

主机安全服务

# 快速入门

文档版本 01  
发布日期 2024-01-15



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

---

1 入门实践.....	1
2 免费试用 HSS 基础版 30 天.....	3
3 快速开启主机安全防护.....	4
4 快速开启网页防篡改防护.....	8
5 快速开启容器安全防护.....	17
6 ECS 安全态势速查.....	21

# 1 入门实践

当您为主机开启安全防护后，可以根据业务需求使用HSS提供的一系列常用实践。

表 1-1 常用实践

实践	描述
主机登录保护	<b>HSS登录安全加固最佳实践</b> 通过HSS登录防护配置，帮助您提升主机登录安全。
漏洞修复	<b>Git用户凭证泄露漏洞 (CVE-2020-5260)</b> 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。 本实践介绍通过HSS检测与修复该漏洞的建议。
	<b>SaltStack远程命令执行漏洞 (CVE-2020-11651/CVE-2020-11652)</b> Saltstack是基于python开发的一套C/S自动化运维工具，国外安全研究人员披露其中存在身份验证绕过漏洞 (CVE-2020-11651) 和目录遍历漏洞 (CVE-2020-11652) 漏洞，攻击者利用这些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。 本实践介绍通过HSS检测与修复这些漏洞的建议。
	<b>OpenSSL高危漏洞 (CVE-2020-1967)</b> 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。 本实践介绍通过HSS检测与修复该漏洞的建议。

实践	描述
	<p><b>Adobe Font Manager库远程代码执行漏洞 ( CVE-2020-1020/ CVE-2020-0938 )</b></p> <p>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。</p> <p>本实践介绍通过HSS检测与修复该漏洞的建议。</p>
	<p><b>Windows内核特权提升漏洞 ( CVE-2020-1027 )</b></p> <p>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。</p> <p>本实践介绍通过HSS检测与修复该漏洞的建议。</p>
	<p><b>Windows CryptoAPI欺骗漏洞 ( CVE-2020-0601 )</b></p> <p>Windows CryptoAPI欺骗漏洞 ( CVE-2020-0601 ) 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。</p> <p>本实践介绍通过HSS检测与修复该漏洞的建议。</p>
多云主机纳管	<p><b>HSS多云纳管部署</b></p> <p>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，主机安全推出的统一管理安全解决方案。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，避免因不同平台安全水位不一致导致的攻击风险。</p>
勒索病毒防护	<p><b>勒索病毒防护最佳实践</b></p> <p>勒索病毒攻击已成为当今企业面临的最大的安全挑战之一。攻击者利用勒索病毒加密锁定受害者的数据或资产设备，并要求受害者支付赎金后才解锁数据，也存在即使受害者支付赎金也无法赎回数据情况。</p> <p>为了预防勒索病毒攻击，避免被勒索面临巨大的经济损失风险，您可以使用“HSS+CBR”组合为服务器做好“事前、事中、事后”的勒索病毒防护。</p>
网页防篡改	<p><b>“WAF+HSS”联动，提升网页防篡改能力</b></p> <p>主机安全HSS网页防篡改功能和Web应用防火墙“双剑合璧”，防止网页篡改事件发生。</p>
等保合规	<p><b>等保二级解决方案</b></p> <p>该解决方案能帮您快速在华为云上搭建等保二级合规安全解决方案，快速、低成本完成安全整改，轻松满足等保二级合规要求。</p>
	<p><b>等保合规安全解决方案</b></p> <p>华为云依托自身安全能力与安全合规生态，为您提供一站式的安全解决方案，帮助您快速、低成本完成安全整改，轻松满足等保合规要求。</p>

# 2 免费试用 HSS 基础版 30 天

主机安全服务为用户提供了30天免费试用基础版的活动，用户在购买ECS主机时可同步选择免费试用HSS基础版30天。HSS基础版支持的防护功能详情请参见[服务版本差异](#)。

## 如何免费试用 HSS 基础版 30 天？

购买ECS主机时，在“基础配置”页勾选“免费试用一个月主机安全基础防护”，您即可享受免费试用HSS基础版30天。支持使用HSS的操作系统请参见[HSS支持的操作系统](#)。

图 2-1 勾选免费试用



## 免费试用 HSS 基础版到期后怎么办？

免费试用HSS基础版30天到期后，主机安全服务将停止为主机提供安全防护，此外不会对您的主机造成任何影响。如果您想要继续使用主机安全服务，您可以在免费试用到期后购买主机安全服务并开启防护，相关操作参考如下：

- 1. 购买防护配额。**  
根据主机防护需求购买对应的主机安全服务版本。HSS各版本支持的防护功能请参见[服务版本差异](#)。
- 2. 安装Agent。**  
免费试用HSS期间，ECS主机默认已安装Agent，如果您卸载了Agent，您需要重新进行安装；如果您未卸载Agent，则可忽略此步骤。
- 3. 开启防护。**  
执行了此操作，主机安全防护才会正常开启。

# 3 快速开启主机安全防护

## 操作场景

主机安全服务是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、主动防御、安全运营等功能，可全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。关于主机安全服务提供的服务器安全防护功能请参见[服务版本差异](#)。

本指南以一台EulerOS 2.9华为云弹性云服务器为例，指引您如何快速开启主机安全防护。

## 前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考[修改云服务器的DNS服务器地址](#)和[华为云内网DNS地址](#)。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。
- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。


## 约束限制

- 主机安全服务支持防护64位华为云主机和非华为云主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见[支持的操作系统](#)。
- 华为云云桌面Workspace镜像中已预置HSS Agent，购买云桌面23.6.0及以后版本将会自动安装Agent，无需您手动安装。如果您购买的云桌面是23.6.0以前的版本，可以参照本文手动为云桌面安装Agent。

## 步骤一：购买防护配额

**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 > 主机安全服务”，进入主机安全服务页面。

**步骤4** 在“总览”页面右上角，单击“购买主机安全”，进入购买主机安全配额页面。

**步骤5** 根据界面提示，选择购买参数。参数配置说明请参见表 [购买主机安全参数说明](#)。

**表 3-1** 购买主机安全参数说明

参数名称	参数说明
计费模式	选择“包年/包月”。
区域	选择主机所属区域。
版本选择	选择“企业版”。
企业项目	<p>企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。</p> <ul style="list-style-type: none"> <li>• 如果需要使用该功能，请联系您的客户经理申请开通。</li> <li>• 如果开通了此功能，请从下拉列表中选择所在的企业项目。</li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 选择企业项目后，产生的费用和资源均在企业项目内。</li> <li>• “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。</li> <li>• 只有注册的华为账号购买HSS时，“企业项目”下拉列表中才可以选择到“default”。</li> </ul>
购买时长	<p>选择1个月，并勾选“自动续费”。</p> <p>勾选“自动续费”后，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。</p>
防护主机数量	输入防护的主机数量为1台。
标签	<ul style="list-style-type: none"> <li>• 如果没有预定义标签，单击“查看预定义标签”，创建一个预定义标签。</li> <li>• 如果已有预定义标签，鼠标依次单击“标签键”和“标签值”选框，选择一个预定义的标签。</li> </ul>
配额管理	<p>勾选自动绑定。</p> <p>开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。</p> <ul style="list-style-type: none"> <li>• 主机：按“旗舰版 &gt; 企业版 &gt; 专业版 &gt; 基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> <li>• 容器节点：按“容器版 &gt; 旗舰版 &gt; 企业版 &gt; 专业版 &gt; 基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> </ul>

**步骤6** 在页面右下角，单击“立即购买”，进入“订单确认”界面。



费率标准请参见[产品价格详情](#)。

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

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

**步骤9** 单击“返回主机安全服务控制台”，返回主机安全服务控制台。

----结束

## 步骤二：安装 Agent

**步骤1** 在主机安全服务控制台左侧导航栏选择“安装与配置”，进入安装与配置页面。

**步骤2** 在“Agent管理”页签，单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。

**步骤3** 在目标服务器的“操作”列，单击“安装Agent”。

图 3-1 安装 Agent



**步骤4** 在“安装Agent”弹窗中，单击“复制”，复制安装Agent的命令。

**步骤5** 远程登录待安装Agent的主机。

**步骤6** 以root权限执行复制的安装命令，在主机中安装Agent。

若界面回显信息如[图 Agent安装成功](#)所示，则表示Agent安装成功。

图 3-2 Agent 安装成功

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

**步骤7** 执行以下命令，查看Agent的运行状态。

**service hostguard status**

若界面回显信息如[图 Agent运行正常](#)所示，则表示Agent运行正常。

图 3-3 Agent 运行正常

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

----结束

### 步骤三：开启防护

- 步骤1** 在主机安全服务控制台左侧导航栏选择“资产管理 > 主机管理”，进入云服务器列表页面。
- 步骤2** 在目标服务器所在行的“操作”列，单击“开启防护”。
- 步骤3** 在“开启防护”弹窗中，选择开启方式。参数配置说明如表 [开启防护参数说明](#)所示。

表 3-2 开启防护参数说明

参数名称	参数说明
计费模式	选择“包年/包月”。
版本选择	选择“企业版”。
选择配额	保持默认“随机选择配额”。

- 步骤4** 确认信息无误后，请阅读《主机安全免责声明》并勾选“我已阅读并同意《主机安全免责声明》”。
- 步骤5** 单击“确认”，开启防护。
- 步骤6** 查看目标服务器的防护状态为“防护中”，表示开启防护成功。

图 3-4 查看防护状态

服务器信息	服务器状态	Agent状态	防护状态	检测结果	版本/到期时间	策略组	操作
<input type="checkbox"/>	运行中	在线	<span style="border: 1px solid red; padding: 2px;">● 防护中</span>	<span style="color: red;">● 有风险</span>	企业版 12天到期	tenant_linux_enterpr...	<a href="#">关闭防护</a> <a href="#">切换版本</a> <a href="#">更多</a>
<input type="checkbox"/>	运行中	在线	● 防护中	<span style="color: red;">● 有风险</span>	企业版 20天到期	tenant_linux_enterpr...	<a href="#">关闭防护</a> <a href="#">切换版本</a> <a href="#">更多</a>

----结束

# 4 快速开启网页防篡改防护

## 操作场景

主机安全服务网页防篡改版提供静态+动态（Tomcat）网页防篡改功能，可实时监控网站目录，并支持通过备份恢复被篡改的文件或目录，从而保护重要系统的网站信息不被恶意篡改；此外还提供多项服务器安全防护功能，详细内容请参见[服务版本差异](#)。

本指南以一台EulerOS 2.9华为云弹性云服务器为例，指引您如何快速网页防篡改防护。

## 前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考[修改云服务器的DNS服务器地址](#)和[华为云内网DNS地址](#)。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。
- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。


## 约束限制

- 主机安全服务支持防护64位华为云主机和非华为云主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见[支持的操作系统](#)。
- 华为云云桌面Workspace镜像中已预置HSS Agent，购买云桌面23.6.0及以后版本将会自动安装Agent，无需您手动安装。如果您购买的云桌面是23.6.0以前的版本，可以参照本文手动为云桌面安装Agent。

## 步骤一：购买防护配额

**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 > 主机安全服务”，进入主机安全服务页面。

**步骤4** 在“总览”页面右上角，单击“购买主机安全”，进入购买主机安全配额页面。

**步骤5** 根据界面提示，选择购买参数。参数配置说明请参见[表 购买主机安全参数说明](#)。

**表 4-1** 购买主机安全参数说明

参数名称	参数说明
计费模式	选择“包年/包月”。
区域	选择主机所属区域。
版本选择	选择“网页防篡改改版”。
企业项目	<p>企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。</p> <ul style="list-style-type: none"> <li>如果需要使用该功能，请联系您的客户经理申请开通。</li> <li>如果开通了此功能，请从下拉列表中选择所在的企业项目。</li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>选择企业项目后，产生的费用和资源均在企业项目内。</li> <li>“default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。</li> <li>只有注册的华为账号购买HSS时，“企业项目”下拉列表中才可以选择到“default”。</li> </ul>
购买时长	<p>选择1个月，并勾选“自动续费”。</p> <p>勾选“自动续费”后，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。</p>
防护主机数量	输入防护的主机数量为1台。
标签	<ul style="list-style-type: none"> <li>如果没有预定义标签，单击“查看预定义标签”，创建一个预定义标签。</li> <li>如果已有预定义标签，鼠标依次单击“标签键”和“标签值”选框，选择一个预定义的标签。</li> </ul>
配额管理	<p>勾选自动绑定。</p> <p>开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。</p> <ul style="list-style-type: none"> <li>主机：按“旗舰版 &gt; 企业版 &gt; 专业版 &gt; 基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> <li>容器节点：按“容器版 &gt; 旗舰版 &gt; 企业版 &gt; 专业版 &gt; 基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> </ul>

**步骤6** 在页面右下角，单击“立即购买”，进入“订单确认”界面。

费率标准请参见[产品价格详情](#)。

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

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

**步骤9** 单击“返回主机安全服务控制台”，返回主机安全服务控制台。

----结束

## 步骤二：安装 Agent

**步骤1** 在主机安全服务控制台左侧导航栏选择“安装与配置”，进入安装与配置页面。

**步骤2** 在“Agent管理”页签，单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。

**步骤3** 在目标服务器的“操作”列，单击“安装Agent”。

图 4-1 安装 Agent



**步骤4** 在“安装Agent”弹窗中，单击“复制”，复制安装Agent的命令。

**步骤5** 远程登录待安装Agent的主机。

**步骤6** 以root权限执行复制的安装命令，在主机中安装Agent。

若界面回显信息如[图 Agent安装成功](#)所示，则表示Agent安装成功。

图 4-2 Agent 安装成功



**步骤7** 执行以下命令，查看Agent的运行状态。

**service hostguard status**

若界面回显信息如[图 Agent运行正常](#)所示，则表示Agent运行正常。

图 4-3 Agent 运行正常

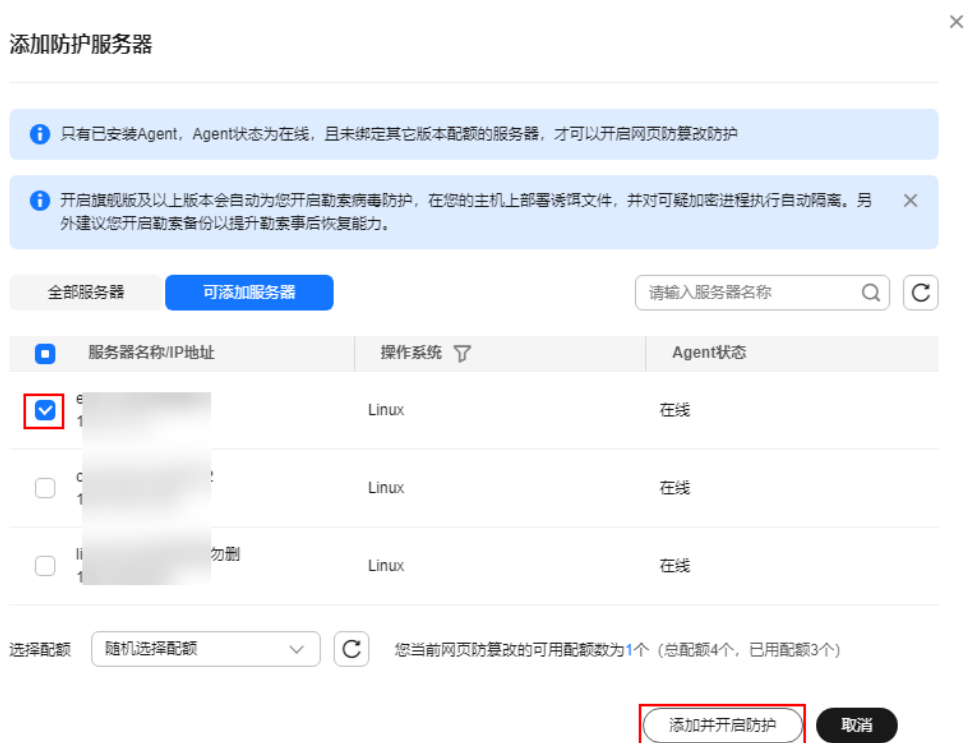
```
your agent is in normal mod.  
hostwatch is running  
hostguard is running with normal mod
```

----结束

### 步骤三：开启防护

- 步骤1** 在主机安全服务控制台左侧导航栏选择“主动防御 > 网页防篡改”，进入网页防篡改页面。
- 步骤2** 在“防护配置”页签，单击“添加防护服务器”。
- 步骤3** 在“添加防护服务器”弹窗中，选择目标服务器并单击“添加并开启防护”。

图 4-4 添加防护服务器



- 步骤4** 阅读添加防护目录的提示，然后单击 **×** 关闭提示。
- 步骤5** 在目标服务器所在行的“操作”列，单击“防护设置”，进入防护设置页面。
- 步骤6** 添加防护目录。
  - 1. 在防护目录设置模块，单击“设置”。
  - 2. 在“防护目录设置”弹窗中，单击“添加防护目录”。

图 4-5 添加防护目录



3. 根据业务实际情况，添加防护目录。参数说明请参见表 添加防护目录参数说明。

表 4-2 添加防护目录参数说明

参数名称	参数说明	取值样例
防护目录	添加需要保护的目录。 - 请勿将操作系统目录添加为防护目录。 - 添加为防护目录后，防护目录下的文件和文件夹将为只读状态，无法直接修改。	/etc/lesuo
排除子目录	排除防护目录下不需要保护的子目录，例如临时文件目录。 多个子目录请用英文分号隔开，最多可添加10个子目录。	lesuo/test
排除文件类型	排除防护目录下不需要保护的的文件类型，例如log类型的文件。 为实时记录主机中的运行情况，请排除防护目录下log类型的文件，您可以为日志文件添加等级较高的读写权限，防止攻击者恶意查看或篡改日志文件。 多个文件类型请用英文分号隔开。	log;pid;text

参数名称	参数说明	取值样例
本地备份路径	<p>服务器操作系统为Linux的用户需要设置此项。</p> <p>设置防护目录文件的本地备份路径，开启网页防篡改防护后，防护目录下的文件会自动备份到设置的本地备份路径中。</p> <p>备份规则说明如下：</p> <ul style="list-style-type: none"> <li>- 本地备份路径须为合法路径，且本地备份路径不能与防护目录路径重叠。</li> <li>- 被排除的子目录和文件类型不会备份。</li> <li>- 防护目录下文件大小不同，备份时间也不同，一般约10分钟完成备份。</li> <li>- 当检测到防护目录下的文件被篡改时，系统将立即使用本地主机备份文件自动恢复被非法篡改的文件。</li> </ul>	/etc/backup
排除文件路径列表	<p>排除防护目录下不需要防护的文件。</p> <p>多个路径请用英文分号隔开，最多可添加50个路径，路径最长字符限制为256；单个路径不能以空格开始，不能以/结束。</p>	lesuo/data;lesuo/list

4. 单击“确认”，完成添加。
5. 在防护目录列表中，查看防护目录防护状态为“防护中”，表示防护目录添加成功。

**步骤7** （可选）启动远端备份。

仅Linux服务器支持远端备份功能，Windows服务器请跳过此项。

1. 在“防护目录设置”弹窗中，单击“管理远端备份服务器”。



图 4-6 管理远端备份服务器



2. 单击“添加远端备份服务器”。
3. 填写远端备份服务器信息并单击“确认”。参数说明请参见表 [添加远端备份服务器参数说明](#)。

表 4-3 添加远端备份服务器参数说明

参数名称	参数说明	取值样例
服务器名称	选择作为远端备份的服务器名称。	test
地址	填写华为云服务器的私网地址。	192.168.1.1
端口	填写服务器端口。请确保设置的端口未被安全组、防火墙等拦截，并且未被占用。	8080

参数名称	参数说明	取值样例
备份路径	<p>填写备份路径，将需要备份的防护目录下的内容备份在该远端备份服务器的目录下。</p> <ul style="list-style-type: none"> <li>- 若多个主机的防护目录同时备份在同一远端备份服务器时，备份路径下生成以“Agentid”为目录的文件夹，存放各主机的防护文件，以使用户手动恢复被篡改的网页。 例如：两台主机的防护目录分别为“/hss01”和“/hss02”，主机Agentid分别为“f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“f2ddbabc-6cdc-43af-abcd-e4e6f086626f”，设置远端备份路径为“/hss01”。</li> <li>- 若设置为远端备份服务器的主机开启了“网页防篡改”防护，那么该备份路径与自身的“防护目录”不能重叠，否则会导致远端备份失败。</li> </ul> <p>备份后路径为“/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f”。</p>	/f1fdbabc-6cdc-43af-acab-e4e6f086625f

4. 在防护目录设置模块，单击“设置”。
5. 在“防护目录设置”弹窗中，单击“启动远端备份”。
6. 选择添加的远端备份服务器，单击“确认”。
7. 远端备份显示“已启动”，表示启动远端备份成功。


**步骤8** （可选）开启动态网页防篡改。

Linux服务器JDK 8的Tomcat应用运行时自我保护，如果您没有Tomcat应用运行时防护的需求或服务器操作系统为Windows，请跳过此项。

1. 在动态网页防篡改模块，单击 。

图 4-7 开启动态网页防篡改



2. 在开启动态网页防篡改弹窗中，填写Tomcat bin目录并单击“确认”。
3. 动态网页防篡改开关按钮显示为 ，表示开启动态网页防篡改成功。

----结束

# 5 快速开启容器安全防护

## 操作场景

节点是容器集群组成的基本元素，主机安全服务容器版以节点为防护单元，提供容器防火墙、容器集群防护、容器镜像安全扫描等功能，可帮助企业解决传统安全软件无法感知的容器环境问题。关于主机安全服务容器版提供安全防护功能请参见[服务版本差异](#)。

本指南以一台EulerOS 2.9华为云容器节点服务器为例，指引您如何快速开启容器安全防护。

## 前提条件

- 云服务器的“状态”为“运行中”，且可正常访问公网。
- 云服务器安全组出方向的设置允许访问100.125.0.0/16网段的10180端口（默认允许访问，如做了改动请修正）。
- 云服务器的DNS服务器地址已配置为华为云内网DNS地址，具体请参考[修改云服务器的DNS服务器地址](#)和[华为云内网DNS地址](#)。
- 安装Agent的磁盘剩余可用容量大于300M，否则可能导致Agent安装失败。
- 云服务器已关闭Selinux防火墙（防止Agent安装失败，请安装成功后再打开）。
- 如果云服务器已安装第三方安全软件，可能会导致主机安全服务Agent无法正常安装，请您关闭或卸载第三方安全软件后再安装Agent。


## 约束限制

- 主机安全服务支持防护64位华为云主机和非华为云主机，不再支持32位主机。
- 主机安全服务支持主流的操作系统，具体请参见[支持的操作系统](#)。

## 步骤一：购买防护配额

**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 > 主机安全服务”，进入主机安全服务页面。

**步骤4** 在“总览”页面右上角，单击“购买主机安全”，进入购买主机安全配额页面。

**步骤5** 根据界面提示，选择购买参数。参数配置说明请参见[表 购买主机安全参数说明](#)。

**表 5-1** 购买主机安全参数说明

参数名称	参数说明
计费模式	选择“包年/包月”。
区域	选择容器节点所属区域。
版本选择	选择“容器版”。
企业项目	<p>企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。</p> <ul style="list-style-type: none"> <li>• 如果需要使用该功能，请联系您的客户经理申请开通。</li> <li>• 如果开通了此功能，请从下拉列表中选择所在的企业项目。</li> </ul> <p><b>说明</b></p> <ul style="list-style-type: none"> <li>• 选择企业项目后，产生的费用和资源均在企业项目内。</li> <li>• “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。</li> <li>• 只有注册的华为账号购买HSS时，“企业项目”下拉列表中才可以选择到“default”。</li> </ul>
购买时长	<p>选择1个月，并勾选“自动续费”。</p> <p>勾选“自动续费”后，当购买的主机安全服务到期时，如果账号余额充足，系统将自动为购买的主机安全服务续费，续费周期与购买时长保持一致。</p>
防护节点数	输入防护的节点数量为1台。
标签	<ul style="list-style-type: none"> <li>• 如果没有预定义标签，单击“查看预定义标签”，创建一个预定义标签。</li> <li>• 如果已有预定义标签，鼠标依次单击“标签键”和“标签值”选框，选择一个预定义的标签。</li> </ul>
配额管理	<p>勾选自动绑定。</p> <p>开启自动绑定配额后，如果您有新增的主机或容器节点，这些主机或容器节点在首次安装Agent之后，HSS会自动为其绑定空闲可用配额。仅自动绑定您已购买的包年/包月配额，不会产生新的订单及费用。</p> <ul style="list-style-type: none"> <li>• 主机：按“旗舰版&gt;企业版&gt;专业版&gt;基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> <li>• 容器节点：按“容器版&gt;旗舰版&gt;企业版&gt;专业版&gt;基础版”的顺序自动绑定空闲可用的包年/包月配额。</li> </ul>

**步骤6** 在页面右下角，单击“立即购买”，进入“订单确认”界面。

费率标准请参见[产品价格详情](#)。

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

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

**步骤9** 单击“返回主机安全服务控制台”，返回主机安全服务控制台。

----结束

## 步骤二：安装 Agent

**步骤1** 在主机安全服务控制台左侧导航栏选择“安装与配置”，进入安装与配置页面。

**步骤2** 在“Agent管理”页签，单击“未安装Agent服务器数”区域的数值，筛选未安装Agent的服务器。

**步骤3** 在目标服务器的“操作”列，单击“安装Agent”。

图 5-1 安装 Agent



**步骤4** 在“安装Agent”弹窗中，单击“复制”，复制安装Agent的命令。

**步骤5** 远程登录待安装Agent的主机。

**步骤6** 以root权限执行复制的安装命令，在主机中安装Agent。

若界面回显信息如图 Agent安装成功所示，则表示Agent安装成功。

图 5-2 Agent 安装成功

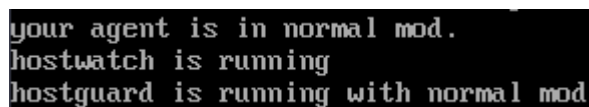


**步骤7** 执行以下命令，查看Agent的运行状态。

```
service hostguard status
```

若界面回显信息如图 Agent运行正常所示，则表示Agent运行正常。

图 5-3 Agent 运行正常



----结束

### 步骤三：开启防护

**步骤1** 在主机安全服务控制台左侧导航栏选择“资产管理 > 容器管理”，进入容器管理页面。

**步骤2** 在目标服务器所在行的“操作”列，单击“开启防护”。

**步骤3** 在“开启防护”弹窗中，选择开启方式。参数配置说明如表 [开启防护参数说明](#) 所示。

表 5-2 开启防护参数说明

参数名称	参数说明
计费模式	选择“包年/包月”。
版本选择	选择“容器版”。
选择配额	保持默认“随机选择配额”。

**步骤4** 确认信息无误后，请阅读《容器安全服务免责声明》并勾选“我已阅读并同意《容器安全服务免责声明》”。

**步骤5** 单击“确认”，开启防护。

**步骤6** 查看目标服务器的防护状态为“防护中”，表示开启防护成功。

图 5-4 查看防护状态

服务器信息	服务器状态	Agent状态	容器防护状态	操作
[模糊]	正常	在线	防护中	关闭防护 部署策略
[模糊]	正常	在线	未防护	开启防护 部署策略

----结束


# 6 ECS 安全态势速查

您在购买华为云弹性云服务器ECS后，如果使用了主机安全服务防护云服务器，可以参考本章节快速查看云服务器的安全态势。

## 在 ECS 控制台查看云服务器安全态势

**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“计算 > 弹性云服务器”，进入弹性云服务器页面。

**步骤4** 鼠标滑动至目标云服务器所在行的“安全”列，查看ECS安全态势。

可查看最近24小时的资产风险、漏洞风险、基线风险以及入侵告警事件个数。单击对应的风险数值，可跳转到对应的风险详情列表，查看并处理安全风险。


图 6-1 查看 ECS 安全态势




----结束

## 在 HSS 控制台查看云服务器安全态势

**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 > 主机安全服务”，进入主机安全服务页面。



**步骤4 查看云服务器安全态势。**

- **查看所有云服务器安全态势**

- 在总览页面的“安全评分”区域，查看当前您拥有的所有云服务器资产安全风险评分，单击“立即处理”，可查看您资产中存在的各类风险分类。安全评分标准以及减少扣分的方法请参见[安全评分扣分标准](#)。

**图 6-2 查看安全评分**



- 在“安全风险处理”弹窗中，单击展开查看风险明细。
- 单击“前往处理”可跳转到对应的风险详情页，查看并处理安全风险。

- **查看单个云服务器安全态势**

- 在左侧导航栏选择“资产管理 > 主机管理”，进入云服务器列表页面。
- 在目标服务器所在行的“检测结果”列，查看云服务器是否有风险。鼠标滑动至风险提示图标处，可查看风险分布。

**图 6-3 查看 ECS 安全态势**

服务器信息	服务器状态	Agent状态	防护状态	检测结果	风险分布
<input type="checkbox"/> #一般 (私)	运行中	在线	● 防护中	🔴 有风险	资产管理: 0 漏洞管理: 11 基线检查: 37 入侵检测: 0
<input type="checkbox"/> #一般 223 (私)	运行中	离线 ?	● 防护中断 ?	🔴 有风险	

- 单击云服务器名称，进入云服务器详情页，查看并处理安全风险。

----结束