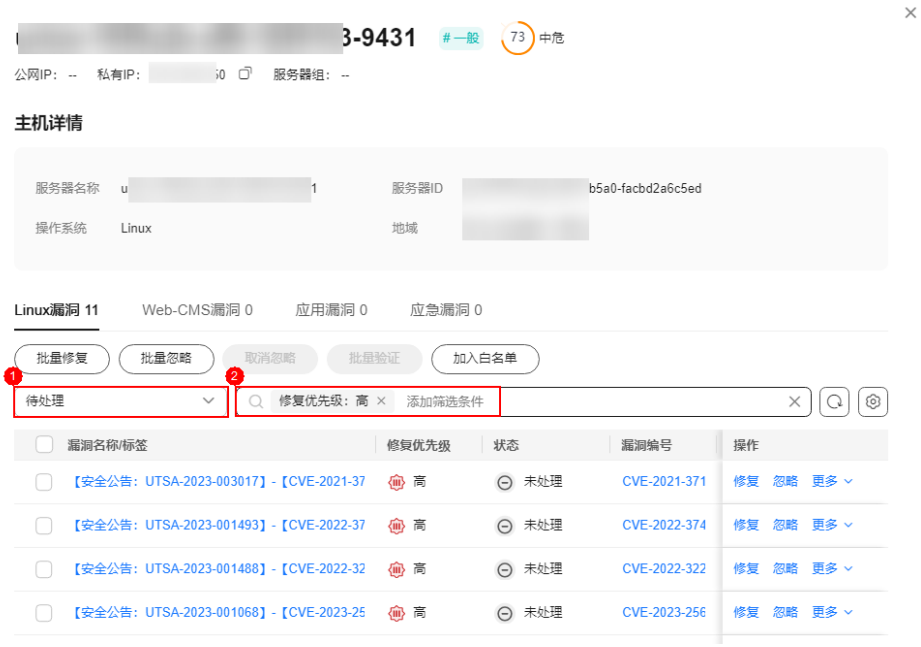
步骤6 单击服务器名称，进入服务器详情页面。

步骤7 筛选“待处理”且修复优先级为“紧急”、“高”、“中”的Linux漏洞、Windows漏洞和应用漏洞，优先进行修复。

须知

在进行漏洞修复前，需提前和您的业务相关人员确认漏洞修复是否会对业务造成影响。

图 8-8 筛选漏洞



- 修复Linux、Windows漏洞
  a. 单击需修复的漏洞所在行“操作”列的“修复”，弹出“修复”对话框。

     或批量勾选漏洞名称前的☐并单击漏洞列表上方的“批量修复”，批量修复漏洞。
  b. 在对话框中，开启创建备份、勾选“我确定知晓如未进行手动创建备份，可能存在修复失败导致业务中断的风险，同时无法进行回滚”。

     创建备份，需确保已为服务器绑定存储库，如未绑定，请参考**CBR入门指引**，为服务器绑定存储库。

图 8-9 修复漏洞

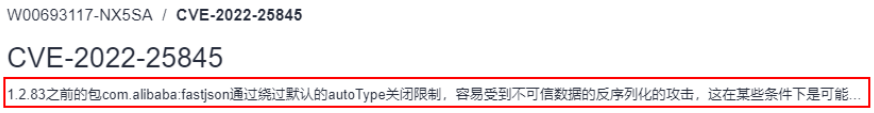
c. 单击“确定”，开始修复。

d. 在界面右上角，单击“任务管理”，可查看漏洞修复进度。

图 8-10 查看漏洞修复进度

- 修复应用漏洞
  a. 单击漏洞名称，进入漏洞详情页面查看漏洞详情。

  图 8-11 查看漏洞详情

  b. 登录漏洞影响的主机，手动修复漏洞。

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

  - **方案一：创建新的虚拟机执行漏洞修复**
    1) 为需要修复漏洞的ECS主机创建镜像，详细操作请参见**通过云服务器创建整机镜像**。
    2) 使用该镜像创建新的ECS主机，详细操作请参见**通过镜像创建云服务器**。
    3) 在新启动的主机上执行漏洞修复并验证修复结果。
    4) 确认修复完成之后将业务切换到新主机。
    5) 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。
  - **方案二：在当前主机执行修复**
    1) 为需要修复漏洞的ECS主机创建备份，详细操作请参见**创建云服务器备份**。
    2) 在当前主机上直接进行漏洞修复。
    3) 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态，详细操作请参见**使用备份恢复服务器**。

说明

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

----结束

8.4.2 整改基线

HSS每日凌晨会自动执行基线检查，如果您需要查看当下的基线检查结果也可以**手动检查**，待检查完成后，可查看并修复配置、弱口令风险。

整改弱口令

- 结合企业主机安全现网攻击态势识别到“账号暴力破解攻击”是最常见的入侵方式之一，且当主机中存在弱口令时，极易被攻击方通过弱口令完成入侵，因此弱口令风险需要优先修复。
- 当前HSS支持SSH、FTP、MYSQL类型弱口令，系统中应用的弱口令或默认口令需要您自行排查，如nacos、weblogic等。

步骤1 **登录管理控制台**。

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

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 选择“经典弱口令”页签，查看主机中当前存在的弱口令。

图 8-12 查看经典弱口令检测

步骤5 根据检测出的弱口令对应的主机名称、账号名和账号类型等信息，登录主机加固所有弱口令。

弱口令加固完成后，建议您立即**手动检测**验证加固结果。

----结束

整改配置检查高风险项

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 > 企业主机安全”，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。

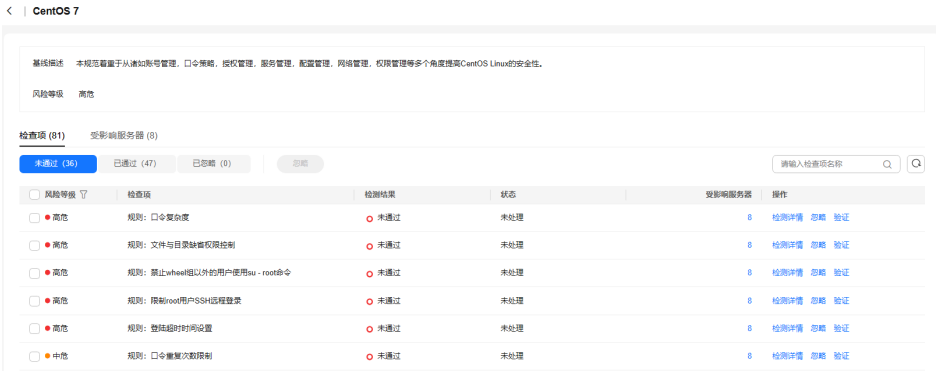
步骤4 选择“配置检查”页签，查看主机中当前存在的基线风险。

图 8-13 查看配置检查统计

步骤5 单击目标基线名称，进入基线详情页面。

步骤6 选择“检查项 > 未通过”页签，查看基线风险项。

图 8-14 查看基线检查详情



步骤7 单击“操作”列的“检测详情”，查看修改建议和受影响的服务器。

步骤8 登录受影响的服务器，根据修改建议加固配置。

步骤9 加固完成后，单击“操作”列的“验证”，验证加固配置结果。

说明

建议重复以上步骤修复所有高风险基线。

----结束

8.5 步骤四：及时处理告警

您接收到来自HSS的短信或邮件形式的风险告警通知后，请及时登录HSS控制台查看告警详情并阻断威胁入侵。

查看告警

步骤1 登录管理控制台。

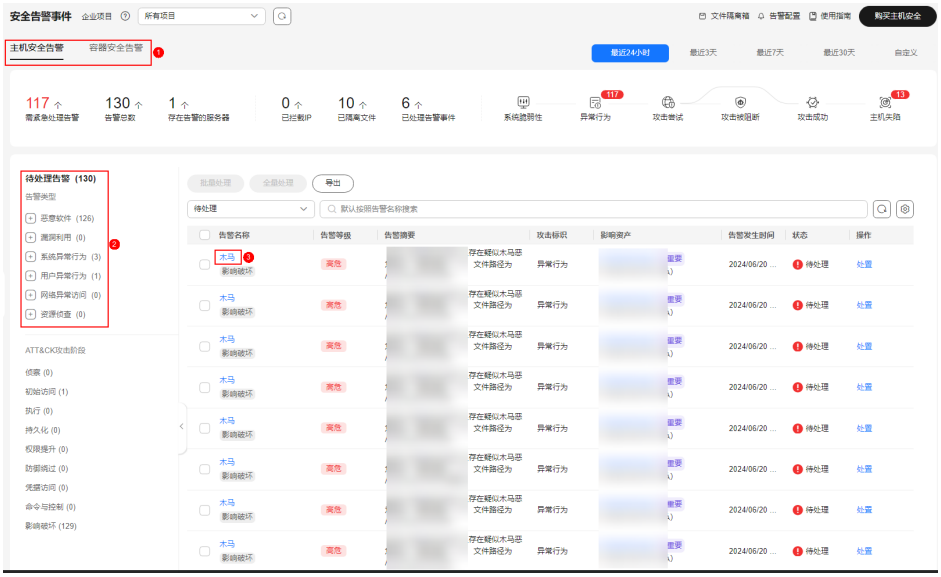
步骤2 在页面左上角选择“区域”，单击，选择“安全与合规 > 企业主机安全”，进入主机安全平台界面。

步骤3 在左侧导航栏中，单击“检测与响应 > 安全告警事件”，进入“安全事件告警”页面。

步骤4 在安全事件告警页面，选择查看主机或容器存在的各类告警。

1. 在事件类型栏，选择告警事件类型。
2. 在事件类型对应的事件列表栏，查看告警信息。
3. 单击事件的告警名称，可查看告警的详细信息。

图 8-15 查看安全告警



4. 参考**告警处理建议**，阻断威胁入侵。

----结束

告警处理建议

告警类型	说明	处理建议
恶意软件	护网场景下企业主机安全检测出病毒、木马、黑客工具、Webshell类型的恶意软件居多，其中黑客工具类型尤其多，因此请重点关注这些类型的恶意软件告警。	发现恶意软件类告警即表示告警主机大概率被攻破，请按以下方式处理： 1. 立即进行安全排查。 2. 对告警主机进行网络隔离，防止横向扩散。

告警类型	说明	处理建议
反弹Shell	反弹shell是攻击机监听在某个TCP/UDP端口为服务端，同时使目标机主动发起请求到攻击机监听的端口，并将其命令行的输入输出转到攻击机。攻击者一般通过漏洞利用获取主机命令执行权限后，建立反弹shell连接，进行下一步的恶意行为。	发现反弹shell告警即表示告警主机大概率被攻破，请分析告警详情中的攻击源IP： ● 如果攻击源IP是外网IP：可以确定主机被攻破，请对主机进行网络隔离，并立即进行安全排查；同时如果反弹shell执行的命令中包含某一应用路径，则大概率是通过此应用的漏洞入侵，需要分析对应应用是否存在高危漏洞。 ● 如果攻击源IP是内网IP：需要确认此反弹shell是否为客户业务进程，如果不是，需要同时排查告警主机和攻击源主机。
异常登录	异常登录是指使用未经授权的账户或者非正常的时间、地点等方式进行的登录行为，这种行为通常是黑客和攻击者尝试获取系统访问权限或滥用现有权限的一种方式。	确认是否为正常登录行为： ● 是：通过安全组限制固定IP登录，不允许任意公网IP登录主机。 ● 否：主机已被攻破，请立即进行安全排查。
文件提权/进程提权/文件目录	● 文件提权 恶意攻击者利用漏洞或错误配置的文件系统权限，获取比其正常权限更高的访问权限的过程。通过文件提权攻击，攻击者可以获取对系统中敏感数据和资源的访问权限，例如加密的密码文件、关键配置文件等，从而实施进一步的攻击。 ● 进程提权 攻击者利用漏洞或错误配置的进程权限，获取比其正常权限更高的访问权限的过程。通过进程提权攻击，攻击者可以获取对系统中敏感数据和资源的访问权限，例如加密的密码文件、关键配置文件等，从而实施进一步的攻击。 ● 文件/目录变更 指系统中对文件和目录的修改、删除、移动等行为，可能会对系统的稳定性、可用性和安全性产生影响。	这类告警一般需要结合其他告警（如反弹shell、异常登录、恶意软件等高危告警）分析。 ● 如果同主机有反弹shell、异常登录或恶意软件等高危告警，则该主机被攻破，需要立刻进行安全排查。 ● 如果此类告警单独出现，无其他高危告警，则优先分析是否为正常业务触发的误报。

告警类型	说明	处理建议
高危命令执行告警	HSS预置策略会将strace、rz、tcpdump、nmap、nc、ncat、sz命令识别为高危命令。	这类告警一般需要结合其他告警（如反弹shell、异常登录、恶意软件等高危告警）分析。 ● 如果同主机有反弹shell、异常登录或恶意软件等高危告警，则该主机被攻破，需要立即进行安全排查。 ● 如果此类告警单独出现，无其他高危告警，则优先分析是否为正常业务触发的误报。
暴力破解	暴力破解是指攻击者尝试使用不同的用户名和密码组合来试图获得访问受保护系统的权限。 这种攻击方式通常利用弱密码、易受攻击的认证机制、未更新的软件等安全漏洞，以实现入侵目标系统或获取潜在的敏感信息。	分析告警详情中的攻击源IP： ● 攻击源IP为外网IP：说明安全组设置不严，请配置安全组规则禁止通过外网IP登录主机，或使用云堡垒机（Cloud Bastion Host，CBH）服务。 ● 攻击源IP为内网IP：需要对攻击源IP主机进行安全排查，确认是否为客户业务密码配置错误， – 是：请获取正确的用户名和密码登录主机。 – 否，请对攻击源主机进行网络隔离，并立即进行安全排查。
端口扫描/主机扫描	● 端口扫描 一种常见的网络侦查技术，攻击者使用特定的工具或程序向目标主机发送数据包，以确定目标主机上开放的端口和正在运行的服务。 ● 主机扫描 指攻击者使用各种工具和技术，对目标主机的操作系统、服务和应用程序等信息进行侦查和枚举，以确定潜在的漏洞和攻击路径。	分析告警详情中的攻击源IP： ● 攻击源IP为外网IP：表示安全组设置不严，主机关键端口被外网扫描，需要加固网络ACL配置。 ● 攻击源IP为内网IP：分析攻击源IP主机，确认是否为客户正常业务， – 是：可视情况进行忽略。 – 否：请对攻击源主机进行网络隔离，并立即进行安全排查。

9 使用 HSS 扫描和修复漏洞

应用场景

HSS漏洞管理支持扫描Linux漏洞、Windows漏洞、Web-CMS漏洞、应用漏洞和应急漏洞，并提供多种漏洞处理方式，帮助您全面掌握和及时修复资产中的漏洞，规避可能的风险。

本文介绍通过HSS发现并修复漏洞的实践教程。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护。详细操作请参见**HSS接入概述**。

判定漏洞修复的紧急程度

如果您的资产中，检测出多个漏洞时，您可以通过如下方式综合判断漏洞修复的紧急程度，优先修复紧急程度高、会对服务器造成影响的漏洞。

- 通过**漏洞修复优先级**判定

  您可以通过漏洞修复优先级过滤出需要尽快修复的漏洞。一般来讲，“修复优先级”为“紧急”的漏洞需立即修复。

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

  说明

  默认情况下资产重要性为“一般资产”，您可以为服务器关联匹配的重要等级，详细操作请参考**管理服务器重要性**。

  漏洞修复优先级主要分为紧急、高、中、低四个等级，您可以参考修复优先级优先修复对您的服务器影响较大的漏洞。

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

- 通过**实际业务情况**判定

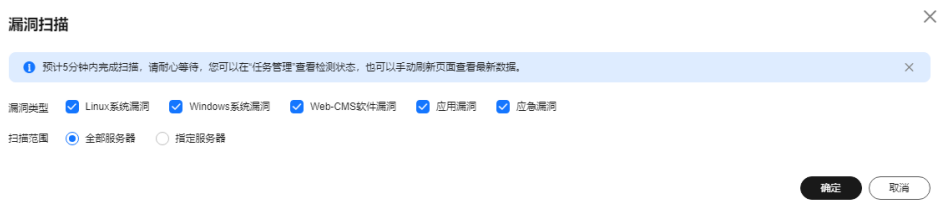
  您可以查看漏洞详情，结合实际业务和受影响的服务器情况，来判定是否需要尽快修复漏洞。

扫描和修复漏洞

步骤1 扫描漏洞。

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 > 企业主机安全”，进入主机安全平台页面。
3. 在左侧导航树，选择“风险预防 > 漏洞管理”，进入漏洞管理页面。
4. 在“漏洞管理”页面右上角，单击“手动扫描”。
5. 在“漏洞扫描”对话框，选中所有“漏洞类型”，并选择“扫描范围”为“全部服务器”，确保能扫描到所有服务器可能存在的各类漏洞。

   图 9-1 配置手动扫描参数

6. 在“漏洞管理”页面右上角，单击“任务管理”。在“扫描任务”页签，确认手动扫描任务已完成，确保所检测的漏洞信息是即时的。

步骤2 修复漏洞。

注意

- 执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云备份（CBR）为ECS创建备份，详细操作请参见创建云服务器备份。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。
- 在线修复主机漏洞时，需要连接Internet，通过外部镜像源提供漏洞修复服务。
  - Linux系统：如果主机无法访问Internet，或者外部镜像源提供的服务不稳定时，可以使用华为云提供的镜像源进行漏洞修复。为了保证漏洞修复成功，请在执行在线升级漏洞前，确认主机中已配置华为云提供的对应操作系统的镜像源，详细的配置操作请参见配置镜像源。
  - Windows系统：如果主机无法访问Internet，请确保拥有自建的补丁服务器。

1. 筛选需要修复的漏洞。
   - 单击“需紧急修复漏洞”上的数字，筛选各类需紧急修复的漏洞。
   - 在扫描出的漏洞列表，筛选出修复优先级高的漏洞，例如“漏洞视图”下，设置“修复优先级”为“紧急”、“高”，“主机视图”下，设置“主机风险等级”为“高危”、“中危”。

2. 修复漏洞。
   - **自动修复漏洞**：仅Linux漏洞、Windows漏洞支持。此处以漏洞视角下，修复Linux漏洞为例，进行介绍。
     i. 在“漏洞管理”页面，单击目标漏洞“操作”的“修复”。
     ii. 在修复对话框，确认待修复的漏洞数量和影响资产数量，单击  ，开启备份。

     图 9-2 确认漏洞和创建备份

     iii. 单击“管理”，在创建备份弹窗，编辑服务器本次备份文件的名称后，单击“确定”。
     iv. 在修复对话框，勾选知晓风险后，单击“自动修复”。
     v. 单击漏洞名称，在漏洞详情页，选择“历史处置记录”页签，在目标漏洞“状态”列，查看漏洞修复状态。
        - “修复成功”表示该漏洞已被成功修复。更多状态说明，请参见**表漏洞修复状态说明**。
        - “修复失败”表示该漏洞修复失败，可能因为漏洞已不存在或漏洞已经被更改。您可以查看修复失败原因，参考HSS提供的方法，修复漏洞。具体操作，请参见**漏洞修复失败怎么办？**。
   - **手动修复漏洞**：Web-CMS漏洞、应用漏洞和应急漏洞不支持自动修复，需参考漏洞修复建议手动修复。
     i. 在“漏洞管理”页面，单击目标漏洞名称，在漏洞详情页面，查看修复建议。

ii. 参考漏洞修复方案，根据业务情况选择一个方案修复漏洞。

方案一：创建新的虚拟机执行漏洞修复

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

方案二：在当前主机执行修复

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

说明

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

- **忽略漏洞、漏洞添加白名单**

  如果某漏洞暂时无害，您可以忽略该漏洞。忽略仅忽略当次告警，下一次漏洞扫描仍然上报该漏洞。如果某漏洞不会对业务产生影响，可将漏洞加入白名单。加入白名单后，已扫描出的漏洞会被处理为忽略，不再上报，且下一次扫描时不再扫描该漏洞。具体操作，请参见**忽略漏洞**、**漏洞添加白名单**。

步骤3 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，否则企业主机安全仍认为您的漏洞未完成修复，将持续为您告警。其他类型的漏洞修复后，则无需重启服务器。

步骤4 修复验证。

在您手动修复漏洞完成后，建议您验证漏洞修复结果。具体操作，请参见**修复验证**。

----结束

相关操作

- HSS支持查看已处理漏洞的历史处置记录。您可以筛选“已处理”的漏洞，单击“漏洞名称”，在漏洞详情面板，查看“历史处置记录”。具体操作，请参见**查看漏洞历史处置记录**。
- HSS支持导出漏洞列表。具体操作，请参见**导出漏洞列表**。

10 使用 HSS 防御弱口令风险

应用场景

弱口令是指密码强度低，或广泛被使用，容易被攻击者破解的口令。常见的弱口令包括但不限于如下几种：

- 常见的系统默认口令，例如admin、root、tomcat、manager等。
- 纯数字、纯字母或简单的数字和字母组合，例如admin123、123456、abcde等。
- 具有特殊含义，容易被别人猜测到的口令，例如生日、姓名、手机号等。
- 多个系统账号使用同一个口令。

在服务器系统中使用弱口令，存在的风险包括但不限于以下几个方面：

- 信息泄露：攻击者通过猜测或暴力破解弱口令，可以入侵账户，获取用户的个人隐私信息和财务数据。
- 破坏系统：攻击者破解弱口令入侵系统，可以对系统进行恶意攻击，如删除重要数据、植入恶意软件、恶意修改程序等，导致系统瘫痪或无法正常运行。

HSS提供了经典弱口令检测，可以检测出主机系统和关键软件中设置的弱口令，包括Linux系统的MySQL、FTP、Redis及系统账号弱口令，Windows系统的系统账号弱口令等；建议您使用HSS检测服务器系统中的弱口令，并及时提升口令安全强度，定期更换口令，从而规避弱口令带来的安全风险。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护。详细操作请参见**HSS接入概述**。

如何规避弱口令风险

步骤1 检测是否存在弱口令。

使用HSS的基线检查中的弱口令检测功能，可以检测出当前服务器是否存在弱口令，具体步骤如下：

1. 配置弱口令检测策略。
   a. **登录管理控制台**。
   b. 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 企业主机安全”，进入主机安全平台界面。

c. 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”界面。

说明

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

d. 单击目标策略组名称，进入策略详情列表。

HSS提供了多个系统预置策略组，主机开启防护后，默认绑定系统预置策略组。您也可以通过单击已有策略组“操作”列的“复制”，新建策略组进行弱口令策略配置。具体操作，请参见**创建自定义策略组**。

e. 筛选出“弱口令检测”策略，在其操作列单击“开启”，开启弱口令检测。

f. 单击“弱口令检测”策略名称，进入到弱口令检测策略详情页面。

g. 自定义弱口令检测的检测时间、检测周期等策略内容，参数说明如**表10-1**所示。

表 10-1 弱口令检测策略内容参数说明

参数	说明
检测时间	配置弱口令检测的时间，可具体到每一天的每一分钟。
随机偏移时间（秒）	检测配置的弱口令时间的随机偏移时间，在“检测时间”的基础上偏移，可配置范围为“0~7200秒”。
检测日	弱口令检测日期。勾选周一到周日检测弱口令的时间。
自定义弱口令	您可以将疑似被泄露的口令添加在自定义弱口令文本框中，防止主机中的账户使用该弱口令，给主机带来危险。 填写多个弱口令时，每个弱口令之间需换行填写，最多可添加300条。
是否开启口令复杂度策略检测	口令复杂度策略是指服务器设置的口令规则和标准。开启“口令复杂度策略”检测，企业主机安全会在用户手动执行基线检查时，对服务器设置的口令复杂度策略进行检测。

h. 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

2. （可选）为服务器部署策略。

如果在**步骤1.1**中，您是基于新创建的自定义策略组进行弱口令策略配置，则完成策略组创建和策略配置后，您需要将新建的策略组部署应用到目标服务器，详细操作请参见**部署策略**。

3. 执行弱口令检查。

企业主机安全默认每日凌晨01：00左右将自动进行一次全量服务器的经典弱口令检测。

若您在**a. 配置弱口令检测策略**中已经自定义弱口令的自动检测时间和周期，则企业主机安全将按照您配置的检测时间和周期自动进行经典弱口令检测。

4. 查看弱口令检查结果。

a. 在主机安全平台界面的左侧导航栏，选择“风险预防 > 基线检查”，进入“基线检查”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。

b. 单击“经典弱口令检测”，在列表中，可以查看存在的弱口令。

步骤2 修改弱口令，提升口令安全强度。

根据**步骤1.4**中检测出的经典弱口令列表中的“服务器名称/IP地址”、“账户名称”、“账户类型”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。更多信息，请参见**如何设置安全的口令**。

步骤3 定期修改口令。

建议每隔90天修改一次口令。

----结束

如何设置安全的口令

- **建议设置的口令复杂度**

  为保证口令的安全，建议您按下述规则设置口令：

  - 密码长度范围为8到26位。
  - 密码至少包含以下4种字符中的3种：
    - 大写字母
    - 小写字母
    - 数字
    - Windows操作系统云服务器特殊字符：包括“!”、“@”、“$”、“%”、“^”、“-”、“_”、“=”、“+”、“[”、“{”、“(”、“)”、“}”、“]”、“:”、“,”、“.”、“/”、“?”、“~”“#”和“*”
    - Linux操作系统云服务器特殊字符：包括“!”、“@”、“$”、“%”、“^”、“-”、“_”、“=”、“+”、“[”、“{”、“}”、“]”、“:”、“,”、“.”、“/”、“?”、“~”“#”和“*”
  - 密码不能包含用户名或用户名的逆序。
  - Windows操作系统的云服务器，不能包含用户名中超过两个连续字符的部分。

- **常见系统的口令修改方法**

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

系统名称	修改登录口令	说明
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 **requirepass <password>;**	• 若已存在登录口令，则将其修改为复杂口令。 • 若不存在登录口令，则添加为新口令。 **说明** “password”为登录口令。
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

11 使用 HSS 查杀系统木马

应用场景

木马程序是当前网络安全领域一个重要问题，它通过不同方式入侵计算机系统，对用户数据安全、隐私保护和系统稳定性构成严重威胁。

为了防范木马，您需要及时更新操作系统和软件，使用安全的网络连接，避免下载和运行来自未知来源的文件。除此之外，您还可以使用HSS，查看和处置上报的木马告警，及时修复系统漏洞，多方位提升系统安全。

本文为您介绍如何通过HSS查杀系统木马。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护，详细操作请参见**HSS接入概述**。

步骤一：查杀系统木马

主机购买并开启HSS防护后，当主机被植入木马时，会触发HSS发送“木马”告警。您需要自行判断检测出的木马告警文件是正常业务文件，还是攻击者运行的恶意文件。如果确认为攻击事件，建议您对恶意文件进行隔离查杀。

步骤1 **登录管理控制台**。

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

步骤3 在左侧导航栏，选择“检测与响应 > 安全告警事件”，进入“主机安全告警”界面。

步骤4 在“待处理告警”区域，选择“恶意软件 > 木马”，查看指定时间范围内上报的木马告警。

图 11-1 木马告警

步骤5 在右侧告警列表中，单击告警事件的告警名称，查看木马告警的详细信息。

步骤6 在告警列表中，单击告警“操作”列的“处理”。

步骤7 在弹出的对话框中，“处理方式”选择“隔离查杀”。

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

----结束

步骤二：数据备份恢复与漏洞修复

- 数据备份恢复

  如果木马恶意程序导致了您的数据丢失，且您开通了CBR服务，可以尝试从CBR服务备份中恢复数据。详细操作，请参见**使用云服务器备份恢复数据**。

- 漏洞修复

  为了防止再次被木马入侵，您可以通过HSS的漏洞管理功能，查看并修复该服务器漏洞。详细操作，请参见**使用HSS扫描和修复漏洞**。

12 使用 HSS 应对挖矿攻击

应用场景

挖矿（Mining），又称加密货币挖矿（Cryptocurrency Mining），是指通过大量计算机运算获取加密货币的过程。由于运算过程需要耗费大量的计算资源和电力，为了降低成本，攻击者会在用户不知情或未经允许的情况下，向个人或企业的计算机和移动设备植入挖矿程序，占用其系统资源和网络资源进行挖矿，从而获取加密货币牟利。

当主机遭受挖矿攻击时，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。攻击者还可能通过挖矿程序窃取机密信息，比如机密文件、关键资产的用户名和密码等，导致资产遭受更进一步的损失。

HSS具备针对挖矿攻击的检测与响应能力，能检出挖矿病毒软件并将其隔离。本文介绍如何使用HSS检测并清除挖矿程序，以及如何对主机进行安全加固。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护，详细操作请参见**HSS接入概述**。

攻击时：快速清除挖矿程序

1. **处理挖矿告警，终止恶意进程。**
   a. **登录管理控制台**。
   b. 在页面左上角选择“区域”，单击☰，选择“安全与合规 > 企业主机安全”，进入主机安全平台界面。
   c. 在左侧导航栏，选择“检测与响应 > 安全告警事件”，进入“主机安全告警”界面。

      说明

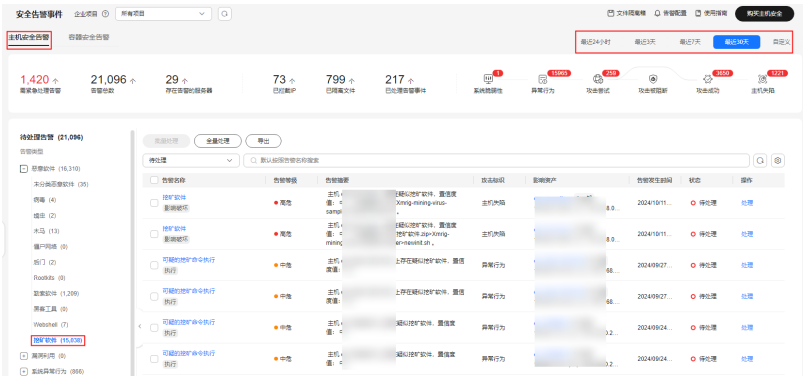
      如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。

   d. 查看并处理“挖矿软件”告警。

      当主机被植入挖矿程序时，会触发HSS发送“挖矿软件”告警。您需要自行判断检测出的挖矿告警文件是正常业务文件，还是攻击者运行的恶意文件。如果确认为攻击事件，建议您对挖矿程序进行隔离查杀。

i. 在待处理告警中，选择“恶意软件 > 挖矿软件”。

图 12-1 挖矿软件告警



ii. 在右侧告警列表中，单击告警事件的告警名称，可查看告警的详细信息。

iii. 在告警列表中，单击告警“操作”列的“处理”。

iv. 在弹出的对话框中，“处理方式”选择“隔离查杀”。

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

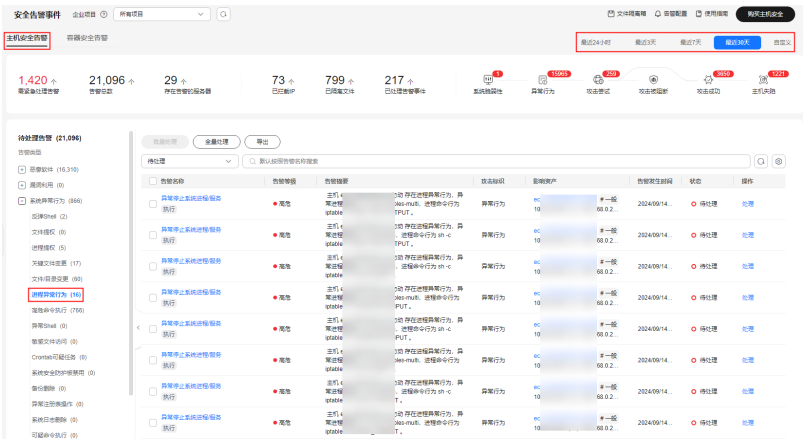
v. 单击“确定”。

e. **查看并处理“进程异常行为”告警。**

当出现主机挖矿行为时，会触发HSS发送“进程异常行为”告警。您需要自行判断检测出的异常进程是否合理，如果确认不合理，建议您对其进行隔离查杀。

i. 在待处理告警中，选择“系统异常行为 > 进程异常行为”。

图 12-2 进程异常行为告警



ii. 在右侧告警列表中，单击告警事件的告警名称，可查看告警的详细信息。

iii. 在告警列表中，单击告警“操作”列的“处理”。

iv. 在弹出的对话框中，“处理方式”选择“隔离查杀”。

v. 单击“确定”。

2. **排查其他自启动项，彻底清除挖矿威胁。**

   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。

   a. 在主机安全平台界面的左侧导航栏，选择“资产管理 > 主机指纹”，进入“主机指纹”界面。

   b. 单击“自启动项”，在下方选择“历史变动记录”页签，查看历史变动情况。

3. **扫描被攻击的服务器，深度查杀病毒。**

   HSS提供病毒查杀功能，使用特征病毒检测引擎，扫描服务器中的病毒文件。您可以快速扫描被攻击的服务器，深度清理潜在的恶意威胁。您需要自行判断扫描出的病毒文件是否合理，如果确认不合理，建议您对其进行隔离。

   a. 在主机安全平台界面的左侧导航栏，选择“主机防御 > 病毒查杀”，进入“病毒查杀”界面。

   b. 单击“快速查杀”。

   c. 根据界面提示，填写“快速查杀”任务相关参数。

      服务器请选择为被挖矿攻击的服务器，其他参数保持默认即可。更多信息，请参见**快速查杀**。

   d. 单击“开始扫描”。

   e. 待扫描任务完成后，在“病毒查杀”界面下方，可以查看扫描到的病毒文件。

   f. 在目标病毒文件所在行的操作列，单击“处理”。

   g. 在弹出的对话框中，“处理方式”选择“手动隔离文件”。

      隔离后，该病毒文件不能执行“读/写”操作，无法再对主机造成威胁。被成功隔离的文件会被添加到“文件隔离箱”中，后续，您可以到“文件隔离箱”中恢复或删除已隔离的文件。

   h. 单击“确定”。

攻击后：对主机进行安全加固

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**

  a. 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。

  b. 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。

     i. 设置安全口令，详细操作请参见**如何设置安全的口令**。

     ii. 使用密钥登录主机，详细操作请参见**使用私钥登录Linux主机**。

  c. 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。

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

- **口令安全加固**

口令	说明	操作步骤
复杂度	必须满足**如何设置安全的口令**的要求。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 密码策略”。 4. 确认“密码必须符合复杂性要求”已启用。
密码最长留存期	对于采用静态口令认证技术的设备，账户口令的留存期不应长于90天。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 密码策略”。 4. 配置“密码最长使用期限”不大于90天。
账户锁定策略	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次后，锁定该用户使用的账户。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“账户策略 > 账户锁定策略”。 4. 配置“账户锁定阈值”不大于10次。

- **授权安全加固**

授权	说明	操作步骤
远程关机	在本地安全设置中，从远端系统强制关机权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“从远端系统强制关机”，权限只分配给Administrators组。
本地关机	在本地安全设置中关闭系统权限只分配给Administrators组。	1. 打开控制面板。 2. 选择“管理工具 > 本地安全策略”。 3. 在“本地安全策略”窗口中，选择“本地策略 > 用户权限分配”。 4. 配置“关闭系统”，权限只分配给Administrators组。

授权	说明	操作步骤
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。

13 使用 HSS 监控 Linux 主机文件完整性

应用场景

文件完整性是指文件内容在存储、传输和处理过程中，保持不被未经授权的修改、删除或损坏的状态，从而确保文件内容的真实性和可靠性。在主机安全防护中，保障文件完整性的意义包括但不限于如下几个方面：

- 防止数据篡改：通过监控文件完整性，可以防止攻击者恶意篡改和破坏数据，以及防止由于软件故障或内部人员操作失误导致的数据损坏，从而保障数据的完整性和真实性。
- 提升主机安全：通过监控文件完整性，可以辅助您快速识别文件被非法修改的行为，从而迅速采取相应的安全措施，从而减少潜在的安全危险，提升主机防御能力。
- 满足合规要求：许多行业标准和法规，要求企业和组织保护敏感数据的完整性和安全性，通过监控文件完整性，可以避免因数据安全问题而面临的法律风险和罚款。

HSS提供主机安全告警和文件完整性管理功能，可以监控服务器中的文件或目录，针对可疑的更改文件或目录的行为进行告警。本文为您介绍如何使用HSS的相关功能监控Linux主机文件完整性。

主机安全告警和文件完整性管理的文件保护差异

HSS的主机安全告警功能和文件完整性管理功能均具备文件完整性监控能力，两者互补共同为文件提供全面的安全防护。两者的差异如表13-1所示。

表 13-1 主机安全告警和文件完整性管理的文件保护差异

差异类别	主机安全告警	文件完整性管理
监控类型	文件、目录	文件
告警类型	• 文件提权：对提升文件权限的行为进行告警。 • 文件/目录变更：实时监控系统文件/目录，对创建、删除、移动、修改属性或修改内容的操作进行告警。	关键文件变更：实时监控系统关键文件（例如：ls、ps、login、top等），对修改文件内容的操作进行告警。

差异类别	主机安全告警	文件完整性管理
文件保护原理	基于行为特征进行分析，关注可疑的行为或活动。	侧重关注文件的完整性，使用对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态。
支持的操作系统	• 文件提权：Linux • 文件/目录变更：Windows、Linux	Linux
优势	不仅能监控文件，还能监控目录，并且监控更改文件的行为类型更多。	永久保有文件被更改的记录，有助于运维人员调查取证攻击者的行为活动。

前提条件

主机已开启HSS专业版/企业版/旗舰版/网页防篡改版/容器版防护。详细操作请参见**HSS接入概述**。

操作步骤

步骤1 配置文件保护策略。

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 > 企业主机安全”，进入主机安全平台界面。
3. 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”界面。

   说明

   如果您的服务器已通过企业项目的模式进行管理，您可选择目标“企业项目”后查看或操作目标企业项目内的资产和检测信息。
4. 单击目标策略组名称，进入策略详情列表。

   HSS提供了多个系统预置策略组，主机开启防护后，默认绑定系统预置策略组。您也可以通过单击已有策略组“操作”列的“复制”，新建策略组进行文件保护策略配置。具体操作，请参见**创建自定义策略组**。
5. 筛选出“文件保护”策略，在“操作”列单击“开启”，开启文件保护检测。

   文件保护策略默认是开启状态，如果您关闭过该策略，则需要开启。
6. 单击“文件保护”策略名称，进入到文件保护策略详情页面。
7. 自定义监控文件目录、监控的操作类型等策略内容，参数说明如**表13-2**所示。

   表13-2中展示了文件保护策略的默认取值，您可以根据实际业务情况自定义配置文件保护策略。为避免文件完整性变更引起大量的误报类告警，从而增加运维的工作量，建议您按如下配置思路配置文件保护策略：

   a. 少量试验：初次配置文件保护策略时，建议仅在少量主机上进行试点。
   b. 策略调优：密切关注策略生效期间的准确性和适用性，根据其结果进一步改进配置的策略，减少误报。
   c. 正式应用：经过多轮的策略调优后，当命中结果已趋于稳定，误报基本不存在时，可以在更多主机上应用。

图 13-1 文件保护策略

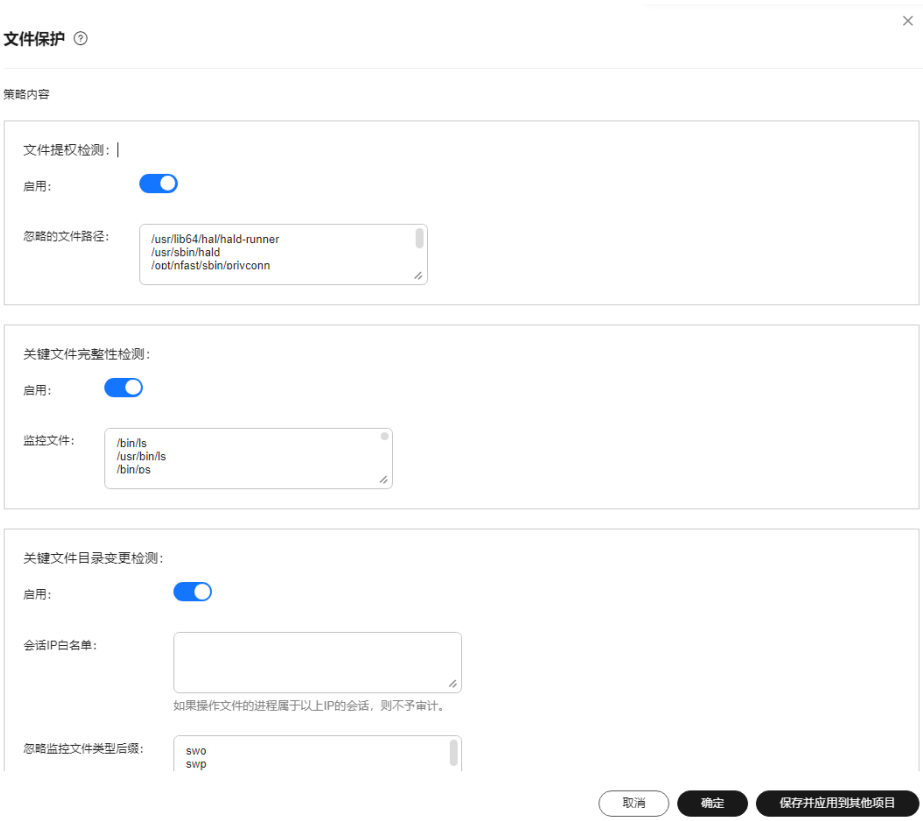


表 13-2 文件保护策略内容参数说明

策略模块	参数	默认参数取值	说明
文件提权检测	启用	**开启**	是否开启文件提权检测。 -  ：开启。 -  ：关闭。
	忽略的文件路径	- **/usr/lib64/hal/hald-runner** - **/usr/sbin/hald** - **/opt/nfast/sbin/privconn** - **/usr/sbin/dhclient** - **/usr/sbin/tcpdump**	填写需要忽略的文件路径。 文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。

策略模块	参数	默认参数取值	说明
关键文件完整性检测	启用	**开启**	是否开启关键文件完整性检测。 -  ：开启。 -  ：关闭。
	监控文件	- **/bin/ls** - **/usr/bin/ls** - **/bin/ps** - **/usr/bin/ps** - **/bin/bash** - **/usr/bin/bash** - **/bin/login** - **/usr/bin/login** - **/usr/bin/passwd** - **/usr/bin/top** - **/usr/bin/killall** - **/usr/bin/ssh** - **/usr/bin/wget** - **/usr/bin/curl**	填写需要监控文件完整性的文件路径。 文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。
关键文件目录变更检测	启用	**开启**	是否开启关键文件目录变更检测。 -  ：开启。 -  ：关闭。
	会话IP白名单	-	如果操作文件的进程属于白名单内的会话IP，则不予审计。
	忽略监控文件类型后缀	- **swo** - **swp** - **swpx** - **lck**	忽略监控的文件类型的后缀。

策略模块	参数	默认参数取值	说明
	忽略监控的文件路径	- **/etc/init.d/.depend.start** - **/etc/init.d/.depend.stop** - **/etc/init.d/.depend.halt** - **/etc/init.d/.depend.boot** - **/var/spool/cron/sed***	填写忽略监控文件的路径。
	监控登录密钥	**启用，并勾选“监控创建”、“监控删除”、“监控移动”、“监控修改”。**	是否开启监控登录密钥。 -  ：开启。 -  ：关闭。
	文件目录监控模式	**文件目录监控内容较多，以下仅展示部分监控路径。更详细的内容，请前往HSS管理控制台查看。** - **/etc/rc.d/rc.local** - **/etc/cron.allow** - **/etc/crontab** - **/var/spool/cron/root** - **/var/spool/cron/root** - **/etc/cron.allow** - **/etc/passwd** - **/etc/profile.d/zzz_euleros_history.sh** - **/etc/profile**	文件目录监控模式分为“日常运营”和“护网/重保”模式，“护网/重保”模式相较于“日常运营”模式默认监控的文件或目录路径更多。 这两种模式下预置了一些文件或目录监控路径，用户可以根据需求自定义添加或删除。 - 文件或目录路径：需要监控的文件或目录路径。添加前，请确认是合法路径；最多可添加50个文件或目录路径。 - 别名：文件或目录路径的别名，您可以定义一个易区分的名称。 - 监控子目录：勾选后会监控对应子目录的所有文件。不勾选，则不监控子目录文件。 - 监视创建、删除、移动、修改等：用户可根据业务实际情况选择是否勾选。

步骤2 （可选）为服务器部署策略。

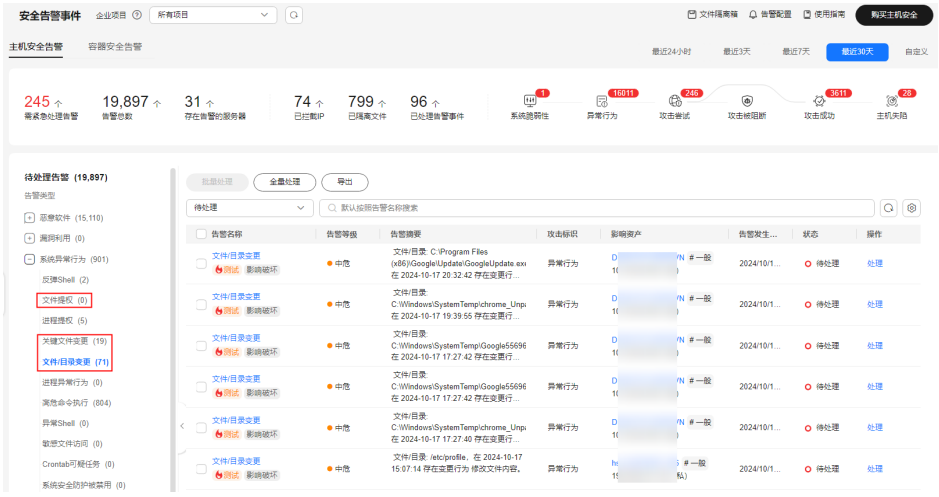
如果在**步骤1**中，您是基于新创建的自定义策略组进行的文件保护策略配置，则完成策略组创建和策略配置后，您需要将新建的策略组部署应用到目标服务器，详细操作请参见**部署策略**。

步骤3 查看并处理文件变更相关告警。

HSS会实时监控“文件保护”策略中配置的文件或目录路径，一旦发现异常更改将会立即告警。在收到告警后，请及时处理告警。

1. 在主机安全平台界面的左侧导航栏，选择“检测与响应 > 安全告警事件”，进入“主机安全告警”界面。
2. 在待处理告警列表中，展开“系统异常行为”类型告警，关注如**图13-2**所示的几类与文件变更相关的告警。

图 13-2 文件变更相关告警



3. 单击任一类型的告警，在右侧告警列表中，单击告警事件的告警名称，可查看告警详情。

图 13-3 查看告警详情

4. 根据告警详情中的“调查取证”信息，判断并处理告警。
   - **正常操作导致告警**

     在告警详情页面的右下方，单击“忽略”，忽略本次告警。
   - **可能是恶意文件或程序导致告警**
     i. 查看并确认主机是否同时存在有反弹shell、异常登录或恶意软件等高危告警，如果有，主机可能被攻破，请立刻对主机进行安全排查。
     ii. 主机排查完毕后，在告警详情页面的右下方，单击“我已手动处理”，关闭该告警。

步骤4 查看文件变更记录。

文件完整性管理功能页面会一直保有服务器的文件变更记录，有助您定位发现可疑的更改。

1. 在企业主机安全控制台的左侧导航栏选择“主机防御 > 文件完整性管理”，进入文件完整性管理界面。
2. 查看云服务器的文件变更情况。

----结束

14 利用白名单机制避免告警误报

应用场景

企业主机安全HSS为主机、容器提供了入侵检测防护，支持检测账户暴力破解、进程异常行为、网站后门、恶意软件等多种恶意行为或攻击，并在检测到异常后会及时告警上报通知用户。用户收到的告警中，可能包含正常业务触发而导致的告警，这种情况下，用户可以通过加白的方式，让HSS后续对信任对象产生的告警进行忽略不再上报，从而减少运维工作量，提升运营运维效率。

本文为您介绍如何通过HSS的白名单机制避免告警误报。

白名单机制

HSS提供了两种不同的白名单机制来处理告警，分别是告警白名单和检测策略白名单，通过这两种白名单加白后的对象，HSS都不会对其产生的行为进行告警。两种白名单的详细说明如表14-1所示。

表 14-1 白名单机制

白名单机制	说明	优势	劣势
告警白名单	在处理告警时，处理方式可以选择将告警加入告警白名单，并配置告警白名单规则，后续命中白名单规则的异常事件，HSS只检测但不上报告警。	HSS会根据告警内容自动联想预置白名单规则，您在处理已产生的告警过程中可快速对告警进行加白。	无法提前加白，只能等待告警触发。
检测策略白名单	HSS通过Agent对服务器进行检测，Agent的检测范围可通过控制台上下发的策略进行控制，因此用户可在策略中为信任的对象加白，策略配置完成下发后，HSS将不对策略加白的对象进行告警。	• 无需等待告警触发，可提前将信任的对象添加到白名单中。 • 容器类告警，Pod、镜像、组织等无法添加告警白名单，可添加检测策略白名单。	无法同步处理已产生的告警。

添加告警白名单

主机安全告警和容器安全告警添加告警白名单的操作流程基本一致，如下操作以处理主机安全告警中的“高危命令执行”告警为例进行说明。

步骤1 登录管理控制台。

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

步骤3 在左侧导航栏中，单击“检测与响应 > 安全告警事件”，在“主机安全告警”页签，查看上报的告警。

步骤4 单击告警名称，查看告警详情，判断该告警是否为正常业务触发。

可通过查看告警详情中的“告警信息”、“调查取证”、“相似告警”等分析确认执行命令操作是否是正常业务触发。

图 14-1 查看告警详情

步骤5 如果该告警是正常业务触发，单击“加入告警白名单”。

图 14-2 加入告警白名单

步骤6 在“处理告警事件”面板，单击“新增规则”，配置告警白名单触发规则。相关参数说明请参见**表14-2**。

图 14-3 告警白名单规则

表 14-2 告警白名单规则参数说明

参数	示例	说明
加白字段	**进程命令行**	加白字段即需要加白的对象类型，主机安全告警支持的加白字段包括： • 进程路径 • 进程命令行 • 文件路径 • 用户名称 • 远程IP 告警类型不同则可加白的字段不同。

参数	示例	说明
通配符	**包含**	支持选择的通配符如下： • 包含：告警信息包含白名单规则“描述”时，HSS不进行告警。 • 相等：告警信息完全匹配白名单规则“描述”时，HSS不进行告警。
描述	**ls -l /run/canal/plugins/yangtse-agent.sock**	HSS会自动联想为检测到的可疑进程、文件等填充加白内容。该内容也支持自定义。

说明

同一个告警支持添加多条白名单规则。如果添加多条规则，相互之间为或的关系。

步骤7 在“处理告警事件”面板，单击“确定”，告警加白完成。

----结束

添加检测策略白名单

HSS支持添加白名单的检测策略以及策略对应的告警请参见**表14-3**。

表 14-3 支持添加白名单的检测策略

策略名称	对应的告警
容器信息收集	容器挂载异常
集群入侵检测	Kubernetes事件删除、创建特权Pod、Pod中使用交互式shell、创建敏感目录Pod、创建主机网络的Pod、创建主机Pid空间的Pod、普通pod访问、APIserver认证失败、普通Pod通过Curl访问APIServer、系统管理空间执行exec、系统管理空间创建Pod、创建静态Pod、创建DaemonSet、创建集群计划任务、List Secrets操作、枚举用户可执行的操作、高权限RoleBinding或ClusterRoleBinding、ServiceAccount创建
容器逃逸	容器高危系统调用、Shocker攻击、DirtCow攻击、容器文件逃逸攻击
容器信息模块	容器命名空间、容器开放端口、容器安全选项、容器挂载目录
容器进程白名单	容器进程异常事件上报
无文件攻击检测	进程注入、动态库注入、内存文件进程
文件保护	文件目录变更、关键文件变更、文件提权

策略名称	对应的告警
HIPS检测	Windows Defender防护被禁用、可疑的黑客工具、可疑的勒索加密行为、隐藏账号创建、读取用户密码凭据、可疑的SAM文件导出、可疑shadow copy删除操作、备份文件删除、可疑勒索病毒操作注册表、可疑的异常进程行为、可疑的扫描探测、可疑的勒索病毒脚本运行、可疑的挖矿命令执行、可疑的禁用windows安全中心行为、可疑的停止防火墙服务行为、可疑的系统自动恢复禁用、Office创建可执行文件、带宏Office文件异常创建、可疑的注册表操作、Confluence远程代码执行、MSDT远程代码执行、使用Wevtutil清除Windows日志、使用Fsutil去除日志、regsvr32发起的可疑http请求、使用Windows Defender下载负载、Windows远程命令执行、Log4shell漏洞执行、可疑的计划任务操作、可疑的Windows命令执行、Windows入侵工具传输、可疑的反弹shell命令、执行远程可疑脚本、可疑的软件安装、perl反弹shell、awk反弹shell、python反弹shell、lua反弹shell、mkfifo/openssl反弹shell、php反弹shell、ruby反弹shell、使用rssocks进行反向代理、bash反弹shell、ncat反弹shell、exec重定向反弹shell、node反弹shell、telnet双端口反弹shell、nc反弹shell、socat反弹shell、php_socket反弹shell、socket/tchsh反弹shell、使用vigr/vipw修改文件、清除或替换系统安全日志、软连接ssh后门、替换ssh密钥、使用curl/wget安装后门 使用代理软件工具、python/base64执行、sudo提权漏洞利用、增加uid为0(root权限)的系统账号、利用$IFS绕过执行命令修改权限、wipe删除文件或目录、github敏感信息泄露、使用命令进行arp欺骗、查看系统数据库passwd相关记录、curl/wget/gcc下载CVE/CNVD漏洞、可疑的驱动加载、卸载或停止主机安全程序、strace获取ssh凭据、Golang反弹shell、ldapsearch探测域内信息、通过perl脚本探测提权漏洞、通过bash脚本探测提权漏洞、通过python脚本探测提权漏洞、Enumy提权枚举工具、Hydra暴力破解工具、CDK容器渗透工具、stowaway代理工具、CF云渗透工具、通过redis-rogue-server入侵redis、通过hack-browser-data收集浏览器数据、可疑的探测主机行为、可疑的下载行为、可疑的交互式bash shell生成、sudo权限提升、vim权限提升、awk权限提升、混淆的shell命令、劫持LD_PRELOAD动态链接库、劫持动态链接器、可疑的敏感文件读取、可疑的敏感文件修改、socat端口转发、ngrok端口转发、rinetd端口转发、portmap端口转发、portforward端口转发、rakshasa端口转发、检测到黑客工具earthworm、设置suid/sgid提权、进程异常行为、可疑的计划任务/自启动项创建、find权限提升、访问恶意域名或IP、使用rcsocks/ssocks进行反向代理、SSH端口转发、HashDump攻击、procdump攻击
登录安全检测	尝试暴力破解、爆破成功、用户登录成功、异地登录、用户登录拒绝、用户首次登录、系统账号弱口令
恶意文件检测	异常shell、反弹shell、恶意软件
端口扫描检测	端口扫描
root提权	进程异常行为、可疑的进程提权、进程异常外联
实时进程	高危命令执行

策略名称	对应的告警
rootkit检测	可疑的rootkit

上表中所述策略配置白名单的详细操作如下：

须知

如果您是基于新创建的自定义策略组进行的文件保护策略配置，则完成策略组创建和策略配置后，您需要将新建的策略组部署应用到目标服务器，详细操作请参见**部署策略**。

容器信息收集

步骤1 **登录管理控制台**。

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

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”页面。

步骤4 选择服务器对应的容器版策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“容器信息收集”策略名称，进入策略详情页面，配置“挂载目录白名单”。

图 14-4 容器信息收集策略

表 14-4 容器信息收集策略白名单参数说明

参数	示例	说明
挂载目录白名单	**/test**	填写允许挂载的挂载目录，多个挂载目录路径以回车符换行分隔。 路径以*结束表示目标路径下的所有子目录，不包括主目录。 例如，设置/var/test/*为白名单目录，表示目录/var/test/下的所有子目录为白名单目录，不包括test这层。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

集群入侵检测

步骤1 登录管理控制台。

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

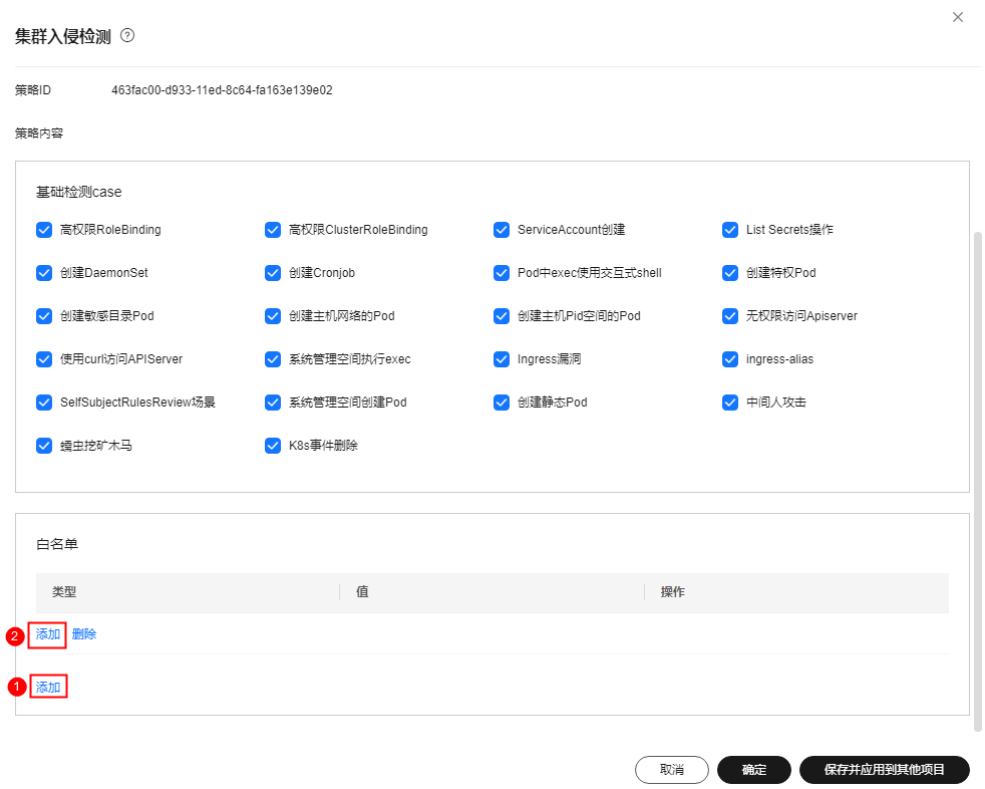
步骤3 在左侧导航栏，选择“安全运营 > 策略管理”，进入“策略管理”页面。

步骤4 选择服务器对应的容器版策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“集群入侵检测”策略名称，进入策略详情页面。

步骤6 在白名单区域，单击“添加”，再单击“添加”，添加一条白名单输入框。

图 14-5 添加白名单输入框



步骤7 在“类型”选框中单击下拉列表，选择添加白名单的类型，并填写对应类型的值。

图 14-6 集群入侵检测策略

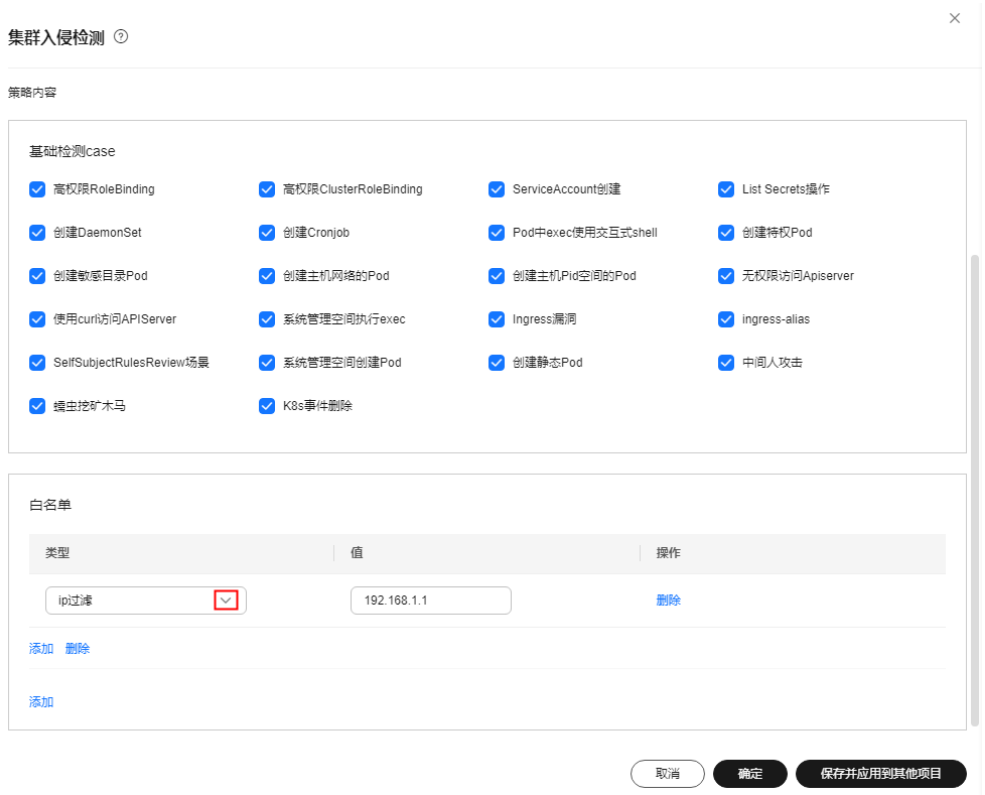


表 14-5 集群入侵检测白名单参数说明

参数	示例	说明
类型	**ip过滤**	自定义添加在检测中需要忽略的类型。 支持的类型如下： • ip过滤 • pod名称过滤 • image名称过滤 • 执行用户过滤 • pod标签过滤 • namespace过滤
值	**192.168.1.1**	填写类型具体的值。此处示例选择“ip过滤”，则填写具体的IP地址。

步骤8 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

容器逃逸策略

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应的容器版策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“容器逃逸”策略名称，进入策略详情页面，配置白名单。

可配置镜像、进程、Pod这些不同级别的白名单，您可以根据需求选择配置任意类型的白名单。

图 14-7 容器逃逸策略策略

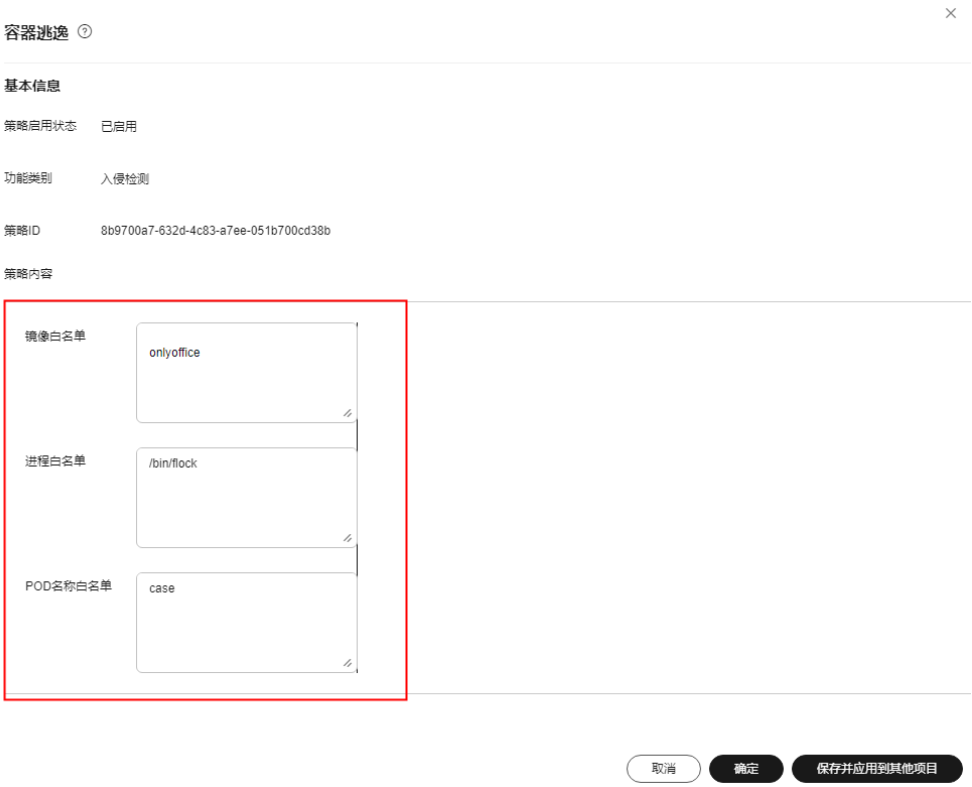


表 14-6 容器逃逸策略白名单参数说明

参数	示例	说明
镜像白名单	**onlyoffice**	填写无需检测容器逃逸行为的**镜像名称**，镜像名只能包含字母、数字、下划线、中划线，多个镜像名以回车换行隔开，最多可添加100个镜像名。
进程白名单	**/bin/flock**	填写无需检测容器逃逸行为的**进程全路径**，进程全路径只能包含字母、数字、下划线、中划线，多个进程名以回车换行隔开，最多可添加100个进程路径。
POD名称白名单	**case**	填写无需检测容器逃逸行为的**Pod名称**（非Pod UID），Pod名称只能包含字母、数字、下划线、中划线，多个Pod名称以回车换行隔开，最多可添加100个Pod名称。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

容器信息模块

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应的容器版策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“容器信息模块”策略名称，进入策略详情页面，配置白名单。

可配置容器、组织白名单，根据需求选择配置即可。

图 14-8 容器信息模块策略

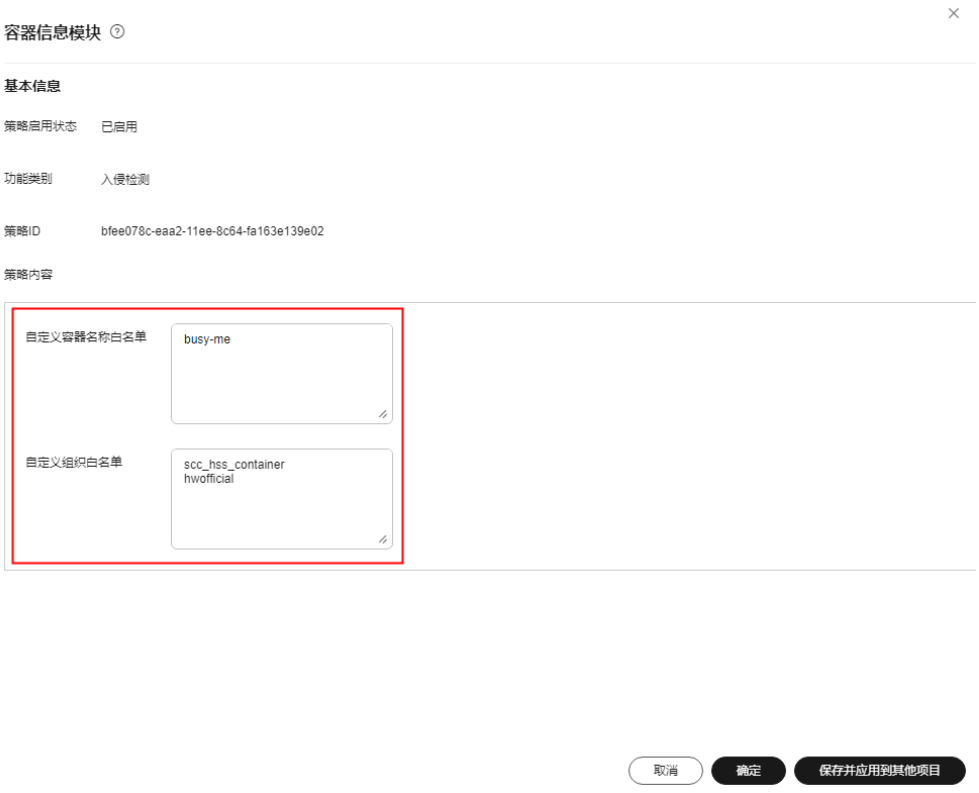


表 14-7 容器信息模块白名单参数说明

参数	示例	说明
自定义容器名称白名单	**busy-me**	自定义填写需要HSS不告警的**容器名称**。 • 基于Docker运行时的容器可以配置简单名称，HSS会自行模糊匹配；其他运行时的容器会根据名称进行精确匹配。 • 多个容器名称以回车换行分隔，最多可添100个白名单。

参数	示例	说明
自定义组织白名单	**scc_hss_container** **hwofficial**	自定义填写需要HSS不告警的镜像所属**组织名称**。 多个组织名称以回车换行分隔，最多可添100个白名单。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

容器进程白名单

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应的容器版策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“容器进程白名单”策略名称，进入策略详情页面，配置容器进程白名单。

图 14-9 容器进程白名单策略

表 14-8 容器进程白名单参数说明

图14-9中参数编号	参数		示例	说明
①	动态白名单			开启动态白名单  ，HSS对容器进程的检测机制如下：HSS默认容器是单进程模型，即容器只运行容器启动参数中配置的进程命令行。HSS会在容器启动时，自动识别容器启动的entrypoint配置，根据启动entrypoint识别主进程，如果容器运行过程，运行了主进程外的其他进程则告警。
②	白名单	模糊匹配	**勾选**	是否启动对目标进程路径的模糊匹配。
		镜像名称	-	填写进程所属镜像的名称。 镜像名称或镜像ID选填一个即可。
		镜像ID	**sha256:ab1305a5e0a87345ad8cd91015990b7c34fb7a7e682266937872cefc9eb36671**	填写进程所属镜像的ID。 镜像名称或镜像ID选填一个即可。
		进程	**/tmp/testw**	填写无需检测的进程路径。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

无文件攻击检测

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应版本的策略组，单击策略组名称，进入策略组详情页面。

步骤5 单击“无文件攻击检测”策略名称，进入策略详情页面，配置白名单。

图 14-10 无文件攻击检测策略

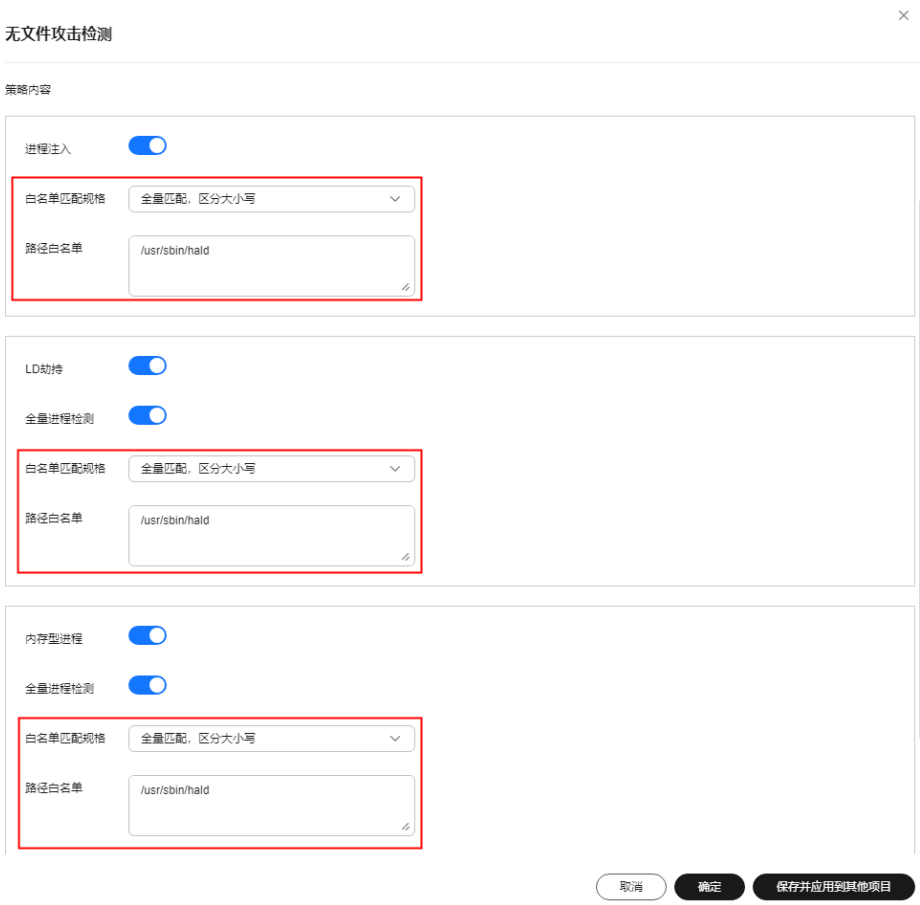


表 14-9 无文件攻击检测白名单参数说明

参数	示例	说明
白名单匹配规则	**全量匹配，区分大小写**	即“路径白名单”匹配规则，单击选择白名单匹配规则，可选项如下： ● 全量匹配，区分大小写 ● 全量匹配，不区分大小写 ● 模糊匹配
路径白名单	**/usr/sbin/hald**	输入无需对“进程注入”、“LD劫持”或“内存型进程”威胁进行检测的路径，多个路径可通过回车换行分隔。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

文件保护

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“文件保护”策略名称，进入策略详情页面，配置忽略检测的文件类型或路径。

图 14-11 文件保护策略

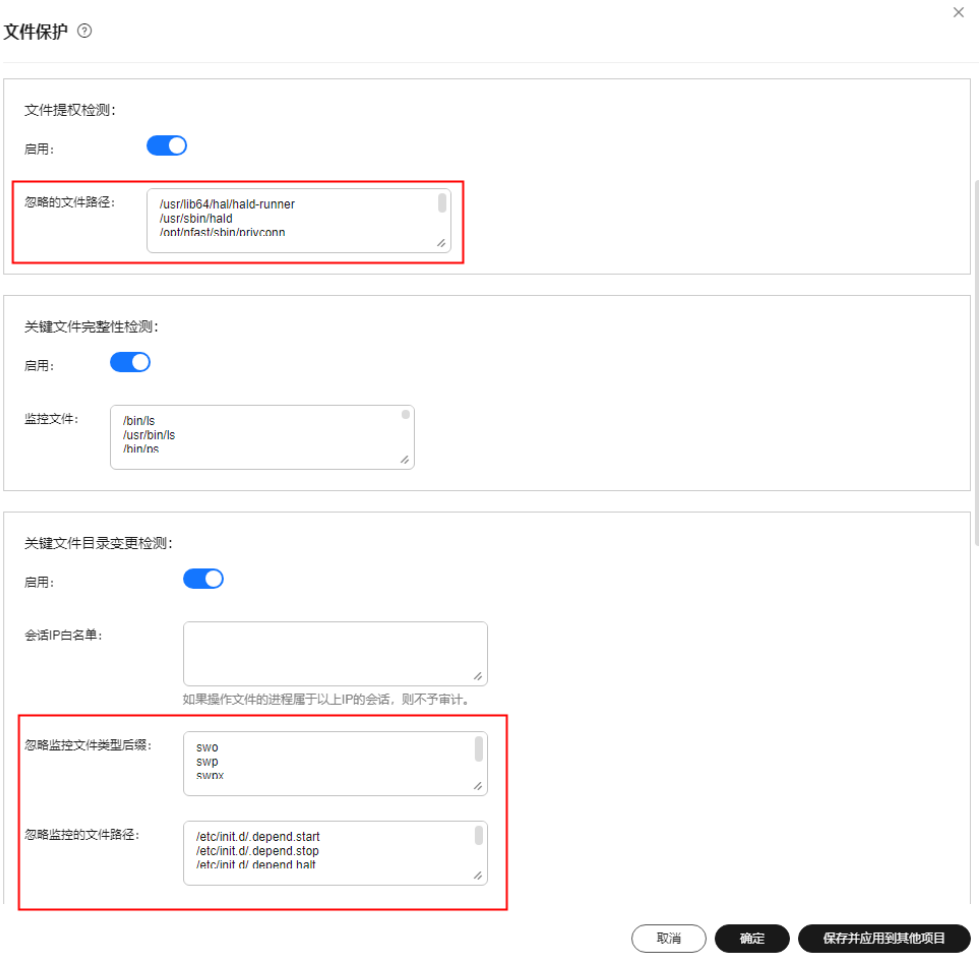


表 14-10 文件保护策略白名单参数说明

参数模块	参数	示例	说明
文件提权检测	忽略的文件路径	**/usr/lib64/hal/hald-runner** **/usr/sbin/hald** **/opt/nfast/sbin/privconn** **/usr/sbin/dhclient** **/usr/sbin/tcpdump**	填写忽略的文件路径。文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。
关键文件目录变更检测	忽略监控文件类型后缀	**swo** **swp** **swpx** **lck**	填写忽略监控的文件类型的后缀。多个文件类型通过回车换行分隔。
	忽略监控的文件路径	**/etc/init.d/.depend.start** **/etc/init.d/.depend.stop** **/etc/init.d/.depend.halt** **/etc/init.d/.depend.boot** **/var/spool/cron/sed***	填写忽略监控文件的路径。文件路径以“/”开头，不能以“/”结尾，多个路径通过回车换行分隔且名称中不能包含空格。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

HIPS 检测

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“HIPS检测”策略名称，进入策略详情页面，配置可信进程。

图 14-12 HIPS 检测策略

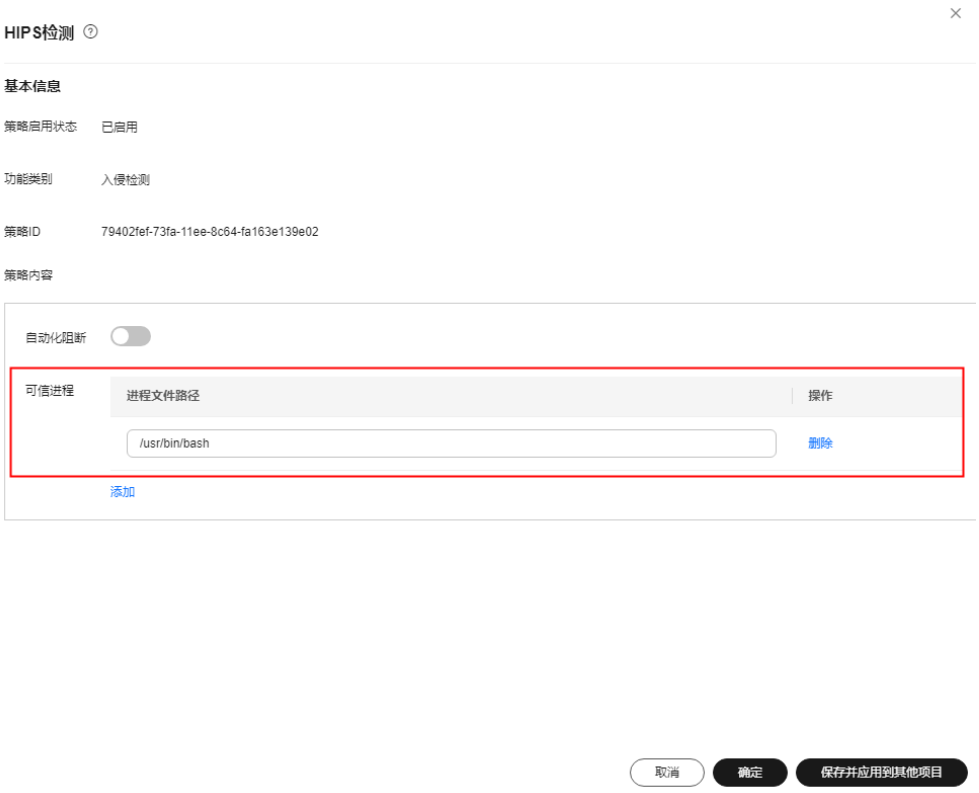


表 14-11 HIPS 检测策略白名单参数说明

参数	示例	说明
可信进程文件路径	**/usr/bin/bash**	添加可信进程全路径。单击“添加”可增加一条路径输入框，单击“删除”可删除进程文件路径。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

登录安全检测

登录安全检测策略对暴力破解账户的行为不仅会进行告警，还会拦截暴力破解IP。如果仅为告警添加登录告警白名单，只能避免后续告警，无法解决可信IP被拦截的问题，您可以在登录安全检测策略中设置可信IP，避免告警和拦截。

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“登录安全检测”策略名称，进入策略详情页面，配置可信IP。

图 14-13 登录安全检测策略

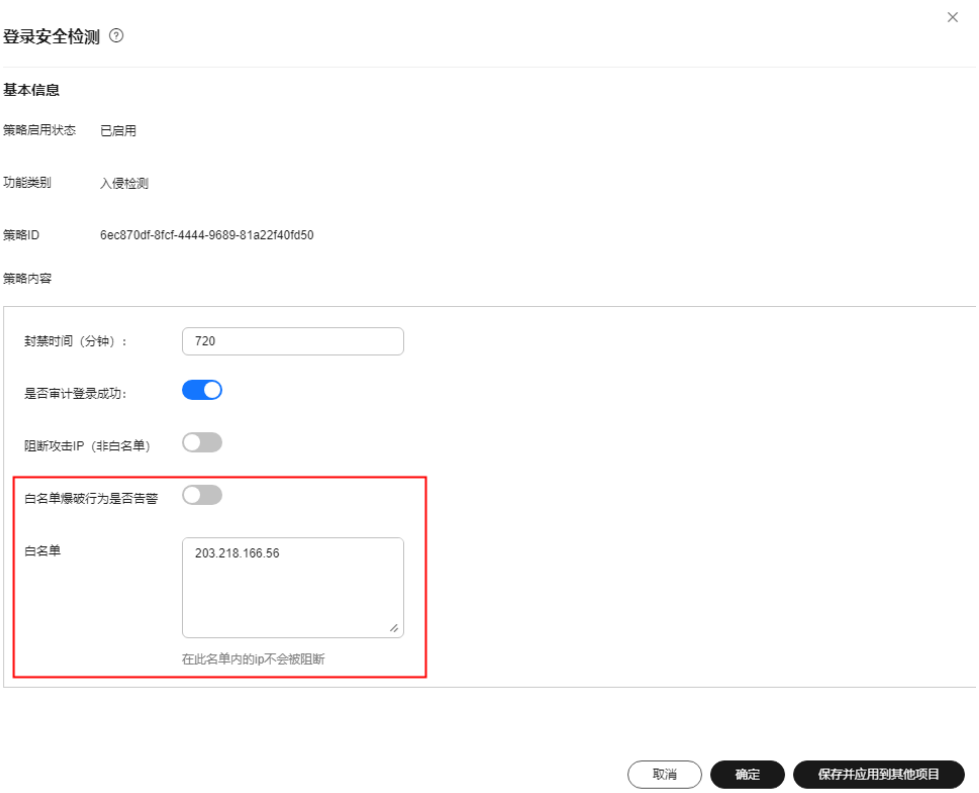


表 14-12 登录安全检测策略白名单参数说明

参数	示例	说明
白名单暴破行为是否告警		在白名单内的IP发生暴力破解行为是否告警。  表示不告警。
白名单	**203.218.166.56**	将IP添加到白名单后，HSS不会阻断白名单内IP的暴破行为。 最多可添加50个IP或网段到白名单，且同时支持IPv4和IPv6。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

恶意文件检测

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“恶意文件检测”策略名称，进入策略详情页面，配置需要忽略检测的内容。

配置需要忽略的内容即可，无需全部填写。

图 14-14 恶意文件检测策略

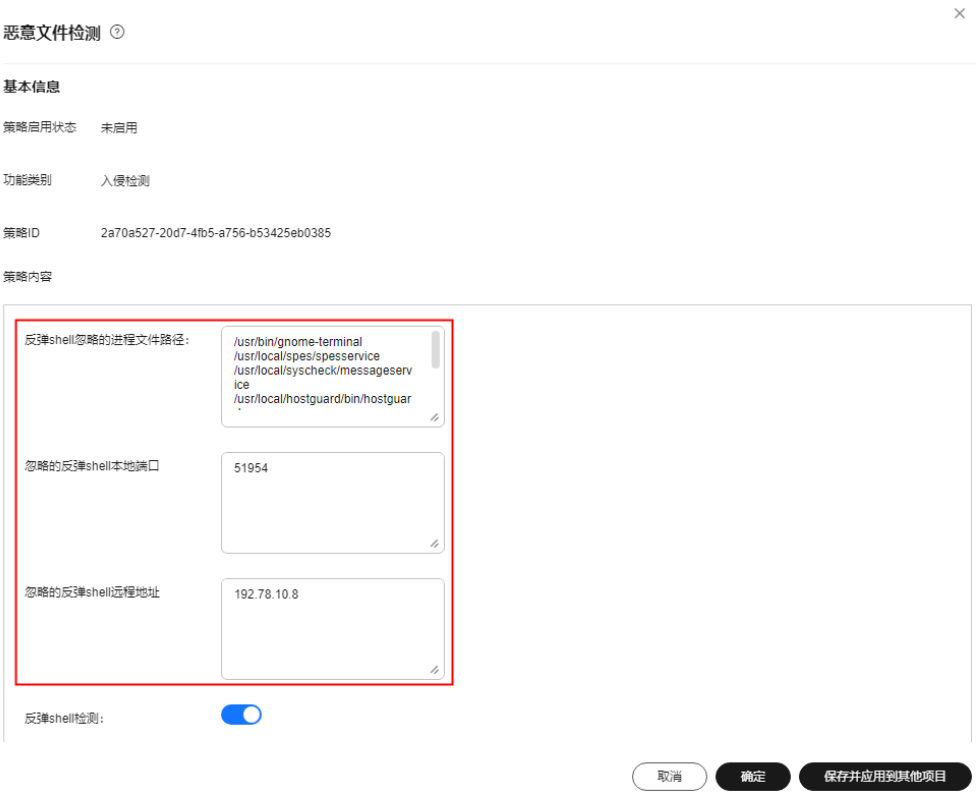


表 14-13 登恶文件检测策略白名单参数说明

参数	示例	说明
反弹shell忽略的进程文件路径	**/usr/bin/gnome-terminal** **/usr/local/spes/spesservice** **/usr/local/syscheck/messageservice** **/usr/local/hostguard/bin/hostguard**	填写反弹shell检测忽略的进程文件全路径。 文件路径以“/”开头，不能以“/”结尾。多个路径通过回车换行分隔且名称中不能包含空格。
忽略的反弹shell本地端口	**51954**	填写反弹shell检测忽略的本地端口。多个端口以英文逗号分隔。
忽略的反弹shell远程地址	**192.78.10.8**	填写反弹shell检测忽略的远程IP地址或网段。多个地址或网段以英文逗号分隔。支持IPv4和IPv6。 例如： • IPv4地址：192.78.10.3 • IPv4网段：192.78.10.0/255.255.255.0或192.78.10.0/24 • IPv6地址：2001:0db8:86a3:08d3:1319:8a2e:0370:7344 • IPv6网段：234e:0:4567 3d/ffff ffff:ffff:ffff::0或2001:db8:832:11::/64

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

端口扫描检测

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“端口扫描检测”策略名称，进入策略详情页面，配置源IP白名单。

图 14-15 端口扫描检测策略

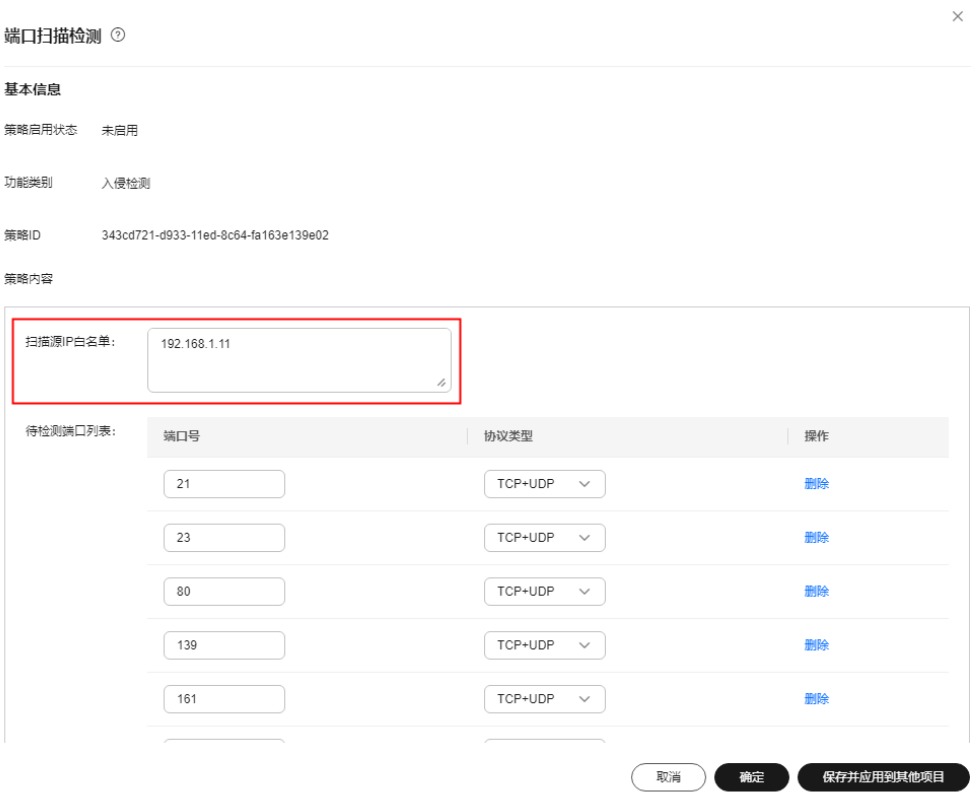


表 14-14 端口扫描检测策略白名单参数说明

参数	示例	说明
扫描源IP白名单	**192.168.1.11**	端口扫描检测忽略的源IP。支持IP地址或IP掩码，多个IP地址或掩码以英文逗号分隔。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

root 提权

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“root提权”策略名称，进入策略详情页面，配置忽略的进程文件路径。

图 14-16 root 提权策略

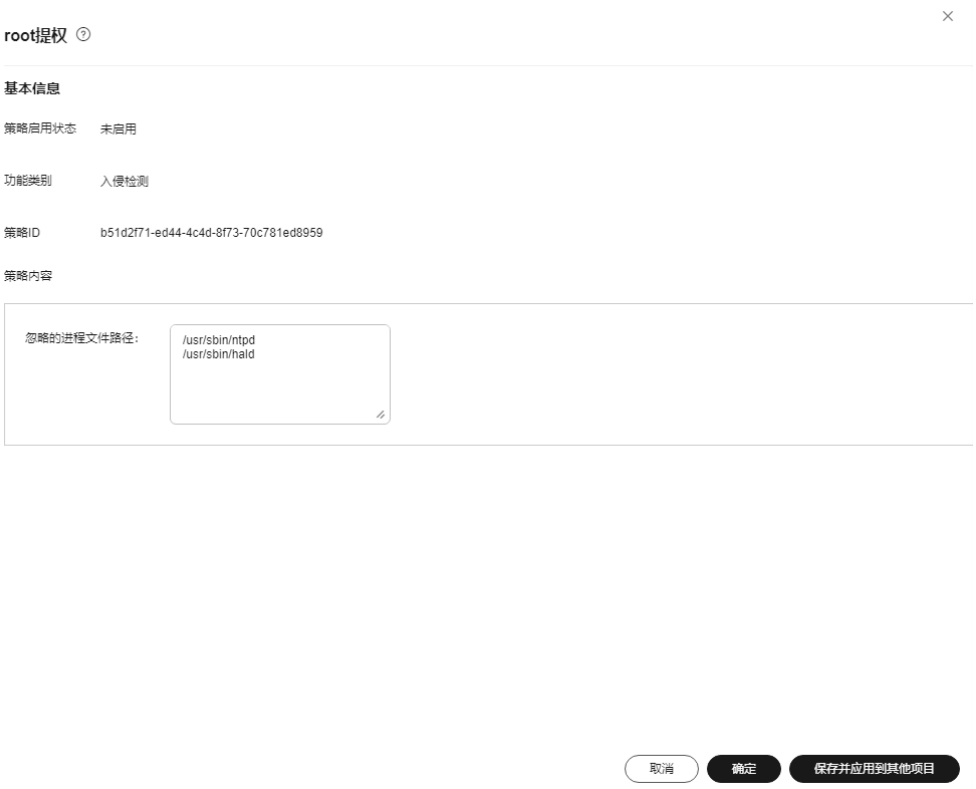


表 14-15 root 提权策略白名单参数说明

参数	示例	说明
忽略的进程文件路径	**/usr/sbin/ntpd** **/usr/sbin/hald**	填写忽略的进程文件全路径。 文件路径以“/”开头，不能以“/”结尾。多个路径通过回车换行分隔且名称中不能包含空格。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

实时进程

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“实时进程”策略名称，进入策略详情页面。

步骤6 在“白名单”区域，单击“添加”，添加一行白名单输入框。

步骤7 根据提示配置白名单参数。

图 14-17 实时进程策略

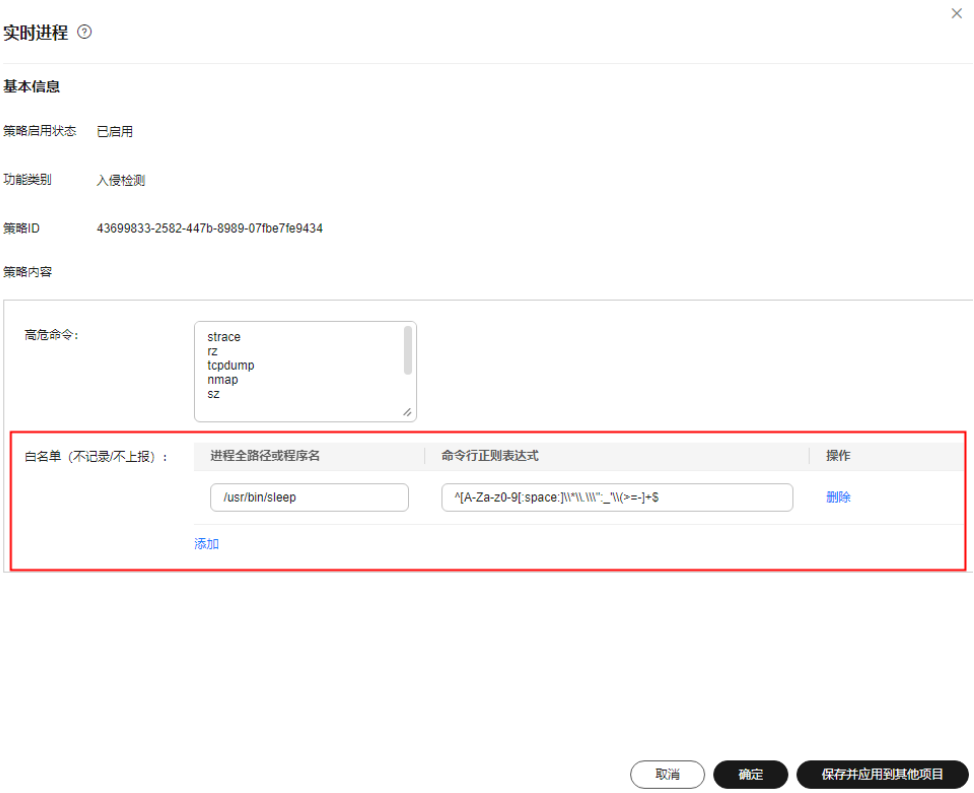


表 14-16 实时进程策略白名单参数说明

参数	示例	说明
进程全路径或程序名	**/usr/bin/sleep**	添加检测时放行、忽略的进程全路径或程序名。
命令行正则表达式	**^[A-Za-z0-9[:space:]*\\.\\\":_'\\(>=-]+$**	填写需要加白的命令行的正则表达式。 此项非必填。

步骤8 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束

rootkit 检测

步骤1 登录管理控制台。

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

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”页面。

步骤4 选择服务器对应防护版本的策略组，进入策略组详情页面。

步骤5 单击“rootkit检测”策略名称，进入策略详情页面，配置内核模块白名单。

图 14-18 rootkit 检测策略

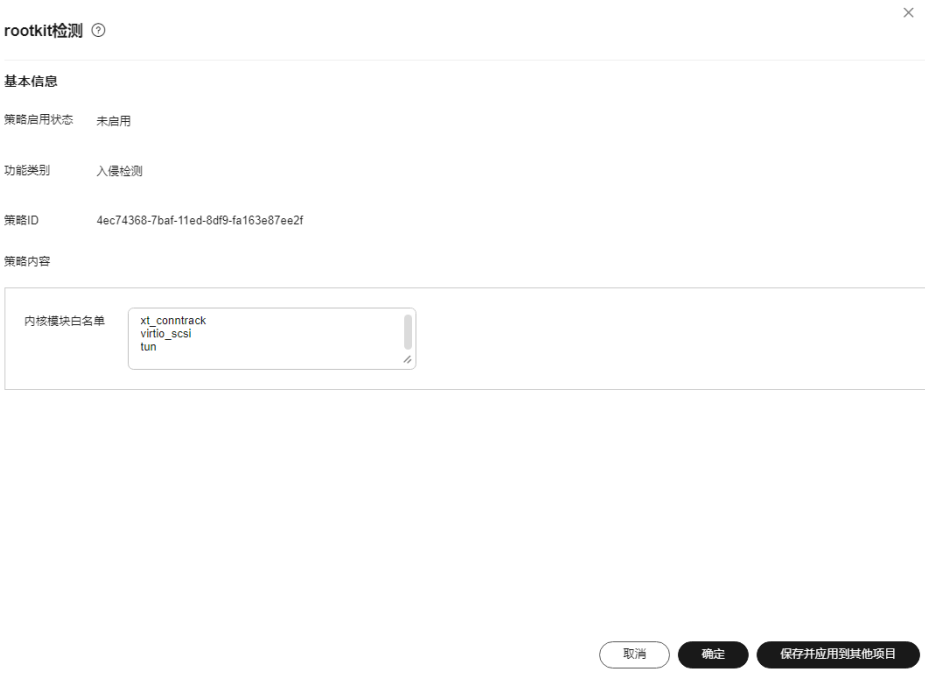


表 14-17 rootkit 检测策略白名单参数说明

参数	示例	说明
内核模块白名单	**xt_conntrack** **virtio_scsi** **tun**	自定义填写检测时忽略的内核模块名称。 可填写多个，不同模块名称之间用回车换行分隔，最多可添加10个。

步骤6 确认无误，单击“确定”，完成修改。

如果企业项目选择的“所有项目”，且修改的默认策略组的策略，您可以单击“保存并应用到其他项目”，将当前策略内容的修改应用到其他同版本策略下。

----结束