主机安全服务

快速入门

文档版本 01

发布日期 2024-01-15

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 免费试用主机安全基础版 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时，在“基础配置”页勾选“免费试用一个月主机安全基础防护”，购买完成后，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**。

如下操作以购买1台包年/包月ECS（规格：c6.xlarge.2，镜像：Huawei Cloud EulerOS 2.0 标准版 64位）为例，为您介绍如何免费试用HSS基础版30天。

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“基础配置”、“网络配置”、“高级配置”、“确认配置”相关参数。

1. 设置“基础配置”参数，设置完成后，单击“下一步：网络配置”。
   - CPU架构：此处示例选择“x86计算”。
   - 规格：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)”。
   - 安全防护：选择“免费试用一个月主机安全基础防护”。
   - 其他参数：请根据实际情况设置。

图 1-1 基础配置

2. 设置“网络配置”参数，设置完成后，单击“下一步：高级配置”。

请根据实际情况设置。

3. 设置“高级配置”参数，设置完成后，单击“下一步：确认配置”。

   请根据实际情况设置。

4. 设置“确认配置”参数。
   - 协议：阅读并勾选《镜像免责声明》。
   - 其他参数：请根据实际情况设置。

步骤3 确认所有信息无误后，单击“去支付”，完成支付后，云服务器将自动创建，并默认开机。

云服务器状态为“运行中”后，将自动安装主机安全服务的Agent并开启“基础版”防护，这个过程预计需要20分钟左右。

步骤4 鼠标悬浮在云服务器所在行的“安全”列，单击“查看详情”，跳转至主机安全服务界面。

步骤5 查看云服务器的“防护状态”为“防护中”，“版本”为“基础版”，“到期时间”为“30天后到期”。

表示试用HSS基础版成功。

----结束

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。

2 购买并开启主机安全防护

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，指引您如何购买并开启主机安全防护。

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”，进入购买主机安全页面。

步骤5 根据界面提示，选择购买参数。

- 计费模式：根据实际需求，选择配额计费模式；此处示例选择“包年/包月”。
- 区域：选择主机所在区域，此处示例选择“中国-香港”。
- 版本规格：选择HSS版本，不同版本提供的防护功能存在差异；此处示例选择“企业版”。
- 购买数量：根据主机数量设置数值，此处示例购买“1”台。
- 其他参数：根据实际情况选择。

步骤6 在页面右下角，单击“立即购买”，进入“订单确认”界面。

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 > 主机安装与配置”，进入主机安装与配置页面。

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 2-1 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 2-2 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

若界面回显如**图 Agent运行正常**所示，则表示Agent运行正常。

图 2-3 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。

根据**步骤一：购买防护配额**，购买的配额版本，进行选择。

- 计费模式：选择“包年/包月”。
- 版本选择：选择“企业版”。

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 2-4 查看防护状态

----结束

3 购买并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，指引您如何购买并开启网页防篡改防护。

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。

- 计费模式：选择“包年/包月”，网页防篡改仅支持“包年/包月”计费模式。
- 区域：选择主机所在区域，此处示例选择“中国-香港”。
- 版本规格：选择“网页防篡改版”。
- 购买数量：根据主机数量设置数值，此处示例购买“1”台。
- 其他参数：根据实际情况选择。

步骤6 在页面右下角，单击“立即购买”，进入“订单确认”界面。

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 > 主机安装与配置”，进入主机安装与配置页面。

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

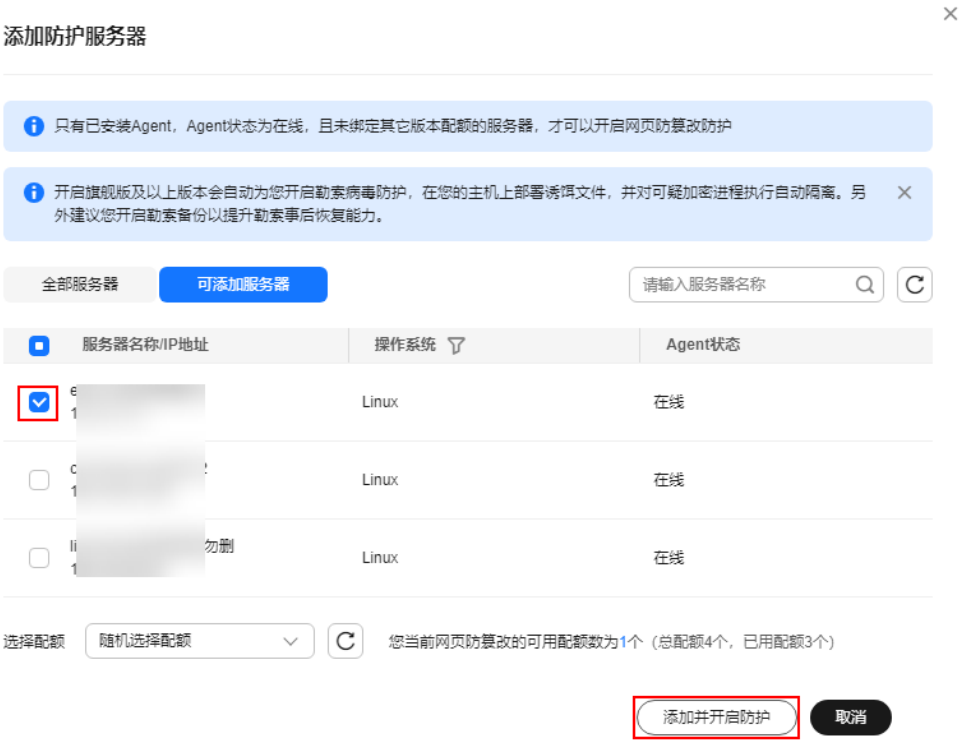
步骤三：开启防护

步骤1 在主机安全服务控制台左侧导航栏选择“主机防御 > 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”。

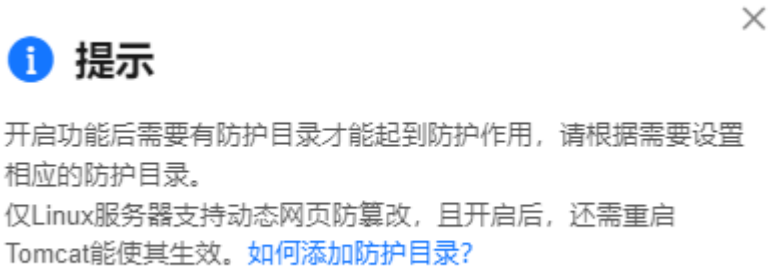
步骤3 在“添加防护服务器”弹窗中，选择目标服务器并单击“添加并开启防护”。

图 3-4 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。

图 3-5 防护目录提示



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。

图 3-6 进入防护设置

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 3-7 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 3-1 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	添加需要防护的目录。 – 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防护的子目录，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防护的文件类型，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	服务器操作系统为Linux的用户需要设置此项。 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。 备份规则说明如下： – 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。 – 被排除的子目录和文件类型不会备份。 – 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。 – 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。	/etc/backup
排除文件路径列表	排除防护目录下不需要防护的文件。 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。	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 3-8 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 3-2 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	填写作为远端备份的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	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。 – 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，以便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”。 备份后路径为“/hss01/f1fdbabc-6cdc-43af-acab-e4e6f086625f”和“/hss01/f2ddbabc-6cdc-43af-abcd-e4e6f086626f”。 – 若设置为远端备份服务器的主机开启了“网页放篡改”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。	/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 3-9 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”。
   此处Tomcat bin目录示例“/usr/workspace/apache-tomcat-8.5.15/bin”
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。
4. 重启Tomcat，生效动态网页防篡改功能。

----结束

相关操作

- **修改防护目录下的文件/文件夹**

  开启网页防篡改防护后，对应防护目录下的文件/文件夹为只读状态，不允许被修改，如果您需要修改防护目录下的文件/文件夹，请参考以下方式：
  - 添加特权进程：特权进程最多支持添加10个，详细操作请参见**添加特权进程**。
  - 定时开启/关闭静态网页防篡改：除了添加特权进程外，您可以设置定时开启/关闭静态网页防篡改，在网页防篡改关闭时段修改文件/文件夹，详细操作请参见**定时开启/关闭静态网页防篡改**。
- **开启服务器主动防护功能**

  主机安全服务**网页防篡改版**为服务器提供了一些主动防护功能，这些功能在开启网页防篡改防护时并未开启或未完全开启，您可以根据自身的业务情况综合考虑是否使用这些功能，需要您自行选择开启的功能及说明如**表 服务器主动防护功能说明**。

表 3-3 服务器主动防护功能说明

功能	说明
勒索病毒防护	勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机业务中断、数据泄露或丢失，主机所有者即使支付赎金也可能难以挽回所有损失，因此勒索病毒是当今网络安全面临的最大挑战之一。主机安全服务支持静态、动态勒索病毒防护，定期备份主机数据，可以帮助您抵御勒索病毒，降低业务损失风险。 开启网页防篡改防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略，同时建议您开启勒索备份以提升勒索事后恢复能力。

功能	说明
应用防护	应用防护功能旨在为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。
应用进程控制	应用进程控制功能支持管控应用进程运行，通过学习服务器中运行的应用进程特征，将应用进程划分为可信进程、恶意进程和可疑进程，允许可疑、可信进程正常运行，对恶意进程运行进行告警，帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。
病毒查杀	病毒查杀功能使用特征病毒检测引擎，支持扫描服务器中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可根据自身需要，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”扫描任务，并及时处置检测到的病毒文件，增强业务系统的病毒防御能力。

4 购买并开启容器安全防护

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华为云集群节点为例，指引您如何购买并开启容器安全防护。

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。

- 计费模式：根据实际需求，选择配额计费模式；此处示例选择“包年/包月”。
- 区域：选择主机所在区域，此处示例选择“中国-香港”。
- 版本规格：选择“容器版”。
- 购买数量：根据容器节点数量设置数值，此处示例购买“1”台。
- 其他参数：根据实际情况选择。

步骤6 在页面右下角，单击“立即购买”，进入“订单确认”界面。

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 > 主机安装与配置”，进入主机安装与配置页面。

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

```
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“资产管理 > 容器管理”，进入容器管理页面。

步骤2 在目标服服务器所在行的“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。

根据**步骤一：购买防护配额**，购买的配额版本，进行选择。

- 计费模式：选择“包年/包月”。
- 版本选择：选择“容器版”。

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 4-4 查看防护状态

----结束

相关操作

开启容器节点服务器防护功能

主机安全服务**容器版**为服务器提供了一些主动防护功能，这些功能在开启容器安全防护时并未开启或未完全开启，您可以根据自身的业务情况综合考虑是否使用这些功能，需要您自行选择开启的功能及说明如**表 容器节点防护功能说明**

表 4-1 容器节点防护功能说明

功能	说明
容器镜像安全扫描	容器镜像安全扫描功能能够扫描镜像中的漏洞、恶意文件等信息，建议您定期扫描，以便您能及时处理镜像安全风险。
勒索病毒防护	勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机业务中断、数据泄露或丢失，主机所有者即使支付赎金也可能难以挽回所有损失，因此勒索病毒是当今网络安全面临的最大挑战之一。主机安全服务支持静态、动态勒索病毒防护，定期备份主机数据，可以帮助您抵御勒索病毒，降低业务损失风险。 开启容器版防护会自动为您开启勒索病毒防护，在您的主机上部署诱饵文件，并对可疑加密程序执行自动隔离。您可以修改勒索病毒防护策略，同时建议您开启勒索备份以提升勒索事后恢复能力。
应用防护	应用防护功能旨在为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。
应用进程控制	应用进程控制功能支持管控应用进程运行，通过学习服务器中运行的应用进程特征，将应用进程划分为可信进程、恶意进程和可疑进程，允许可疑、可信进程正常运行，对恶意进程运行进行告警，帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。

功能	说明
病毒查杀	病毒查杀功能使用特征病毒检测引擎，支持扫描服务器中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件；用户可根据自身需要，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”扫描任务，并及时处置检测到的病毒文件，增强业务系统的病毒防御能力。
容器集群防护	容器集群防护功能支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。 用户可根据自身业务场景灵活配置容器集群防护策略，加固集群安全防线，防止含有漏洞、恶意文件和不合规基线等安全威胁的镜像部署到集群，降低容器生产环境的安全风险。
容器防火墙	容器防火墙是一种为容器环境提供的防火墙服务，支持对容器集群内部与外部的网络流量进行控制和拦截，防止恶意访问和攻击。

5 快速查看 ECS 安全态势

如果您未开通主机安全服务，主机安全服务针对未开启防护的ECS，每周提供一次全量的免费安全体检，检测时间为每周一凌晨。您可以参考本章节查看未开启防护的ECS安全态势。

如果您使用了主机安全服务防护弹性云服务器ECS，可以参考本章节查看已开启防护的ECS安全态势。

查看未开启防护的 ECS 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 在左侧导航栏，选择“安全运营 > 安全报告”，进入“安全报告”页面。

步骤5 选择“免费体检”页签。

步骤6 查看未开启防护的ECS安全态势。

图 5-1 查看安全态势

- 安全评分：当前区域内，所有ECS的综合安全评分，以及存在的风险数量。

- 服务器风险分布：风险服务器占比和服务器风险等级分布。
- 明细报告：如需查看ECS的详细体检报告，可在目标ECS所在行的“操作”列，单击“查看报告”，查看报告详情。

  说明

  - 免费体检的报告每月1日生成，生成后仅支持线上查看，不支持下载。
  - 在报告中单一体检项仅支持展示总结果数的一半，且最多仅展示5条体检结果。

----结束

查看已开启防护的 ECS 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**
  - 查看安全评分
    i. 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 5-2 查看安全评分

    ii. 在“安全风险处理”弹窗中，单击展开查看风险明细。
    iii. 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。
  - 查看安全风险分布及趋势。
    i. 在总览页面的“安全风险”区域。查看当前资产安全风险分布情况，和近7天的安全风险趋势。
    ii. 单击主机风险或容器风险的数值，可跳转到对应的风险详情页面，查看并处理风险。
- **查看单个云服务器安全态势**
  a. 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。
  b. 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 5-3 查看 ECS 安全态势

c. 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

6 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 6-1 常用实践

实践		描述
主机登录保护	HSS登录安全加固最佳实践	通过HSS登录防护配置，帮助您提升主机登录安全。
漏洞修复	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。 本实践介绍通过HSS检测与修复该漏洞的建议。
	SaltStack远程命令执行漏洞（CVE-2020-11651/CVE-2020-11652）	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。
	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。 本实践介绍通过HSS检测与修复该漏洞的建议。

实践		描述
	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。 本实践介绍通过HSS检测与修复该漏洞的建议。
	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。 本实践介绍通过HSS检测与修复该漏洞的建议。
	Windows CryptoAPI欺骗漏洞（CVE-2020-0601）	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。 本实践介绍通过HSS检测与修复该漏洞的建议。
多云主机纳管	HSS多云纳管部署	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，避免因为不同平台安全水位不一致导致的攻击风险。
勒索病毒防护	勒索病毒防护最佳实践	勒索病毒攻击已成为当今企业面临的最大安全挑战之一。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。 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。
网页防篡改	“WAF+HSS”联动，提升网页防篡改能力	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。