ALIBABA CLOUD

阿里云

云安全中心（态势感知）

安全运营

文档版本：20201120

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.安全报告

云安全中心高级版和企业版支持安全报告功能，支持对安全报告进行自定义配置。您可以通过自定义报告内容、报告展示的数据类型和接收人邮箱地址，实现安全报告的自定义，更好地满足您对于您资产安全状况数据的需求。本文档介绍如何创建安全报告。

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 > 安全报告**。
3. 在**安全报告**页面，单击**创建新报告**。

   > **注意** 云安全中心除默认已创建的安全日报，最多支持创建9个安全报告。

   

4. 在**设置报告基础信息**页签中，配置安全报告的基本信息。

   

   您可以参考以下说明配置安全报告参数：
   - **报告名称**：手动输入安全报告的名称。
   - **报告类型**：单击下拉框选择创建报告的类型，可选*日报*、*周报*、*月报*和*自定义周期*报告。

     如果选择*自定义周期*，您需要在**统计周期**中选择该自定义安全报告统计的周期。

     

   - **报告发送时间**：单击下拉列表，选择报告每天、每周一或每月一号发送的时间，可选*00:00~6:00*、*6:00~12:00*、*12:00~18:00*和*18:00~24:00*。
   - **报告邮件接收人**：手动输入接收报告的邮箱地址，可输入多个邮箱地址。
5. 单击**下一步**。
6. 在**设置报告内容**页签中，选中需要在报告中展示的数据，可以选择资产、告警、漏洞、基线、攻击、安全运营相关统计数据。

   
7. 单击右下角**保存报告内容**，完成报告的创建。
   您可在**安全报告**页面查看到您新建的报告。

   

相关操作

您可以根据需要执行以下操作：

- 报告完成创建后，默认启用。云安全中心会在您设置的**报告发送时间**内，向您添加的报告邮箱地址中发送该安全报告。如果您后续不再需要接收该报告，可在该报告页面单击**启用**按钮，关闭该报告的发送。
- 云安全中心会默认创建一个安全日报。仅支持对该日报进行编辑和克隆，您可以修改该日报的基础信息和报告内容。 对于其他您创建的安全报告，您可以进行编辑、克隆和删除操作。

> **说明** 云安全中心默认创建的安全日报的**报告类型**为**日报**，修改该安全报告的基础信息时不支持修改其**报告类型**。

- 完成自定义周期的安全报告创建后，您可单击**立即发送**，发送自定义周期内的安全报告内容至报告邮件收件人。
- 安全报告支持通过筛选报告启用状态、报告类型或输入报告名称搜索定位到相关安全报告。

2.任务中心

2.1. 任务中心概述

任务中心提供自动化响应编排能力，将安全事件响应过程中重复性的任务逻辑编排成自动化处置策略，帮助您高效地进行系统安全加固。您创建自动化任务后，任务中心会在您选择的资产上自动化批量执行该任务。本文介绍了任务中心的策略模板和任务管理等模块提供的功能。

背景信息

云安全中心仅有企业版支持任务中心功能。

> **说明** 目前，任务中心仅支持漏洞自动化修复，后续会逐步开放更多自动化任务类型。

策略模板

策略模板页面展示了云安全中心提供的**漏洞自动化批量修复策略**模板。该策略支持多主机、自动化批量修复漏洞。在该页面，您可以基于已有模板快速创建策略。在操作栏单击**添加到我的策略**，可以创建一个新的策略并将该策略添加到**我的策略**页签中。

策略模板

我的策略

我的策略页面展示了所有已创建的自动化策略的信息，包括策略名称、类型、执行模式、创建时间、最近更新时间。在该页面，您可以在已有策略模板下创建任务 。更多信息，请参见创建任务。

我的策略

任务管理

任务管理页面展示了所有已创建任务的信息，包括任务名称、执行数、执行模式、创建时间、完成时间和进程状态。在此页面，您可以查看已有任务的详情。更多信息，请参见查看任务详情。

任务管理

2.2. 创建任务

任务中心可根据您添加的策略模板来快速创建自动化任务。创建任务后，该任务会在设置的任务执行时间开始时，对已选择的服务器资产自动化批量执行漏洞修复，帮助您提高系统安全加固的效率。本文档介绍如何创建任务。

前提条件

创建任务前，您必须先添加策略模板。

背景信息

任务中心的批量漏洞修复任务支持修复Linux漏洞、Windows漏洞和Web-CMS漏洞。

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 > 任务中心**。

3. 在**任务中心**页面单击**我的策略**页签。
4. 在**我的策略**页面，定位到需要创建任务的策略，单击操作栏**创建任务**。
5. 在**创建任务**页面，参考以下表格完成任务配置。

配置项	说明
任务名称	填写任务名称。
服务器资产列表	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当前任务的资产： ○ 在**服务器资产列表**中，选中**资产分组**模块中的分组，自动选中该分组下的所有资产。您可在右侧**资产**模块下，对已自动选中的资产取消选中。 ○ 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，您可选中需要执行自动化处理任务的资产。 **说明** 自动化任务仅处理在**资产**模块中选中的资产。
漏洞列表	漏洞列表展示了您在资产列表中已选择的资产中存在的漏洞。选择需要修复的漏洞。您可以单击**Linux软件漏洞**、**Windows系统漏洞**或**Web-CMS漏洞**页签，选择相应类型漏洞。 **说明** 您最多可以选择200个需要修复的漏洞。
通知配置	支持**钉钉机器人**和**邮件**两种通知方式。系统在任务执行完成后，通过您配置的通知方式向您发送通知。 以下是通知方式的配置方法： ○ **钉钉机器人**：选中需要发送通知的钉钉机器人。您也可单击**添加钉钉机器人**添加新的钉钉机器人。添加钉钉机器人的操作步骤，请参见配置钉钉机器人通知。 ○ **邮件**：输入您的邮箱地址。如果有多个邮箱地址请使用英文逗号（,）隔开。
执行时间	自动化任务执行的时间支持选择以下方式： ○ **立即执行**：创建任务后，设置的任务将立即执行。 ○ **自定义执行时间**：创建任务后，任务将在设置的**自定义执行时间**自动执行。

6. 单击**创建任务**。

执行结果

创建任务成功后，系统会提示**创建成功**，并自动跳转到**任务管理**页面。

后续步骤

任务执行完成后，您可在**任务管理**页面查看该任务详情。查看任务详情的操作步骤，请参见查看任务详情。

2.3. 查看任务详情

成功创建任务后，通过查看任务详情，您可以查看该任务的服务器资产列表、通知配置和其他信息。

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 > 任务中心**。
3. 在**任务中心**页面，单击**任务管理**页签。
4. 在任务列表中，单击目标任务操作栏的**详情**。
5. 在任务详情页面，查看**服务器资产列表**、**通知配置**和**其他**信息。 单击**服务器资产列表**、**通知配置**或**其他**页签可快速定位到对应模块。各模块的详细说明如下表所示。

模块	说明
服务器资产列表	展示当前漏洞修复任务相关的**资产**、**漏洞名称**和**最新扫描时间**。 
通知配置	当前任务的通知方式，包含**钉钉机器人**和**邮件**的详细配置。 
其他	当前任务执行的**日志记录**和**策略流程**信息。 ○ **日志记录**：记录任务执行的状态、进程总数、失败/成功进程数和各步骤执行的详细情况。 ○ **策略流程**：批量修复漏洞任务的流程图。 

3.荷鲁斯之眼Beta

荷鲁斯之眼为您提供云上资产全景、网络拓扑和安全态势的可视化界面。从安全评分、安全产品和云产品三个维度全面展示您资产的安全态势。

背景信息

荷鲁斯之眼提供云上资产安全态势全景、网络拓扑和安全风险处理入口，帮助您统一管控云上资产进行安全运营。

> **说明** 荷鲁斯之眼Beta为云安全中心企业版功能。基础版、基础杀毒版或高级版用户需升级到企业版，才能使用荷鲁斯之眼Beta的功能。有关升级的更多信息请参见升级与降配。

开通并访问荷鲁斯之眼

推荐使用最新版Chrome浏览器登录安全大屏。

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. 定位到**安全大屏**区域并单击**开通**。

   开通安全大屏
4. 在**变配**页面的**安全大屏**位置单击**是**。

   选择安全大屏配置
5. 选中**我已阅读并同意云安全中心服务协议**，并单击**立即购买**完成支付。
6. 返回云安全中心控制台页面，在左侧导航栏单击**安全运营 > 荷鲁斯之眼**。
   您会直接进入**荷鲁斯之眼**页面。在**荷鲁斯之眼**页面您可以查看您的资产安全全景和网络拓扑等信息，更多信息请参见荷鲁斯之眼介绍。

荷鲁斯之眼介绍

荷鲁斯之眼统一展示了您的云上资产、网络拓扑和安全态势。在**荷鲁斯之眼**页面您可以查看您资产的以下信息。

- **资产全景和网络拓扑**

  荷鲁斯之眼页面为您展示您所有区域下的资产安全态势和网络拓扑，您可以查看当前区域下的ECS实例、负载均衡实例、Nat网关实例等的安全态势。从网络拓扑中，您可以看到各ECS归属的VPC和互联网流量访问您的服务器所需要经过的安全防线。例如互联网流量先通过DNS解析，经过DDoS高防服务、Web应用防火墙和云防火墙三道安全防线，再经过负载均衡（SLB）均衡，流经Nat网关后才能访问您的ECS服务器。

  实例的不同颜色表示实例不同的安全风险等级，以下是实例颜色和安全风险等级的对应关系：

  - **红色**：表示该资产存在高安全风险。建议您尽快查看并处理相应风险。
  - **橙色**：表示该资产存在中安全风险。
  - **绿色**：表示该资产不存在安全风险。

  将鼠标移动到某个资产上方，可查看该资产的详细信息。包括资产ID、防护状态、公网IP、私网IP和检测出的告警、漏洞等信息。以下介绍相关图标的含义：

- ：告警标识。右侧数字为在该资产中检测出的告警数量。
- ：漏洞标识。右侧数字为在该资产中检测出的漏洞数量。
- ：基线检查风险项标识。右侧数字为在该资产中检测出的基线检查风险项数量。

查看单个资产详情

- **安全评分**

  安全评分区域展示您资产的安全分值。您可以单击**加固**处理您资产中检测出的安全风险问题。安全分值的详细内容请参见总览。如何提高资产的安全分值，请参见提高安全评分最佳实践。

  安全评分

- **安全产品**

  安全产品区域展示您已开通的阿里云安全产品数量和控制台的入口。您可以单击产品名称跳转至相应安全产品控制台。

- **云产品**

  云产品区域展示了您已开通的云产品的数量。支持您按照可用区查看云上资产的网络拓扑图，在左侧列表中单击**可用区**可查看该可用区的风险统计情况，单击具体可用区，即可查看对应可用区的资产网络拓扑图。单击云产品名称可查看该云产品的风险统计情况，单击具体资产名称可跳转至云安全中心该资产的详情页面。更多信息请参见查看单个资产详情。

  云产品

4.安全大屏

阿里云云安全中心基础杀毒版、高级版和企业版支持安全大屏，可从您资产的当前安全情况、外部攻击情况、威胁情况三个维度为您全面展现当前资产的网络安全态势。

背景信息

安全大屏将安全攻防数据转化并呈现到安全大屏上，秒级更新实时数据，可实时展现资产、漏洞、基线情况，帮助您一眼看清资产当前的安全状态；实时展现攻击来源、攻击分布、明确攻击者来源及攻击情况，帮助您建立安全防线，提升资产的整体防御能力；实时为您呈现告警概览并及时响应，帮助您构建实时威胁感知能力，将入侵损失降低到最小。

开通并访问安全大屏

推荐使用最新版Chrome浏览器登录安全大屏。

> **说明** 云安全中心安全大屏为**基础杀毒版**、**高级版**和**企业版**的增值服务，您可在购买页面选择安全大屏后查看大屏的实际价格。

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. 定位到**安全大屏**区域并单击**开通**。

   开通安全大屏
4. 在**变配**页面的**安全大屏**位置单击**是**。

   选择安全大屏配置
5. 选中**我已阅读并同意云安全中心服务协议**，并单击**立即购买**完成支付。
6. 返回控制台页面，在左侧导航栏单击**安全运营 > 安全大屏**。
7. 访问安全大屏页面。

   安全大屏

   支持以下两种访问方式：
   - **直接访问**：单击**直接访问**进入大屏页面。
   - **免登配置**：单击**免登配置**创建大屏免登地址，方便您在不登录云安全中心控制台的情况下直接通过免登链接打开安全大屏页面。

     5

     > **说明**
     > - 使用免登地址访问大屏前仍需先登录您的阿里云账号。
     > - 免登天数可设置为1~100天；最多可创建5个免登地址。

自定义当前大屏展示内容

云安全中心安全大屏支持展示您的资产、漏洞、基线、告警、安全运营、业务运营和云平台配置检查相关的数据。您可根据业务需要自定义安全大屏需要展示的内容。

1. 在**安全大屏**页面单击右上角 图标。
2. 在**内容配置**页面配置需要在大屏上显示的**标题文案**、**标题图片**、**标题装饰**和**监控URL**地址。

   8
3. （可选）单击**选择数据**页签并完成数据配置。 选中需要在大屏上实时展示的数据类型。您可以选中**全部**或单个数据分类。

   7
4. 单击**保存设置**。

大屏内容设置完成后，您可以在大屏页面看到根据您自定义设置展示的大屏内容。

自定义大屏场景

为满足不同业务领域展示不同场景数据的需要，安全大屏支持自定义场景。您可以根据业务的需要自定义多个不同的大屏场景。

1. 在**安全大屏**页面单击右上角 图标。
2. 在**场景列表**页面单击**新增场景**。

3. 在**内容配置**页面配置需要在大屏上显示的**标题文案**、**标题图片**、**标题装饰**和**监控URL**地址。

   8
4. 单击**选择数据**页签并完成数据配置。 选中需要在大屏上实时展示的数据类型。您可以选中**全部**或单个数据分类。

   7
5. 单击**保存设置**。

新增场景完成后，会默认启用该场景，您可以在大屏页面看到该场景的相关数据展示。

如果您需要展示其它场景，可在**场景列表**页面定位到需要展示的场景并单击**立即启用**。

> **说明** 安全大屏自定义场景不限数量。

攻击地域地图

云安全中心安全大屏正中间位置以动态方式展示了攻击地域地图，显示云安全中心检测到您资产受到的攻击来源方向、攻击来源地区、攻击来源IP地址和攻击次数等信息。

12

您可以选择查看中国或全球的攻击地域地图。

以下是攻击地域地图的相关信息：

- **实时安全态势**上方的数字表示您资产的安全评分分数。详细信息请参见安全评分。
- 红色动态球体表示攻击来源地区。
- 绿色动态球体表示受云安全中心保护的区域。
- 该区域会动态显示攻击来源IP地址、攻击次数和攻击来源所在的城市，您可以方便地查看攻击来源的相关

信息。

资产

资产区域展示了云安全中心检测到的资产统计信息。

13

资产区域包含以下信息：

- **总量**：您资产的总数量。
- **已失陷**：您资产中存在未处理的高危级别告警的服务器数量。状态符号为红色。
- **存在风险**：您资产中存在漏洞、基线和中低级别告警的服务器数量。状态符号为橙色。
- **安全**：您资产中不存在漏洞、基线风险和告警的服务器数量。状态符号为绿色。
- 存在安全风险情况最为严重的排名前5的资产及其状态。

漏洞

漏洞区域展示了您资产中漏洞的总数量、不同危险等级漏洞的环形占比图、需处理的漏洞类型和对应的数量、最近7天不同风险等级的漏洞的数据统计柱状图。

14

漏洞区域包含以下信息：

- **总量**：您资产中漏洞的总数量。
- **需紧急修复**：您资产中需立即修复的漏洞数量。状态符号为红色。
- **可延后修复**：您资产中可稍后再进行修复的漏洞总数量。状态符号为橙色。
- **暂可不修复**：您资产中暂时无法进行修复的漏洞数量。状态符号为灰色。
- 最近7天不同风险等级的漏洞的数据统计柱状图。

基线

基线区域展示了您资产中基线检查风险项的总数量、不同等级的基线风险项及其对应的数量、最近7天不同风险等级的基线风险项的数据统计柱状图。当天统计数据为实时数据。

15

基线区域包含以下信息：

- **总量**：您资产中基线风险项的总数量。
- **高危**：您资产中的高危基线风险项数量。状态符号为红色。建议立即进行排查和修复。详细内容请参见查看和处理基线检查结果。
- **中危**：您资产中的中危基线风险项数量。状态符号为橙色。
- **低危**：您资产中的低危基线风险项数量。状态符号为灰色。
- 最近7天不同危险等级的基线风险项的数据统计柱状图。

安全态势

安全态势区域展示了最近7天、15天或30天安全评分的趋势图。当天统计数据为实时数据。

16

安全运营

安全运营区域展示了最近7天、15天或30天内已处理的告警（红色状态符号表示）、已处理漏洞（紫色状态符号表示）和已处理的基线风险（蓝色状态符号表示）的数量柱状图。

17

告警

告警区域展示了最近24小时内未处理的、排名前5的高风险告警列表，包括告警事件发生的时间、事件名称和服务器名称。

18

攻击来源TOP5

攻击来源TOP5区域展示了最近24小时内您服务器受到的攻击次数排名前5的攻击来源IP地址及其发起的攻击次数。

19

攻击类型

攻击类型区域展示了最近24小时内您服务器受到的攻击类型和对应的被攻击次数。

20

访客分布TOP5

访客分布TOP5区域展示了最近24小时内您服务器来访次数排名前5的国家名称及其发起的访问次数。

云平台最佳实践

云平台最佳实践区域展示了云平台配置检查功能实时检测出的项目信息。

以下是检测项、风险等级和影响资产的说明：

- **检测项**：云平台配置检查支持的检测项目，具体内容请参见云平台配置检查项列表。
- **风险等级**：检测项目的风险级别。以下是风险等级颜色和风险级别的对应关系：
  - 红色代表高风险。
  - 橙色代表中风险。
  - 灰色代表低风险。
  - 绿色代表正常。
- **影响资产**：检测项目对应风险影响的资产数量。

5.应用市场

应用市场展示了云安全中心提供的扩展能力和您已购买的安全产品概况。您可以在应用市场页面申请或开通云安全中心提供的扩展能力，例如：应用白名单、安全大屏、自定义告警、网页防篡改等。

申请或开通云安全中心扩展能力

在云安全中心控制台的**安全运营 > 应用市场**页面的**云安全中心扩展能力**区域，查看云安全中心提供的扩展能力。

您可以申请或开通以下扩展能力：

- 应用白名单

  应用白名单功能可防止您的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。目前应用白名单功能处于邀测阶段，您可以单击**应用白名单**区域的**申请**，提交使用白名单功能的申请。申请审批会在5个工作日内完成。

- 安全大屏

  安全大屏为云安全中心基础杀毒版、高级版和企业版提供的增值服务，可从您资产的当前安全情况、外部攻击情况、威胁情况三个维度为您全面展现当前资产的网络安全态势。您可以单击**安全大屏**区域的**开通**，前往云安全中心购买页购买安全大屏服务。

- 自定义告警

  云安全中心支持配置自定义的告警规则，帮助您更全面和深入地获取您服务器中存在的威胁信息。自定义告警功能目前处于公测阶段，您可以单击**自定义告警**区域的**申请**，提交自定义告警开通的申请。完成申请审批一般需要5~7个工作日。

- 网页防篡改

  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。您可以单击**网页防篡改**区域的**开通**，前往云安全中心购买页购买防篡改服务。

- 微步威胁情报

  微步威胁情报为云盾合作伙伴微步在线，基于行业领先威胁情报数据，为您提供的高质量威胁情报服务，帮助您快速精准定位并处理安全威胁。您可以单击**微步威胁情报**区域的**开通**，在微步威胁情报购买页购买微步威胁情报服务。

查看云盾产品概况

在云安全中心控制台的**安全运营 > 应用市场**页面的**云盾产品**区域，您可以查看已购买的安全产品概况，包括已开通产品购买的实例数量、到期日期等信息。如果需要了解该产品的更多信息，您可以单击需要查看的云产品名称跳转至该产品控制台。

6.容器签名

容器签名可实现对容器镜像的可信签名，确保只允许部署您认可的容器镜像，防止未经签名授权的镜像启动，从根本上帮助您提升资产的安全性。

前提条件

使用容器签名功能前，您需要先完成以下操作：

- 已创建了非对称加密算法的KMS密钥。

  有关创建KMS密钥的详细内容，请参见创建密钥。

  > **注意** 由于非对称密钥算法才支持容器签名功能，创建KMS密钥时，**密钥类型**必须选择*RSA_2048*，**密钥用途**必须选择*SIGN/VERIFY*。关于KMS密钥算法的详细内容，请参见密钥的算法。

- 已创建了部署在中国香港地域的Kubernetes集群，并且集群已安装了kritis-validation-hook组件。

  > **说明** 目前，仅部署在中国香港地域的Kubernetes集群支持容器签名。

  有关创建Kubernetes集群的详细内容，请参见创建Kubernetes专有版集群。

  有关kritis-validation-hook组件的详细内容，请参见组件介绍。

- 首次使用容器签名，需要先完成云资产访问授权。

限制说明

仅云安全中心企业版支持容器签名，基础版、基础杀毒版和高级版需要升级到企业版后才能使用该功能。

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 > 容器签名**。
3. （可选）在**容器签名 > 证明者**页签中创建证明者。如果您已创建过证明者，可直接进入步骤4。

   您可在**证明者**页签中单击**创建证明者**，完成配置后并单击**确定**，完成证明者的创建。

   创建证明者的配置说明如下。

参数	描述
证明者名称	配置容器签名安全策略时需要选择证明者，用于对您的目标容器进行可信授权。建议输入便于识别的名称。
选择证书	在证书列表中选择您已创建的KMS密钥。 **说明** 由于非对称密钥算法才支持容器签名功能，创建KMS密钥时，**密钥类型**必须选择*RSA_2048*，**密钥用途**必须选择*SIGN/VERIFY*。关于KMS密钥算法的详细内容，请参见密钥的算法。
描述	输入该证明者的备注信息。

4. 创建安全策略。

   您可在**安全策略**页签中单击**添加策略**，完成配置后并单击**确定**，完成策略的创建。

   添加策略的配置说明如下。

参数	描述
策略名称	配置签名安全策略时需要选择证明者，用于对您的目标集群进行可信授权。 建议输入便于识别的名称。
证明者	在证明者列表中选择您已创建的证明者。 具体操作，请参见步骤3。
应用集群	单击需要进行容器签名的集群分组后，选中目标**集群命名空间**。
策略开启状态	单击开关，创建策略后策略会立即启用。 **说明** 默认不开启策略。策略如果未开启将不会生效。
备注	输入安全策略的备注信息。

后续步骤

成功创建并启用容器签名安全策略后，已开启安全策略的容器镜像会标识为**可信的镜像**。

说明 目前暂不支持展示可信标签，该功能将于近期上线。

7.多账号安全管控

云安全中心支持统一管控多个云账号和资源账号，并能够通过统一的界面展示各个账号中检测出的安全风险。

前提条件

您已在资源管理控制台创建了成员或邀请了其他云账号。有关创建成员的详细内容，请参见创建成员。

背景信息

首次使用多账号安全管控时，需要完成对云安全中心使用资源管理产品的授权。

> 说明
>
> - 目前，仅云安全中心企业版支持多账号安全管控。
> - 仅企业实名账号可使用多账号安全管控功能，个人账号无法使用。

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 > 多账号安全管控**。
3. 在**多账号安全管控**页面单击**添加账号**。
4. 在**添加账号**页面单击**请选择需要管控的账号**下拉列表，选择需要进行安全管控的账号。

   如果在**添加账号**页面没有可以添加的账号，您需要前往资源管理控制台，在**资源目录**页面进行以下操作：
   - 创建成员（支持创建资源账号和云账号成员，请参见创建成员）。
   - 邀请其他云账号（仅支持邀请阿里云账号，请参见邀请其他成员加入资源目录）。
5. （可选）选择**当有新增账号时，默认添加至管控列表**，将新增的账号自动同步到多账号安全管控列表中。
6. 单击**确定**。

成功添加账号后，您可以在**多账号安全管控**页面进行以下操作：

- 搜索已添加到多账号安全管控列表中的账号。
- 查看所有账号的云安全中心版本、安全分和存在的安全风险信息。
- 单击**前往查看**，跳转到**资源管理**控制台的**资源目录**页面。您可以在**资源目录**页面查看所有资产目录信息、新建成员、邀请成员、将资源账号升级为账号。
- 单击**删除**，将该账号从多账号安全管控中删除。