容器安全服务

操作指南

腾讯云

文档目录

操作指南
- 安全概览
- 资产管理
  - 概述
  - 容器
  - 集群资产
  - 进程端口
  - 应用 Web 资产
- 漏洞管理
  - 漏洞检测
  - 漏洞防御
- 镜像风险管理
  - 概述
  - 本地镜像
  - 仓库镜像
    - 仓库镜像
    - 接入 AWS 镜像仓库
  - 镜像拦截事件
- 集群安全管理
  - 集群检查
  - 自建集群
  - 风险分析
- 基线管理
  - 概述
  - 容器
  - 镜像
  - 主机
  - Kubernetes
- 运行时安全
  - 概述
  - 容器逃逸
  - 反弹 Shell
    - 事件列表
    - 配置白名单
  - 文件查杀
  - 恶意外连
- 高级防御
  - 概述
  - 异常进程
    - 事件列表
    - 规则配置
  - 文件篡改
    - 事件列表
    - 规则配置
  - 高危系统调用
    - 事件列表
    - 白名单管理
  - K8s API 异常请求
- 策略管理

镜像拦截策略
防护开关
告警设置
日志分析
概述
查询日志
配置日志
日志投递
混合云安装指引
概述
配置非腾讯云机器
连接专线 VPC
热点问题
失陷容器隔离说明
日志字段数据解析

操作指南
安全概览

最近更新时间：2025-05-13 18:11:12

本文档为您介绍容器安全服务各个安全模块的整体安全情况概览。

- 实时展示容器安全风险概览信息和容器安全事件新增趋势等信息。
- 容器安全服务的版本和使用情况，并提供升级、续费等功能。

主要功能

登录 容器安全服务控制台，在左侧导航中，单击**安全概览**，进入安全概览页面。

查看资产信息

1. 在安全概览页面，资产信息模块展示容器、镜像、集群、主机节点的资产数量信息。

2. 在安全概览页面，单击“模块总数”，可跳转到资产管理的对应模块列表。

查看版本和使用情况，升级、续费

在安全概览页面，版本信息窗口展示当前容器安全服务版本信息和版本到期时间，以专业版为例具体信息如下：

- 若当前版本即将到期将提醒用户进行续费，用户可单击**续费**，进入续费页面完成续费。

- 版本信息窗口同时展示当前用户的授权情况，包括总核数和授权核数、已购镜像授权。
  - 总核数和授权核数：总核数是指用户业务节点的虚拟核数总和；授权核数是指用户开通专业版的核数。

> **说明：**
> - 当授权核数小于总核数时，将提示用户需补充购买的核数，用户可单击**查看**，进入购买页面购买授权。

- 当用户未补充购买所需授权核数时，将进入弹性计费模式，即超过授权核数将按1元/核/天进行弹性计费。

- 已购镜像授权：用户已购买的镜像安全扫描数量。

> **说明：**
> - 当业务环境中存在未开启镜像安全扫描的本地镜像或仓库镜像时，用户可单击**授权**，可进行批量授权和自动授权。
> - 镜像授权购买后，进入容器安全服务控制台，在左侧导航中，**镜像风险管理>本地镜像/仓库镜像**页面对授权进行配置，用户可自定义配置需开启安全扫描的镜像。
> - 因产品调整，镜像授权于2023年12月29日-2024年07月31日暂停新购，已购用户仍可正常使用，给您带来不便，敬请谅解。

查看待处理漏洞风险

1. 在安全概览页面，待处理漏洞风险事件模块展示当前待处理的全部漏洞、应急漏洞、系统漏洞、Web应用漏洞、漏洞影响本地镜像、漏洞影响仓库镜像。

2. 在安全概览页面，单击“模块总数”，可进入到相应的安全事件页面查看详情并进行处理。

查看待处理集群风险

1. 在安全概览页面，待处理集群风险事件模块展示当前待处理的风险集群、集群漏洞、严重漏洞、高危漏洞、配置风险、严重风险、高风险。

2. 在安全概览页面，单击“模块总数”，可进入到相应的安全事件页面查看详情并进行处理。

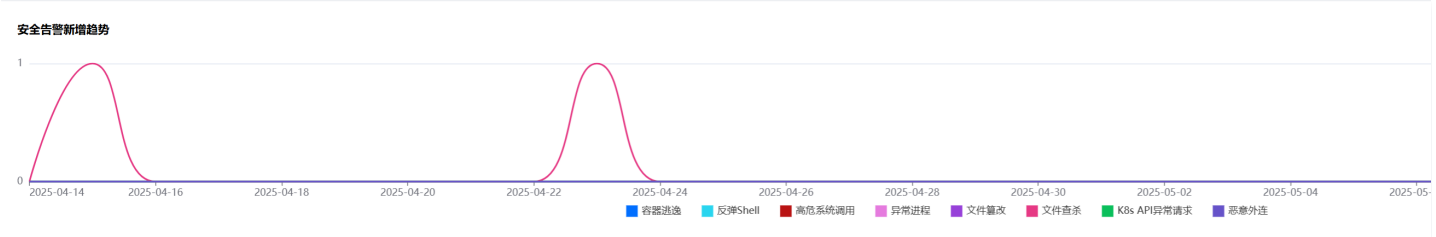
查看待处理安全告警

1. 在安全概览页面，待处理安全事件模块展示当前待处理的安全事件的数量。

2. 在安全概览页面，单击“模块总数”，可进入到相应的安全事件页面查看详情并进行处理。

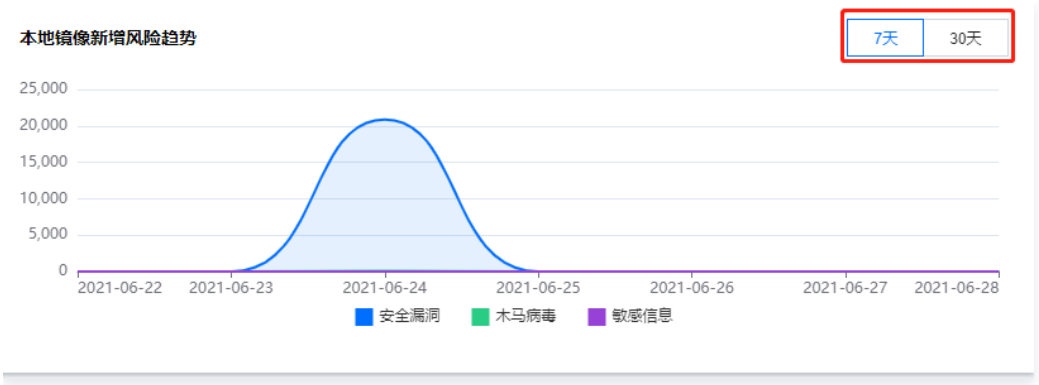
查看安全告警新增趋势

在安全概览页面，安全事件新增趋势模块展示7天或30天内运行时安全事件新增趋势。单击**7天**或**30天**可切换时间。



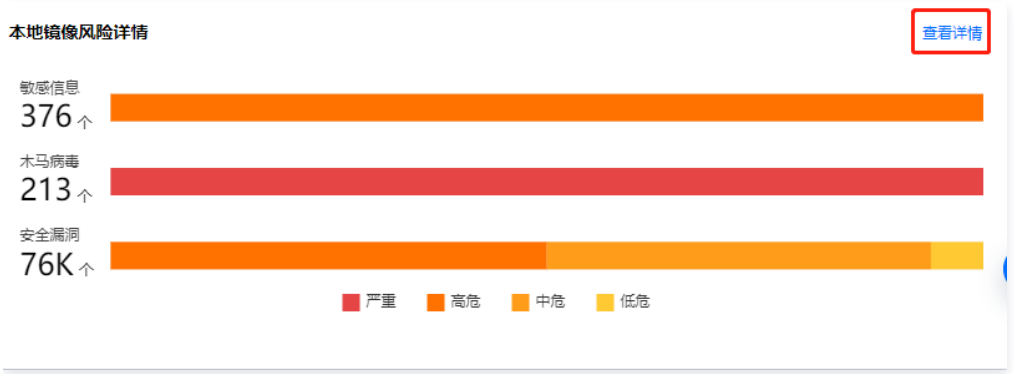
查看本地镜像新增风险趋势

在安全概览页面，展示7天或30天内本地镜像新增的安全漏洞、木马病毒、敏感信息数量趋势。单击**7天**或**30天**可切换时间。



查看本地镜像风险详情

在安全概览页面，本地镜像风险详情模块展示当前镜像存在的敏感信息、木马病毒、安全漏洞的风险总数和威胁等级分布。单击**查看详情**，可进入镜像安全模块查看详情并进行处理。



资产管理

概述

最近更新时间：2025-05-13 18:11:12

本文档为您介绍资产管理所提供的自动化资产清点功能，支持清点容器、本地镜像和仓库镜像等关键资产信息，帮助企业实现资产可视化。

- **资产管理的数据每隔24小时自动同步一次，支持手动同步。**
- **资产管理支持采集以下14种资产的信息：容器、本地镜像、仓库镜像、集群、主机节点、超级节点、进程、端口、Web 服务、运行应用、数据库应用。**
- **目前支持识别的资产有：**

资产类型	资产信息
容器	容器、本地镜像、仓库镜像、主机节点、超级节点。
集群资产	集群、Pod、Service、Ingress。
进程端口	进程、端口。
应用 Web 资产	Web 服务、运行应用、数据库应用。

容器

最近更新时间：2025-05-20 15:13:01

本文档为您介绍容器模块功能，以及如何查看容器、镜像和主机等资产详情。

查看容器模块

容器展示模块中提供容器资产总数，以及正在运行、暂停运行和停止运行和其他容器的数量。

筛选容器列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

3. 在容器列表页面，可按运行状态对容器资产进行筛选，或搜索框通过“容器名称、容器 ID、镜像名称、主机 IP”等关键字对容器进行查找。
   - 单击左上角的状态下拉框，按运行状态对容器资产进行筛选。

   - 单击搜索框，通过“容器名称、容器ID、镜像名称、主机IP”等关键字对容器进行查找。

查看容器列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

3. 在容器列表页面，单击“容器名称”，右侧弹出抽屉展示该容器详情，页面可切换查看容器基本信息、进程和端口等信息。

4. 在资产管理页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

3. 在容器列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

列表重点字段说明

1. 运行状态：包括正常运行、暂停运行和停止运行三种状态。
2. 镜像：关联镜像名称。
3. 所属 Pod：容器所属 Pod。
4. CPU|占用率：CPU 使用率。
5. 内存|占用：内存占用大小。

查看本地镜像模块

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，镜像模块展示了模块中镜像资产总数。单击“镜像总数”，可跳转**镜像风险管理** > **本地镜像**页面查看镜像详情。

> **说明：**
> 更多详细内容，请参见 本地镜像 。

查看镜像仓库模块

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，镜像仓库模块展示了镜像仓库资产总数。单击“镜像仓库总数”，可跳转**镜像风险管理** > **仓库镜像**页面查看镜像仓库详情。

> **说明：**
> 更多详细内容，请参见 镜像仓库 。

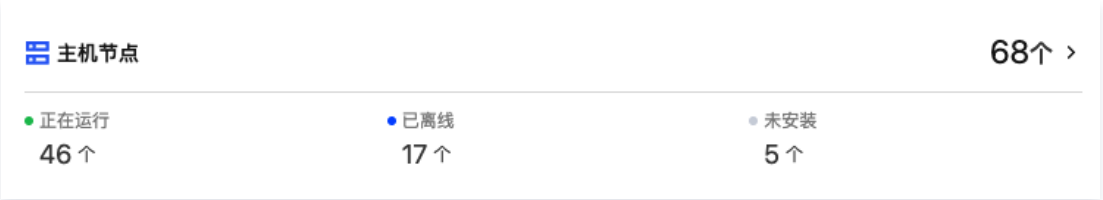
查看主机模块

主机展示模块中提供主机资产总数，以及正在运行和已离线主机的数量。

筛选主机列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。

2. 在资产管理页面，单击“主机总数”，可查看全部主机资产列表。

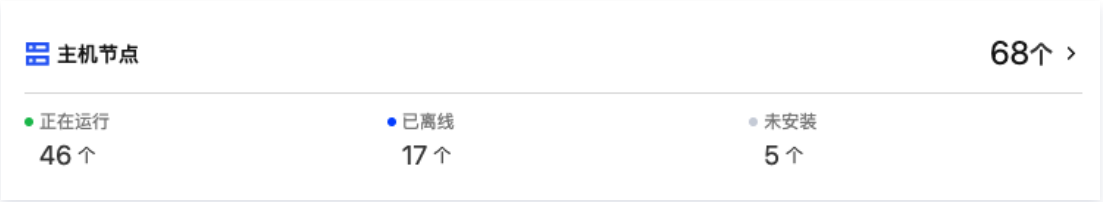


3. 在主机列表页面，可按主机状态对主机资产进行筛选，或搜索框通过“主机名、业务组、Docker 版本、主机 IP”等关键字对主机进行查找。
   - 单击左上角的状态下拉框，按主机状态对主机资产进行筛选。

   - 单击搜索框，通过“主机名、业务组、Docker 版本 、主机 IP”等关键字对主机进行查找。

查看容器列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“主机总数”，可查看全部主机资产列表。



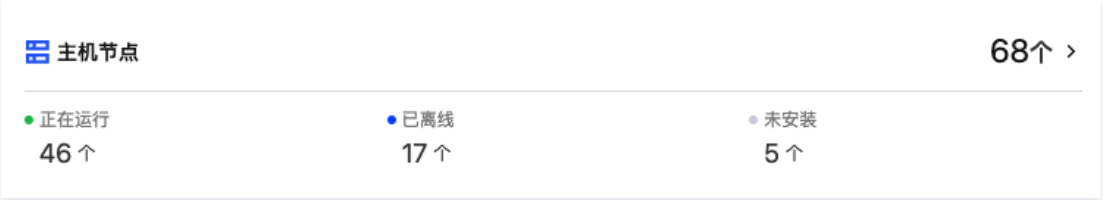
3. 在主机列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

4. 在主机列表页面，单击“关联镜像数”，可查看关联镜像详情。

5. 在主机列表页面，单击“关联容器数”，可查看关联容器详情。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“主机总数”，可查看全部主机资产列表。



3. 在主机列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

列表字段说明

1. 主机名称：主机名称。
2. 主机 IP：单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。
3. 业务组：主机所属业务组名称。
4. Docker 版本：展示 Docker 版本号，如未安装，则显示“未安装”。
5. Docker 文件系统类型：Docker 文件系统类型。
6. 镜像数：主机关联镜像数。单击“数字”可查看关联镜像详情。
7. 容器数：主机关联容器数。单击“数字”可查看关联容器详情。

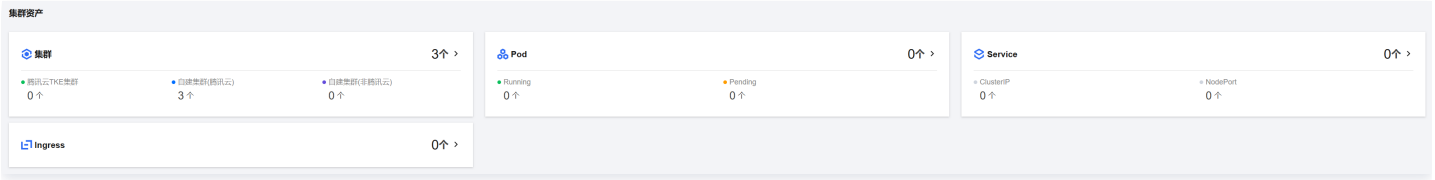
集群资产

最近更新时间：2025-05-20 15:13:01

本文档为您介绍集群资产功能，以及如何查看集群、Pod、Service、Ingress 资产详情。

查看集群模块

集群模块展示了集群总数以及每种集群类型的数量。



查看集群列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。
2. 在资产管理页面，单击**“集群总数”**，进入集群检查页面，可查看全部集群资产。

3. 在集群检查页面，单击**搜索框**，通过“集群名称、集群 ID、所属地域”等关键字可对集群进行查找。

自定义列表管理

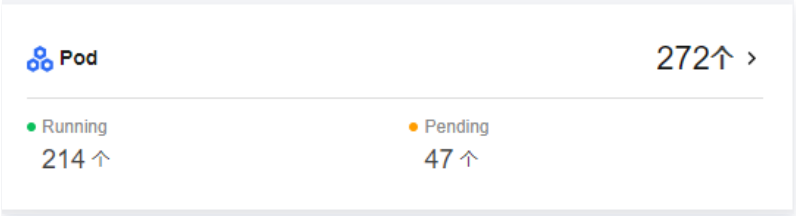
1. 在集群检查页面，单击 图标，弹出自定义列表管理对话框。
2. 在自定义列表管理对话框，选择所需的类型后，单击**确认**，即可完成设置自定义列表。

查看 Pod 模块

Pod 模块展示了集群 Pod 总数，以及 Running、Pending 状态的 Pod 数量。

查看 Pod 列表

1. 在资产管理页面，单击**“Pod 总数”**，进入 Pod 列表页面，可查看全部 Pod 资产。



2. 在 Pod 列表页面，可按“集群名称、命名空间”对 Pod 资产进行筛选；单击**更多筛选**可按“Pod 状态、工作负载类型、工作负载名称、集群 ID、Pod IP、所在节点 IP、容器名称、容器 ID、镜像名称”对 Pod 资产进行筛选；或单击**搜索框**通过“Pod 名称”关键字可对 Pod 资产进行查找。

3. 找到目标 Pod，单击 **Pod 名称**，右侧弹出抽屉展示该 Pod 详情，页面可切换查看 Pod 基本信息、Service 和容器等信息。

自定义列表管理

1. 在 Pod 列表页面，单击 ⚙ 图标，弹出自定义列表管理对话框。

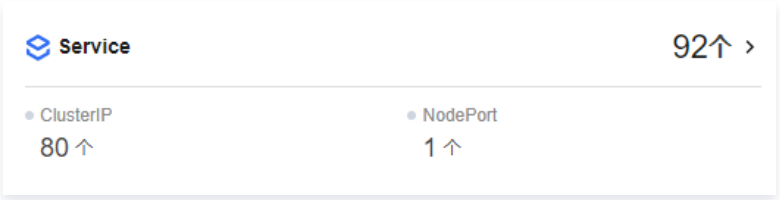
2. 在自定义列表管理对话框，选择所需的类型后，单击**确认**，即可完成设置自定义列表。

查看 Service 模块

Service 模块展示了集群 Service 总数，以及 ClusterIP、NodePort 类型的 Service 数量。

查看 Service 列表

1. 在资产管理页面，单击**“Service 总数”**，进入 Service 列表页面，可查看全部 Service 资产。



2. 在 Service 列表页面，可按“集群名称、命名空间、地域”对 Service 资产进行筛选，单击**更多筛选**可按“集群 ID、Service 类型、负载均衡 IP、服务 IP、Labels、端口”对 Service 资产进行筛选。或单击**搜索框**通过“Service 名称”关键字可对 Service 资产进行查找。

3. 找到目标 Service，单击**“Service 名称”**，右侧弹出抽屉展示该 Service 详情，页面可切换查看 Service 基本信息、Pod、YAML 和端口映射规则等信息。

自定义列表管理

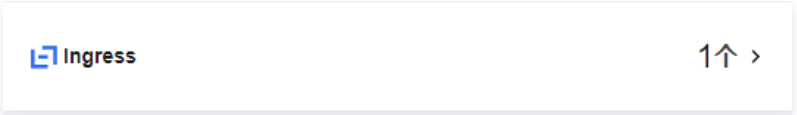
1. 在 Service 列表页面，单击 图标，弹出自定义列表管理对话框。
2. 在自定义列表管理对话框，选择所需的类型后，单击**确认**，即可完成设置自定义列表。

查看 Ingress 模块

Ingress 模块展示了集群 Ingress 总数。

查看 Ingress 列表

1. 在资产管理页面，单击**“Ingress 总数”**，进入 Service 列表页面，可查看全部 Ingress 资产。



2. 在 Ingress 列表页面，可按“集群名称、命名空间、地域”对 Ingress 资产进行筛选；单击**更多筛选**可按“Ingress 名称、VIP、Labels、后端服务”对 Ingress 资产进行筛选；或单击**搜索框**通过“Ingress 名称”关键字可对 Ingress 资产进行查找。

3. 找到目标 Ingress，单击“**Ingress 名称**”，右侧弹出抽屉展示该 Ingress 详情，页面可切换查看 Ingress 基本信息、转发配置和 YAML 信息。

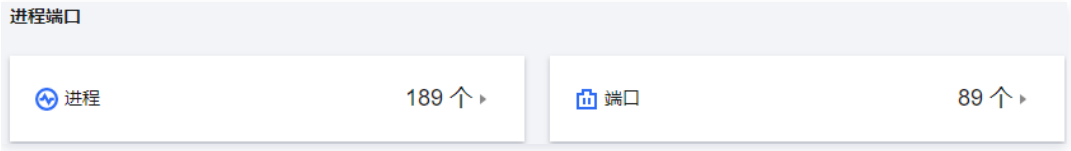
自定义列表管理

1. 在 Ingress 列表页面，单击 图标，弹出自定义列表管理对话框。
2. 在自定义列表管理对话框，选择所需的类型后，单击**确认**，即可完成设置自定义列表。

进程端口

最近更新时间：2025-05-20 15:13:01

本文档为您介绍进程端口功能提供进程和端口数量，以及如何查看进程列表和端口列表。

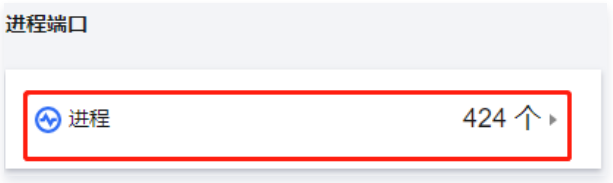


查看进程模块

进程模块展示了进程总数。

筛选进程列表

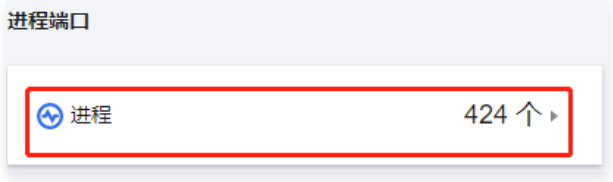
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“进程总数”，进入进程列表页面，可查看全部进程资产列表。



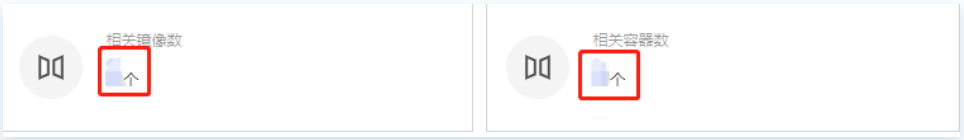
3. 在进程列表页面，单击搜索框，通过“运行用户、主机名、进程名”等关键字可对进程进行查找。

查看进程列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“进程总数”，进入进程列表页面，可查看全部进程资产列表。

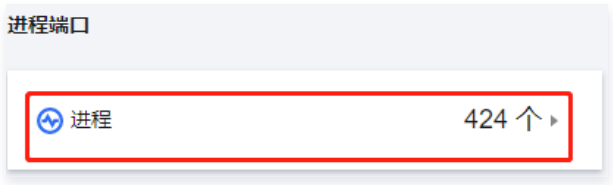


3. 在进程列表页面，单击“**主机名称**”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
> 在抽屉中，单击“数字”查看主机相关镜像数和相关容器数详情。
>
> 
>

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“进程总数”，进入进程列表页面，可查看全部进程资产列表。



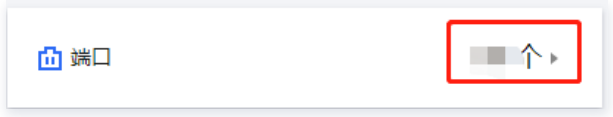
3. 在进程列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

查看端口模块

端口模块展示了端口总数。

筛选端口列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。

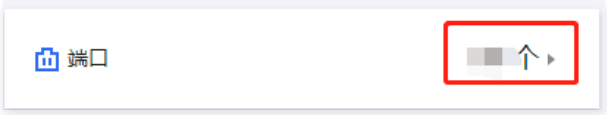


3. 在端口列表页面，单击搜索框，通过“主机 IP、进程名和宿主机端口”等关键字可对端口进行查找。

查看端口列表

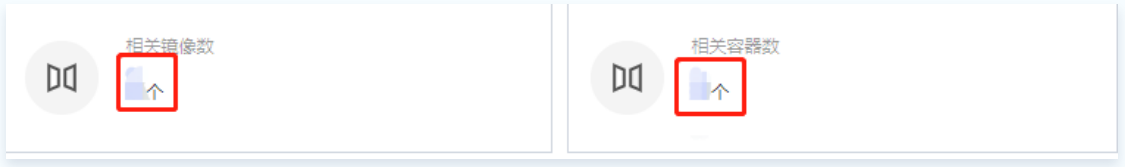
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。

2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。



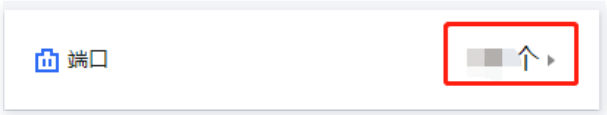
3. 在端口列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

说明：
在抽屉中，单击“数字”查看主机相关镜像数和相关容器数详情。



自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。
2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。



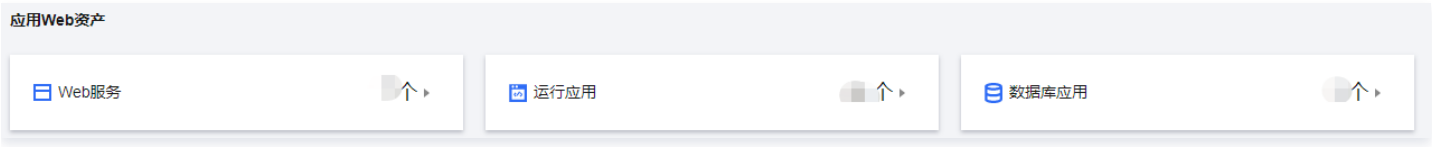
3. 在端口列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

应用 Web 资产

最近更新时间：2025-05-20 15:13:01

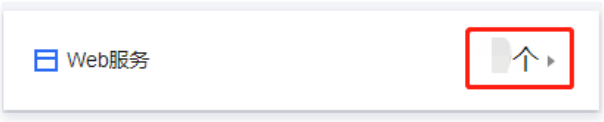
本文档为您介绍应用 Web 资产功能，以及如何查看Web 服务、运行应用和数据库应用详情。

查看Web 服务



筛选 Web 服务

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“Web 服务总数”进入Web 服务列表页面，可查看全部 Web 服务资产列表。

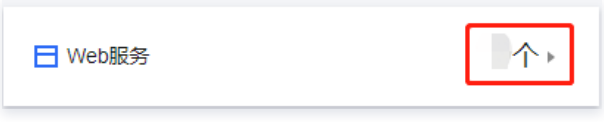


3. 在 Web 服务列表页面，可按服务类型对 Web 服务资产进行筛选，或搜索框通过“容器名称、主机名、启动用户”等关键字对 Web 服务进行查找。
   - 单击左上角的服务类型下拉框，按服务类型对 Web 服务资产进行筛选。

   - 单击搜索框，可通过“容器名称、主机名、启动用户”等关键字对 Web 服务进行查找。

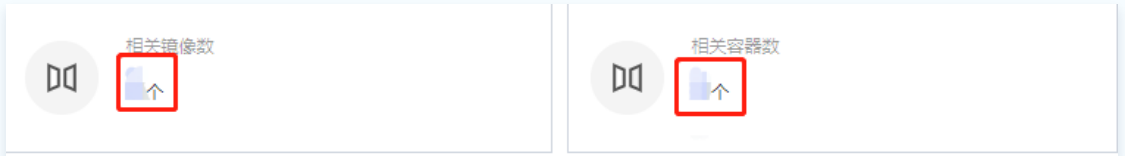
查看 Web 服务列表

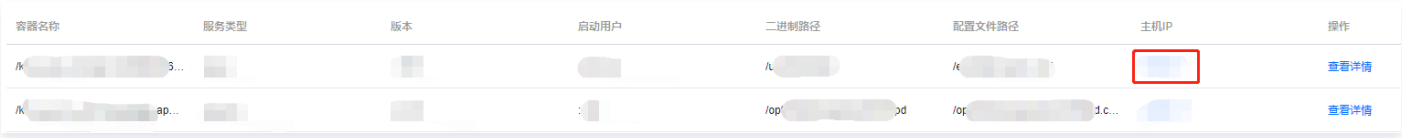
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“Web 服务总数”进入Web 服务列表页面，可查看全部 Web 服务资产列表。



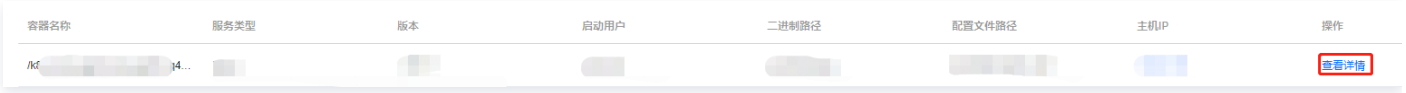
3. 在 Web 服务列表页面，主机名称/IP：单击“主机名称”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
> 在抽屉中，可单击“数字”查看主机相关镜像数和相关容器数详情。



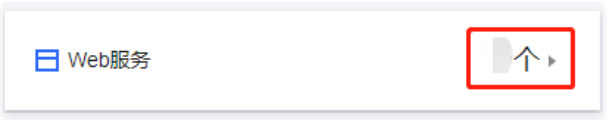


4. 在 Web 服务列表页面，单击**查看详情**，对话框展示 Web 应用服务详情，包括基本信息和关联进程列表。



自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“Web 服务总数”进入Web 服务列表页面，可查看全部 Web 服务资产列表。



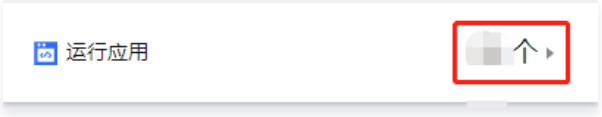
3. 在 Web 服务列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

查看运行应用

筛选运行应用

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。

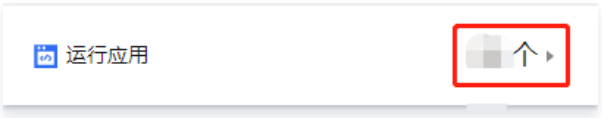
2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。



3. 在运行应用列表页面，单击搜索框，可通过“容器名称、主机 IP 和应用类别”等关键字对运行应用进行查找。

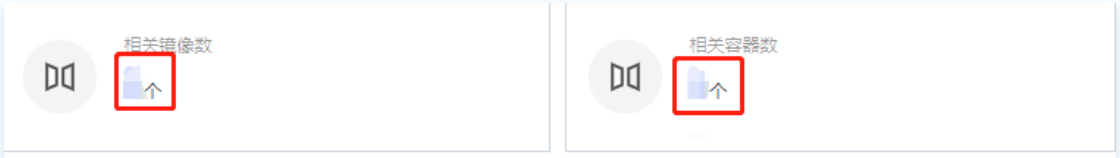
查看运行应用列表

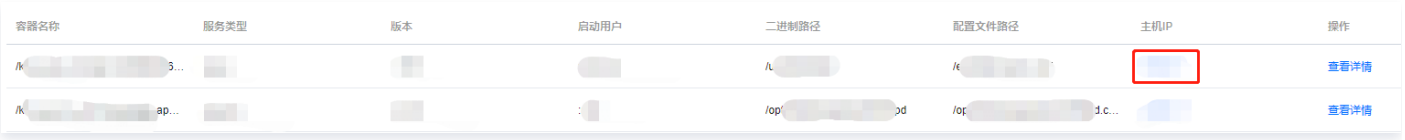
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。



3. 在运行应用列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

说明：
在抽屉中，可单击“数字”查看主机相关镜像数和相关容器数详情。





4. 在资产管理页面，单击**查看详情**，对话框展示运行应用关联进程详情列表。

自定义列表管理

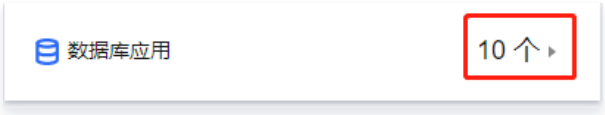
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。

3. 在运行应用列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

查看数据库应用

筛选数据库应用

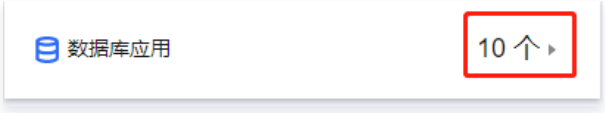
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“数据库应用总数”，进入运行应用列表页面，可查看全部数据库应用资产列表。



3. 在数据库应用资产列表页面，单击搜索框，通过“容器名称、主机IP和数据库类型”等关键字可对数据库应用进行查找。

查看数据库应用列表

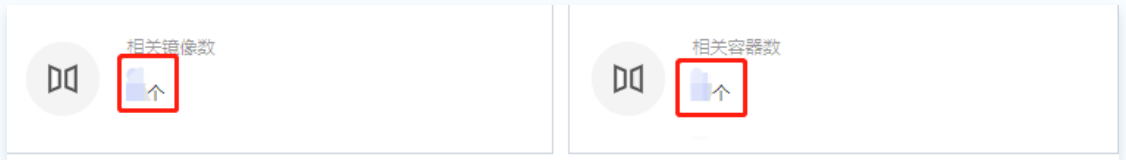
1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“数据库应用总数”，进入运行应用列表页面，可查看全部数据库应用资产列表。

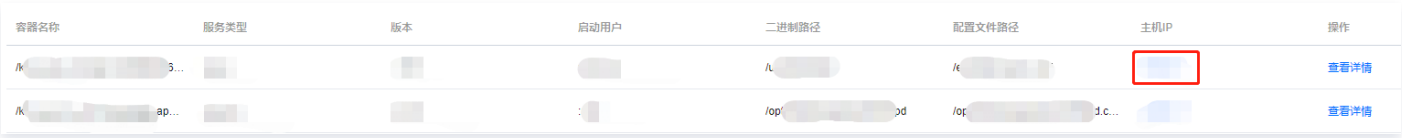


3. 在数据库应用资产列表页面，单击“主机名称”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**

在抽屉中，可单击“数字”查看主机相关镜像数和相关容器数详情。

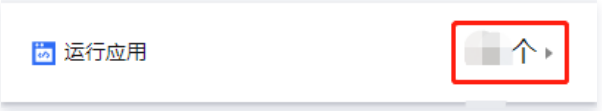




4. 在运行应用列表页面，单击**查看详情**，对话框展示数据库服务详情，包括基本信息和关联进程列表。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**资产管理**。
2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。



3. 在数据库应用资产列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

漏洞管理
漏洞检测

最近更新时间：2025-04-29 16:22:55

腾讯云容器安全服务支持对本地镜像和仓库镜像上的漏洞，进行周期性和及时性的检测功能。支持对指定镜像和漏洞类别的检测，同时支持忽略漏洞等功能，可为您提供漏洞的风险、特征、严重等级及修复建议等信息，可视化界面有助于您更好的管理镜像的漏洞风险。
本文档将介绍如何使用漏洞管理功能，帮助您管理镜像的漏洞风险。漏洞管理功能支持一键检测系统漏洞、Web 应用漏洞及应急漏洞。

漏洞检测

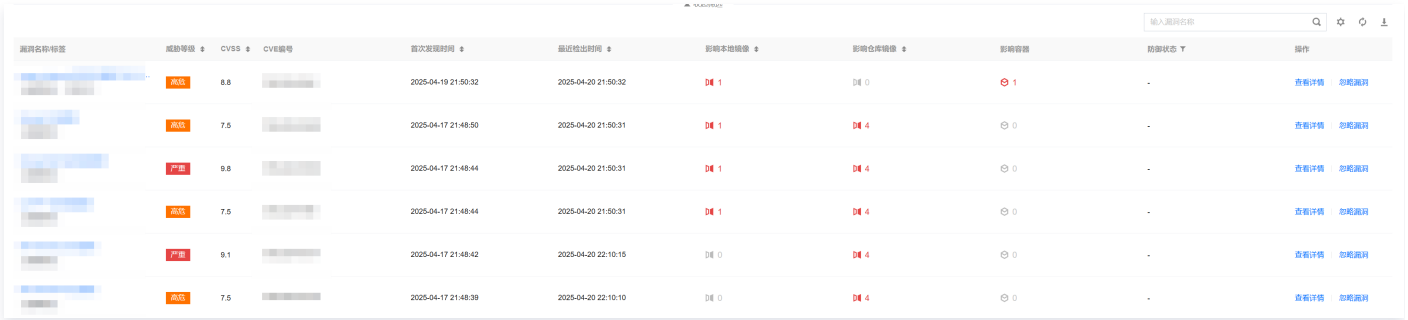
1. 登录 容器安全控制台，在左侧导航栏中选择**漏洞管理**，进入漏洞管理页面。
2. 在漏洞管理页面，可进行漏洞检测并查看漏洞检测数据，单击**一键扫描**。

3. 在**一键扫描**设置弹窗中，选择需要检测的镜像，单击**立即扫描**，检测完成后，检测结果会以可视化图表的方式显示在漏洞管理页面。

> **说明：**
> - 需要先对镜像完成授权方可进行镜像检测。
> - 检测时间与检测镜像数量、镜像大小、是否第一次检测等因素有关，检测一般持续2-60分钟。

查看漏洞

1. 在 漏洞管理页面，查看镜像检测到的系统漏洞、Web 应用漏洞、应急漏洞的漏洞信息。查看漏洞影响的本地镜像、仓库镜像、运行容器资产信息以及漏洞风险统计情况、TOP5漏洞、存在严重&高危漏洞镜像趋势。
   - TOP5漏洞图：系统根据漏洞 CVSS 分数和动态风险等级等因素计算出漏洞 TOP5排名，并展示 TOP5漏洞的威胁等级、影响镜像数（只统计最新版本）和影响容器数量。
   - 严重&高危漏洞镜像趋势图：展示存在有严重或高危漏洞的镜像（最新版本）的数量变化趋势，当切换为运行容器时，展示存在有严重或高危漏洞且启动了容器的镜像（最新版本）的数量变化趋势。可查看7天或30天的趋势图。
2. 在漏洞列表中，可以查看漏洞名称、威胁等级、CVE 编号、首次发现时间、最近检出时间等信息，影响本地镜像数量，影响仓库镜像数量，影响容器数量，防御状态，操作处理。



字段说明：

- 漏洞名称：漏洞公开的命名。

- 威胁等级：根据漏洞的危险程度，将其划分为严重、高危、中危和低危四个等级。
- 首次发现时间：取第一次镜像检测出该漏洞的时间。
- 最近检出时间：取最近一次镜像检测出该漏洞的时间。
- 影响本地镜像（个）：表示所有检测出的镜像漏洞中，有多少个本地镜像存在该漏洞，即该漏洞影响的本地镜像数量。
- 影响仓库镜像（个）：表示所有检测出的镜像漏洞中，有多少个仓库镜像存在该漏洞，即该漏洞影响的仓库镜像数量。
- 影响容器（个）：表示所有检测出的镜像漏洞中，有多少个运行容器存在该漏洞，即该漏洞影响的运行的容器数量。

> **说明：**
> 影响容器数量为系统依据漏洞影响的本地镜像所启动的容器进行统计，容器数量目前为检测当时的统计数量，容器状态变化不会更新该统计值。

3. 在漏洞管理页面，支持根据影响资产紧急度和重点关注漏洞筛选查看相关漏洞列表。

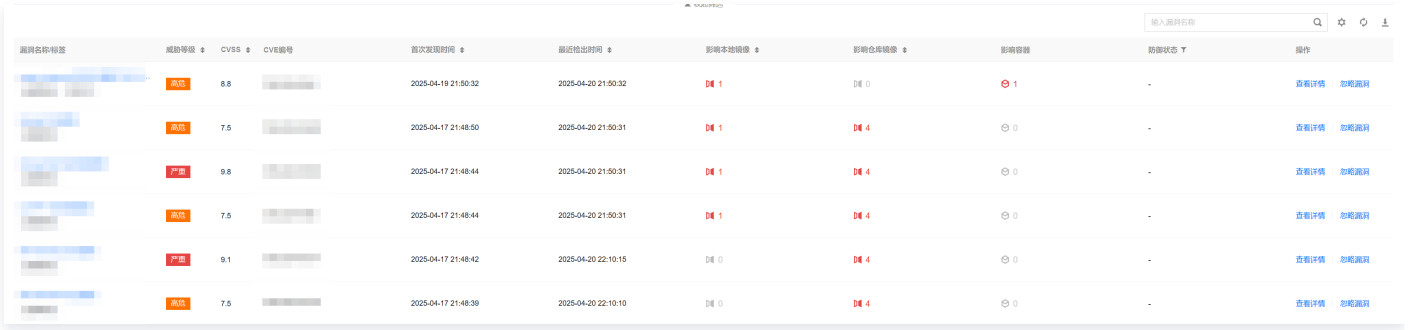
- 影响资产紧急度说明
  - 仅展示影响容器的漏洞：该选项控制过滤影响容器数量不为零的漏洞列表。
  - 仅展示影响最新版本的镜像：该选项控制过滤展示最新版本镜像的漏洞列表。
- 重点关注漏洞说明
  - 漏洞威胁等级为高危或严重且cvss分数≥7.5且具有存在POC、存在EXP、在野利用或必修漏洞的标签并且可被远程利用的漏洞。可自定义重点关注漏洞范围。

- 单击**更多筛选**，支持通过威胁等级、是否可修复、风险标签、CVE 编号、影响镜像 ID、影响镜像名称、影响容器 ID、影响容器名称、漏洞组件版本、漏洞组件名称搜索相关漏洞。

> **说明：**
> 基于影响镜像 ID、影响镜像名称、影响容器 ID、影响容器名称搜索漏洞为搜索相关漏洞的可视化信息，相关漏洞的影响本地镜像数量、影响仓库镜像数量、影响容器数量不会变化。

查看漏洞详情

1. 在 漏洞管理页面 下方，查看检测到的漏洞页面的漏洞信息概览。
2. 在漏洞管理页面，单击该漏洞的**漏洞名称**或操作列的**查看详情**。



3. 在漏洞详情页面，可以查看漏洞详情、影响本地镜像、影响仓库镜像和影响容器。
   - 漏洞详情：包含漏洞描述、漏洞类型、危险等级、披露时间、修复方案、影响组件范围以及漏洞特征等信息。

> **说明：**
> - 漏洞详情影响范围中的组件及其版本来源为国家漏洞数据库（NVD）中漏洞 CPE 的 Vendor Product 信息，不代表检测的镜像中存在该组件，该影响范围组件名称与影响镜像下实际组件名称可能不一致。
> - 要查看镜像中检出的实际受影响组件，可进入影响本地镜像或影响仓库镜像页面，单击镜像左侧**展开按钮**或单击操作列的**查看组件**。

- 影响本地镜像：查看该漏洞影响本地镜像列表，支持通过镜像名称、组件名称、IP 等信息搜索镜像，支持查看镜像关联主机数和关联容器数。
- 影响仓库镜像：查看该漏洞影响仓库镜像列表，支持通过仓库名称、仓库地址等信息搜索镜像。
- 影响容器：查看该漏洞影响容器列表，支持通过容器名称、容器 ID 等信息搜索镜像。

> **说明：**
> 当容器状态发生变化时可能导致影响容器列表数据与漏洞列表中影响容器数不一致。

漏洞防御

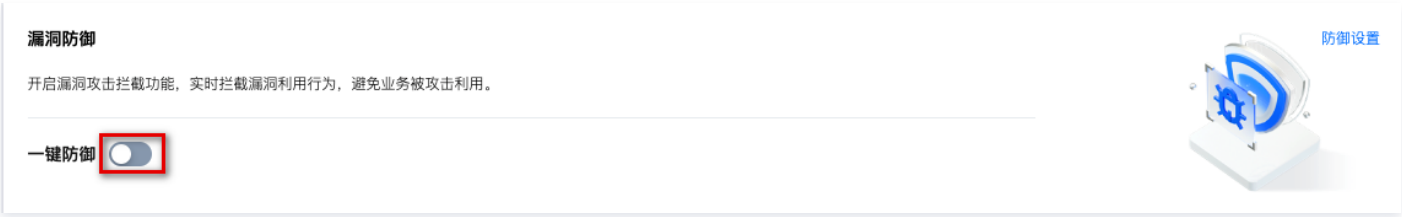
最近更新时间：2025-06-03 14:14:33

漏洞防御是腾讯云安全为应对频发的 0-day、n-day 漏洞而开发的一套基于虚拟补丁的漏洞防御系统。该系统融合了腾讯的漏洞挖掘技术、实时高危漏洞预警技术，通过捕捉、分析 0-day 漏洞，结合腾讯专家知识，生成虚拟补丁，自动在云服务器上生效虚拟补丁，有效拦截黑客攻击行为，为客户修复漏洞争取时间。

开启漏洞防御

开启漏洞防御功能，实时拦截漏洞利用行为，避免业务被攻击利用。

1. 登录 容器安全控制台，在左侧导航栏中，选择**漏洞管理**。
2. 在漏洞管理页面，开启一键防御开关，右侧抽屉展示漏洞防御配置页面。



3. 在漏洞管理页面，单击右上角的**漏洞设置**。

4. 在漏洞设置页面，单击支持防御的漏洞范围的“数字”，进入支持防御漏洞范围页面，可查看防御漏洞范围。

5. 在漏洞设置页面，**选择需防御的节点范围**，单击抽屉下方的**立即生效**，等待策略下发完成，即可对配置中选择的防御节点上的容器漏洞利用行为进行防御。

说明：

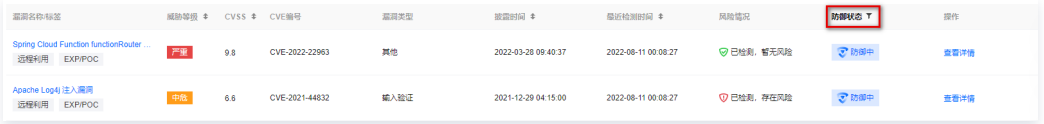
- 防御节点范围选择全部主机节点，当新增主机节点时，新增的主机节点将自动加入漏洞防御范围，减少漏洞攻击。
- 开启漏洞防御时，将会有短暂的资源占用升高（平均1~2分钟），建议您避开业务高峰时期，分批开启。

6. 在漏洞管理页面，单击**防御设置**可查看或调整漏洞防御开关的开启和关闭，调整漏洞防御生效的节点范围，查看节点上防御插件的状态详情等。

7. 在漏洞管理页面，单击**漏洞设置**或**防御设置**，选择**定时扫描**，可开启对本地镜像或仓库镜像自定义周期进行漏洞扫描。

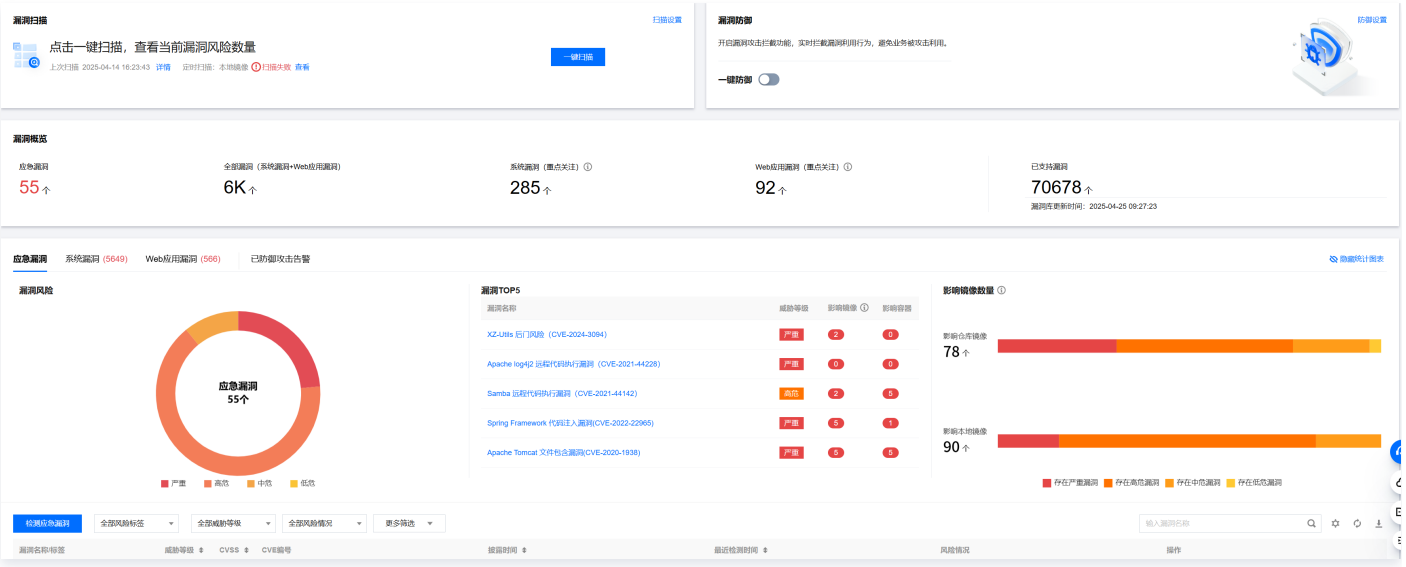
查看防御漏洞

1. 开启漏洞防御后，可在应急漏洞、系统漏洞和应用漏洞页面，筛选防御状态为“防御中”的漏洞，查看支持防御的漏洞详情。



2. 鼠标悬停在防御中图标上时，可快速查阅已支持防御的节点数量和该漏洞已防御攻击次数，且支持单击**防御设置**和**已防御攻击**跳转到防御设置抽屉和漏洞攻击事件页面。

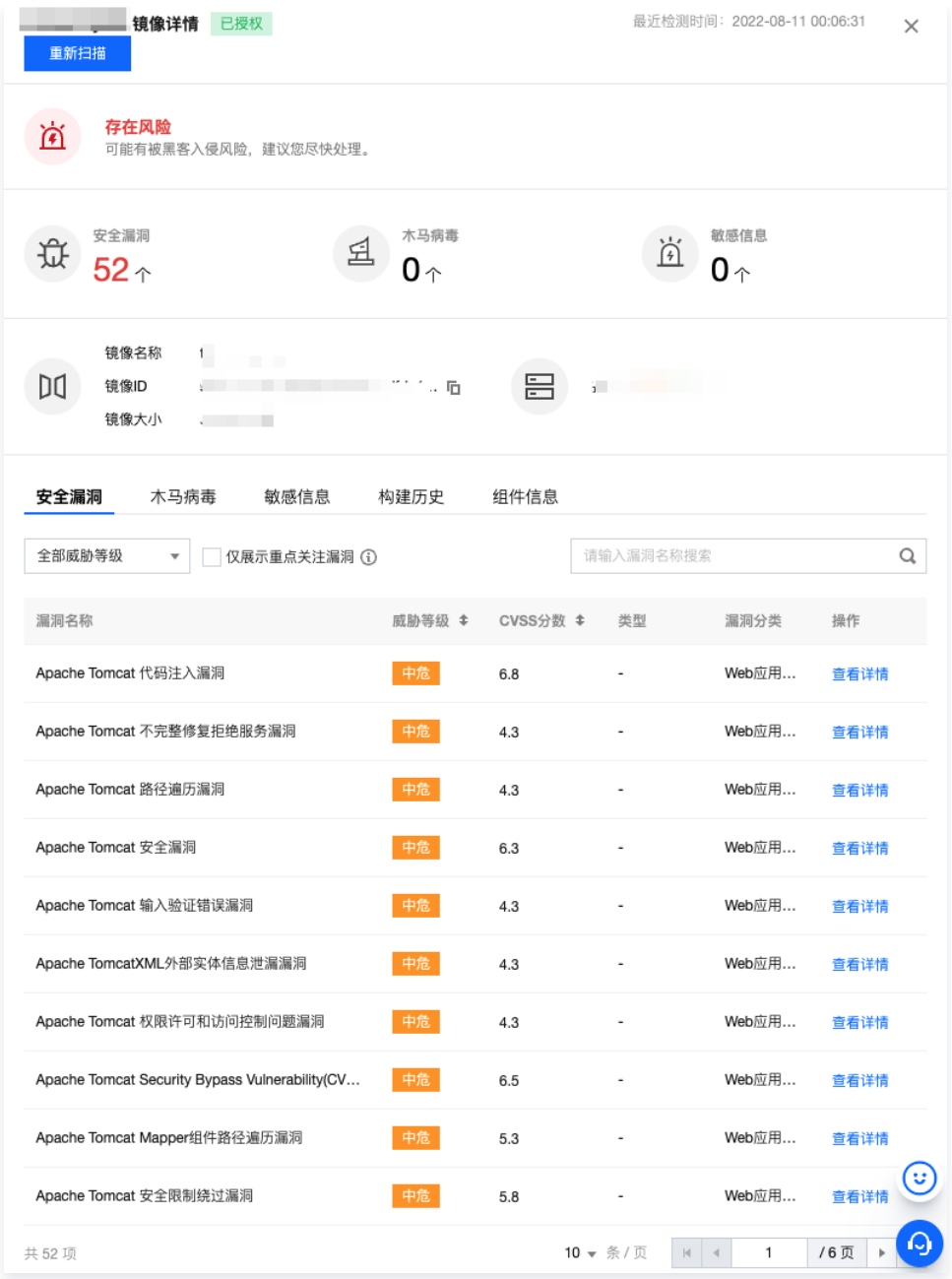
> **说明：**
> 漏洞防御功能未开启时，可在应急漏洞、系统漏洞和应用漏洞页面，筛选防御状态为“未防御”的，查看对应漏洞详情。



漏洞攻击事件

1. 在漏洞管理页面，单击**已防御攻击告警**，可查看防御成功的漏洞攻击事件。

2. 单击**查看详情**，可在详情中查看攻击 IP、攻击包和防御插件信息，并单击**镜像详情**查看漏洞详细信息，建议对攻击 IP 进行封禁，对业务镜像上的漏洞进行修复。


镜像详情
已授权
重新扫描
最近检测时间：2022-08-11 00:06:31
存在风险
可能有被黑客入侵风险，建议您尽快处理。
安全漏洞
52 个
木马病毒
0 个
敏感信息
0 个
镜像名称
镜像ID
镜像大小
安全漏洞
木马病毒
敏感信息
构建历史
组件信息
全部威胁等级
仅展示重点关注漏洞
请输入漏洞名称搜索
漏洞名称
威胁等级
CVSS分数
类型
漏洞分类
操作
Apache Tomcat 代码注入漏洞 中危 6.8 - Web应用... 查看详情
Apache Tomcat 不完整修复拒绝服务漏洞 中危 4.3 - Web应用... 查看详情
Apache Tomcat 路径遍历漏洞 中危 4.3 - Web应用... 查看详情
Apache Tomcat 安全漏洞 中危 6.3 - Web应用... 查看详情
Apache Tomcat 输入验证错误漏洞 中危 4.3 - Web应用... 查看详情
Apache TomcatXML外部实体信息泄漏漏洞 中危 4.3 - Web应用... 查看详情
Apache Tomcat 权限许可和访问控制问题漏洞 中危 4.3 - Web应用... 查看详情
Apache Tomcat Security Bypass Vulnerability(CV... 中危 6.5 - Web应用... 查看详情
Apache Tomcat Mapper组件路径遍历漏洞 中危 5.3 - Web应用... 查看详情
Apache Tomcat 安全限制绕过漏洞 中危 5.8 - Web应用... 查看详情
共 52 项
10 条 / 页
1
/ 6 页

镜像风险管理
概述

最近更新时间：2025-05-13 18:11:12

镜像风险管理是可针对本地镜像、仓库镜像提供一键检测功能，支持对漏洞、木马病毒及敏感信息等多维度安全扫描。

本地镜像安全风险

- 镜像是容器的静态表示形式，镜像的安全决定了容器运行时的安全。
- 镜像的安全风险分布在创建过程、获取来源、获取途径等方面。镜像有以下情况可能存在危险：
- 镜像存在漏洞或被插入恶意脚本，那么生成的容器也可能产生漏洞或被恶意利用。

> **说明：**
> 例如：攻击者可构造特殊的镜像压缩文件，在编译时触发漏洞获取执行任意代码的权限。

- 在镜像中没有指定 USER，默认以 Root 用户的身份运行该镜像创建的容器，当该容器遭到攻击，那么宿主机的 Root 访问权限也可能会被获取。
- 在镜像文件中存储了固定密码等敏感信息并对外进行发布，则可能导致数据泄露的风险。
- 在镜像的编写中添加了不必要的应用，如 SSH、Telnet 等，则会产生攻击面扩大的风险。

仓库镜像安全风险

镜像仓库作为搭建私有镜像存储仓库的工具，主要安全风险来自仓库本身的安全风险和镜像拉取过程中的传输安全风险。

- 仓库自身安全：镜像仓库特别是私有镜像仓库若被恶意攻击者所控制，那么其中所有镜像的安全性将无法得到保证。

> **说明：**
> 例如：私有镜像仓库由于配置不当而开启了2357端口，将会导致私有仓库暴露在公网中，攻击者可直接访问私有仓库并篡改镜像内容，造成仓库内镜像的安全隐患。

- 镜像拉取安全：容器镜像从镜像仓库到用户端的完整性也是镜像安全需关注的内容。

> **说明：**
> 例如：用户以明文形式拉取镜像，在与镜像仓库交互的过程中容易遭遇中间人攻击，会导致拉取的镜像在传输过程中被篡改或被冒名发布恶意镜像，造成镜像仓库和用户双方的安全风险。

本地镜像

最近更新时间：2025-05-20 15:13:01

本文档为您介绍本地镜像功能，并指导您开启扫描数据和查看本地镜像列表。

开启扫描数据

扫描数据展示模块中提供最近扫描检测后的存在风险的镜像数量和镜像总数，镜像存在的安全漏洞、木马病毒和敏感信息数量。

开启一键扫描

1. 登录 容器安全服务控制台，在左侧导航中，单击**镜像风险管理** > **本地镜像**。
2. 在本地镜像页面，单击**一键扫描**，可重新扫描获取最新镜像数据或镜像风险信息。
3. 在扫描设置页面，可根据需求选择检测风险类别和镜像范围。
   - 检测风险类别：安全漏洞、敏感信息和木马病毒。
   - 镜像范围：推荐扫描镜像、全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

4. 选择所需内容后，单击**立即扫描**，即可开始扫描。

> **注意：**
> 开始扫描后，相同镜像 ID 的镜像均会被扫描，且只消耗一次镜像扫描次数配额。

开启定时扫描

1. 在本地镜像页面，单击右侧**定时扫描设置**，可自定义设置是否开启定时扫描功能。

2. 在定时扫描设置页面，单击开启**扫描开关**，并根据需求设置定时扫描时间、扫描风险类别和扫描镜像范围。
   - 定时扫描时间：可以选择固定周期：1天、7天、15天、30天；以及具体更新时间点。
   - 扫描风险类别：单击 图标、按需选择安全漏洞、敏感信息和木马病毒。
   - 扫描镜像范围：推荐扫描镜像、全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

3. 选择所需内容后，单击**保存**或**取消**，即可完成或取消设置。

开启数据更新

在本地镜像页面，单击右侧**同步资产 > 开始更新**，可对所有镜像相关资产信息和安全信息进行立即更新。支持自选节点和全量主机节点进行更新。

> **说明：**
> 最长时间需要1~3分钟。

查看本地镜像列表

筛选镜像资产

在本地镜像页面，可通过以下操作对镜像资产进行筛选：

- 在本地镜像页面，单击**扫描状态下拉框**，按扫描状态对镜像资产进行筛选。

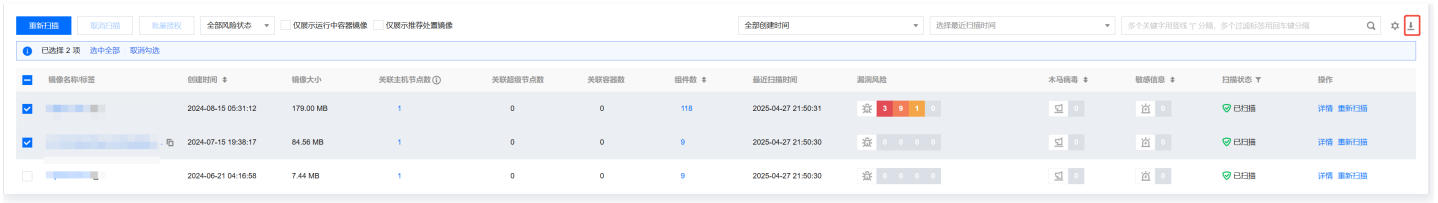
- 在本地镜像页面，单击**安全状态下拉框**，按安全状态对镜像资产进行筛选。

- 在本地镜像页面，单击 勾选仅展示运行中的容器镜像、仅展示推荐处置镜像，可以根据系统对风险紧急程度等因素的判断，确定需要重点关注的镜像资产。

- 在本地镜像页面，单击搜索框通过“镜像名称、镜像 ID”等关键词对镜像资产进行查询。

导出镜像资产

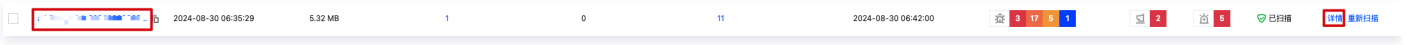
在本地镜像页面，单击 图标勾选所需的本地镜像后，单击 图标即可导出镜像资产。



查看列表详情

1. 在本地镜像页面，单击“镜像名称”，右侧弹出抽屉展示镜像详情。

> **说明：**
> - 镜像风险：镜像扫描是否成功、安全漏洞数量、木马病毒数量和敏感信息数量。
> - 镜像详情：镜像名称、镜像 ID、镜像大小、操作系统类型。
> - 安全漏洞列表：可按漏洞威胁等级对镜像安全漏洞事件进行筛选，或按漏洞名称检索安全漏洞事件。单击**查看详情**可查看漏洞详情及其修复建议。
> - 木马病毒列表：可按木马病毒威胁等级对镜像安全事件进行筛选，或按文件名称检索安全事件。单击**查看详情**可查看木马病毒详情及其处置建议。
> - 敏感信息列表：可按敏感信息威胁等级、敏感信息名称和类型对安全事件进行筛选。
> - 组件信息：该镜像包括的全部组件信息。
> - 镜像构建历史：镜像构建历史日志。



2. 在本地镜像页面，单击“关联主机数”，弹出关联主机详情弹窗，展示了主机名称、主机 IP、Docker 版本等信息。

> **说明：**
> 若关联多个主机，还可以通过以下操作筛主机：
> - 单击主机状态下拉框，按主机状态对主机进行筛选。
> - 单击搜索框通过“主机名、业务组、Docker 版本”等关键词对主机进行查询。

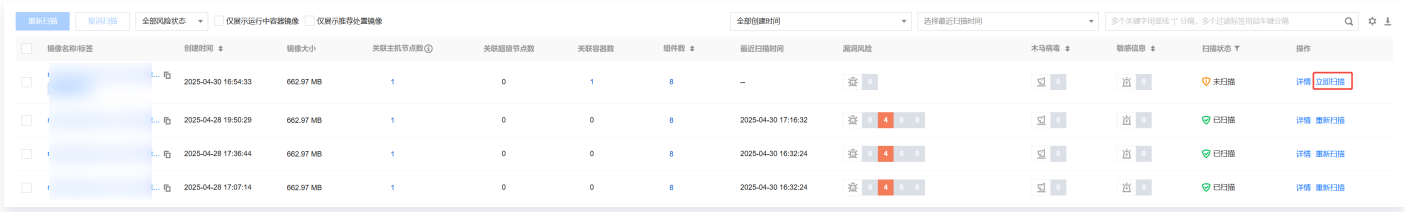
3. 在本地镜像页面，单击“关联容器数”，弹出关联的容器弹窗，展示了容器名称、容器 ID、容器运行状态、CMD、最近更新时间。

> **说明：**
> 若关联多个容器，还可以通过以下操作筛容器：
> - 单击状态下拉框，按容器状态对容器进行筛选。
> - 输入主机名称单击 图标，对主机进行查询。

4. 在本地镜像页面，单击**详情**，右侧抽屉将展示镜像详情。

扫描镜像事件

1. 在本地镜像页面，对镜像扫描状态为“未扫描”时，单击**立即扫描** > **确定**，对镜像进行立即扫描。



2. 在本地镜像页面，上一个扫描任务停止后，单击**重新扫描**，对镜像重新扫描。

> **说明：**
> 可单击 勾选多个镜像后，单击**重新扫描**进行批量重新扫描。

3. 在本地镜像页面，镜像扫描状态为“扫描中”时，单击**取消扫描**，取消扫描镜像。

> **说明：**
> 可单击 勾选多个镜像后，单击**取消扫描**批量取消扫描任务。

自定义列表管理

1. 在本地镜像页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

列表重点字段说明

1. 创建时间：镜像创建时间。
2. 最近扫描时间：显示最近一次扫描时间。
3. 安全风险：展示容器存在的安全风险类型。
4. 状态：展示容器扫描状态，包括已扫描、未扫描、扫描中、已取消和扫描异常。

> **说明：**
> 扫描异常时建议重新扫描。

仓库镜像
仓库镜像

最近更新时间：2025-05-20 15:13:01

本文档为您介绍仓库镜像功能，并指导您开启扫描数据和查看仓库镜像列表。

> **说明：**
> 支持的镜像仓类型：
> - 腾讯云容器镜像服务 TCR/CCR。
> - 第三方镜像仓 Harbor、Quay、JFrog、AWS、AZURE。

前提条件

已购买容器安全 镜像扫描 。

接入腾讯云容器镜像服务

容器安全服务与腾讯云容器镜像服务已默认集成，支持对 TCR 和 CCR 仓库进行镜像扫描。

> **说明：**
> - 容器安全服务默认通过公网请求 TCR 仓库资产，若您的仓库实例启用了访问控制，使用前请先添加服务 IP 地址段白名单，或切换网络类型。在 仓库镜像页面，单击页面上方的**操作指南**展开弹窗，按照配置方法添加 IP 地址白名单或切换网络类型使用 VPC 网络。
> - 首次使用时需手动同步仓库镜像资产，单击 仓库镜像页面 右上方的**同步资产**，更新仓库镜像资产，首次同步时间可能较长。
> - 后台每天凌晨0点至3点间会自动同步仓库镜像资产数据。

接入第三方镜像仓 Harbor

1. 登录 容器安全服务控制台 ，在左侧导航中，单击**镜像风险管理** > **仓库镜像**。
2. 在仓库镜像页面，单击右上角的**镜像仓管理**。

3. 在镜像仓库列表中，单击**添加镜像仓**。
4. 在添加镜像仓弹窗中，配置相关参数，单击**确定**。

参数说明：

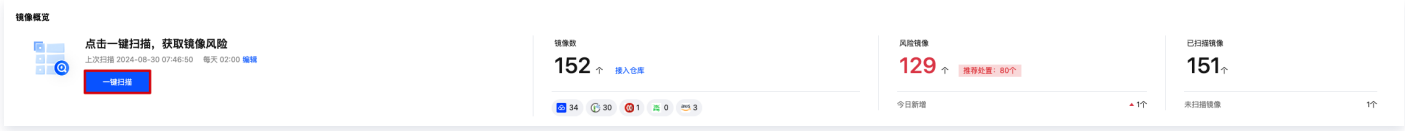
参数名称	说明
实例名称	填写镜像仓实例名称，实例名称唯一，不可为空
仓库类型	选择第三方镜像仓库类型。目前支持选择 Harbor 仓。
版本	选择第三方镜像仓库的版本。支持选择以下版本： • V1：镜像仓库版本为1.X.X。 • V2：镜像仓库版本为2.X.X及以上。
网络类型	选择第三方镜像仓库的网络访问类型。目前支持公网。
地域	选择第三方镜像仓库所在区域，Harbor 类型为默认值“默认地域”。
地址	输入第三方镜像仓库访问地址。
用户名	输入访问第三方镜像仓库的用户名。
密码	输入访问第三方镜像仓库的密码。
限速	选择每小时可同步拉取的镜像个数。默认为不限制。可选值：5、10、20、50、100、500、1000、不限制。
跳过证书认证	确定镜像同步是否要验证远程镜像仓库实例的证书，如果远程实例使用的是自签或者非信任证书，不要勾选此项。默认为勾选。

开启扫描数据

在 仓库镜像页面 扫描数据展示模块中提供最近扫描检测后的存在风险的镜像数量和镜像总数，镜像存在的安全漏洞、木马病毒和敏感信息数量。

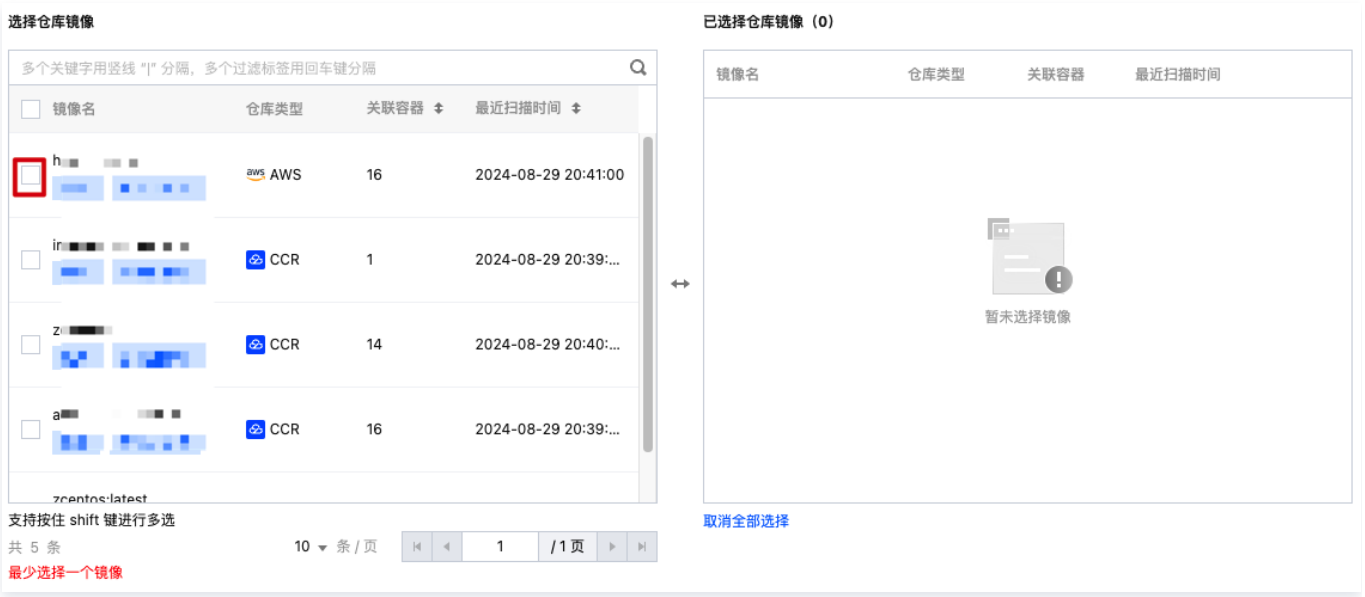
开启一键扫描

1. 在仓库镜像页面，单击右侧**一键扫描**，可获取最新镜像数据或镜像风险信息。



2. 在扫描设置页面，可根据需求选择检测风险类别和镜像范围。
   - 检测风险类别：包含安全漏洞、敏感信息和木马病毒。
   - 超时设置：若单次扫描时长超出设置时间，即视为扫描失败。
   - 镜像范围：推荐扫描镜像、全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。



3. 选择所需内容后，单击**立即扫描**，即可开始扫描。

> **注意：**
> 开始扫描后，相同镜像 ID 的镜像均会被扫描，且只消耗一次镜像扫描次数配额。

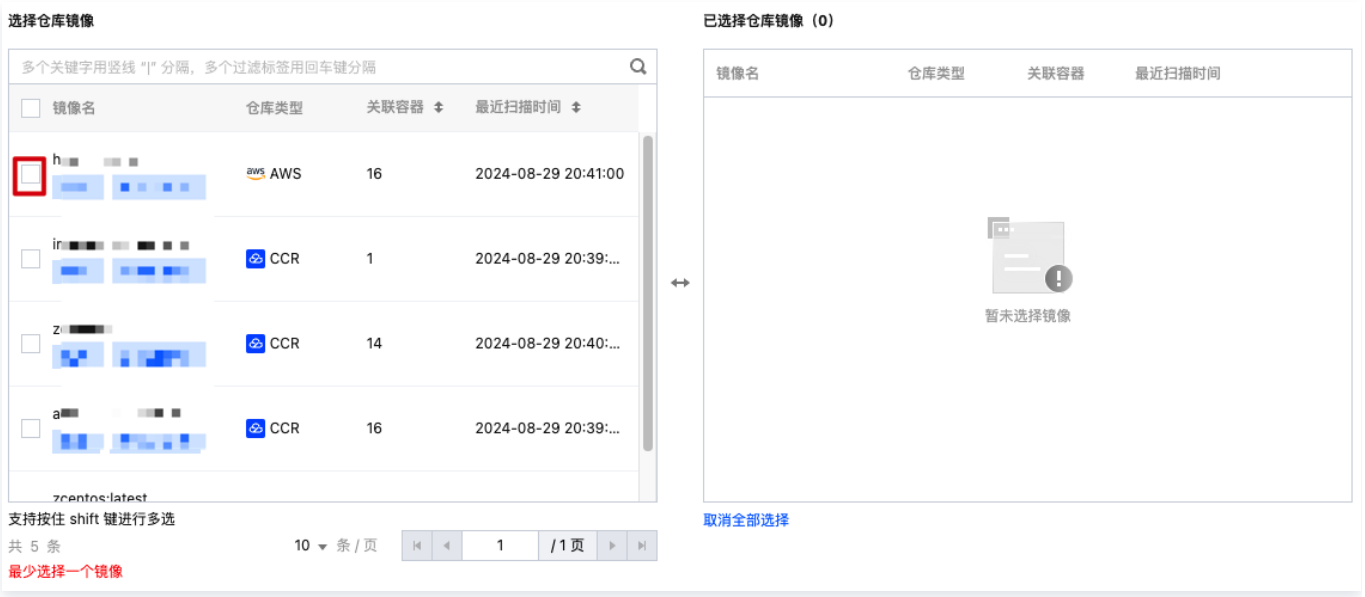
开启定时扫描

1. 在仓库镜像页面，单击右侧**定时扫描设置**，可自定义设置是否开启定时扫描功能。

2. 在定时扫描设置页面，单击开启**扫描开关**，并根据需求设置定时扫描时间、检测风险类别和镜像范围。
   - 定时扫描时间：可以选择固定周期：1天、7天、15天、30天；以及具体更新时间点。
   - 检测风险类别：单击 图标、按需选择安全漏洞、敏感信息和木马病毒。

- 镜像范围：推荐扫描镜像、全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。



3. 选择所需内容后，单击**保存**或**取消**，即可完成或取消设置。

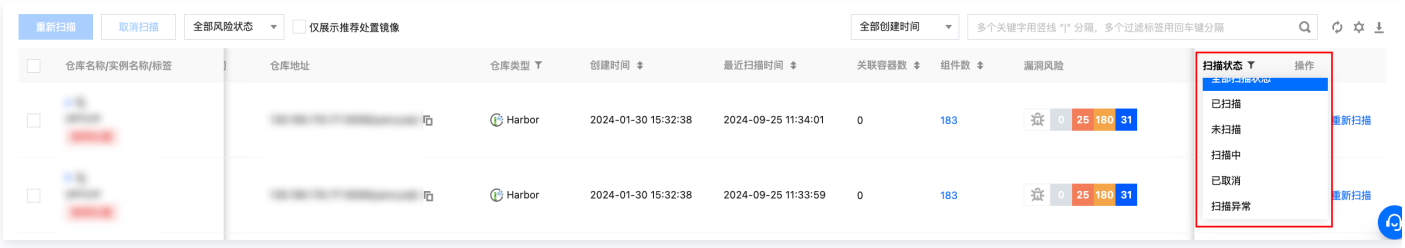
查看仓库镜像列表

登录 容器安全服务控制台，在左侧导航中，单击**镜像风险管理** > **仓库镜像**，进入仓库镜像页面。

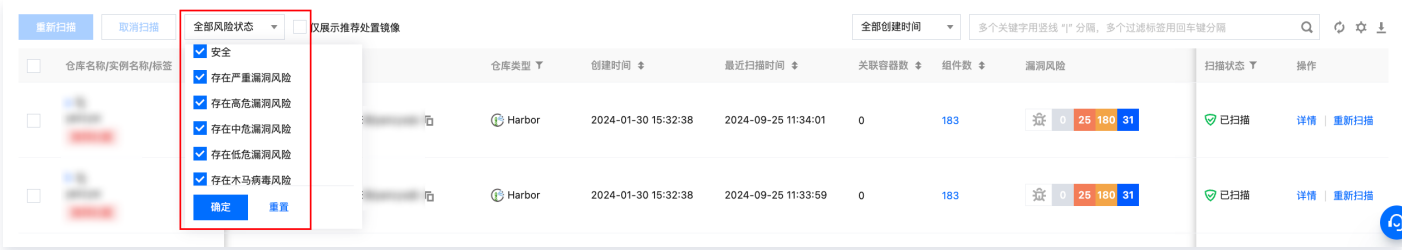
筛选镜像资产

在仓库镜像页面，可通过以下操作对镜像资产进行筛选：

- 在仓库镜像页面，单击扫描状态下拉框，按扫描状态对镜像资产进行筛选。



- 在仓库镜像页面，单击安全状态下拉框，按安全状态对镜像资产进行筛选。



- 在仓库镜像页面，单击仓库类型下拉框，按仓库类型对镜像资产进行筛选。

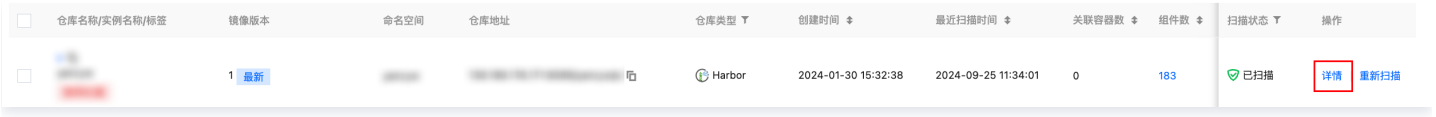
- 在仓库镜像页面，单击搜索框，可通过“镜像名称、镜像 Digest”等关键词对镜像资产进行查询。

导出镜像资产

在仓库镜像页面，单击 图标勾选所需的镜像仓库后，单击 图标即可导出镜像资产。

查看列表详情

在仓库镜像页面，单击**详情**，右侧抽屉展示镜像详情，可查看镜像风险、镜像详情和安全漏洞列表等信息。



说明：

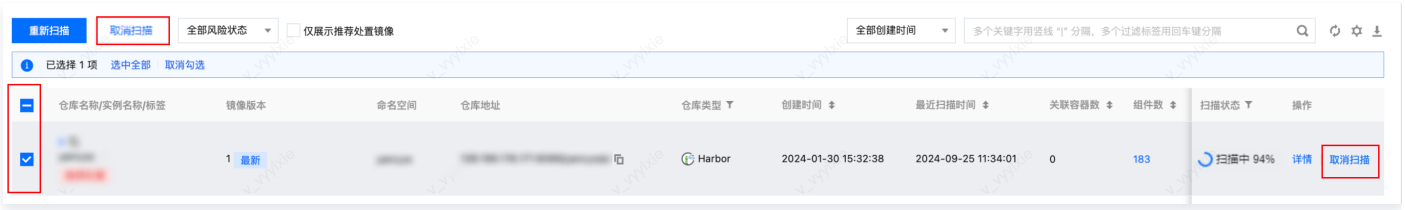
- 镜像风险：镜像扫描是否成功、安全漏洞数量、木马病毒数量和敏感信息数量。
- 镜像详情：镜像名称、镜像 Digest、镜像大小。
- 安全漏洞列表：可按漏洞威胁等级对镜像安全漏洞事件进行筛选，或按漏洞名称检索安全漏洞事件。单击**查看详情**查看漏洞详情及其修复建议。
- 木马病毒列表：可按木马病毒威胁等级对镜像安全事件进行筛选，或按文件名称检索安全事件。单击**查看详情**查看木马病毒详情及其处置建议。
- 敏感信息列表：可按敏感信息威胁等级、敏感信息名称和类型对安全事件进行筛选。
- 镜像层：该镜像详细的层信息。
- 关联容器：该镜像下载到主机上运行的容器。
- 组件信息：该镜像包括的全部组件信息。
- 构建历史：镜像构建历史日志。

扫描镜像事件

1. 在仓库镜像页面，对镜像扫描状态为“未扫描”时，单击**立即扫描** > **确定**，对镜像进行立即扫描。

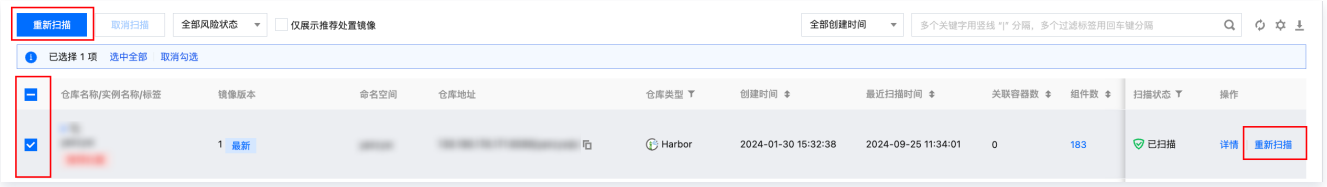
2. 在仓库镜像页面，镜像扫描状态为“扫描中”时，单击**取消扫描**，取消扫描镜像。

> **说明：**
>
> 可单击 勾选多个镜像后，单击**取消扫描**取消扫描任务。



3. 在仓库镜像页面，上一个扫描任务停止后，单击**重新扫描**，对镜像重新扫描。

> **说明：**
>
> 可单击 勾选多个镜像后，单击**重新扫描**进行批量重新扫描。



自定义列表管理

1. 在仓库镜像页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

列表字段说明

1. 镜像仓库地址：仓库镜像来源地址。

2. 仓库类型：镜像仓库的类型，目前包括 TCR、CCR 等。
3. 镜像版本：仓库镜像的版本号。
4. 最近扫描时间：显示最近一次扫描时间。
5. 安全风险：展示容器存在的安全风险类型。
6. 状态：展示容器扫描状态，包括已扫描、未扫描、扫描中、已取消和扫描异常。

> **注意：**
> 扫描异常时建议重新扫描。

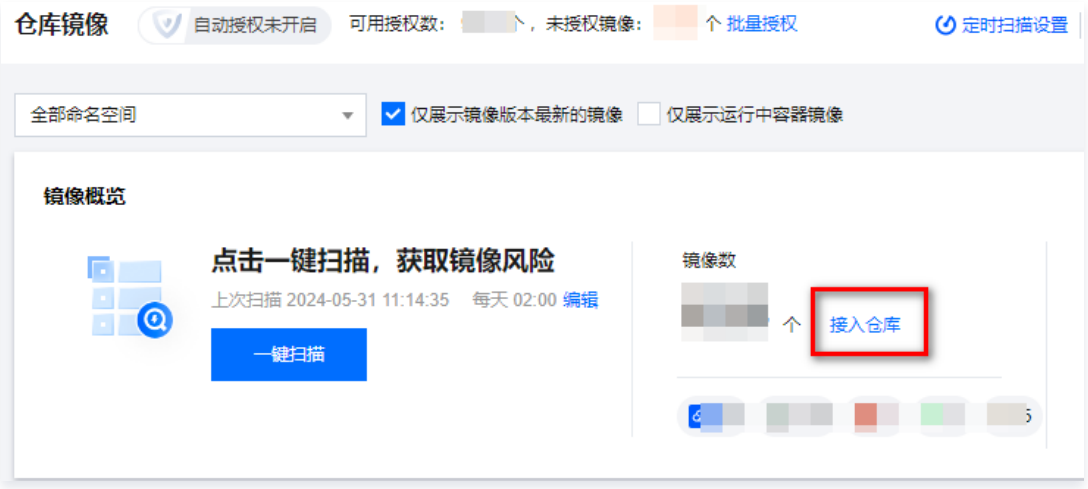
接入 AWS 镜像仓库

最近更新时间：2025-05-13 18:11:12

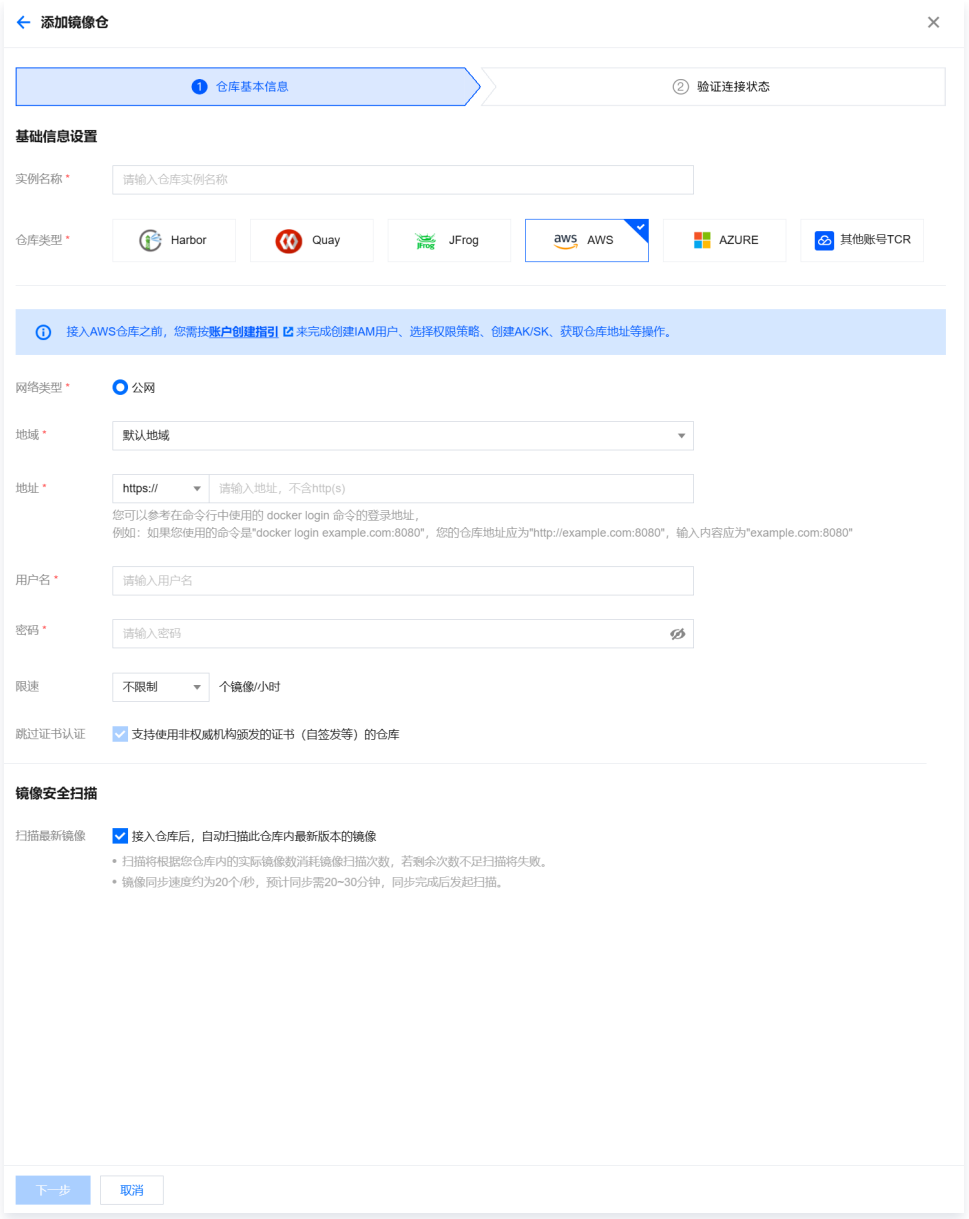
当您需要将 AWS 账户上的仓库镜像接入腾讯云容器安全服务控制台进行安全扫描时，可以参考本文接入 AWS 镜像仓库。

接入仓库

1. 登录 容器安全服务控制台，在左侧导航中，单击**镜像风险管理** > **仓库镜像**。
2. 在仓库镜像页面，单击**接入仓库**。



3. 在添加镜像仓弹窗中，配置相关参数，单击**下一步**。



参数名称	说明
实例名称	填写镜像仓实例名称，实例名称唯一，不可为空。
仓库类型	选择第三方镜像仓库类型。目前支持的选择包括 Harbor、Quay、JFrog 和 AWS。接入 AWS 仓库时，请选择 AWS。
网络类型	选择第三方镜像仓库的网络访问类型。AWS 仓库仅支持公网。
地域	选择第三方镜像仓库所在区域，AWS 类型为默认值“默认地域”。
地址	输入第三方镜像仓库访问地址。您可以参考在命令行中使用的 docker login 命令的登录地址，例如：如果您使用的命令是"docker login example.com:8080"，您的仓库地址应为"http://example.com:8080"，输入内容应为"example.com:8080"
用户名	输入访问第三方镜像仓库的用户名。详情请参见 创建 AWS 账户。
密码	输入访问第三方镜像仓库的密码。详情请参见 创建 AWS 账户。
限速	选择每小时可同步拉取的镜像个数。默认为不限制。可选值：5、10、20、50、100、500、1000、无限制。
跳过证书认证	确定镜像同步是否要验证远程镜像仓库实例的证书，如果远程实例使用的是自签或者非信任证书，不要勾选此项。默认为勾选。

扫描最新镜像	自动扫描此仓库内最新版本的镜像。镜像同步速度约为20个/秒，预计同步需20~30分钟，同步完成后发起扫描。

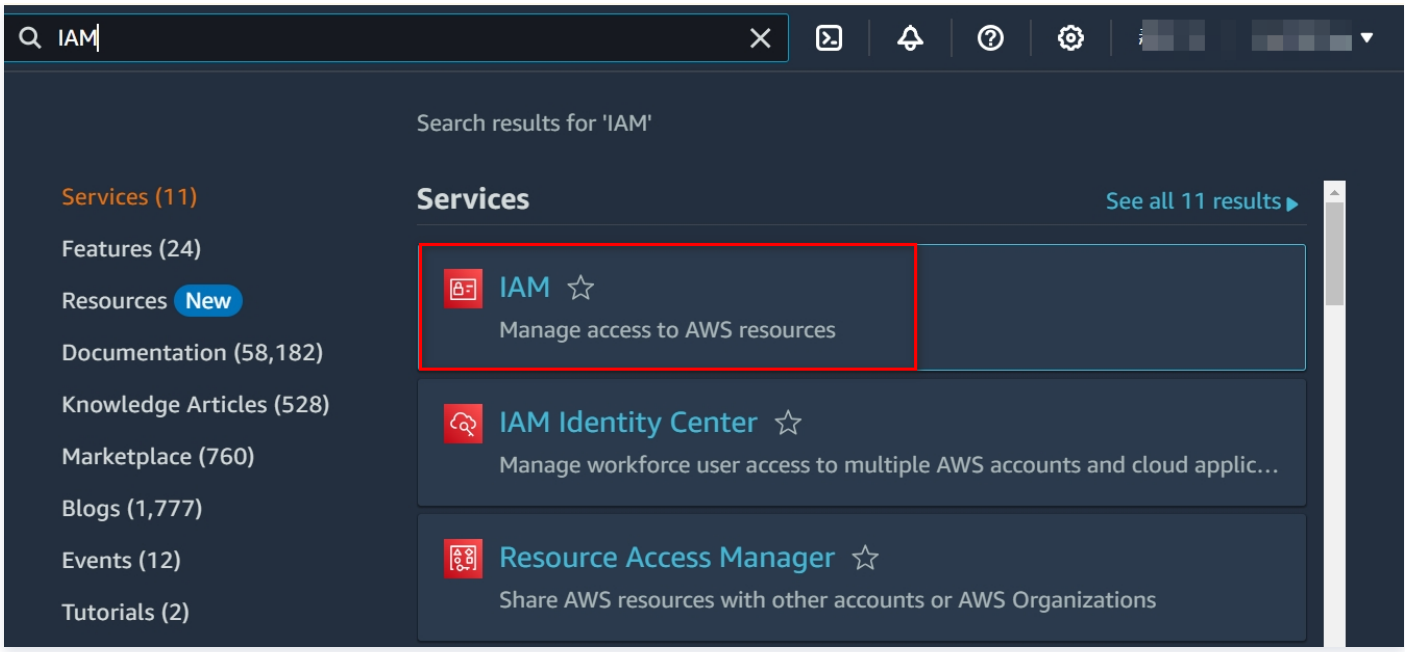
4. 在验证链接状态，选择**连接方式**，单击**确认添加**。

> **说明：**
> 验证连接状态：可选择**自有主机节点连接**或**产品后台连接**。
> - 自有主机节点连接：选择您自有的主机节点进行仓库镜像拉取及扫描。建议您选择自有主机节点连接，以获得更好的镜像扫描速度。
> - 产品后台连接：使用容器安全服务产品侧后台服务进行仓库镜像拉取及扫描，扫描速度较慢，耗时较长。

创建 AWS 账户

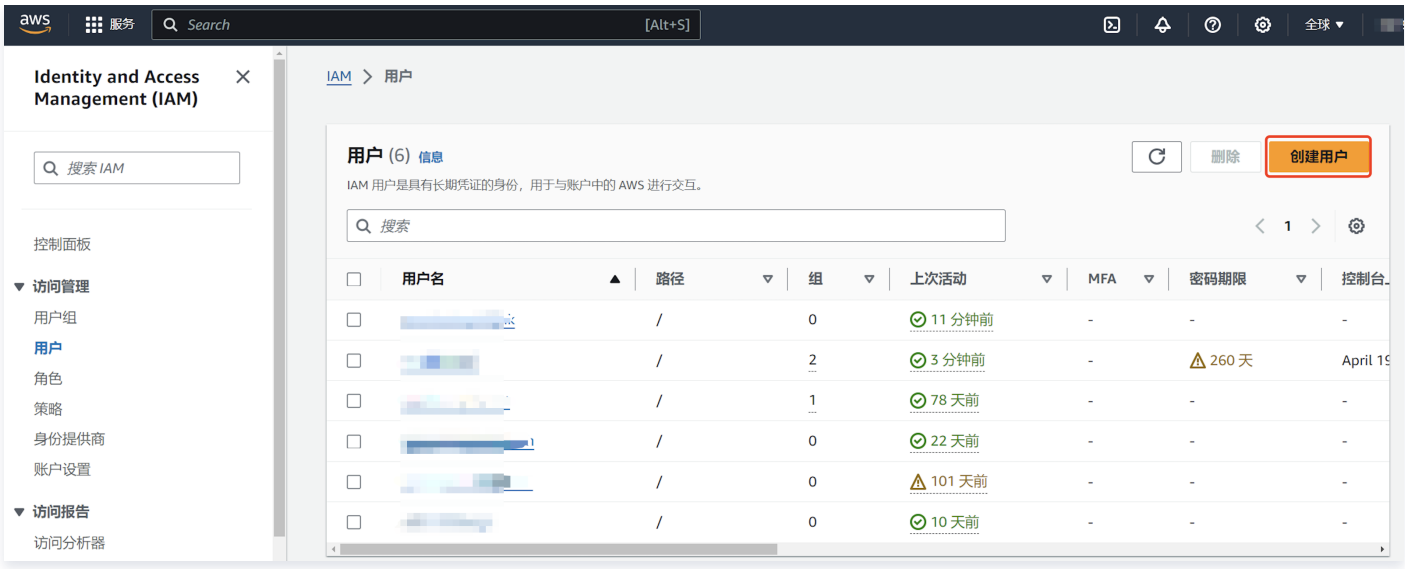
步骤1：创建 IAM 用户

1. 登录 AWS 控制台，选择 IAM 服务。



2. 在 IAM 控制面板中，单击**用户数**，进入用户列表。

3. **在用户列表中，单击创建用户。**

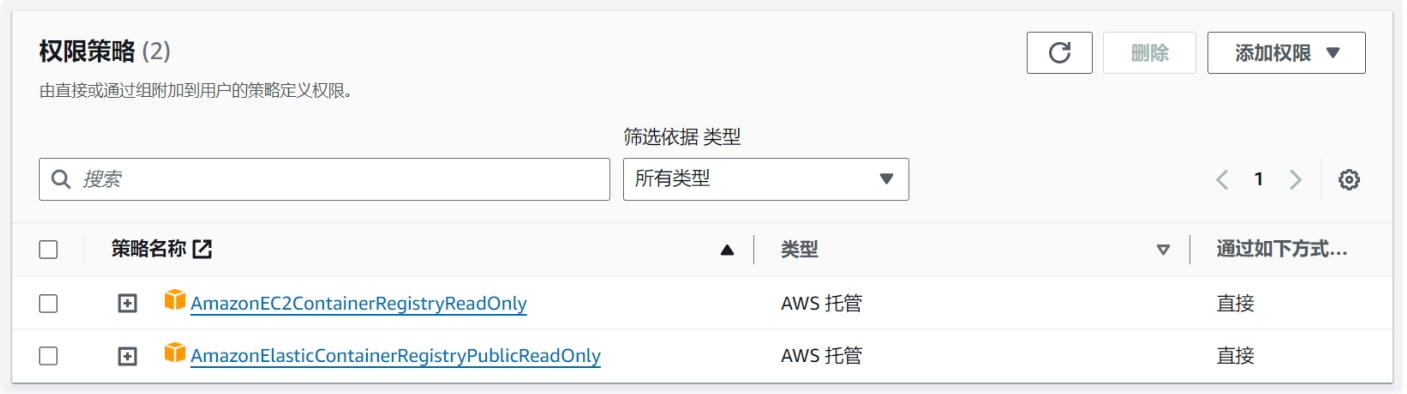


4. 在创建用户页面，按页面提示输入用户名，单击**下一步**。

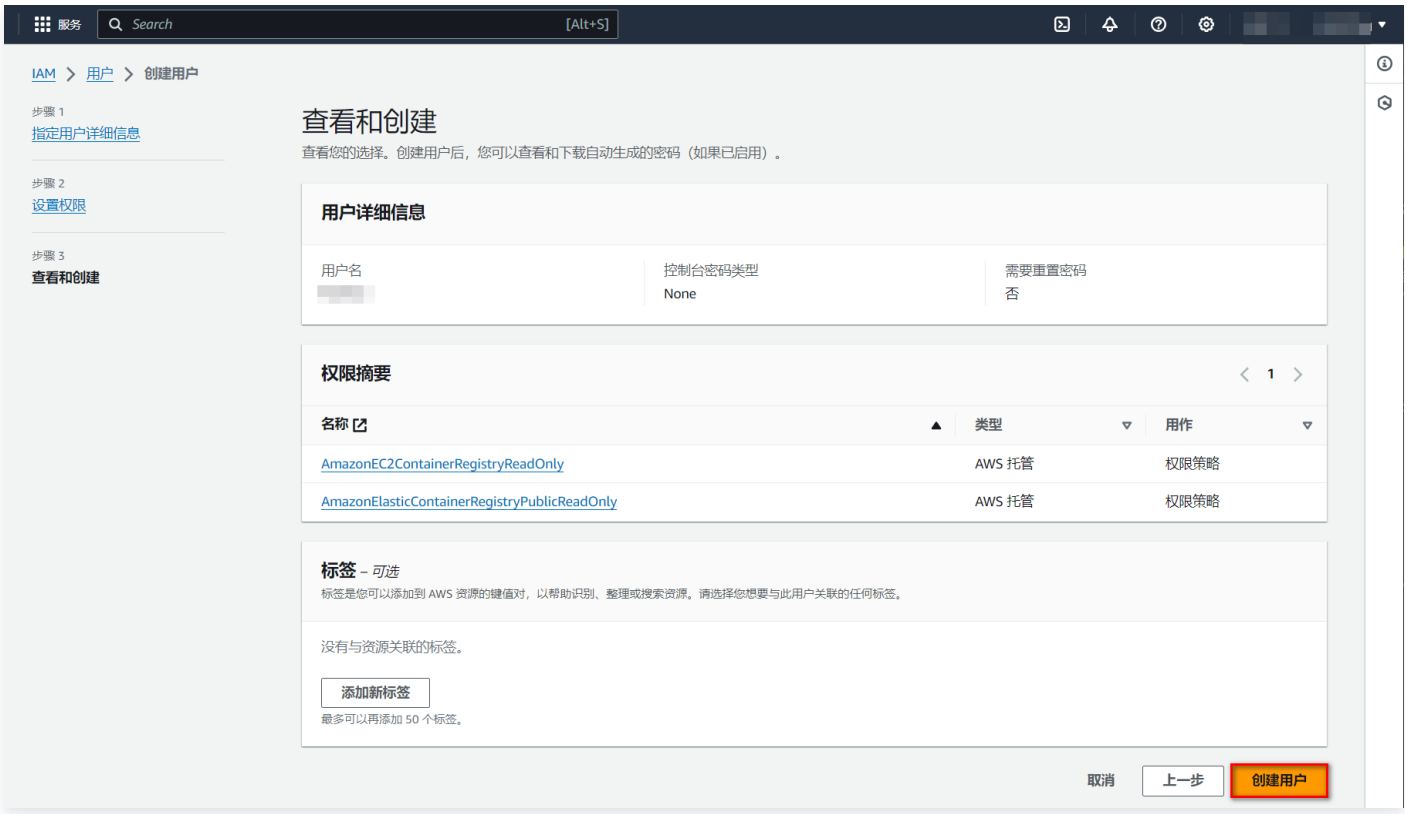
> **说明：**
> 启用控制台访问选项可根据需要进行配置，本指引不要求勾选。

5. 在设置权限页面，选择**直接附加策略**。

6. **在权限策略选择时，选择如下两个策略：**AmazonEC2ContainerRegistryReadOnly、AmazonElasticContainerRegistryPublicReadOnly。

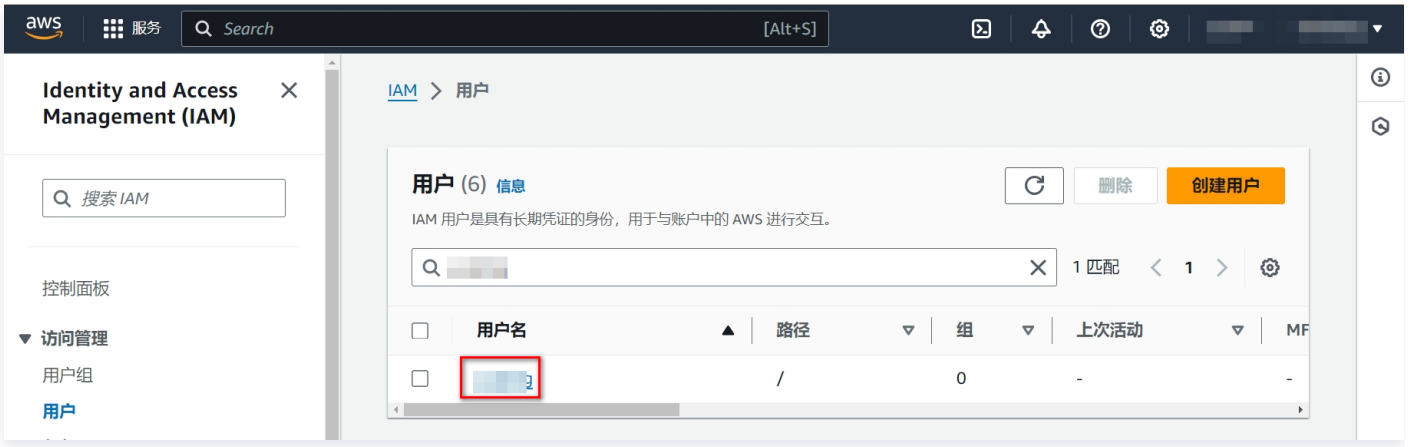


7. **完成上述配置，单击下一步进入查看和创建页面，单击创建用户完成创建 IAM 用户。**



步骤2：创建 AK/SK

1. 在用户列表中，单击**用户名**，进入用户摘要页面。

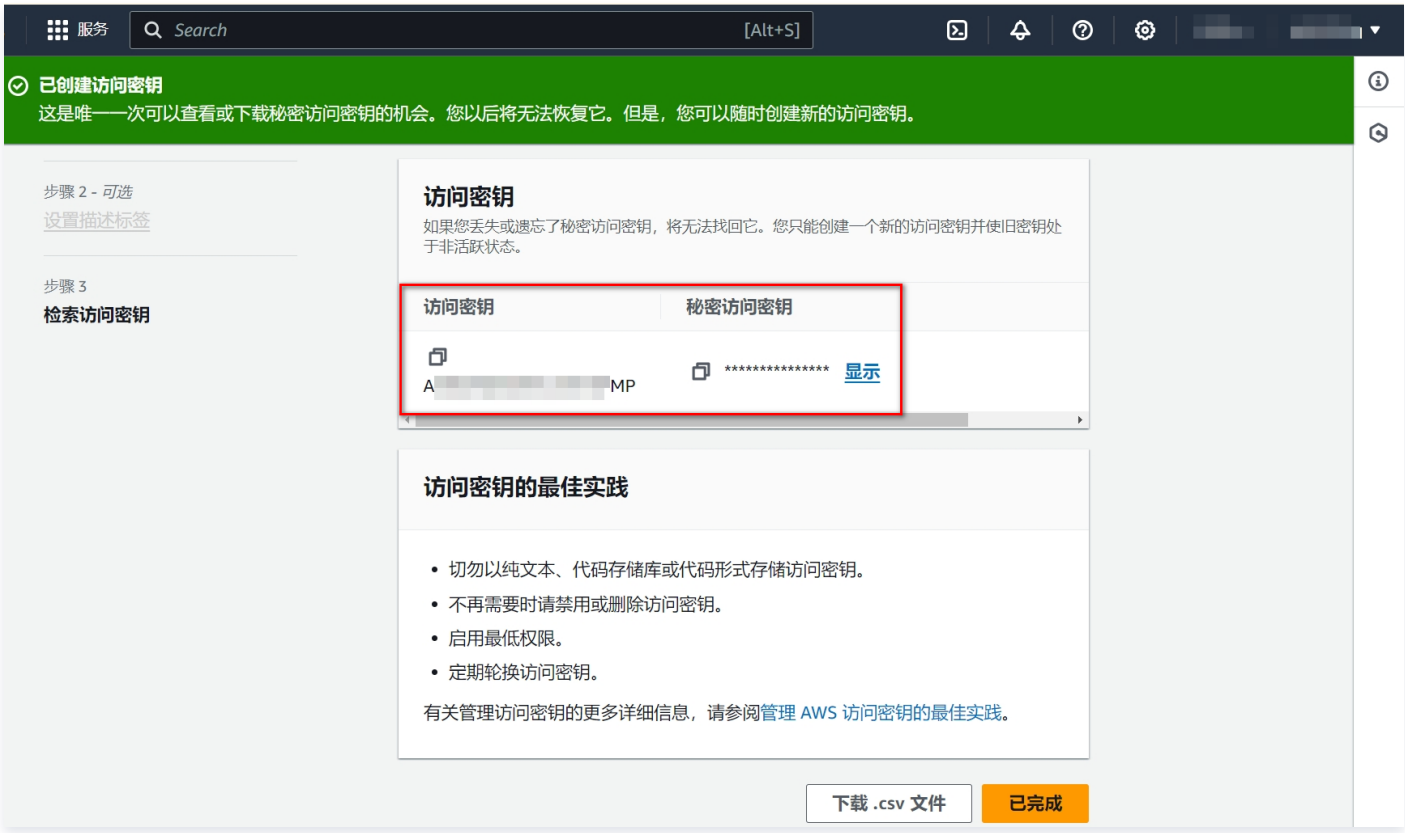


2. 在用户摘要页面，单击访问密钥处的**创建访问密钥**。

3. 在访问密钥最佳实践和替代方案中，选择“在 AWS 之外运行的应用程序”。

4. 在设置描述标签中，输入标签值，单击**创建访问密钥**，即可完成 AK/SK 访问密钥的创建。

5. 在检索访问密钥页面，访问密钥即接入 AWS 仓库所需的用户名，秘密访问密钥即接入 AWS 仓库所需的密码。



镜像拦截事件

最近更新时间：2025-04-29 10:57:52

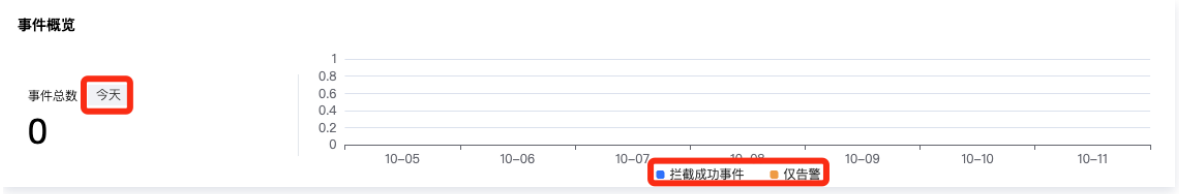
用户可在 镜像拦截策略页面 配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

- 创建并生效拦截策略后，约3-5分钟左右生效。生效后，如命中的风险镜像存在启动容器行为，系统将按照策略配置的告警、拦截要求，对镜像启动行为进行告警、或拦截容器启动并上报拦截记录。
- 目前支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像。
- 拦截特权模式镜像仅支持配置一条规则，如需修改拦截镜像的范围，可编辑调整已配置规则。

事件概览

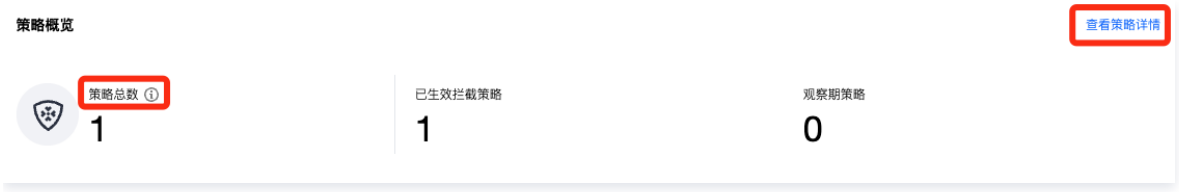
用户配置镜像启动拦截策略后，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录。
在 镜像拦截事件 > **事件概览**中，将对每日镜像启动拦截事件和仅告警的事件进行统计，展示近7日两类事件的趋势图和当前的事件总数。

> **说明：**
> 容器告警事件仅保留半年以内的数据，每天定时检测并自动清理超过180天的告警事件，超出时间范围将无法显示和查询。如有需要，建议使用 日志投递 留存。



策略概览

在 镜像拦截策略页面 配置告警和拦截策略后，系统将统计开启的策略总数，以及其包含的已生效拦截策略和观察期策略数量。在 镜像拦截事件 > **策略概览**中，单击**查看策略详情**，跳转**策略管理** > **镜像拦截策略**页面查看镜像拦截策略详情。



事件列表

在 镜像拦截事件 > **事件列表**中，记录的为已生效拦截策略产生的镜像启动拦截事件和观察期策略产生的镜像启动告警事件。用户可通过事件类型、执行动作、最近生成时间等进行筛选，或通过命中策略、镜像名称、镜像 ID、镜像所在节点名称、节点内网 IP、节点外网 IP 等进行关键字检索。

- 事件类型包括：风险镜像拦截，即镜像包括某些漏洞、木马或敏感信息，需对包含这些风险的镜像进行拦截；特权镜像拦截，即镜像以特权模式启动容器时，进行拦截。
- 执行动作包括：拦截成功，即已生效拦截策略产生的镜像启动拦截事件；告警，即观察期策略产生的镜像启动告警事件。
- 用户可单击操作列的**详情**，查看事件详情，包括事件详情、命中策略、影响范围、风险描述和解决方案。
  - 事件详情：系统会对同一镜像的同一拦截或告警事件进行聚合，聚合时间为当天。此部分展示拦截或拦截事件的事件类型、事件数量和发生的时间段。
  - 命中策略：展示已生效拦截策略或观察期策略的名称、类型、启动状态、策略状态、开始拦截时间、策略描述和策略拦截内容。用户可单击策略名称/策略类型旁的**详情**，查看此条事件关联的策略详情。
  - 影响范围：展示需拦截的目标镜像的名称、镜像 ID、镜像所在节点的名称和 IP 等。

- 风险描述：展示详细的拦截事件或告警事件的原因，例如由于存在严重漏洞，命中拦截策略。同时展示详细的镜像启动参数。
- 解决方案：建议用户对存在漏洞、木马病毒或敏感信息的镜像进行修复，避免影响业务。

集群安全管理

集群检查

最近更新时间：2025-05-13 18:11:12

集群检查功能提供集群检查列表、集群风险统计、集群检查详情、检查项管理等功能，通过集群检查对指定集群安装检查组件并执行风险检查，查看集群风险详情。

安装集群检查组件

1. 登录 容器安全服务控制台，在左侧导航单击**集群安全管理 > 集群检查**。
2. 在集群检查页面，已内置每1小时定期同步集群资产；单击**同步资产**，可进行手动同步集群资产。

> **说明**
> - 目前集群检查列表支持同步的集群资产为 TKE 托管集群 和 TKE 独立集群。
> - 首次使用集群安全时，需要手动进行一次“同步资产”，后续系统会进行自动同步。

3. 在集群检查页面，支持单个或批量接入集群。
   - 单个：选择所需集群 ID，单击**接入集群**，弹出“集群接入”窗口。

   - 多个：选择多个腾讯云集群 ID，单击**批量接入集群**，弹出“集群接入”窗口。自建集群暂不支持批量接入。

4. 在“集群接入”窗口中，选择需要接入的TKE集群，或按页面提示针对自建集群进行接入。

5. 确认接入后，系统将在集群内所有节点部署 DaemonSet 组件，安装成功后防护状态将展示为未防护；开通容器安全服务后，将展示为已防护。

> **说明**
> - 集群接入后，将会在该集群创建“tcss命名空间”，并创建如下工作负载资源，需确保以下3个工作负载正常运行：
>   1.1 tcss 命名空间下安装名称为“init-tcss-agent”的 Job 类型工作负载。
>   1.2 tcss 命名空间下安装名称为“tcss-asset”的 Deployment类型工作负载。
>   1.3 kube-system 命名空间下安装名称为“yunjing-agent” 的 DaemonSet 类型工作负载。
> - DaemonSet 对集群运行和性能无影响，占用资源限制为：
>   - cpu：100-250m。
>   - mem：100Mi-250Mi。
> - 若需要删除集群检查组件可登录 容器服务控制台，在集群详情页面单击**工作负载**，选择 DaemonSet，在 kube-system 命名空间下选择 yunjing-agent 操作单击**更多** > **删除**。

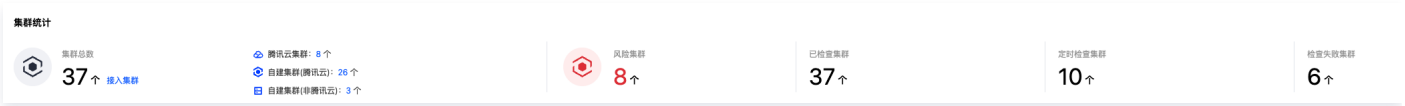
执行集群检查

在 集群检查页面，您可指定集群单击**重新检查**或指定多个集群单击**批量检查**执行集群检查。

> **说明**
> 集群检查组件默认为未接入状态，执行集群检查前需要先接入集群。

查看集群检查结果

1. 在 集群检查页面，集群统计卡片展示集群总数、风险集群等数量。



2. 在集群检查页面，单击集群列表操作列的**详情**，进入“集群详情”页面。

3. 在“集群详情”页面，展示了当前集群所有被检出的集群状态、集群详情和风险详情。


集群详情：aliyun
集群信息
主机节点 (5)
命名空间 (6)
Workload (11)
Pod (11)
Service (19)
Ingress (0)
重新检查
同步资产
集群状态
近一次检查时间：2024-08-29 15:00:47
检查失败
由于任务扫描超时，检查失败，请 点击重试
点击查看异常处理指南
严重 0 个
高危 0 个
中危 0 个
低危 0 个
集群详情
集群名称/ID
节点总数 5
集群状态 • 运行中
集群类型 自建集群(非腾讯云)
地域 其他地域（其他）
Kubernetes版本
运行时组件
集群Master IP
风险详情
威胁等级
检查项
检查对象
风险类别
风险类型
操作
高危 K8S开启Seccomp安全机制 Pods 配置风险 权限提升 查看详情
低危 镜像Tag未配置或者使用了latest Pods 配置风险 配置异常 查看详情
中危 未配置最大内存资源限制 Pods 配置风险 抢占资源 查看详情
低危 未配置最少内存资源需求 Pods 配置风险 抢占资源 查看详情
中危 未配置CPU最大资源限制 Pods 配置风险 抢占资源 查看详情
低危 未配置最少CPU资源需求 Pods 配置风险 抢占资源 查看详情
中危 未配置系统文件修改权限 Pods 配置风险 恶意篡改 查看详情
高危 配置了容器进程特权capabilities Pods 配置风险 恶意篡改 查看详情
高危 未配置容器进程权限 Pods 配置风险 权限提升 查看详情
高危 启用了特权模式运行容器 Pods 配置风险 权限提升 查看详情
共 18 项
10 条 / 页
1
/ 2 页

4. 在风险详情列表，选择所需风险检查项，单击**查看详情**，进入“风险检查项详情”页面。

5. 在“风险检查项详情”页面，展示该风险检测项的风险详情、风险描述、解决方案以及当前集群的影响资产范围。

定时检查设置

1. **单击**页面上方的**定时检查设置**，可对需要开启定时检查的集群进行配置。

2. 在定时检查设置抽屉中，可配置定时检查开关、定时检查周期、检查项管理和检查集群范围选择。
   - 定时检查开关：用户可自定义开启或关闭。
   - 定时检查周期：可选择每天、每隔7天、每隔15天、每隔30天，设置后会在周期选定的时间点开始定时检测。
   - 检查项管理：点击编辑按钮打开检查项管理抽屉，可针对每一个检查项进行开启和关闭。
   - 检查集群范围选择：可选择全部集群或自选集群开启定时检查。

3. 在“定时检查设置”窗口中，单击**保存**，配置的定时检查设置将生效。

> **说明**
> 确认后，自动检查将开启。检测内容如下：
> - 开启集群定时检查后，当集群节点有新增时，将自动检查集群新增节点。

管理集群检查项

1. 在 集群检查页面，单击界面右上角的**检查项管理**，进入检查项设置页面。
2. 在检查项设置页面，检查项列表展示了系统执行集群检查的所有检查项，单击**查看详情**可查看检查项的详细信息。

全部风险等级 | 全部检查对象 | 全部风险类别 | 全部风险类型 | 请输入检查项名称进行

威胁等级	检查项	检查对象	风险类别	风险类型	忽略资产	检查项开关	操作
高危	禁止授予ServiceAccount default写入/修改权限	RBAC	配置风险	恶意篡改	0		查看详情
高危	未开启内核保护	Kubelet	配置风险	恶意篡改	0		查看详情
高危	未配置安全的授权模式	Kubelet	配置风险	未授权访问	0		查看详情
高危	未加密 etcd 键值存储。	API Server	配置风险	敏感信息泄露	0		查看详情
高危	未使用TLS加密对Etcd客户端的连接	API Server	配置风险	未授权访问	0		查看详情
高危	未在 API 服务器上设置 TLS 连接。	API Server	配置风险	未授权访问	0		查看详情
高危	未在 apiserver 上为服务帐户设置服务帐户公钥文件。	API Server	配置风险	未授权访问	0		查看详情
高危	未在验证令牌之前验证服务帐户。	API Server	配置风险	未授权访问	0		查看详情
中危	未禁用程序分析	API Server	配置风险	抢占资源	0		查看详情
高危	未限制kubelet 可以修改的Node和Pod资源	API Server	配置风险	恶意篡改	0		查看详情

共 161 项 | 10 条 / 页 | 1 / 17 页

自建集群

最近更新时间：2025-05-13 18:11:12

本文介绍接入自建集群的步骤，您可以将自建集群接入容器安全服务进行统一管理，对自建集群开展集群风险检查和管理。

> **说明**
> K8s 集群支持1.13以上版本。

限制条件

接入自建集群节点规模小于500节点。

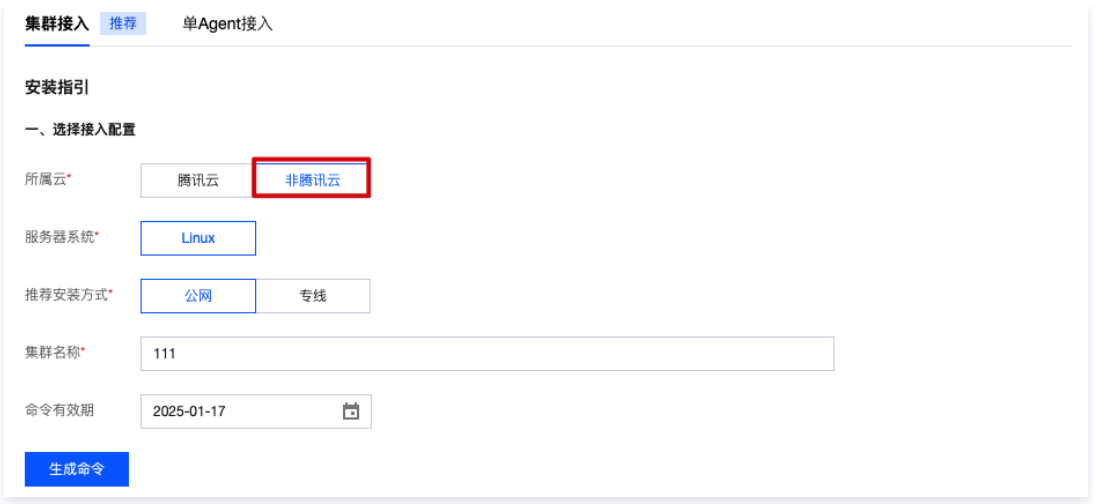
操作步骤

1. 登录 容器安全服务控制台，在左侧导航中，单击**集群安全管理** > **集群检查**。
2. 在集群检查页面，单击**接入集群**。

3. 在集群接入页面，选择所属云为**腾讯云**或**非腾讯云**。
   - 腾讯云：**自建集群**的云服务器资源来源于**腾讯云**，需按页面提示选择推荐安装方式和集群名称。

   - 非腾讯云：选择**非腾讯云**，按页面提示配置推荐方案方式、集群名称、命令有效期。

> **说明：**
> 接入集群的云服务器资源来源于其他云，包括其他云的自建集群、独立集群、托管集群等。



4. 单击**生成命令**，可复制并执行相关命令。可以下方下载或复制 Yaml 文件内容，并通过以下两种方式安装。

> **说明：**
> 建议您针对单个集群生成单个接入命令，以避免集群名称重复。

- 方式一：单击**复制命令链接**，拷贝到可以执行k8s命令的机器执行。您也可以先下载下方 Yaml 文件，拷贝到机器上并执行 `kubectl apply -f tcss.yaml` 。
- 方式二：前往 容器服务控制台 -集群详情页面，通过“使用 Yaml 文件创建资源”复制命令内容。

```
---
apiVersion: v1
kind: Namespace
metadata:
name: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
apiGroup: ""
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io
```

```
---
apiVersion: v1
kind: ServiceAccount
metadata:
name: tcss-agent
namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes", "services", "serviceaccounts", "configmaps",
"componentstatuses"]
verbs: ["get", "list", "watch"]
- apiGroups:
["apps","batch","extensions","rbac.authorization.k8s.io","networking.k8s.io","cilium.io"]
resources: ["*"]
verbs: ["get", "list","watch"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["apiextensions.k8s.io"]
resources: ["customresourcedefinitions"]
verbs: ["list", "get","create"]
- apiGroups: ["apiextensions.k8s.io"]
resourceNames: ["tracingpolicies.cilium.io", "tracingpoliciesnamespaced.cilium.io"]
resources: ["customresourcedefinitions"]
verbs: ["list", "get", "update"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io


---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
```

```
type: kubernetes.io/service-account-token


---
apiVersion: batch/v1
kind: Job
metadata:
name: init-tcss-agent
namespace: tcss
spec:
template:
spec:
serviceAccountName: tcss-agent
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
imagePullPolicy: Always
name: init-tcss-agent
command: ["/home/work/yunjing-agent"]
args: ["-token",'',"-vip",'','-cc']
resources:
limits:
cpu: 100m
memory: 512Mi
requests:
cpu: 100m
memory: 128Mi
env:
- name: user_tags
value: "default"
- name: k8s_name
value: "11"
- name: appid
value: "*********"
securityContext:
privileged: true
volumeMounts:
- mountPath: /run/secrets/kubernetes.io/tcss-agent
name: token-projection
securityContext: {}
hostPID: true
restartPolicy: Never
volumes:
- name: token-projection
secret:
secretName: tcss-agent-secret
backoffLimit: 5

---
apiVersion: apps/v1
kind: DaemonSet
metadata:
labels:
k8s-app: yunjing-agent
name: yunjing-agent
namespace: kube-system
annotations:
config.kubernetes.io/depends-on: batch/v1/namespaces/tcss/jobs/init-tcss-secrets
spec:
selector:
```

```
matchLabels:
k8s-app: yunjing-agent
template:
metadata:
annotations:
eks.tke.cloud.tencent.com/ds-injection: "true"
labels:
k8s-app: yunjing-agent
spec:
tolerations:
- operator: Exists
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
imagePullPolicy: Always
name: yunjing-agent
command: ["/home/work/yunjing-agent"]
args: ["-d","-token",'',"-vip",'']
resources:
limits:
cpu: 250m
memory: 512Mi
requests:
cpu: 100m
memory: 128Mi
securityContext:
privileged: true
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
dnsPolicy: ClusterFirst
restartPolicy: Always
schedulerName: default-scheduler
securityContext: {}
terminationGracePeriodSeconds: 30
hostNetwork: true
hostPID: true


---
apiVersion: apps/v1
kind: Deployment
metadata:
labels:
k8s-app: tcss-asset
name: tcss-asset
namespace: tcss
spec:
selector:
matchLabels:
k8s-app: tcss-asset
replicas: 1
template:
metadata:
labels:
k8s-app: tcss-asset
annotations:
eks.tke.cloud.tencent.com/ds-injection: "true"
spec:
serviceAccountName: tcss-agent
tolerations:
```

```
- operator: Exists
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
imagePullPolicy: Always
name: tcss-asset
command: ["/home/work/yunjing-agent"]
args: ["-asset"]
resources:
limits:
cpu: 100m
memory: 256Mi
requests:
cpu: 50m
memory: 64Mi
securityContext:
privileged: true
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
dnsPolicy: ClusterFirst
restartPolicy: Always
schedulerName: default-scheduler
securityContext: {}
terminationGracePeriodSeconds: 30
hostPID: true
```

5. 安装后，检查是否安装成功。集群接入后，将会在该集群创建“tcss 命名空间”，并创建如下工作负载资源，需确保以下3个工作负载正常运行：
   - tcss 命名空间下安装名称为“init-tcss-agent”的 Job 类型工作负载。
   - tcss 命名空间下安装名称为“tcss-asset”的 Deployment 类型工作负载。
   - kube-system 命名空间下安装名称为“yunjing-agent” 的 DaemonSet 类型工作负载。

5.1 检测 Job 工作负载是否部署成功。

查看 Job 是否创建成功，执行命令：`kubectl get jobs -n tcss`。

```
[root@VM-0-17-tencentos ~]# kubectl get jobs -n tcss
NAME              COMPLETIONS   DURATION   AGE
init-tcss-agent   1/1           8s         9m27s
[root@VM-0-17-tencentos ~]#
```

查看 Job 是否部署成功，执行命令：`kubectl get pods -n tcss | grep init-tcss-agent`。

```
[root@VM-0-17-tencentos ~]# kubectl get pods -n tcss | grep init-tcss-agent
init-tcss-agent-8jpkp         0/1     Completed   0          7m17s
[root@VM-0-17-tencentos ~]#
```

5.2 查看 DaemonSet 是否部署成功。

查看 DaemonSet 是否创建成功，执行命令：`kubectl get daemonset -A -l k8s-app=yunjing-agent`。

```
[root@VM-0-17-tencentos ~]# kubectl get daemonset -A -l k8s-app=yunjing-agent
NAMESPACE     NAME             DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
kube-system   yunjing-agent    1         1         1       1            1           <none>          30d
[root@VM-0-17-tencentos ~]#
```

查看 DaemonSet 是否部署成功，执行命令：`kubectl get pods -A -l k8s-app=yunjing-agent`。

```
[root@VM-0-17-tencentos ~]# kubectl get pods -A -l k8s-app=yunjing-agent
NAMESPACE     NAME                   READY   STATUS    RESTARTS   AGE
kube-system   yunjing-agent-bl4w7    1/1     Running   0          30d
[root@VM-0-17-tencentos ~]#
```

5.3 检测 Deployment 工作负载是否部署成功。

查看 Deployment 是否创建成功，执行命令：`kubectl get deployment -n tcss`。

```
[root@VM-0-17-tencentos ~]# kubectl get deployment -n tcss
NAME          READY   UP-TO-DATE   AVAILABLE   AGE
tcss-asset    1/1     1            1           15m
[root@VM-0-17-tencentos ~]#
```

查看 Deployment 是否部署成功，执行命令：`kubectl get pods -n tcss | grep tcss-asset`。

```
[root@VM-0-17-tencentos ~]# kubectl get pods -n tcss | grep tcss-asset
tcss-asset-79c5c77756-zc5x8   1/1     Running     0          16m
[root@VM-0-17-tencentos ~]#
```

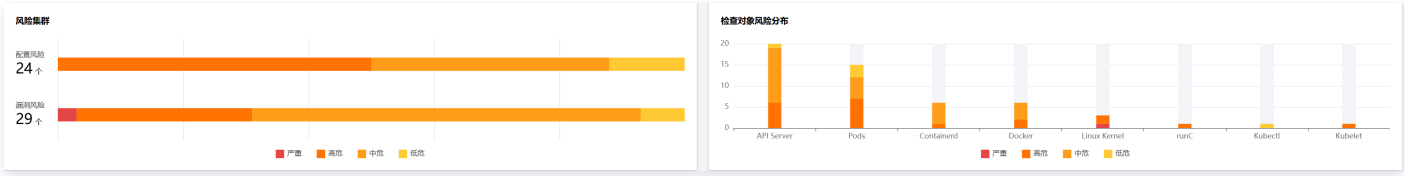
风险分析

最近更新时间：2025-05-13 18:11:12

风险分析功能展示所有已检查集群存在的风险统计，包括风险节点趋势以及风险项信息。

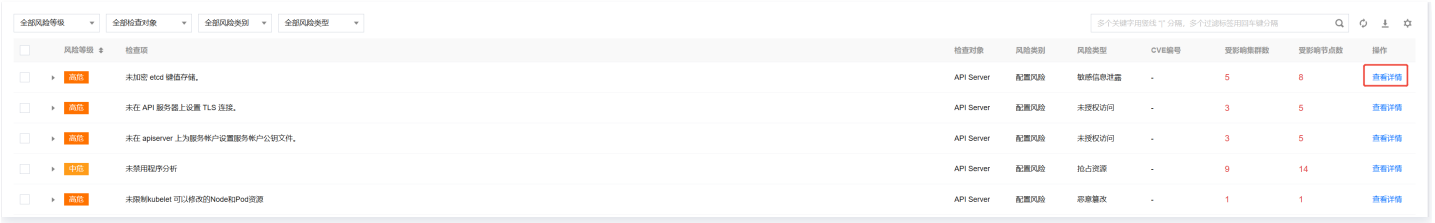
查看风险节点统计

1. 登录 容器安全服务控制台，在左侧导航单击**集群安全管理 > 风险分析**。
2. 在风险分析页面，展示风险集群的配置风险和漏洞风险数据，鼠标悬停可查看每一类风险的严重、高危、中危和低危数据；展示检查对象风险分布，检查对象包括 API Server、Pods、Containerd、Docker、Kubelet、Linux Kernel、runC、Kubectl，鼠标悬停可查看每一类风险的严重、高危、中危和低危数据。



查看风险项信息

在 风险分析页面 的风险项列表，展示了当前集群检查发现的所有风险项，风险项信息包括风险等级、检查项信息、检查对象、风险类别、风险类型、受影响集群数、受影响节点数、CVE 编号、操作。单击风险项的**查看详情**，进入风险项详情弹窗，可查看当前风险项的风险详情、风险描述、解决方案以及风险的所有影响范围。



基线管理

概述

最近更新时间：2025-05-13 18:11:12

安全基线支持 CIS Benchmark 标准并结合腾讯云鼎实验室基线配置实践，可对容器、镜像、主机、Kubernetes 资产环境配置进行安全标准检查，多维度展现容器资产的基线合规情况并帮助建立容器运行环境下的基线配置，减少攻击面。

容器

最近更新时间：2025-05-13 18:11:12

容器页面展示容器资产的基线合规情况，包括基线概览、检测信息、容器检测项结果列表。包括 Docker 容器和 Containerd 容器，以下操作指南以 Docker 容器为例。

查看容器概览

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理 > 容器**。
2. 在容器页面，基线概览窗口展示合规容器占比百分比和严重、高危、中危、提示四个威胁等级的未通过检测项数量。

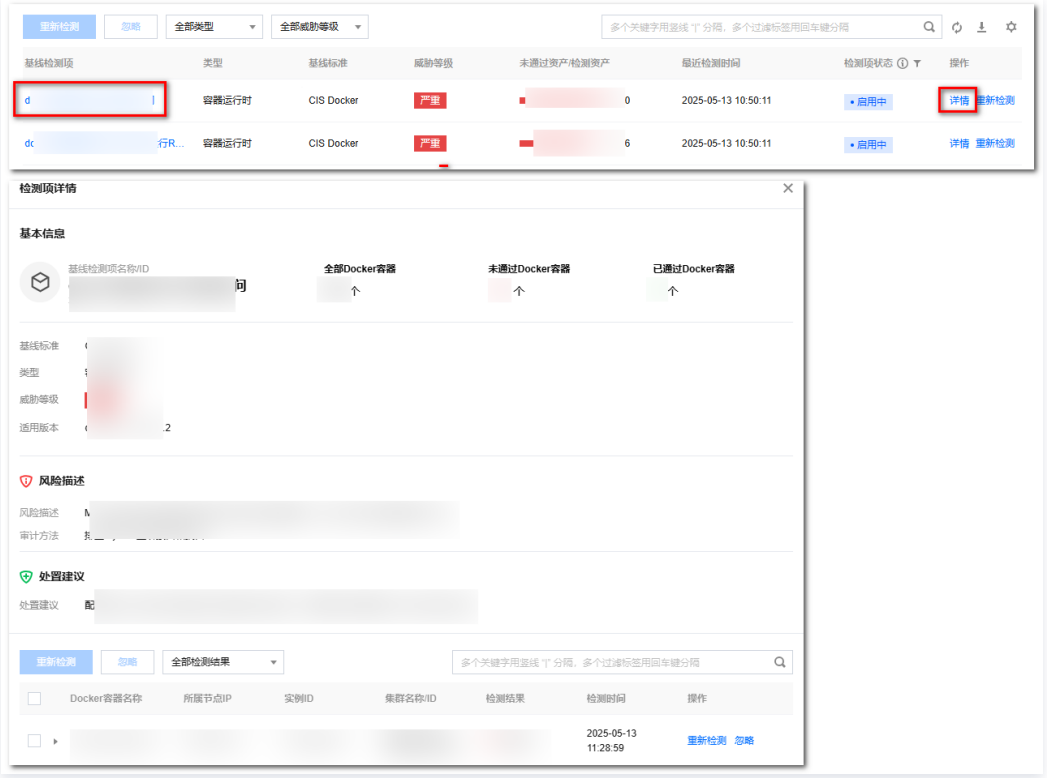
> **说明：**
> 合规容器占比百分比计算逻辑为：合规容器资产数量/容器总数（含检查失败数量）。

3. 在容器页面，单击百分比中的**详情**，可在弹出的容器抽屉中查看容器资产的检测结果列表。

4. 在容器抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对容器资产的检测结果进行查询。

5. 在容器抽屉中，单击 图标勾选所需的容器基线检测项后，单击**重新检查 > 确定**，对选中的容器基线检测项进行重新检测。

6. 在容器抽屉中，单击**基线检测项或详情**，可查看指定容器的基线检测情况。



查看检测信息

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理 > 容器**。
2. 在容器页面，检测信息窗口展示容器资产最近一次的基线检测时间、启用的检测项、检测主机节点和周期检测配置信息。

3. 在容器页面，单击**编辑策略**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

4. 在容器页面，单击**一键检测**，可针对已启用检测项和生效主机下发基线检测。

设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击 图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击**编辑**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。
3. 在检测周期设置弹窗，单击**详情**，可查看周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

基线忽略列表

基线忽略列表展示已忽略的容器基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过“基线检测项”关键词对容器基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的容器基线检测项后，单击**取消忽略**，将会对选中的容器基线检测项取消忽略。

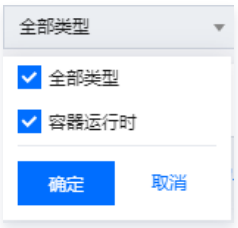
> **说明：**
> 检测项取消忽略后，检测内容将恢复正常检测。

查看检测结果列表

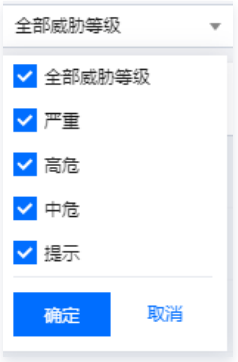
筛选刷新基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **容器**。
2. 在容器页面，单击搜索框，可通过“ID 和基线检测项”关键词对容器基线检测项进行查询。

3. 在容器页面，单击左上角的类型下拉框，按类型对容器基线检测项进行筛选。



4. 在容器页面，单击左上角的威胁等级下拉框，按威胁等级对容器基线检测项进行筛选。



3.在容器页面，单击操作栏右侧 图标，即可刷新容器基线检测项。

重新检测基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理 > 容器**。

2. 在容器页面，单击 图标勾选所需容器基线检测项后，单击**重新检测 > 确认**，可对容器基线检测项进行重新检测。

> **说明：**
> 选定多个容器基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理 > 容器**。

2. 在容器页面，单击 图标勾选所需基线检测项后，单击**忽略 > 确定**，可对基线检测项进行忽略。

> **说明：**
> 选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理 > 容器**。

2. 在容器页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确认**，即可完成设置自定义列表管理。

列表重点字段说明

1. 基线检测项：单击“基线检测项”，可查看检测项详情。
2. 未通过检测项：未通过的检测项数量。
3. 检测结果：存在未通过的检测项检测结果为未通过，所有检测项通过则检测结果为已通过。
4. 最近检测时间：最近一次的检测时间。
5. 检测项状态：即策略中检测项开启/未开启状态，状态为“未启用”的检测项将不会进行检测（包含一键、周期检测），过往检测的记录将保留。如您需要编辑检测项状态，单击**编辑策略**即可。

镜像

最近更新时间：2025-05-13 18:11:12

镜像页面展示镜像资产的基线合规情况，包括基线概览、检测信息、镜像检测项结果列表。

查看镜像概览

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，基线概览窗口展示合规镜像占比百分比，严重、高危、中危、提示四个威胁等级的未通过检测项数量。

> **说明：**
> 合规镜像占比百分比计算逻辑为：合规镜像资产数量/镜像总数（含检查失败数量）。

3. 在镜像页面，单击百分比中的**详情**，可在弹出的镜像抽屉中查看镜像资产的检测结果列表。

4. 在镜像抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对镜像资产的检测结果进行查询。

5. 在镜像抽屉中，单击 图标勾选所需的镜像基线检测项后，单击**重新检测** > **确定**，将会对选中的资产基线检测项进行重新检测。

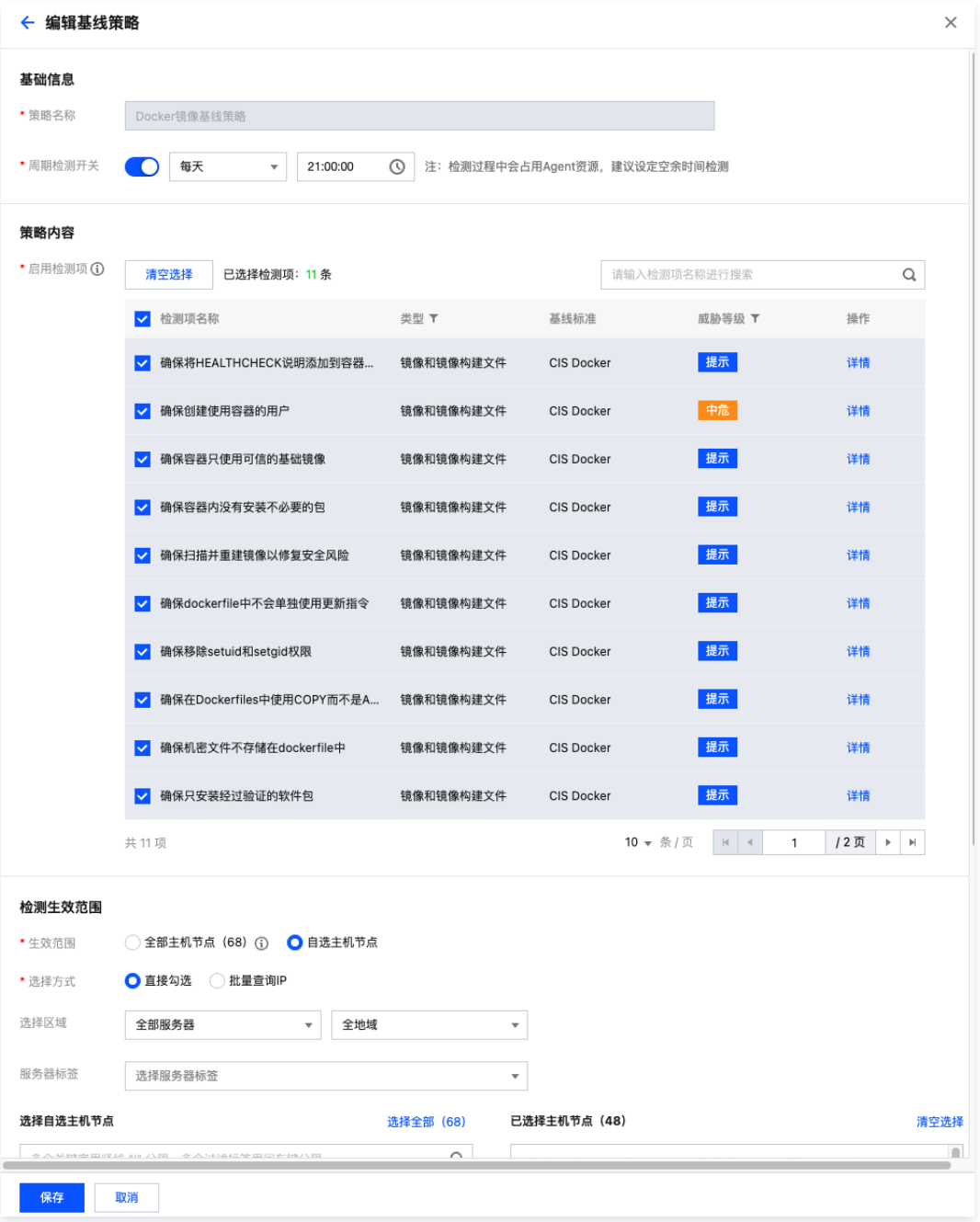
> **说明：**
> 选定多个镜像基线检测项，单击②处的**重新检测**，可进行批量重新检测。

6. 在镜像抽屉中，单击**基线检测项**，可查看指定镜像的基线检测情况。

查看检测信息

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，检测信息窗口展示镜像资产最近一次的基线检测时间、启用的检测项、检测主机节点和周期检测配置信息。

3. 在镜像页面，单击**编辑策略**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。



4. 在镜像页面，单击**一键检测**，可针对已启用检测项和生效主机下发基线检测。

设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击 图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击**编辑**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。
3. 在检测周期设置弹窗，单击**详情**，可查看周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

基线忽略列表

基线忽略列表展示了忽略的镜像基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过“基线检测项”关键词对镜像基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的镜像基线检测项后，单击**取消忽略**，将会对选中的镜像基线检测项取消忽略。

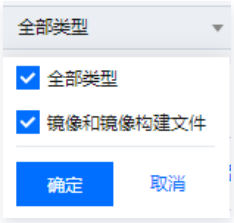
> **说明：**
> 检测项取消忽略后，检测内容将恢复正常检测。

查看检测结果列表

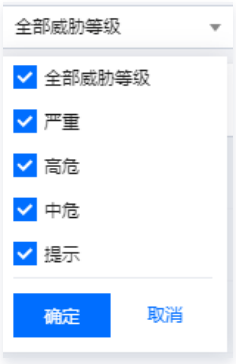
筛选刷新基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，单击搜索框，可通过“ID 和基线检测项”关键词对镜像基线检测项进行查询。

3. 在镜像页面，单击左上角的类型下拉框，按类型对镜像基线检测项进行筛选。



4. 在镜像页面，单击左上角的威胁等级下拉框，按威胁等级对镜像基线检测项进行筛选。



5. 在镜像页面，单击操作栏右侧 图标，即可刷新事件列表。

重新检测基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，单击 图标勾选所需镜像基线检测项后，单击**重新检测** > **确认**，可对镜像基线检测项进行重新检测。

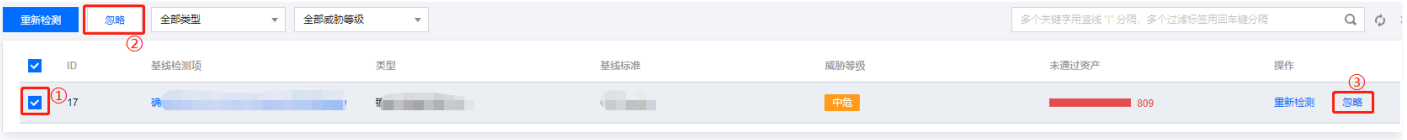
> **说明：**
> 选定多个镜像基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，单击 图标勾选所需基线检测项后，单击**忽略** > **确定**，可对基线检测项进行忽略。

> **说明：**

选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。



自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **镜像**。
2. 在镜像页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项ID，该ID全局唯一。
2. 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
3. 类型：检测项的类型。
4. 基线标准：检测项所属基线标准。
5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、提示。
6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。
7. 最近检测时间：该基线最近下发扫描的时间。
8. 检测项状态：即策略中检测项开启/未开启状态，状态为“未启用”的检测项将不会进行检测（包含一键、周期检测），过往检测的记录将保留。如您需要编辑检测项状态，单击**编辑策略**即可。
9. 操作：详情、重新检测和忽略。

主机

最近更新时间：2025-05-13 18:11:12

主机页面展示主机资产的基线合规情况，包括基线概览、检测信息、主机检测项结果列表。包括 Docker 主机和 Containerd 主机，以下操作指南以 Docker 主机为例。

查看 Docker 主机概览

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Docker 主机**。
2. 在 Docker 主机页面，基线概览窗口展示合规主机占比百分比和严重、高危、中危、提示四个威胁等级的未通过检测项数量。

> **说明：**
> 合规 Docker 主机占比百分比计算逻辑为：合规 Docker 主机资产数量/Docker 主机总数（含检查失败数量）。

3. 在 Docker 主机页面，单击百分比中的**详情**，可在弹出的主机抽屉中查看主机资产的检测结果列表。
4. 在 Docker 主机抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对主机资产的检测结果进行查询。

5. 在 Docker 主机抽屉中，单击 图标勾选所需的 Docker 主机基线检测项后，单击**重新检测** > **确定**，将会对选中的基线检测项进行重新检测。

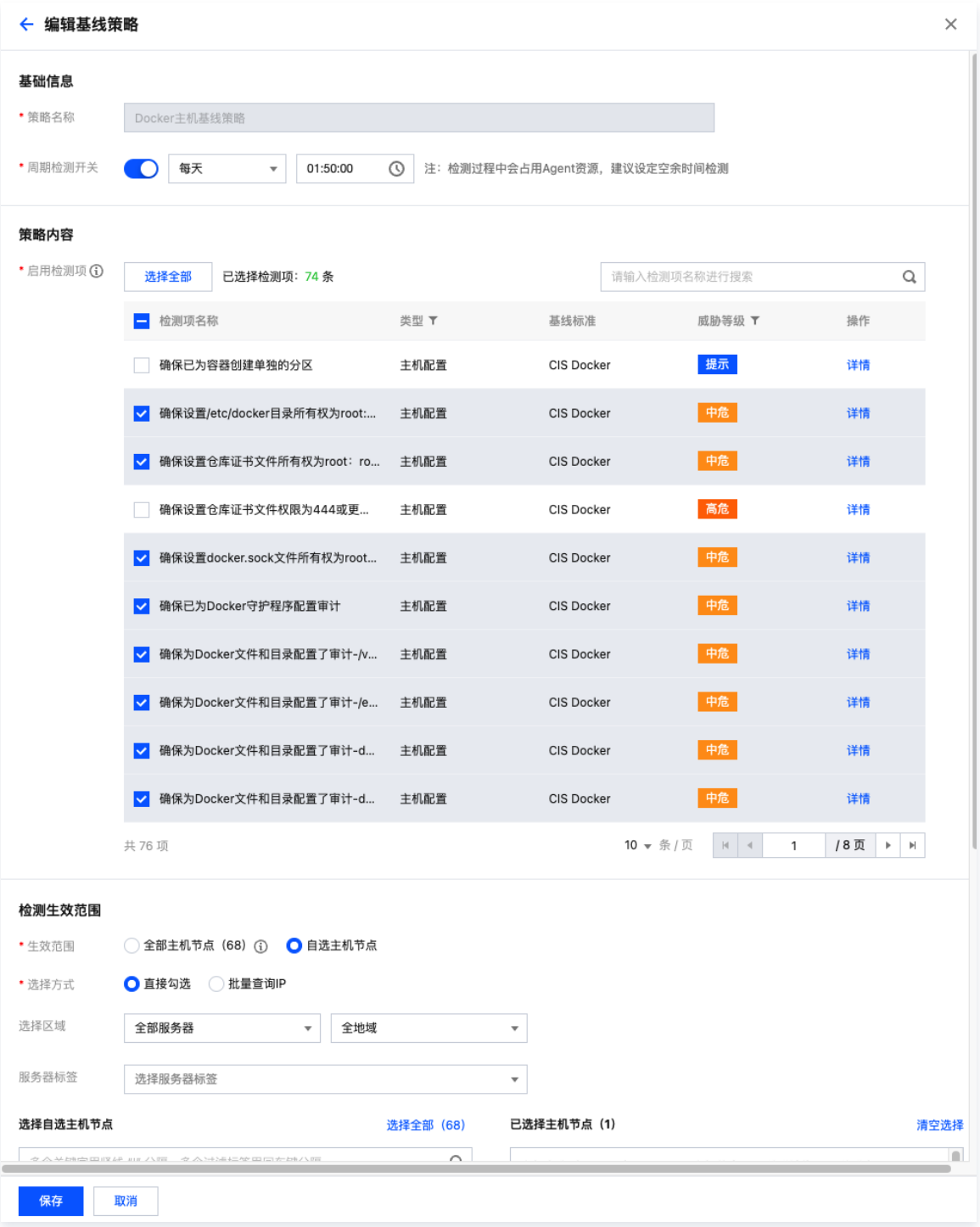
> **说明：**
> 选定多个主机基线检测项，单击②处的**重新检测**，可进行批量重新检测。

6. 在 Docker 主机抽屉中，单击**基线检测项**，可查看指定 Docker 主机的基线检测情况。

查看检测信息

1. 在 Docker 主机页面，检测信息窗口展示主机资产最近一次的基线检测时间、启用的检测项、检测主机节点和周期检测配置信息。

2. 在 Docker 主机页面，单击**编辑策略**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。



3. 在 Docker 主机页面，单击**一键检测**，可针对已启用检测项和生效主机下发基线检测。

设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

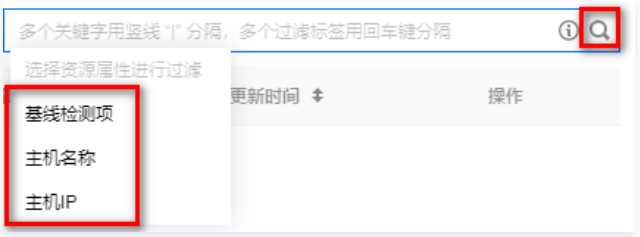
1. 在基线策略设置页面，可通过单击图标开关开启或关闭当前基线标准的周期性检测。
2. 在基线策略设置页面，单击**编辑**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

3. 在基线策略设置页面，单击**详情**，可查看周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

基线忽略列表

基线忽略列表展示了忽略的主机基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过“基线检测项、主机名称、主机 IP”关键词对主机基线检测项进行查询。



2. 在基线忽略列表页面，单击图标勾选所需的主机基线检测项后，单击**取消忽略**，将会对选中的主机基线检测项取消忽略。

> **说明：**
> 检测项取消忽略后，检测内容将恢复正常检测。

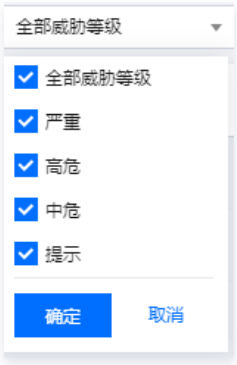
查看检测结果列表

筛选刷新基线检测项

1. 在 Docker 主机页面，单击搜索框，可通过“ID 和基线检测项”关键词对 Docker 主机基线检测项进行查询。

2. 在 Docker 主机页面，单击左上角的类型下拉框，按类型对 Docker 主机基线检测项进行筛选。

3. 在 Docker 主机页面，单击左上角的威胁等级下拉框，按威胁等级对 Docker 主机基线检测项进行筛选。



4. 在 Docker 主机页面，单击操作栏右侧 图标，即可刷新事件列表。

重新检测基线检测项

在 Docker 主机页面，单击 图标勾选所需 Docker 主机基线检测项后，单击**重新检测** > **确认**，可对主机基线检测项进行重新检测。

> **说明：**
> 选定多个主机基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

在 Docker 主机页面，单击 图标勾选所需基线检测项后，单击**忽略** > **确定**，可对基线检测项进行忽略。

> **说明：**
> 选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 在 Docker 主机页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项 ID，该 ID 全局唯一。
2. 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
3. 类型：检测项的类型。
4. 基线标准：检测项所属基线标准。
5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、提示。
6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。
7. 最近检测时间：最近一次的检测时间。
8. 检测项状态：即策略中检测项开启/未开启状态，状态为“未启用”的检测项将不会进行检测（包含一键、周期检测），过往检测的记录将保留。如您需要编辑检测项状态，单击**编辑策略**即可。
9. 操作：重新检测和忽略。

Kubernetes

最近更新时间：2025-05-13 18:11:12

Kubernetes 页面基于 CIS Kubernetes Benchmark 标准展示 K8s 资产的基线合规情况，包括基线概览、检测信息、Kubernetes 检测项结果列表。

查看 Kubernetes 概览

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，基线概览窗口展示合规 K8s 检测项通过率占比以及严重、高危、中危、提示四个威胁等级的未通过检测项数量。

> **说明：**
> 检测项通过率计算逻辑为：通过的检测项数量/检测项总数。

3. 在 Kubernetes 页面，单击百分比中的**详情**，可在弹出的抽屉中查看 Kubernetes 资产的检测结果列表。

4. 在 Kubernetes 页面，单击搜索框，可通过“ID 和基线检查项”关键词对 Kubernetes 基线检测项的检测结果进行查询。

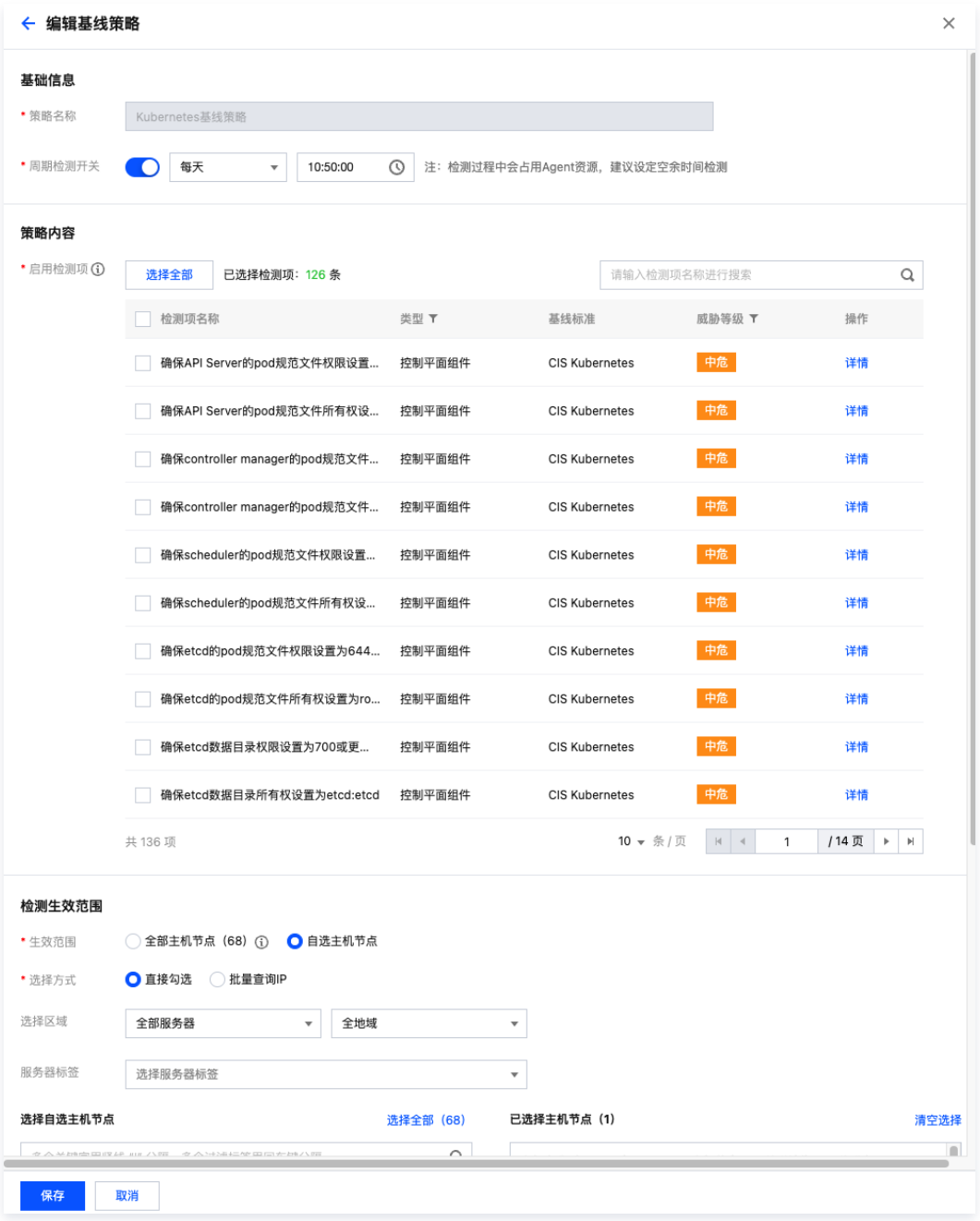
5. 在 Kubernetes 页面，单击 图标勾选所需的 Kubernetes 基线检测项后，单击**重新检测** > **确定**，将会对选中的 Kubernetes 基线检测项进行重新检测。

> **说明：**
> 选定多个 Kubernetes 基线检测项，单击②处的**重新检测**，可进行批量重新检测。

查看检测信息

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，检测信息窗口展示 Kubernetes 基线检测项最近一次的基线检测时间、启用的检测项、检测主机节点和周期检测配置信息。

3. 在 Kubernetes 页面，单击**编辑策略**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。



4. 在 Kubernetes 页面，单击**一键检测**，可针对已启用检测项和生效主机下发基线检测。

设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

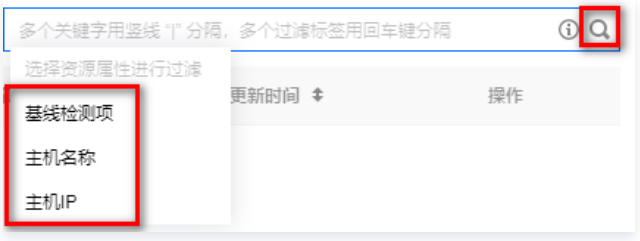
1. 在基线策略设置页面，可通过单击图标开关开启或关闭当前基线标准的周期性检测。
2. 在基线策略设置页面，单击**编辑**，可配置周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

3. 在基线策略设置页面，单击**详情**，可查看周期检测开关是否开启、周期检测时间、自定义选择启用的检测项、自定义检测生效范围。

基线忽略列表

基线忽略列表展示了忽略的容器基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过“基线检测项、主机名称、主机 IP”关键词对 Kubernetes 基线检测项进行查询。



2. 在基线忽略列表页面，单击图标勾选所需的 Kubernetes 资产后，单击**取消忽略**，将会对选中的 Kubernetes 基线检测项取消忽略。

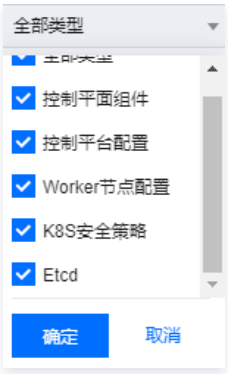
> **说明：**
> 检测项取消忽略后，检测内容将恢复正常检测。

查看检测结果列表

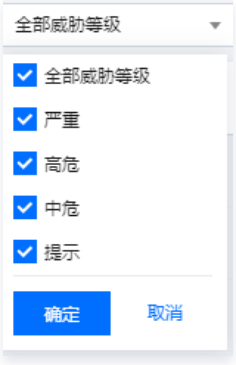
筛选刷新基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，单击搜索框，可通过“基线检测项”关键词对 Kubernetes 基线检测项进行查询。

3. 在 Kubernetes 页面，单击左上角的类型下拉框，按类型对 Kubernetes 基线检测项进行筛选。



4. 在 Kubernetes 页面，单击左上角的威胁等级下拉框，按威胁等级对 Kubernetes 基线检测项进行筛选。



5. 在 Kubernetes 页面，单击操作栏右侧 图标，即可刷新Kubernetes 基线检测项。

重新检测基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，单击 图标勾选所需 Kubernetes 基线检测项后，单击**重新检测** > **确认**，可对 Kubernetes 基线检测项进行重新检测。

> **说明：**
> 选定多个 Kubernetes 基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，单击 图标勾选所需 Kubernetes 基线检测项后，单击**忽略** > **确定**，可对 Kubernetes 基线检测项进行忽略。

> **说明：**
> 选定多个 Kubernetes 基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**基线管理** > **Kubernetes**。
2. 在 Kubernetes 页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项ID，该ID全局唯一。
2. 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
3. 类型：检测项的类型。
4. 基线标准：检测项所属基线标准。
5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、提示。
6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。
7. 最近检测时间：最近一次的检测时间。
8. 检测项状态：即策略中检测项开启/未开启状态，状态为“未启用”的检测项将不会进行检测（包含一键、周期检测），过往检测的记录将保留。如您需要编辑检测项状态，单击**编辑策略**即可。
9. 操作：重新检测和忽略。

运行时安全
概述

最近更新时间：2025-04-29 16:22:55

运行时安全支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供容器逃逸、反弹 Shell 和文件查杀安全功能。

- 容器逃逸：指的是容器利用系统漏洞，“逃逸”出了其自身所拥有的权限，实现了对宿主机和宿主机上其他容器的访问。由于容器与宿主机共享操作系统内核，为了避免容器获取宿主机的 root 权限，通常不允许采用特权模式运行容器。按照入侵者执行容器逃逸的顺序，容器安全服务将风险事件类型划分为三类，分别是：风险容器、程序提权、容器逃逸。
  - 风险容器：指当前容器存在部分潜在风险行为，可能会存在被提权或被逃逸的风险，包含敏感路径挂载、特权容器。
  - 程序提权：指当前容器出现了提权的风险行为，可能会进一步导致其逃逸，需要您进行关注。
  - 容器逃逸：指当前容器已经出现了逃逸行为，此时您应该立即对出现的风险事件进行关注，并立即通过推荐解决方案进行对应的处置响应。
- 反弹 Shell：基于腾讯云安全技术及多维度多手段，对 Shell 反向连接行为进行识别记录，为您运行时容器提供反弹 Shell 行为的实时监控能力。
- 文件查杀：通过实时监测运行容器调用的文件是否存在风险；或手动触发一键扫描，检查容器内是否存在恶意的木马病毒、WebShell 等。
- 恶意外连：实时检测容器外连恶意域名/IP 的行为。当发现容器存在访问恶意域名/IP 的行为时，您的容器可能已经失陷，因为恶意域名/IP 可能是黑客的远控服务器、恶意软件下载源、矿池地址等，建议及时进行排查。

> **说明：**
> 容器告警事件仅保留半年以内的数据，每天定时检测并自动清理超过180天的告警事件，超出时间范围将无法显示和查询。如有需要，建议使用 日志投递 留存。

容器逃逸

最近更新时间：2025-05-13 18:11:12

事件列表

查看设置状态

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **容器逃逸**，进入容器逃逸页面。
2. 在容器逃逸页面，安全状态模块展示是否存在容器逃逸事件。如检测发现容器逃逸事件，建议立即处理。

3. 在容器逃逸页面，监控状态模块展示系统支持检测的容器逃逸事件类型，单击可开启图标，可自定义设置监控状态。

查看容器逃逸列表

登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **容器逃逸**，进入容器逃逸页面。

筛选刷新容器逃逸

1. 在容器逃逸页面，单击搜索框，可通过“容器名称、镜像名称和节点名称”等关键词对容器逃逸事件进行查询。

2. 在容器逃逸页面，单击操作栏右侧 图标，即可刷新容器逃逸事件。

导出容器逃逸

在容器逃逸页面，单击 图标勾选所需的容器逃逸事件后，单击 图标即可导出容器逃逸事件。

> **说明：**
>
> 可单击 图标勾选多个逃逸事件后，单击 图标可进行批量导出。

事件状态处理

在容器逃逸页面，可对容器逃逸事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击 图标勾选所需的容器逃逸事件后，单击**标记已处理 > 确定**，即可将选中事件标记已处理。

  > **说明：**
  > 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击 图标勾选所需的容器逃逸事件后，单击**忽略 > 确定**，即可将选中事件忽略。

  > **说明：**
  > 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击 图标勾选所需的容器逃逸事件后，单击**删除 > 确定**，即可将选中事件删除。

  > **注意：**
  > 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看列表详情

1. 在容器逃逸页面，单击事件类型左侧 ▸ 图标，可查看事件描述。

2. 在容器逃逸页面， 单击“容器名称/ID ”或“镜像名称/ID”，可跳转至对应的资产管理列表。

3. 在容器逃逸页面，单击**查看详情**，右侧抽屉展示事件详情信息，包括告警事件详情、进程信息和事件描述。

4. 在容器逃逸页面，事件状态包含已处理、已忽略和待处理。可对不同状态的事件进行以下操作：
   - 已处理：单击**删除**，并在弹窗中进行二次确认删除，可将事件删除。

     说明：
     删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

   - 待处理：单击**立即处理**，可将事件标记为已处理、忽略或删除该事件，详情请参见 事件状态处理 。

   - 已忽略：单击**取消忽略**或**删除**，可将事件变为待处理或删除。

自定义列表管理

1. 在容器逃逸页面，单击 ⚙ 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表字段说明

1. 事件类型：容器逃逸告警事件类型，包括敏感路径挂载、提权事件、逃逸漏洞利用、访问 Docker API 接口逃逸、篡改敏感文件逃逸和利用 cgroup 机制逃逸。
2. 首次生成时间：该逃逸事件首次触发告警的时间。

> **说明：**
> 系统默认对未处理的相同逃逸事件进行告警聚合。

3. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧“排序”按钮对列表事件按时间正序和时间反序进行排列。
4. 事件数量：聚合时间范围内该逃逸事件触发告警的总数量。
5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

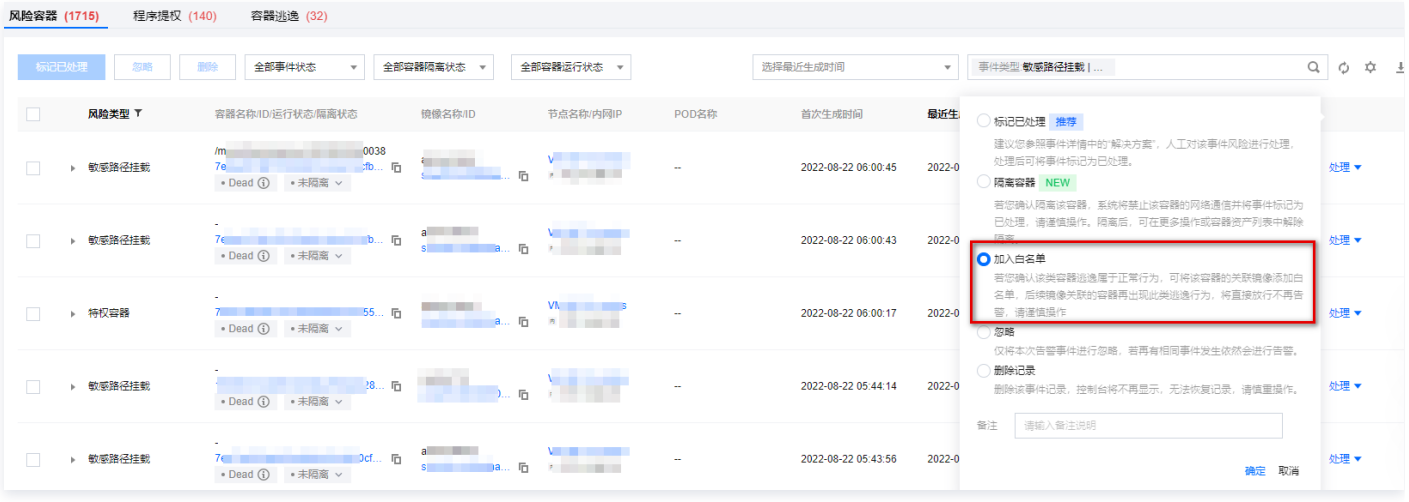
逃逸白名单

排查容器逃逸告警时，如部分业务容器需以特权模式启动、需挂载敏感路径或其他会导致逃逸告警的配置，可进行加白处理。加白操作分类为两类：根据告警事件加白和在白名单管理页面新建白名单。

加白告警事件

1. 在 容器逃逸页面，如需对告警事件进行加白，单击**处理**，选择加入白名单，单击**确定**。

> **注意：**
> 若您确认该类容器逃逸属于正常行为，可将该容器的关联镜像添加白名单，**后续镜像关联的容器再出现此类逃逸行为，将直接放行不再告警，请谨慎操作**。



2. 在添加白名单镜像页面，默认勾选告警事件中关联的逃逸告警类型和来源镜像，您也可以在此基础上增加勾选加白事件类型和需要加白的镜像，单击**确定**即可完成白名单配置。

3. 如需对某种事件类型进行全部镜像加白，您可以单击监控状态右侧的**监控设置**，对开启监控的风险类型进行调整。

白名单管理

用户也可在白名单管理页面，批量新增白名单，避免后续产生告警。

添加白名单

1. 在 容器逃逸 > **白名单管理**页面，单击**添加白名单策略**。

2. 在添加白名单镜像页面，选择添加方式、加白事件类型和生效的镜像，也可批量选择需加白的事件类型和生效的镜像，单击**确定**。

3. 添加白名单完毕后，白名单管理列表以镜像 ID 对白名单进行统一管理，展示每一个镜像已加白的事件类型。例如添加白名单时勾选了3个镜像，那么列表中将更新3条白名单镜像记录。

编辑白名单

- 编辑单个白名单

  a. 在 容器逃逸 > **白名单管理**页面，单击目标镜像操作列的**编辑加白类型**。

  b. 在编辑加白事件类型对话框中，修改加白事件类型，单击**保存**。

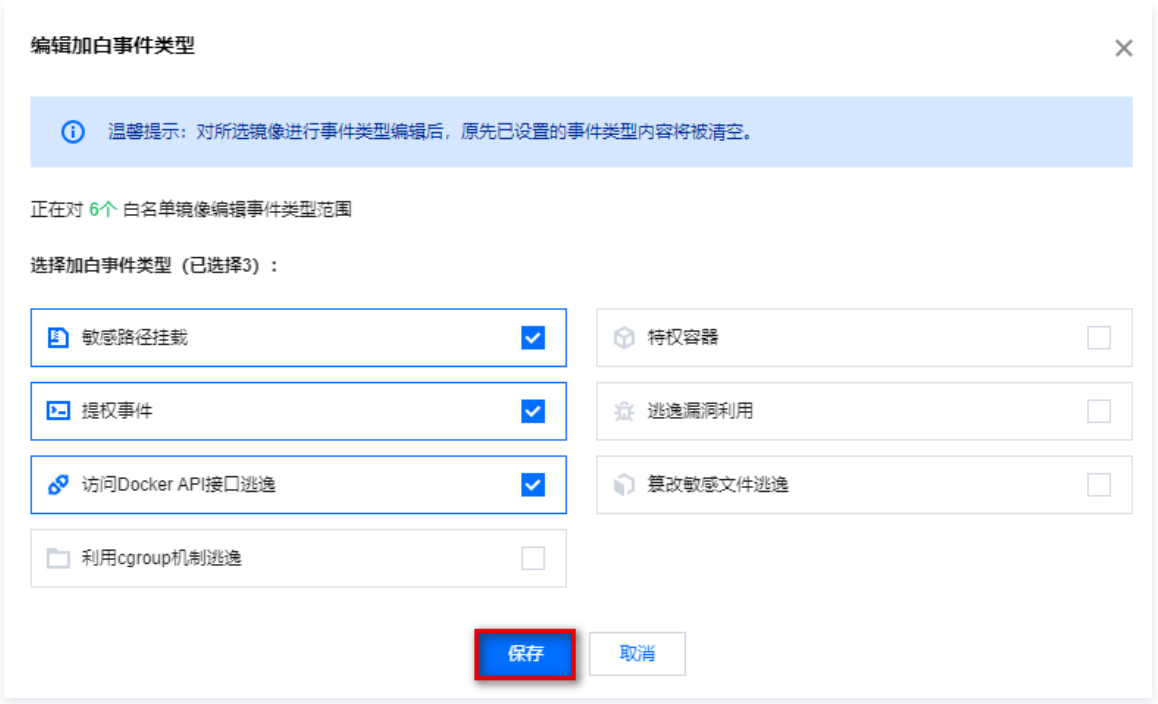
- **批量编辑白名单**

  如需批量对多个镜像进行加白事件类型变更、且这些镜像需加白的类型一致，按照如下操作修改：

  a. 在 容器逃逸 > **白名单管理**页面，选择一个或多个镜像，单击左上角的**编辑加白类型**。

  b. 在编辑加白事件类型对话框中，修改加白事件类型，单击**保存**。

> **注意：**
> 对所镜像进行事件类型编辑后，原先已设置的事件类型内容将被清空。



删除白名单

1. 在 容器逃逸 > **白名单管理**页面，可删除单个白名单或批量删除白名单。
   - 删除单个白名单： 选择所需镜像，单击操作列的**删除**。

   - 批量删除白名单：选择一个或多个镜像，单击左上角的**删除**。

2. 在确认删除对话框中，单击**确认**，即可删除目标白名单。

> **注意：**
> 确认删除后将无法恢复，该白名单镜像在触发此类逃逸时将再次产生告警。

反弹 Shell 事件列表

最近更新时间：2025-05-13 09:54:52

本文档介绍反弹 Shell 功能的事件列表。

筛选刷新事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **事件列表**，进入事件列表页面。
2. 在事件列表页面，单击搜索框，可通过“进程名称、父进程名称”等关键词对反弹 Shell 事件进行查询。

3. 在事件列表页面，单击操作栏右侧 图标，即可刷新反弹 Shell 事件列表。

导出事件列表

在事件列表页面，单击 图标勾选所需的反弹 Shell 事件后，单击 图标即可导出反弹 Shell 事件。

> **说明：**
>
> 可单击 图标勾选多个反弹 Shell 事件后，单击 图标可进行批量导出。

事件状态处理

在事件列表页面，可对反弹 Shell 事件列表进行标记已处理、忽略和删除处理。

- 标记已处理：单击 图标勾选反弹 Shell 事件后，单击**标记已处理** > **确定**，即可将选中事件标记已处理。

  > **说明：**
  > 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击 图标勾选所需的反弹 Shell 事件后，单击**忽略** > **确定**，即可将选中事件忽略。

> **说明：**
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

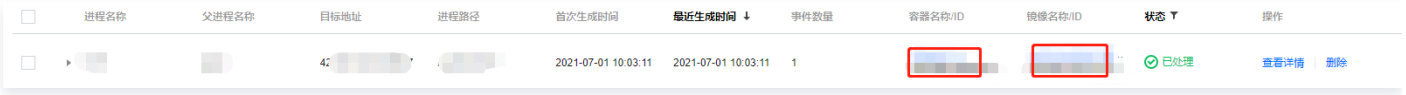
- 删除：单击 图标勾选所需的反弹 Shell 事件后，单击**删除** > **确定**，即可将选中事件删除。

> **注意：**
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看列表详情

1. 在事件列表页面，单击事件类型左侧 图标，可查看事件描述。

2. 在事件列表页面，单击“容器名称/ID ”或“镜像名称/ID”，可跳转至对应的资产管理列表。



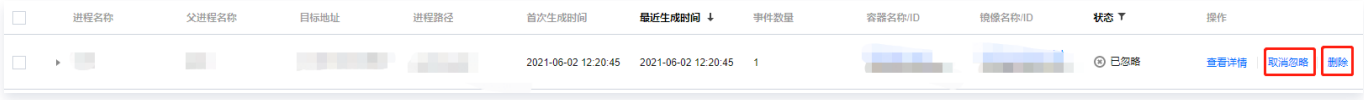
3. 在事件列表页面，单击**查看详情**，右侧抽屉展示事件详细信息，包括告警事件详情、进程信息、父进程信息和事件描述。

4. 在事件列表页面，事件状态包含已处理、已忽略、待处理。可对不同状态的事件进行以下操作：
   - 已处理/已加白：单击**删除**，并在弹窗中进行二次确认删除，可将事件删除。

     > **说明：**
     > 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

   - 待处理：单击**立即处理**，可将事件标记为已处理、忽略、删除和添加白名单，详情请参见 事件状态处理 。
   - 隔离容器：单击**隔离容器**，可将事件标记为已隔离。若您确认隔离该容器，系统将禁止该容器的网络通信并将事件标记为已处理，请谨慎操作。隔离后，可在更多操作或容器资产列表中解除隔离。

- **已忽略：单击取消忽略或删除，可将事件变为待处理或删除。**



自定义列表管理

1. 在事件列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该 Shell 反向连接事件首次触发告警的时间。

> **说明：**

> 系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。
3. 事件数量：聚合时间范围内该 Shell 反向连接事件触发告警的总数量。
4. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

配置白名单

最近更新时间：2025-05-13 09:54:52

本文档为您介绍如何配置白名单管理。

筛选刷新白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全 > 反弹 Shell > 白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击搜索框，可通过“连接进程”关键词对白名单事件进行查询。

3. 在白名单管理页面，单击操作栏右侧 图标，即可刷新白名单管理列表。

新增白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全 > 反弹 Shell > 白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，选择常规加白或正则加白，单击**新增白名单**，右侧弹出新增白名单设置页面。

- 常规加白：在新增白名单设置页面，需配置白名单生效的目标地址、连接进程和选择白名单生效范围。
  - 单击目标地址左侧 图标，输入目标地址的 IP 和端口。

    说明：
    - IP 不能为空。
    - IP 地址格式：单个 IP（127.0.0.1）； IP 范围（127.0.0.1-127.0.0.254）；IP网段（127.0.0.1/24）。
    - 端口格式：80,8080（支持多个，用英文逗号分隔。不限端口请留空）。
  - 单击连接进程左侧 图标，输入支持命令行通配符。
  - 白名单生效范围为全部镜像或自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

    说明：
    支持按住 Shift 键进行多选。

- 正则加白：在新增白名单设置页面，需配置白名单的规则名称和正则表达式。支持添加多个正则表达式，配置正则表达式时，逻辑符合包括 AND、OR 和 NOT；匹配字段包括容器名称、镜像 ID、镜像名称、节点名称、节点 IP、进程路径、进程参数、进程链、父进程路径、父进程参数、祖先进程路径、祖先进程参数、目标 IP、目标端口。

3. 选择所需内容后，单击**确定**或**取消**，即可完成或取消新增白名单。
4. 配置完成后，满足条件的反弹shell将直接放行不再告警。

编辑白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击右侧**编辑**，右侧弹出编辑白名单设置页面。

3. 在编辑白名单设置页面，支持修改如下内容：
   - 常规加白的白名单可修改白名单生效的目标地址、连接进程和白名单生效范围。

- 正则加白的白名单可修改规则名称和正则表达式内容。

4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改白名单。

删除白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击右侧**删除**，弹出“确认删除”弹窗。

3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除白名单。

> **说明：**
> 删除后，白名单将无法恢复，该白名单的关联镜像触发系统策略时将再次产生告警。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

- 常规加白
  - 镜像数：白名单生效的镜像。
  - 连接进程：白名单生效的连接进程。
  - 目标主机：白名单生效的主机 IP 及端口。
- 正则加白
  - 规则名称：用户自定义的白名单名称。
  - 生效表达式：白名单中配置的正则表达式数量。

文件查杀

最近更新时间：2025-05-13 18:11:12

文件查杀提供实时检测和定期扫描容器内木马病毒文件功能。

查看风险趋势

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **文件查杀**。
2. 在文件查杀页面，可以查看待处理风险、影响容器的数量和趋势。
   - 待处理风险：展示近7天待处理风险趋势图和较昨日新增风险数据。将鼠标悬停在趋势图上，展示某一天的待处理风险数据。
   - 影响容器：展示近7天影响容器趋势图和较昨天新增影响容器数据。将鼠标悬停在趋势图上，展示某一天的影响容器数据。
   - 已隔离：展示近7天已隔离容器趋势图和较昨天新增已隔离容器数据。将鼠标悬停在趋势图上，展示某一天的已隔离容器数据。

设置风险检测

在 文件查杀页面 的风险检测模块，支持对定时检测和实时监控功能进行设置。

> **说明：**
> - 实时监控是客户配置的路径的增量文件实时检测。
> - 定时检测是客户配置的路径全部文件检测。

设置定时检测

1. 在风险检测模块，单击定时检测右侧的**设置**，进入定时检测设置页面。
2. 在定时检测设置页面，单击  ，开启定时检测，并依次设置检测时间、检测路径、检测范围。

参数说明：

- 实时检测开关：支持通过单击“开关”，可开启或关闭实时检测功能。
- 检测时间
  - 检测周期：包括每天、每隔三天、每隔七天。
  - 开始检测时间：配置定时任务何时开始扫描。
  - 超时时长：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。
- 检测路径
  - 全部路径：检测容器内全部文件路径。
  - 默认路径：包括系统敏感路径、黑客通用的木马和病毒保存目录。

- 自选路径：按自选的配置路径检测容器内文件。
- 检测范围
  - 节点：选择主机节点/超级节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。
  - 容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器。

3. 单击**保存设置**，即可完成定时检测设置。

设置实时监控

1. 在风险检测模块，单击实时监控右侧的**设置**，进入实时监控设置页面。
2. 在实时监控设置页面，单击，开启实时监控，配置相关参数。

参数说明：

- 实时监控开关：支持通过单击或开启或关闭实时监控功能。
- 检测路径
  - 全部路径：检测容器内全部文件路径。
  - 默认路径：包括系统敏感路径、黑客通用的木马和病毒保存目录。
  - 自选路径：按自选的配置路径检测容器内文件。
- 选择路径：根据实际需求选择**检测以下文件路径**或**检测除以下文件路径外的其他路径**。单击可添加多个路径，最多为30个。

3. 单击**保存设置**，即可完成实时监控设置。

设置一键检测

1. 在风险检测模块，单击**一键检测**，进入一键检测页面。
2. 在一键检测页面，选择检测路径、检测范围，并设置超时时长。

参数说明：

- 检测路径：
  - 全部路径：检测容器内全部文件路径。
  - 默认路径：包括系统敏感路径、黑客通用的木马和病毒保存目录。
  - 自选路径：按自选的配置路径检测容器内文件。
- 检测范围：
  - 主机节点：选择主机节点/超级节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。
  - 容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器。
- 超时设置：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。

3. 单击**开始检测**，即按配置条件开始扫描容器内文件。

查看最近一次检测结果

在风险检测模块，单击**最近一次检测结果**，可查看近一次扫描任务详情。

检测详情展示内容：

- **检测详情概览**
- 近一次扫描任务是否发现风险文件，如有发现，将展示风险文件数量、风险容器数量和扫描容器数量。
- 近一次扫描任务开始检测和结束检测时间。
- **检测详情列表**：展示近一次扫描任务扫描出的风险文件概况，按容器资产进行聚合。
- 列表字段包括：容器名称/ID、镜像名称/ID、主机节点名称/IP、检测状态、检测用时、风险数和操作项。
- 支持对扫描任务进行重新检测，或停止正在检测中的任务。
- 支持按主机名称、主机 IP、容器名称、容器 ID、镜像名称、镜像 ID 进行检索。
- 单击 ▸ 可查看风险文件的文件名称、文件路径、病毒名称和查看详情按钮；单击**查看详情**，可查看恶意文件详情。

查看事件列表

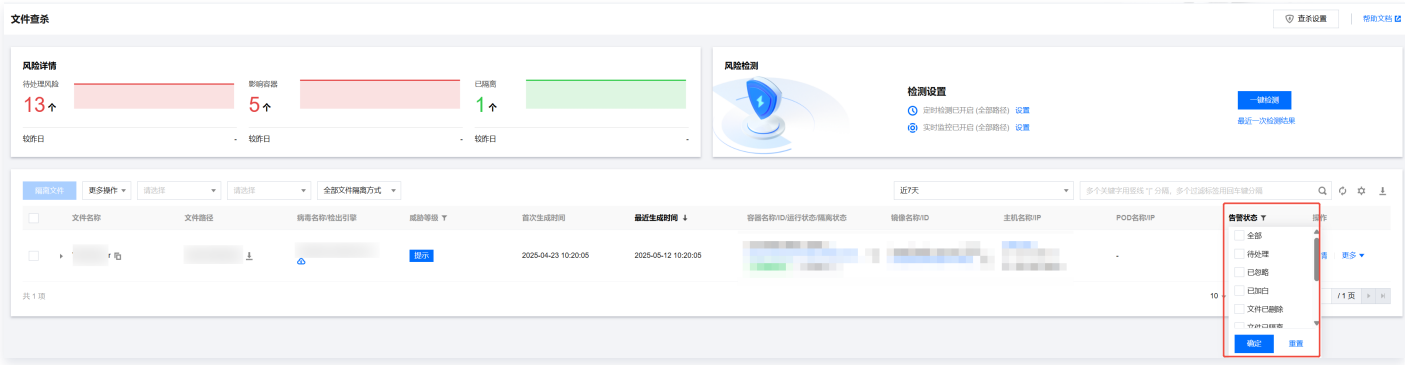
在 文件查杀页面 的事件列表模块中，展示模块中提供容器木马病毒检测结果。

筛选事件

在事件列表模块中，支持通过如下两种方法对事件进行筛选。

- 单击搜索框通过“文件名称、文件路径、病毒名称、容器名称”等关键词查询木马病毒事件。

- 单击告警状态，可以通过容器状态和事件状态对木马病毒事件进行查询。



查看详情

在事件列表模块中，单击**查看详情**，右侧抽屉展示事件详情信息，包括病毒文件基本信息、事件详情、事件描述和进程信息。仅实时监控上报的事件详情中展示进程信息。

处理事件

在事件列表模块中，单击立即处理，可以选择对事件进行添加白名单、隔离（推荐）、忽略、删除，单击确定，即可对事件进行上述处理。

参数说明：

- **添加白名单：若您确认该文件无恶意并添加白名单，系统将不再对该文件进行检测，请谨慎操作。**
- **隔离（推荐）：隔离此病毒文件，让黑客无法再次启动它，便于您定位病毒文件位置，对其进行查杀。**
- **忽略：仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。**
- **删除：删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。**

自动隔离文件

容器安全服务新增木马自动隔离功能，支持自动隔离检测出的系统黑名单文件，以及用户自定义的恶意文件。

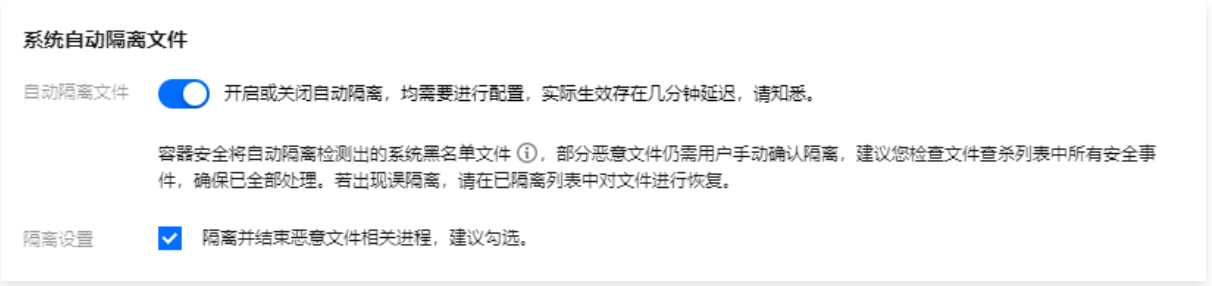
系统自动隔离文件

容器安全将自动隔离检测出的系统黑名单文件，部分恶意文件仍需用户手动确认隔离，建议您检查文件查杀列表中所有安全事件，确保已全部处理。若出现误隔离，请在已隔离列表中对文件进行恢复。

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **文件查杀**。
2. 在文件查杀页面，单击右上角的**查杀设置**。

3. 在查杀设置窗口中，单击**自动隔离文件**。
4. 在系统自动隔离文件模块，可单击开启或关闭自动隔离，同时，支持隔离并结束恶意文件相关进程。

> **说明：**
> - 系统黑名单文件：腾讯云容器安全运营专家与算法专家经过沉淀的文件名单，此名单中的文件可进行自动隔离。
> - 自动隔离开关默认关闭，客户可根据需求进行开启。启动自动隔离时，客户可自定义勾选是否隔离并结束恶意文件相关进程。
>   - 自动隔离开启时，系统黑名单和用户自定义黑名单均生效，支持对黑名单中的文件进行自动隔离。
>   - 自动隔离关闭时，系统黑名单和用户自定义黑名单均不对告警关联的恶意文件进行自动隔离。



用户自定义隔离文件

支持查看用户自定义隔离文件列表，自定义开启或关闭该文件的自动隔离开关。

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **文件查杀**。
2. 在文件查杀页面，单击右上角的**查杀设置**。

3. 在查杀设置窗口中，单击**自动隔离文件**。

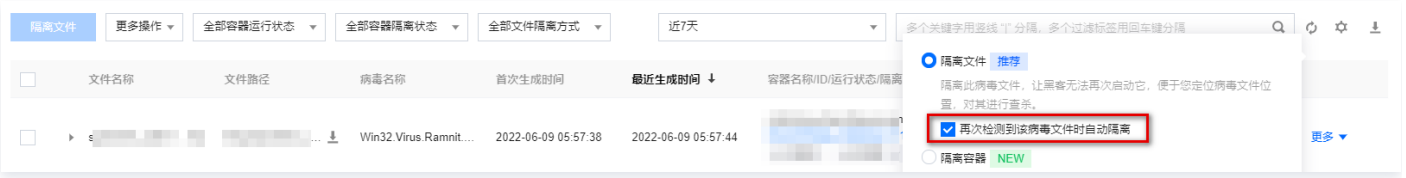
4. 在用户自定义隔离文件模块，支持控制自动隔离开关、查看详情和下载文件。

操作说明：

- 单击**自动隔离开关**，可开启或关闭自动隔离。
- 单击**详情**查看恶意文件的基本信息、危害描述和修复建议。
- 单击**下载**，可下载该恶意文件。

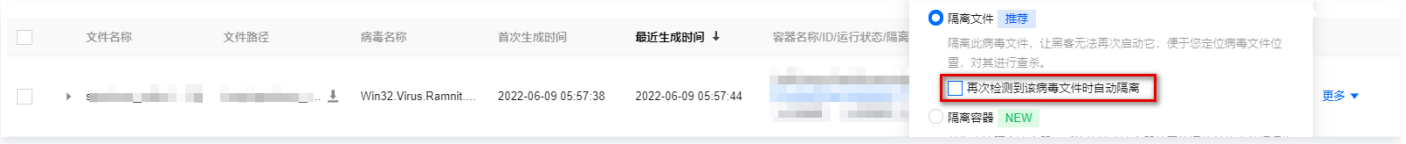
隔离文件列表

- 在 文档查杀页面 的事件列表中，手动隔离恶意文件时，如勾选“再次检测到该病毒文件时自动隔离”，该恶意文件的 MD5值将记录在用户自定义隔离文件列表，自动隔离开关状态为开启。系统将对后续检出的同样文件进行自动隔离。当事件列表中手动隔离的恶意文件取消隔离后，用户自定义隔离文件列表中将删除该条记录，自动隔离配置也不再生效。



- 文档查杀页面 的事件列表中，手动隔离恶意文件时，不勾选“再次检测到该病毒文件时自动隔离”，该恶意文件的MD5值将记录在用户自定义隔离文件列表，自动隔离开关状态为关闭。

> **说明：**
> 用户自定义隔离文件自动隔离生效，需开启系统自动隔离开关；否则，即使处理安全事件时勾选“再次检测到该病毒文件时自动隔离”，系统也不会对自定义黑名单进行隔离。



恶意外连

最近更新时间：2025-05-13 18:11:12

当容器向恶意域名或 IP 发起外连请求时，容器安全服务将检测此类行为，为您提供实时告警。当发现容器存在访问恶意域名/IP 的行为时，您的容器可能已经失陷，因为恶意域名/IP 可能是黑客的远控服务器、恶意软件下载源、矿池地址等。您需要及时进行如下排查：

1. 检查容器内的恶意进程及非法端口，删除可疑的启动项和定时任务。
2. 对容器存在的风险进行排查，如进行漏洞扫描、木马扫描等。
3. 对容器所使用的镜像进行加固，并替换运行中的容器。

事件列表

事件概览

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全** > **恶意外连**，默认进入事件列表页面。
2. 在事件列表页面的事件概览中，将根据系统上报的安全事件，实时统计待处理的恶意外连事件及其影响的容器数量。

事件列表

在事件列表中，默认展示近7天的恶意外连事件，如需查看更多事件，可调整查询时长。列表展示字段如下表所示。

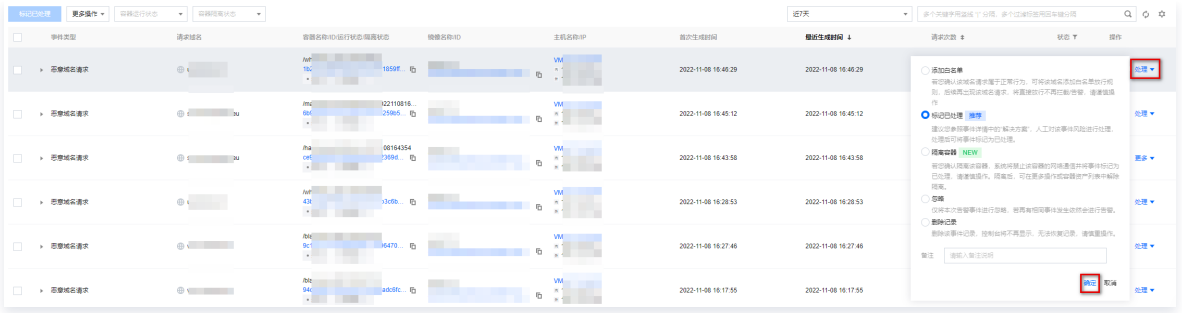
字段名称	字段详情
事件类型	恶意域名请求。
请求域名	触发安全事件的域名详情。
容器名称/ID/运行状态/隔离状态	展示容器资产相关的名称、ID、运行状态等信息；如客户认为该条安全事件属实，即容器可能已经失陷，可点击隔离容器避免风险在内网扩散。
镜像名称/ID	触发安全事件的容器的来源镜像，可通过单击**镜像 ID** 查看镜像详情，例如镜像安全风险、组件信息、构建历史等。
主机名称/IP	触发安全事件的容器所在的云服务器节点。展示该节点的名称和内外网 IP 信息。
POD 名称/IP	触发安全事件的容器所在的 Pod 状态和 IP 信息。
首次生成时间	该条安全事件首次发生的时间。
最近生成时间	该条安全事件最近发生的时间。
请求次数	系统按容器 ID、域名、进程路径、进程启动用户等对待处理安全事件进行聚合展示，聚合周期为当天。
状态	包括待处理、已处理、已忽略、已加白。
操作	• 单击**详情**查看事件详情。详情包括事件详情，关联容器、镜像、主机等资产信息，风险描述，解决方案，请求域名详情和三层进程信息。 • 单击**处理**对安全事件进行处理并备注说明。包括添加白名单、标记已处理、隔离容器、忽略和删除记录。

查看详情

在事件列表中，单击**详情**，进入事件详情，展示事件详情，关联容器、镜像、主机等资产信息，风险描述，解决方案，请求域名详情和三层进程信息。

处理事件

1. 在事件列表中，单击**处理**，可以选择对事件进行添加白名单、标记已处理、隔离容器、忽略和删除记录，单击**确定**。



2. 在二次确认窗口中，进行如下操作：
   - 添加白名单：输入白名单域名和备注，单击**确认**。添加白名单时，系统会根据加白的来源事件自动填入请求的域名，如有需要可手动调整为母域名。同时可勾选“批量处理相同事件（将相同域名触发的待处理事件批量加白）”，勾选并确认后，系统将批量对相同域名产生的安全事件批量加白处理。

     > **注意：**
     > 若您确认该域名请求属于正常行为，可将该域名添加白名单放行规则，后续再出现该域名请求，**将直接放行不再拦截/告警，请谨慎操作**。

   - 标记已处理：建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，单击**确定**，处理后可将事件标记为已处理。
   - 隔离容器：若您确认隔离该容器，系统将禁止该容器的网络通信并将事件标记为已处理，请谨慎操作。单击**确定**隔离后，可在更多操作或容器资产列表中解除隔离。
   - 忽略：单击**确定**，仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。
   - 删除：单击**删除**，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

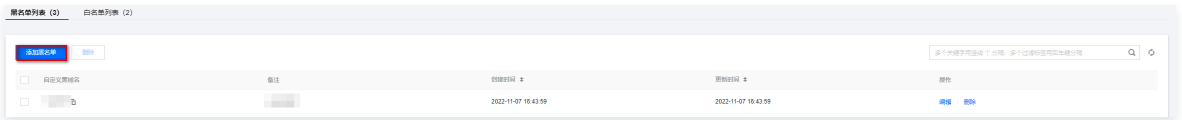
黑白名单管理

除容器安全服务产品提供的系统黑名单，客户也可自定义域名黑名单和域名白名单。黑白名单生效优先级为：**白名单 > 黑名单**。

- 黑名单：当容器向名单中的域名发起外连请求时，系统将判定为恶意外联行为，为您产生实时告警，可前往 事件列表 查看。
- 白名单：当容器向白名单中的域名发起外连请求时，系统将直接放行，不再进行告警。

黑名单管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**运行时安全 > 恶意外联 > 黑白名单管理**。
2. 在黑名单列表页签，单击**添加黑名单**。

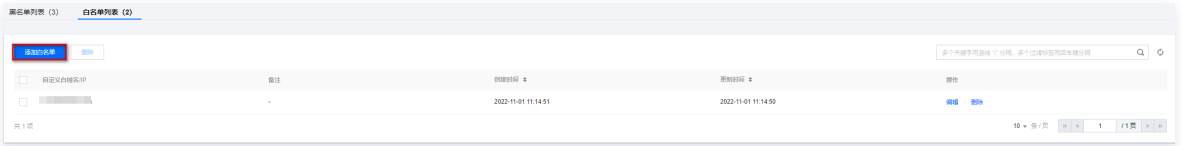


3. 在添加黑名单窗口中，可支持批量新增多个自定义黑域名；输入域名时，支持前缀置空的泛域名，例如 `*.tencent.com`；泛域名下的子域名均会告警。

4. 单击**确认**，列表将根据实际输入的域名生成记录；当输入多个域名时，将生成多条记录。

白名单管理

1. 登录 容器安全服务控制台 ，在左侧导航中，单击**运行时安全** > **恶意外联** > **黑白名单管理**。
2. 在白名单列表页签，单击**添加白名单**。



3. 在添加白名单窗口中，可支持批量新增多个自定义白域名；输入域名时，支持前缀置空的泛域名，例如 `*.tencent.com`；泛域名下的子域名均会被放行，不产生告警。

4. 单击**确认**，列表将根据实际输入的域名生成记录；当输入多个域名时，将生成多条记录。

高级防御
概述

最近更新时间：2025-05-13 18:11:12

高级防御支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供异常进程、文件篡改和高危系统调用安全功能。

- 异常进程：通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并告警通知或拦截。系统监控策略包括代理软件、横向渗透、恶意命令、反弹 Shell、无文件程序执行、高危命令、敏感服务异常子进程启动等。
- 文件篡改：通过系统规则和用户自定义检测规则，实时监控核心文件被修改的文件异常访问行为，并告警通知或拦截。系统监控策略包括篡改计划任务、篡改系统程序、篡改用户配置等。
- 高危系统调用：基于腾讯云安全自适应学习技术，实时审计容器内发起的可能引起安全风险的 Linux 系统调用行为。
- K8s API 异常请求：支持实时监控集群 API 异常请求行为，包括系统策略和用户自定义策略两部分。
  - 系统规则：基于腾讯云安全技术及多维度多种手段，通过“匿名访问”“异常 UA 请求”“匿名用户权限变动”“凭据信息获取”“敏感路径挂载”“命令执行”“异常定时任务”“静态 Pod 创建”“可疑容器创建”等共9个规则类型，对集群API异常请求行为进行多方位监测。
  - 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求。

> **说明：**
> 容器告警事件仅保留半年以内的数据，每天定时检测并自动清理超过180天的告警事件，超出时间范围将无法显示和查询。如有需要，建议使用日志投递留存。

异常进程
事件列表

最近更新时间：2025-05-13 09:54:52

异常进程是基于自适应学习技术，通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并实时告警通知或拦截。异常进程包含事件列表和规则配置两大模块。本文档介绍高级防御的事件列表功能。

筛选刷新事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击搜索框，可通过“连接进程”关键词对白名单事件进行查询。

3. 在事件列表页面，单击操作栏右侧 图标，即可刷新事件列表。

导出事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击 图标勾选所需的异常进程事件后，单击 图标即可导出异常进程事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

事件状态处理

登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对异常进程事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击 图标勾选所需的异常进程事件后，单击**标记已处理>确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击 图标勾选所需的异常进程事件后，单击**忽略>确定**，即可将选中事件忽略。

> **说明：**
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击 图标勾选所需的异常进程事件后，单击**删除>确定**，即可将选中事件删除。

> **注意：**
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理、隔离容器、忽略和删除记录等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

> **说明：**
> - 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
> - 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

> **说明：**
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 事件列表**，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧 ▸ 图标，可查看事件描述。

3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

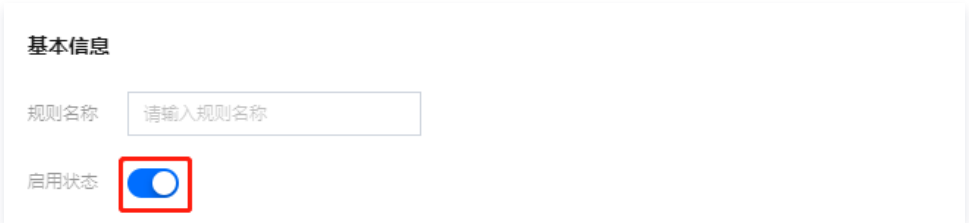
4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
> 标记已处理、忽略和删除：相应操作处理请参考 事件状态处理 。

5. 在事件详情页面，单击**加白**进入复制规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击  图标开启或关闭规则检查。

> **说明：**
> 关闭后，将不再进行该规则检测！



- 配置规则：需输入进程路径和执行动作。单击**添加**或**删除**，可进行添加或删除规则。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或  图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。
2. 在事件列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该异常进程事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。
2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。
3. 事件数量：聚合时间范围内该异常进程事件触发告警的总数量。
4. 动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。
5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

最近更新时间：2025-05-13 18:11:12

异常进程是基于自适应学习技术，通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并实时告警通知或拦截。异常进程包含事件列表和规则配置两大模块。本文档介绍高级防御的规则配置功能。

筛选刷新规则

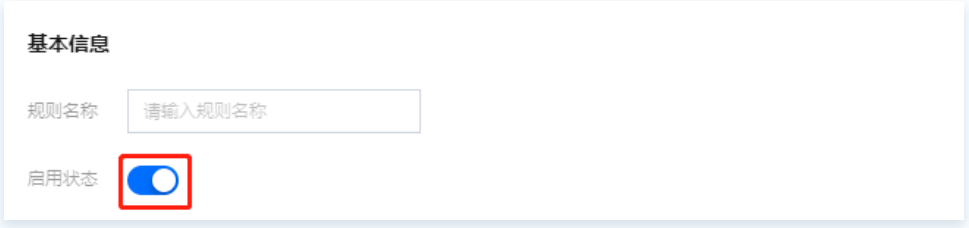
1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。
2. 在规则配置页面，单击搜索框，可通过“规则名称”关键词对配置规则进行查询。

3. 在规则配置页面，单击操作栏右侧 图标，即可刷新规则列表。

新增规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。
2. 在规则配置页面，单击**创建规则**，右侧抽屉弹出新增规则页面。

3. 在新增规则页面，需配置基本信息、配置规则和镜像生效范围。
   - 基本信息：输入事件的规则名称，单击 图标开启或关闭规则检查。

> **说明：**
> 关闭后，将不再进行该规则检测！
>
> 
>

   - 配置规则：需输入进程路径和执行动作。单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
> - 配置规则最多可添加30条。

- 执行动作有：
- 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
- 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。
- 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

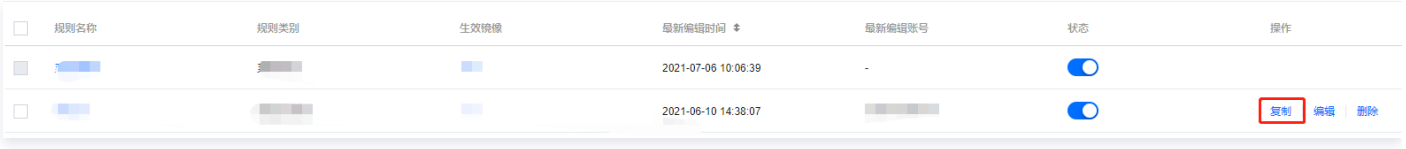
○ 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

说明：
支持按住 Shift 键进行多选。

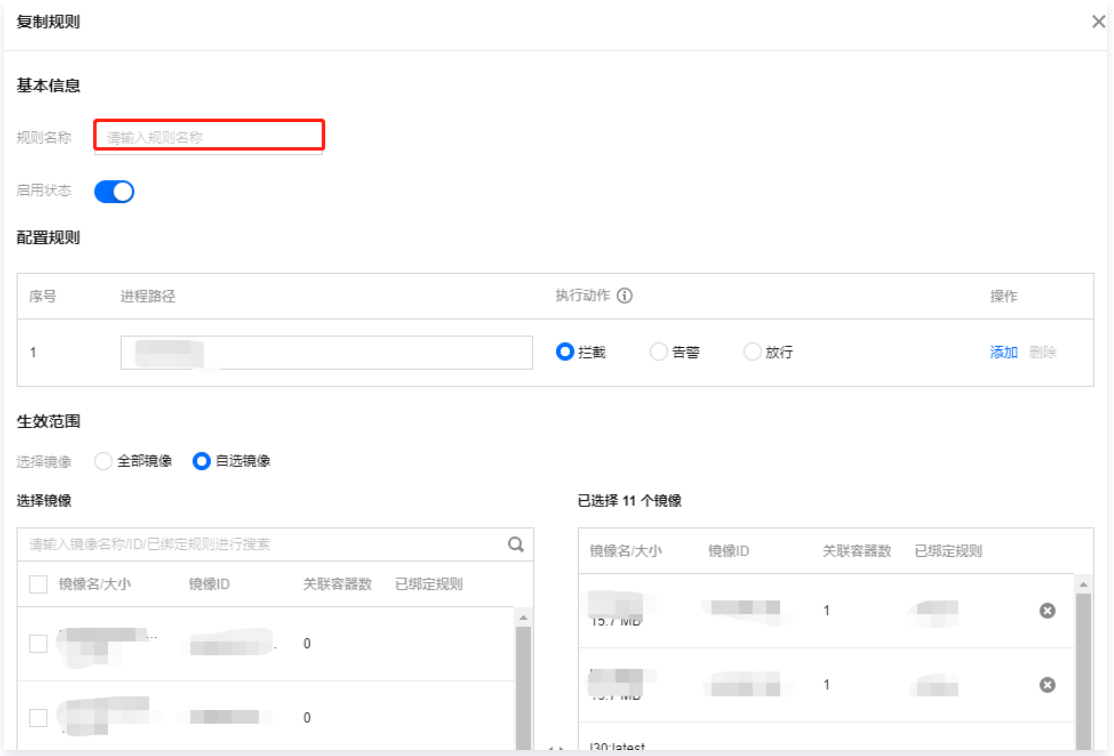
4. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

复制规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。
2. 在规则配置页面，单击右侧**复制**，右侧弹出复制规则页面。



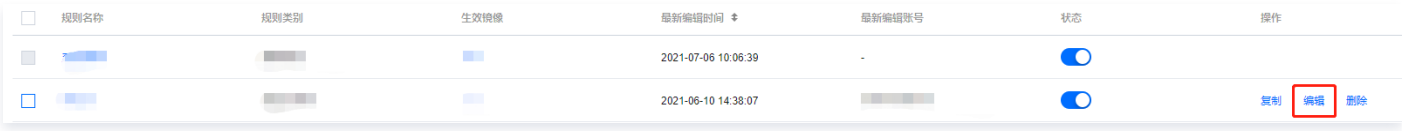
3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。



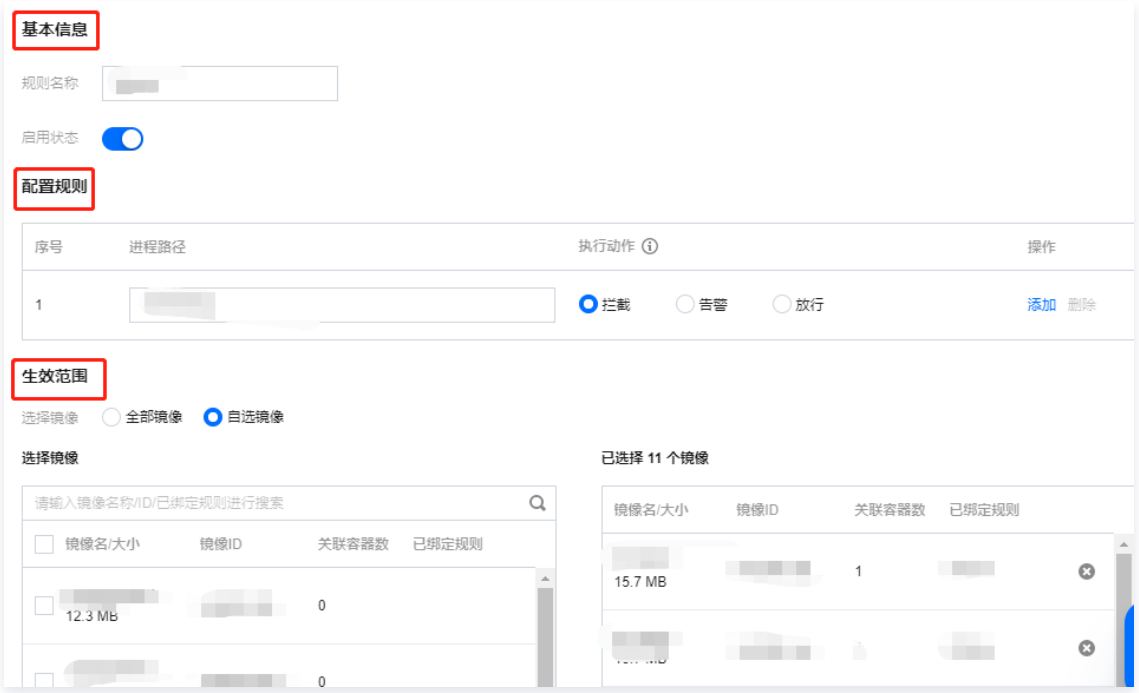
4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消复制规则。

编辑规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。
2. 在规则配置页面，单击右侧**编辑**，右侧弹出编辑规则设置页面。



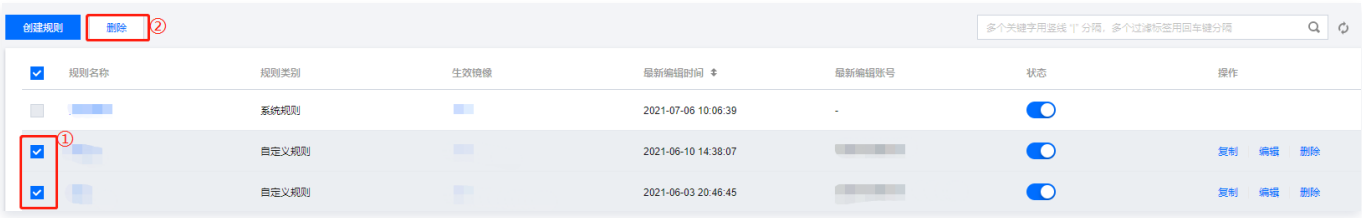
3. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。



4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改规则。

删除规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，可选择如下两种方式删除规则：
   - 选择所需的规则单击 图标，后单击操作栏左侧**删除**，弹出“确认删除”弹窗。



   - 选择所需规则的所在行，单击右侧**删除**，弹出“确认删除”弹窗。

3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除规则。

> **说明：**
> 删除后，规则将无法恢复，该规则的关联镜像将自动关联系统默认规则。

导出规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击 图标勾选所需的异常进程规则后，单击 图标即可导出异常进程规则。

> **说明：**
> 单击操作栏处 图标，可进行批量勾选。

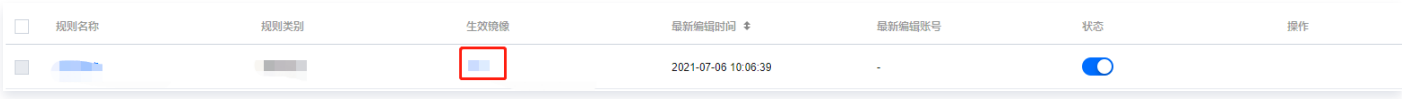
自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 异常进程 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 规则类别：系统规则或自定义规则。
2. 生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。



3. 状态：启用/禁用。
4. 操作：系统策略操作栏仅复制规则，用户自定义规则支持复制、编辑和删除。

文件篡改
事件列表

最近更新时间：2025-05-13 18:11:12

文件篡改功能提供文件篡改监测事件列表和规则配置列表。事件列表展示模块中提供文件篡改检测结果。

筛选刷新事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击搜索框，可通过“文件名称、进程路径和命中规则”等关键词对文件篡改检测结果进行查询。

3. 在事件列表页面，单击操作栏右侧 图标，即可刷新事件列表。

导出检测结果

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击 图标勾选所需的文件篡改检测事件后，单击 图标即可导出文件篡改检测事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

更改事件状态

登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对文件篡改检测事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击 图标勾选所需的文件篡改检测事件后，单击**标记已处理>确定**，即可将选中事件标记已处理。

> **说明：**

> 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击 图标勾选所需的文件篡改检测事件后，单击**忽略>确定**，即可将选中事件忽略。

> **说明：**
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击 图标勾选所需的文件篡改检测事件后，单击**删除>确定**，即可将选中事件删除。

> **注意**
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理和忽略等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

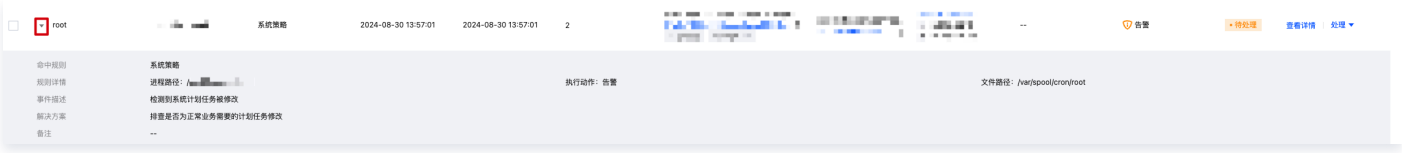
> **说明：**
> - 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
> - 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

> **说明：**
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。
2. 在事件列表页面，单击进程路径左侧 ▸ 图标，可查看事件描述。



3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

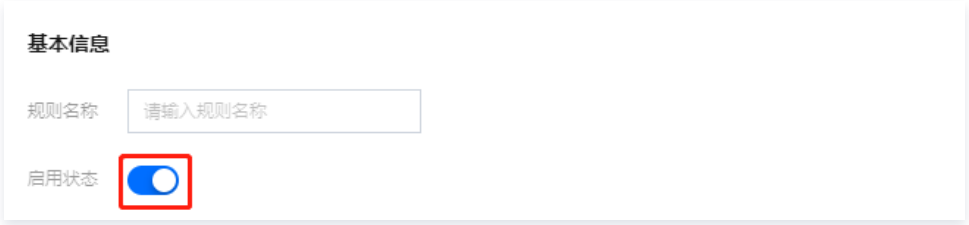
4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
> 标记已处理、忽略和删除：相应操作处理请参考 更改事件状态 。

5. 在事件详情页面，单击**加白**进入复制规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击  图标开启或关闭规则检查。

> **说明：**
> 关闭后，将不再进行该规则检测！



- 配置规则：输入需放行的进程路径和被访问文件路径，选择执行动作。单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
> - 配置规则最多可添加30条。
> - 执行动作有：
> - 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
> - 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。
> - 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。
2. 在事件列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该文件篡改事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。
2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。
3. 事件数量：聚合时间范围内该文件篡改事件触发告警的总数量。
4. 动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。
5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

最近更新时间：2025-05-13 22:04:12

文件篡改功能提供文件篡改监测事件列表和规则配置列表。规则配置展示模块中提供配置规则列表。

使用限制

目前只支持对具体文件的读写操作进行拦截，暂未支持文件创建、删除、移动、重命名、权限修改等操作拦截。

筛选刷新规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击搜索框，可通过“规则名称”关键词对配置规则进行查询。

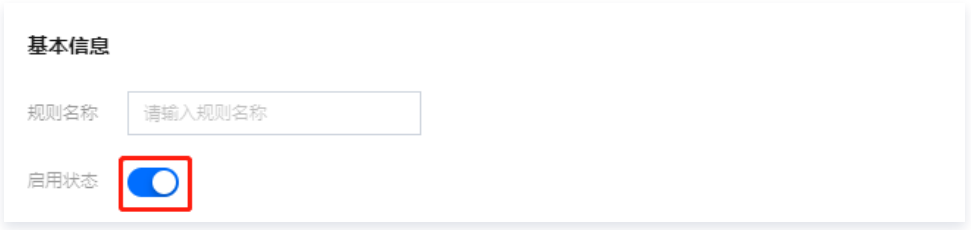
3. 在规则配置页面，单击操作栏右侧 图标，即可刷新规则列表。

新增规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击**创建规则**，右侧抽屉弹出新增规则页面。

3. 在新增规则页面，需配置基本信息、配置规则和镜像生效范围。
   - 基本信息：输入事件的规则名称，单击 图标开启或关闭规则检查。

> **说明：**
> 关闭后，将不再进行该规则检测！



   - 配置规则：需输入进程和被访问文件的实际路径，并选择执行动作，单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
> - 配置规则最多可添加30条。
> - 执行动作有：
>   - 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
>   - 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。

- 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

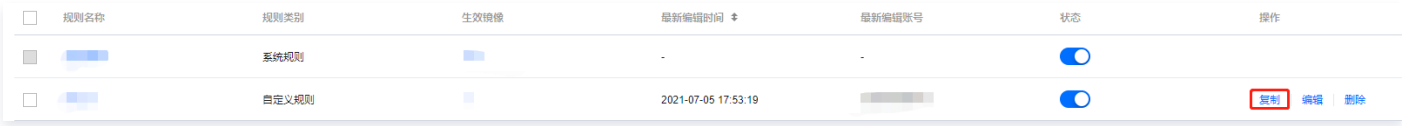
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

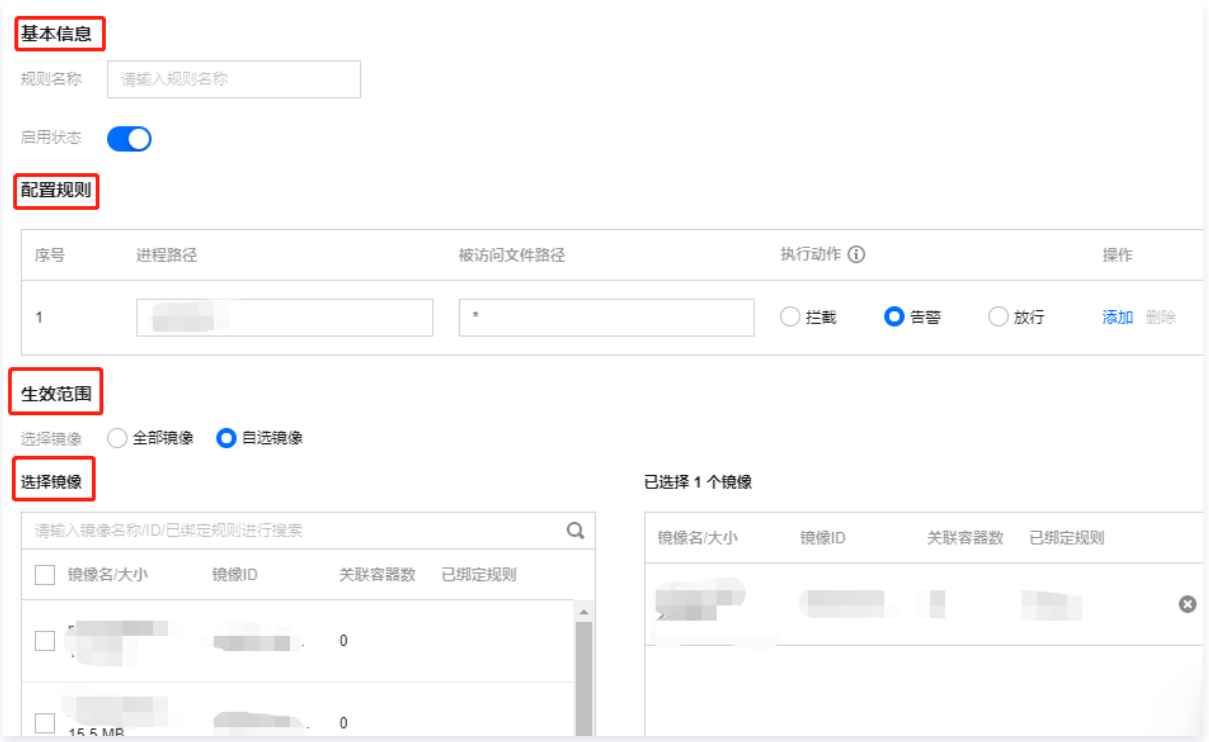
4. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

复制规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。
2. 在规则配置页面，单击右侧**复制**，右侧弹出复制规则页面。



3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。

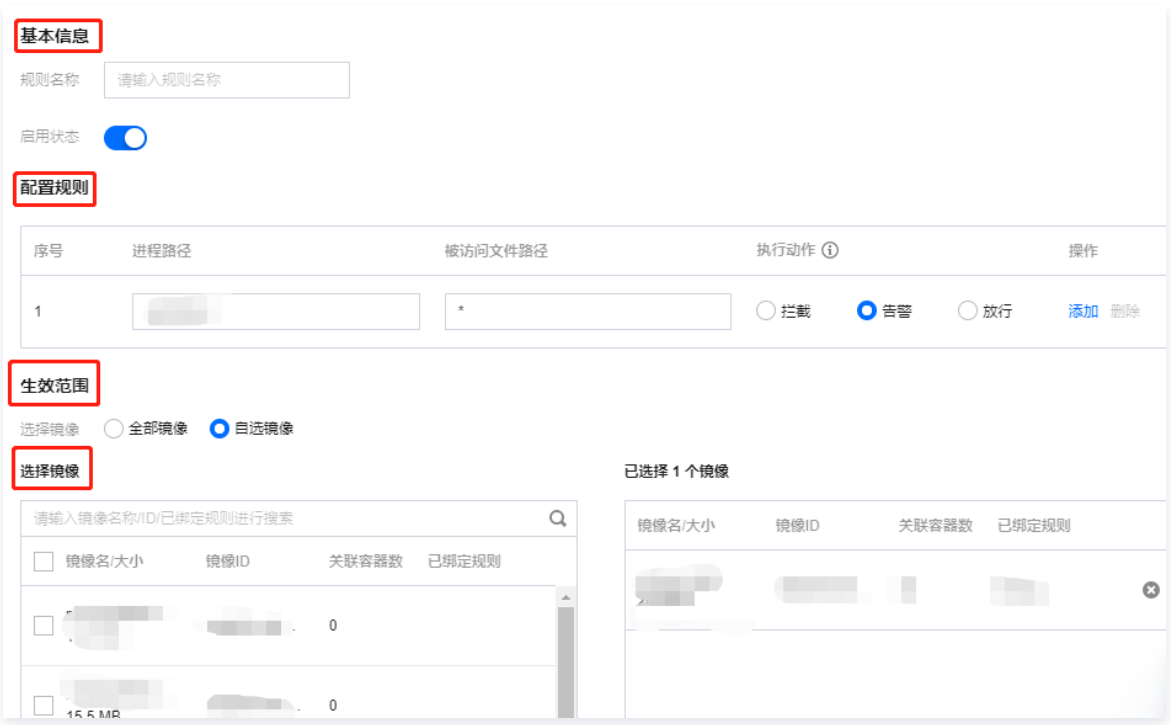


4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消复制规则。

编辑规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击右侧**编辑**，右侧弹出编辑规则设置页面。

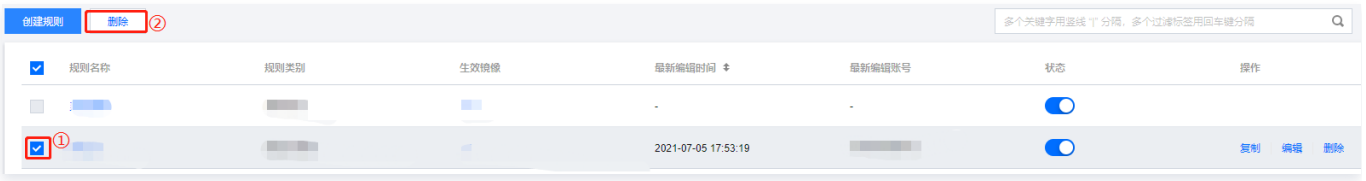
3. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。



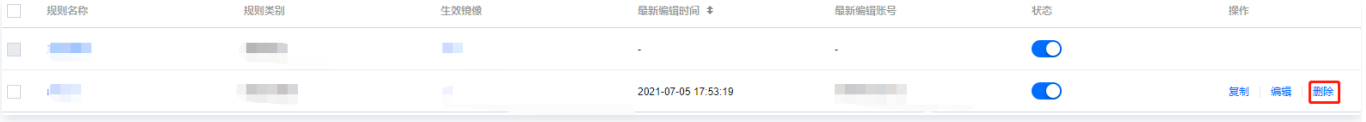
4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改规则。

删除规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御>文件篡改>规则配置**，进入规则配置页面。
2. 在规则配置页面，可选择如下两种方式删除规则：
   - 选择所需的规则单击 图标，后单击操作栏左侧**删除**，弹出“确认删除”弹窗。



   - 在规则配置页面，选择所需规则的所作行，单击右侧**删除**，弹出“确认删除”弹窗。



3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除规则。

> **说明**
> 删除后，规则将无法恢复，该规则的关联镜像将自动关联系统默认规则。

导出规则

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击 图标勾选所需的文件篡改规则后，单击 图标即可导出文件篡改规则。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 文件篡改 > 规则配置**，进入规则配置页面。
2. 在规则配置页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 规则类别：系统规则或自定义规则。
2. 生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。
3. 状态：启用/禁用
4. 操作：系统策略操作栏仅复制规则；用户自定义规则支持复制、编辑和删除。

高危系统调用
事件列表

最近更新时间：2025-05-20 15:13:02

高危系统调用提供可能存在风险的系统调用行为检测事件列表和白名单管理列表。事件列表展示模块中提供高危系统调用检测结果。

筛选刷新事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 高危系统调用 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击搜索框，可通过“进程路径、系统调用名称和容器名称”等关键词对高危系统调用检测事件进行查询。

3. 在事件列表页面，单击操作栏右侧 图标，即可刷新事件列表。

导出事件列表

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 高危系统调用 > 事件列表**，进入事件列表页面。
2. 在事件列表页面，单击 图标勾选所需的文件篡改检测事件后，单击 图标即可导出高危系统调用事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

更改事件状态

登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 高危系统调用 > 事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对高危系统调用事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击 图标勾选所需的高危系统调用事件后，单击**标记已处理>确定**，即可将选中事件标记已处理。

> **说明：**

建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击 图标勾选所需的高危系统调用事件后，单击**忽略>确定**，即可将选中事件忽略。

说明：
仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击 图标勾选所需的高危系统调用事件后，单击**删除>确定**，即可将选中事件删除。

注意
删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理和忽略等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

说明：
- 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
- 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

说明：
删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > 高危系统调用 > 事件列表**，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧 ▸ 图标，可查看事件描述。

3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
> 标记已处理、忽略和删除：相应操作处理请参考 更改事件状态 。

5. 在事件详情页面，单击**加白**进入新增白名单页面，需确认满足条件（进程路径、系统调用名称）和镜像生效范围。

- 满足条件：进程路径和系统调用名称，不可更改内容。

- 镜像生效范围：全部镜像和自选镜像。其中单击所需的自选镜像 ☐ 或 ⊗ 图标，即可选中或删除自选镜像。

> **说明：**
> 支持按住 Shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消新增白名单。

自定义列表管理

1. 登录 容器安全服务控制台 ，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击 ☼ 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该系统调用事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。
2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。
3. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。
4. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。
5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

白名单管理

最近更新时间：2025-05-20 15:13:02

白名单管理展示模块中提供配置白名单接口和白名单展示列表。

筛选刷新白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击搜索框，可通过“进程路径、系统调用名称”关键词对配置的白名单进行查询。

3. 在白名单管理页面，单击操作栏右侧 图标，即可刷新白名单管理列表。

新增白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击**新增白名单**，右侧弹出新增白名单设置页面。

3. 在新增白名单设置页面，需配置白名单生效的进程路径、系统调用名称和生效范围。
   - 单击进程路径和系统调用名称左侧 图标，输入进程路径，并选择系统调用名称。

     说明：
     进程路径不能为空。

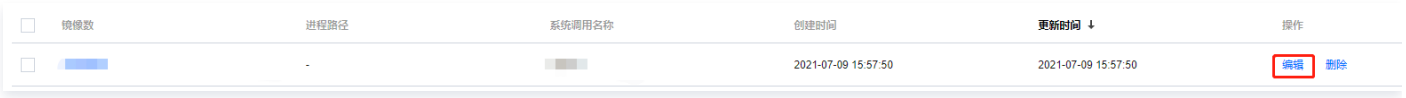
   - 白名单生效范围为全部镜像或自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

     说明：
     支持按住 Shift 键进行多选。

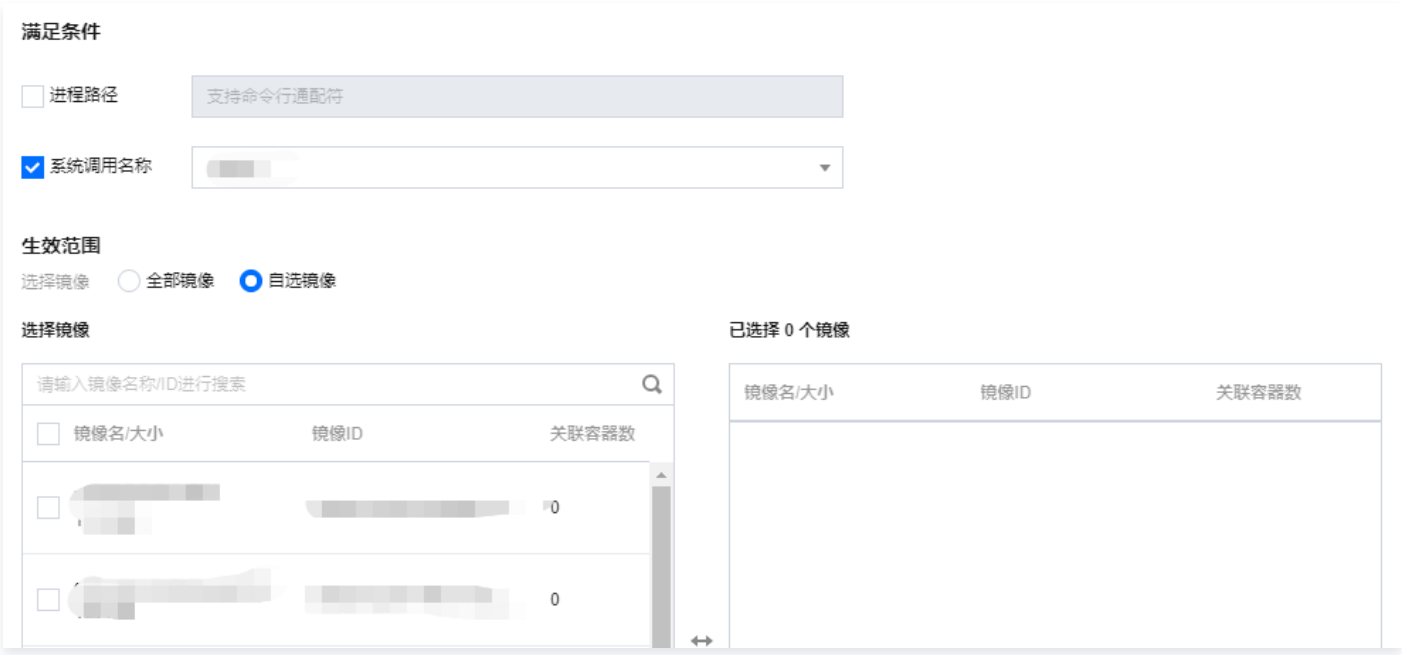
4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消新增白名单。

编辑白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击右侧**编辑**，右侧弹出编辑白名单设置页面。



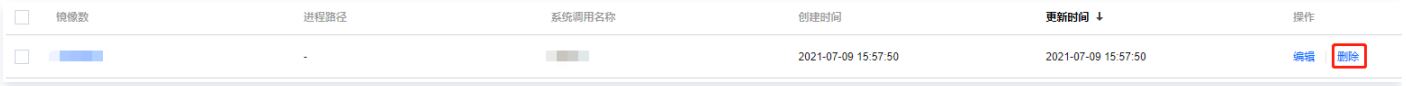
3. 在编辑白名单设置页面，可修改白名单生效的进程路径、系统调用名称和生效范围。



4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改白名单。

删除白名单

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击右侧**删除**，弹出“确认删除”弹窗。

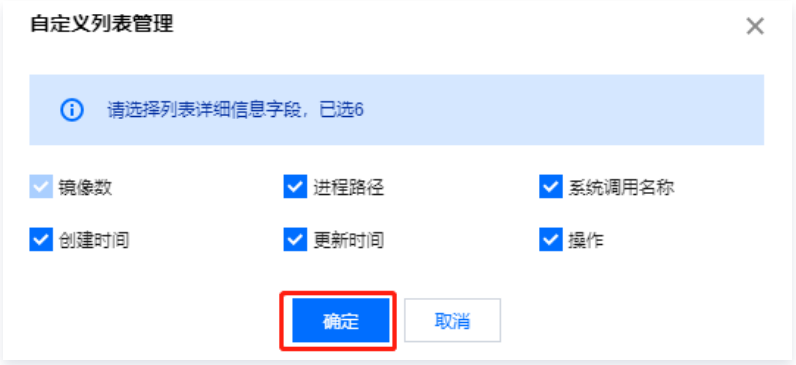


3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除白名单。

> **说明：**
> 删除后，白名单将无法恢复，该白名单的关联镜像触发系统策略时将再次产生告警。

自定义列表管理

1. 登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。
2. 在白名单管理页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。



列表重点字段说明

1. 镜像数：白名单生效的镜像。
2. 进程路径：白名单生效的进程路径。
3. 系统调用名称：白名单生效的系统调用名称。
4. 操作：用户可编辑、删除白名单。

K8s API 异常请求

最近更新时间：2025-05-13 18:11:12

支持实时监控集群 API 异常请求行为，包括系统策略和用户自定义规则两部分。

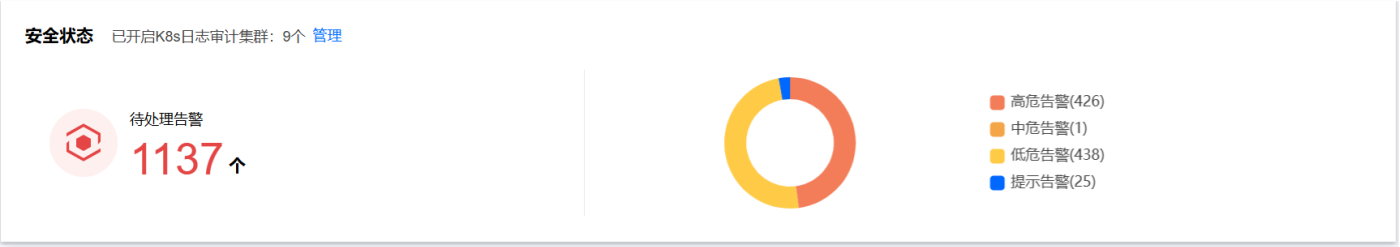
- 系统策略：基于腾讯云安全技术及多维度多种手段，通过匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 Pod 创建、可疑容器创建等共9个规则类型，对集群 API 异常请求行为进行监测。
- 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求。

事件列表

登录 容器安全服务控制台，在左侧导航中，单击**高级防御** > **K8s API 异常请求**，默认进入事件列表页面。

安全状态和事件趋势

- 安全状态将根据系统上报的安全事件，实时统计待处理的 K8s API 异常请求事件，以及按高危、中危、低危、提示来统计安全告警数量。



- 事件趋势将根据系统上报的安全事件，按命中的系统规则和自定义规则来统计近七天安全事件趋势。

事件列表

您可以选择“最近生成时间”来查看安全事件，或通过集群名称或集群 ID 来检索关联的安全事件。事件列表字段包括：

字段名称	字段详情
命中规则	匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 pod 创建、可疑容器创建等9个系统规则和用户自定义规则。
规则类型	系统规则、用户自定义规则。
威胁等级	高危、中危、低危和提示。
受影响集群名称/ID/运行状态	展示安全事件影响的集群名称、集群 ID 以及集群运行状态。
首次生成时间	该条安全事件首次发生的时间。
最近生成时间	该条安全事件最近发生的时间。
告警数量	系统按集群名称、集群 ID、命中规则、请求日志等对待处理安全事件进行聚合展示，聚合周期为当天。
状态	待处理、已处理、已忽略、已加白。
操作	单击**详情**，查看事件详情。

查看详情

在事件列表中，单击**详情**，查看事件详情。详情包括事件详情，集群名称/ID，集群运行时组件，风险描述，建议方案，异常请求信息和 json 日志。

处理事件

1. 在事件列表中，单击**处理**，可以选择对事件进行标记已处理、添加白名单、忽略和删除记录，单击**确定**。
2. 在二次确认窗口中，进行如下操作：
   - 标记已处理：建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，单击**确定**，处理后可将事件标记为已处理。
   - 添加白名单：配置相关参数，单击**确定**。

> **说明：**
> - 若您确认该 K8s API 请求属于正常行为，可添加白名单放行规则，后续再出现该请求，将直接放行不再告警，请谨慎操作。
> - 添加白名单时，系统会根据加白的来源事件自动填入触发告警的字段和集群。如有需要，可手动调整白名单的生效字段和生效集群范围。

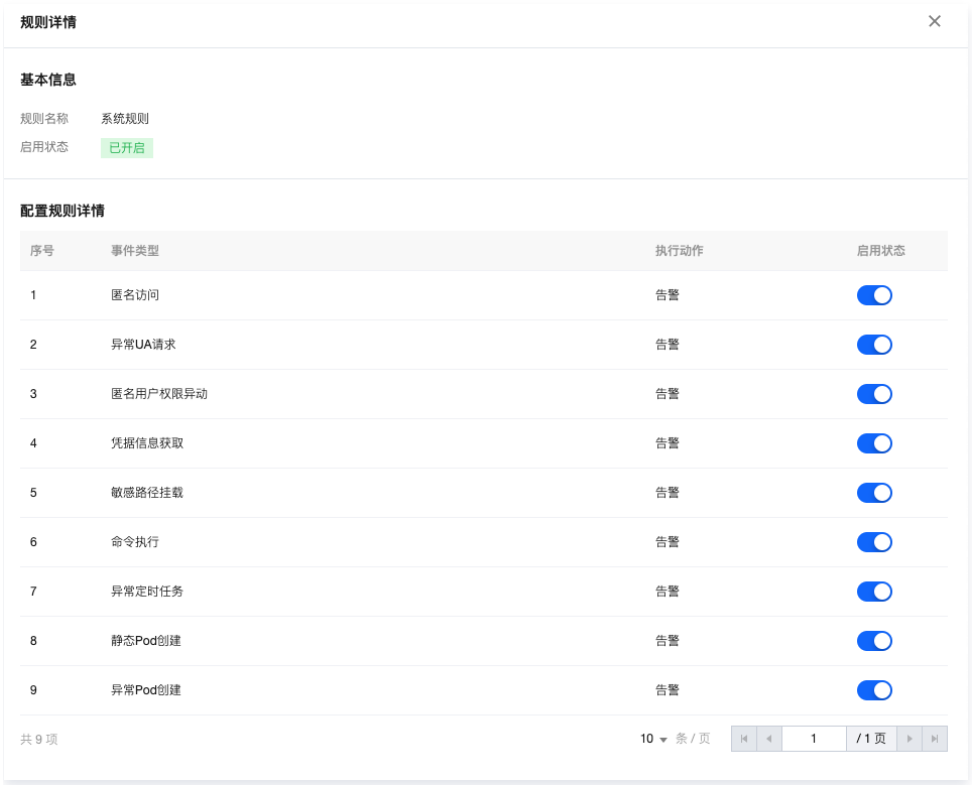
- 忽略：单击**确定**，仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。
- 删除记录：单击**确定**，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

规则配置

登录 容器安全服务控制台，在左侧导航中，单击**高级防御 > K8s API 异常请求 > 规则配置**，进入规则配置页面。

系统规则

在规则配置页面，开启或关闭系统规则和自定义规则。单击系统**规则名称**，可查看全部系统规则类型，如下图所示。用户也可以通过此页面，关闭部分系统规则类型。



自定义规则

除容器安全服务产品提供的系统规则，用户也可以自定义创建规则。
在规则配置页面，单击**创建规则**，配置相关参数，单击**保存**。

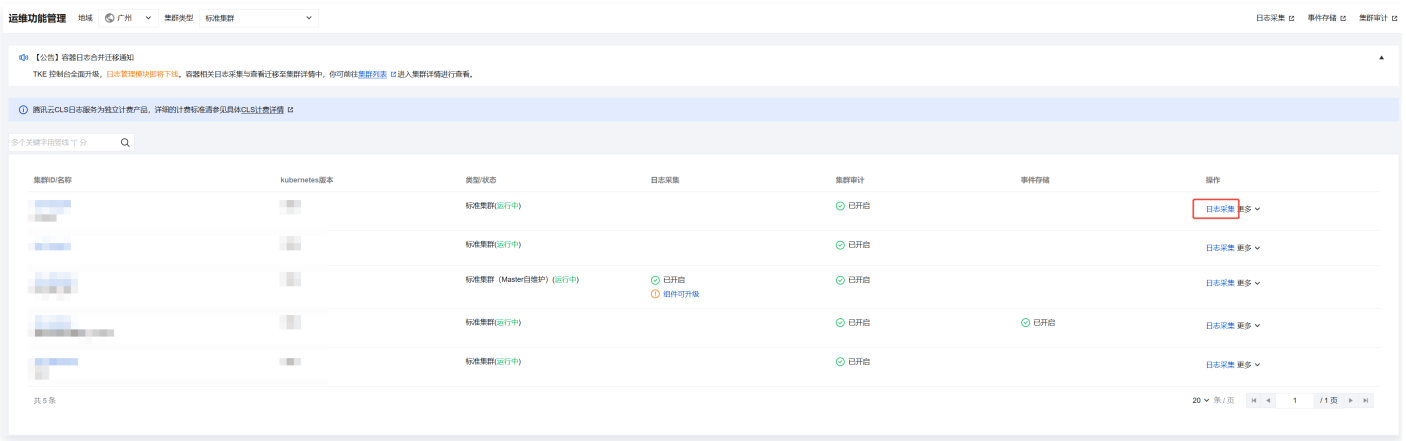
字段名称	字段详情
基础设置	包括自定义规则的名称，以及是否启用规则的开关。
规则设置	• 在此部分配置告警和放行的字段，配置告警字段时需同步配置规则的威胁等级。 • 当配置内容多条时，单击下方的**添加规则**即可。 • 配置规则的具体内容时，单击匹配范围列的**编辑**，规则配置支持正则表达式。
生效范围	用户可自定义选择配置规则的生效集群范围。 注意：**同一个集群只能绑定一个自定义规则**，如需对一个集群配置多条检测规则，建议在同一条规则中编辑添加。

TKE K8s集群开启审计流程

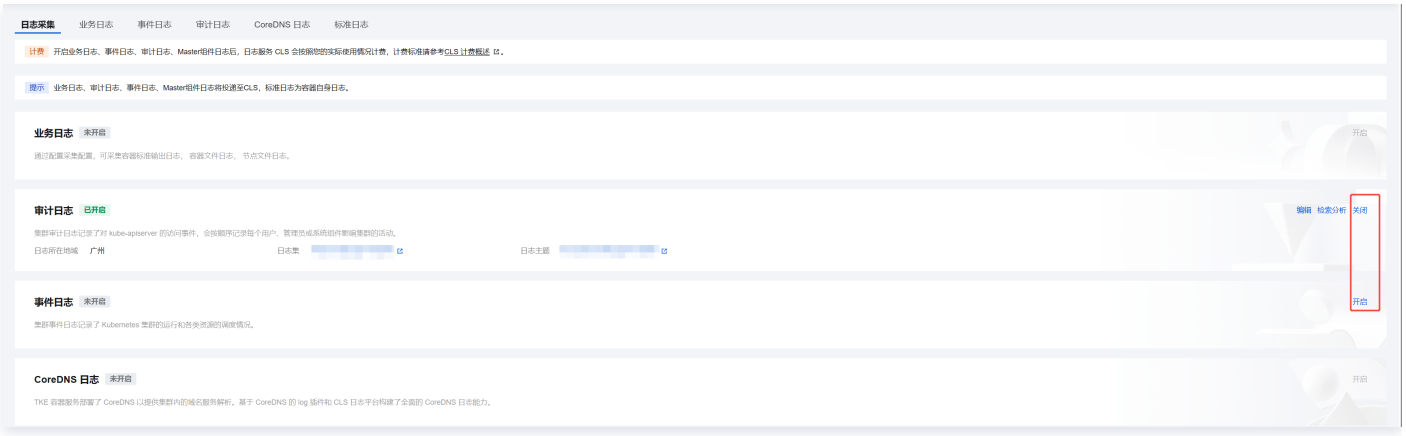
当集群的审计功能未开启时，无法采集到 K8s API 的审计日志来进行风险检测。

> **说明：**
> 开启集群审计后，日志服务 CLS 会按照您的实际使用情况计费，计费标准请参考 CLS 计费概述 。

1. 在容器服务控制台的 运维功能管理页面 ，选中需要开启审计的集群，单击**日志采集**。



2. 在**日志采集**页面，单击审计日志功能的**开启**。



3. 单击**开启**后可修改日志所在地域与日志集，单击**确定**即可。

策略管理
镜像拦截策略

最近更新时间：2025-05-13 18:11:12

用户可在 镜像拦截策略页面 配置告警和拦截策略。镜像拦截策略支持您对云内外集群（前提：节点主机已安装容器安全服务 Agent）存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

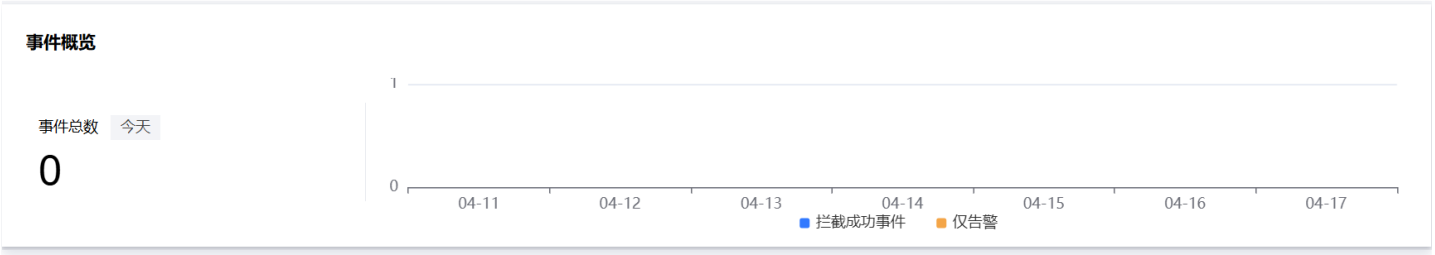
- 创建拦截策略后，约3-5分钟生效。生效后，如命中的风险镜像存在启动容器行为，系统将按照策略配置的告警、拦截要求，对镜像启动行为进行告警、或拦截容器启动并上报拦截记录。
- 目前支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像。
- 拦截特权模式镜像仅支持配置一条规则，如需修改拦截镜像的范围，可编辑调整已配置规则。

查看策略概览

用户配置告警和拦截策略后，系统将统计开启的策略总数，以及其包含的已生效拦截策略和观察期策略数量。

查看事件概览

用户配置镜像启动拦截策略后，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录。
在事件概览中，将对每日镜像启动拦截事件和仅告警的事件进行统计，展示近7日两类事件的趋势图和当前的事件总数。



创建策略

1. 登录 容器安全服务控制台，在左侧导航中，选择**策略管理** > **镜像拦截策略**。
2. 在镜像拦截策略页面，单击**创建策略**，配置相关参数，单击**保存**。

> ⚠ **注意：**
> 根据设置的策略，对节点上启动的容器进行拦截，镜像拦截可能对业务造成影响，请谨慎操作。

- 新建拦截存在严重或高危风险的镜像拦截策略。

参数类别	参数名称	参数详情
基本信息	策略模板	必选，选择“拦截存在严重&高危风险的镜像”。
	策略名称	必填，不超过128字符。
	策略描述	非必填，不超过256字符。
	启用状态	• 开启：开始执行镜像拦截动作，或观察期开始倒计时。 • 关闭：策略不生效。
	策略生效状态	• 立即生效：即策略下发完成后，命中目标镜像时，立即执行拦截动作。 • 观察 n 天生效：即观察期仅告警不拦截，观察期结束立即执行拦截动作。
拦截策略详情	策略类型	策略模板选择“拦截存在严重&高危风险的镜像”，策略类型为风险镜像拦截；如需修改策略类型，需调整策略模板。
	拦截详情	存在漏洞、存在木马病毒、存在敏感信息这三类至少需配置一项。 • 配置“存在漏洞”，可按CVE编号、组件名称及版本号、或按漏洞分类进行配置。 • 配置“存在木马病毒”，可按文件 MD5、或按木马病毒类型进行配置。 • 配置“存在敏感信息”，可按威胁等级和敏感信息的类型进行配置。
策略生效范围	选择镜像	配置风险镜像拦截时，策略生效的范围需为已扫描镜像，未扫描镜像系统无法判断是否存在漏洞、木马病毒或敏感信息风险。

- **新建特权模式镜像拦截策略**

  新建特权模式镜像拦截策略时，**如已创建过特权镜像拦截策略，则无法新建**，需对已创建策略进行编辑新增；未新建时，可单击**创建策略**直接配置。

参数类别	参数名称	参数详情
基本信息	策略模板	必选，选择“拦截以特权模式启动的容器镜像”。
	策略名称	必填，不超过128字符。
	策略描述	非必填，不超过256字符。
	启用状态	• 开启：开始执行镜像拦截动作，或观察期开始倒计时。 • 关闭：策略不生效。
	策略生效状态	• 立即生效：即策略下发完成后，命中目标镜像时，立即执行拦截动作。 • 观察 n 天生效：即观察期仅告警不拦截，观察期结束立即执行拦截动作。
拦截策略详情	策略类型	策略模板选择“拦截以特权模式启动的容器镜像”，策略类型为特权镜像拦截；如需修改策略类型，需调整策略模板。
	拦截详情	用户可对特权启动参数进行勾选，默认选择全部。系统将特权参数类型分为5大类，基础权限、文件操作权限、系统操作、网络操作和高危权限。用户可对大类，或某种大类中的具体分类进行调整。

策略生效范围	生效方式	配置特权镜像拦截策略时，生效方式包括“选中的镜像不允许以特权模式运行”，或“仅选中的镜像允许以特权模式运行（其他镜像特权启动将阻止运行）”。
	选择镜像	用户可选择全部镜像或自选镜像。

管理策略

- 查看：在镜像拦截策略页面，单击**镜像拦截策略名称**，查看拦截策略详情，
- 开启或关闭：通过开启或关闭启动状态列的按钮调整策略是否生效。
- 开启后，开始执行镜像拦截动作，或观察期开始倒计时。
- 关闭时，策略不生效。
- 编辑：单击**编辑**，对策略的名称、描述、启动状态、策略生效状态、拦截策略详情、策略生效范围进行调整；策略模板不可调整。

防护开关

最近更新时间：2025-04-03 17:33:02

开通容器安全服务后，可在 防护开关页面 对集群和静态启动容器的云主机进行容器安全服务开通的调整。

防护概况

展示容器安全服务开通详情，包括全量防护和自选资产防护两种，可根据防护需求进行切换：

- 全量防护：当前业务环境中所有集群以及静态启动容器的云主机开通容器安全服务，且后续当您的业务存在新增集群或新增静态启动容器的云主机时，将自动为您新增的资产开通容器安全服务。开通时，将默认消耗您的未使用核数，若剩余核数不足将通过弹性计费进行后付费扣费。
- 自选资产防护：即选择部分集群或静态启动容器的云主机开通容器安全服务，非全量开通。

字段名称	说明
已防护核数	防护开关打开且处于有效防护的集群、云主机节点资源核数。部分资产可能由于 Agent 长期离线、未安装 Docker 等原因而不算做有效防护，此部分核数将不被统计在已防护核数范围内。
资产总核数	该账号下所有运行容器的集群和云主机的总核数。
未防护核数	未开通容器安全服务的运行容器的集群和云主机的核数。
已购买核数	计费购买的核数。当需要为更多资产开启容器安全服务且已购买核数不足时，可单击**补充购买核数**，进行补充购买。
弹性计费核数	弹性计费将按照每日未防护核数平均值进行计算（每小时统计一次），此处仅为您展示截止当前的当日弹性计费核数总数。可单击**编辑**调整弹性计费核数，默认值为5000。

防护资产

展示已开通容器安全服务的集群、未开通服务的集群、全量集群资产（包括未接入控制台的集群）的数量。以及开通容器安全服务的静态启动容器的云主机、未开通容器安全服务的静态启动容器的云主机的数量。

> **说明：**
> 静态启动容器的云主机：未关联在集群资源下且运行有容器的云主机。

防护列表

可在列表中查看集群和静态启动容器的云主机开通容器安全服务的详情，或对集群和云主机的开启或关闭服务进行调整。建议在开启服务前，单击页面右上角的**同步资产**进行资产更新，以获取最新的资产详情。

集群防护

①单击**全部开启防护**，批量开启全部集群的容器安全服务。
②也可勾选多个集群，单击**关闭防护**进行批量关闭。

> **说明：**
> - 当开启的集群数量较多、超出购买核数时，多余的核数建议进行补充购买，如未及时购买，多余的核数将进行弹性计费。
> - 如超出的核数超过购买核数和弹性计费核数的上限时，将不支持继续开启集群防护的开关，建议补充购买或调高弹性计费核数再继续操作。

③如需对单个集群进行开启或关闭操作，可在防护开关列，单击**防护开关**进行调整。

字段名称	说明
集群名称/ID	已接入容器安全服务的集群的名称/ID。未接入的集群可先在 集群检查页面 完成接入后再开启服务。
集群类型	包括腾讯云托管集群、腾讯云独立集群、腾讯云 Serverless 集群、自建集群（腾讯云）、自建集群（非腾讯云）。
Master-IP	集群控制节点，用来标识集群，可使用此信息检索集群。
地域	所属地域。
包含节点数	集群内包含的节点数。
集群状态	集群运行状态，包括运行中、创建中和异常。
已防护核数/总核数	开启容器安全服务的集群处于防护中的核数，以及该集群总核数。当购买核数或弹性核数足够时，集群处于全量防护中。当购买核数或弹性核数不够时，该列会展示部分防护或未防护，即提示需要补充购买或调高弹性计费核数。
防护开关	可开启或关闭单个集群的容器安全服务。
操作	单击**查看集群风险**，可跳转集群检查页查看该集群的配置风险和漏洞风险。

云主机节点防护

①单击**全部开启防护**，批量开启全部静态启动容器的云主机的容器安全服务。
②也可勾选多个节点，单击**关闭防护**进行批量关闭。

> **说明：**
> - 当开启的云主机数量较多、超出购买核数时，多余的核数建议进行补充购买，如未及时购买，多余的核数将进行弹性计费。
> - 如超出的核数超过购买核数和弹性计费核数的上限时，将不能继续打开云主机防护的开关，建议补充购买或调高弹性计费核数再继续操作。

③如需对单个云主机进行开启或关闭操作，可在防护开关列，单击**防护开关**进行调整。

字段名称	说明
云主机名称/实例 ID	静态启动容器的云主机的名称/实例 ID。
IP 地址	静态启动容器的云主机内外网 IP。
所属项目	购买云主机时配置的所属项目信息，便于筛选。
主机来源	包括腾讯云主机和非腾讯云主机。
容器数	静态启动容器的云主机上运行的容器数。
镜像数	静态启动容器的云主机上的本地镜像数。
Agent 状态	包括在线、离线和未安装。
核数	静态启动容器的云主机的核数。
已防护核数	购买核数或弹性核数足够时，云主机处于全量防护中，已防护核数与云主机核数相同。当购买核数和弹性计费核数不够且云主机已开启容器安全服务时，已防护将小于云主机核数，建议补充购买或调高弹性计费核数再继续操作。 或者可能是由于您的主机节点上 Agent 长时间离线，处于异常情况，当前主机节点防护核数将展示为0，不进入计费。
防护开关	可开启或关闭单个云主机的容器安全服务。
操作	单击**管理资产**，可跳转主机节点列表进行安装容器安全服务和卸载 Agent 等操作。

告警设置

最近更新时间：2025-05-20 15:13:02

本文档将指导您如何为镜像安全事件和运行时安全事件配置告警策略。

前提条件

请确认消息订阅中“安全消息-安全事件通知”已打开，单击 进入设置 。

事件类型

告警设置中事件类型、默认告警时间和告警如列表所示：

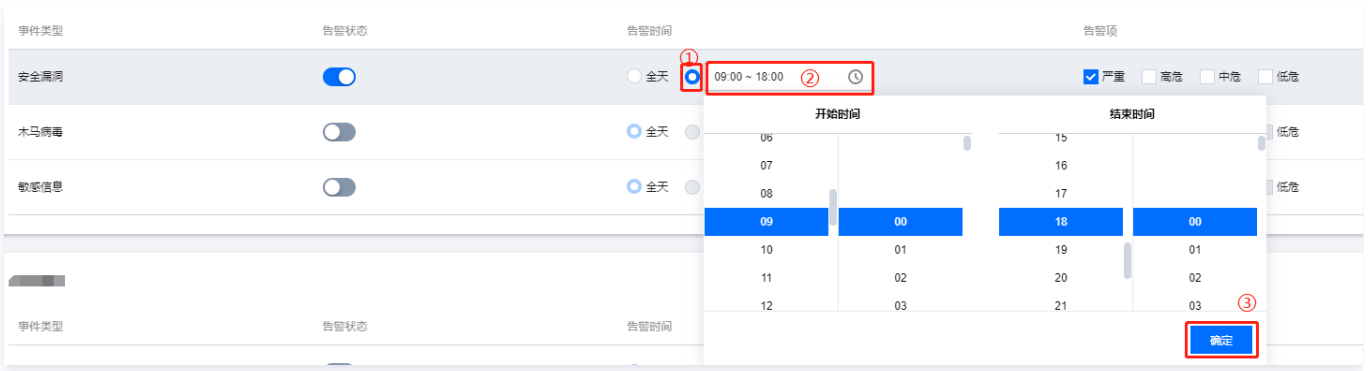
事件类型	默认告警时间	默认告警项
安全漏洞	全天	严重
木马病毒	全天	严重、高危、中危、低危
敏感信息	全天	严重、高危、中危、低危
镜像拦截	全天	拦截成功
容器逃逸	全天	-
异常进程	全天	拦截失败、告警
文件篡改	全天	拦截失败、告警
反弹 Shell	全天	-
文件查杀	全天	-
高危系统调用	全天	-
K8s API异常请求	全天	严重、高危、中危、低危
恶意外连	全天	-
容器安全K8s资源异常	全天	-
日志分析存储	全天	当日志存储量达到100%触发日志存储告警

操作步骤

1. 登录 容器安全服务控制台 ，在左侧导航中，单击**告警设置**。
2. 在告警设置页面，单击开启“告警状态”，开启告警设置模式。

3. 开启告警设置模式后，告警时间可以单击 图标选择全体或自定义时间。
   - 单击全天左侧 图标，即可完成全天告警通知设置。

- 单击自定义时间框左侧 图标，按需选择开始时间和结束时间后，单击**确定**，即可完成自定义时间通知设置。



日志分析
概述

最近更新时间：2025-03-04 16:42:32

本文档将为您介绍如何使用日志分析功能，查看容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志，以及相关日志配置和日志投递操作。

背景信息

日志分析提供容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志等多维度日志，支持语句检索和查询，并提供可视化报表、统计分析和导出功能，帮助用户能够快速的查询容器相关业务日志、溯源容器安全事件，提升运营效率。

- 容器 bash 日志：提供 bash 日志审计，帮助用户溯源异常进程。
- 容器启动审计日志：提供容器启动日志审计，帮助用户记录容器启动行为。
- Kubernetes API 审计日志：帮助用户记录 k8s API 调用的日志。（此类型日志需开启集群日志审计开关后才能采集日志数据）

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》规定，日志存储时长不少于6个月，建议用户对核心资产开启日志审计功能，根据实际所需购买存储，以便采集和留存日志数据。
容器安全服务专业版提供日志采集功能，建议用户购买专业版后再购买日志存储。若已购买日志存储，但出现容量不够的情况，此时日志分析服务将会对历史日志数据进行清理，建议用户及时升级扩容。

前提条件

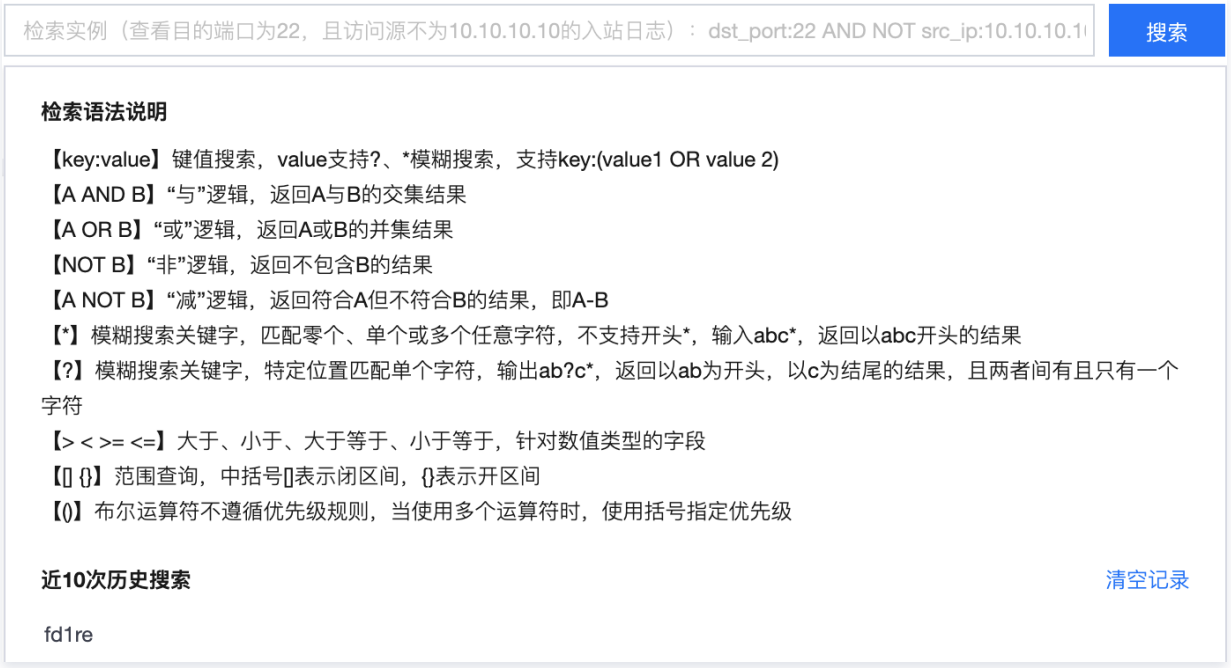
日志分析存储为容器安全服务的增值服务，需进入 容器安全服务购买页 独立购买。

查询日志

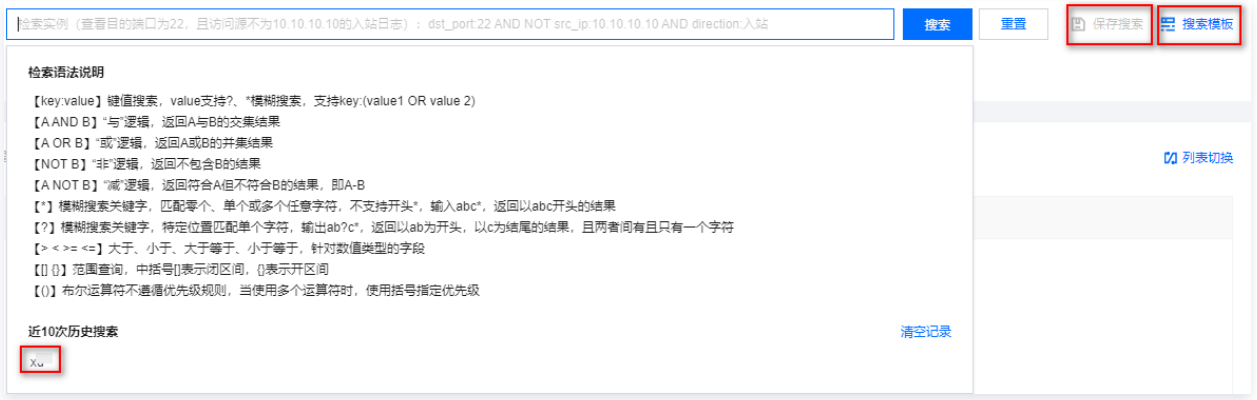
最近更新时间：2025-05-13 18:11:12

1. 登录 容器安全服务控制台，在左侧导航中，单击**安全运营 > 日志分析**。
2. 在日志分析页面，检索日志分析结果并进行相关操作。
   - 按时间类型筛选日志：在日志分析页面上方，支持按时间（近15分钟、近60分钟、近12小时、近24小时、今天、近7天、近14天、近30天、近90天及自定义日期）、日志类型筛选日志分析结果，选择需要查看的时间和日志类型，单击**确定**即可。

   - 按记录字段筛选日志：在日志分析页面上方，支持按日志记录字段筛选，提供手动输入字段、自动输入字段两种方式。
     - 手动输入字段：在输入框内以字段名和字段值成对的形式输入需要筛选的字段，单击**搜索**即可。可参考下图检索语法说明。

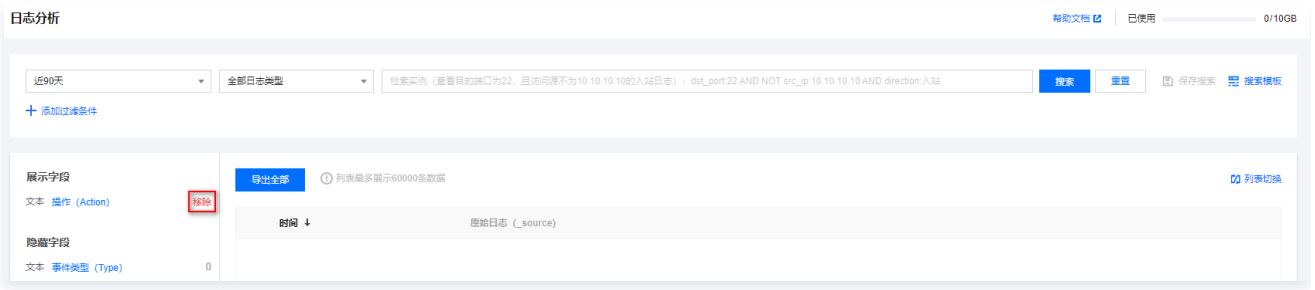


     - 自动输入字段：单击**搜索模板**，选中需要复用的查询模板名称即可。或单击筛选输入框中的**历史记录**，如上图所示。复用查询模板，需用户在手动输入查询语句时，单击**保存搜索**以达到保存当前配置（日志类型、检索语句）的目的。

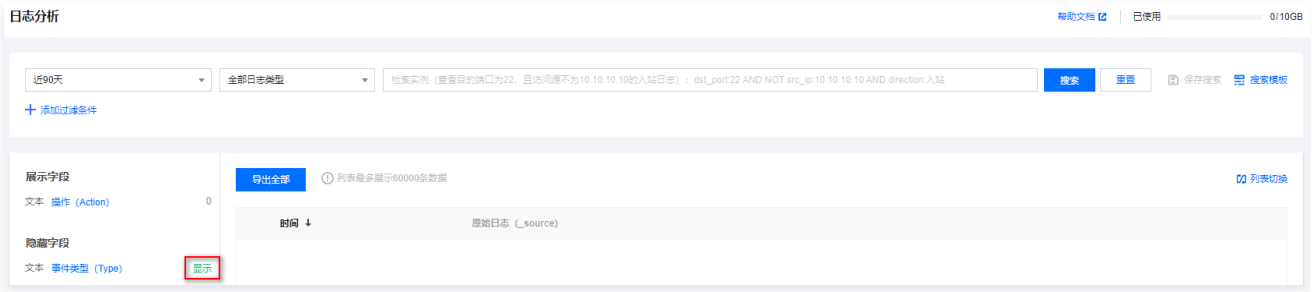


- 快速检索查看日志趋势图：
  - 方式1：为了方便对指定时间范围内的日志量进行查看，您可以滑动鼠标快速查看日志趋势图上的“蓝色柱形图”，查看日志统计时间和日志量。
  - 方式2：单击日志趋势图“蓝色柱形图”，可进一步对日志进行放大检索。

3. 在日志分析页面的日志列表中，根据“展示字段”模块内容，在列表中展示并查看相关字段详情。展示字段中为“原始日志（_source）”时，列表中展示所有日志字段。列表最多展示60000条数据。
   - 自定义需要展示或隐藏的字段：
     - 显示：将鼠标移动至隐藏字段上方，在隐藏字段右侧，单击**显示**，该隐藏字段将出现在展示字段中，列表中仅展示选定显示的字段，其他隐藏字段不展示。



     - 隐藏：将鼠标移动至展示字段上方，在展示字段右侧，单击**移出**，该隐藏字段将在展示字段中删除，对应右侧日志列表将不再展示该字段内容。



   - 导出：在字段详情左上角，单击**导出全部**，日志分析会将满足检索条件的60000条日志导出为文件，并通过浏览器下载到本地。

   - 切换表格列展示：在字段详情右上角，单击**列表切换**，可将展示字段切换为表格列展示。


展示字段
原始日志（_source）
隐藏字段
文本 容器名称（container_name） 1
文本 镜像ID（image_id） 1
导出全部
列表最多展示60000条数据
列表切换
时间
api版本（apiVersion）
日志唯一索引id（auditID）
容器ID（container_id）
容器名称（container_name）
镜像ID（image_
-
-
-

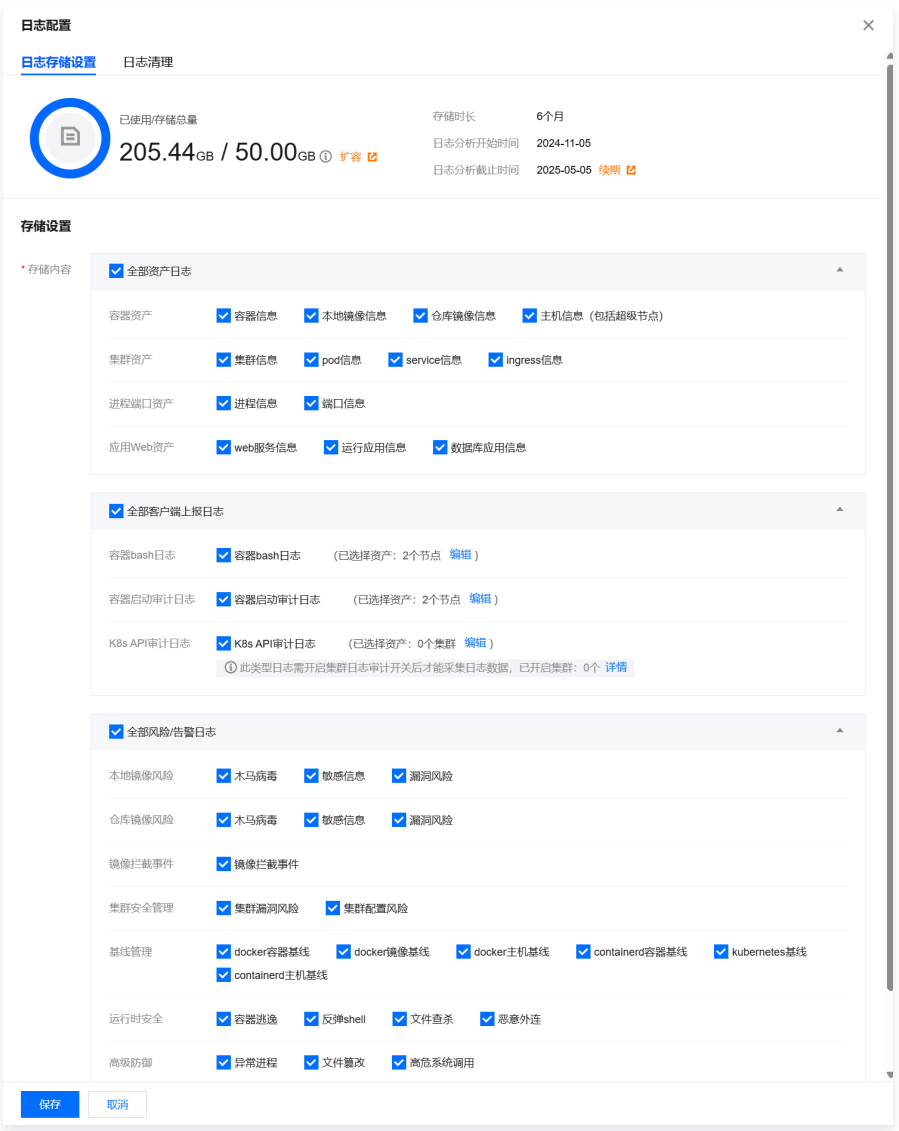
配置日志

最近更新时间：2025-04-18 17:44:02

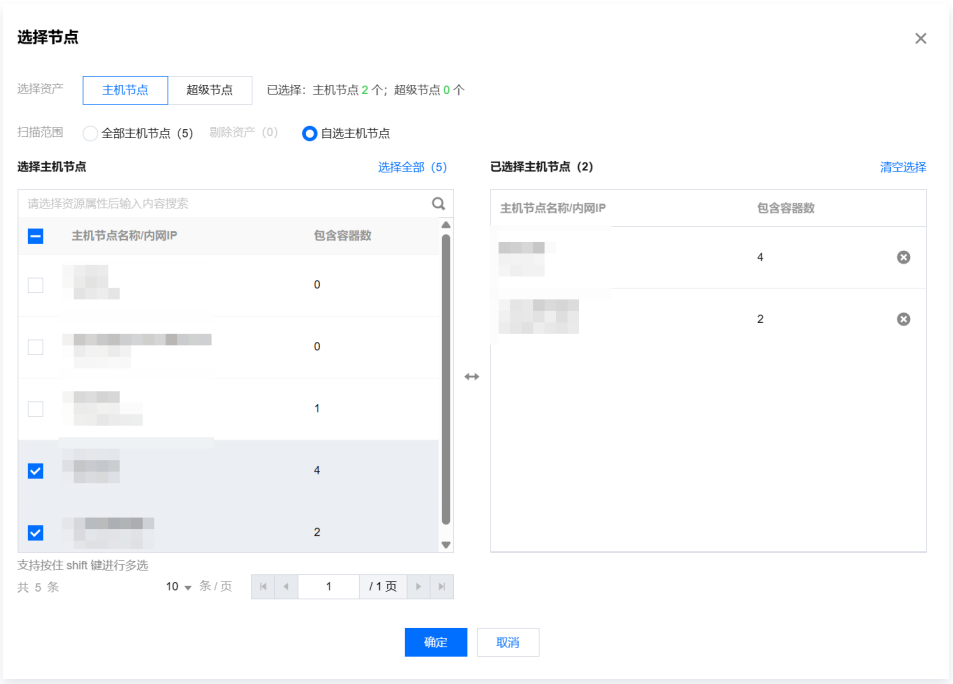
日志接入

1. 在 日志分析页面，单击页面上方的**日志配置 >日志存储设置**。

2. 在日志存储设置页面，支持对资产日志、客户端上报日志和 风险告警审计日志是否开启采集进行配置。勾选即可对该类日志进行采集。

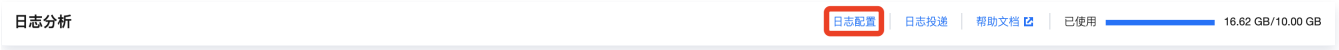


3. 在日志存储设置页面，单击客户端上报日志列的**编辑**，即可配置采集日志的节点范围。勾选需要采集日志的主机节点，单击**保存**后，配置生效。



日志清理

1. 在 日志分析页面，单击页面上方的**日志配置 > 日志清理**。



2. 在日志清理页面，支持用户按百分比或存储天数清理日志。
   - 按百分比清理日志：当日志存储量达到用户配置百分比时，开始清理历史日志，清理到用户配置的清理百分比。
   - 按存储天数清理日志：当日志存储天数达到用户配置数值时，开始清理历史日志，仅保留用户配置天数的日志。

> **说明：**
> 两种日志清理方式同时生效，当任一情况满足时即开始日志清理。

日志投递

最近更新时间：2025-05-13 18:11:12

支持将日志投递到 消息队列 CKafka 和 日志服务 CLS 平台。

投递至消息队列 kafka

1. 在 日志分析页面，单击页面上方的**日志投递 > kafka**。
2. 在 kafka 页面，单击**立即配置**。

3. 在 CKafka 投递配置页面，需授权接入，并配置地域、消息队列实例、公网域名接入、用户名和密码，单击**确定**。

> **注意：**
> - **网络接入方式默认选择公网域名接入。**
> - **投递方式可选择投递至当前腾讯云账号或** 投递至其他腾讯云账号 。

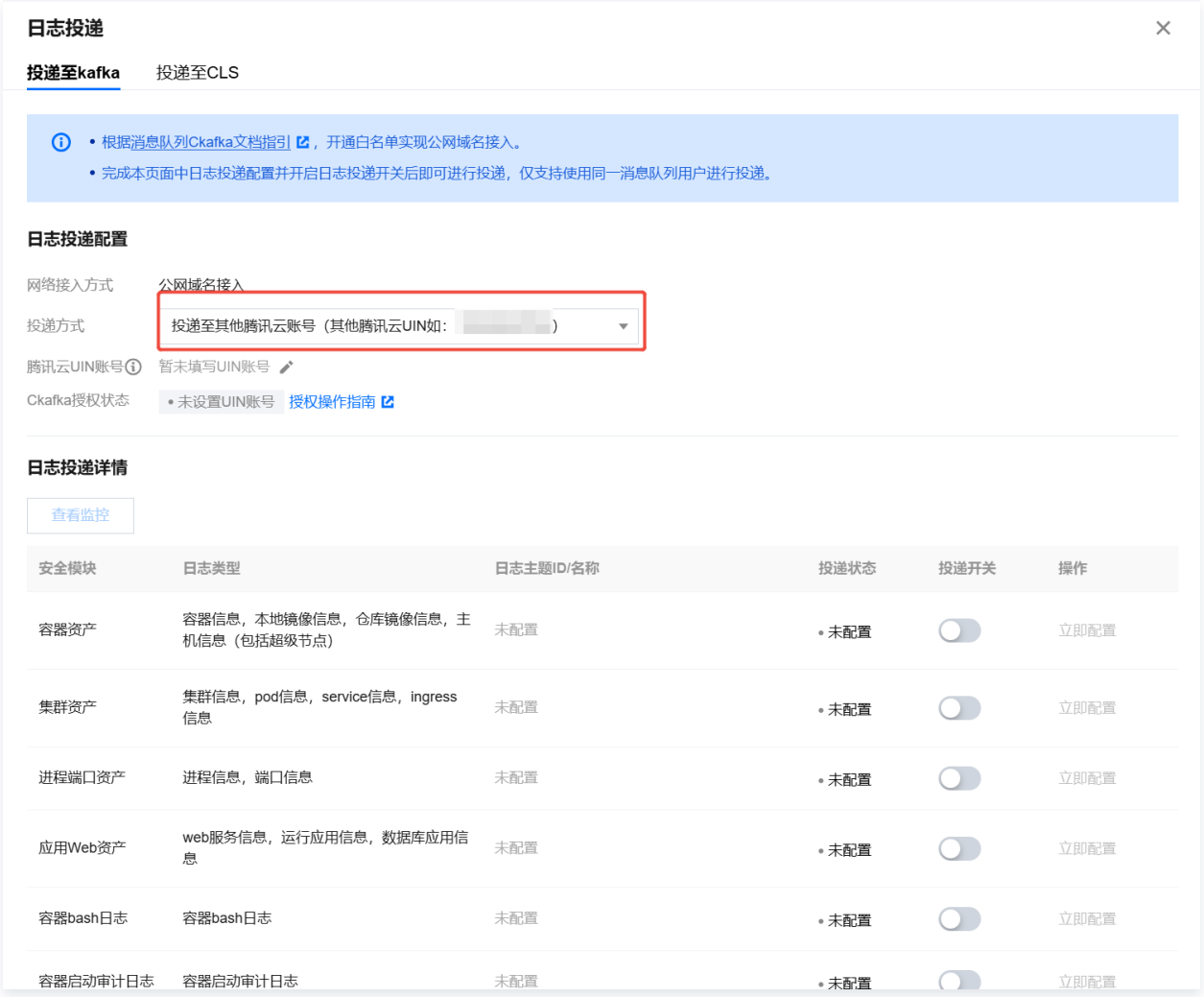
4. 配置完成，确认每一类日志是否开启投递以及投递的 Topic ID/名称。

跨账号公网域名投递日志

步骤1：选择投递方式

1. 在 日志分析页面，单击页面上方的**日志投递**，并选择 kafka 或 CLS。
2. 在 kafka 页面，选择**投递至其他腾讯云账号**，并输入接收账号的 uin。

> **注意：**
> - **接收账号在腾讯云 Ckafka 控制台 配置消息实例时，需选择**公网域名方式，并创建3个可接收容器安全服务审计日志的 topic。
> - 将该消息实例的 ID、公网域名，以及接收3类日志所需的 topic ID 和名称记录备份，牢记用户名和密码信息。跨账号授权完成后需在投递账号填写上述信息。



步骤2：配置日志跨账号投递授权

当选择跨账号投递容器安全服务（TCSS）日志时，需在接收账号上授权，允许投递账号核对接收账号的 Ckafka 消息实例、拉取Topic ID和名称等内容。

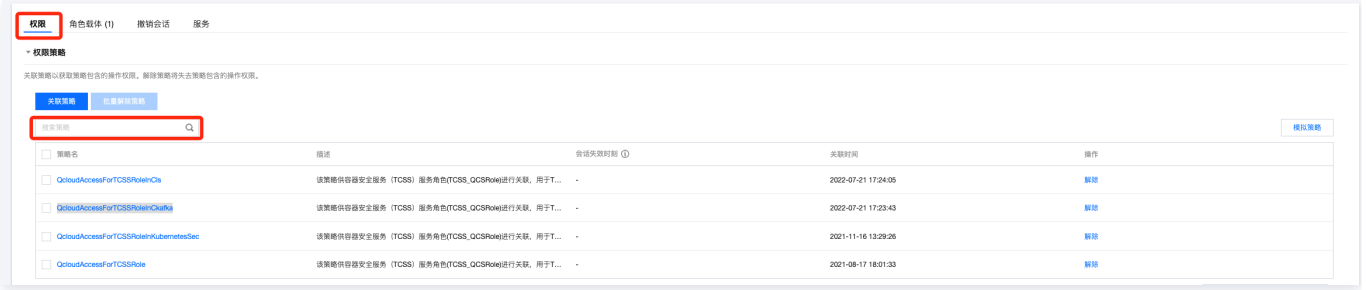
容器安全服务产品角色已存在

1. 登录 访问管理控制台，在左侧导航中，单击**角色**。
2. 在角色页面的搜索框中，输入 **TCSS**，如检索到下图中的内容，角色名称为：TCSS_QCSRole，角色载体为：产品服务 - tcss。则说明该账号已绑定过容器安全服务产品角色，在关联策略中增加访问管理（CAM）的策略权限和 Ckafka 策略权限即可。

> **注意：**
> 登录的接收账号 UIN 需与 步骤1 中输入的 UIN 保持一致。

3. 单击 **TCSS_QCSRole**，进入角色的权限页面。
4. 在权限页面，检索策略名 `QcloudAccessForTCSSRoleInCkafka` 。
   - **策略已存在**

     返回 **容器安全服务控制台** 登录投递账号，按界面提示测试跨账号策略授权是否成功，成功后配置 Ckafka 日志投递所需的公网域名、消息队列、topic 等信息。

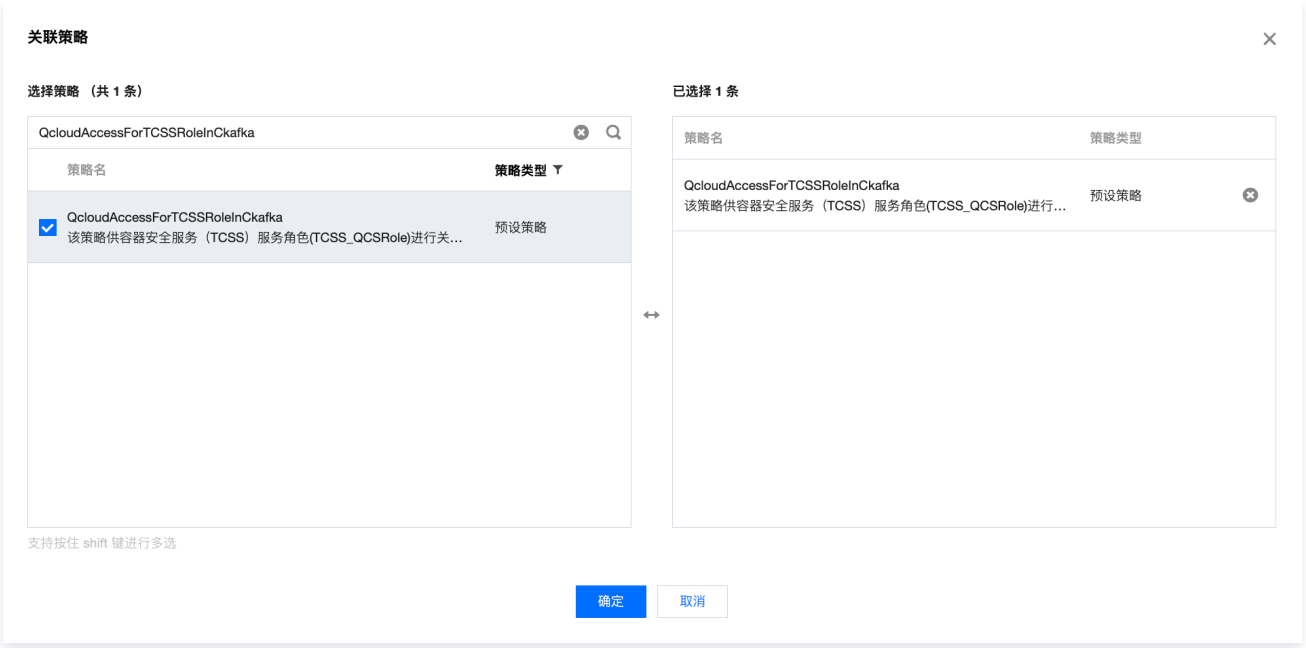
   - **策略不存在**

     a. 单击**关联策略**，经过二次确认后，进入关联策略弹窗。

     > **注意：**
     > 该角色为您授权的服务角色，擅自更改角色内容（角色关联策略或者角色载体）可能导致您授权的服务无法正确使用该角色。

     b. 在关联策略弹窗中，检索策略名 `QcloudAccessForTCSSRoleInCkafka` ，勾选策略并单击**确定**，即可在 TCSS_QCSRole 角色详情中查看到该条策略。



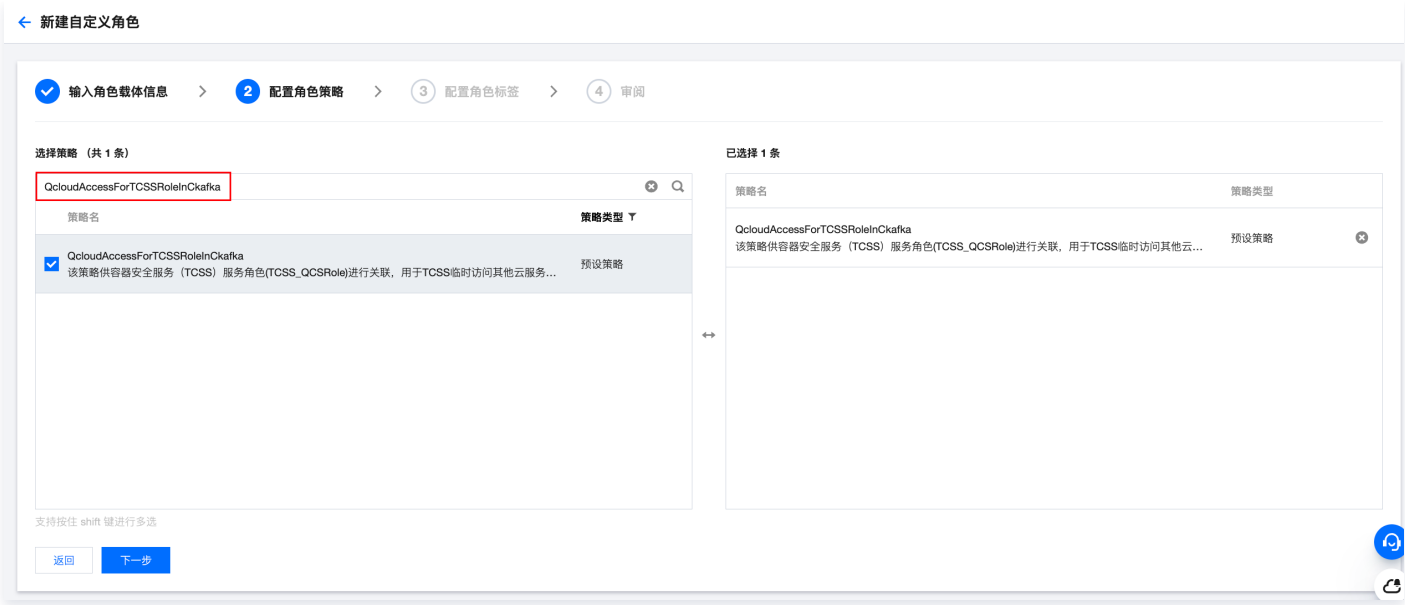
c. 配置完成后，返回 容器安全服务控制台 登录投递账号，按界面提示测试跨账号策略授权是否成功，成功后配置 Ckafka 日志投递所需的公网域名、消息队列、topic 等信息。

容器安全服务产品角色不存在

1. 在 角色页面 的搜索框中，输入 **TCSS**，如检索不到下图中角色名称为：TCSS_QCSRole、角色载体为：产品服务 - tcss 的内容，则说明该账号未绑定过容器安全服务产品的任何策略角色，需在列表中新建角色。

2. 在角色页面，单击**新建角色**，选择**腾讯云产品服务**。

3. 在输入角色载体信息中，勾选**容器安全服务 (tcss)，单击下一步**。
4. 在配置角色策略中，检索并勾选策略名 `QcloudAccessForTCSSRoleInCkafka` ，**单击下一步**。



5. 在配置角色标签中，用户可自定义或为空，单击**下一步**。
6. 在审阅中，角色名称务必配置为 `TCSS_QCSRole`，容器安全服务严格按该角色名称拉取配置权限；角色描述可用户自定义或为空。配置完成，单击**完成**，验证身份信息后即可在角色页面查看该角色和关联的策略。

7. 配置完成， 返回 容器安全服务控制台 登录投递账号，按界面提示测试跨账号策略授权是否成功，成功后配置 Ckafka 日志投递所需的公网域名、消息队列、topic 等信息。

投递至日志服务 CLS

使用日志服务 CLS 投递时，需授权接入。授权完成后，确认每一类日志是否开启投递以及投递的日志集和日志主题。

1. 在 日志分析页面，单击页面上方的**日志投递** > **CLS**。
2. 在 CLS 页面，选择需要投递的日志类型，单击**立即配置**。

3. 在投递设置页面，配置相关参数，单击**确定**。

> **说明：**
> 当您的账号授权访问日志服务 CLS 服务和开启日志投递到 CLS后，将为您自动在日志服务 CLS 服务中创建后付费的存储空间，同时也会生成后付费账单。具体计费详情请参见 购买指南 。


容器bash日志日志-投递设置
投递内容
*日志类型
容器bash日志
投递对象
*目标地域
请选择目标地域
*选择日志集
选择已有日志集
创建日志集
*日志集
请选择日志集
*选择日志主题
选择已有日志主题
创建日志主题
*日志主题
请选择日志主题（仅限当前产品平台内创建的主题）
确定
取消

混合云安装指引
概述

最近更新时间：2024-05-28 14:15:31

背景信息

随着企业上云率提升，更多中大型企业选择公有云+私有云的混合云模式，兼具公有云成本低、敏捷、灵活、使用方便及私有云可控、安全、高可用部署的优点。而混合云管理功能的上新能够支持客户接入非腾讯云机器，帮助用户更好地统一管理和监控容器安全。

功能概述

- 支持腾讯云的边缘计算机器、轻量应用服务器自动接入容器安全。
- 支持非腾讯云服务器，如：私有云、阿里云、华为云、青云、亚马逊云、UCloud 等云服务器手动接入容器安全。

客户端支持版本说明

Linux 系统支持版本：

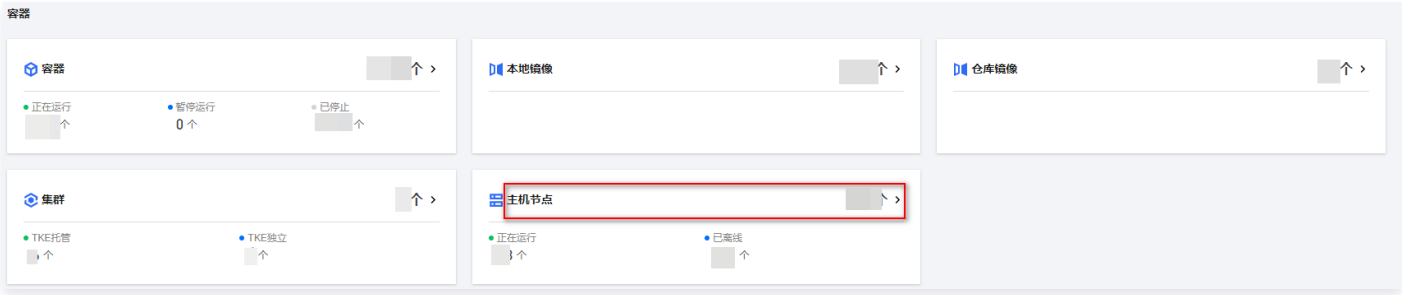
- RHEL: Versions 6 and 7(64 bit)。
- Ubuntu: 9.10 – 18.04(64 bit)。
- Debian: 6, 7, 8, 9(64 bit)。
- CentOS: Versions 6 (64 bit)及以上。

配置非腾讯云机器

最近更新时间：2025-05-13 18:11:12

步骤1：安装容器安全服务客户端

1. 登录 容器安全服务控制台，在左侧导航中单击**资产管理**，进入资产管理页面。
2. 在资产管理页面，单击容器的**主机节点** > **安装容器安全**，在右侧弹窗中查看安装指引详情。



3. 在安装指引中选择服务器类型、服务器产品及推荐安装方式。如果是通过专线打通云上云外的话，选择专线安装方式，否则选择公网直连或公网代理的安装方式。
   - 通过公网直连接入：单击图标复制并执行相应命令，即可安装容器安全服务客户端，**需注意命令有效期**。

   - 通过公网代理接入：选择代理接入方式，按页面提示生成安装命令。单击图标复制并执行相应命令，即可安装容器安全客户端，**需注意命令有效期**。
     - 单台 Nginx 代理：需在 nginx1 服务器上执行命令，并输入 `proxy_ip`（即 nginx1 服务器的内网 IP）后，生成安装命令。

- VIP 高可用集群：

  在搭建高可用集群选择 VIP+Keepalived 时，需要在 nginx1，nginx2...服务器上执行如下命令，安装 nginx 代理并申请VIP，依次输入 VIP 及nginx1，nginx2…服务器的内网 IP，输入 `proxy_ip`（即 VIP）生成客户端安装命令。

搭建高可用集群选择负载均衡时，需在 nginx1，nginx2...服务器上执行命令安装 nginx 代理，新建负载均衡实例、得到系统自动分配的 VIP，输入proxy_ip（即VIP）生成客户端安装命令。

- 通过专线接入：选择已连专线的 VPC，单击 图标复制并执行相应命令，即可安装容器安全服务客户端，**需注意命令有效期**。

> **说明**
> - 如需了解专线相关，可单击**了解专线**跳转专线接入控制台。
> - 如防火墙需开放目标 IP，参考图片对命令中 IP 开放访问权限。

步骤2：确认是否安装成功

1. 按照安装指引判断是否安装成功的命令执行，打开任务管理器确认 YDLive 进程有运行，即安装成功。

- 执行命令：`ps -ef | grep YD` 查看 YDService，YDLive 进程是否有运行。
- 进程无运行，root 用户可手动启动程序，执行命令：`/usr/local/qcloud/YunJing/YDEyes/YDService` 。

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

2. 安装成功后在 主机节点 页面，单击选择**主机来源 > 非腾讯云服务器**，即可查看对应服务器。

3. 当 Agent 状态显示为**在线**状态，即已安装成功服务已上线。

> **说明**
> 如未正常上线，请 联系我们 获得支持。

连接专线 VPC

最近更新时间：2025-05-13 18:11:12

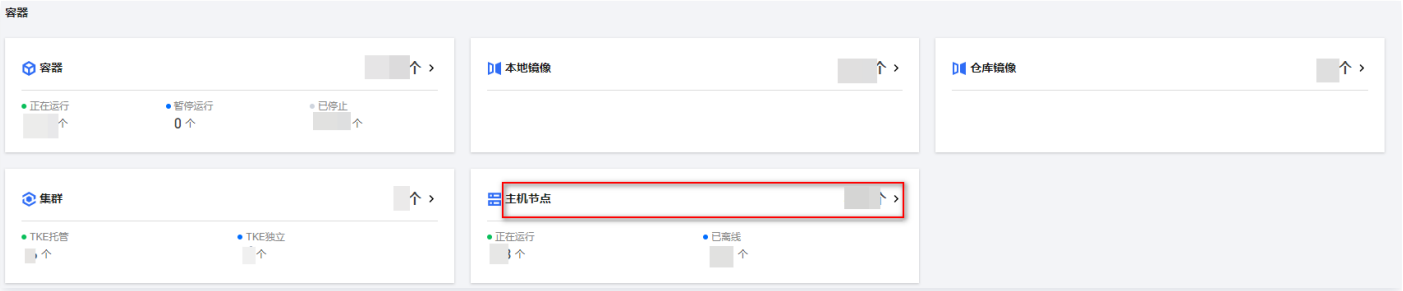
背景信息

目前 VPC 专线接入暂时只支持华南地区（广州、深圳金融）、华北地区（北京）、华东地区（上海、上海金融、南京）， 西南地区（成都），已经支持公有云与客户机房网络在 VPC 内互通，可以直接安装客户端。
若需要接入的地区不在 VPC 专线接入的范围之内，需要通过 云联网，将专线网关（VPN）与 VPC 打通。专线网关需要客户另行 购买 和搭建完成对 VPC 专线接入的工作。

操作指南

步骤1：确认是否需要通过云联网进行接入

1. 登录 容器安全服务控制台，在左侧导航中单击**资产管理**，进入资产管理页面。
2. 在资产管理页面，单击容器的**主机节点** > **安装容器安全**，在右侧弹窗中查看安装指引详情。



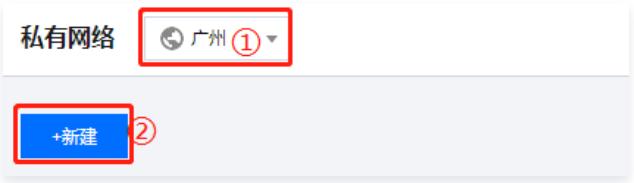
3. 在安装指引中，服务器类型单击选择**非腾讯云**，推荐安装方式单击选择**专线**。

4. 如您在华南地区（广州）、华南地区（深圳金融）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区：
   - 已有和非腾讯云机房网络互联的 VPC，则选择已连接专线的 VPC 网络，直接使用安装命令安装。
   - 没有找到相应的 VPC 网络与您的非腾讯云机房网络进行互联，可参考 步骤2 云联网。

步骤2：确认用于连接专线的私有网络

1. 如您在当前华南地区（广州）、华南地区（深圳金融）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区没有 VPC 网络，则登录 私有网络 控制台，单击**私有网络**进入私有网络页面。

2. 在私有网络页面中，单击“下拉框”选择所需区域，单击 **+新建**，弹出新建 VPC 弹窗。



3. 在新建 VPC 弹窗中，输入所需参数单击**确定**，即可完成新建 VPC。

步骤3：通过云联网实现 VPC 和已连接专线的非腾讯云机房网络互通

1. 如已存在和非腾讯云机房通信的云联网，则将 步骤2 中选择的 VPC 实例添加到云联网中。
   1.1 登录 私有网络 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
   1.2 在云联网页面，单击右侧**管理实例** > **关联实例**，进入关联实例页面。
   1.3 在关联实例页面，单击**新增实例**，将 步骤2 中选择的 VPC 实例添加到云联网中，单击**确定**即完成关联实例。

2. 如尚未配置云联网，则需要新建。
   2.1 登录 私有网络 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
   2.2 在云联网页面中，单击**新建**，弹出新建云联网实例弹窗。
   2.3 在新建云联网实例弹窗，输入所需参数单击**确定**，即可完成新建云联网实例。

> **说明：**
> - 专线网关：请选择您和非腾讯云机房通信连接的专线网关。
> - 私有网络：请选择 步骤2 中选择的 VPC 实例。
> - 如出现 IP 地址段冲突，请返回 步骤2 重新选择或新建一个不会冲突的 VPC 实例。

3. 回到 容器安全服务控制台，参考 步骤1 获取安装命令进行安装。您的非腾讯云机房需要放通对 步骤1 中描述的 IP 的5574、8080、80、9080共4个端口的访问。

热点问题

最近更新时间：2025-05-13 18:11:12

专线连接到云端，目标地址和开放端口是多少?

请参考下图的目标地址和开放端口，放通防火墙权限。

> **说明：**
> 地址和开放端口是不会变化的。

国外的 IDC 是否支持安装 Agent?

支持，目前只要机器能够联网，系统满足要求，就可以安装容器安全服务 Agent。

安装 Agent 后，控制台目前多久会展示非腾讯云机器?

目前是秒级支持。

非腾讯云机器，需要另外购买控制台吗?

不需要，统一在公有云控制台进行管理、计费。

需要开 IDC 到云上的网络端口访问权限，目标 IP 和端口是什么?

目标 IP 是安装命令内的 IP，端口5574、80、8080、9080。

内网机器，无法访问公网或者没有专线的情况下是不是无法使用主机安全?

目前是的。

混合云的客户端会和 Zabbix 进程冲突吗?

我们没有对 Zabbix 做特殊处理，也没有注入，可以关注下机器上是否有其他的客户端安装驱动。

失陷容器隔离说明

最近更新时间：2025-04-29 16:22:55

当用户业务环境中的容器遭遇攻击，例如发生容器逃逸、容器中了木马病毒或传播性较强的蠕虫病毒、容器失陷后对内发起横向探测或横向攻击、攻击者利用集群和节点等的漏洞或配置不当风险拉起恶意容器时，急需对相应的风险容器进行网络隔离。

> **说明：**
> 隔离容器网络的操作可能会影响业务正常运行，建议您排查确认为风险容器、且需要隔离来避免入侵行为进一步恶化时使用该功能。

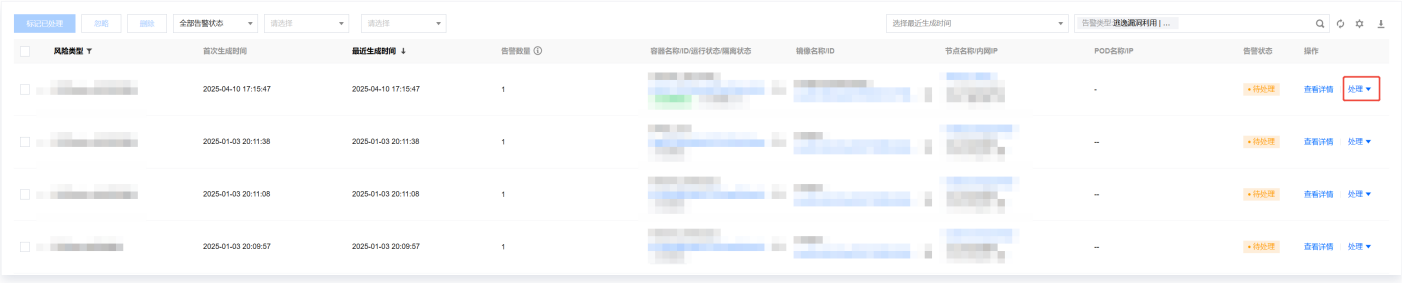
隔离容器网络

用户可在 运行时安全 、高级防御 或 资产管理 使用隔离容器网络功能。在不同模块使用该功能的效果有所不同，具体如下表所示：

模块名称	功能详情
容器逃逸	在某个安全事件处隔离容器成功后，系统将禁止该容器的网络通信，并将该安全事件标记为已处理。
反弹 Shell	
异常进程	
文件篡改	
高危系统调用	
文件查杀	由于仅隔离容器并不能清除容器木马病毒风险，所以在某个安全事件处隔离容器成功后，系统将禁止该容器的网络通信，但并不会将该安全事件标记为已处理，用户仍需对容器内的木马病毒进行自动隔离或手动隔离来更改事件状态。

运行时安全或高级防御

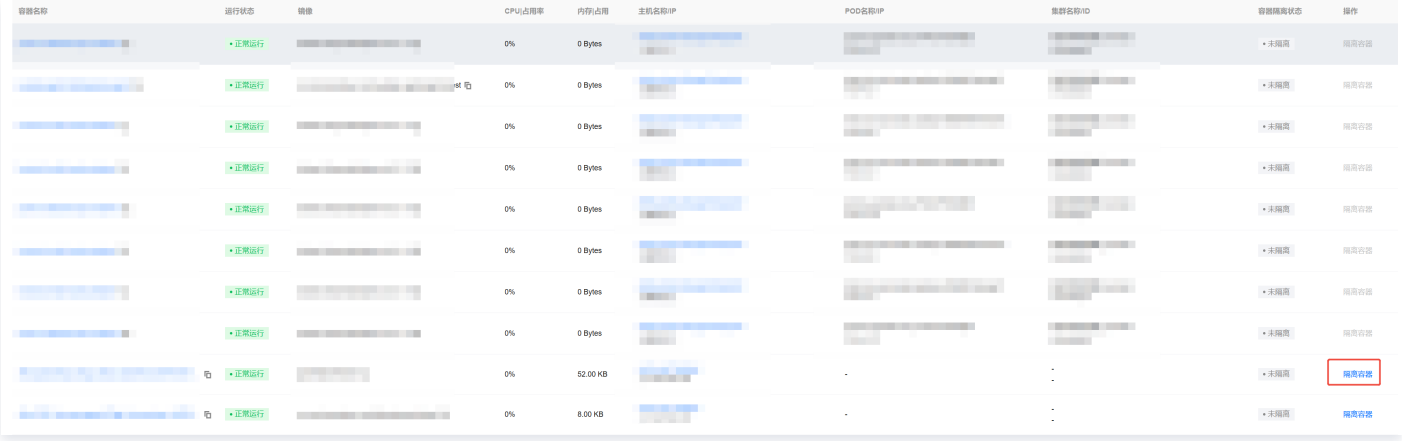
1. 登录 容器安全服务控制台 ，在左侧导航中，单击**运行时安全** > **容器逃逸**。
2. 在容器逃逸页面，选择所需容器，单击操作列的**处理**。



3. 选择**容器隔离**，并填写备注，单击**确定**。

资产管理

1. 在 资产管理页面，单击**容器**。
2. 在容器页面，选择所需容器，单击**隔离容器**。



3. 在确认隔离弹窗中，单击**确定**，即可隔离该容器。

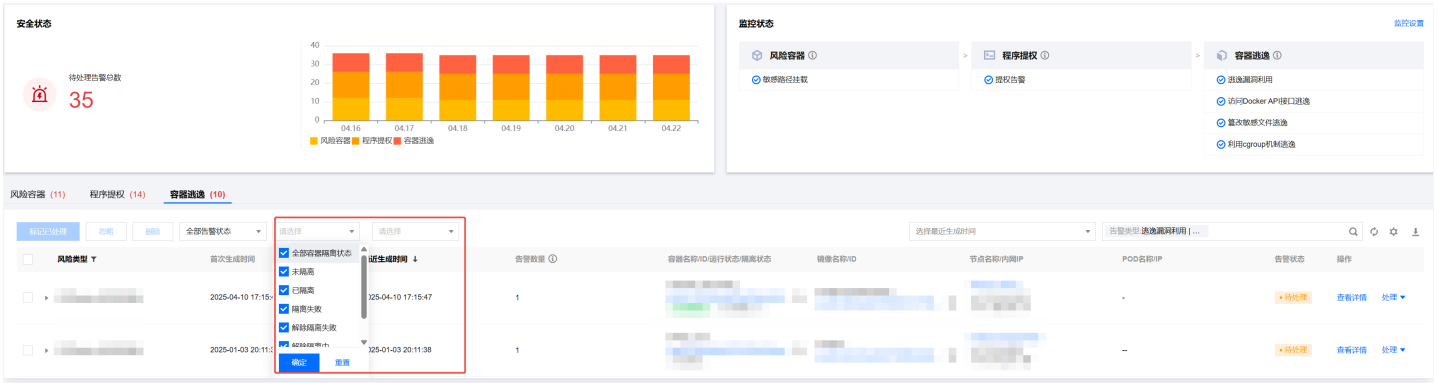
> **注意：**
> 确认后，将隔离此容器，系统将禁止该容器的网络通信，请谨慎操作。

解除容器网络隔离

当用户对容器存在的风险处理完毕、需恢复容器网络通信时，可在 运行时安全 或 高级防御 的安全事件列表中，单击**更多**，选择**解除隔离**；或者在 资产管理 > **容器**，选择所需容器，单击**解除隔离**。

查看容器隔离状态

不论在 运行时安全 、高级防御 或 资产管理 中隔离容器，容器隔离状态会作为容器资产属性之一进行刷新。例如在**运行时安全 > 容器逃逸**事件列表中对某一个容器进行网络隔离，隔离成功后，在**资产管理 > 容器**列表中查看该容器时，容器为已隔离。同理，在**资产管理 > 容器**列表中隔离容器网络，也会同步刷新运行时安全或高级防御的安全事件中的容器隔离状态。
用户可通过列表上方的全部容器隔离状态和容器运行状态筛选框，对不同隔离状态的容器事件进行筛选。



日志字段数据解析

最近更新时间：2025-05-13 18:11:12

容器 Bash 日志

名称	类型	含义
image_id	string	镜像 ID
container_id	string	容器 ID
image_name	string	镜像名称
container_name	string	容器名称
cmd	string	命令行参数


```
{
  "cmd": "exit",
  "container_id": "fcdbbfae",
  "container_name": "/reverseshell",
  "image_id": "sha256:eeb6ee3f",
  "image_name": "centos:7"
}
```


容器启动审计日志

名称	类型	含义
image_id	string	镜像 ID
container_id	string	容器 ID
image_name	string	镜像名称
container_name	string	容器名称
status	string	容器状态
id	string	容器 ID
from	string	基础镜像名称
Type	string	事件类型
Action	string	操作
scope	string	部署方式


```
{
  "Action": "exec_start",
  "container_id": "a197708a59b2809",
  "container_name": "-",
  "from": "registry.xxx.com/service/mysql@sha256:xxx",
  "id": "a197708a59b2809",
  "image_id": "-",
  "image_name": "-",
  "scope": "local",
  "status": "exec_start",
  "Type": "container"
```

```
}
```

Kubernetes API 审计日志

名称	类型	含义
image_id	string	镜像 ID
container_id	string	容器 ID
image_name	string	镜像名称
container_name	string	容器名称
clusterId	string	集群 ID
kind	string	API 事件类型
apiVersion	string	API 版本
level	string	日志等级
auditID	string	日志唯一索引 ID
stage	string	K8s API 请求状态
requestURI	string	K8s API 请求 URI
verb	string	操作类型
sourceIPs	string	请求用户 IP
userAgent	string	请求用户容器/用户对应客户端
requestReceivedTimestamp	string	请求到达 Apiserver 的时间戳
stageTimestamp	string	当前阶段处理请求的时间戳

```
{
  "apiVersion": "audit.k8s.io/v1",
  "auditID": "xxx-xxx-xxx-9d69-xxx",
  "clusterId": "-",
  "container_id": "-",
  "container_name": "-",
  "image_id": "-",
  "image_name": "-",
  "kind": "Event",
  "level": "Request",
  "requestReceivedTimestamp": "2024-01-01T13:20:48.899288Z",
  "requestURI": "/apis/batch/v1beta1/cronjobs?limit=500",
  "sourceIPs": "127.0.0.0",
  "stage": "ResponseComplete",
  "stageTimestamp": "2024-01-01T13:20:48.900236Z",
  "userAgent": "kube-controller-manager/v1.18.0 (linux/amd64) kubernetes",
  "verb": "list"
}
```