ALIBABA CLOUD

Alibaba Cloud

云安全中心（态势感知）

主动防御

文档版本：20220711

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

目前，勒索病毒已成为网络安全最大的威胁之一。云安全中心针对勒索病毒，提供了通用的防勒索解决方案，该方案包括服务器防勒索和数据库防勒索两大功能，帮您解决服务器、数据库被勒索病毒入侵的后顾之忧。

版本限制

仅云安全中心的防病毒版、高级版、企业版、旗舰版支持该功能，免费版不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

背景信息

防勒索为云安全中心提供的增值服务，防病毒版、高级版、企业版或旗舰版用户购买防勒索容量后才可使用防勒索数据备份功能。免费版用户需要先升级到防病毒版、高级版、企业版或旗舰版，或选择仅采购增值服务并购买防勒索容量后，才可使用防勒索功能。

支持的地域

为服务器配置勒索防护策略时，如果待防护的服务器是非阿里云服务器，您需要选择该服务器所在的地域。如果阿里云ECS服务器不在服务器防勒索支持的地域，则该服务器不会出现在可选择的资产列表当中。

服务器防勒索支持的地域如下：

地域	城市	地域ID
华东 1	杭州	cn-hangzhou
华东2	上海	cn-shanghai
华东2金融云	上海	cn-shanghai-finance-1
深圳金融云	深圳	cn-shenzhen-finance-1
华北1	青岛	cn-qingdao
华北2阿里政务云1	北京	cn-north-2-gov-1
华北2	北京	cn-beijing
华北3	张家口	cn-zhangjiakou
华北5	呼和浩特	cn-huhehaote
西南1	成都	cn-chengdu
华南1	深圳	cn-shenzhen
中国香港	香港	cn-hongkong
印度尼西亚	雅加达	ap-southeast-5
澳大利亚	悉尼	ap-southeast-2

地域	城市	地域ID
美国	硅谷	us-west-1
美国	弗吉尼亚	us-east-1
德国	法兰克福	eu-central-1
日本	东京	ap-northeast-1
印度	孟买	ap-south-1
阿联酋	迪拜	me-east-1

数据库防勒索支持的地域如下：

地域	城市	地域ID
华东 1	杭州	cn-hangzhou
华东2	上海	cn-shanghai
华北2	北京	cn-beijing
华北3	张家口	cn-zhangjiakou
华北5	呼和浩特	cn-huhehaote
西南1	成都	cn-chengdu
华南1	深圳	cn-shenzhen
中国香港	香港	cn-hongkong

限制条件

服务器防勒索功能使用时有以下限制：

- 仅支持防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买了勒索防护容量的用户创建勒索防护策略，免费版用户需要升级到防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买勒索防护容量，才能创建勒索防护策略。
- 您服务器的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。服务器防勒索功能支持的操作系统详情，请参见服务器防勒索支持的操作系统版本。

数据库防勒索功能使用时有以下限制：

- 仅支持防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买了勒索防护容量的用户创建勒索防护策略，免费版用户需要升级到防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买勒索防护容量，才能创建勒索防护策略。
- 您数据库的版本及服务器操作系统版本在支持范围内，不在支持范围内的数据库将无法进行数据备份。数据库防勒索功能支持的数据库版本及操作系统版本详情，请参见数据库防勒索支持的数据库版本和操作系统版本。

勒索病毒防护原理

服务器防勒索支持的操作系统版本

注意 服务器防勒索仅支持在以下表格中的操作系统安装防勒索客户端，不在以下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。

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、7.5、7.6、7.7、7.8、8、8.1、8.2
CentOS	6.5、6.9、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9、8.2、8.3
Ubuntu	14.04、16.04、18.40、20.04
SUSE Linux Enterprise Server	11、12、15

数据库防勒索支持的数据库版本和操作系统版本

注意 数据库防勒索仅支持在以下表格中的数据库以及操作系统安装防勒索客户端，不在以下表格中的数据库及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版本、数据库版本是否在以下支持范围内。

数据库类型	支持的数据库的版本	支持的操作系统的版本
Oracle	9i	SUSE 9.3、RHEL 4、RHEL 5、SLES 9、CentOS 4.5
	10g	RHEL 9、RHEL 4、RHEL 5、CentOS 4.6、SUSE 11 SP4、RHEL 6.5
	11g	RHEL 5、RHEL 6、CentOs 6.4、RHEL 6.5、CentOS 6.5、Oracle Enterprise Linux6.7、RHEL 7、Windows 2008 R2、Windows 2012 R2、RHEL 6.0
	12c	Windows 2008 R2、RHEL 6.5、RHEL 6.5、RHEL 7.5
	18c	RHEL 7.0、Windows 2008 R2
	19c	Oracle Enterprise Linux7.0
Oracle RAC	9i	SUSE 9.3、RHEL
	10g	RHEL 5、Windows 2008 R2
	11g	Windows 2008 R2、RHEL 5、Oracle Linux 6.4、RHEL 6.5、iSoft Server 3.0

数据库类型	支持的数据库的版本	支持的操作系统的版本
	12c	CentOS 6、RHEL 6.5、Windows 2008 R2、CentOS 6.7、Oracle Enterprise Linux6
	18c	Windows 2008 R2
	19c	RHEL 7.6
Oracle Data Guard	11g	CentOS 6.4、CentOS 6.5、RHEL 6、Windows 2008 R2
	12c	Oracle Enterprise Linux6
MySQL	5.0	RHEL 5.0、RHEL 6.0 、RHEL 6.5 、Ubuntu 12.10、SLES 10、SUSE 11 SP4、Ubuntu 11.10、Neokylin 6.0
	5.1	RHEL 6.5、SUSE 11 SP4、RHEL 6.5、RHEL 6.0
	5.4	RHEL 6.5、SUSE 11 SP4
	5.5	Ubuntu 12.04、Ubuntu 14.04、Debian 7.8、Debian 8.3 、CentOS 6.0、RHEL 6.5
	5.6	RHEL 5.0、RHEL 6.0、RHEL 6.5、Ubuntu 14.04 、CentOS 6.0、CentOS 7.2
	5.7	RHEL 6.0、RHEL 7.0 、CentOS 7.0、RHEL 6.5、Ubuntu 16.04、CentOS 7.2、RHEL 7.0、Neokylin 7.0
	8.0	CentOS 6.7、RHEL 6.5、CentOS 7.0
SQL Server	2005	Windows 2008 R2 SP1
	2008	Windows 2008 R2、Windows 2008 R2 SP1
	2008 R2	Windows 2008 R2
	2012	Windows 2012 RC
	2014	Windows 2008 R2 SP1、Windows 2016
	2016（RTM）	Windows 2012 R2
	2017	Windows 2012、Windows 2016
	2019	Windows 2016
SQL Server Always On	2012、2016、2017	Windows 2012 R2

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。本文介绍如何开通防勒索功能。

版本限制说明

仅云安全中心的防病毒版、高级版、企业版、旗舰版支持该功能，免费版不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

开通服务

1. 登录云安全中心控制台，在左侧导航栏，选择**主动防御 > 防勒索**。
2. 在**防勒索**页面，单击**立即授权**。

查看及购买防勒索容量

防勒索容量不足，会导致防勒索策略自动关闭，备份任务无法正常进行。在创建勒索防护策略前，请确认已购买足够的防勒索容量。查看及购买防勒索容量的具体操作如下。

> **说明** 建议每台服务器配置50 GB的防勒索容量。

1. 登录云安全中心控制台，在左侧导航栏，选择**主动防御 > 防勒索**。
2. 在**防勒索**页面的**已使用容量/总容量**区域查看或购买防勒索容量。
   - 查看防勒索容量
     已使用容量/总容量区域展示了您已购买和使用的防勒容量。
   - 购买防勒索容量
     单击**升级**，在**升级**页面按需购买防勒索容量并完成支付。

1.3. 服务器防勒索

1.3.1. 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

无论您的服务器是阿里云服务器或非阿里云服务器、服务器使用的是专有网络或者经典网络，您都可以使用云安全中心的服务器防勒索功能为您的服务器创建防护策略。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。
防勒索数据备份通过在您的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，请参见查看防勒索客户端状态。

支持的地域

服务器防勒索支持的地域如下：

地域	城市	地域ID
华东 1	杭州	cn-hangzhou

地域	城市	地域ID
华东2	上海	cn-shanghai
华东2金融云	上海	cn-shanghai-finance-1
深圳金融云	深圳	cn-shenzhen-finance-1
华北1	青岛	cn-qingdao
华北2阿里政务云1	北京	cn-north-2-gov-1
华北2	北京	cn-beijing
华北3	张家口	cn-zhangjiakou
华北5	呼和浩特	cn-huhehaote
西南1	成都	cn-chengdu
华南1	深圳	cn-shenzhen
中国香港	香港	cn-hongkong
印度尼西亚	雅加达	ap-southeast-5
澳大利亚	悉尼	ap-southeast-2
美国	硅谷	us-west-1
美国	弗吉尼亚	us-east-1
德国	法兰克福	eu-central-1
日本	东京	ap-northeast-1
印度	孟买	ap-south-1
阿联酋	迪拜	me-east-1

限制条件

服务器防勒索功能使用时有以下限制：

- 仅支持防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买了勒索防护容量的用户创建勒索防护策略，免费版用户需要升级到防病毒版、高级版、企业版、旗舰版或仅采购增值服务并购买勒索防护容量，才能创建勒索防护策略。
- 您服务器的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。服务器防勒索功能支持的操作系统详情，请参见服务器防勒索支持的操作系统版本。

客户端版本说明

云安全中心防勒索客户端已升级为V2.0及以上版本。目前在客户端版本为V1.X.X时，创建的1.0版本的勒索防护策略已不支持编辑。当前服务器防勒索功能仅支持基于客户端V2.X.X版本，创建2.0版本的勒索防护策略。

勒索防护策略1.0版本与2.0版本的差异如下：

差异项	1.0版本	2.0版本
自定义排除目录	不支持	支持
VSS		
经典网络		
兼容混合云备份HBR使用		
备份方式	多个备份任务同时进行备份（易导致CPU高）	多个备份任务依次进行备份

防护策略一键升级

1.0版本的勒索防护策略支持一键升级至2.0版本的勒索防护策略，您可在防护策略列表中单击**操作**列的**升级**进行一键升级。勒索防护策略升级的同时，该策略生效的服务器上的防勒索客户端也会同步被替换为客户端V2.X.X版本。

> **说明**
>
> - 客户端版本升级是对客户端进行更换，不影响已备份数据，更换后备份任务正常进行。如果客户端升级失败会自动回退为客户端V1.X.X版本，不影响数据备份。
> - 可能存在部分服务器上的客户端无法一键升级的情况。如果客户端无法升级，建议将客户端升级失败的服务器从策略中删除，然后再次单击防护策略**操作**列的**升级**，将防护策略升级至2.0版本。防护策略升级成功后，再将删除的服务器重新添加回该策略，服务器上会自动安装客户端V2.X.X版本。

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，在为您降低服务器资源消耗的同时，避免了消耗过多的防勒索容量。
- 根据您防护策略的版本及备份目录的不同，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：

备份目录	1.0版本的策略	2.0版本的策略

备份目录	1.0版本的策略	2.0版本的策略
备份全部目录	○ Linux系统：整个服务器生成一个数据备份任务。 ○ Windows系统：每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。	整个服务器生成一个数据备份任务。多个数据备份任务依次进行，占用的CPU和内存资源较少，不会对您的业务产生影响。
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。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。 **注意** 建议您根据实际情况，设置合理数量的备份目录。	

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**。以下是在防勒索客户端V2.X.X版本上创建防护策略的操作步骤。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**服务器防勒索**页签。
4. 在**服务器防勒索**页签下，单击**创建防护策略**。
5. 在**创建防护策略**面板，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。

配置项	说明
策略名称	设置防护策略的名称。
是否为阿里云服务器	选择防护策略生效的服务器是否为阿里云服务器。

配置项	说明
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** ○ 选择资产时，阿里云服务器支持单个策略内配置多个地域的服务器，非阿里云服务器仅支持单个策略中配置同一地域的服务器。 ○ 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条防护策略中。
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） ■ **是否排除系统目录**：排除 ■ **排除指定目录**：显示排除目录的列表 ■ **防护文件类型**：全部文件类型 ■ **数据备份开始时间**：00:00~03:00的任意时刻 ■ **备份策略执行间隔**：1天 ■ **备份数据保留时间**：7天 ■ **备份网络带宽限制**：0 MByte/s **说明** 0 MByte/s代表不限制备份网络带宽。 ■ **VSS（Windows）**：是 **说明** 该功能仅为Windows系统开启，开启后会有效降低因进程占用导致的个别文件备份失败的问题，建议开启。启用VSS后，将不支持exFAT和FAT32磁盘格式的文件备份。 ○ **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（MByte/s）等参数。

配置项	说明
防护目录	选择需要进行备份的目录，支持选择以下类型： ○ **指定目录**：即备份已选中资产的指定目录。您需要在**防护目录地址**文本框中输入需要备份的目录地址。防护目录地址最多可添加20条。 ○ **全部目录**：即备份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**不排除**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**不排除**。
是否排除系统目录	选择备份或不备份的系统目录。当您**排除**下方的**排除指定目录**时，右侧文本框中会显示云安全中心默认支持不备份的所有系统目录，您可根据自己的业务需求进行删减。 **说明** Windows系统和Linux系统默认支持不备份的系统目录在持续更新中，具体以控制台**排除指定目录**右侧文本框中显示的系统目录为准。
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： ○ **全部文件类型**：即针对所有类型的文件进行备份防护。 ○ **指定文件类型**：即针对指定文件进行备份防护。支持选择以下文件类型： ■ **文档类** ■ **压缩包类** ■ **数据库类** ■ **音频视频类** ■ **脚本代码类** **注意** ■ 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。 **注意** 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。

配置项	说明
备份策略执行间隔	设置备份策略执行间隔，默认为1天。支持选择以下时间： ○ 0.5天 ○ 1天 ○ 3天 ○ 7天
备份数据保留时间	设置备份数据保留时间，默认为7天。 **注意** 超过备份数据保留时间后，备份数据会自动清理，建议您根据业务需求合理设置备份数据保留时间。 支持选择以下保存方式： ○ **永久保存** ○ **自定义** **说明** 自定义保存天数，最小可设置1天，最大支持设置65535天。
备份网络带宽限制（MByte/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 MByte/s~不限流量。 **注意** ECS服务器仅占用内网带宽，不影响外网带宽。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。

6. 单击**确定**。

   创建防护策略后，策略状态默认为开启状态。云安全中心将自动在您的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。

相关操作

- 查看防勒索客户端状态

  防护策略创建后，您需要在**服务器防勒索**页签下的策略列表中，单击策略左侧的图标，展开策略生效的服务器列表，查看该策略下每个服务器上的防勒索客户端的状态，确保防勒索客户端状态为**客户端在线**。只有防勒索客户端的状态为**客户端在线**，云安全中心才能正常备份服务器上的数据。
  如果备份客户端状态为**未安装**、**安装失败**或**服务异常**，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。

  说明 服务异常可能是备份异常或恢复异常，恢复异常的情况下可以正常备份，请根据页面提示处理异常。

  您可以通过以下方式排查防勒索客户端的异常：

  ○ 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。

- 提交工单联系阿里云安全工程师协助您处理。

- 手动安装防勒索客户端
  创建防护策略后，云安全中心将自动在您的服务器上安装防勒索客户端。如果您的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，然后为该服务器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
  如果策略中服务器上的客户端状态为**服务异常**或**安装失败**，您可以单击该服务器**操作**列的**卸载**，将防勒索客户端卸载后，再重新安装。

> **说明** 防勒索客户端卸载后，云安全中心在该服务器防勒索策略的**备份数据保留时间**内，不会删除该客户端已备份的服务器数据。如果超过**备份数据保留时间**，已备份的服务器数据则会被删除。

- 删除防勒索客户端
  如果某一个服务器不再需要防勒索策略的防护，您可以删除该服务器上的防勒索客户端。删除防勒索客户端的同时会将该服务器从策略生效的服务器列表中移除，服务器的备份数据也会被删除。服务器备份数据的删除会为您释放相应的勒索防护容量，勒索防护容量释放有24~72小时的延时，建议您保持充足的存储容量，请勿耗尽容量。如果因存储容量耗尽，备份停止后又进行全量备份，会导致服务器性能消耗过高。

> **注意** 删除客户端会导致备份数据删除，备份数据删除后将无法恢复，请您谨慎操作。

1.3.2. 管理防护策略

防护策略创建后，您可以停用、启用策略或修改策略名称、管理防护资产、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。本文介绍如何停用、启用、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。

停用或启用防护策略

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**服务器防勒索**页签。
4. 在**服务器防勒索**页签下，定位到需要停用或启用的策略，在该策略的**策略状态**下停用或启用策略。
   - **停用策略**
     防勒索策略首次进行数据备份时，会消耗服务器较多的CPU和内存资源，可能会影响您的正常业务。为了避免此情况发生，您可以停用该策略，即关闭该策略的**策略状态**开关。该策略停用后，正在运行的备份任务也会停止。您可在业务低峰期，重新启用该策略，执行数据备份任务。
   - **启用策略**
     服务器防勒索防护策略创建后默认为启用状态。如果您因为备份任务占用您服务器较多CPU和内存资源，临时停用了某个策略，您可以在业务低峰时段重新启用该策略。防护策略启用状态下，才能根据您的策略备份服务器的数据。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。

修改防护策略

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**服务器防勒索**页签。
4. 在**服务器防勒索**页签下，定位到需要修改的防护策略，单击操作列的**编辑**。

5. 在**编辑防护策略**面板，修改防护策略的参数。

   防护策略的参数说明，请参见防护策略参数说明。
6. 单击**确定**。
   云安全中心将按照您修改后的防护策略执行数据备份任务。

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，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**服务器防勒索**页签。
4. 在**服务器防勒索**页签下，定位到需要管理服务器的防护策略，单击左侧图标，展开该策略防护的服务器列表。
5. 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，请参见修改防护策略。

     > **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条防护策略中。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**

     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**。

     > **说明** 防勒索客户端卸载后，云安全中心在该服务器防勒索策略的**备份数据保留时间**内，不会删除该客户端已备份的服务器数据。如果超过**备份数据保留时间**，已备份的服务器数据则会被删除。

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，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**服务器防勒索**页签。
4. 在**服务器防勒索**页签下，定位到需要删除的防护策略，单击其操作列的**删除**。
5. 在**确认**对话框中，单击**确定**。

1.3.3. 服务器防勒索客户端异常状态排查

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

前提条件

已为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，无法正常进行数据备份以及保护您的服务器，请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，选择**主动防御 > 防勒索**。
3. 在**服务器防勒索**页签下，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**对话框中的错误详情提示，处理客户端异常。

   客户端异常状态的原因和处理建议，请参见客户端异常的原因及解决方案。

客户端异常的原因及解决方案

客户端错误码	错误详情提示	产生异常的原因	解决方案

客户端错误码	错误详情提示	产生异常的原因	解决方案
CLOUD_ASSIST_NOT_RUN	云助手未开启。	云助手未正常启动。	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。
RoleNotExist	授权问题。	账号权限不足。	使用阿里云账号在**服务器防勒索**页签下，单击**立即授权**，为当前账号授权**AliyunHBRDefaultRole**和**AliyunECSAccessingHBRRole**角色。
CLIENT_CONNECTION_ERROR	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 count：446。	ECS对应的RAM角色缺少AliyunECSAccessingHBRRolePolicy策略，导致客户端安装失败。	为ECS添加RamRole后，重新安装防勒索客户端。操作步骤如下： 1. 为ECS添加RamRole。具体操作，请参见客户端安装失败，提示“EcsRamRole上缺少AliyunECSAccessingHBRRolePolicy的策略”错误。 2. 重新安装防勒索客户端。详细操作步骤，请参见相关操作。 **注意** 为ECS添加RamRole后，不会自动触发重新安装防勒索客户端，请您登录云安全中心控制台在防勒索页面进行手动安装。
CHECK_ACTIVATION_COMMAND_TIMEOUT	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。

客户端错误码	错误详情提示	产生异常的原因	解决方案
ECS_STOPPED	ECS停机。	ECS服务器未开机， 导致客户端安装失败。	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。
UNINSTALL_FAILED	卸载客户端失败。	云助手命令超时，导致客户端卸载失败。	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**服务器防勒索**页签下，定位到卸载客户端失败的服务器，单击其操作列下**删除**。 **说明** 删除策略中的服务器需要约2分钟时间，请您耐心等待。 2. 将ECS服务器重新添加到之前的防护策略中。详细操作步骤，请参见修改防护策略。 3. 重新安装防勒索客户端。详细操作步骤，请参见相关操作。
INSTALL_FAILED	安装失败。	云助手命令超时，导致客户端安装失败。	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。

客户端错误码	错误详情提示	产生异常的原因	解决方案
AGENT_NOT_RUN_AFTER_INSTALLATION	安装后服务未启动。	之前卸载客户端时存在卸载注册表残留未清理，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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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. 根据策略的客户端版本，清理以下两项注册表。 ○ 策略的客户端版本为V1.X.X #1**代客户端** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hybridbackup HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrupdater ○ 策略的客户端版本为V2.X.X #**二代客户端** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrclient HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\hbrclientupdater HKEY_LOCAL_MACHINE\SOFTWARE\Alibaba, Inc.\Aliyun Hybrid Backup Service Client #64**位特有** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B1F066FC-D85C-46F8-9ED7-88A4385AF9A6}}_is1 #32**位特有** 32**位的系统删这个** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9A3FBAB2-A9B0-4F3B-951A-ABC72D58BA6D}}_is1 3. 重新安装防勒索客户端。详细操作步骤，请参见相关操作。

客户端错误码	错误详情提示	产生异常的原因	解决方案
FAILED_TO_DOWNLOAD_INSTALLER	下载安装包失败。	网络连接失败，导致安装包下载失败。	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。
PRECHECK_COMMAND_FAILED	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。
INSTALL_COMMAND_TIMEOUT	安装命令超时。	客户端安装命令超时，导致客户端安装失败。	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。
ServiceUnavailable	ServiceUnavailable。	授权问题或者超过QPS限制。	• 使用阿里云账号在**服务器防勒索**页签下，单击**立即授权**，为当前账号授权**AliyunHBRDefaultRole**和**AliyunECSAccessingHBRRole**角色。 • 请提交工单解决该问题。
CONFLICT_WITH_EXISTING_AGENT	跟已有客户端冲突。	与该服务器上已安装的客户端冲突。	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。

客户端错误码	错误详情提示	产生异常的原因	解决方案
ACTIVATE_COMMAND_FAILED	客户端出现异常错误，您可以重新安装客户端，恢复业务正常运行，若仍失败，请您提工单进行咨询，由阿里技术专家协助您一同排查解决问题。	客户端异常。	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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。 3. 如果仍然失败，请提交工单解决该问题。
CHECK_RUNNING_COMMAND_FAILED	检查服务启动命令失败。	服务异常。	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**服务器防勒索**页签下，卸载服务器上的防勒索客户端。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

地域	公网接入点	ECS内网接入点
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

金融云

地域名称	公网接入点	ECS内网接入点
华东2金融云（上海金融云）	https://hbr.cn-shanghai-finance-1.aliyuncs.com	https://hbr-vpc.cn-shanghai-finance-1.aliyuncs.com

1.3.4. 清理防勒索备份占用的服务器的磁盘空间

为了提高数据备份效率，防勒索服务备份数据时，默认会占用您服务器上的磁盘空间进行数据缓存备份。如果发现您服务器中防勒索备份数据缓存的目录下的文件占用了较大的磁盘空间，您可以通过清理防勒索备份的缓存文件或修改缓存数据位置的方式，释放该目录的磁盘空间。

背景信息

正常情况下，防勒索备份占用服务器的磁盘空间为临时占用，待备份数据上传到云端后，备份数据会自动删除。在备份文件过多、过大或程序运行异常时，会出现备份占用服务器的磁盘空间过大的情况。建议您定时清理备份占用的磁盘空间，提升服务器运行的效率。

清理磁盘空间

为了释放更多的磁盘空间，您可以参考以下步骤清理防勒索备份占用的磁盘空间。

1. 如果您的服务器开启了客户端自保护，您需要关闭服务器的客户端自保护功能。

   服务器开启客户端自保护功能后，云安全中心会默认保护Agent目录下的文件。只有为服务器关闭客户端自保护功能后，您才能修改Agent目录下的文件，才可以清理防勒索缓存文件。关于客户端自保护的具体操作，请参见客户端自保护。

2. 使用root用户登录需要操作的服务器。
3. 清理服务器中防勒索备份缓存目录下的缓存文件。

   不同防勒索客户端版本的防勒索备份缓存的目录如下：

客户端版本	服务器的操作系统	防勒索备份的缓存目录
1.x.x	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbr\cache*

客户端版本	服务器的操作系统	防勒索备份的缓存目录
1.X.X	Linux	*/usr/local/aegis/hbr/cache*
2.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbrclient\cache*
	Linux	*/usr/local/aegis/hbrclient/cache*

> **说明** 防勒索功能已为您备份防护策略中需要防护的文件，删除该缓存文件不会对已备份文件产生任何影响。

修改备份缓存的位置、状态及占用系统内存空间的上限

1. 使用root用户登录需要操作的服务器。
2. 找到并进入防勒索客户端的安装路径。

   不同版本的防勒索客户端的安装目录如下：

客户端版本	服务器的操作系统	防勒客户端的安装目录
1.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbr\client*
	Linux	*/usr/local/aegis/hbr/client*
2.X.X	Windows	*C:\Program Files (x86)\Alibaba\Aegis\hbrclient\client*
	Linux	*/usr/local/aegis/hbrclient/client*

3. 在 `client` 文件夹下，新建文件 `hbr.config` 。
4. 在 `hbr.config` 文件中按照以下参数添加数据ID及元数据缓存信息，并保存该文件。

   通过配置 `hbr.config` 文件中的参数，可以设置缓存数据存放的位置、缓存数据占用系统内存空间的上限等缓存配置。

参数	说明
disable_blob_cache	是否启用数据ID缓存。取值： ○ **true**：不启用数据ID缓存。 ○ **false**：启用数据ID缓存。
max_blob_cache_weight	数据ID缓存最多使用系统内存的百分比。 数值需大于0小于1。默认值0.15，即最多使用15%的系统总内存。
cache_prefix	缓存存放位置的路径字符串。 必须为绝对路径。
max_retain_count	最多保留的数据ID缓存的个数。 取值需为整型。

参数	说明
disable_file_cache	是否启用元数据缓存。取值： ○ **true**：不启用元数据缓存。 ○ **false**：启用元数据缓存。
file_cache_max_size_hint	元数据缓存文件能够使用的磁盘空间的最大值，实际大小可能超出该项设置。 默认值2 GB。 **说明** ○ 2 GB文件缓存至少能支持备份4 TB的数据。 ○ 此参数值不得超过磁盘剩余可用空间大小。 ○ 此参数设置过小时，会降低缓存的效果，但不会导致备份失败。

hbr.config文件的配置示例如下：

```
disable_blob_cache = false    //启用数据ID缓存。
max_blob_cache_weight = 0.15    //数据ID缓存最多使用系统内存的15%。
cache_prefix = D:\CacheFolder    //缓存数据存放的位置为D:\CacheFolder。
max_retain_count = 16    //最多保留16个数据ID缓存。
disable_file_cache = false    //启用元数据缓存。
file_cache_max_size_hint = 2g    //元数据缓存最多可占用2 GB的磁盘空间。
```

说明 备份数据缓存文件位置修改完成后，无需重启防勒索备份客户端，下次备份时修改后的配置会自动生效。

1.4. 数据库防勒索

1.4.1. 创建防护策略

云安全中心提供数据库防勒索功能。您可使用此功能为数据库创建勒索防护策略，备份您数据库中的数据。在数据库被勒索病毒入侵后，您就可以使用已备份数据快速恢复数据库的数据，确保您的业务正常进行。本文介绍如何为数据库创建勒索防护策略。

背景信息

如果您已在使用阿里云的混合云备份服务（HBR）备份您数据库的数据，不建议您再使用数据库防勒索功能重复备份。

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。

操作步骤

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

3. 在**防勒索**页面，单击**数据库防勒索**页签，然后单击**创建防护策略**。
4. 在**数据库防护策略**面板，为数据库创建防护策略。
   i. 配置您要防护的数据库的信息，然后单击**下一步**。

配置项	说明
策略名称	设置防护策略的名称。
类型	选择添加数据库的方式。取值： ■ **自动识别数据库** 系统会自动识别出您服务器上已安装的数据库。建议您使用此功能快速选择您要防护的数据库。 ■ **手动录入数据库** 如果使用**自动识别数据库**功能未能找到您要防护的数据库，您可以使用此功能，手动录入要防护的数据库。
数据库	选择您要防护的数据库或者数据库所在的服务器实例。
数据库类型	选择添加的数据库的类型。仅选择**手动录入数据库**时需要设置此项。取值： ■ MYSQL ■ ORACLE ■ MSSQL
账号	输入待添加的数据库账号，该账号必须有该数据库的备份权限。Oracle数据库无需输入账号和密码。 **注意** 请输入已选择的数据库的账号和密码，而非服务器的账号和密码。
密码	输入数据库账号的密码。

ii. 配置数据库防护策略的信息，然后单击**完成**。

配置项	说明
防护策略	您可单击**使用推荐策略**，直接使用云安全中心提供的推荐策略。如果推荐策略不符合您的业务需求，您可对推荐策略稍作修改，使其更符合您业务需求。
全量备份策略	配置全量备份的**间隔周期**、**周中执行日期**和**备份开始时间**。 全量备份指对某一时间点上数据库中的所有数据进行备份。全量备份所需的防勒索容量较多、备份的时间较长。
增量备份策略	配置增量备份的**间隔周期**和**备份开始时间**。 增量备份是指在一次全备份或上一次增量备份后，备份与前一次相比增加或者有变化的数据。增量备份没有重复的备份数据，因此备份所需的防勒索容量较少，备份的时间较短。
备份数据保留时间	选择备份保留的时间。
备份网络带宽限制	设置备份时的网络带宽。设置为0表示不限制带宽。

数据库的勒索防护策略创建后，云安全中心将自动在您的服务器上安装防勒索客户端，此时该防护策略进入**初始化中**状态。客户端安装完成后，云安全中心将根据防护策略中设置的备份策略对数据库进行数据备份。

后续步骤

创建防护策略后，您需要对策略中添加的数据库进行预检，以确保该数据库可以正常备份。具体操作，请参见预检数据库。

数据库的勒索防护策略创建后，建议您重点关注防护策略的状态，并及时处理防护策略的异常状态。更多信息，请参见数据库防勒索策略状态异常排查。

1.4.2. 预检数据库

数据库防勒索防护策略创建后，您需要对该策略中的数据库的OSS连接性、管控网络连接性等进行预检，以确保该数据库的数据可以正常备份。数据库防勒索功能仅支持安装在阿里云ECS服务器上的MySQL数据库、Oracle数据、SQL Server数据库这三种数据库。本文介绍如何对这三种数据库进行预检。

背景信息

阿里云ECS服务器上安装的MySQL数据库、Oracle数据、SQL Server数据库这三种数据库在备份时各数据库版本、功能支持信息，请参见概述。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**通用防勒索解决方案**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中定位到您新建的策略，在**操作**列单击**预检**。
5. 在预检页面，单击**开始检查**。

   以下为不同数据库的检查项说明。

   - MySQL数据库：

检查项	说明
OSS连接性检查	检查MySQL实例和所在地域的OSSECS的VPC网络访问（内网）域名的连通性。如果OSS连接性异常，则该数据库无法执行备份和恢复操作。
管控网络连接性检查	检查MySQL数据库实例至管控网络的连通性。如果管控网络连接性异常，则该数据库无法执行备份和恢复操作。
支持全量备份的版本检查	检查支持全量备份的数据库版本。 **说明** MySQL 8.0版本不支持增量备份。
BINLOG检查	检查MySQL数据库实例的BINLOG配置是否正常。如果BINLOG配置异常，则该数据库无法执行备份和恢复操作。

- Oracle数据库：

检查项	说明
OSS连接性检查	检查Oracle数据库实例和所在地域OSS的VPC网络连通性。 如果OSS连接性异常，则该数据库无法执行备份和恢复操作。
管控网络连接性检查	检查Oracle数据库实例至管控网络的连通性。如果管控网络连接性异常，则该数据库无法执行备份和恢复操作。
Oracle实例状态检查	检查Oracle数据库实例状态是否正常。如果Oracle实例状态异常，则该数据库无法执行备份和恢复操作。
Oracle数据库状态检查	检查Oracle数据库实例中所有数据库状态是否正常。如果Oracle数据库状态异常，则该数据库无法进行备份和恢复操作。
归档模式检查	检查Oracle数据库实例的归档模式是否正常。如果归档模式异常，则该数据库无法执行备份和恢复操作。如何开启Oralce归档模式，请参见开启Oracle归档模式。

- SQL Server数据库：

检查项	说明
OSS连接性检查	检查SQL Server数据库实例和所在地域OSS的VPC网络连通性。 如果OSS连接性异常，则该数据库无法执行备份和恢复操作。
管控网络连接性检查	检查SQL Server数据库实例至管控网络的连通性。如果管控网络连接性异常，则该数据库无法执行备份和恢复操作。

检查项	说明
恢复模式检查	检查数据库的恢复模式。如果恢复模式异常，则数据库无法进行增量或日志备份。 **注意** ■ 由于SQL Server存在限制，检查提示不通过的数据库只支持简单恢复模式，无法进行日志备份。 ■ master数据库只支持全量备份。若配置为增量备份和日志备份，数据库防勒索默认会转换为全量备份。 ■ 您可以参考SQL Server产品文档，修改恢复模式。
SQL Server数据库状态检查	检查SQL Server数据库实例是否在线。如果SQL Server数据库实例状态异常，则该数据库无法执行备份和恢复操作。

预检大约需要1分钟时间，请您耐心等待。
当存在异常的检查项时，请根据界面提示确认对应数据库是否影响备份和恢复操作。若有影响，请参考检查项说明及时处理影响备份和恢复的问题。

1.4.3. 管理防护策略

防护策略创建后，您可以停用策略、编辑该策略。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。本文介绍如何停用、编辑、删除防护策略以及手动安装或卸载防勒索客户端。

前提条件

已创建数据库防勒索策略。更多信息，请参见创建防护策略。

背景信息

防护策略的最新备份状态为**执行成功**时，说明已按照策略正常备份数据库的数据。如果您的防护策略的最新备份状态为**执行失败**，需要及时处理该异常状态。更多信息，请参见数据库防勒索策略状态异常排查。

停用、启用防护策略

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要停用或者启用的防护策略，在该策略的**策略状态**列启用或停用策略。
   - **停用策略**
     如果您想停用某个策略，您可以在**策略状态**列，关闭策略状态的开关。

     注意 策略停用后，数据库防勒索的数据备份任务将会停止，请您谨慎操作。
   - **启用策略**

防护策略启用后，防勒索客户端才能备份您数据库中的数据（即根据您的策略备份数据）。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。

编辑防护策略

防护策略创建后，如果想修改防护策略，您可以使用**编辑**功能对策略进行修改。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要修改的防护策略，单击**操作**列的**编辑**。
5. 在**数据库防护策略**面板上，修改**策略名称**。
6. 填写数据库的账号和密码后，单击**下一步**。
7. 修改防护策略。

配置项	说明
防护策略	您可单击**使用推荐策略**，直接使用云安全中心提供的推荐策略。如果推荐策略不符合您的业务需求，您可对推荐策略稍作修改，使其更符合您业务需求。
全量备份策略	配置全量备份的**间隔周期**、**周中执行日期**和**备份开始时间**。 全量备份指对某一时间点上数据库中的所有数据进行备份。全量备份所需的防勒索容量较多、备份的时间较长。
增量备份策略	配置增量备份的**间隔周期**和**备份开始时间**。 增量备份是指在一次全备份或上一次增量备份后，备份与前一次相比增加或者有变化的数据。增量备份没有重复的备份数据，因此备份所需的防勒索容量较少，备份的时间较短。
备份数据保留时间	选择备份保留的时间。
备份网络带宽限制	设置备份时的网络带宽。设置为0表示不限制带宽。

8. 单击**完成**。

   防勒索客户端将按照您修改后的策略，备份数据库的数据。

删除策略

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。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要修改的防护策略，单击**操作**列的 ⋮ 图标。
5. 在下拉列表中，单击**删除**。
6. 在提示对话框中，单击**确定**。

   删除策略需要一段时间，请您耐心等待。

手动安装客户端

如果某个数据库防勒索策略初始化失败，或者您手动卸载了该策略防护的服务器上的客户端，您可以为该策略防护的服务器手动安装客户端。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要安装客户端的防护策略，单击**操作**列的图标。
5. 在下拉列表中，单击**安装客户端**。
   该策略的**客户端状态**会显示**安装中**。客户端安装大约需要5分钟，请您耐心等待。

手动卸载客户端

> **注意** 卸载防勒索客户端后，数据库防勒索策略无法为您的数据库提供防勒索服务，请您谨慎操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要卸载客户端的防护策略，单击**操作**列的图标。
5. 在下拉列表中，单击**卸载客户端**。
6. 在弹出的确认对话框中，单击**确定**。
   该策略的**客户端状态**会显示**卸载中**。客户端卸载大约需要5分钟，请您耐心等待。

1.4.4. 创建恢复任务

如果数据库的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。

前提条件

- 已为该数据库创建防护策略并且该策略运行正常（可以正常备份数据库的数据）。
- 防护策略下的可恢复版本数不为0。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在防护策略列表中，定位到您要恢复备份数据的数据库，单击**操作**列的**恢复**。
5. 在**创建恢复任务**对话框中，配置恢复任务。

   针对不同数据库，创建恢复任务的配置项略有不同。

   > **注意** 备份数据恢复，支持跨服务器恢复（目标服务器创建了防护策略并成功安装了防勒索客户端），但不支持跨系统恢复。

   - 恢复备份的数据库为MySQL数据库时，需要进行以下配置。

配置项说明如下：

配置项	描述
恢复的时间点	选择要恢复的备份数据的备份时间点。如果您的数据库被勒索病毒入侵，您可以在创建恢复任务时选择离入侵时间最近的一个备份，以确保恢复后的数据与入侵前的数据差异较小。
恢复到机器	选择将数据恢复到那台服务器。

- 恢复备份的数据库为SQL Server数据库时，需要进行以下配置。

配置项	描述
选择数据库	选择要恢复的备份数据库。
恢复备份的集	选择要恢复的备份数据。如果您的数据库被勒索病毒入侵，您可以在创建恢复任务时选择离入侵时间最近的一个备份，以确保恢复后的数据与入侵前的数据差异较小。
恢复到机器	选择将数据恢复到那台服务器。

- 恢复备份的数据库为Oracle数据库时，需要进行以下配置。
  配置项说明如下：

配置项	描述
选择恢复版本	选择要恢复的备份数据的版本，即选择要恢复那个时间段备份的数据。
恢复的时间点	选择要恢复备份的具体时间点。可选择该恢复版本备份的时间段中的任意一个时间点作为恢复时间点。
恢复到机器	选择将数据恢复到那台服务器。

6. 单击**确定**。

   防勒索客户端将开始执行备份数据的恢复任务。

   > 注意 执行数据恢复任务时，如果目标服务器同时在执行数据备份任务，则会导致恢复任务失败。建议您在开始创建恢复任务前，关闭恢复任务的目标服务器上的备份任务。

查看恢复任务

您可以在策略列表上方，单击**恢复中/恢复记录**下方的恢复数据，进入**恢复记录**面板查看已创建的恢复记录。恢复任务完成后，**恢复记录**面板上的**恢复状态**列会显示**执行成功**。

1.4.5. 数据库防勒索策略状态异常排查

如果您已为数据库创建勒索防护策略，但在云安全中心控制台上数据库防勒索的防护策略状态处于异常状态，并有账号密码错误、初始化失败、超量被自动关闭等提示，请参考本文排查原因并进行相应处理。

前提条件

前提条件

已为您的数据库创建防护策略。更多信息，请参见创建防护策略。

背景信息

数据库防勒索的防护策略状态异常时将无法正常进行数据备份，无法正常防护您的数据库。建议您及时排查数据库防勒索的防护策略状态异常原因并进行相应处理。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 防勒索**。
3. 在**防勒索**页面，单击**数据库防勒索**页签。
4. 在**数据库防勒索**页签下的防护策略列表中，查看策略状态异常的原因。

5. 根据策略状态异常的原因处理异常。

   数据库防勒索策略状态异常状态的原因和处理建议，请参见策略状态说明。

策略状态说明

策略状态	说明	解决方案
账号密码错误	数据库账号密码错误	请填写正确的数据库账号、密码后，重新开启策略。
初始化中	环境初始化中	请耐心等待策略初始化完成。
初始化失败	初始化失败	请先尝试重新安装客户端，然后重新编辑策略。安装客户端、编辑防护策略的具体操作，请参见手动安装客户端、编辑防护策略。
启用中	策略正在启用中	请耐心等待策略完成启用。
已启用	策略已成功启用	无
已停用	策略已停用	无
停用中	正在停用策略中	请您耐心等待策略完成停用。
超量被自动关闭	防勒索容量空间已满	请手动清理历史数据释放空间或进行续费扩容。具体操作，请参见已购买的防勒索数据保护容量不够用怎么办？。
正在删除	策略删除中	请耐心等待策略完成删除。

策略状态	说明	解决方案
删除失败	策略删除失败	请稍后重新尝试删除策略。删除策略的具体操作，请参见删除策略。
恢复中	数据恢复中	请耐心等待数据恢复任务完成。
备份中	数据备份中	请耐心等待备份数据任务完成。

2.病毒防御

病毒防御使用了阿里云机器学习病毒查杀引擎和实时更新的病毒库，提供丰富的系统扫描项，覆盖了持久化启动项、活动进程、内核模块、敏感目录、SSH后门公钥等系统薄弱模块，可有效清理服务器上的各类恶意威胁。本文介绍如何使用病毒防御功能。

背景信息

在使用云安全中心病毒防御功能时，建议您同时开启防病毒功能。开启防病毒后，云安全中心会自动拦截主流木马病毒、勒索软件、挖矿病毒、DDoS木马等威胁，阻断其恶意行为。开启防病毒功能的具体操作，请参见主动防御。

病毒防御功能支持扫描及清理的病毒类型、扫描项如下：

- 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、可疑程序及自变异木马。
- 扫描项：活动进程、隐藏进程、Docker进程、内核模块、已安装程序、动态库劫持、服务、计划任务、开机自启动项及敏感目录。

版本限制

仅防病毒版、高级版、企业版、旗舰版支持该功能，免费版不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

扫描病毒

病毒防御功能会对云安全中心防护的所有服务器，针对勒索病毒、挖矿程序等顽固病毒提供深度扫描服务。病毒扫描支持立即扫描和周期性扫描。

1. 登录云安全中心控制台，在左侧导航栏，选择**主动防御 > 病毒防御**。
2. 在**病毒防御**页面，立即进行病毒扫描或设置周期性扫描。单击**开始病毒扫描**或**重新扫描**。
   - 立即进行病毒扫描
     a. 在**病毒防御**页面，单击**开始病毒扫描**或**重新扫描**。
     b. 在**请选择您要扫描的资产**对话框，选择需要扫描的资产，然后单击**开始扫描**。

     > **说明** 扫描完成预计需要2~5分钟，请您耐心等待。

   - 设置周期性扫描
     a. 在**病毒防御**页面，单击右上角**扫描设置**。
     b. 在**防御配置**面板，设置扫描病毒的周期、方式和要扫描的资产，然后单击**确定**。
     云安全中心会按照您设置的扫描周期、方式对要扫描的资产执行自动扫描病毒。

扫描完成后，建议您及时查看并处理扫描结果，以确保您的服务器不受恶意病毒的威胁。更多信息，请参见处理告警。

处理告警

针对病毒扫描检出的威胁项，还提供了完整的威胁处置能力，支持对勒索、挖矿等顽固病毒一键深度查杀。深度查杀通过查杀恶意病毒进程、隔离恶意文件和清除病毒木马的持久化驻留项可以彻底清理各类顽固性病毒。

1. 登录云安全中心控制台，在左侧导航栏，选择**主动防御 > 病毒防御**。
2. 在**病毒防御**页面，单击**立即处理**。
3. 在检查结果列表中定位到需要处理的告警，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，单击**批量处理**。您也可以在页面左上角单击**一键处理**，同时处理所有的告警。

4. 在**告警处理**对话框中选择处理方式，然后单击**立即处理**。

处理方式	说明
深度查杀	对服务器中的病毒进行深度查杀。 深度查杀是云安全中心产品对持久化、顽固型病毒进行深度分析和测试后，提供的专项查杀能力。 深度查杀模式下，支持选择先自动创建快照备份您的服务器系统盘，再进行病毒查杀，帮助您在执行病毒查杀时有效降低操作风险。
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	忽略当前告警。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**，当前告警状态将更新为**已处理**。

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

- 网页防篡改为云安全中心增值功能。免费版不支持该功能。免费版用户需先升级至防病毒版、高级版、企业版、旗舰版或仅采购增值服务，才可开通和使用网页防篡改服务。
- 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。
- 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。

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。

网页防篡改支持以下两种防护模式：

- **拦截模式**：云安全中心会主动拦截异常进程和异常文件变动，确保您服务器网站和文件的安全。在**防护状态**页签下，您可以查看云安全中心已为您拦截的异常进程告警信息。
- **告警模式**：云安全中心会对识别到的异常进程和异常文件变动进行告警。如果您无法确认哪些进程需要放行时，可以使用该防护模式。在**防护状态**页签下，您可以查看告警信息并判断是否需要将相应告警加入白名单。确认需要加入白名单的进程后，建议为需要防护的服务器开启拦截模式，确保服务器的文件安全。加入白名单的具体操作，请参见加入白名单。

如何通过进程白名单防止正常进程被拦截

您可以在云安全中心控制台的**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。

操作系统和内核版本限制

使用网页防篡改功能时，服务器需要运行特定版本的操作系统和内核，否则您添加的防篡改进程白名单将无法生效，告警模式也将无法使用。

操作系统	操作系统版本号	内核版本号
Windows（32位或64位）	Windows Server 2008、2012、2016和2019	所有版本

操作系统	操作系统版本号	内核版本号
CentOS（64位）	• CentOS 6.3 • CentOS 6.5 • CentOS 6.6 • CentOS 6.7 • CentOS 6.8 • CentOS 6.9 • CentOS 6.10 • CentOS 7.0-1406 • CentOS 7.1-1503 • CentOS 7.2-1511 • CentOS 7.3-1611 • CentOS 7.4-1708 • CentOS 7.5-1804 • CentOS 7.6-1810 • CentOS 7.7-1908 • CentOS 7.8-2003 • CentOS 7.9-2009	• 2.6.32-**（表示所有2.6.32版本的CentOS系统内核） • 3.10.0-**（表示所有3.10.0版本的CentOS系统内核）
	• CentOS 8.0-1905 • CentOS 8.1-1911 • CentOS 8.2-2004 • CentOS 8.3-2011 • CentOS 8.4-2105 • CentOS 8.5 • CentOS Stream 8	• 4.18.0-80.11.2.el8_0.x86_64 • 4.18.0-147.3.1.el8_1.x86_64 • 4.18.0-147.5.1.el8_1.x86_64 • 4.18.0-147.8.1.el8_1.x86_64 • 4.18.0-193.el8.x86_64 • 4.18.0-193.6.3.el8_2.x86_64 • 4.18.0-193.14.2.el8_2.x86_64 • 4.18.0-193.28.1.el8_2.x86_64 • 4.18.0-240.1.1.el8_3.x86_64 • 4.18.0-240.15.1.el8_3.x86_64 • 4.18.0-240.22.1.el8_3.x86_64 • 4.18.0-305.3.1.el8.x86_64 • 4.18.0-305.7.1.el8_4.x86_64 • 4.18.0-305.10.2.el8_4.x86_64 • 4.18.0-305.12.1.el8_4.x86_64 • 4.18.0-305.19.1.el8_4.x86_64 • 4.18.0-305.25.1.el8_4.x86_64 • 4.18.0-348.2.1.el8_5.x86_64 • 4.18.0-348.7.1.el8_5.x86_64 • 4.18.0-358.el8.x86_64

操作系统	操作系统版本号	内核版本号
	Ubuntu 14.04	• 3.13.0-32-generic • 3.13.0-65-generic • 3.13.0-86-generic • 3.13.0-145-generic • 3.13.0-164-generic • 3.13.0-170-generic • 3.19.0-80-generic • 4.4.0-93-generic
	Ubuntu 16.04	• 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-79-generic • 4.4.0-93-generic • 4.4.0-96-generic • 4.4.0-104-generic • 4.4.0-117-generic • 4.4.0-124-generic • 4.4.0-142-generic • 4.4.0-146-generic • 4.4.0-151-generic • 4.4.0-154-generic • 4.4.0-157-generic • 4.4.0-161-generic • 4.4.0-170-generic • 4.4.0-174-generic • 4.4.0-176-generic • 4.4.0-177-generic • 4.4.0-178-generic • 4.4.0-179-generic • 4.4.0-184-generic • 4.4.0-194-generic • 4.4.0-198-generic • 4.4.0-210-generic

操作系统	操作系统版本号	内核版本号
Ubuntu（64位）	Ubuntu 18.04	• 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-48-generic • 4.15.0-52-generic • 4.15.0-54-generic • 4.15.0-66-generic • 4.15.0-70-generic • 4.15.0-72-generic • 4.15.0-88-generic • 4.15.0-91-generic • 4.15.0-96-generic • 4.15.0-101-generic • 4.15.0-106-generic • 4.15.0-109-generic • 4.15.0-112-generic • 4.15.0-117-generic • 4.15.0-118-generic • 4.15.0-121-generic • 4.15.0-122-generic • 4.15.0-124-generic • 4.15.0-128-generic • 4.15.0-143-generic • 4.15.0-151-generic • 4.15.0-162-generic • 4.15.0-166-generic • 4.15.0-169-generic • 4.15.0-170-generic
	Ubuntu 20.04	• 5.4.0-47-generic • 5.4.0-70-generic • 5.4.0-77-generic • 5.4.0-86-generic • 5.4.0-90-generic • 5.4.0-92-generic • 5.4.0-94-generic • 5.4.0-100-generic • 5.4.0-102-generic

操作系统	操作系统版本号	内核版本号
Anolis OS（64位）	• Anolis OS 7.9 RHCK • Anolis OS 7.9 ANCK • Anolis OS 8.4 RHCK	• 3.10.0-1062.an7.x86_64 • 3.10.0-1160.an7.x86_64 • 4.18.0-348.2.1.an8_4.x86_64 • 4.18.0-348.12.2.an8.x86_64 • 4.19.91-25.2.an7.x86_64
RHEL	• RHEL 6.2 • RHEL 7.7 • RHEL 7.8 • RHEL 7.9 • RHEL 8.0	• 2.6.32-220 • 3.10.0-1062 • 3.10.0-1127 • 3.10.0-1160 • 4.18.0-80
AliyunOS（64位）	AliyunOS 2.1903	• 4.4.95-1.al7.x86_64 • 4.4.95-2.al7.x86_64 • 4.4.95-3.al7.x86_64 • 4.19.24-7.al7.x86_64 • 4.19.24-7.14.al7.x86_64 • 4.19.81-17.al7.x86_64 • 4.19.81-17.2.al7.x86_64 • 4.19.91-18.al7.x86_64 • 4.19.91-19.1.al7.x86_64 • 4.19.91-21.al7.x86_64 • 4.19.91-22.2.al7.x86_64 • 4.19.91-23.al7.x86_64 • 4.19.91-24.al7.x86_64 • 4.19.91-24.1.al7.x86_64 • 4.19.91-25.1.al7.x86_64 • 4.19.91-25.3.al7.x86_64 • 4.19.91-25.6.al7.x86_64 • 5.10.23-5.al8.x86_64 • 5.10.60-9.al8.x86_64 • 5.10.84-10.2.al8.x86_64

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. 启用网页防篡改保护

使用网页防篡改功能对您的网站进行防护之前，您需要为部署该网站的服务器创建防护规则，在防护规则中添加需要防护的网站文件目录，并开启防护开关。

前提条件

- 已开通网页防篡改增值服务。
- 确保您当前阿里云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** 网页防篡改配额的到期时间等同于云安全中心服务的到期时间。云安全中心服务到期后，网页防篡改服务将无法继续使用，防篡改配额也将自动失效。

背景信息

基础版用户需升级到基础杀毒版、高级版或企业版，才能使用网页防篡改服务。
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

- 如果待防护的服务器系统和内核版本在防护限制列表范围内，将受到以下限制：
  - 每台服务器最多可添加10个防护目录。
  - 每个被防护的文件或目录的完整路径长度不能超过1000个英文字符或500中文字符。
- 如果待防护的服务器系统和内核版本不在防护限制列表范围内，将受到以下限制：
  - 每台服务器最多可添加10个防护目录。
  - 每个被防护的目录大小不超过20 GB。
  - 每个被防护的目录下的文件夹个数不超过20,000个。
  - 每个被防护的目录文件夹层级不超过20个。
  - 每个被防护的文件大小不超过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。关闭1台服务器的防护状态开关，将会释放出1个可用授权配额。

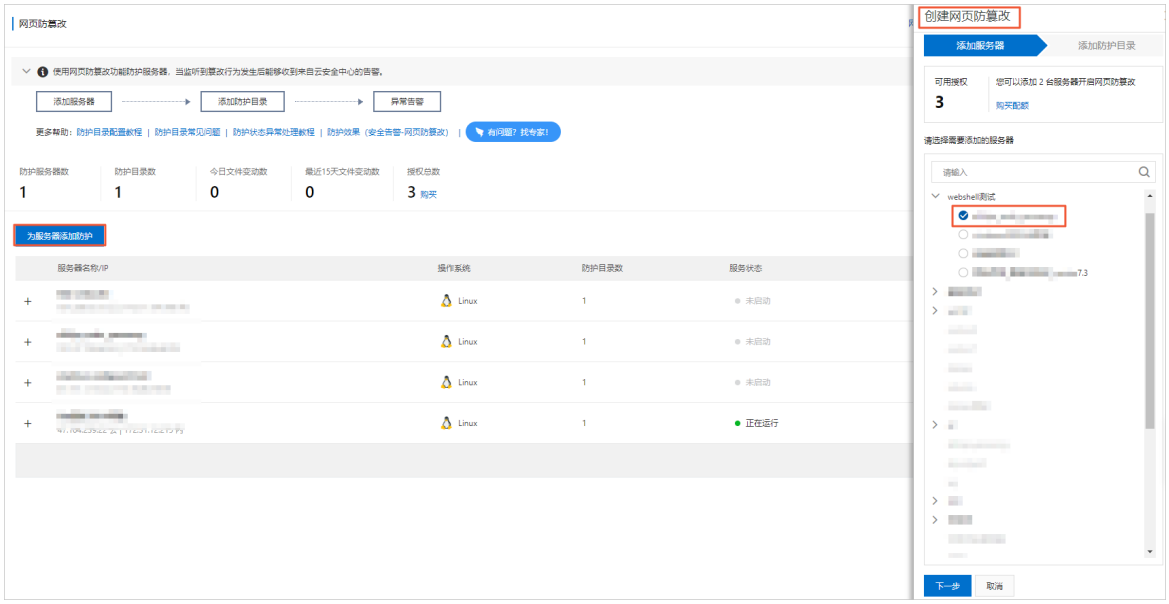
> **说明**
> - 建议您开启防护前检查文件夹目录层级、文件夹个数和防护目录大小是否超过限制。
> - 建议您排除 *LOG*、*PNG*、*JPG*、*MP4*、*AVI*、*MP3*等无需防护的文件类型。

操作步骤

1. 登录云安全中心控制台。

2. 在左侧导航栏，选择**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。



> **注意** 可使用的授权配额为0时，您将无法添加新的防护服务器。

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路径。 **说明** Linux服务器和Windows服务器防护目录路径的格式不同，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。 您也可以在此处手动输入下拉列表中未列出的文件类型。
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路径。
排除子目录	手动输入无需开启网页防篡改的子目录路径。 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**。您也可以手动输入这3类文件格式以外的其他文件类型。 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路径。 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。

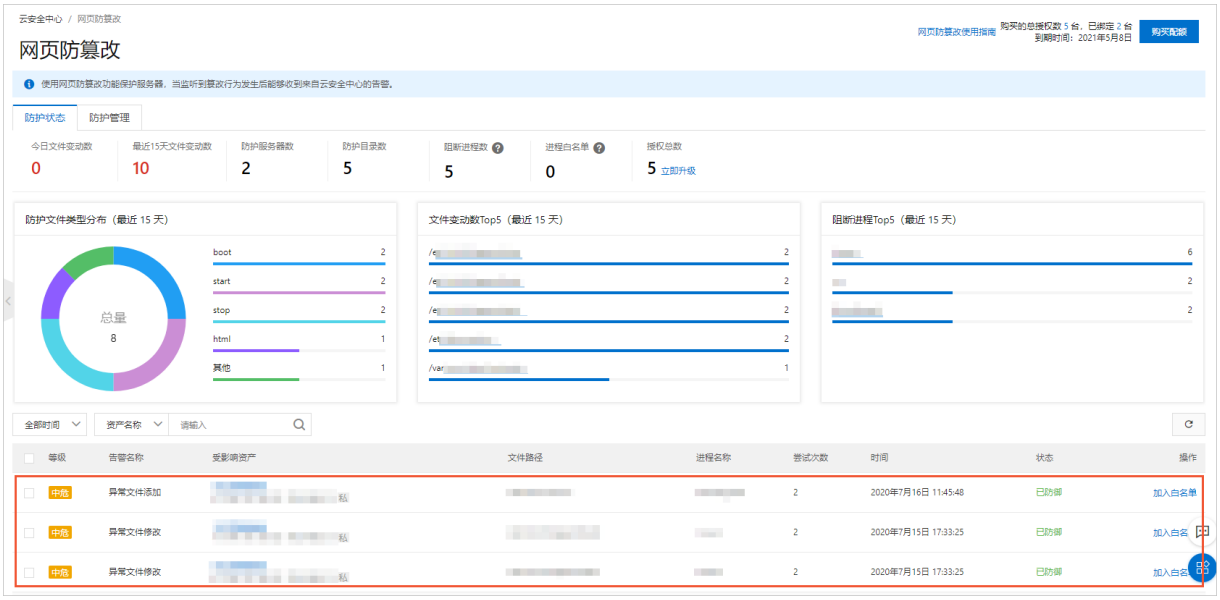
   > **说明** 添加服务器后，服务器的网页防篡改防护是**默认关闭**状态的。您需要在**网页防篡改**列表中开启目标服务器的防护状态。

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**。

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

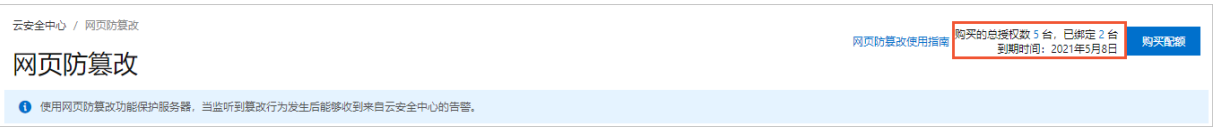
服务状态	说明	建议
启动中	网页防篡改防护服务正在开启。	首次开启防护时，目标主机的服务状态将会显示为**启动中**。请耐心等待数秒。
正在运行	防护状态已成功开启，服务正常运行中。	无
异常	防护开启异常。	将鼠标移动到目标服务器的服务状态上，查看发生异常的原因并单击**重试**。
未启动	防护状态为未开启。	需将防护状态设置为**开启**。

3.3. 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，选择**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142.6 USD/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。

3.4. 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，选择**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。

3.5. 加入白名单

网页防篡改功能检测到异常文件变动时，会实时拦截该异常变动的进程。如果您确认被拦截的异常进程为正常的业务进程，可通过白名单功能恢复该进程使其正常运行。本文介绍如何将被网页防篡改拦截的进程加入到白名单。

背景信息

网页防篡改功能支持将正常的业务进程批量加入白名单。加入白名单功能支持Windows服务器和Linux服务器。

限制条件

网页防篡改的加入白名单和告警模式功能，需要服务器运行特定版本的操作系统和内核。如果服务器运行的操作系统及与之对应的内核版本不属于以下列表中的操作系统和内核版本，则无法使用网页防篡改的加入白名单和告警模式功能。

操作系统	操作系统版本号	内核版本号
Windows（32位或64位）	Windows Server 2008、2012、2016和2019	所有版本

操作系统	操作系统版本号	内核版本号
CentOS（64位）	• CentOS 6.3 • CentOS 6.5 • CentOS 6.6 • CentOS 6.7 • CentOS 6.8 • CentOS 6.9 • CentOS 6.10 • CentOS 7.0-1406 • CentOS 7.1-1503 • CentOS 7.2-1511 • CentOS 7.3-1611 • CentOS 7.4-1708 • CentOS 7.5-1804 • CentOS 7.6-1810 • CentOS 7.7-1908 • CentOS 7.8-2003 • CentOS 7.9-2009	• 2.6.32-**（表示所有2.6.32版本的CentOS系统内核） • 3.10.0-**（表示所有3.10.0版本的CentOS系统内核）
	• CentOS 8.0-1905 • CentOS 8.1-1911 • CentOS 8.2-2004 • CentOS 8.3-2011 • CentOS 8.4-2105 • CentOS 8.5 • CentOS Stream 8	• 4.18.0-80.11.2.el8_0.x86_64 • 4.18.0-147.3.1.el8_1.x86_64 • 4.18.0-147.5.1.el8_1.x86_64 • 4.18.0-147.8.1.el8_1.x86_64 • 4.18.0-193.el8.x86_64 • 4.18.0-193.6.3.el8_2.x86_64 • 4.18.0-193.14.2.el8_2.x86_64 • 4.18.0-193.28.1.el8_2.x86_64 • 4.18.0-240.1.1.el8_3.x86_64 • 4.18.0-240.15.1.el8_3.x86_64 • 4.18.0-240.22.1.el8_3.x86_64 • 4.18.0-305.3.1.el8.x86_64 • 4.18.0-305.7.1.el8_4.x86_64 • 4.18.0-305.10.2.el8_4.x86_64 • 4.18.0-305.12.1.el8_4.x86_64 • 4.18.0-305.19.1.el8_4.x86_64 • 4.18.0-305.25.1.el8_4.x86_64 • 4.18.0-348.2.1.el8_5.x86_64 • 4.18.0-348.7.1.el8_5.x86_64 • 4.18.0-358.el8.x86_64

操作系统	操作系统版本号	内核版本号
	Ubuntu 14.04	• 3.13.0-32-generic • 3.13.0-65-generic • 3.13.0-86-generic • 3.13.0-145-generic • 3.13.0-164-generic • 3.13.0-170-generic • 3.19.0-80-generic • 4.4.0-93-generic
	Ubuntu 16.04	• 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-79-generic • 4.4.0-93-generic • 4.4.0-96-generic • 4.4.0-104-generic • 4.4.0-117-generic • 4.4.0-124-generic • 4.4.0-142-generic • 4.4.0-146-generic • 4.4.0-151-generic • 4.4.0-154-generic • 4.4.0-157-generic • 4.4.0-161-generic • 4.4.0-170-generic • 4.4.0-174-generic • 4.4.0-176-generic • 4.4.0-177-generic • 4.4.0-178-generic • 4.4.0-179-generic • 4.4.0-184-generic • 4.4.0-194-generic • 4.4.0-198-generic • 4.4.0-210-generic

操作系统	操作系统版本号	内核版本号
Ubuntu（64位）	Ubuntu 18.04	• 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-48-generic • 4.15.0-52-generic • 4.15.0-54-generic • 4.15.0-66-generic • 4.15.0-70-generic • 4.15.0-72-generic • 4.15.0-88-generic • 4.15.0-91-generic • 4.15.0-96-generic • 4.15.0-101-generic • 4.15.0-106-generic • 4.15.0-109-generic • 4.15.0-112-generic • 4.15.0-117-generic • 4.15.0-118-generic • 4.15.0-121-generic • 4.15.0-122-generic • 4.15.0-124-generic • 4.15.0-128-generic • 4.15.0-143-generic • 4.15.0-151-generic • 4.15.0-162-generic • 4.15.0-166-generic • 4.15.0-169-generic • 4.15.0-170-generic
	Ubuntu 20.04	• 5.4.0-47-generic • 5.4.0-70-generic • 5.4.0-77-generic • 5.4.0-86-generic • 5.4.0-90-generic • 5.4.0-92-generic • 5.4.0-94-generic • 5.4.0-100-generic • 5.4.0-102-generic

操作系统	操作系统版本号	内核版本号
Anolis OS（64位）	• Anolis OS 7.9 RHCK • Anolis OS 7.9 ANCK • Anolis OS 8.4 RHCK	• 3.10.0-1062.an7.x86_64 • 3.10.0-1160.an7.x86_64 • 4.18.0-348.2.1.an8_4.x86_64 • 4.18.0-348.12.2.an8.x86_64 • 4.19.91-25.2.an7.x86_64
RHEL	• RHEL 6.2 • RHEL 7.7 • RHEL 7.8 • RHEL 7.9 • RHEL 8.0	• 2.6.32-220 • 3.10.0-1062 • 3.10.0-1127 • 3.10.0-1160 • 4.18.0-80
AliyunOS（64位）	AliyunOS 2.1903	• 4.4.95-1.al7.x86_64 • 4.4.95-2.al7.x86_64 • 4.4.95-3.al7.x86_64 • 4.19.24-7.al7.x86_64 • 4.19.24-7.14.al7.x86_64 • 4.19.81-17.al7.x86_64 • 4.19.81-17.2.al7.x86_64 • 4.19.91-18.al7.x86_64 • 4.19.91-19.1.al7.x86_64 • 4.19.91-21.al7.x86_64 • 4.19.91-22.2.al7.x86_64 • 4.19.91-23.al7.x86_64 • 4.19.91-24.al7.x86_64 • 4.19.91-24.1.al7.x86_64 • 4.19.91-25.1.al7.x86_64 • 4.19.91-25.3.al7.x86_64 • 4.19.91-25.6.al7.x86_64 • 5.10.23-5.al8.x86_64 • 5.10.60-9.al8.x86_64 • 5.10.84-10.2.al8.x86_64

加入白名单

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 网页防篡改**。
3. 在**防护状态**页签下的告警事件列表中，查看或搜索需要加入白名单的异常进程告警事件。
4. 将异常进程告警事件加入白名单。

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。

- **单个告警事件加白名单**
  a. 在防护状态的告警事件列表中，定位到您要加入白名单的异常进程。
  b. 在**操作**列单击**处理**。
  c. 在弹出的对话框中，**处理方式**选择**加白名单**。
  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**。
  d. 单击**立即处理**。
- **多个告警事件批量加白名单**
  a. 在防护状态的告警事件列表中，选中多个您要加入白名单的异常进程。
  b. 单击列表底部的**加入白名单**。
  c. 单击**确定**。

您还可以单击**进程白名单**下方的数字进入**进程管理**面板，单击右上角的**录入白名单**，填写**进程路径**、**服务器名称/IP**将多个异常进程批量加入白名单。

查看、取消白名单

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 网页防篡改**。
3. 在防护状态页签下，单击**进程白名单**下方的数字。

4. 在**进程管理**面板上查看或取消白名单。
   - **查看白名单**
   进程管理面板上的**进程白名单**列表中会展示所有已加入白名单的异常进程，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。
   - **取消白名单**
   如果您需要将异常进程从白名单中移除，可以单击**操作**列的**取消白名单**进行移除白名单操作。
   您也可以选中多个白名单后，单击下方**取消白名单**进行批量移除白名单操作。

4.容器防火墙

4.1. 概述

容器防火墙是云安全中心为容器环境提供的防火墙服务。当黑客利用漏洞或恶意镜像入侵容器集群时，容器防火墙会对异常行为进行告警或拦截。

版本限制

仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

容器防火墙原理

容器防火墙通过将容器中应用的命名空间、应用名称、镜像以及标签等信息整合为网络对象，用于区别不同的容器应用。然后基于容器应用的网络对象，为集群创建网络访问的拦截规则，对异常访问流量进行检测和拦截。关于容器防火墙的配置和使用，请参见新增网络对象、创建防御规则、防御状态与规则管理和查看防护状态。

操作流程概述

支持的操作系统版本

集群防御规则的正常运行依赖于恶意网络行为防御的AliNet插件（AliNet插件主要用于网络连接拦截、DNS拦截、暴力破解拦截），使用容器防火墙功能前请确保您的集群节点的系统内核版本在AliNet插件支持的系统内核版本范围内。如果集群节点的系统内核版本不在AliNet插件支持的系统内核版本范围内，会导致集群防御规则无法生效。AliNet插件支持的系统内核版本如下：

操作系统	操作系统版本号	内核版本号

操作系统	操作系统版本号	内核版本号
Ubuntu（64位）	• Ubuntu 14.04 • Ubuntu 16.04 • Ubuntu 18.40 • Ubuntu 20.04	• 3.13.0-32-generic • 3.13.0-86-generic • 4.4.0-104-generic • 4.4.0-117-generic • 4.4.0-124-generic • 4.4.0-142-generic • 4.4.0-146-generic • 4.4.0-151-generic • 4.4.0-170-generic • 4.4.0-174-generic • 4.4.0-179-generic • 4.4.0-184-generic • 4.4.0-185-generic • 4.4.0-62-generic • 4.4.0-63-generic • 4.4.0-93-generic • 4.4.0-96-generic • 4.15.0-23-generic • 4.15.0-42-generic • 4.15.0-45-generic • 4.15.0-52-generic • 4.15.0-54-generic • 4.15.0-72-generic • 4.15.0-96-generic • 4.15.0-109-generic • 4.15.0-106-generic • 4.15.0-111-generic • 4.15.0-118-generic • 4.15.0-1047-gcp • 4.15.0-128-generic • 5.4.0-31-generic • 5.4.0-42-generic • 5.4.0-47-generic • 5.4.0-58-generic • 5.4.0-73-generic

操作系统	操作系统版本号	内核版本号
CentOS（64位）	• CentOS 6.5 • CentOS 6.6 • CentOS 6.7 • CentOS 6.8 • CentOS 6.9 • CentOS 6.10 • CentOS 7.0-1406 • CentOS 7.1-1503 • CentOS 7.2-1511 • CentOS 7.3-1611 • CentOS 7.4-1708 • CentOS 7.5-1804 • CentOS 7.6-1810 • CentOS 7.7-1908 • CentOS 8.0-1905 • CentOS 8.1-1911 • CentOS 8.2-2004	• 2.6.32-**（表示所有2.6.32版本的CentOS系统内核） • 3.10.0-**（表示所有3.10.0版本的CentOS系统内核） • 4.18.0-** (版本号小于4.18.0-240.15.1的版本) • 5.4.42-200.el7.x86_64
AliyunOS（64位）	AliyunOS 2.1903	• 3.10.0-1160.al7.1.x86_64 • 4.4.95-1.al7.x86_64 • 4.4.95-3.al7.x86_64 • 4.19.24-7.al7.x86_64 • 4.19.24-7.14.al7.x86_64 • 4.19.81-17.al7.x86_64 • 4.19.81-17.2.al7.x86_64 • 4.19.91-19.1.al7.x86_64 • 4.19.91-21.al7.x86_64 • 4.19.91-21.2.al7.x86_64 • 4.19.91-22.al7.x86_64 • 4.19.91-22.2.al7.x86_64 • 4.19.91-23.al7.x86_64 • 4.19.91-24.1.al7.x86_64

操作演示视频

4.2. 新增网络对象

使用云安全中心的容器防火墙服务，首先要创建源网络对象和目的网络对象，然后再创建防御。本文介绍如何创建网络对象。

前提条件

前提条件

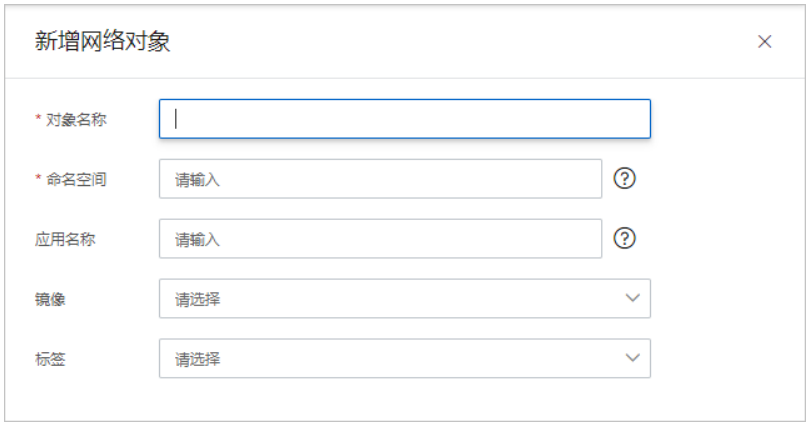
已为您的资产开启了恶意网络行为防御功能。相关文档，请参见主动防御。

版本限制

仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**网络对象**页签。
4. 在**防御对象**页签，单击**新增网络对象**。
5. 在**新增网络对象**面板，参考以下表格配置网络对象参数。



配置项	说明
对象名称	输入网络对象的名称。
命名空间	选择或输入网络对象所在的命名空间。 **说明** 命令空间是集群的namesSpace，支持模糊匹配，例如：a*。
应用名称	选择或输入网络对象所属应用的名称。 **说明** 应用名称是集群中Tag为App的标签，支持模糊匹配，例如：a*。
镜像	选择或输入要防御的网络对象所使用的容器镜像。
标签	选择或输入要防御的容器组的。您可以选择多个标签。标签

6. 单击**确定**。
   新增的网络对象会出现在网络对象列表中。
   - 您可单击网络对象**操作**列的**编辑**或**删除**修改或删除该网络对象。

- 您也可以选中多个网络对象，然后单击下方的**批量删除**，批量删除网络对象。

> **说明** 网络对象没有应用在任何容器防火墙规则中时，才可以被删除。

后续步骤

创建了源网络对象和目的网络对象后，您可以在这两个网络对象之间创建访问流量防御规则，即设置对源网络访问目的网络的异常流量是放行、告警还是拦截。创建防御规则的具体操作，请参见创建防御规则。

4.3. 创建防御规则

您可以在两个网络对象之间创建访问流量的防御规则，实现对源网络对象访问目的网络对象的流量进行管控。本文介绍如何创建防御规则。

背景信息

容器防火墙的防御规则可以实现网络的隔离，它由一个源网络对象、一个目的网络对象、一组端口范围、一个过滤动作和规则优先级这五部分组成。

操作步骤

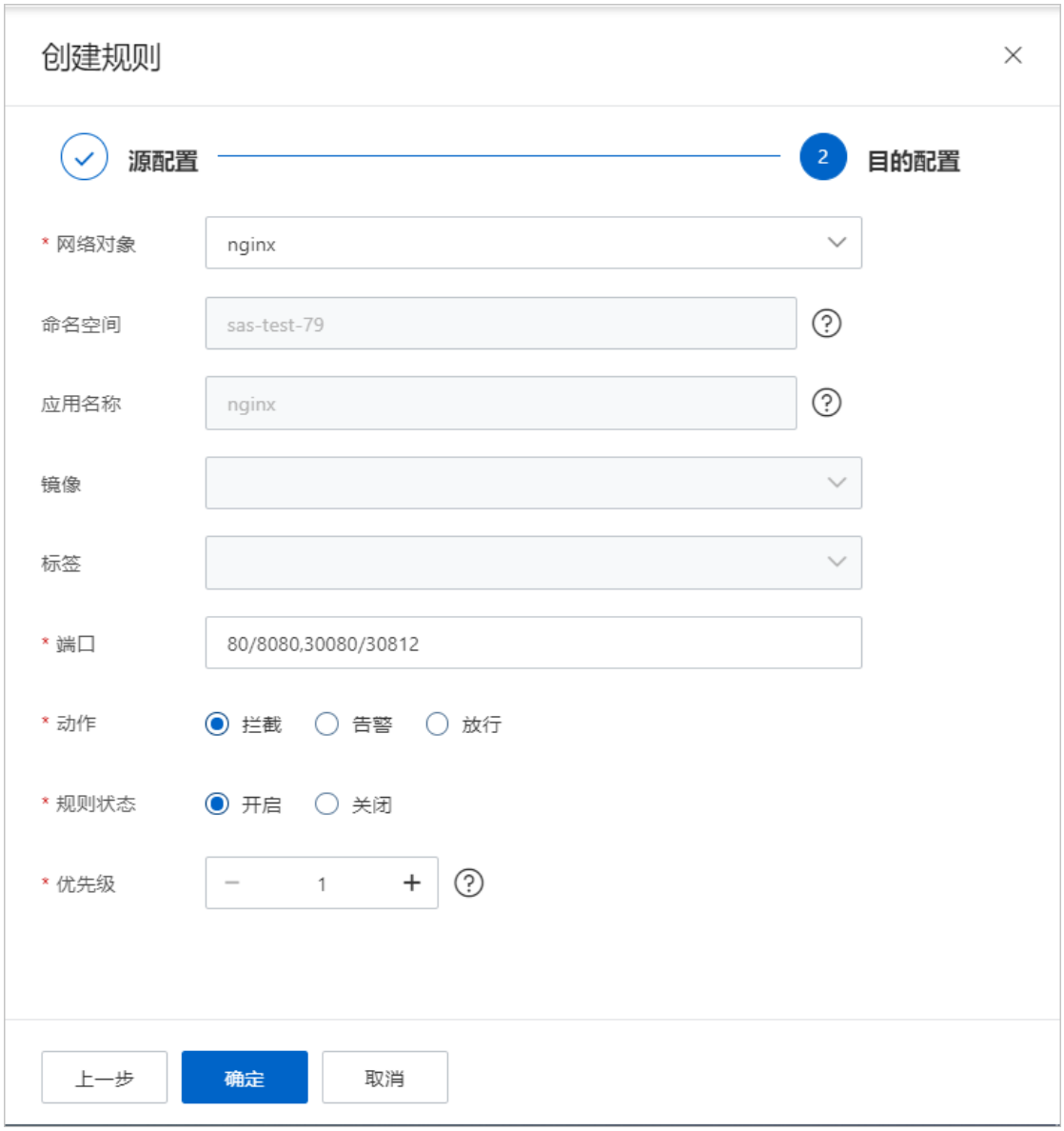
1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**防护管理**页签。
4. 在**防护管理**页签下的集群列表中，定位到要创建防御规则的集群，单击其**操作**列的**规则管理**。
5. 在**防御规则**面板上，单击**创建规则**。
6. 在**创建规则**面板上为该集群创建防御规则。
   i. 配置源网络对象。

      您需要进行以下配置：

      - 规则名称：为该防御规则设置名称。
      - 网络对象：选择源网络对象，即访问流量的来源。

   ii. 单击**下一步**。

   iii. 配置目的网络对象。



您需要进行以下配置：

配置项	说明
网络对象	选择访问流量的目的对象。
端口	输入访问的端口范围。 **说明** 最多支持设置8组端号范围，端号范围不可重复。多个端口范围使用半角逗号（,）隔开，例如：20/30,80/90。

配置项	说明
动作	选择规则的执行动作。取值： ■ **拦截**：对访问流量进行拦截。 ■ **告警**：对访问流量放行并进行告警。 ■ **放行**：对访问流量放行（不会告警）。
规则状态	防御规则的状态。取值： ■ **开启**：该防御规则创建成功后为生效状态。 ■ **关闭**：该防御规则创建成功后为不生效状态。
优先级	设置该防御规则的优先级。优先级为1~1000，数字越小优先级越高。

7. 单击**确定**。
   新创建的防御规则会展示在防御规则列表中，并按照优先级由高到低的顺序排列。新建的防御规则默认为关闭状态，您需要开启防御规则，规则才会生效。开启防护规则的具体操作，请参见防御状态与规则管理。
   防御规则启用后，该集群的防御规则会按照您新建防御规则时设置的优先级顺序依次执行。

   > **说明** 如果防御规则列表中的第一条规则未命中，则继续尝试匹配规则列表中的第二条规则，直到命中规则后，按规则中的动作来执行。如果没有命中任何规则，容器防火墙会执行放行的动作。

4.4. 防御状态与规则管理

创建防御规则后，您可以对集群防御状态进行开启或关闭，也可对该集群下的防御规则进行启用、停用、编辑等操作。如果您的业务已不再需要某个防御策略，您可以删除该防御策略。本文介绍如何对集群的防御规则进行启用、停用、编辑和删除。

前提条件

已为该集群创建了防御规则。创建防御规则的具体操作，请参见创建防御规则。

背景信息

集群防御规则的可拦截状态为正常时，该集群的防御规则才能生效。如果集群防御规则的可拦截状态异常，您需要及时处理该异常状态。更多信息，请参见集群防御规则可拦截状态异常排查。

防御状态管理

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**防护管理**页签。
4. 在**防护管理**页签下的集群列表中，定位到要管理防御状态的集群，对该集群的**防御状态**进行管理。

   单击目标防御规则**防御状态**列的  图标，开启或关闭该集群的防御状态。您也可以选中多个集群，单击下方的**批量开启**或**批量关闭**，对多个集群防御状态进行管理。

> **注意** 只有集群防御规则的**可拦截状态**显示为**正常**，该集群的防御规则才能正常开启。如果集群的防御规则的**可拦截状态**显示为**异常**或**正常待确认**，该集群的防御规则无法开启。**可拦截状态**异常问题处理，请参见集群防御规则可拦截状态异常排查。

防御规则管理

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**防护管理**页签。
4. 在**防护管理**页签下的集群列表中，定位到要管理防御规则的集群，对该集群下的防御规则进行管理。
   i. 单击目标集群**操作**列的**规则管理**，展开**防御规则**面板。
   ii. 在**防御规则**面板上的集群防御规则列表中，定位到要管理的防御规则。
   - 开启或关闭规则
     单击目标防御规则**启用状态**列的图标，开启或关闭该防御规则。
     选中多个防御规则，单击列表下方的**批量开启**或**批量关闭**，对多个防御规则进行批量开启或关闭
   - 查看规则详情
     单击**操作**列的**详情**展开规则**详情**面板，查看该规则的源网络对象、目的网络对象以及规则的详情。
   - 编辑规则
     单击**操作**列的**编辑**展开**编辑规则**面板，对该规则进行修改。

     > **说明** 集群防御规则修改最长需要1分钟生效。

   - 删除规则
     单击目标防御规则**操作**列的**删除**，删除改规则。
     选中多个防御规则，单击列表下方的**批量删除**，对多个防御规则进行批量删除操作。

     > **说明** 集群防御规则删除最长需要1分钟生效。

4.5. 查看防护状态

防御规则创建并启用后，该防御规则开始对访问该集群的流量进行放行、告警和拦截的防御动作。您可以通过防护状态功能查看触发防御规则产生的告警事件。本文介绍如何查看容器防火墙的防护状态。

背景信息

防护状态功能页签下只展示告警或拦截的防御动作产生的告警事件。如果防御规则动作为放行，则不会产生告警事件。

操作步骤

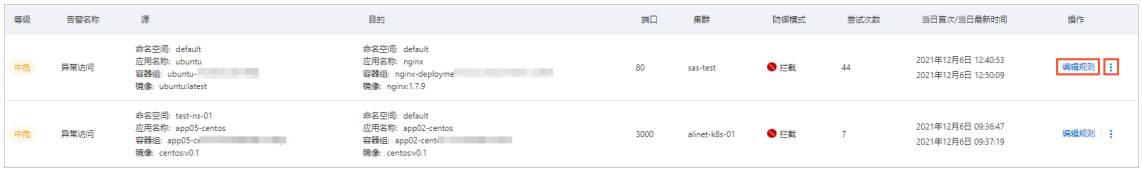
1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**防护状态**页签。
4. 在**防护状态**页签下，查看容器防火墙的防护状态。

防护状态页签分为防御总览和告警事件列表两个区域。

- 防御总览
  防御总览区域为您展示**最近24小时风险数**、**最近30天风险数**、**最近180天风险数**、**未防护集群/总集群数** 、**规则总数**。

- 告警事件列表
  防御列表中按照防御规则触发的时间由近到远，为您展示已触发防御规则（规则执行动作为告警和拦截）的告警事件。相同源容器组、目的容器组、端口号和集群的告警事件，按自然天被归类为一条告警事件，多次告警在**尝试次数**列累计尝试访问的次数。
  您可单击告警事件操作列的**编辑规则**对该告警事件的防御规则进行修改。您也可以单击**编辑规则**右侧的 ⋮ 修改该告警事件对应防御规则执行的动作。

> **说明** 防御规则修改最长需要1分钟生效。



4.6. 集群防御规则可拦截状态异常排查

当集群防御规则的可拦截状态为异常或正常待确认时，该集群防御规则无法对访问该集群的异常流量进行告警或者拦截。本文介绍如何处理集群防御规则的可拦截状态为异常或正常待确认的问题。

前提条件

已为该集群创建了防御规则。创建防御规则的具体操作，请参见创建防御规则。

背景信息

集群防御规则的正常运行依赖于云安全中心的AliNet插件（AliNet插件主要用于网络连接拦截、DNS拦截、暴力破解拦截），只有AliNet插件的安装状态为已安装、在线状态为在线，集群防御规则才能正常运行。使用容器防火墙功能前，请确保集群节点的系统内核版本在AliNet插件支持系统内核版本范围内。详细信息，请参见支持的操作系统版本。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 容器防火墙**。
3. 在**容器防火墙**页面，单击**防护管理**页签。
4. 在**防护管理**页签下的集群列表中，定位到防御规则的可拦截状态为**异常**或**正常待确认**的集群，针对不同的异常状态按照以下方案进行处理。
   - 异常

集群防御规则的**可拦截状态**为**异常**时，会导致**防御状态**开关关闭，云安全中心无法为该集群提供防火墙服务。
您可以单击**异常**右侧的**查看**展开**防护插件状态**面板，在**防护插件状态**面板上，查看AliNet插件的**安装状态**和**在线状态**。AliNet插件的**安装状态**、**在线状态**的异常，会导致集群防御规则的**可拦截状态**发生异常。请按照以下方案处理AliNet插件的**安装状态**、**在线状态**的异常：

- 如果**防护插件状态**面板的**安装状态**列显示某个集群节点未安装AliNet插件，或者**在线状态**列显示某个集群节点的AliNet插件不在线，您可以尝试为该集群重新开启恶意网络行为防御功能来解决。关于如何开启恶意网络行为防御，请参见主动防御。
- 如果已为该集群开启了恶意网络行为防御功能，但**防护插件状态**面板的**安装状态**列仍然显示该集群节点为未安装AliNet插件，则可能是该集群节点的操作系统的内核不支持安装AliNet插件。支持安装AliNet插件的集群节点的操作系统内核版本，请参见支持的操作系统版本。
  您也可以登录集群执行以下命令，查看AliNet插件的安装日志。如果集群节点操作系统的内核不支持安装AliNet插件，则安装日志中会有`install,driver file not exist`的提示。

  ```
  cat /usr/local/aegis/PythonLoader/data/AliNet_config.log
  ```

- 正常待确认
  集群防御规则的**可拦截状态**为**正常待确认**时，表明您已处理了导致集群防御规则的**可拦截状态**为**异常**的问题，但还需要您确认该集群的所有防御规则是否存在问题（如防御规则的**启用状态**是否开启、防御规则**优先级**顺序是否合理等）。
  在确保集群的所有防御规则无误后，在集群防御规则的**可拦截状态**列，单击**正常待确认**右侧的**恢复**，即可将该集群防御规则的**可拦截状态**恢复为**正常**状态。

5.恶意行为防御

云安全中心提供恶意行为防御功能。您可以根据业务需要启用、停用某个系统防御规则以及管理该规则中的资产。本文介绍如何使用恶意行为防御功能。

版本限制说明

仅云安全中心的高级版、企业版、旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

应用场景

- 选用适合业务场景的系统防御规则
  如果在日常业务场景当中，您发现某个系统防御规则不适合您的业务场景，并且会影响您资产的安全得分，您可以停用该系统防御规则。具体操作，请参见管理系统防御规则。
- 处理误报的安全告警事件
  在处理告警类型为**精准防御**的告警事件时，如果您发现云安全中心的系统防御规则检测出的安全告警事件，在经过您识别后为正常的业务进程，您可以在**恶意行为防御**页面的**系统防御规则**页签下关闭该系统防御规则，或者将告警事件中的受影响服务器，从系统防御规则防御的资产的列表中移除。具体操作，请参见处理误报的安全告警事件。

管理系统防御规则

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**主动防御 > 恶意行为防御**。
3. 在**恶意行为防御**页面，单击**系统防御规则**页签。
4. 在**系统防御规则**列表中，查找目标系统防御规则。
   - 在**系统防御规则**页签的搜索框中，输入系统防御规则的名称，快速查找目标系统防御规则。
   - 在**系统防御规则**页签的左侧的**ATT&CK攻击阶段**菜单中，通过告警的**ATT&CK攻击阶段**筛选目标系统防御规则。
5. 管理系统防御规则。
   - **启用或停用规则**

     > **注意** 停用某个系统防御规则后，云安全中心将不会检测并上报该规则对应的安全风险，并且**安全告警处理**页面的告警列表中也不会再显示与该规则相关的告警事件。请您谨慎操作。

     a. 选中（支持多选）目标规则。
     b. 单击规则列表下方的**启用**或**停用**。
   - **管理主机**

     > **注意** 将资产从规则中移除后，该资产将不会再受到此系统防御规则的防护。请您谨慎操作。

     a. 选中要管理的系统防御规则。
     b. 单击**操作**列的**管理主机**。
     c. 在**主机管理**面板上，添加或删除该规则防御的资产。
     d. 单击**确定**。

处理误报的安全告警事件

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**威胁检测 > 安全告警处理**。
3. 在**安全告警处理**页面，单击**精准防御**下方的数字。

4. 在下方的告警事件列表中，定位到误报的安全告警事件，单击**操作**列的**详情**，查看告警事件的详情。

   以下以处理告警名称为**可疑蠕虫脚本行为**的告警事件为例，为您介绍如何处理误报的安全告警事件。在告警详情面板上，您需要获取并记录以下信息，用于后续处理该告警事件。
   - 记录检测并上报该告警事件的系统防御规则的名称。本案例中为**可疑蠕虫脚本行为**。
   - 记录该告警事件的**ATT&CK攻击阶段**。本案例中为**影响破坏**。
   - 记录受该告警事件影响的资产的名称和IP。

5. 在云安全中心控制台左侧导航栏，单击**恶意行为防御**。
6. 在系统防御规则列表中，查找检测上报该告警事件的系统防御规则。
   - 您可以在恶意搜索框中输入规则名称**可疑蠕虫脚本行为**查找系统防御规则。
   - 您也可以在左侧的**ATT&CK攻击阶段**菜单中，单击**影响破坏**查找系统防御规则。
7. 在系统防御规则列表中定位到规则名称为**可疑蠕虫脚本行为**，管理该系统防御规则。
   - 如果该系统防御规则不适合您的业务场景，您不想云安全中心再上报这个系统防御规则检测出的安全告警事件，您可以单击该规则**开关**列的 图标，关闭该系统防御规则。

> **注意** 关闭某个系统防御规则后，云安全中心将不会检测并上报该规则对应的安全风险到**安全告警处理**页面的告警列表中，请您谨慎操作。

- 如果您仅想处理这一个误报的安全告警事件，您可以单击**操作**列的**管理主机**，将受该告警事件影响的资产从该系统规则防御的资产列表中移除即可。
  您也可以**在安全告警处理**页面，单击误报的安全告警事件**操作**列的**处理**，在告警处理对话框中，处理方式选中**关闭恶意行为防御**，单击**立即处理**。告警事件处理完成后，受该告警事件影响的资产，也会从系统防御规则防御的资产列表中移除。

  > **注意** 如果您仅想处理该系统防御规则上报的这一次安全告警事件，并且后续还需要云安全中心的系统防御规则继续防护该资产，您可以在恶意行为防御页面的系统防御规则中，将该资产添加回规则防御的资产列表中。

6.容器主动防御

6.1. 概述

云安全中心的容器主动防御功能可在该集群内使用镜像创建资源时，对镜像进行安全风险校验，对命中容器主动防御策略的镜像执行拦截、告警或放行动作，确保集群内启动的镜像符合您的安全要求。

版本限制说明

仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

容器主动防御的原理

为集群创建容器防御策略之后，当您在该集群内使用镜像创建资源时（如创建Pod），会触发安全风险校验请求至云安全中心，云安全中心会按照该集群的容器主动防御策略，对该镜像进行安全风险校验，校验该镜像是否存在漏洞风险、基线风险和恶意样本，对命中容器主动防御策略的镜像，云安全中心会对其执行告警、拦截或放行的操作，并且会产生一条关于该镜像安全风险校验结果的告警事件。

关于容器主动防御功能的配置和使用的具体操作，请参见创建防御策略、管理防御策略、查看和处理告警事件。

支持的容器服务ACK的集群类型

容器主动防御功能目前仅支持容器服务ACK的部分集群类型，具体支持的集群类型如下表。

容器服务ACK的集群类型	是否支持
ACK托管版集群	支持
ACK专有版集群	支持
ASK集群	不支持
ACK边缘托管版集群	不支持
注册集群	不支持

6.2. 创建防御策略

云安全中心提供的容器主动防御功能，可在集群内的镜像启动时，对该镜像进行安全风险校验。您可为集群创建防御策略，对命中防御策略的镜像执行告警、拦截和放行，以确保集群运行的镜像符合您的安全要求。本文介绍如何为集群创建主动防御策略。

前提条件

创建防御策略前，请确保已在容器服务ACK控制台安装安全策略治理组件policy-template-controller。详细信息，请参见安装策略治理组件。

版本限制说明

仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

创建策略

> **说明** 每个集群最多支持创建40个防御策略。

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。
3. 在**策略**页签左侧的集群列表中，单击要创建防御策略的集群的名称。
4. 单击**新建策略**，展开**新建策略**面板。
5. 在**新建策略**面板上，进行策略配置。

   配置项说明如下：

配置项	说明
策略模版	选择策略的模板。您可以选择空白模板创建一组自定义配置项，也可以选用包含一组预定义风险配置项的模板。
未扫描镜像	选择是否支持未使用云安全中心镜像扫描功能进行扫描的镜像的启动。 **说明** 该配置项能够帮助您确认策略范围内运行的镜像均通过安全扫描。开启该配置项时，建议先配置规则动作为**告警**。如有更严格的安全管控需求，可先观察一段时间内的告警事件，确认该策略不会影响业务部署需求后再切换为**拦截**。
互联网恶意镜像	选择是否支持拦截互联网传播的恶意镜像启动，如从公开镜像仓库下载的恶意镜像或从Dockerhub公开仓库拉取的包含后门木马等恶意程序的镜像等。

配置项	说明
告警策略	告警策略的配置包含以下三类配置项： ○ 基线 ○ 漏洞 ○ 恶意样本 您可以按照您的业务需要，分别配置基线、漏洞和恶意样本的策略。 注意 ○ 如果您同时配置了多个配置项，则任意一项配置命中后，云安全中心会立即执行规则动作，不会继续匹配其他配置项。策略匹配的顺序依次为：互联网恶意镜像、未扫描镜像、恶意样本、基线、漏洞。 ○ 每一类配置项的可选条件之间为“或”的关系。例如漏洞配置中，如果您配置风险等级为**高危**，并指定了一些具体的CVEID，那么只要启动的镜像包含高危漏洞，或者包含您指定的CVEID漏洞，则会命中该策略。
策略名称	填写策略的名称。
策略描述	填写策略的描述。
命名空间	选择镜像启动的命名空间，支持多选。
镜像	选择镜像，支持多选。
标签	选择镜像的标签，支持多选。
规则动作	选择策略执行的动作。取值： ○ **告警**：镜像启动后，会产生一条**规则动作**为**告警**的告警事件。 ○ **拦截**：镜像启动时，符合策略的镜像将被阻止启动，并且会产生一条**规则动作**为**拦截**的告警事件。 ○ **放行**：镜像启动后，会产生一条**规则动作**为**放行**的告警事件。

配置项	说明
加白名单	填写需要加入白名单的镜像名。白名单最多可设置20个。 支持填写部分关键字进行模糊匹配。以镜像地址yundun-example-registry.cn-hangzhou.aliyuncs.com/yundun-example/yun-repo:test为例，您可以填写部分关键字进行模糊匹配。以下白名单配置方式均有效： ○ yun-repo ○ test ○ yun-repo:test ○ repo:test 注意 将镜像加入策略白名单后，该镜像的启动时，云安全中心将不会对该镜像进行安全风险的校验动作，请您谨慎操作。

6. 单击**确定**。
   策略创建成功后，云安全中心将在镜像启动时，按照策略内容对该镜像进行安全风险校验，并将校验结果生成一条告警事件展示在告警列表中。

通过复制的方式创建策略

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。
3. 在**策略**页签左侧的集群列表中，单击要创建防御策略的集群的名称。
4. 在策略列表中，单击已有策略**操作**列的**复制**，展开**复制策略**面板。
5. 在**复制策略**策略面板上，根据您的业务需要修改策略的配置。
6. 单击**确定**。
   策略创建成功后，云安全中心将在镜像启动时，按照策略内容对该镜像进行安全风险校验，并将校验结果生成一条告警事件展示在告警列表中。

后续步骤

策略创建后，您可以根据您的业务需要，对该策略进行编辑或删除。具体操作，请参见管理防御策略。

6.3. 管理防御策略

防御策略创建成功后，您可以根据业务需要编辑策略内容。如果某个策略不再需要，您也可以删除该策略。本文介绍如何编辑、删除防御策略。

前提条件

已创建防御策略。创建防御策略的具体操作，请参见创建防御策略。

编辑策略

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。

3. 在**策略**页签左侧的集群列表中，单击要创建防御策略的集群的名称。
4. 在策略列表中，单击已有策略**操作**列的**编辑**，展开**编辑策略**面板。
5. 在**编辑策略**策略面板上，根据您的业务需要修改策略的配置。
6. 单击**确定**。
   策略修改后，云安全中心将按照修改后的策略在镜像启动时，按照策略内容对该镜像进行安全风险校验，并将校验结果生成一条告警事件展示在告警列表中。

删除策略

> **注意** 删除容器主动防御策略后，镜像启动时，云安全中心将不会对该镜像进行安全风险校验，为了您的容器运行安全，请您谨慎操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。
3. 在**策略**页签左侧的集群列表中，单击要创建防御策略的集群的名称。
4. 在策略列表中，单击已有策略**操作**列的**删除**。
5. 在**确定删除策略**对话框中，单击**确认删除**。
6. 单击**确定**。

6.4. 查看和处理告警事件

您可以在容器主动防御页面的告警页签下，查看启动镜像的集群命中防御策略产生的告警事件。为保障您容器的安全运行，建议您及时查看和处理云安全中心上报的告警事件。本文介绍如何查看和处理告警事件。

前提条件

已创建防御策略。创建防御策略的具体操作，请参见创建防御策略。

查看告警事件

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。
3. 在**告警**页签下，查看告警数据。

   告警页签下分为**防御趋势**、**风险集群TOP 10**和**策略告警检测**三个区域。

   - 在**防御趋势**区域，您可以通过防御趋势图表，查看所有配置了容器主动防御策略的集群近期的防御趋势。
   - 在**风险集群TOP 10**区域，您可以查看容器主动防御策略触发量TOP 10的集群。
   - 在**策略告警检测**区域，您可以查看告警的详细信息。告警的详细信息中包括策略的信息和镜像的信息。
     - 在告警列表中，单击**镜像**列的镜像名称，可以跳转该镜像的镜像详情页面。您可以在镜像详情页面，查看并处理镜像中存在的安全风险。

       > **说明** 仅已接入云安全中心的镜像，单击镜像名称才可以跳转到镜像详情页面。镜像接入云安全中心的具体操作，请参见接入镜像仓库。

- 在告警列表中，将鼠标悬停在**规则动作**列的图标上，在弹出的对话框中，您可以查看该镜像在进行安全风险校验时，命中的容器主动防御的告警策略的详细信息。

  > **注意** 在上述对话框中，仅展示该镜像在进行安全风险校验时，命中的一个安全风险的信息。如果您想成功启动该镜像，您需要处理该镜像中存在的其他安全风险问题，以免该镜像再次启动时，再次命中防御策略，再次被拦截无法成功启动。具体操作，请参见处理告警事件。

- 在告警列表中，单击**操作**列的**策略变更**，可以快捷地变更策略的**规则动作**。

处理告警事件

1. 登录云安全中心控制台。
2. 在左侧导航栏选择**主动防御 > 容器主动防御**。
3. 在**告警**页签下，单击目标告警事件的**镜像**列的镜像名称，跳转该镜像的镜像详情页面。

   仅已接入云安全中心的镜像，单击镜像名称才可以跳转到镜像详情页面。镜像接入云安全中心的具体操作，请参见接入镜像仓库。
4. 在镜像详情页面，处理镜像中存在的安全风险。

   您需要在镜像详情页面的**镜像系统漏洞**、**镜像应用漏洞**、**镜像基线检查**及**镜像恶意样本**这4个页签下，将与该镜像所在集群的容器主动防御策略相关的风险问题全部都处理后，才能确保再次启动镜像不会被拦截或当前已运行的容器不存在安全风险问题。

7.常见问题

本文汇总了云安全中心防勒索、病毒防御、网页防篡改和应用白名单功能的常见问题。

- **防勒索问题**
  - 怎么购买防勒索容量？
  - 防勒索是什么功能？为什么要单独付费？
  - 云安全中心防勒索功能和阿里云混合云备份服务有什么关系？
  - 购买防勒索数据保护容量后数据备份会自动启动吗？
  - 防勒索备份缓存占用磁盘空间较大，如何清理？
  - 防勒索备份缓存数据占用了服务器过多的C盘空间，我能修改缓存数据的位置吗？
  - 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？
- **病毒防御问题**
  - 购买病毒防御后，之前购买的其他服务是否受影响？
  - 怎么使用云安全中心病毒防御功能？
- **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，提示“防护模块初始化失败，请检查是否存在其他软件对创建服务进行了拦截管控”？
  - 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？
  - 为什么开启了防篡改，SSH登录并修改了受保护的文件，却没有见到告警提示？
  - 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？
- **容器防火墙问题**
  - 目前我使用的是云安全中心的企业版，是否能使用容器防火墙功能？
  - 使用容器防火墙功能否需要额外付费？
  - 如果升级到了云安全中心旗舰版，是否就只能保护容器，而无法保护ECS了？

怎么购买防勒索容量？

云安全中心免费版用户，可以在云安全中心购买页购买云安全中心防病毒版、高级版、企业版或旗舰版的同时购买防勒索容量。您也可以选择仅采购增值服务并购买防勒索容量。具体操作，请参见开通服务。

防病毒版、高级版、企业版或旗舰版用户可以通过升级功能来购买防勒索容量。具体操作，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。

防勒索是什么功能？为什么要单独付费？

防勒索是云安全中心新发布的功能，包含防勒索。防勒索病毒进行数据备份使用的存储容量需要单独付费。

防病毒版、高级版、企业版或旗舰版用户可以通过升级功能来购买防勒索容量。具体操作，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。
防勒索功能支持一键恢复被勒索病毒加密的文件，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50 GB的防勒索保护空间，每台服务器仅需2.25 USD/月。

云安全中心防勒索功能和阿里云混合云备份服务有什么关系？

云安全中心防勒索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，在您购买了防勒索容量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。

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。

如何查看已购买的防勒索容量和防勒索容量的使用情况？

开通防勒索服务后，您可以在**主动防御 > 防勒索**的**防勒索**页面，查看您已购买的防勒索容量及防勒索容量的使用情况。

防勒索备份缓存占用磁盘空间较大，如何清理？

防勒索功能备份数据时，为了提高数据备份速度，默认会占用您服务器上的磁盘空间进行数据缓存备份。如果发现您服务器*C:\Program Files (x86)\Alibaba\Aegis\hbr\cache*（Windows服务器）或*/usr/local/aegis/hbr/cache*（Linux服务器）路径下占用的磁盘空间较大，您可以清理上述路径下的缓存文件。具体操作，请参见清理磁盘空间。

防勒索备份缓存数据占用了服务器过多的C盘空间，我能修改缓存数据的位置吗？

可以。

您可以通过修改防勒索备份客户端的配置文件修改防勒索备份缓存数据的位置。具体操作，请参见修改备份缓存的位置、状态及占用系统内存空间的上限。

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08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08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08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。详细操作步骤如下：

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。快照必须对整个磁盘空间进行备份，不支持选择需要打快照的文件。快照按照0.02 USD/GB/月收费。更多信息，请参见快照计费。
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。防勒索支持文件级别的防护，按照您的实际使用量来收取数据备份费用，您无需支持整个磁盘的备份费用。更多信息，请参见计费方式。

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。您可通过扩容或释放防勒索容量空间来解决。

- 扩容防勒索容量空间
  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。您可以在云安全中心控制台选择**主动防御 > 防勒索**，在**防勒索**页面，单击**已使用容量/总容量**下的**升级**，扩容防勒索容量空间。

  > **说明** 建议每台服务器配置50 GB的数据防护容量。

- 释放防勒索容量空间
  - 减少服务器
    您可以通过删除防护策略下的非生产状态服务器（如测试服务器、闲置服务器等），节约防勒索容量空间。具体操作，请参见管理防护策略中的服务器。
  - 减少防护目录
    您可以在创建防护策略时，选择**自定义策略**，通过备份指定目录，节约防勒索容量空间。具体操作，请参见创建防护策略。
  - 删除历史备份数据
    如果您确认某个服务器上的历史备份数据已没有保留的必要，您可以将该服务器已备份的历史数据删除来释放防勒索容量空间。具体操作，请参见删除已备份数据。

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**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**。

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针对勒索病毒、挖矿程序等持久化 、顽固型病毒提供的病毒扫描、告警和深度查杀能力。不会影响已购买的其他服务。

怎么使用云安全中心病毒防御功能？

针对勒索病毒云安全中心提供以下功能：

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？

支持。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？

支持。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，提示“防护模块初始化失败，请检查是否存在其他软件对创建服务进行了拦截管控”？

网页防篡改启动时显示异常，并提示“防护模块初始化失败，请检查是否存在其他软件对创建服务进行了拦截管控”，表示云安全中心防篡改程序被您服务器中的其他安全软件拦截了。

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。

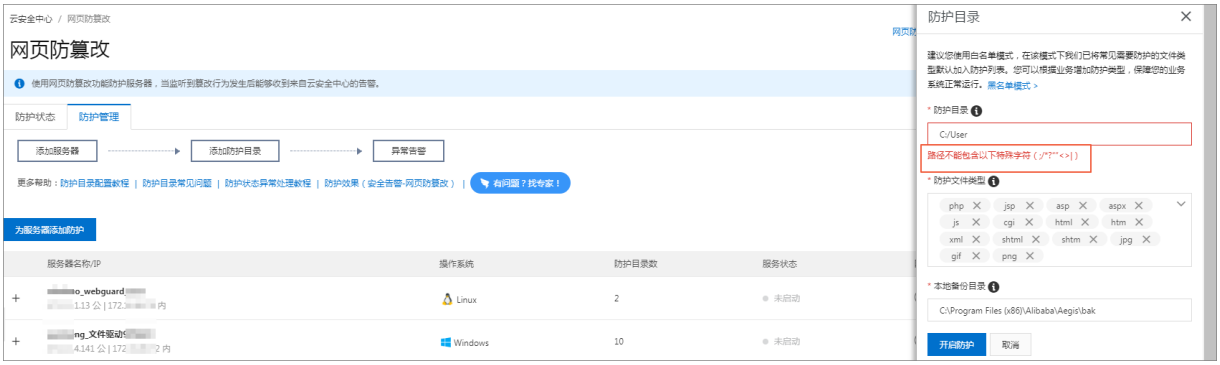
网页防篡改本地备份目录有什么要求？

网页防篡改本地备份目录是指将您网站文件（即防篡改防护目录下的文件）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（\），例如 `C:\Program Files\Common Files` 。



> **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：

- 需要防护的文件是否已添加到了防护目录中。
- 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。
- 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**页签中，查看目标服务器的服务状态，如果服务状态显示为**异常**，建议您重试；如果服务器状态为**已离线**，建议您为该服务器重新安装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。

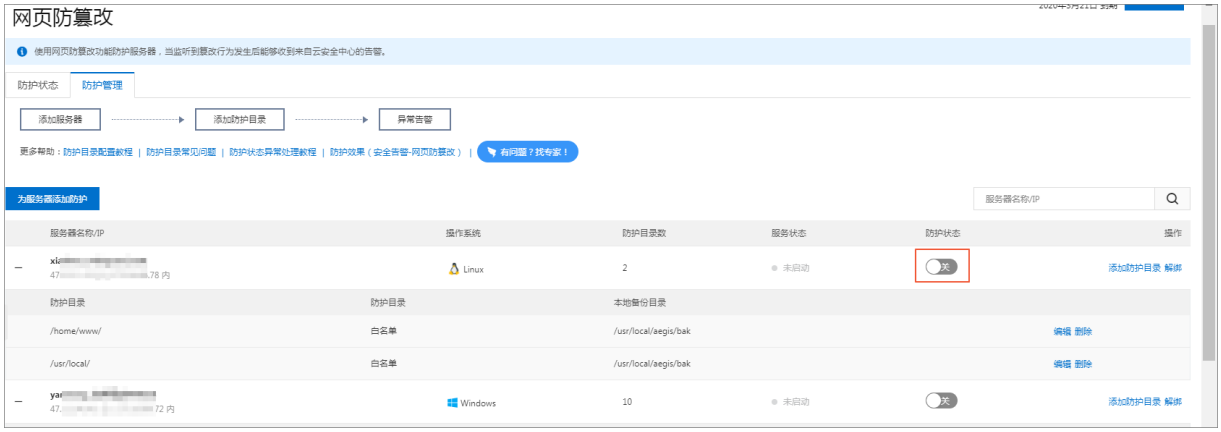
配置了防护目录后还可以对该防护目录写入文件吗？

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，请参考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？。

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。



为什么开启了防篡改，SSH登录并修改了受保护的文件，却没有见到告警提示？

如果您已为某台服务器开启了防篡改防护，并将需要防护的文件目录添加到了防篡改防护目录中，您通过SSH登录该服务器后对该防护目录中的文件进行了修改，但是在云安全中心控制台**网页防篡改**页面没有看到告警信息，提示该文件有改动，可能是以下原因：

- **防护状态**开关未开启。
- **防护状态**开关已开启后修改了防护目录配置，但是修改完成后没有重启**防护状态**开关。
- 该文件已添加到了白名单中。
  防篡改白名单中的文件默认是可信的，防篡改功能不会对白名单文件的修改进行告警或拦截。相关内容，请参见加入白名单。

- 该服务器内核不在防篡改支持的范围内。
  服务器防护目录中的文件修改时，防篡改功能会直接对该文件改动进行拦截，不告警。

  > **说明** 您在服务器中修改文件并保存后，返回云安全中心控制台**网页防篡改**页面时，可以看到**已处理**列表中，该文件已被防篡改功能拦截。然后再回到服务器中查看该文件，会发现之前的修改并未保存成功。

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** 网页防篡改支持将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。更多信息，请参见加入白名单。

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。

目前我使用的是云安全中心的企业版，是否能使用容器防火墙功能？

不可以。仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

使用容器防火墙功能否需要额外付费？

不需要。开通了云安全中心旗舰版后，即可直接使用容器防火墙功能。

如果升级到了云安全中心旗舰版，是否就只能保护容器，而无法保护ECS了？

不会。云安全中心会同时防护容器和ECS。