ALIBABA CLOUD

阿里云

云安全中心（态势感知）

主动防御

文档版本：20201026

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	**单击设置> 网络> 设置网络类型。**
粗体	表示按键、菜单、页面名称等UI元素。	**在结果确认页面，单击确定。**
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.防勒索

1.1. 防勒索概述

勒索病毒已成为网络安全的最大威胁。云安全中心针对勒索病毒提供了通用防勒索解决方案，帮助您从勒索病毒入侵前、入侵时和入侵后全方位应对勒索病毒。

背景信息

防勒索为云安全中心提供的增值服务，基础杀毒版、高级版或企业版用户购买防勒索容量后才可使用防勒索数据备份功能。基础版用户需要先升级到基础杀毒版、高级版或企业版，才可使用防勒索功能。

防勒索功能支持的操作系统版本有限，不在支持范围内的服务器将无法成功安装防勒索客户端并进行数据备份。支持的操作系统请参见防勒索支持的操作系统。

> 说明
>
> - 防勒索数据备份功能现已支持西南1（成都）、华东2金融云（上海）、华北2阿里政务云、华东2（上海）、华东1（杭州）、华北2（北京）、华南1（深圳）、华北3（张家口）、华北5（呼和浩特）、华北1（青岛）、中国香港、新加坡、印度尼西亚（雅加达）、澳大利亚（悉尼）、美国（硅谷）、美国（弗吉尼亚）、德国（法兰克福）、日本（东京）和印度（孟买）地域。
> - 目前，仅支持使用VPC（专有网络）的ECS服务器进行防勒索备份，暂不支持使用经典网络的ECS服务器进行防勒索备份。

勒索病毒防护原理

通用防勒索解决方案为您提供逐层递进的纵深式防御体系：

- **实时防御已知勒索病毒**

  借助云上全方位的威胁情报，云安全中心实现了对大量已知勒索病毒的实时防御。在服务器被病毒感染的第一时间拦截勒索病毒，避免发生文件被病毒加密而进行勒索的情况。

- **诱捕、拦截新型未知勒索病毒**

  通过放置诱饵的方式，云安全中心实时捕捉可能存在的勒索病毒行为。针对新型未知的勒索病毒，一旦识别到有异常加密行为发生，会立刻拦截病毒，同时通知您进行排查清理。

  > 说明 您可以在云安全中心控制台设置页面的主动防御区域开启防勒索（诱饵捕获）功能。开启该功能后，云安全中心为捕捉勒索病毒会在您的服务器中设置目录陷阱。如果您服务器中出现可疑目录，请您及时联系售后人员或提交工单确认该目录是否为云安全中心设置的诱饵目录。诱饵目录不会对您的业务造成影响，也不存在任何的恶意行为，并且不支持手动删除。

- **支持恢复被病毒感染文件**

  在对勒索病毒进行防御的同时，云安全中心还支持文件备份服务，能定期对指定文件进行备份，支持按时间或文件版本恢复服务器数据。在发生极端情况导致文件被加密时，能够通过文件恢复的方式找回数据，确保服务器数据的安全。

防勒索支持的操作系统

系统	支持的版本
Windows	7、8、10
Windows Server	2008 R2、2012、2012 R2、2016、2019
RHEL	7.0、7.2、7.4
CentOS	6.5、6.9、7.2、7.3、7.4、8.2
Ubuntu	14.04、16.04、18.40、20.04
SUSE Linux Enterprise Server	11、12、15

说明 防勒索仅支持在以上表格中的操作系统安装防勒索客户端，不在以上表格中的操作系统将无法安装防勒索客户端并进行数据备份。建议您在使用防勒索功能前，先确认您服务器的操作系统是否在以上支持范围内。

1.2. 开通服务

使用云安全中心防勒索功能前需先购买并开通该服务。

背景信息

- 防勒索为云安全中心提供的增值服务，基础杀毒版、高级版或企业版用户购买防勒索容量后才可使用防勒索数据备份功能。基础版用户需要先升级到基础杀毒版、高级版或企业版，才可使用防勒索功能。

  注意 防勒索客户端支持的操作系统类型有限，不在支持范围内的操作系统将无法安装防勒索客户端并进行数据备份。防勒索支持的操作系统请参见防勒索支持的操作系统。建议您在购买防勒索容量前，先确认您服务器的操作系统在支持的操作系统范围内。

- 首次使用防勒索功能需要先完成授权，赋予当前账号AliyunHBRDefaultRole和AliyunECSAccessingHBRRole这两个角色。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面单击**立即授权**。
4. 在**云资源访问授权**页面单击**同意授权**。为了防勒索功能的正常使用，您需要授权当前账号AliyunHBRDefaultRole和AliyunECSAccessingHBRRole这两个角色。
5. 单击**立即升级**。

   立即购买页面

6. 在**请选择适合您的产品版本**页面单击**升级**。

7. 说明 防勒索客户端支持的操作系统类型有限，不在支持范围内的操作系统将无法安装防勒索客户端并进行数据备份。防勒索支持的操作系统请参见防勒索支持的操作系统。建议您在购买防勒索容量前，先确认您服务器的操作系统在支持的操作系统范围内。

   在购买页面选择合适的云安全中心版本和防勒索数据防护容量。

   

   您可以根据以下说明购买适合您的云安全中心产品。

   - 云安全中心支持购买基础杀毒版、高级版和企业版。各版本的功能差异详情请参见功能特性。
   - 数据防护容量是指通用防勒索解决方案备份服务器数据时使用的存储容量。建议您根据需要防护的服务器数据的实际规模来购买数据防护容量。如果无法预估需要防护的服务器数据规模，建议您为每台服务器购买40 GB的防护容量。更多计费信息请参见计费模式。

8. 单击立即购买，并完成支付。

后续步骤

开通防勒索功能后，您需要通过创建防护策略为您的服务器添加勒索防护，详细操作步骤请参见创建防护策略。

1.3. 创建防护策略

勒索病毒已经成为网络安全最大的威胁，云安全中心针对勒索病毒提供防御、告警和数据备份的能力，可预防勒索病毒入侵您的服务器。您可以为您的服务器创建勒索病毒防护策略，备份您服务器上的数据。本文介绍如何创建防护策略。

前提条件

已购买防勒索容量并完成授权。更多信息请参见开通服务。

背景信息

- 为您的服务器创建防护策略后，云安全中心会自动备份您服务器防护目录下的数据。如果您的服务器数据被勒索病毒感染，您可以随时恢复已备份的数据，避免勒索病毒对您的业务产生影响。
- 为保证您的防护容量得到合理和有效地利用，每台服务器只支持添加到一个防护策略中。每个防护策略中，最多只能添加100台服务器。
- 防勒索数据备份通过在您的ECS服务器上安装的防勒索客户端进行，防勒索客户端为正常状态才能进行数据备份。创建防护策略后，建议您重点关注防勒索客户端的状态，及时处理防勒索客户端的异常状态。更多信息请参见相关操作的查看防勒索客户端状态。

> 说明
> - 仅基础杀毒版、高级版和企业版支持创建勒索防护策略，基础版需要升级到基础杀毒版、高级版或企业版才能创建勒索防护策略。
> - 可创建防护策略的服务器需要满足一定的限制条件。详细限制条件请参见限制条件。

支持的地域

防勒索数据备份功能现已支持西南1（成都）、华东2金融云（上海）、华北2阿里政务云、华东2（上海）、华东1（杭州）、华北2（北京）、华南1（深圳）、华北3（张家口）、华北5（呼和浩特）、华北1（青岛）、中国香港、新加坡、印度尼西亚（雅加达）、澳大利亚（悉尼）、美国（硅谷）、美国（弗吉尼亚）、德国（法兰克福）、日本（东京）和印度（孟买）地域。

限制条件

使用防勒索功能的服务器需要同时满足以下限制条件：

- 您的服务器为阿里云ECS服务器。防勒索功能仅支持备份阿里云ECS服务器数据，不支持备份非阿里云服务器数据。您只能为您的阿里云ECS服务器创建防护策略。
- 您的ECS服务器使用VPC（专有网络）。目前，仅支持使用VPC（专有网络）的ECS服务器进行防勒索备份，暂不支持使用经典网络的ECS服务器进行防勒索备份。
- 您的服务器操作系统版本在支持范围内。不在支持范围内的服务器将无法进行数据备份。支持的操作系统详情请参见防勒索支持的操作系统。

数据备份说明

- 防勒索数据备份采用增量备份的方式。防护策略创建后，初次进行数据备份时由于要全量备份防护目录下的数据，会消耗一定量的CPU和内存资源。为避免对您的业务造成影响，建议您选择业务量较小的时段进行数据备份。后续再次进行备份时，云安全中心只备份有变化（修改、增加或删除）的文件，为您降低服务器资源消耗同时避免消耗过多的防勒索容量。
- 根据您防护策略中设置的备份目录不同，云安全中心会自动启动不同数量的备份任务。以下是相关说明：
  - **备份全部目录**
    - Linux系统：只生成一个备份任务。
    - Windows系统：一个数据盘会生成一个数据备份任务。例如您的Windows服务器上有C、D两个数据盘，云安全中心将生成两个数据备份任务，这两个任务会同时启动，消耗的CPU和内存资源会高于Linux服务器。

      > **注意** 建议您根据Windows服务器的CPU和内存资源使用情况，合理安排数据备份的时间。

  - **备份指定目录**

    对防护策略中每个目录地址，云安全中心会启动相应的数据备份任务。目前多个数据备份任务会同时进行，可能会占用较多的CPU和内存资源。建议您根据实际情况，设置合理数量的备份目录。

    > **说明** 云安全中心正在优化现有的备份流程，后续一个客户端将只启动一个数据备份任务，为您进一步降低数据备份带来的CPU和内存资源消耗。敬请期待。

创建防护策略

创建防护策略时您可以选择**推荐策略**快速创建防护策略，也可以根据实际情况选择**自定义策略**。参考以下步骤创建防护策略：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面单击**创建防护策略**。您也可以单击**未防护的服务器**下的数字进入**创建防护策略**页面。

   未保护服务器入口

4. 在创建防护策略页面，配置防护策略相关参数。

您可以参考以下表格中的参数说明配置防护策略。

参数	说明
策略名称	输入防护策略的名称。
选择资产	支持选中单台资产、跨组选中多台资产或者选中资产分组。 执行以下操作选择需要防护的资产： ○ 在资产分组区域选择某一资产分组，系统将自动选择该分组下的所有资产。您可在右侧资产模块下，取消选中不需要的防护的资产。 ○ 在资产模块下输入资产名称（支持模糊查询），单击搜索框的搜索按钮后会为您展示相关资产，您可选中需要防护的资产。 说明 ○ 为保证您的防护容量得到合理和有效地利用，每台服务器只支持添加到一个防护策略中。每个防护策略中，最多只能添加100台服务器。 ○ 防勒索功能仅支持备份阿里云ECS服务器数据，不支持备份非阿里云服务器数据。您只能为您的阿里云ECS服务器创建防护策略。 ○ 防勒索数据备份功能现已支持西南1（成都）、华东2金融云（上海）、华北2阿里政务云、华东2（上海）、华东1（杭州）、华北2（北京）、华南1（深圳）、华北3（张家口）、华北5（呼和浩特）、华北1（青岛）、中国香港、新加坡、印度尼西亚（雅加达）、澳大利亚（悉尼）、美国（硅谷）、美国（弗吉尼亚）、德国（法兰克福）、日本（东京）和印度（孟买）地域。其他地域暂不支持。目前您只能选择防勒索支持的地域下的ECS服务器。
防护策略	支持选择以下策略： ○ 推荐策略 选择推荐策略后，默认选择以下配置： ■ 防护目录：全部目录（排除系统目录） ■ 防护文件类型：全部文件类型 ■ 数据备份开始时间：00:00~03:00的任一时刻 ■ 备份策略执行间隔：一天 ■ 备份数据保留时间：七天 ■ 备份网络带宽限制（MB/s）：5 MB/s ○ 自定义策略 选择自定义策略后，您需要自定义防护策略的防护目录、防护文件类型、数据备份开始时间、备份策略执行间隔、备份数据保留时间、备份网络带宽限制（MB/s）等参数。

参数	说明
防护目录	选择需要进行防护的目录，支持选择以下类型： ○ **指定目录**：防护已选中资产的指定目录。您需要在**目录地址**文本框中输入需要防护的目录地址。 ○ **全部目录**：防护已选中资产的全部目录。 您需要在**是否排除系统目录**处选择是否排除系统目录。 **说明** 为防止出现系统冲突，选择**全部目录**后，建议您在设置**是否排除系统目录**时选择**排除**。

参数	说明
是否排除系统目录	选择**排除**或**不排除**系统目录。以下是选择**排除**后Windows和Linux系统的排除目录： ○ **Windows**： ■ Windows\ ■ python27\ ■ Program Files (x86)\ ■ Program Files\ ■ ProgramData\ ■ Boot\ ■ $RECYCLE.BIN\ ■ System Volume Information\ ■ Users\Administrator\NTUSER.DAT ■ pagefile.sys ○ **Linux**： ■ /bin/ ■ /usr/bin/ ■ /sbin/ ■ /boot/ ■ /proc/ ■ /sys/ ■ /srv/ ■ /lib/ ■ /selinux/ ■ /usr/sbin/ ■ /run/ ■ /lib32/ ■ /lib64/ ■ /lost+found/ ■ /var/lib/kubelet/
目录地址	输入需要防护的目录地址。如果有多个目录需要防护，您可以单击**新增**增加目录地址。如果不需要防护某条目录，您可以单击**删除**来删除该目录地址。 **说明** ○ 仅在**防护目录**选择**指定目录**时需要配置该参数。 ○ 对防护策略中每个目录地址，云安全中心会启动相应的数据备份任务。目前多个数据备份任务会同时进行，可能会占用较多的CPU和内存资源。建议您根据实际情况，设置合理数量的备份目录。

参数	说明
防护文件类型	选择需要进行防护的文件类型，支持选择以下类型： ○ **指定类型**：防护指定类型的文件。您需要在**选择文件类型**中选择需要防护的具体文件类型。 ○ **全部文件类型**：防护所有类型的文件。
选择文件类型	支持选择以下文件类型： ○ **文档类** ○ **图片类** ○ **压缩包类** ○ **数据库类** ○ **音频视频类** ○ **脚本代码类** 说明 ○ 仅在**防护文件类型**选择**指定文件类型**时需要配置该参数。 ○ 支持同时选中多个文件类型。云安全中心仅防护您资产中此处选中类型的文件。
数据备份开始时间	设置数据备份开始时间。数据备份可能会占用少量CPU和内存，建议您将数据备份开始时间设置为业务量较小的时段，例如00:00。 说明 防护策略创建后，初次进行数据备份时由于要全量备份防护目录下的数据，会消耗一定量的CPU和内存资源。为避免对您的业务造成影响，建议您选择业务量较小的时段进行数据备份。
备份策略执行间隔	设置备份策略执行间隔，默认为一天。支持选择以下时间： ○ **半天** ○ **一天** ○ **三天** ○ **七天**
备份数据保留时间	设置备份数据保留时间，默认为7天。支持选择以下时间： ○ **7天** ○ **30天** ○ **半年** ○ **一年** ○ **永久**

参数	说明
备份网络带宽限制（MB/s）	受防勒索保护的备份数据占用的带宽流量阈值。可以设置的范围：1 MB/s~不限流量。 说明 建议您根据服务器的带宽，设置合理的流量阈值，避免备份占用过多带宽对您业务产生影响。

5. 单击**确定**。创建并启用防护策略后，云安全中心将自动在您的ECS服务器上安装防勒索客户端，并根据防护策略中设置的备份条件对生效服务器的防护目录进行数据备份。

后续步骤

创建策略后还需要在防护策略列表中开启该策略，云安全中心才会备份该策略中设置的文件目录。详细操作步骤请参见启用或停用防护策略。

开启防护策略

相关操作

- **查看防勒索客户端状态**

  创建防护策略完成后，您需要在**通用防勒索解决方案**页面查看防勒索客户端的状态。只有备份客户端的状态为**客户端在线（正常状态）**，才能正常备份服务器数据。如果备份客户端状态为**未安装**、**安装失败**或**服务器异常**，则防护策略无法进行正常备份。您需要排查异常状态原因并处理防勒索客户端的异常。您可以通过以下方式排查异常：

  - 根据界面提示自行排查并解决防勒索客户端状态异常问题，详细操作步骤请参见防勒索客户端异常状态排查。
  - 提交工单联系阿里云安全工程师协助您处理。

- **安装防勒索客户端**

  创建防护策略后，云安全中心将自动在您的ECS服务器上安装防勒索客户端。您的ECS服务器未启动或配置了特定的防火墙策略可能会导致系统自动安装失败。防勒索客户端安装失败后，您需要先排查并处理安装失败原因，然后在**通用防勒索解决方案**页面手动安装防勒索客户端。手动安装防勒索客户端的操作步骤请参见管理防护策略中的服务器。

- **卸载防勒索客户端**

  注意
  - 防勒索客户端卸载后，云安全中心将删除该客户端已备份的服务器数据。备份数据删除后将无法找回，建议您谨慎进行卸载客户端操作。
  - 云安全中心删除该客户端已备份的服务器数据后，会为您释放相应的勒索防护容量。勒索防护容量释放存在12~48小时的延时，建议您等待足够时间后再重新查看勒索防护容量。

  如果防勒索客户端需要升级版本时，您可以在**通用防勒索解决方案**卸载防勒索客户端后，再重新安装。

1.4. 管理防护策略

防护策略创建后，您可以启用、停用策略或修改策略名称、绑定的资产、防护目录等信息。如果您的业务已经不再需要某个防护策略，您可以删除该防护策略。本文介绍如何启用、停用、编辑、删除防护策略以及管理防护策略下的服务器。

前提条件

已创建勒索防护策略。更多信息请参见创建防护策略。

背景信息

防护策略状态为**正常**时，防护策略才能生效。如果您的防护策略状态为**异常**，需要及时处理该异常状态。更多信息请参见防护策略为异常状态怎么办。

启用或停用防护策略

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面定位到需要启用或停用的策略，在该策略的**策略状态**下启用或停用策略。
   - **启用策略**

     防护策略启用后，防勒索才能保护您的服务器数据。您可以打开**策略状态**开关为策略中的服务器开启防勒索保护。

     
   - **停用策略**

     > **注意** 如果当前防护策略下正在运行数据恢复任务，停用该策略后恢复任务将停止。建议您确认当前策略无正在运行的恢复任务后，再停用该策略。

     如果您的服务器暂时不需要勒索病毒防护，您可以关闭防护策略**策略状态**开关。

编辑防护策略

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面定位到需要修改的防护策略并单击操作列的**编辑**。

   
4. 在**编辑防护策略**页面，修改防护策略的参数。

   

   防护策略的参数说明请参见创建防护策略参数表。
5. 单击**确定**。

管理防护策略中的服务器

创建防护策略后，您可以为防护策略添加或删除服务器，并在您的服务器上安装或卸载防勒索客户端。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。

3. 在**通用防勒索解决方案**页面定位到需要管理服务器的防护策略，单击 图标。

4. 管理该防护策略生效的服务器列表。您可以执行以下操作：

   - **为防护策略添加服务器**

     您可以在编辑防护策略时，为该防护策略添加生效服务器。详细操作步骤请参见编辑防护策略。

     为保证您的防护容量得到合理和有效地利用，每台服务器只支持添加到一个防护策略中。每个防护策略中，最多只能添加100台服务器。

   - **删除防护策略下的服务器**

     > 注意 防护策略下的服务器被删除后，云安全中心对该服务器的勒索防护将失效，并且云安全中心将删除该服务器已备份的所有数据。备份数据删除后将无法找回，建议您谨慎删除防护策略下的服务器。

     如果您的某台服务器不再需要进行勒索防护，您可以单击该服务器操作列的**删除**并在提示对话框中单击**确定**。如果在同一防护策略下有多台服务器需要删除，您可以选中需要删除的服务器并单击服务器列表下方的**删除**。

   - **安装或卸载防勒索客户端**

     > 注意
     >
     > - 防勒索客户端卸载后，云安全中心将删除该客户端已备份的服务器数据。备份数据删除后将无法找回，建议您谨慎进行卸载客户端操作。
     > - 云安全中心删除该客户端已备份的服务器数据后，会为您释放相应的勒索防护容量。勒索防护容量释放存在12~48小时的延时，建议您等待足够时间后再重新查看勒索防护容量。

     如果您需要安装或卸载某台服务器上的防勒索客户端，您可以单击该服务器操作列的**安装或卸载**。如果在同一防护策略下，您有多台服务器需要安装或卸载防勒索客户端，您可以选中需要安装或卸载防勒索客户端的服务器并单击服务器列表下方的**安装或卸载**。

删除防护策略

> 注意 删除防护策略后，该策略正在执行的备份任务会终止，并且该策略在所有生效服务器上备份的数据会被删除。备份数据删除后将无法找回，建议您谨慎进行删除防护策略操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面定位到需要删除的防护策略并单击操作列的**删除**。
4. 在确认对话框中单击**确定**。

1.5. 创建恢复任务

如果服务器数据已被勒索病毒入侵，您可以创建恢复任务恢复被勒索病毒加密的数据，降低勒索病毒给您带来的损失。本文介绍如何创建恢复任务、查看恢复任务状态、扩充防勒索容量和删除已备份数据等操作。

前提条件

在服务器被勒索病毒感染前，您已为该服务器创建防护策略并且该策略运行正常（可以正常备份服务器数

据）。同时满足以下情况可以创建恢复任务：

- 防护策略下的可恢复版本数不为0。
- 服务器Agent客户端状态为**开启**。

背景信息

云安全中心根据您创建的防护策略备份您的服务器数据。如果您创建防护策略时使用了推荐策略，您可以选择已备份的任一版本恢复当前服务器的数据。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面定位到需要创建恢复任务的防护策略，单击 图标。
4. 定位到需要恢复数据的服务器并单击操作列下的**恢复**。

   创建恢复任务入口

   您也可以单击**可恢复版本数**下的数字，进入**创建恢复任务**页面。

   可恢复版本数
5. 在**创建恢复任务**页面，选择恢复版本、恢复文件，输入恢复目录地址。

   以下是Windows和Linux系统**恢复目录地址**的样例：
   - Windows：*D:\Documents\Restore*
   - Linux：*/home/Restore*

   > **说明** 恢复目录地址是您服务器数据还原的目标文件夹。备份数据存储在云上，创建恢复任务后文件将会恢复至**恢复目录地址**。如果您填写的目录地址不存在，将导致数据恢复任务执行失败。建议您填写正确的目录地址。
6. 单击**确定**。
   恢复任务创建成功后，您将收到**恢复任务创建成功**的提示。

相关操作

- **查看恢复任务状态**

  您可以在**恢复任务**页面查看已创建的恢复任务的执行状态、恢复总文件数、恢复失败文件数等信息。如果恢复任务执行失败，您可以查看恢复任务失败的原因。如果恢复目录地址不存在，导致恢复任务失败，您需要重新创建恢复任务，再次恢复数据。
- **扩充防勒索容量**

  如果可用的防勒索容量不足，会导致您的服务器数据备份失败。为了避免数据备份失败导致您不能恢复服务器的数据，建议您及时升级防勒索容量。您可以在**通用防勒索解决方案**页面查看您的防勒索总容量和已使用容量，需要升级容量时，请单击**升级**并在**变配**页面购买防勒索容量。您也可以通过删除已备份数据来获得更多的可用容量。

  升级防勒索容量

- **删除已备份数据**

  > **说明** 已备份数据删除后将无法恢复，请您谨慎操作。

  如果您确认已备份的数据无需使用，可以删除已备份的数据版本。在**可恢复数据版本**页面，定位到需要删除的数据并单击**删除**。删除备份数据后，将释放相应的防勒索容量。

1.6. 防勒索客户端异常状态排查

如果您已为服务器创建勒索防护策略，但在云安全中心控制台上防勒索客户端处于异常状态（非客户端在线状态），请参考本文排查原因并处理异常。

前提条件

已为您的服务器创建防护策略。更多信息请参见创建防护策略。

背景信息

防勒索客户端状态异常时将无法正常进行数据备份，无法正常保护您的服务器。建议您及时排查防勒索客户端状态异常原因并处理相关异常。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面，查看状态为**异常**的服务器。单击策略名称前的  图标可查看当前策略下的所有服务器信息。

4. 单击异常信息右侧的  图标，查看客户端异常状态原因。

5. 根据**错误详情**对话框中的提示处理客户端异常。客户端异常状态的原因和处理建议请参见客户端状态异常的原因。

客户端状态异常的原因

异常信息	错误详情提示	产生异常原因	解决方案

异常信息	错误详情提示	产生异常原因	解决方案
	云助手未启动	云助手未正常启动，导致防勒索客户端安装失败。	解决云助手未启动问题。操作步骤如下： 1. 登录ECS管理控制台。 2. 查看云助手是否正常启动。详细操作步骤请参见云助手故障排查问题。 ○ 如果云助手未正常启动，请启动云助手客户端。更多信息请参见停止或启动云助手客户端。 ○ 如果云助手已正常启动，请提交工单解决该问题。 3. （可选步骤）云助手正常启动后，重新安装防勒索客户端。详细操作步骤请参见相关操作。
	授权问题	账号权限不足。	使用阿里云账号在**通用防勒索解决方案**页面单击**立即授权**，为当前账号授权AliyunHBRDefaultRole和AliyunECSAccessingHBRRole角色。
	客户端连接异常，请检查ECS实例网络后，再次重试	网络连接失败。	解决网络连接问题。操作步骤如下： 1. 在ECS服务器上使用 `ping` 或 `telnet` 命令检查与防勒索网络接入点的网络是否连通，并检查是否配置了防火墙策略。防勒索网络接入点详情请参见防勒索网络接入点。 2. 网络连接问题解决后，重新安装防勒索客户端。详细操作步骤请参见相关操作。
	ECS_ROLE_POLICY_NOT_EXIST ecs role没有AliyunECSAccessingHBRRolePolicy	ECS对应的RAM角色缺少AliyunECSAccessingHBRRolePolicy策略，导致客户端安装失败。	授予RAM角色AliyunECSAccessingHBRRolePolicy的策略。详细操作步骤请参见客户端安装失败，提示“EcsRamRole上缺少AliyunECSAccessingHBRRolePolicy的策略”错误。
	检查激活命令超时	安装防勒索客户端超时。	重新安装防勒索客户端。操作步骤如下： 1. 在云安全中心控制台**通用防勒索解决方案**页面，卸载防勒索客户端。详细操作步骤请参见相关操作。 卸载完成后客户端状态显示为**未安装**。 2. 重新安装防勒索客户端。详细操作步骤请参见相关操作。

异常信息	错误详情提示	产生异常原因	解决方案
安装失败	ECS停机	ECS处于关机状态。	启动ECS服务器后，再安装防勒索客户端。操作步骤如下： 1. 在ECS管理控制台启动ECS服务器。详细操作步骤请参见启动实例。 2. 重新安装防勒索客户端。详细操作步骤请参见相关操作。
	卸载客户端失败	云助手命令超时。	重新安装防勒索客户端。具体操作步骤如下： 1. 在云安全中心控制台通用防勒索解决方案页面，定位到卸载客户端失败的服务器，单击其操作列下删除。 2. 等待2分钟。 3. 将ECS服务器重新添加到之前的防护策略中。详细操作步骤请参见编辑防护策略。 4. 重新安装防勒索客户端。详细操作步骤请参见相关操作。
	安装失败	云助手命令超时。	重新安装防勒索客户端。操作步骤如下： 1. 在云安全中心控制台通用防勒索解决方案页面，卸载防勒索客户端。详细操作步骤请参见相关操作。 卸载完成后客户端状态显示为未安装。 2. 重新安装防勒索客户端。详细操作步骤请参见相关操作。

异常信息	错误详情提示	产生异常原因	解决方案
	客户端安装后，服务未启动	存在卸载注册表的残留文件，导致新的客户端无法启动。	清理注册表后，重新安装客户端。操作步骤如下： 1. 在云安全中心控制台通用防勒索解决方案页面，卸载防勒索客户端。详细操作步骤请参见相关操作。 卸载完成后客户端状态显示为未安装。 2. 清理以下两项注册表。 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hybridbackup HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrupdater 3. 重新安装防勒索客户端。详细操作步骤请参见相关操作。
	下载安装包失败	网络连接失败。	解决网络连接问题。操作步骤如下： 1. 在ECS服务器上使用 ping 或 telnet 命令检查与防勒索网络接入点的网络是否连通，并检查是否配置了防火墙策略。防勒索网络接入点详情请参见防勒索网络接入点。 2. 网络连接问题解决后，重新安装防勒索客户端。详细操作步骤请参见相关操作。
	预检命令失败	云助手命令超时。	重新安装防勒索客户端。操作步骤如下： 1. 在云安全中心控制台通用防勒索解决方案页面，卸载防勒索客户端。详细操作步骤请参见相关操作。 卸载完成后客户端状态显示为未安装。 2. 重新安装防勒索客户端。详细操作步骤请参见相关操作。

以下表格介绍了各地域的防勒索网络接入点。

地域	公网接入点	ECS内网接入点
华东1（杭州）	https://hbr.cn-hangzhou.aliyuncs.com	https://hbr-vpc.cn-hangzhou.aliyuncs.com
华东2（上海）	https://hbr.cn-shanghai.aliyuncs.com	https://hbr-vpc.cn-shanghai.aliyuncs.com
华北1（青岛）	https://hbr.cn-qingdao.aliyuncs.com	https://hbr-vpc.cn-qingdao.aliyuncs.com
华北2（北京）	https://hbr.cn-beijing.aliyuncs.com	https://hbr-vpc.cn-beijing.aliyuncs.com
华北3（张家口）	https://hbr.cn-zhangjiakou.aliyuncs.com	https://hbr-vpc.cn-zhangjiakou.aliyuncs.com
华北5（呼和浩特）	https://hbr.cn-huhehaote.aliyuncs.com	https://hbr-vpc.cn-huhehaote.aliyuncs.com
华南1（深圳）	https://hbr.cn-shenzhen.aliyuncs.com	https://hbr-vpc.cn-shenzhen.aliyuncs.com
西南1（成都）	https://hbr.cn-chengdu.aliyuncs.com	https://hbr-vpc.cn-chengdu.aliyuncs.com
中国香港	https://hbr.cn-hongkong.aliyuncs.com	https://hbr-vpc.cn-hongkong.aliyuncs.com
新加坡	https://hbr.ap-southeast-1.aliyuncs.com	https://hbr-internal.ap-southeast-1.aliyuncs.com
澳大利亚（悉尼）	https://hbr.ap-southeast-2.aliyuncs.com	https://hbr-vpc.ap-southeast-2.aliyuncs.com
马来西亚（吉隆坡）	https://hbr.ap-southeast-3.aliyuncs.com	https://hbr.ap-southeast-3.aliyuncs.com
印度尼西亚（雅加达）	https://hbr.ap-southeast-5.aliyuncs.com	https://hbr-vpc.ap-southeast-5.aliyuncs.com
日本（东京）	https://hbr.ap-northeast-1.aliyuncs.com	https://hbr.ap-northeast-1.aliyuncs.com
德国（法兰克福）	https://hbr.eu-central-1.aliyuncs.com	https://hbr.eu-central-1.aliyuncs.com
美国（硅谷）	https://hbr.us-west-1.aliyuncs.com	https://hbr.us-west-1.aliyuncs.com
上海金融云	https://hbr.cn-shanghai-finance-1.aliyuncs.com	https://hbr-vpc.cn-shanghai-finance-1.aliyuncs.com

2.病毒防御

2.1. 病毒防御概述

勒索病毒、挖矿程序等持久化、顽固型病毒已经成为网络安全最大的威胁。云安全中心病毒防御功能针对此类病毒提供扫描、告警、深度查杀和数据备份的能力，可有效预防此类病毒入侵您的服务器。

背景信息

病毒防御为基础杀毒版、高级版和企业版增值服务，为您提供病毒查杀和防勒索数据备份服务。基础版用户需要先升级到基础杀毒版、高级版或企业版，才可使用病毒查杀功能。基础杀毒版、高级版或企业版用户购买防勒索容量后才可使用防勒索数据备份功能。

在使用云安全中心病毒防御功能时，建议您同时在**设置**页面开启**病毒拦截**功能。开启**病毒拦截**后，云安全中心会自动检测主流木马病毒、勒索软件、挖矿病毒、DDoS木马并自动隔离查杀。更多信息请参见主动防御和病毒拦截和病毒防御对比。

> **说明** 防勒索数据备份功能支持的操作系统版本有限，不在支持范围内的服务器将无法进行数据备份。支持的操作系统请参见防勒索支持的操作系统。

功能说明

针对勒索病毒，病毒防御提供了通用防勒索解决方案。更多信息请参见勒索病毒防护原理。病毒防御还为您提供以下功能：

- **病毒扫描**

  云安全中心安全专家团队通过对海量病毒样本持久化攻击方式的自动化分析，推出了阿里云机器学习病毒查杀引擎。病毒防御提供的病毒扫描功能使用阿里云机器学习病毒查杀引擎和实时更新的病毒库，可以帮助您及时发现此类危害性较大的病毒。您可以创建病毒扫描任务，查看您的服务器是否已被病毒入侵。更多信息请参见扫描病毒。

- **告警处理**

  病毒防御提供处理病毒查杀告警的能力，支持对勒索、挖矿等顽固性病毒进行一键深度查杀。深度查杀通过查杀恶意病毒进程、隔离恶意文件和清除黑客植入的持久化的方式可以彻底清理此类顽固性病毒。更多信息请参见处理病毒查杀告警。

- **数据备份**

  病毒防御提供防勒索数据备份服务。如果您的服务器被勒索病毒入侵，您可以及时恢复数据，降低勒索病毒给您带来的损失。您可以创建防护策略备份核心服务器的数据。更多信息请参见创建防护策略。需要恢复服务器数据时，您可以创建恢复任务。更多信息请参见创建恢复任务。

  > **说明**
  > - 防勒索功能仅支持备份阿里云ECS服务器数据，不支持备份非阿里云服务器数据。您只能为您的阿里云ECS服务器创建防护策略。
  > - 防勒索备份数据采用增量备份的方式。初次进行数据备份时会全量备份防护目录下的数据，后续再次进行备份时，云安全中心只备份有变化（修改、增加或删除）的文件。

勒索病毒防护原理

勒索病毒对企业或个人用户来说都是危害极大的安全风险，如果企业或个人服务器上的核心数据或文件被加密，除了缴纳赎金，基本上无法解密。防勒索病毒已经给无数企业和个人造成了难以估量的损失。为了帮助企业或个人用户应对勒索病毒，阿里云云安全中心发布了通用防勒索解决方案功能，帮助您实现逐层递进的纵深式防御。

> 说明
>
> - 防勒索数据备份功能现已支持西南1（成都）、华东2金融云（上海）、华北2阿里政务云、华东2（上海）、华东1（杭州）、华北2（北京）、华南1（深圳）、华北3（张家口）、华北5（呼和浩特）、华北1（青岛）、中国香港、新加坡、印度尼西亚（雅加达）、澳大利亚（悉尼）、美国（硅谷）、美国（弗吉尼亚）、德国（法兰克福）、日本（东京）和印度（孟买）地域。
> - 目前，仅支持使用VPC（专有网络）的ECS服务器进行防勒索备份，暂不支持使用经典网络的ECS服务器进行防勒索备份。

通用防勒索解决方案为您提供逐层递进的纵深式防御体系：

- **实时防御已知勒索病毒**

  借助云上全方位的威胁情报，云安全中心实现了对大量已知勒索病毒的实时防御。在服务器被病毒感染的第一时间拦截勒索病毒，避免发生文件被病毒加密而进行勒索的情况。

- **诱捕、拦截新型未知勒索病毒**

  通过放置诱饵的方式，云安全中心实时捕捉可能存在的勒索病毒行为。针对新型未知的勒索病毒，一旦识别到有异常加密行为发生，会立刻拦截病毒，同时通知您进行排查清理。

  > 说明 您可以在**云安全中心控制台**设置页面的**主动防御**区域开启**防勒索（诱饵捕获）**功能。开启该功能后，云安全中心为捕捉勒索病毒会在您的服务器中设置目录陷阱。如果您服务器中出现可疑目录，请您及时联系售后人员或提交**工单**确认该目录是否为云安全中心设置的诱饵目录。诱饵目录不会对您的业务造成影响，也不存在任何的恶意行为，并且不支持手动删除。

- **支持恢复被病毒感染文件**

  在对勒索病毒进行防御的同时，云安全中心还支持文件备份服务，能定期对指定文件进行备份，支持按时间或文件版本恢复服务器数据。在发生极端情况导致文件被加密时，能够通过文件恢复的方式找回数据，确保服务器数据的安全。

防勒索支持的操作系统

系统	支持的版本
Windows	7、8、10
Windows Server	2008 R2、2012、2012 R2、2016、2019
RHEL	7.0、7.2、7.4
CentOS	6.5、6.9、7.2、7.3、7.4、8.2
Ubuntu	14.04、16.04、18.40、20.04
SUSE Linux Enterprise Server	11、12、15

> **说明** 防勒索仅支持在以上表格中的操作系统安装防勒索客户端，不在以上表格中的操作系统将无法安装防勒索客户端并进行数据备份。建议您在使用防勒索功能前，先确认您服务器的操作系统是否在以上支持范围内。

病毒防御建议

使用云安全中心病毒防御功能防护勒索病毒时，您需要进行以下操作：

1. **事前：开通病毒防御功能并创建防护策略**

   病毒防御提供数据备份功能。您需要开通病毒防御功能并创建防护策略才能备份您的核心服务器数据。更多信息请参见开通服务和创建防护策略。

2. **事中：处理勒索病毒告警并创建恢复任务**

   云安全中心为您提供勒索病毒告警功能。如果您收到了勒索病毒告警，建议您及时处理告警并排查告警出现原因。更多信息请参见查看和处理告警事件。如果您的服务器数据已被勒索病毒加密，您可以创建恢复任务来恢复被加密的数据。更多信息请参见创建恢复任务。

3. **事后：排查服务器安全漏洞并进行安全加固**

   为了进一步降低被勒索病毒攻击的风险，建议您同时做好以下三点：

   - 定期修复系统漏洞，避免漏洞被黑客利用。您可以使用云安全中心漏洞修复功能修复系统漏洞。更多信息请参见漏洞修复概述。
   - 服务器中不要使用弱密码，重要的服务器开启双因子认证。
   - 避免不必要的网络端口暴露在互联网，减小病毒的攻击面。

2.2. 扫描病毒

病毒防御功能针对勒索病毒、挖矿程序等顽固性病毒，对云安全中心防护的所有服务器提供深度扫描服务。云安全中心支持立即扫描和周期性扫描病毒。本文介绍如何使用这两种方式扫描病毒。

前提条件

已购买云安全中心基础杀毒版、高级版或企业版。更多信息请参见购买云安全中心。

背景信息

病毒防御功能支持扫描以下类型的病毒：

- 勒索病毒
- 挖矿程序
- DDoS木马
- 木马程序
- 后门程序
- 恶意程序
- 高危程序
- 蠕虫病毒
- 可疑程序
- 自变异木马

立即扫描和周期性扫描支持在以下场景中使用：

- 立即扫描病毒：仅支持扫描指定资产分组下的所有服务器，即您只能选择一个或多个资产分组中的所有服务器执行病毒扫描。
- 周期性扫描：支持扫描指定资产分组下的所有或部分服务器。

立即扫描病毒

如果需要立即扫描您的服务器中是否存在病毒，请参考以下步骤执行立即扫描操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 病毒防御**。
3. 在**病毒防御**页面单击**重新扫描**。如果您是首次进行病毒扫描，单击**开始病毒扫描**。
4. 在**请选择您要扫描的资产**对话框中选择需要扫描的**资产分组**。

   

   在扫描时直接选择需要检测的服务器分组，该分组下的所有服务器将被默认选中，不支持选择单台服务器。您可以同时选择多个分组下的服务器。

   > **说明** 目前仅支持以分组为单位扫描病毒。您可以根据需要添加新的分组，更多信息请参见添加分组。

5. 单击**开始扫描**。扫描完成预计需要2~5分钟，请您耐心等待。扫描完成后，建议您及时查看扫描结果并处理相应告警。更多信息请参见处理病毒查杀告警。

周期性扫描病毒

如果需要周期性扫描您的服务器中是否存在病毒，请参考以下步骤设置病毒扫描周期。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 病毒防御**。
3. 在**病毒防御**页面右上角单击**设置**。
4. 在**防御配置**页面设置扫描病毒的周期和资产。您可以根据以下说明配置病毒扫描的周期和资产：
   - **扫描间隔**：可选择**每隔3天**、**每隔一周**、**每隔两周**或**停止扫描**。
   - **执行时间**：可选择**00:00~24:00**、**00:00~06:00**、**06:00~12:00**、**12:00~18:00**或**18:00~24:00**。
   - **扫描资产**：支持选中单台资产、跨组选中多台资产或者选中资产分组。执行以下操作选择需要执行周期性病毒扫描的资产：
     - 选中**资产分组**区域中的分组，该分组下的所有资产都会被选中。您可在右侧**资产**区域下，对已自动选中的资产取消选中。
     - 在**资产**区域下输入资产名称（支持模糊查询），单击图标搜索相关资产，您可选择需要执行病毒扫描的资产。

   > **说明** 云安全中心会根据您设置的扫描时间间隔，在选择的扫描时间段内的随机时间点开始扫描病毒。

5. 单击**确定**。

> **注意** 如果设置了多个扫描周期，仅最近一次的设置会生效。云安全中心会按照最近一次您选择的扫描周期和资产自动扫描病毒。

2.3. 处理病毒查杀告警

云安全中心病毒防御为您提供深度的病毒扫描、告警和处理功能。本文介绍如何使用病毒防御功能处理告警。

云安全中心 病毒防御 病毒查杀

背景信息

病毒防御为您提供深度查杀持久化、顽固型病毒的功能。病毒防御支持处理以下类型病毒：

- 勒索病毒
- 挖矿程序
- DDoS木马
- 木马程序
- 后门程序
- 恶意程序
- 高危程序
- 蠕虫病毒
- 可疑程序
- 自变异木马

> **说明** 云安全中心扫描出的以上类型告警会对您的服务器产生非常大的安全威胁，建议您及时处理病毒查杀告警。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 病毒防御**。
3. 在**病毒防御**页面单击**立即处理**。
4. 定位到需要处理的告警并单击操作列的**处理**。 如果需要同时处理多个告警，您可以选中需要处理的告警并单击**批量处理**。如果需要同时处理全部告警，您可以单击**一键处理**。
5. 在**告警处理**对话框中，选择处理方式。 下表描述了病毒查杀告警的处理方式。

处理方式	说明

处理方式	说明
深度查杀	选择**深度查杀**处理您服务器中的病毒。 深度查杀是云安全中心安全专家团队对持久化、顽固型病毒进行深度分析和测试后，提供的专项查杀能力。深度查杀采取以下方式处理病毒： ○ **查杀恶意病毒进程** 拦截正在运行的恶意病毒进程，使其无法再次破坏业务运行。 ○ **隔离恶意文件** 隔离病毒文件，防止黑客再次启动病毒文件。同时云安全中心会将病毒文件隔离至文件隔离箱中，方便您下载分析或还原。更多信息请参见文件隔离箱。 ○ **清除黑客植入的持久化方式** 黑客常常利用Crontab、恶意下载源等植入持久化任务，以便不断植入更多的病毒并确保病毒的持久运行。云安全中心针对Crontab、恶意下载源等持久化方式提供专项分析清除能力，同时引入AI智能学习能力，不断提升安全对抗能力，实现小时级的快速响应处置能力。
加白名单	选择**加白名单**将告警加入白名单。告警加入白名单后，云安全中心将不再检测该告警。
忽略	选择**忽略**对当前告警进行忽略。忽略当前告警后，该告警状态将更新为**已忽略**。如果再次出现当前告警事件，云安全中心会正常提供告警。
我已手工处理	如果您已手动处理当前告警，请选择**我已手工处理**。选择**我已手工处理**后，当前告警状态将更新为**已处理**。

6. 单击**立即处理**。

2.4. 病毒拦截和病毒防御对比

本文对比了病毒拦截和病毒防御功能的差异。

功能名称	功能入口	功能原理	功能描述	检测范围	处置能力	扫描方式	扫描周期	支持检测的病毒类型

功能名称	功能入口	功能原理	功能描述	检测范围	处置能力	扫描方式	扫描周期	支持检测的病毒类型
病毒拦截（即病毒查杀）	左侧导航栏**设置** > **设置**	在**病毒程序启动时**进行检测和拦截，达到**防御病毒入侵**的目的。 检测阶段：病毒程序启动时。	开启后，云安全中心会帮助您自动隔离常见网络病毒，并在**安全告警处理**页面为您展示病毒隔离的事件记录；未开启自动隔离时，云安全中心仅会以安全告警的形式向您展示在服务器上检测出的病毒，不为您自动隔离检测出的病毒，需要您在控制台**安全告警处理**页面手动处理病毒告警。	病毒程序	清理病毒样本。	实时自动扫描（前提是已开启病毒拦截开关）	实时	均支持检测以下病毒类型： • 勒索病毒 • 挖矿程序 • DDoS木马 • 木马程序 • 后门程序 • 恶意程序 • 高危程序 • 蠕虫病毒 • 可疑程序 • 自变异木马
病毒防御	左侧导航栏**主动防御** > **病毒防御**	对服务器上正在运行的服务和定时任务进行全面扫描。对**已启动的病毒程序、计划任务、恶意下载源**进行检测，并提供一键清理的能力，实现恶意病毒的彻底清除，防止顽固病毒重新启动进一步扩大破坏范围。 检测阶段：病毒程序启动后。	在**病毒防御**页面，您可以根据业务需求对可能存在病毒入侵的服务器进行不定期的病毒扫描，扫描完成后会在控制台检查结果列表中为您展示扫描出的病毒，需要您手动进行处理。	病毒程序、计划任务和恶意下载源	清理病毒样本、计划任务和恶意下载源，彻底清除病毒。	手动扫描	非实时	

3.网页防篡改

3.1. 概述

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

背景信息

网络攻击者通常会利用被攻击网站中存在的漏洞，通过在网页中植入非法暗链对网页内容进行篡改等方式，进行非法牟利或者恶意商业攻击等活动。网页被恶意篡改会影响用户正常访问网页内容，还可能会导致严重的经济损失、品牌损失甚至是政治风险。

网页防篡改支持将Linux和Windows服务器进程加入白名单，可实现网站防护文件实时更新。

防护原理

云安全中心Agent通过自动化采集获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对导致异常文件变动的进程进行阻断。

您可以在云安全中心控制台**主动防御 > 网页防篡改**页面的告警列表中，查看云安全中心检测出的异常文件变动告警、异常进程和该进程尝试写文件的次数。如果您确定该异常文件相关的进程是正常的业务结果，可以将该进程添加到白名单中。网页防篡改功能不再对加入到白名单中的进程进行拦截。对于新闻、教育类网站需要频繁修改网站内容的场景，可有效避免需要频繁开启和关闭防篡改功能的问题。详细内容请参见加入白名单。

> **说明** 网页防篡改为基础杀毒版、高级版和企业版增值功能，基础版不支持该功能。基础版用户需先升级至基础杀毒版、高级版或企业版，才可开通和使用网页防篡改服务。

网页防篡改支持的系统内核版本

OS	支持的OS版本	支持的内核（Kernel）版本
Windows（32位&64位）	Windows Server 2008、2012、2016和2019	所有版本
CentOS（仅64位）	6.3、6.5、6.6、6.7、6.8、6.9、6.10、7.0、7.1、7.2、7.3、7.4、7.5、7.6、7.7、7.8 **说明** 网页防篡改功能仅支持CentOS 64位服务器，不支持32位服务器。	• 2.6.32-x • 3.10.0-x

OS	支持的OS版本	支持的内核（Kernel）版本
Ubuntu（仅64位）	14.04、16.04、18.04 说明 网页防篡改功能仅支持Ubuntu 64位服务器，不支持32位服务器。	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-151-generic • 4.4.0-117-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic

说明

- 目前，防篡改支持的服务器Kernel版本有限，不在支持范围内的服务器将无法使用防篡改进程白名单功能。请确认您的服务器Kernel版本是否在上述支持列表覆盖范围内。如果不在支持范围内，需要手动升级Kernel到支持列表里的版本，才能使用进程加白名单的功能。
- 升级服务器Kernel前请使用快照备份您的资产数据。

相关文档

开通服务

启用网页防篡改保护

查看防护状态

加入白名单

3.2. 开通服务

使用云安全中心网页防篡改功能前需先开通并购买该功能。本文介绍如何开通并购买网页防篡改功能。

背景信息

网页防篡改功能为云安全中心增值服务，需单独购买，费用为980元/台/月。

说明 云安全中心基础版不支持网页防篡改功能，基础版用户需先升级到基础杀毒版、高级版或企业版，才可开通和使用网页防篡改服务。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**安全运营 > 应用市场**。
3. 在**网页防篡改**区域单击**开通**。

4. 在变配页面，将**网页防篡改**配置为**是**并设置**防篡改授权数**。

   防篡改授权数表示您需要网页防篡改防护的服务器数量。例如，**防篡改授权数**设置为3时，您可以为3台服务器添加防篡改保护。

   > **说明** 网页防篡改授权数有效期与您已开通的云安全中心服务（基础杀毒版、高级版、企业版）有效期时间一致。

5. 单击**立即购买**并完成支付。

3.3. 启用网页防篡改保护

云安全中心基础杀毒版、高级版和企业版支持对服务器开启网页防篡改防护，全面保护您网站的安全。

前提条件

- 基础版用户需升级到基础杀毒版、高级版或企业版，才能购买和使用网页防篡改服务。
- 网页防篡改支持Windows 32位和64位系统、Linux 64位系统，在网页防篡改支持范围内的服务器可防护的目录和文件大小以及数量不受限制，具体支持的系统版本和内核版本请参见网页防篡改支持的系统内核版本。不在网页防篡改支持的系统内核版本范围内的服务器可防护的目录和文件有一定的限制，具体的限制说明请参见限制条件。
- 使用网页防篡改服务前，需确保您当前账号有足够的网页防篡改配额。1个网页防篡改配额可防护1台服务器。已使用的网页防篡改配额也就是开启防篡改防护的服务器数量。您可在云安全中心控制台**网页防篡改**页面右上角，查看您当前的配额数、已消耗的配额数和配额有效期（即云安全中心产品有效期）。如果配额不足，需要购买**防篡改授权数**，更多信息请参见扩充配额。

> **说明** 网页防篡改配额有使用期限的限制，您需要在有效期内使用完授权配额。超过有效期后，该授权配额将自动失效，失效的授权配额不支持退款。

背景信息

- 购买网页防篡改授权配额数后，添加需要防护的服务器及其目录。
- 配置完成防护目录后网页防篡改未立即生效，并且此时仍然可以对该防护目录写入文件。这种情况下，您需在**防护管理**列表中对该目录所在的服务器关闭**防护状态**开关，然后重新打开**防护状态**开关。

> **说明** 如何打开防护状态开关，请参见步骤9开启防护状态。

限制条件

- 每台服务器最多可添加10个防护目录。
- Windows系统和Linux系统防护目录的限制条件相同，以下是具体的限制条件：
  - 单个防护目录大小不超过20 GB。
  - 单个防护目录下的文件夹个数不超过20,000个。
  - 防护目录文件夹层级不超过20个。
  - 单文件大小不超过20 GB。

- 可使用的授权配额为0时，您将无法添加新的防护服务器。如果有无需防护的服务器，可以暂时关闭该服务器的**防护状态**。关闭防护后，将会释放出对应数量的可用授权配额，以便您添加新的服务器。例如：关闭1台服务器的防护状态，将会释放出1个可用授权配额。

> 说明
> - 网页防篡改可防护的目录和文件数量以及大小限制只对不在网页防篡改支持的系统和内核版本范围内的服务器生效，在支持范围内的服务器可防护的目录和文件不受限制。具体支持的系统版本和内核版本请参见网页防篡改支持的系统内核版本。
> - 建议您开启防护前检查文件夹目录层级、文件夹个数和防护目录大小是否超过限制。
> - 建议您排除 *LOG*、*PNG*、*JPG*、*MP4*、*AVI*、*MP3*等无需进行防护的文件类型（多个文件类型之间用分号隔开）。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 网页防篡改**。
3. 在**网页防篡改**页面单击**防护管理**页签。
4. 在**防护管理**页签单击**为服务器添加防护**，将需要保护的服务器添加到网页防篡改防护列表中。

5. 在**创建网页防篡改**对话框中选择目标服务器。

> 说明 可使用的授权配额为0时，您将无法添加新的防护服务器。如果有无需防护的服务器，可以暂时关闭该服务器的**防护状态**。关闭防护后，将会释放出对应数量的可用授权配额，以便您添加新的服务器。例如：关闭1台服务器的防护状态，将会释放出1个可用授权配额。

6. 单击**下一步**，进入**添加防护目录**页签。
7. 在**添加防护目录**页签中，完成以下配置。

选择防护模式。可选**白名单模式**或**黑名单模式**。白名单模式下，会对添加的防护目录和文件类型进行保护；黑名单模式下，会防护目录下所有未排除的子目录、文件类型和指定文件。默认开启白名单模式。

- 白名单模式配置：

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。 说明 Linux服务器和Windows服务器防护目录地址的格式可能会有区别，请根据页面提示输入正确的格式。
防护文件类型	单击下拉列表，选择该目录中需要防护的文件类型，例如：*JS*、*HTML*、*XML*、*JPG*等。

配置项	描述
本地备份目录	展示防护目录的默认备份存储路径。 云安全中心为您指定的默认备份目录为*/usr/local/aegis/bak*（Linux服务器）和*C:\Program Files (x86)\Alibaba\Aegis\bak*（Windows服务器），您可手动修改默认的备份路径。

- **黑名单防护模式：**

配置项	描述
防护目录	手动输入该服务器下需要开启防篡改保护的目录地址。
排除子目录	手动输入无需开启网页防篡改的子目录地址。 单击**添加子目录**，支持添加多个子目录。 添加排除子目录后，云安全中心将不会对该子目录中的文件进行防护。
排除文件类型	选择无需进行网页防篡改检测的文件格式。 可选值包含**log**、**txt**、**ldb**。 选择排除文件类型后，云安全中心将不会对该防护目录下该类型的文件进行防护。
排除指定文件	手动输入无需开启网页防篡改的文件目录地址。 单击**添加文件**，支持添加多个文件。 输入指定文件后，云安全中心将不会对该指定文件进行防护。
本地备份目录	展示防护目录的默认备份存储路径。 云安全中心为您指定的默认备份目录为*/usr/local/aegis/bak*（Linux服务器）和*C:\Program Files (x86)\Alibaba\Aegis\bak*（Windows服务器），您可手动修改默认的备份路径。

8. **单击开启防护，完成添加服务器和目录的操作。**
   添加服务器完成后，该服务器将显示在网页防篡改页面的防护服务器列表中。

   > **说明** 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**页面**开启**目标服务器的防护状态。

9. **在防篡改防护列表中，单击目标服务器防护状态开关，为该服务器开启防护服务。**

   > **说明** 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**列表中开启目标服务器的防护状态。

首次开启防护时，目标主机的服务状态将会显示为**启动中**，并显示启动进度条。请耐心等待数秒，启动成功后服务状态将会显示为**正在运行**。

当防护服务状态为**异常**时，在目标服务器服务状态栏单击**异常**，显示异常状态的详细原因并单击**重试**。详情请参见防护异常状态处理。

后续操作

为服务器开启网页防篡改保护后，您可在**网页防篡改**页面，查看云安全中心为您检测到的网页篡改事件和告警信息。

> **说明**
>
> 配置完成防护目录后网页防篡改未立即生效，并且此时仍然可以对该防护目录写入文件。这种情况下，您需在**防护管理**列表中对该目录所在的服务器关闭**防护状态**开关，然后重新打开**防护状态**开关。

网页防篡改服务状态

服务状态	说明	建议
启动中	网页防篡改防护服务正在开启。	首次开启防护时，目标主机的服务状态将会显示为**启动中**。请耐心等待数秒。
正在运行	防护状态已成功开启，服务正常运行中。	无
异常	防护开启异常。	将鼠标移动到目标服务器的服务状态上，查看发生异常的原因并单击**重试**。
未启动	防护状态为未开启。	需将防护状态设置为**开启**。

3.4. 扩充配额

为每一台服务器开启网页防篡改功能会消耗1个网页防篡改授权数（即网页防篡改配额）。如果您已消耗了所有的网页防篡改配额，您必须先扩充足够的配额，才能为其他服务器开启网页防篡改保护。本文档介绍了如何扩充网页防篡改授权数。

背景信息

您可在网页防篡改页面右上角查看您已购买的授权数、已使用的授权数和有效期。

如果已购买的授权数量已经消耗完毕（即已开启网页防篡改的服务器数量等于已购买的授权数），网页防篡改页面会提示**开启机器数量已达上限**。您需要扩充授权网页防篡改防护的服务器数量。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 网页防篡改**。
3. 在网页防篡改页面右上角单击**购买配额**。 您也可以在网页防篡改页面的**防护状态**统计数据模块中，单击**授权总数**下方的**立即升级**扩充配额。

4. 在**变配**页面**防篡改授权数**区域选择您需要的网页防篡改授权数的总量。

> **注意** 此处您需要选择的**防篡改授权数**是您现有的防篡改授权数和需要新增的授权数相加得到的和。例如，您已购买了5个授权数，需要再扩充2个授权数，此处您需要选择的**防篡改授权数**应为7。云安全中心将按照980元/台/月对扩充的授权数（即这2个授权数）收取相应的费用。扩充的防篡改授权数的到期时间和您之前购买的防篡改授权数的到期时间一致。

5. 单击**立即购买**并完成支付。

后续步骤

扩充配额完成后，您可以为您其他需要保护的服务器开启网页防篡改服务。相关内容请参见启用网页防篡改保护。

3.5. 查看防护状态

网页防篡改功能可实时监控网站目录文件的变化并对异常的文件变动事件进行拦截。您可以在网页防篡改页面查看云安全中心为您检测到的网页防篡改防护状态和详细信息。本文档介绍如何查看您资产的网页防篡改防护状态。

前提条件

您已开通防篡改服务并为服务器启用了网页防篡改保护。更多信息请参见开通服务和启用网页防篡改保护。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 网页防篡改**。
3. 在**防护状态**页签下查看网页防篡改防护的详细信息。您可以查看以下网页防篡改信息：
   - 网页防篡改统计数据

     

     您可以在统计数据总览模块中查看当天以及最近15天内发生变动的文件总数、已被防护的服务器数量和目录数量、已被网页防篡改功能阻断的可疑进程数量、已被加入到白名单中的进程数量、您当前账号下已购买的网页防篡改授权总数。
   - 防篡改防护文件类型分布数据

     防护文件类型包括TXT、PNG、MSI、ZIP等文件类型。您也可以手动添加需要防护的其他文件类型。

     > **说明** 目前防护文件类型不受限制，所有文件类型都支持网页防篡改防护。

   - 文件变动数Top 5

     该模块展示了最近15天内检测到的变动次数排名前5的文件名称和文件所在路径。
   - 阻断进程Top 5

该模块展示了最近15天内检测到的被防篡改服务阻断的排名前5的异常进程名称和数量。

- 网页防篡改告警详情列表

该列表展示了网页防篡改功能为您资产拦截到的所有异常文件变动及其详细信息，包括告警等级、告警名称、受影响资产、异常变动文件的路径、异常进程名称、防御状态等信息。

> 说明
>
> - 如果告警尝试次数（进程写文件次数）超过100次，建议您及时关注并处理该告警。
> - 目前告警等级只有**中危**等级。
> - 防御状态只有**已防御**一种状态，表示网页防篡改功能在检测到异常文件变动事件时，已及时为您拦截执行该异常变动的进程。如果您确认被拦截的异常变动为正常业务需求，可通过白名单功能恢复该进程的正常运行。详细内容请参见加入白名单。

3.6. 加入白名单

网页防篡改功能在检测到异常文件变动时，会实时为您拦截执行该异常变动的进程。本文档介绍了被网页防篡改拦截的进程如何加入到白名单中。

背景信息

支持批量加入白名单功能。

> 说明 进程白名单功能支持Windows服务器和Linux服务器。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**主动防御 > 网页防篡改**。
3. 在**防护状态**页面告警列表中查看或搜索需要加入白名单的异常文件变动事件，并复制该告警事件涉及的异常进程路径和影响的资产名称/IP地址。
4. 使用以下两种方式之一将进程加入到白名单中。

> 警告 黑客有可能利用白名单进程入侵主机，建议您根据业务场景谨慎录入白名单。

- 在防护状态页面告警列表中操作。

  在防护状态页面告警列表中定位到需要加入白名单的进程，单击**操作**栏的**加入白名单**。

  如果您需要对不同服务器中存在的同一个进程进行加白、或者对同一个服务器中不同文件路径下的同一个进程进行加白，请勾选**同时处理存在相同进程的服务器**。

  

  加入白名单后，您可以在防护状态告警列表中查看到该进程，其状态显示为**已加入白名单**。如果后续您需要将该进程从白名单中移除，可以单击该进程**取消白名单**。取消白名单支持批量操作。

  

- 在进程管理列表中操作。

a. 在防护状态统计模块中单击**进程白名单**下面的统计数字，展开**进程管理**列表。

该统计数字表示已加入到白名单的不同服务器中的进程，因此同一个进程可能会存在多条白名单记录。

单击进程白名单统计数字

b. 在**进程管理**页面单击左上方的**录入白名单**。

录入白名单

进程管理页面包含了**阻断进程**列表和**进程白名单**列表。

进程管理

- **阻断进程**列表展示了所有被网页防篡改功能阻断的异常进程。
- **进程白名单**列表展示了所有已被您加入到进程白名单中的进程信息。

c. 在**录入进程白名单**对话框中输入需要加入白名单的进程所在的路径和服务器名称/IP地址，然后单击**确定**。

录入进程白名单

录入进程白名单后，您可以在进程管理列表中查看到该进程，状态显示为 。如果后续您需要将该进程从白名单中移除、在**进程管理**页面中定位到该进程并单击**取消白名单**。

后续步骤

您可以在**进程管理**页面的**进程白名单**列表中查看到所有已加入白名单的进程信息，包括该进程所在的服务器、进程路径、尝试写文件次数等信息。

白名单列表

4.应用白名单

云安全中心支持应用白名单的功能，可防止您服务器上有未经过认证或授权的程序运行，为您提供可信的资产运行环境。

背景信息

云安全中心应用白名单功能支持将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑和恶意程序，防止未经白名单授权的程序运行。可避免您的主机受到不可信或恶意程序的侵害，还能防止不必要的资源浪费、保证您的资源被合理利用。

在创建白名单策略之后，您可以通过在需要重点防御的服务器中应用该白名单策略，云安全中心将检测服务器中是否存在可疑或恶意进程，并对不在白名单中的进程进行告警提示。

> **说明** 不在白名单中的程序启动时会触发安全告警。云安全中心检测到的非白名单程序启动，可能是新启动的正常程序，或是被入侵后植入的恶意程序。如果提示告警的应用为正常程序、常用程序或者您安装的第三方程序，建议您将该程序加入白名单。已加入白名单的程序再次启动时将不再触发告警；如果该进程为恶意程序，建议您及时清理该进程，并查看计划任务等配置文件是否被篡改。

试用说明

目前应用白名单功能处于邀测阶段，您可通过云安全中心控制台**安全运营 > 应用市场**提交开通试用的申请。

步骤一：配置应用白名单策略

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 应用白名单**。
3. 在**应用白名单**页面单击**策略管理**页签。
4. 在**策略管理**页面单击**创建策略**。
5. 在**创建白名单策略**页面完成以下配置：
   - **策略名称**：自定义白名单策略的名称。
   - **智能学习时长**：选择策略的智能学习时长，可选1天、3天、7天或15天。智能学习功能通过机器学习引擎实现自动化聚类和搜集大量告警数据，帮助提升对可疑或恶意进程的识别能力。
   - **智能学习服务器**：勾选需要加入到该白名单的服务器。
6. 单击**下一步**完成白名单策略的创建。
   白名单策略创建完成后，该策略的详情将会自动展示在策略列表中。

   以下表格介绍白名单策略列表的参数。

参数	描述
策略名称	创建的白名单策略的名称。
生效服务器	应用该白名单策略的服务器数量。

参数	描述
状态	策略的生效状态。包含以下状态： ○ **策略已生效**：该策略已完成智能学习，并且已应用到服务器中。 ○ **智能学习完成，待确认**：该策略已完成智能学习，需确认并启用策略。 智能学习完成后，您还需单击该策略**策略状态**下的开启按钮启用该策略。启用策略后，策略才能生效，云安全中心会自动识别您服务器中进程的风险类型（可信、可疑和恶意）。 ○ **暂停**：智能学习被手动暂停。您可单击**继续**恢复智能学习功能。 ○ **学习中**：智能学习进行中。 策略创建完成后，云安全中心会对其自动执行智能学习。新创建的策略状态都为**学习中**。
应用	表示应用该策略的服务器中各类进程的分布情况，包含**可信**、**可疑**和**恶意**类型进程的数量。
操作	可对该策略执行的操作。支持进行以下操作： ○ **应用**：单击**应用**打开**应用白名单策略**页面，可增加或删除应用该策略白名单的服务器。 ○ **编辑**：单击**编辑**打开**编辑策略白名单**页面，对该策略进行修改。可修改该策略的**策略名称**、**智能学习时长**和需自动执行智能学习的服务器。 ○ **暂停学习**：暂停智能学习。 ○ **继续**：继续执行智能学习。 单击**继续**，该策略的状态会转为**学习中**，您可在**状态**栏查看策略的学习进度。 ○ **删除**：删除策略。 策略删除后，对应的服务器进程将不再受到该策略的保护。

步骤二：将服务器添加到应用白名单

将白名单策略应用到服务器之前，您需已购买足够的应用白名单授权份额。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 应用白名单**。
3. 在**生效服务器**页签单击**添加服务器**。
4. 在**添加服务器**页面完成相应配置。

   添加服务器

   在**添加服务器**页面您可以参考以下内容完成参数配置：

   - **白名单策略**：从策略列表中选择已创建的白名单策略。
   - **异常处理模式**：默认为**告警**，表示云安全中心检测到了可疑进程。

     不在白名单内的服务器进程启动时会自动触发告警。您可单击**异常行为数**一栏的告警数量，跳转到该服务器**资产管理 > 安全处理告警**页面，查看这些告警的详细信息。
   - **生效服务器**：勾选需要添加到该白名单的服务器。 支持选择多台服务器。

您可通过在**生效服务器**搜索框输入服务器名称，搜索需要添加到白名单的服务器。**生效服务器**名称支持模糊查询。

5. 单击**确认**完成服务器的添加。
   应用白名单创建完成后，您可以在**生效服务器**页面的服务器列表中，查看您已添加到应用白名单的服务器和该服务器使用的白名单策略名称。

   生效服务器列表

   生效服务器页面展示应用了白名单策略的服务器的以下信息：

   - **服务器/IP**：应用了白名单策略的服务器名称和IP地址。
   - **白名单策略**：该服务器应用的白名单。
   - **异常行为数**：不在白名单策略中，并且已启动的进程数量。异常进程启动时，会触发云安全中心的检测机制，并进行实时告警。
   - **异常处理模式**：默认为**告警**，表示云安全中心检测到了可疑进程。

     不在白名单内的服务器进程启动时会自动触发告警。您可单击**异常行为数**一栏的告警数量，跳转到该服务器**资产管理 > 安全处理告警**页面，查看这些告警的详细信息。
   - **操作**：单击**操作**栏的**删除**会将该服务器从应用白名单中删除。

     删除后，白名单策略会对该服务器失效，服务器进程启动时云安全中心将会对其进行告警提示。

将进程加入或取消白名单

服务器配置了应用白名单后，您可以在**生效服务器**页面的服务器列表中，查看您已添加到应用白名单的服务器和该服务器使用的白名单策略名称。您可在**白名单策略**栏中单击对应的策略名称，打开该服务器的白名单进程列表，查看服务器中检测到的可信、可疑和恶意进程及其详细信息。

白名单策略列表中包含服务器进程的以下信息：

- **类型**：该白名单服务器中运行的进程类型，分为可信、可疑和恶意3种类型。
- **进程名称**：该白名单服务器中的进程。
- **Hash**：进程的哈希函数。哈希函数用于判断进程的唯一性，避免程序被恶意伪造。
- **路径**：进程在服务器中的文件路径。
- **可信程度**：云安全中心判断该进程的可信任程度，分为0%（恶意进程）、60%（可疑进程）、100%（可信进程）。

  > **说明** 建议您对可信程度为0%的恶意进程进行重点排查和处理。

- **操作**：对该进程可执行的操作。您可结合服务器上业务的部署情况确定是否要将该进程加入白名单。 您可以进行以下操作：
  - **加入白名单**：将进程加入白名单表示信任该进程。
  - **取消白名单**：将进程从白名单中取消表示云安全中心将该进程标识为不可信进程，该进程启动后将触发告警。

5.常见问题

本文汇总了云安全中心病毒防御、网页防篡改和应用白名单功能的常见问题。

- **病毒防御问题**
  - 怎么购买防勒索容量？
  - 病毒防御是什么功能？为什么要单独付费？
  - 购买病毒防御后，之前购买的其他服务是否受影响？
  - 病毒防御和阿里云混合云备份服务有什么关系？
  - 怎么使用云安全中心病毒防御功能？
  - 购买防勒索数据保护容量后数据备份会自动启动吗？
  - 防勒索客户端占用服务器CPU或内存资源过多怎么办？
  - 防勒索解决方案和快照备份的区别？
  - 已购买的防勒索数据保护容量不够用怎么办？
  - 防护策略为异常状态怎么办？
- **网页防篡改问题**
  - 云安全中心还有接近三年的有效期，能只购买一年的网页防篡改吗？
  - 网页防篡改支持防护任意大小的文件吗？
  - 如果我服务器里有超过3 MB的文件，网页防篡改是否无法防护超过3 MB的文件？其他不超过3 MB的文件是否都能正常防护？
  - 网页防篡改启动时为什么会显示异常并报错30006？
  - 网页防篡改本地备份目录有什么要求？
  - 配置防篡改目录提示路径错误
  - 为什么配置了防护目录后防篡改还是失效？
  - 配置了防护目录后还可以对该防护目录写入文件吗？
  - 配置了防护目录后防篡改未立即生效该怎么办？
  - 配置防篡改后无法修改和更新网站的内容和图片该怎么办？
  - 收到短信或邮件提示存在网站后门该怎么办？

怎么购买防勒索容量？

云安全中心基础版用户，可以在云安全中心购买页购买云安全中心基础杀毒版、高级版或企业版的同时购买防勒索容量。详细信息请参见购买云安全中心。

基础杀毒版、高级版或企业版用户可以通过升级功能来购买防勒索容量，详细信息请参见升级与降配。防勒索容量购买成功并完成云资源使用授权后，云安全中心自动为您开启防勒索功能。

病毒防御是什么功能？为什么要单独付费？

病毒防御是云安全中心新发布的功能，目前包含通用防勒索解决方案。防勒索病毒进行数据备份使用的存储容量需要单独付费。

基础杀毒版、高级版或企业版用户可以通过升级功能来购买防勒索容量，详细信息请参见升级与降配。防勒索容量购买成功并完成云资源使用授权后，云安全中心自动为您开启防勒索功能。

通用防勒索解决方案支持防御所有未知勒索病毒，支持一键恢复被勒索病毒加密的文件。通用防勒索解决方案支持一键开启服务器关键目录及文件的备份保护，推荐您为每台服务器配置40 GB的防勒索保护空间，每台服务器仅需12元/月。

购买病毒防御后，之前购买的其他服务是否受影响？

不受影响。

病毒防御是云安全中心新发布的功能，目前包含通用防勒索解决方案。防勒索病毒进行数据备份使用的存储容量需要单独付费。

病毒防御和阿里云混合云备份服务有什么关系？

云安全中心病毒防御功能使用阿里云混合云备份（HBR）服务提供的存储能力。如果您以前未开通过混合云备份服务，在您购买了病毒防御服务并完成云产品授权后，会启用混合云备份服务。启用混合云备份服务不会收取您额外的费用。

怎么使用云安全中心病毒防御功能？

勒索病毒对企业或个人用户来说都是危害极大的安全风险，如果企业或个人服务器上的核心数据或文件被加密，除了缴纳赎金，基本上无法解密。防勒索病毒已经给无数企业和个人造成了难以估量的损失。为了帮助企业或个人用户应对勒索病毒，阿里云云安全中心发布了通用防勒索解决方案功能，帮助您实现逐层递进的纵深式防御。

针对勒索病毒云安全中心提供以下功能：

- **实时防御已知勒索病毒**

  借助云上全方位的威胁情报，云安全中心实现了对大量已知勒索病毒的实时防御。在服务器被病毒感染的第一时间拦截勒索病毒，避免发生文件被病毒加密而进行勒索的情况。

- **诱捕、拦截新型未知勒索病毒**

  通过放置诱饵的方式，云安全中心实时捕捉可能存在的勒索病毒行为。针对新型未知的勒索病毒，一旦识别到有异常加密行为发生，会立刻拦截病毒，同时通知您进行排查清理。

  > **说明** 您可以在云安全中心控制台设置页面的**主动防御**区域开启**防勒索（诱饵捕获）**功能。开启该功能后，云安全中心为捕捉勒索病毒会在您的服务器中设置目录陷阱。如果您服务器中出现可疑目录，请您及时联系售后人员或提交工单确认该目录是否为云安全中心设置的诱饵目录。诱饵目录不会对您的业务造成影响，也不存在任何的恶意行为，并且不支持手动删除。

- **支持恢复被病毒感染文件**

  在对勒索病毒进行防御的同时，云安全中心还支持文件备份服务，能定期对指定文件进行备份，支持按时间或文件版本恢复服务器数据。在发生极端情况导致文件被加密时，能够通过文件恢复的方式找回数据，确保服务器数据的安全。

使用云安全中心病毒防御功能防护勒索病毒时，您需要进行以下操作：

1. **事前：开通病毒防御功能并创建防护策略**

   病毒防御提供数据备份功能。您需要开通病毒防御功能并创建防护策略才能备份您的核心服务器数据。更多信息请参见开通服务和创建防护策略。

2. **事中：处理勒索病毒告警并创建恢复任务**

云安全中心为您提供勒索病毒告警功能。如果您收到了勒索病毒告警，建议您及时处理告警并排查告警出现原因。更多信息请参见查看和处理告警事件。如果您的服务器数据已被勒索病毒加密，您可以创建恢复任务来恢复被加密的数据。更多信息请参见创建恢复任务。

3. **事后：排查服务器安全漏洞并进行安全加固**

   为了进一步降低被勒索病毒攻击的风险，建议您同时做好以下三点：

   - 定期修复系统漏洞，避免漏洞被黑客利用。您可以使用云安全中心漏洞修复功能修复系统漏洞。更多信息请参见漏洞修复概述。
   - 服务器中不要使用弱密码，重要的服务器开启双因子认证。
   - 避免不必要的网络端口暴露在互联网，减小病毒的攻击面。

购买防勒索数据保护容量后数据备份会自动启动吗？

不会。

购买防勒索数据保护容量后，您需要先创建并开启防护策略。您开启了防护策略后，云安全中心才会启动数据备份，实现防勒索保护。如何创建防护策略请参见创建防护策略。

防勒索客户端占用服务器CPU或内存资源过多怎么办？

由于防勒索客户端历史版本的原因，防勒索客户端在备份数据时可能会占用较多的服务器CPU或内存资源。2020年8月19日云安全中心已通过升级防勒索客户端版本修复了该问题。如果您在2020年8月19日之后安装的防勒索客户端，您无需进行任何操作。如果您是在2020年8月19日（包括该日期）之前安装的防勒索客户端，您需要先卸载并重新安装防勒索客户端。详细操作如下：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**主动防御 > 防勒索**。
3. 定位到需修复该问题的服务器，单击其操作列下的**卸载**并在确认提示框中单击**确定**。

   执行卸载操作后，该服务器的防勒索客户端状态将变更为**客户端卸载中**。卸载完成大约需要5分钟，请您耐心等待。

4. 卸载完成后，单击该服务器操作列下的**安装**并在确认提示框中单击**确定**。

   执行安装操作后，该服务器的防勒索客户端状态将变更为**安装中**。完成安装大约需要5分钟，请您耐心等待。

> **说明** 如果您执行了以上步骤，防勒索客户端占用服务器CPU或内存资源过多的问题没有解决，建议您提交工单联系阿里云安全工程师协助您处理该问题。

防勒索解决方案和快照备份的区别？

以下表格介绍了快照备份和防勒索解决方案的区别。

功能	数据备份	病毒防御能力	费用
快照	对整个系统盘进行一次性备份，恢复数据时需要重启系统。	无病毒防御能力。	费用较高。详细信息请参见快照计费。

功能	数据备份	病毒防御能力	费用
防勒索解决方案	支持文件级别的多版本、灵活备份，可恢复已备份的任意版本。恢复数据时无需要重启系统。	支持已知勒索病毒的实时拦截和告警，对未知勒索病毒进行诱捕，可一键恢复被勒索病毒加密的数据。	费用较低。详细信息请参见计费模式。

已购买的防勒索数据保护容量不够用怎么办？

已购买的防勒索数据保护容量不够用时，可能会导致服务器数据备份失败。建议您及时使用云安全中心升级功能，购买足够的防勒索保护容量。详细操作步骤请参见升级与降配。

防护策略为异常状态怎么办？

防护策略为异常状态时，防护策略不能正常备份服务器数据。建议您及时在**防勒索通用解决方案**页面排查防护策略异常原因，按照界面提示处理异常情况。以下是防护策略状态异常的可能原因和解决方案：

- **防勒索容量不足**

  备份服务器数据时如果已使用容量超过了总容量，正在进行的备份任务会暂停，也无法创建新的恢复任务。您需要购买足够的防勒索容量，才能继续使用防勒索功能。更多信息请参见升级与降配。

- **服务器Agent离线**

  服务器Agent离线也会造成防护策略为异常状态，您需要排查Agent离线状态的原因并处理Agent离线状态。更多信息请参见Agent离线排查。

- **数据备份异常**

  恢复任务备份路径错误或服务器磁盘空间不足将导致恢复任务执行失败，也会造成防护策略为异常状态。您需要重新创建恢复任务，填写正确的备份路径并确保服务器磁盘空间充足。新创建的恢复任务执行成功后，防护策略状态才会变为**正常**。

云安全中心还有接近三年的有效期，能只购买一年的网页防篡改吗？

不能，网页防篡改服务的有效期需要和云安全中心服务的有效期保持一致。

网页防篡改支持防护任意大小的文件吗？

目前，网页防篡改支持防护已开启防篡改保护的服务器上任意大小的文件。

如果我服务器里有超过3 MB的文件，网页防篡改是否无法防护超过3 MB的文件？其他不超过3 MB的文件是否都能正常防护？

目前，网页防篡改支持防护已开启防篡改保护的服务器上任意大小的文件。无论您服务器上文件大小是否超过3 MB，都能正常防护。

网页防篡改启动时为什么会显示异常并报错30006？

网页防篡改启动时显示异常并报错30006表示云安全中心防篡改程序被您服务器中的第三方安全软件（例如安全狗、云锁等）拦截了。建议您在服务器的安全软件中将云安全中心Agent进程加入白名单，或者关闭安全软件中驱动服务创建的拦截功能。

网页防篡改本地备份目录有什么要求？

网页防篡改本地备份目录是指将您网站文件进行备份时存放备份文件的目录，可以是空目录。如果需要防护同一个服务器的多个目录，分开的备份地址和同一个备份地址都可以使用。

配置防篡改目录提示路径错误

配置Windows防护目录时不可以使用正斜线（/），需要使用反斜线（\）。

> **说明** 防护目录路径中不可以输入以下字符：
>
> /;*?""<>|

为什么配置了防护目录后防篡改还是失效？

配置了防护目录后，您还需要开启防护状态开关，并且确保客户端在正常的状态下，防篡改防护才会生效。

建议您排查以下三点：

- 防护目录配置完成后，是否开启了防护状态开关。您需要为该防护目录开启防护状态开关，防篡改防护才会生效。
- 防护目录配置完成并且也开启了防护状态，客户端是否存在异常情况。您可以在云安全中心控制台**主动防御 > 网页防篡改**的**防护管理**页签下查看目标服务器的服务状态，如果服务状态显示为异常，建议您为该服务器重新安全Agent。更多信息请参见安装Agent。
- 该服务器的磁盘空间是否足够。如果不够，请及时清理磁盘。

配置了防护目录后还可以对该防护目录写入文件吗？

不可以。完成网页防篡改服务的防护目录配置后，无法再对该防护目录写入文件。如果后续您需要再对该防护目录写入文件，您需要先将该目录从防篡改服务器中删除。

配置了防护目录后防篡改未立即生效该怎么办？

配置完成防护目录后网页防篡改未立即生效，并且此时仍然可以对该防护目录写入文件。这种情况下，您需在**防护管理**列表中对该目录所在的服务器关闭**防护状态**开关，然后重新打开**防护状态**开关。

配置防篡改后无法修改和更新网站的内容和图片该怎么办？

您可选择以下解决方案中的任意一种：

- 先关闭防篡改功能，关闭后再更新网站内容。待更新完成后再开启防篡改防护。开启防篡改防护的操作指导请参见启用网页防篡改保护。
- 将需要修改的网站路径排除在防篡改目录外。

> **说明** 网页防篡改支持Linux和Windows服务器进程加入白名单，实现网站防护文件实时更新。

收到短信或邮件提示存在网站后门该怎么办？

当您收到邮件或是短信提示您的服务器存在网站后门，说明您的服务器已经被黑客入侵，并上传了后门文件。此时，黑客可以操作您的网站或数据库的数据。您可以通过云安全中心对该后门文件进行隔离，但具体的入侵原因还需要进一步排查，否则黑客还是会通过该漏洞进行入侵。

如需排查具体漏洞，您可以通过购买安全管家服务进一步咨询。