

主机安全服务

# 最佳实践

文档版本 07  
发布日期 2023-11-17



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

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

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为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

<b>1 HSS 登录安全加固最佳实践</b>	<b>1</b>
<b>2 漏洞检测与修复最佳实践</b>	<b>11</b>
2.1 Git 用户凭证泄露漏洞 ( CVE-2020-5260 )	11
2.2 SaltStack 远程命令执行漏洞 ( CVE-2020-11651/CVE-2020-11652 )	13
2.3 OpenSSL 高危漏洞 ( CVE-2020-1967 )	14
2.4 Adobe Font Manager 库远程代码执行漏洞 ( CVE-2020-1020/CVE-2020-0938 )	15
2.5 Windows 内核特权提升漏洞 ( CVE-2020-1027 )	17
2.6 Windows CryptoAPI 欺骗漏洞 ( CVE-2020-0601 )	18
<b>3 HSS 多云纳管部署</b>	<b>20</b>
3.1 应用场景	20
3.2 安装部署流程	21
3.3 安装部署	24
3.3.1 华为云解决方案	24
3.3.2 混合云解决方案	24
3.4 验证使用	25
3.5 线下主机专线接入公有云	25
3.5.1 步骤一：创建代理服务器	25
3.5.2 步骤二：为代理服务器安装 Agent	26
3.5.3 步骤三：安装配置 nginx	27
3.5.4 步骤四：制作安装包/安装命令	33
3.5.5 步骤五：为线下服务器安装 Agent	36
<b>4 勒索病毒防护最佳实践</b>	<b>37</b>
4.1 什么是勒索软件攻击	37
4.2 被勒索软件攻击的过程	37
4.3 如何避免成为勒索受害者 ( 通用举措 )	38
4.4 华为云勒索防护组合拳 “HSS+CBR”	39
4.4.1 概述	39
4.4.2 识别并修复勒索风险入口	41
4.4.3 开启勒索病毒防护和备份	43
4.4.4 恢复服务器数据	46
<b>5 通过云堡垒机安装主机安全服务的 Agent</b>	<b>47</b>

---

A 修订记录.....	50
-------------	----

# 1 HSS 登录安全加固最佳实践

在使用服务器的过程中，频频出现服务器被入侵、攻击的事件，但在被入侵、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，增强登录时的安全性成为了防护服务器安全、保证业务正常运行的第一道安全门。

## 前提条件

所有登录安全加固的配置场景均需要已购买云服务器且已开启防护。

## 登录安全加固场景

您可在主机安全服务通过配置常用登录地、常用登录IP、SSH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。

为了登录时的高度安全性，建议您对所有场景进行配置。

### 说明

双因子登录认证需购买基础版的包年/包月模式或企业版及以上版本方可支持，登录安全检测需购买企业版及以上版本才可支持，其余配置场景购买基础版即可满足。

图 1-1 HSS 登录安全加固场景



## 常用登录地配置

配置常用登录地后，主机安全服务将对非常用登录地登录云服务器的行为进行告警，每台云服务器可添加多个登录地。

### 约束限制

单一账号最多可添加10个常用登录地。

### 操作步骤

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

图 1-2 添加常用登录地



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

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

----结束

## 常用登录 IP 配置

配置常用登录IP后，主机安全服务将对非常用IP登录服务器的行为进行告警。

### 约束限制

单一账号最多可添加20个常用登录IP。

### 操作步骤

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

图 1-3 添加常用登录 IP



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

### 说明

- “常用登录IP”必须填写公网IP或者IP段。
- 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。

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

----结束

## SSH 登录 IP 白名单配置

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

## 说明

- 单一账号最多可添加10个SSH登录IP白名单。
- 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。

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

图 1-4 添加 IP 白名单



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

## 说明

- “常用登录IP”必须填写公网IP或者IP段。
- 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。

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

----结束

## 双因子认证配置

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

开启双因子认证功能后，登录云服务器时，主机安全服务将根据绑定的“消息通知服务主题”验证登录者的身份信息。

### 前提条件

- 用户已创建“协议”为“短信”或“邮箱”的消息主题。
- 主机已开启防护。
- Linux主机使用“密码”登录方式。
- 在Windows主机上，双因子认证功能可能会和“网防G01”软件、服务器版360安全卫士存在冲突，建议停止“网防G01”软件和服务器版360安全卫士。

### 约束与限制



- 开启双因子认证后，不能通过已安装图形化界面的Linux系统登录主机。
- 在Linux主机上，开启双因子认证后，不能通过云堡垒机登录主机。
- linux的openssh版本仅小于8时才支持双因子。

### 操作步骤

**步骤1** 选择“安装与配置 > 双因子认证”，进入“双因子认证”页面。

- 单击“操作”列“开启双因子认证”开启单台服务器双因子认证
- 勾选多台目标服务器，单击上方“开启双因子认证”批量开启多台服务器双因子认证。

**步骤2** 在“开启双因子认证”弹窗中，选择“验证方式”。

- **短信邮件验证**

短信邮件验证需要选择消息通知服务主题。

- 下拉框只展示状态已确认的消息通知服务主题。
- 如果没有主题，请单击“查看消息通知服务主题”进行创建。具体操作请参见[创建主题](#)。
- 若您的主题里包含多个手机号码/邮箱，在认证过程中，该主题内的手机号码/邮箱都会收到系统发出的验证码短信或邮件。若您只希望有一个手机号码/邮箱收到验证码，请修改对应主题，仅在主题中保留您希望收到验证码的手机号码/邮箱。

图 1-5 短信邮件验证



- **验证码验证**

选择验证码验证，仅通过实时收到的验证进行验证。

图 1-6 验证码验证



**步骤3** 单击“确定”，完成开启双因子认证的操作。

**步骤4** 返回“安装与配置 > 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。

----结束

## 弱口令检测配置

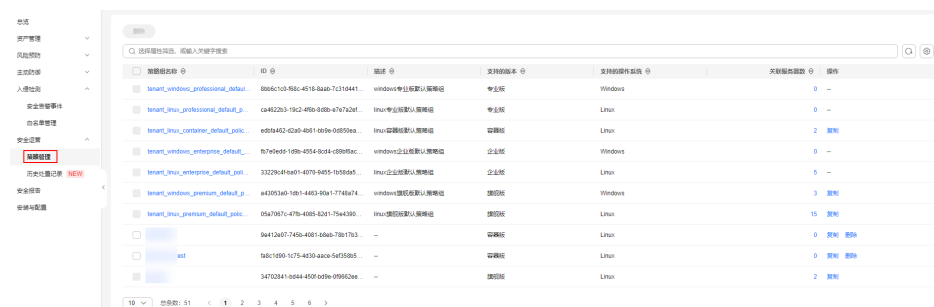
弱口令/密码不归属于某一类漏洞，但其带来的安全隐患却不亚于任何一类漏洞。

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。

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

**步骤1** 选择“安全运营 > 策略管理”，进入“策略管理”页面。

图 1-7 进入策略组页面



**步骤2** 单击目标策略组名称，进入策略组界面。

可根据默认“策略组名称”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。

**步骤3** 进入策略组列表，单击“策略名称”为“弱口令检测”的名称。

**步骤4** 进入策略内容配置页面，可对“策略内容”中的参数进行修改，建议保持默认值，参数说明如[表1-1](#)所示。

**表 1-1 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。

**步骤5** 确认无误，单击“确认”，完成修改。

**步骤6** 进入“资产管理 > 主机管理 > 云服务器”页面勾选目标服务器，单击上方“部署策略”。

**说明**

若需同时为多台服务器部署同一策略，需确认“操作系统”和“防护版本”与目标策略保持一致。

**步骤7** 在部署策略弹窗选择目标策略组，单击“确认”，完成策略部署。

**步骤8** 部署完成后在“安全运营 > 策略管理”页面，单击目标策略“关联服务器数”列的数值，页面跳转后筛选结果包含部署的目标服务器表示部署成功。

**说明**

部署完成后需等待1分钟左右再查看是否部署成功。

---结束

## 登录安全检测配置

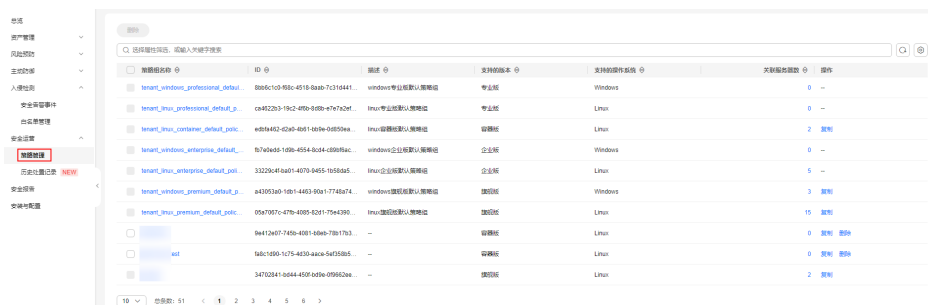
配置登录安全后，可为目标服务器开启登录安全检测，可有效检测爆破攻击，自动阻断爆破IP，触发告警并上报。

## 说明

登录安全检测仅支持企业版及以上版本支持，其中企业版不支持自定义配置参数，部署后企业版按照默认参数执行检测。

**步骤1** 选择“安全运营 > 策略管理”，进入“策略管理”页面。

图 1-8 进入策略组页面



**步骤2** 单击目标策略组名称，进入策略组界面。

可根据默认“策略组名称”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。

**步骤3** 进入策略组列表，单击“策略名称”为“登录安全检测”的名称。

**步骤4** 进入策略内容配置页面，可对“策略内容”中的参数进行修改，建议保持默认值，参数说明如[表1-2](#)所示。

图 1-9 修改安全检测策略

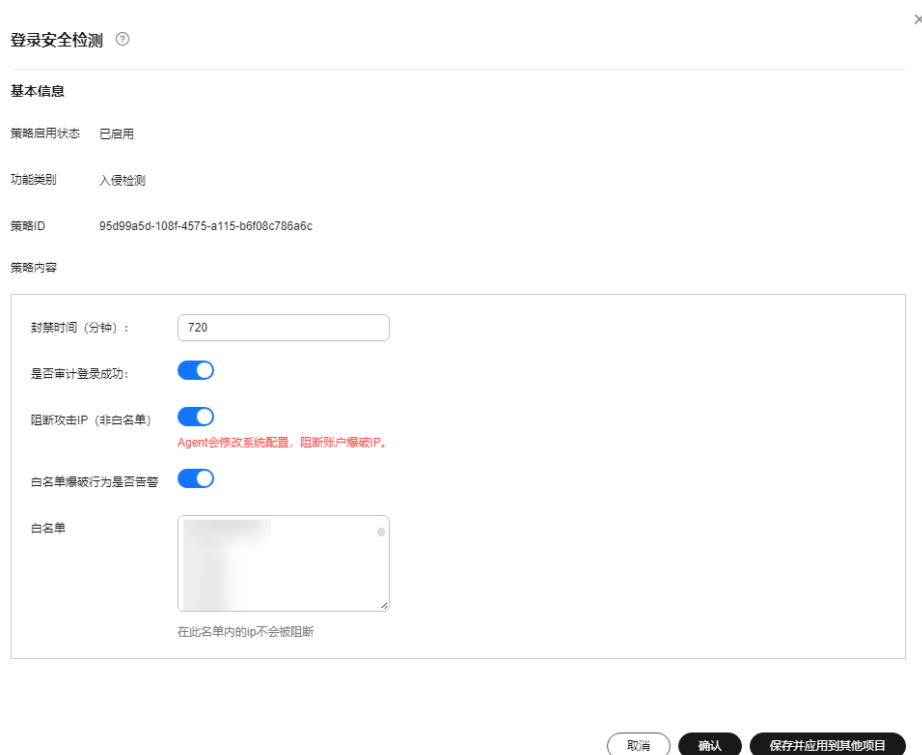






表 1-2 登录安全检测策略内容参数说明

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	<ul style="list-style-type: none"> <li>开启此功能后，HSS将上报登录成功的事件。</li> </ul> <ul style="list-style-type: none"> <li>：开启。</li> <li>：关闭。</li> </ul>
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	<ul style="list-style-type: none"> <li>开启后，HSS将对白名单IP产生的爆破行为进行告警。</li> </ul> <ul style="list-style-type: none"> <li>：开启。</li> <li>：关闭。</li> </ul>
白名单	将IP添加到白名单后，HSS不会阻断白名单内IP的爆破行为。最多可添加50个IP或网段到白名单，且同时支持IPV4和IPV6。

步骤5 确认无误，单击“确认”，完成修改。

**步骤6** 进入“资产管理 > 主机管理 > 云服务器”页面勾选目标服务器，单击上方“部署策略”。

 **说明**

若需同时为多台服务器部署同一策略，需确认“操作系统”和“防护版本”与目标策略保持一致。

**步骤7** 在部署策略弹窗选择目标策略组，单击“确认”，完成策略部署。

**步骤8** 部署完成后在“安全运营 > 策略管理”页面，单击目标策略“关联服务器数”列的数值，页面跳转后筛选结果包含部署的目标服务器表示部署成功。

 **说明**

部署完成后需等待1分钟左右再查看是否部署成功。

----**结束**

# 2 漏洞检测与修复最佳实践

## 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。

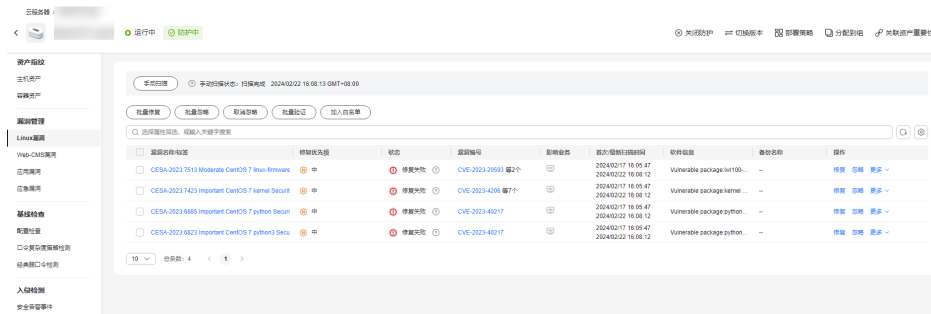
官方下载链接：<https://github.com/git/git/releases>

### 检测与修复建议

华为云主机安全服务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

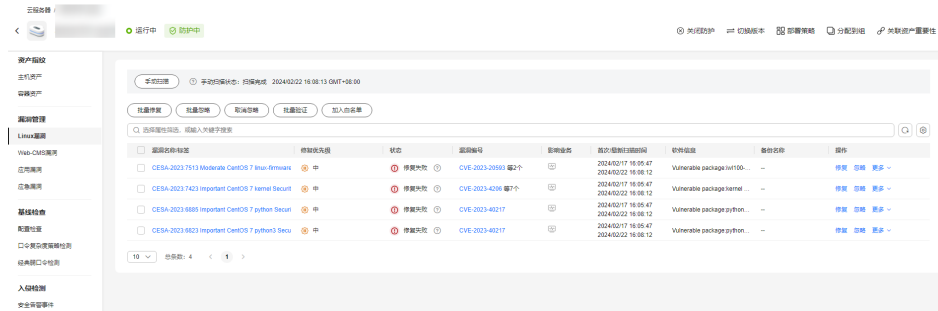
- 目前官方已在最新版本中修复了这两处漏洞，请受影响的用户及时升级到安全版本。  
下载地址：<https://repo.saltstack.com>。
- Salt Master默认监听端口为“4505”和“4506”，用户可通过配置安全组，禁止将其对公网开放，或仅对可信对象开放。

### 检测与修复建议

华为云主机安全服务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[开放端口检测](#)。

图 2-3 开放端口检测



- 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。

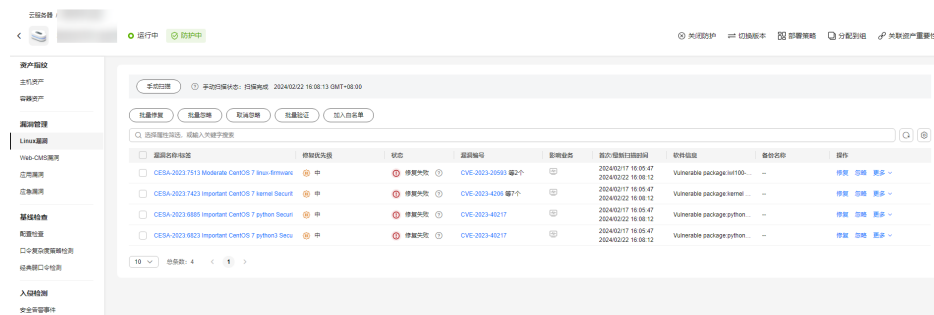
- <https://www.debian.org/security/2020/dsa-4661>
- <https://security.gentoo.org/glsa/202004-10>
- <https://lists.suse.com/pipermail/sle-security-updates/2020-April/006722.html>

## 检测与修复建议

华为云主机安全服务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。

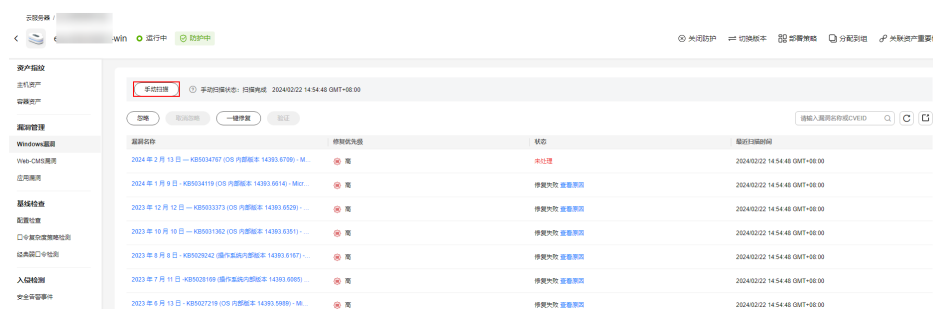
详情请参见<https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1020>。

## 检测与修复建议

华为云主机安全服务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。

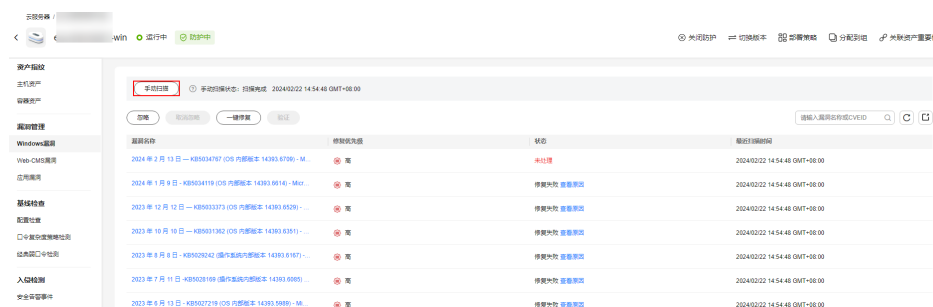
详情请参见<https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-1027>。

### 检测与修复建议

华为云主机安全服务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://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0601>。

### 检测与修复建议

华为云主机安全服务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，已安装主机安全服务客户端 ( Agent )，并开启防护。

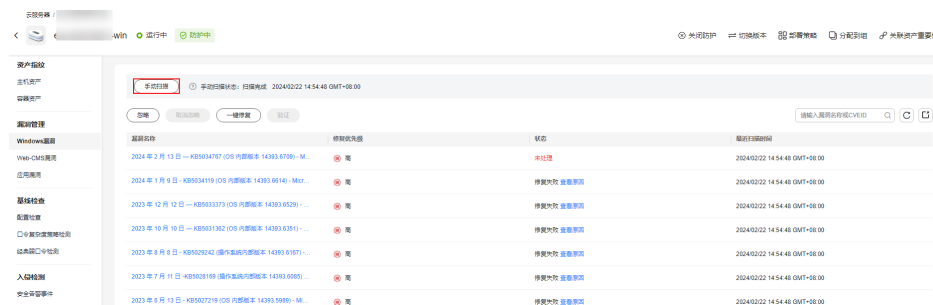
**步骤1** 登录管理控制台。

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

**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

您也可以通过在主机安全服务中，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 HSS 多云纳管部署

## 3.1 应用场景

随着混合云的发展，企业对于在混合云架构上实现统一安全管理的需求也越发强烈。主机安全支持多个云平台，为混合云场景提供了一套完整的安全运营管理解决方案，助力企业通过统一的视图、体验和管理，降低混合云架构下的业务负载面临的安全风险，有效提升整体安全运营效率。

### 应用场景

为了适配用户的全场景工作负载监控，实现云上云下、混合云资源的统一纳管，主机安全推出了华为云和混合云统一管理的安全解决方案。借助主机安全提供的适配能力，通过一个控制台实现一致的安全策略，避免因为不同平台安全水位不一致导致的攻击风险。

#### 华为云解决方案

可将华为云上服务器、数据中心、边缘云与其他线上云在华为云主机安全控制台实现统一管理。

#### 混合云解决方案

可将华为云上服务器、数据中心、边缘云与其他线上云在混合云主机安全控制台实现统一管理。



图 3-1 华为云解决方案

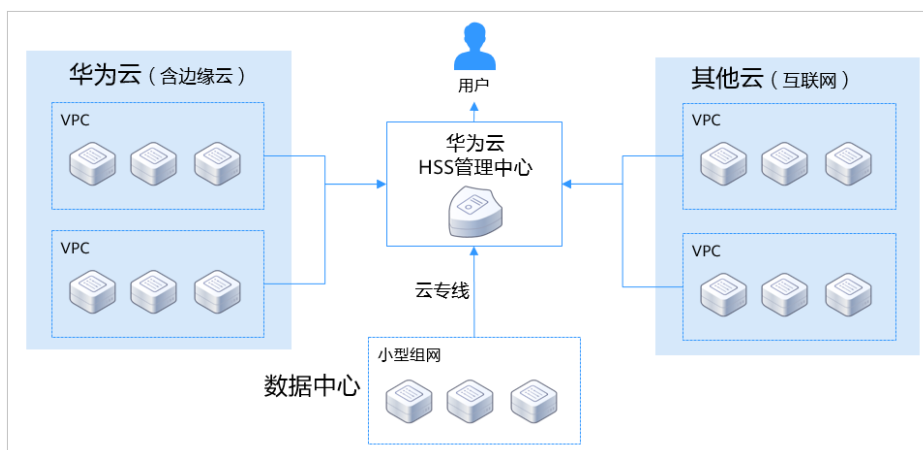
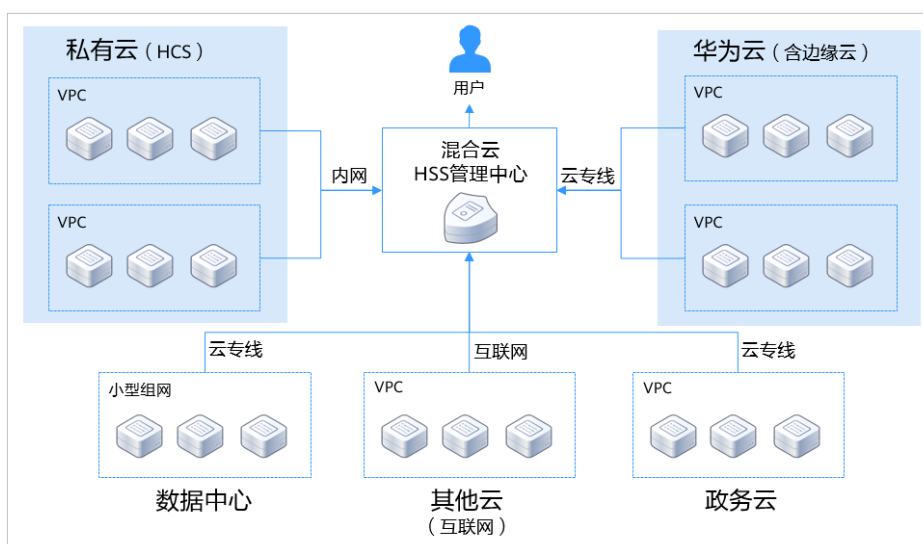


图 3-2 混合云解决方案



## 3.2 安装部署流程

若您使用的服务器需要通过华为云主机安全控制台或混合云主机安全控制台进行统一管理，且服务器使用场景包含了华为云服务器、非华为云服务器（互联网）、局域网服务器（包含数据中心、政务云等），你需按照服务器不同场景进行依次安装后方可实现统一管理。

### 华为云解决方案

根据服务器的不同类别会采用不同的安装方式进行Agent安装，获取安装命令的方式也不一样。

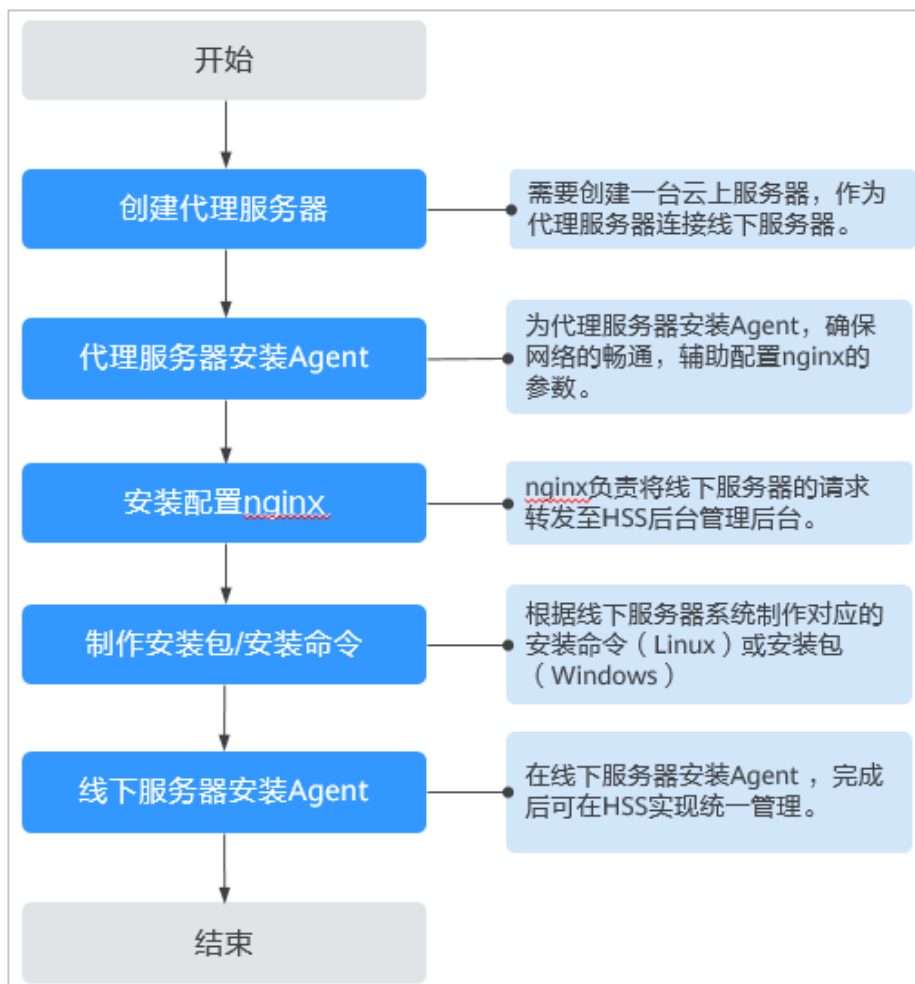
表 3-1 华为云方案安装命令获取方式

服务器场景类别	安装命令获取
华为云服务器	华为云控制台复制华为云安装命令。

服务器场景类别	安装命令获取
非华为云服务器（互联网）	华为云控制台复制非华为云安装命令。 <b>说明</b> 非华为云安装命令支持的局点包含：北京一、北京四、上海一、上海二、广州、香港、新加坡、贵阳一、雅加达，其他所有Region需按照局域网服务的方式获取安装命令。
局域网服务器（包含数据中心、政务云等）	搭建代理服务，生成安装命令或安装包，使用专线代理服务器可避免访问公网。

若使用的服务器包含了华为云服务器、非华为云服务器（互联网）、局域网服务器（包含数据中心、政务云等），华为云服务器和非华为云服务器（互联网）的安装流程详情请参见[安装Agent](#)，局域网服务器（包含数据中心、政务云等）安装流程如[图 3-3](#)所示。

图 3-3 局域网服务器搭建流程



## 混合云解决方案

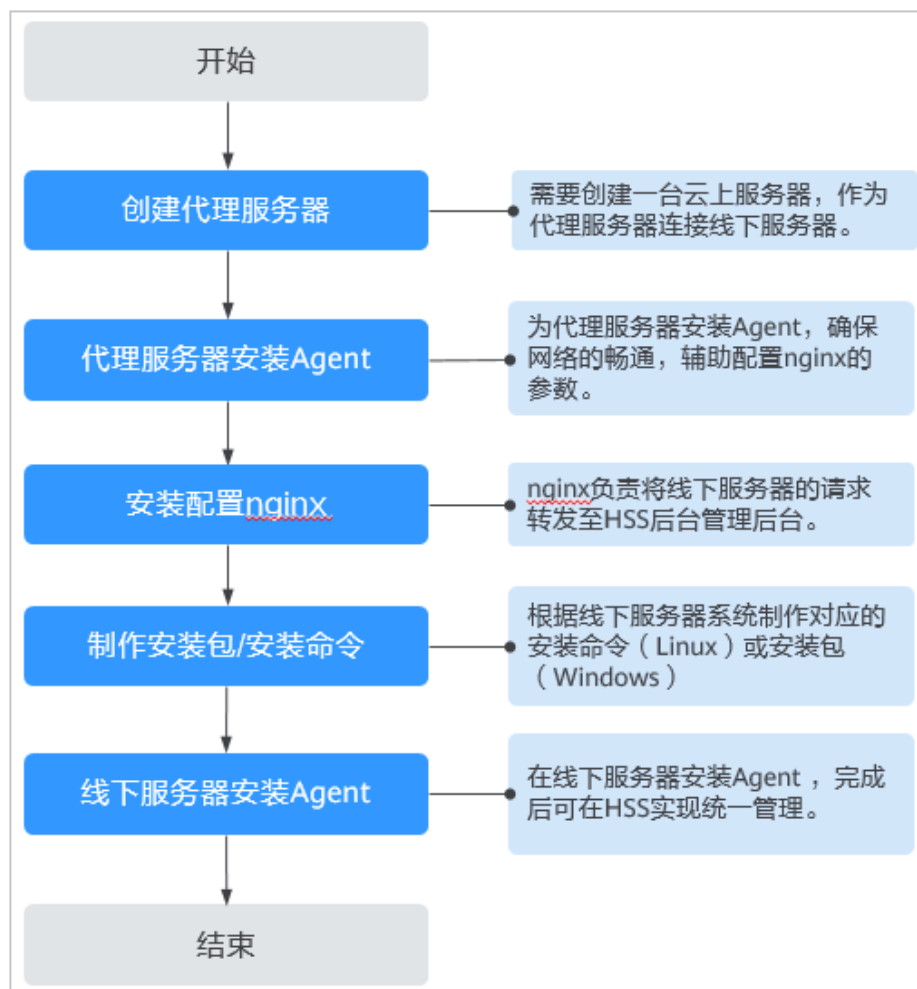
根据服务器的不同类别会采用不同的安装方式进行Agent安装，获取安装命令的方式也不一样。

表 3-2 混合云方案安装命令获取方式

服务器场景类别	安装命令/安装包获取方式
华为云服务器	华为云控制台复制华为云安装命令。
非华为云服务器（互联网）	搭建代理服务，生成安装命令或安装包，使用专线代理服务器可避免访问公网。
局域网服务器（包含数据中心、政务云等）	

若使用的服务器包含了华为云服务器、非华为云服务器（互联网）、局域网服务器（包含数据中心、政务云等）场景，华为云服务器的安装流程详情请参见[安装Agent](#)，非华为云服务器和局域网服务器（包含数据中心、政务云等）安装操作流程如[图3-4](#)所示。

图 3-4 局域网服务器搭建流程



## 3.3 安装部署

### 3.3.1 华为云解决方案

通过华为云主机安全对服务器进行统一管理，若使用的服务器类别包含华为云服务器、非华为云服务器（互联网）、局域网服务器（包含数据中心、政务云等），需按照不同的服务器类别进行分别安装。

#### 华为云服务器/非华为服务器（互联网）

- 在华为云主机安全控制台管理华为云服务器和非华为云服务器（互联网），可直接在华为云目标Region的服务器执行Agent安装即可。
  - 华为云服务器和非华为云服务器（互联网）的Linux服务器Agent安装详情请参见[安装Linux版本Agent](#)。
  - 华为云服务器和非华为云服务器（互联网）的Windows服务器Agent安装详情请参见[安装Windows版本Agent](#)。

#### 📖 说明

非华为服务器（互联网）安装目前支持的Region包含：北京一、北京四、上海一、上海二、广州、香港、新加坡、贵阳一、雅加达，其他所有Region需按照局域网服务的方式获取安装命令进行安装。

#### 局域网服务器（数据中心、政务云、私有云等）

局域网服务器需要创建专线代理服务器，手动制作Agent安装命令（或安装包）后执行安装，便可实现在华为云主机安全的统一管理。

操作详情请参见[线下主机专线接入公有云](#)。

### 3.3.2 混合云解决方案

通过混合云主机安全对服务器进行统一管理，若使用的服务器类别包含华为云服务器、非华为云服务器（互联网）、局域网服务器（包含数据中心、政务云等），需按照不同的服务器类别进行分别安装。

#### 华为云服务器

在混合云主机安全控制台管理华为云服务器，可直接在华为云目标Region的服务器执行Agent安装即可。

- 华为云服务器的Linux服务器Agent安装详情请参见[安装Linux版本Agent](#)。
- 华为云服务器的Windows服务器Agent安装详情请参见[安装Windows版本Agent](#)。

#### 非华为服务器（互联网）/局域网服务器（数据中心、政务云、私有云等）

非华为云服务器（互联网）和局域网服务器需要创建专线代理服务器，手动制作Agent安装命令（或安装包）后执行安装，便可实现在混合云主机安全的统一管理。

操作详情请参见[线下主机专线接入公有云](#)。

## 3.4 验证使用

安装完成后可登录华为云或混合云主机安全控制台进入云服务器列表页面，查看服务器已存在在列表中，表示线下服务器已接入主机安全控制台，已实现统一纳管。

### 说明

- 安装完成后确认目标服务器的10180端口可以正常连接，并确认服务器为开机在线状态。
- 非华为服务器（互联网）和局域网服务器（数据中心、政务云、私有云等）连接到主机安全控制台后不显示服务器状态。

## 3.5 线下主机专线接入公有云

### 3.5.1 步骤一：创建代理服务器

创建一台云上服务器，作为连接线下服务器的代理服务器。

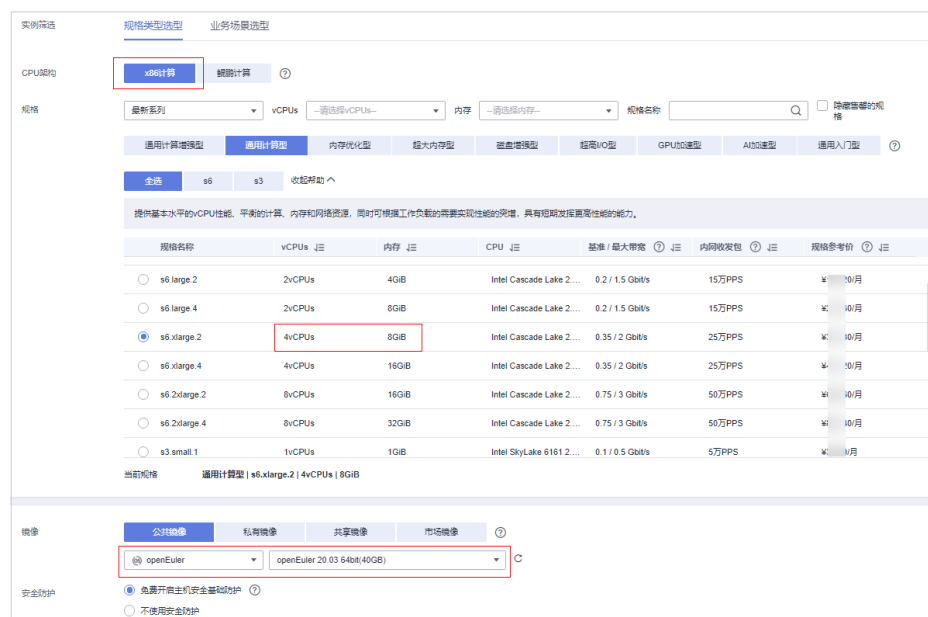
### 创建操作

登录华为云控制台购买弹性云服务器，操作详情请参见[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。

图 3-5 创建代理服务器



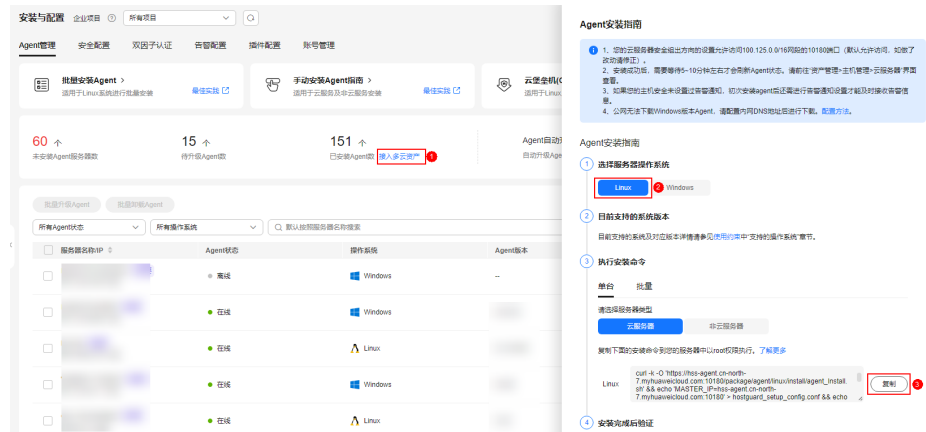
### 3.5.2 步骤二：为代理服务器安装 Agent

为代理服务器安装Agent，确保网络的畅通，辅助配置nginx的参数。

#### 操作步骤

**步骤1** 登录控制台进入主机安全新版控制台页面，选择“安装与配置”页面，单击“接入多云资产”，复制Linux华为云服务器x86架构EulerOS的安装命令。

图 3-6 复制安装命令



**步骤2** 登录代理服务器粘贴并执行复制的命令，完成Agent的自动安装，操作详情可参照[安装Linux版Agent](#)。

图 3-7 Agent 安装完成



**步骤3** 约10分钟后进入主机安全云服务器列表页面，查看代理服务器的“Agent状态”是否为“在线”。

#### 须知

需确保代理服务器Agent成功在线之后，再进行后续步骤，否则后续步骤无法正常执行。

图 3-8 查看 Agent 状态



---结束

### 3.5.3 步骤三：安装配置 nginx

nginx负责将线下服务器的请求转发至HSS后台管理后台。

#### 安装前准备：检查 yum 源

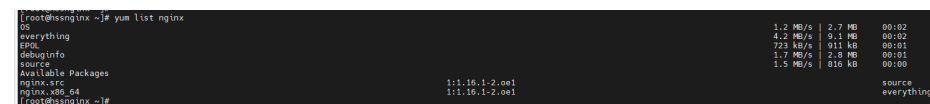
检查yum源是否有nginx软件包，如果没有nginx软件包需完成yum源配置，并临时绑定公网ip，待安装结束之后再解绑公网ip。

**步骤1** 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。

```
yum list nginx
```

**步骤2** 显示如图3-9所示表示nginx包存在。

图 3-9 nginx 包存在



----结束

#### 安装 nginx

**步骤1** 执行以下命令使用yum安装nginx。

```
yum install -y nginx
```

图 3-10 安装 nginx

```
[root@hssnginx ~]#
[root@hssnginx ~]# yum install -y nginx
Last metadata expiration check: 0:03:43 ago on Sat 17 Dec 2022 08:53:35 PM CST.
Dependencies resolved.
-----
Package                               Architecture      Version           Repository        Size
-----
Installing:
nginx                                  x86_64            1:1.16.1-2.0el1  everything        480 k
Installing dependencies:
gd                                      x86_64            2.2.5-6.0el1     OS                142 k
gperftools-libs                        x86_64            2-7-7.0el1       OS                267 k
libbwmnd                               x86_64            1:1.1-3.0el1     OS                54 k
libwebp                                 x86_64            1.0.0-5.0el1     OS                246 k
libxslt                                 x86_64            1:1.32-7.0el1    OS                233 k
mailcap                                 noarch            2.1-48-6.0el1    noarch            31 k
nginx-all-modules                     noarch            1:1.16.1-2.0el1  everything        7.7 k
nginx-filesystem                      noarch            1:1.16.1-2.0el1  everything        8.8 k
nginx-mod-http-image-filter           x86_64            1:1.16.1-2.0el1  everything        17 k
nginx-mod-http-perl                   x86_64            1:1.16.1-2.0el1  everything        26 k
nginx-mod-http-xslt-filter            x86_64            1:1.16.1-2.0el1  everything        16 k
nginx-mod-mail                         x86_64            1:1.16.1-2.0el1  everything        45 k
nginx-mod-stream                      x86_64            1:1.16.1-2.0el1  everything        68 k
-----
Transaction Summary
-----
Install 14 Packages
-----
Total download size: 1.6 M
Installed size: 5.3 M
Downloading Packages:
(1/14): libbwmnd-1.3.1-3.0el1.x86_64.rpm                249 kB/s | 54 kB  00:00
(2/14): gd-2.2.5-6.0el1.x86_64.rpm                    417 kB/s | 142 kB 00:00
(3/14): gperftools-libs-2.7.7.0el1.x86_64.rpm          745 kB/s | 267 kB 00:00
(4/14): libwebp-1.0.0-5.0el1.x86_64.rpm                1.3 MB/s | 246 kB 00:00
(5/14): mailcap-2.1-48-6.0el1.noarch.rpm              570 kB/s | 31 kB  00:00
(6/14): nginx-all-modules-1:1.16.1-2.0el1.noarch.rpm  143 kB/s | 7.7 kB 00:00
(7/14): nginx-filesystem-1:1.16.1-2.0el1.noarch.rpm   164 kB/s | 8.8 kB 00:00
-----
```

步骤2 自动执行安装，出现如图3-11所示“Complete!”表示安装成功。

图 3-11 nginx 安装成功

```
Running scriptlet: nginx-mod-http-image-filter-1:1.16.1-2.0el1.x86_64 13/14
Installing : nginx-all-modules-1:1.16.1-2.0el1.noarch                14/14
Running scriptlet: nginx-all-modules-1:1.16.1-2.0el1.noarch          14/14
Verifying  : gd-2.2.5-6.0el1.x86_64                                  1/14
Verifying  : gperftools-libs-2.7.7.0el1.x86_64                      2/14
Verifying  : libbwmnd-1.3.1-3.0el1.x86_64                            3/14
Verifying  : libwebp-1.0.0-5.0el1.x86_64                             4/14
Verifying  : libxslt-1.1.32-7.0el1.x86_64                            5/14
Verifying  : mailcap-2.1-48-6.0el1.noarch                             6/14
Verifying  : nginx-1:1.16.1-2.0el1.x86_64                            7/14
Verifying  : nginx-all-modules-1:1.16.1-2.0el1.noarch               8/14
Verifying  : nginx-filesystem-1:1.16.1-2.0el1.noarch                9/14
Verifying  : nginx-mod-http-image-filter-1:1.16.1-2.0el1.x86_64     10/14
Verifying  : nginx-mod-http-perl-1:1.16.1-2.0el1.x86_64            11/14
Verifying  : nginx-mod-http-xslt-filter-1:1.16.1-2.0el1.x86_64     12/14
Verifying  : nginx-mod-mail-1:1.16.1-2.0el1.x86_64                 13/14
Verifying  : nginx-mod-stream-1:1.16.1-2.0el1.x86_64               14/14
Installed:
nginx-1:1.16.1-2.0el1.x86_64      gd-2.2.5-6.0el1.x86_64      gperftools-libs-2.7.7.0el1.x86_64      libbwmnd-1.3.1-3.0el1.x86_64
libwebp-1.0.0-5.0el1.x86_64      libxslt-1:1.32-7.0el1.x86_64      mailcap-2.1-48-6.0el1.noarch          nginx-all-modules-1:1.16.1-2.0el1.noarch
nginx-filesystem-1:1.16.1-2.0el1.noarch  nginx-mod-http-image-filter-1:1.16.1-2.0el1.x86_64  nginx-mod-http-perl-1:1.16.1-2.0el1.x86_64  nginx-mod-http-xslt-filter-1:1.16.1-2.0el1.x86_64
nginx-mod-mail-1:1.16.1-2.0el1.x86_64  nginx-mod-stream-1:1.16.1-2.0el1.x86_64
Complete!
[root@hssnginx ~]#
[root@hssnginx ~]#
[root@hssnginx ~]#
```

---结束

## 配置 nginx

步骤1 执行以下命令进入nginx目录。

```
cd /etc/nginx/
```

步骤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 3-12 自签证书

```
[root@hssnginx nginx]# openssl req -new -x509 -nodes -out server.pem -keyout server.key -days 36500
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:cn
State or Province Name (full name) [Some-State]:test
Locality Name (eg, city) []:test
Organization Name (eg, company) [Internet Widgits Pty Ltd]:tes
Organizational Unit Name (eg, section) []:test
Common Name (e.g. server FQDN or YOUR name) []:test
Email Address []:null
[root@hssnginx nginx]#
```

### 说明

第一项Country Name受长度限制，只能填写两个字符。



**步骤3** 执行以下命令修改nginx.conf。

```
vi nginx.conf
```

**步骤4** 配置upstream。在http下找到server，在server上方添加以下信息。

```
upstream backend_hss {
server ADDR:10180;
}
```

图 3-13 配置 upstream

```
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.
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;

upstream backend_hss {
server ADDR:10180;
}

server {
listen 80 default_server;
listen [::]:80 default_server;
server_name _;
root /usr/share/nginx/html;

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

location / {
}

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

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

**步骤5** 配置server。server下的监听端口保留一条listen并将值修改为10180，server\_name的值修改为ADDR。

图 3-14 配置 server

```
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;

    location / {
    }

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

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

**步骤6** 在server下添加以下信息开启ssl认证。

```
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;
```

图 3-15 开启 ssl 认证

```
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 / {
    }

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

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

**步骤7** 配置location。在server下找到location，在location下的{}中添加以下信息。

```
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";
```

图 3-16 配置 location

```
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 {
    }
}
```

**步骤8 可选:** 填写完成后键入ECS，输入以下命令，键入回车键退出，完成配置。

:wq!

图 3-17 保存退出

```

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

# Settings for a TLS enabled server.
#
#   server {
#       listen      443 ssl http2 default_server;
#       listen      [::]:443 ssl http2 default_server;
#       server_name _;
#       root         /usr/share/nginx/html;
#
#       ssl_certificate "/etc/pki/nginx/server.crt";
#       ssl_certificate_key "/etc/pki/nginx/private/server.key";
#       ssl_session_cache shared:SSL:1m;
#       ssl_session_timeout 10m;
#       ssl_ciphers PROFILE=SYSTEM;
#       ssl_prefer_server_ciphers on;
#
#       # Load configuration files for the default server block.
#       include /etc/nginx/default.d/*.conf;
#
#       location / {
#       }
#
#       error_page 404 /404.html;
#               location = /40x.html {
#               }
#
#       error_page 500 502 503 504 /50x.html;
#               location = /50x.html {
#               }
#   }
}

:wq!

```

**步骤9** 依次执行以下命令完成启动nginx。

```
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
```

```
echo '*/*/*/* root systemctl start nginx' >> /etc/crontab
```

```
systemctl start nginx
```

----结束

### 3.5.4 步骤四：制作安装包/安装命令

根据线下服务器系统制作对应的安装命令（Linux）或安装包（Windows）。

#### 制作 Linux 安装命令

**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 3-18 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，即线下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3 确认ip可用后依次执行以下命令生成安装命令。

- X86 rpm软件包镜像：  
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：  
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：  
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：  
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
- 替换为可用IP：  
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

- 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4** 查看生成的命令，生成的目标命令将用于线下Linux服务器Agent的安装使用。

图 3-19 Linux 安装命令

```
root@hssingix tmp# cat x86_rpm_install.sh
# For Linux x86 CentOS EulerOS OpenSUSE Fedora
curl -k -O 'https://192.168.10180/package/agent/linux/x86/hostguard_x86_64.rpm' && echo 'MASTER_IP=192.168.10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.168.10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06' >> hostguard_setup_config.conf && rpm -ivh hostguard_x86_64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp# cat x86_deb_install.sh
# For Linux x86 Ubuntu Debian
curl -k -O 'https://192.168.10180/package/agent/linux/x86/hostguard_x86_64.deb' && echo 'MASTER_IP=192.168.10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.168.10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06' >> hostguard_setup_config.conf && dpkg -i hostguard_x86_64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp# cat arm_rpm_install.sh
# For Linux ARM CentOS EulerOS OpenSUSE Fedora UOS Kylin
curl -k -O 'https://192.168.10180/package/agent/linux/arm/hostguard_aarch64.rpm' && echo 'MASTER_IP=192.168.10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.168.10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06' >> hostguard_setup_config.conf && rpm -ivh hostguard_aarch64.rpm && rm -f hostguard_setup_config.conf && rm -f hostguard*.rpm
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp#
root@hssingix tmp# cat arm_deb_install.sh
# For Linux ARM Ubuntu Debian
curl -k -O 'https://192.168.10180/package/agent/linux/arm/hostguard_aarch64.deb' && echo 'MASTER_IP=192.168.10180' > hostguard_setup_config.conf && echo 'SLAVE_IP=192.168.10180' >> hostguard_setup_config.conf && echo 'ORG_ID=06' >> hostguard_setup_config.conf && dpkg -i hostguard_aarch64.deb && rm -f hostguard_setup_config.conf && rm -f hostguard*.deb
root@hssingix tmp#
root@hssingix tmp#
```

----结束

## 制作 Windows 安装包

**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，将用于线下Windows服务器Agent的安装使用。

图 3-20 Windows 安装包

```
[root@hssnginx tmp]#
[root@hssnginx tmp]# cd /tmp/
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# 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
% Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 14.2M  0 14.2M  0  107M  0 --:--:-- --:--:-- --:--:-- 107M
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]#
[root@hssnginx tmp]# zip hostguard_setup.zip hostguard_setup.exe hostguard_setup_config.ini
updating: hostguard_setup.exe (deflated 9%)
updating: hostguard_setup_config.ini (deflated 18%)
[root@hssnginx tmp]#
[root@hssnginx tmp]# ll
total 29M
-rw-r--r-- 1 root root 431 Dec 18 23:03 arm_deb_install.sh
-rw-r--r-- 1 root root 459 Dec 18 23:03 arm_rpm_install.sh
-rw-r--r-- 1 root root 99 Dec 19 09:59 hostguard_setup_config.ini
-rw-r--r-- 1 root root 15M Dec 19 09:59 hostguard_setup.exe
-rw-r--r-- 1 root root 15M Dec 19 09:59 hostguard_setup.zip
drwxr-xr-x 2 root root 60 Dec 18 20:42 nspcr-private-4a5d7687a4f4498eb4f971f686f46d41-chronyd.service-lm13T
-rw-r--r-- 1 root root 13 Dec 19 22:37 private_ip.conf
drwx----- 3 root root 60 Dec 18 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-chronyd.service-lm13T
drwx----- 3 root root 60 Dec 18 22:20 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-nginx.service-vjH0T
drwx----- 3 root root 60 Dec 19 20:43 systemd-private-4a5d7687a4f4498eb4f971f686f46d41-systemd.logind.service-pq10jm
prw-r--r-- 1 root root 0 Dec 19 09:59 wrapper-7508-1-in
prw-r--r-- 1 root root 0 Dec 19 09:59 wrapper-7508-2-out
-rw-r--r-- 1 root root 429 Dec 18 23:03 x86_deb_install.sh
-rw-r--r-- 1 root root 447 Dec 18 23:03 x86_rpm_install.sh
[root@hssnginx tmp]#
[root@hssnginx tmp]#
```

---结束

### 3.5.5 步骤五：为线下服务器安装 Agent

在线下服务器安装Agent，完成后可在HSS实现对服务器的统一管理。

#### 线下 Linux 服务器安装 Agent

登录线下目标服务器，将制作的Linux安装命令复制粘贴到目标服务器，即可执行Agent安装。

安装操作详情请参见[安装Linux服务器的Agent](#)中的步骤8。

#### 线下 Windows 服务器安装 Agent

将制作Windows安装包hostguard\_setup.zip拷贝到本地PC机，然后上传到其他需要安装Agent的线下Windows服务器，解压安装包后双击hostguard\_setup.exe即可安装。

#### 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。



# 4 勒索病毒防护最佳实践

## 4.1 什么是勒索软件攻击

勒索软件攻击已成为当今企业面临的最大的安全挑战之一。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的发展产生重大阻碍，出现一蹶不振的现象。

近年来，勒索病毒攻击量呈倍增趋势，且隐蔽性极强、变种多、变化快，攻击目标更多元，攻击路径更多样化，应对勒索软件攻击当下刻不容缓。

图 4-1 勒索概述



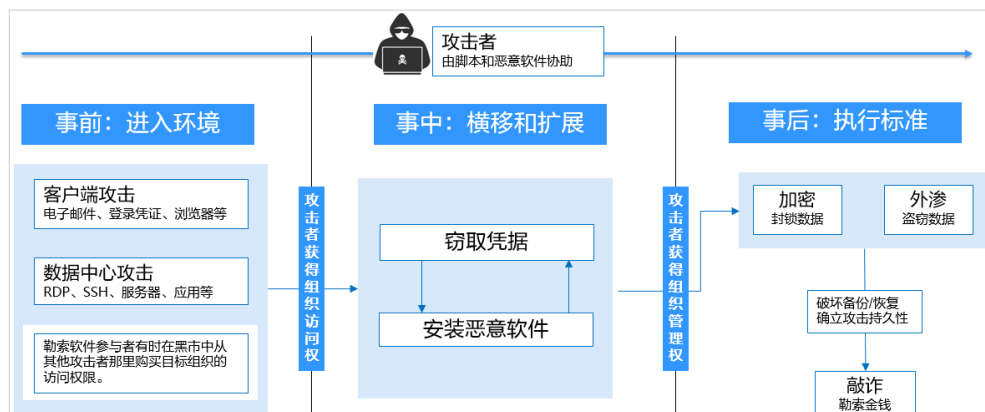
## 4.2 被勒索软件攻击的过程

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 4-2 被勒索过程



## 4.3 如何避免成为勒索受害者（通用举措）

### 事前举措

由于勒索攻击高强度加密算法的难破解性和数字货币交易方式的隐蔽性，**解决勒索攻击的首要**是构建“安全能力前置”，提升自身的“免疫力”。

建议按照如下加固方式开展事前勒索防护：

- **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。
- **减少系统风险入口：**定期开展漏洞扫描及系统风险配置参数扫描，第一时间修复漏洞及风险项，减小系统风险等级。同时，应关注软件厂商发布的安全漏洞信息和补丁信息，及时做好漏洞管理和修复工作。
- **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。
- **关键数据备份：**加强重要数据备份工作，可靠的数据备份可以最小化勒索软件带来的损失。需要主动加密存储和定期备份关键业务数据，并合理设置备份保留策略，确保被勒索攻击后存在有效副本可以恢复数据。
- **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。

## 事中举措

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。

建议按照如下处理方式开展事中勒索防护：

- **迅速隔离感染设备：**确保在遭受勒索攻击后，立即采取断网、断电等方式切断勒索病毒外联扩散行为。及时修改感染设备的密码及同一局域网其他设备密码。
- **及时处置告警入侵事件：**确保对业务资源进行实时安全检测，可及时隔离阻断勒索病毒运行、拦截勒索主控端恶意IP及尝试爆破攻击源IP，阻断其运行、通信及联接行为。

## 事后举措

当前勒索攻击发展迅速，任何工具都无法提供100%防护。所以在事后应及时恢复业务、开展网络安全加固以减弱勒索攻击带来的影响。

建议按照如下处理方式开展事后勒索恢复：

- **利用备份数据恢复数据：**根据遭受勒索攻击的设备备份情况，确认数据恢复范围、顺序及备份版本，利用备份副本恢复数据。
- **排查修复网络风险：**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。

## 4.4 华为云勒索防护组合拳“HSS+CBR”

### 4.4.1 概述

除了勒索软件防护的通用举措（[如何避免成为勒索受害者（通用举措）](#)），HSS与CBR对勒索综合防御能力均具有影响：

当前勒索病毒频繁升级、变种，主机安全HSS可支持对勒索病毒的检测及系统风险项的识别，但无法做到百分百的病毒防护能力，需要通过配置CBR备份服务进一步提升勒索病毒防护能力、消减勒索带来的影响。仅配置CBR备份服务，可能出现备份副本到勒索攻击时间节点间的业务无法恢复，需要同步配置HSS勒索病毒防护功能实时检测勒索病毒，减小业务受损范围。推荐您使用华为云HSS+CBR的勒索防护最佳实践，帮助企业打好事前、事中、事后的勒索攻防“组合拳”。

- **事前：安全能力前置，勒索入口“早发现、早治疗”**  
详细操作请参见[识别并修复勒索风险入口](#)。
- **事中：及时阻断攻击，实时检测、隔离勒索攻击**  
详细操作请参见[开启勒索病毒防护和备份](#)。
- **事后：损失最小化，被勒索后“及时恢复”**  
详细操作请参见[恢复服务器数据](#)。

## 勒索防护配置说明

华为云安全事件数据表明，HSS与CBR对勒索综合防御能力均具有影响，为使您的业务环境处于最佳勒索防御状态，强烈建议开通HSS旗舰版勒索防护策略，开通并配置小时级别永久保存的CBR备份：

主机安全 HSS服务状态		云备份 CBR服务状态		被加密概率	加密后恢复概率	防御勒索病毒侵害的综合得分（0~100）
开通版本	勒索防护策略	配置状态	最短备份周期（推荐）			
-	-	-	-	非常高（90%）	0%	0
基础版	不支持	-	-	非常高（90%）	0%	0
企业版	不支持	-	-	非常高（85%）	0%	10
旗舰版	未配置	-	-	中（50%）	0%	15
基础版/未开通	不支持	已配置	天	非常高（90%）	50%	20
企业版	不支持	已配置	天	非常高（85%）	50%	30
基础版/未开通	不支持	已配置	小时	非常高（90%）	90%	30
旗舰版	未配置	已配置	天	中（50%）	50%	35
企业版	不支持	已配置	小时	非常高（85%）	90%	40
旗舰版	未配置	已配置	小时	中（50%）	90%	45
旗舰版	已配置	-	-	非常低（<10%）	0%	60
旗舰版	已配置	已配置	天	非常低（<10%）	50%	80
旗舰版	已配置	已配置	小时	非常低（<10%）	90%	90
<b>旗舰版</b>	<b>已配置</b>	<b>已配置</b>	<b>小时（永久备份）</b>	<b>非常低（&lt;10%）</b>	<b>90%</b>	<b>99（推荐）</b>

## 4.4.2 识别并修复勒索风险入口


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。华为云主机安全服务首创防入侵、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。

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。华为云主机安全服务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 > 主机安全服务”，进入主机安全平台界面。

**步骤3** 在左侧导航栏，选择“风险预防 > 基线检查”，进入基线检查页面。

**步骤4** 选择“经典弱口令”页签，查看主机中当前存在的弱口令。

图 4-3 查看经典弱口令检测



服务器名称/IP地址	账号名称	账号类型	弱口令使用时长 (单位: 天)
201	root	系统账号	1361
	root	系统账号	1358

**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3** 选择“配置检查”页签，查看主机中当前存在的基线风险。

**步骤4** 单击目标基线名称，进入基线详情页面。

**步骤5** 选择“检查项 > 未通过”页签，查看基线风险项。

图 4-4 查看基线检查详情



**步骤6** 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7** 登录受影响的服务器，根据修改建议加固配置。

**步骤8** 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3** 选择“Linux漏洞”、“Windows漏洞”、“Web-CMS漏洞”和“应用漏洞”页签，查看主机当前存在的各类漏洞。

**步骤4** 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
  - 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。

#### 📖 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

### 4.4.3 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。华为云主机安全服务首创防入侵、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：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，开启主机安全服务旗舰版、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** 选择“主动防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

**步骤3** 选择“防护服务器”页签。

**步骤4** 在目标服务器勒索防护状态栏，单击“开启防护”。

您也可以选中多台服务器，并单击列表上方的“开启勒索病毒防护”，批量为服务器开启防护。

**步骤5** 在“开启勒索病毒防护”弹窗中，确认服务器信息并选择防护策略。

**步骤6** 单击“确认”，开启防护。

服务器勒索防护状态显示已开启，表示开启勒索病毒防护成功。

----结束

## 步骤二：配置勒索病毒防护策略

根据自身业务需求，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** 选择“主动防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

**步骤3** 选择“防护服务器”页签。

**步骤4** 在目标服务器所在行的防护策略列，单击策略名称，进入策略编辑页面。

**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。

表 4-1 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。 <ul style="list-style-type: none"> <li>告警并自动隔离</li> <li>告警</li> </ul>	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。 <b>说明</b> 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



参数名称	参数说明	取值样例
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或格式，自定义勾选即可。 涵盖数据库、容器、代码、证书密钥、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“确认”，完成防护策略修改。

----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** 选择“主动防御 > 勒索病毒防护”，进入“勒索病毒防护”界面。

**步骤3** 选择“防护服务器”页签。

**步骤4** 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 4-5 开启勒索备份



**步骤5** 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6** 单击“确认”，开启备份。

----结束

## 4.4.4 恢复服务器数据

当前勒索攻击发展迅速，任何工具都无法提供100%防护。若不幸失陷，备份恢复能够将损失最小化。通过华为云云备份服务快速恢复业务，保障业务安全运行。

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。

### 操作步骤

**步骤1** [登录管理控制台](#)。

**步骤2** 在左侧导航栏选择“主动防御 > 勒索病毒防护”，进入勒索病毒防护界面。

**步骤3** 选择“防护服务器”页签。

**步骤4** 在目标服务器所在行的“操作”列，选择“更多 > 恢复数据”。

**步骤5** 在弹窗中选择需要恢复的备份数据源。

**步骤6** 在目标备份数据源所在行的“操作”列，单击“恢复数据”。

**步骤7** 在弹窗中确认服务器信息并配置数据存放磁盘等参数。

- 恢复后立即重启云服务器：勾选后表示同意数据恢复后重启服务器。
- 指定磁盘：选择需要备份数据源的存储磁盘。

**步骤8** 单击“确认”，执行备份恢复。

----结束

# 5 通过云堡垒机安装主机安全服务的 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主机安全服务的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”。

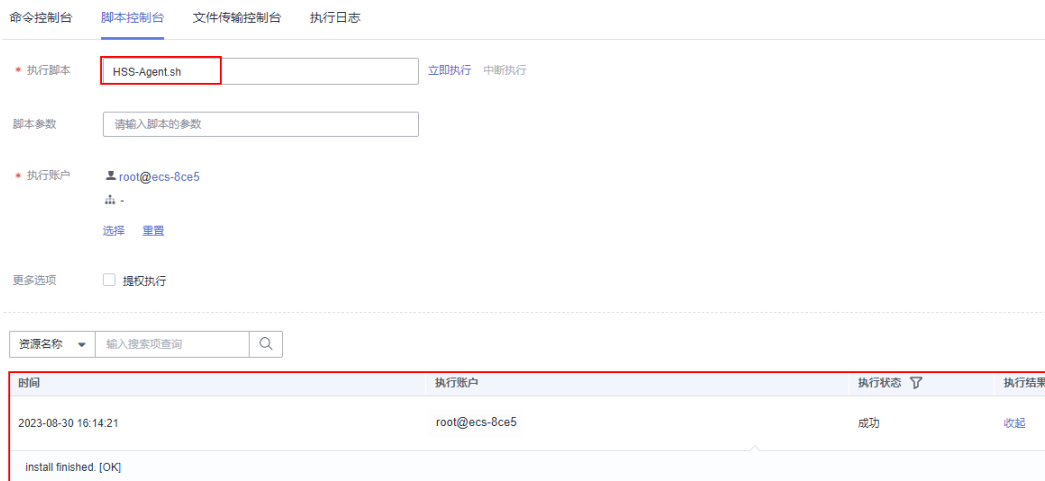
步骤5 单击“立即执行”，执行脚本任务。

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** 在主机安全服务控制台，确认Agent安装结果。

1. 登录主机安全服务控制台。
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

# A 修订记录

发布日期	修改说明
2023-11-17	第七次正式发布。 优化： <a href="#">勒索病毒防护最佳实践</a> ，增加防护配置操作。
2023-10-27	第六次正式发布。 服务中文名称修改为“主机安全服务”
2023-10-10	第五次正式发布。 新增： <a href="#">通过云堡垒机安装主机安全服务的Agent</a>
2023-01-18	第四次正式发布。 新增如下： <a href="#">HSS多云纳管部署</a> <a href="#">勒索病毒防护最佳实践</a>
2022-12-10	第三次正式发布。 修改勒索防护最佳实践。
2022-10-20	第二次正式发布。 新增 <a href="#">HSS登录安全加固最佳实践</a> 。
2022-06-15	第一次正式发布。