# 容器安全（TCSS）

## 产品文档



腾讯云TCE

# 目录

容器安全（TCSS） 3
- 产品简介 3
  - 产品简介 3
- 快速入门 7
  - 快速入门 7
- 产品架构 9
  - 产品架构 9
- 操作指南 11
  - 安全概览 11
  - 资产管理 14
    - 概述 14
    - 容器 15
    - 集群资产 23
    - 进程端口 29
    - 应用Web资产 33
  - 漏洞管理 39
    - 漏洞检测 39
  - 镜像风险管理 44
    - 概述 44
    - 本地镜像 46
    - 仓库镜像 52
    - 镜像拦截事件 60
  - 集群安全管理 62
    - 集群检查 62
    - 自建集群 69
    - 风险分析 85
  - 基线管理 86
    - 概述 86
    - 容器 87
    - 镜像 93
    - Docker主机 99
    - Kubernetes 105
  - 运行时安全 111
    - 概述 111
    - 容器逃逸 112
    - 反弹shell 122
      - 事件列表 122
      - 配置白名单 126
    - 文件查杀 130
    - 恶意外连 140
  - 高级防御 147
    - 概述 147
    - 异常进程 148
      - 事件列表 148
      - 规则配置 154
    - 文件篡改 159
      - 事件列表 159
      - 规则配置 165
    - 高危系统调用 172
      - 事件列表 172
      - 白名单管理 177
    - K8s API异常请求 181
  - 策略管理 191
    - 镜像拦截策略 191
  - 告警设置 197
  - 混合云安装指引 199
    - 概述 199
    - 配置Overlay云服务商机器 200
    - 热点问题 203
  - 失陷容器隔离说明 204
- 最佳实践 207
  - 容器安全等保测评解读 207
  - 镜像漏洞扫描和漏洞管理 208
- 常见问题 213
  - 常见问题 213

# 产品简介
产品简介

## 概述

容器安全服务（Container Security Service, TCSS）提供容器资产管理、镜像安全、运行时入侵检测、安全基线等安全服务，保障容器从镜像生成、存储到运行时的全生命周期，帮助企业构建容器安全防护体系。
容器安全服务提供多项安全特性，包含：资产管理、镜像安全、运行时安全、基线合规、低资源占用特性。资产管理，提供自动化资产清点，包括容器、镜像、镜像仓库、主机等关键资产信息，帮助企业实现资产可视化。镜像安全，针对镜像、镜像仓库提供一键检测，支持漏洞、木马病毒、可信镜像等多维度安全扫描。运行时安全，自适应识别黑客攻击，实时监控和防护容器运行时安全，提供入侵检测、容器逃逸、进程黑白名单、文件访问控制等安全功能。基线合规，基于 CIS Benchmark 的 Docker、Kubernetes 最佳安全实践，提供一键检测和专业修复方案。低资源占用，一键部署轻量级 Agent，高性能，低占用 CPU/内存，兼容多个主流操作系统。

## 版本介绍

容器安全服务主要功能版本介绍：

| 分类 | 类别 | | 详细描述 |
| --- | --- | --- | --- |
| 安全概览 | 安全概览 | | 以可视化的图形、图表等方式展示资产信息（容器、镜像、主机）、漏洞风险、集群风险、待处理安全事件数量、运行时安全事件新增趋势、本地镜像新增风险趋势及详情 |
| 资产中心 | 资产管理 | | 支持自动化统计容器、镜像、主机、进程端口、应用 Web 资产、运行应用、数据库应用等资产基本信息。 |
| 安全加固 | 漏洞管理 | | 漏洞管理模块支持对容器环境中的镜像漏洞开展一键检测，为漏洞应急响应及漏洞运营场景提供更好体验。根据实际处理及漏洞响应类型，将漏洞划分为两类，分别是：应急漏洞、系统漏洞、Web应用漏洞。<br>（1）应急漏洞：支持按威胁等级、风险情况、是否可修复、风险标签、CVE 编号、影响镜像名称/ID、漏洞组件名称和版本号筛选漏洞；扫描后，支持展示应急漏洞的披露时间、最新检测时间、影响本地镜像、影响仓库镜像和影响容器等。<br>（2）系统漏洞& Web 应用漏洞：支持按影响资产紧急度和关注紧急度快速筛选漏洞，例如仅展示影响容器的漏洞、仅展示影响最新版本的镜像、重点关注、高危及严重、远程 EXP 等。同时关联漏洞影响的本地镜像、仓库镜像、容器等资产数据。 |
| | 镜像 | 本地镜像 | 支持定时扫描、一键扫描本地镜像获取镜像资产基本信息及镜像安全风险详情，并对业务环境存在风险的镜像总数、安全漏洞、木马病毒、敏感信息进行汇总 |

| 分类 | 类别 | | 详细描述 |
| --- | --- | --- | --- |
| | 风险管理 | 仓库镜像 | 支持定时扫描、一键扫描仓库镜像获取镜像资产基本信息及镜像安全风险详情，并对业务环境存在风险的镜像仓库总数、安全漏洞、木马病毒、敏感信息进行汇总 |
| | | 镜像拦截事件 | 用户可在“策略管理-镜像拦截策略”页面配置告警和拦截策略，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 |
| | 集群风险管理 | 集群检查 | 支持自动检查、手动检查获取集群资产基本信息及其存在的配置和漏洞风险，并对业务环境中存在风险的集群及每个集群存在的风险数据进行汇总 |
| | | 风险分析 | 支持按严重、高危、中危、低危对存在风险的集群节点进行统计，并按检查项对受影响的集群数、受影响的节点数进行统计 |
| | 基线管理 | | 支持 CIS Benchmark 基线检查标准，检测 Docker 及 Kubernetes 安全基线，并对业务环境中合规容器占比、严重检查项、高危检查项、中危检查项、低危检查项进行统计；<br>基线检测结果包括基线检测项、类型、基线标准、威胁等级、检测结果、检测项详情等，检测对象包括容器、镜像、主机和 Kubernetes；<br>支持用户自定义安全基线检测周期和检测时间、配置基线忽略项 |
| 入侵防御 | 运行时安全 | 容器逃逸 | 支持实时检测容器内存在的敏感路径挂载、特权容器、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、利用 Cgroup 机制逃逸等行为，并自定义开启/关闭检测规则；<br>支持按风险容器、程序提权、容器逃逸等对告警事件进行分类，明确区分存在风险的容器和容器逃逸行为；<br>告警信息包括：逃逸事件类型、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD 名称等，同时告警详情提供事件描述、解决方案、进程信息、父进程信息、祖先进程信息等详情 |
| | | 反弹 Shell | 支持实时检测容器内存在的反弹 Shell 行为并产生告警，告警信息包括：进程名称、父进程名称、目标地址、进程路径、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID等，同时告警详情提供进程和父进程详细信息；<br>支持用户对告警事件加白处理，或按目标地址（IP、端口）、连接进程和生效镜像范围自定义新增白名单 |
| | | 文件查杀 | 支持实时检测容器运行时存在的木马病毒并产生告警，告警信息包括文件名称、文件路径、病毒名称、首次生成时间、最近生成时间、容器名称/ID、镜像名称/ID、容器状态等，同时告警详情提供恶意文件详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息；<br>支持实时监控、一键扫描和定时扫描容器内恶意文件；同时支持客户自定义开启自动隔离恶意文件开关 |

| 分类 | 类别 | | 详细描述 |
| --- | --- | --- | --- |
| | | 恶意外连 | 支持实时检测容器外连恶意域名的行为并产生告警，告警信息包括事件类型、请求域名、容器名称/容器ID/运行状态/容器隔离状态、镜像名称/ID、主机名称/IP、首次生成时间、最近生成时间、请求次数等，同时告警详情提供恶意域名详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息。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 |
| | 高级防御 | 异常进程 | 支持实时检测容器内存在的进程异常启动行为并告警通知或拦截异常进程。告警信息包括：进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等，同时告警详情提供进程和父进程详细信息；<br>异常进程系统策略至少包括代理软件、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；<br>支持用户对告警事件加白处理，或按进程路径和生效镜像范围自定义新增进程放行规则；<br>支持用户自定义新增进程检测规则，配置内容包括规则名称、进程路径、执行动作（拦截、告警、放行）和生效镜像范围 |
| | | 文件篡改 | 支持实时检测容器内存在的文件篡改行为并告警通知或拦截异常访问。告警信息包括：文件名称、进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等。同时告警详情提供进程和被篡改文件详细信息；<br>文件篡改系统策略至少包括篡改计划任务、篡改系统程序、篡改用户配置等规则；<br>支持用户对告警事件加白处理，或按进程路径、被访问文件路径和生效镜像范围自定义新增放行规则；<br>支持用户自定义新增访问控制规则，配置内容包括规则名称、进程路径、被访问文件路径、执行动作（拦截、告警、放行）和生效镜像范围 |
| | | 高危系统调用 | 支持实时检测容器内存在的高危系统调用行为并产生告警，告警信息包括：进程路径、系统调用名称、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD名称等，同时告警详情提供进程和父进程详细信息；<br>支持用户对告警事件加白处理，或按进程路径、系统调用名称和生效镜像范围自定义新增白名单 |
| | | 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。<br>系统规则：基于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异常请求行为进行全方位监测。<br>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 |

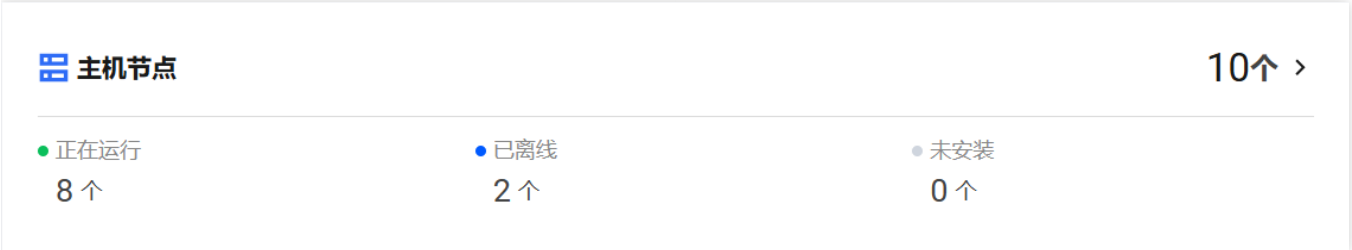
| 分类 | 类别 | 详细描述 |
| --- | --- | --- |
| 策略配置 | 策略管理 镜像拦截策略 | 用户可在“策略管理-镜像拦截策略”页面配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像 |
| 设置中心 | 告警设置 | 可点击告警状态开关开启或关闭镜像安全事件和运行时安全事件告警，镜像安全事件包含本地镜像和仓库镜像的安全漏洞、木马病毒、敏感信息事件，运行时安全事件包括容器逃逸、异常进程、文件篡改等运行时事件 |

# 快速入门
快速入门

## 前提条件

是否安装 Agent
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。
在资产管理页面，单击“主机总数”，可查看已安装容器安全服务主机列表。

> 说明：
>
> 如果不在列表中，需安装容器安全服务 Agent。可根据指引进行安装。




开通专业版和增值功能
Agent 安装完毕，确认是否开通容器安全服务专业版和增值功能。

- 开通了专业版和增值功能的用户，可享有容器安全服务带来的全面多维度的安全保障。
- 未开通专业版和增值功能的用户，可选择开通容器安全服务专业版和增值功能，开通后可查看控制台相关功能、享有容器安全服务提供的安全保障。
  Linux 适配版本
  目前支持的版本：
- RHEL：Versions 6 and 7（64 bit）
- CentOS： 6 ，7，8（64 bit）
- Ubuntu：9.10 - 18.04（64 bit）
- Debian：6，7， 8，9（64 bit）
  Agent 安装指引****下载安装 Agent
  在 Linux 系统中，输入以下指令下载安装 Agent：

> 说明：
>
> 用户可根据自身网络状态，选择其中一个下载地址即可。

- 基础网络下载地址（非 VPC 服务器）：

- wget http://u.yd.qcloud.com/ydeyesinst_linux64.tar.gz && tar -zxvf ydeyesinst_linux64.tar.gz && sh self_cloud_install_linux64.sh

- VPC 和裸金属云服务器下载：

- wget http://u.yd.tencentyun.com/ydeyesinst_linux64.tar.gz && tar -zxvf ydeyesinst_linux64.tar.gz && sh self_cloud_install_linux64.sh
  查看是否安装成功

- 执行完安装命令后查看 YDService，YDLive 进程是否有调用，有调用则安装成功。命令为：
  ps -ef|grep YD

```
[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
```

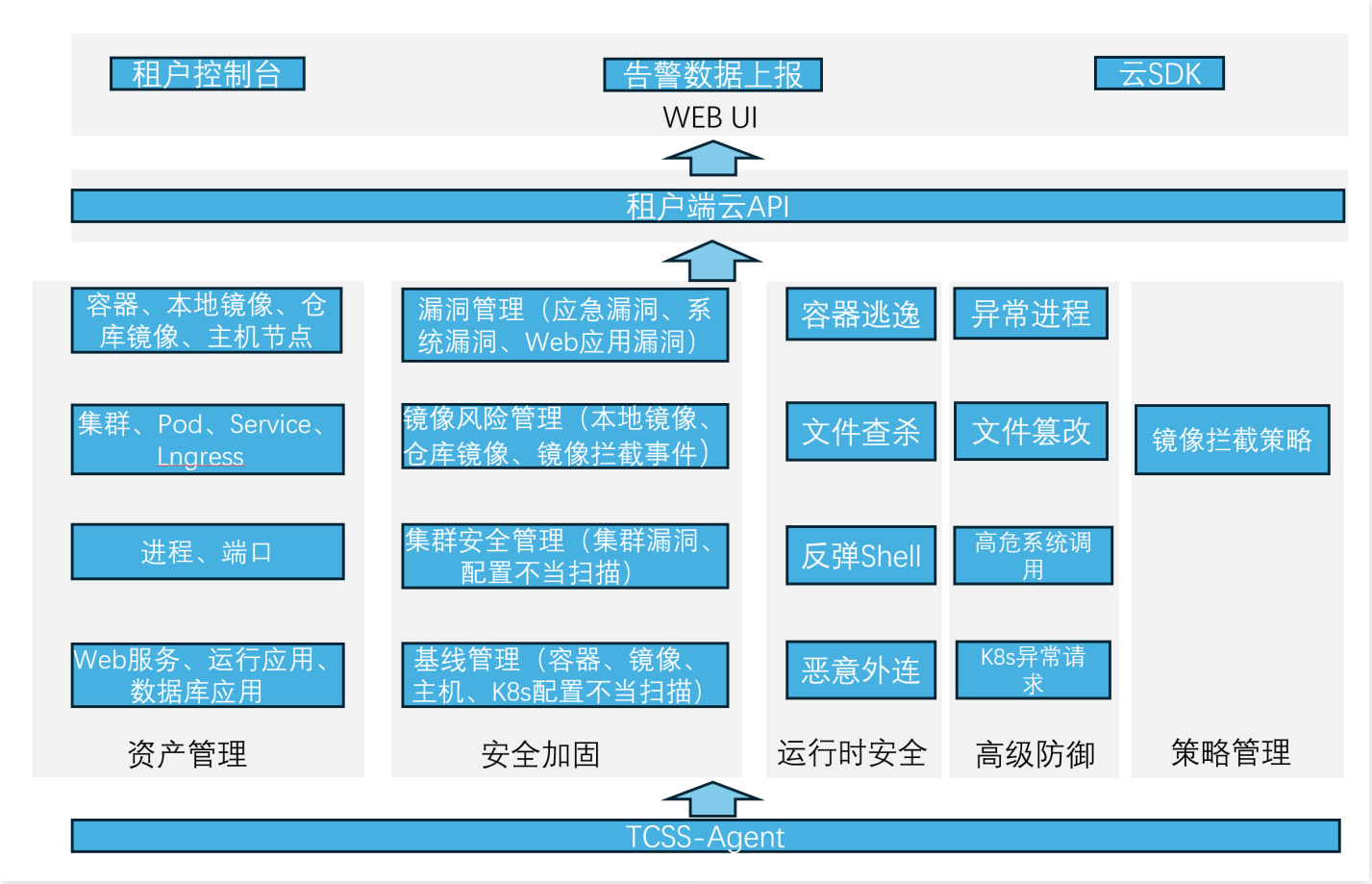
- 如果进程没有起来，可以使用 root 用户手动执行命令，启动程序。命令为： /usr/local/qcloud/YunJing/YDEyes/YDService
  卸载容器安全服务 Agent
  在Linux 系统中，输入以下命令即可卸载： /var/lib/qcloud/YunJing/uninst.sh

故障排除
若产品使用过程中，存在一些使用疑问或功能异常，可参考常见问题。

# 产品架构

# 产品架构

下图是容器安全服务的产品架构示意图。




# 容器安全服务 Agent

Agent 是一个常驻在云主机操作系统中的轻量化进程，部署在需要保护的宿主机上，主要功能是根据用户配置的安全策略上报容器运行时存在的安全风险等，本地镜像扫描、提供资产识别、镜像安全扫描、集群安全扫描、安全基线扫描、运行时入侵检测、容器网络策略配置等功能。同时响应用户和云端防护中心的指令，对容器上恶意攻击拦截进行拦截。

# 防护引擎

基于云平台的大数据处理能力，云端防护中心接收全网 Agent 上报的安全事件和威胁数据，通过云端的多个威胁识别模型，对每一条上报的安全事件进行分析，根据分析结果给 Agent 下发相关拦截和处理指令，云端防护中心是容器安全服务的中枢神经系统，相关安全威胁的识别算法依赖于云平台安全团队的运营和智能调优，云端防护中心同时保存用户自己创建的相关安全策略配置，满足用户个性化的安全防护需求。

# 云 API

提供给用户资产管理、漏洞管理、镜像安全管理、基线管理、运行时安全、容器网络策略等相关云 API 服务。

# 租户端控制台

提供给用户使用的网页版本控制台，主要功能包括安全概览、资产管理（容器、集群、进程端口、应用 Web 资产）、漏洞管理、镜像风险管理（本地镜像、仓库镜像、镜像拦截事件）、集群安全管理、基线管理、运行时安全、高级防御、策略管理（镜像拦截策略）、日志分析、告警设置等供用户操作和查看的功能，以及对应的云 SDK。

# 操作指南
# 安全概览

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

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：

- 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。
- 已购镜像授权：用户已拥有的镜像安全扫描数量。

> 说明：
>
> - 镜像授权开通后，还需用户进入镜像安全>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。

### 查看待处理安全事件

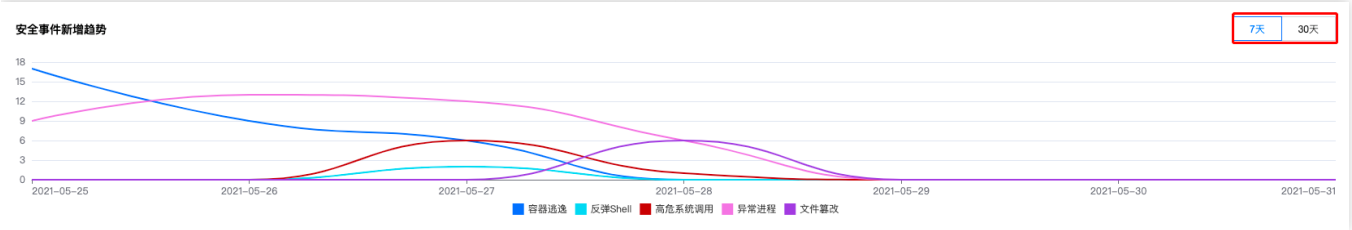
1. 在安全概览页面，待处理安全事件模块展示当前待处理的安全事件的数量。




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。

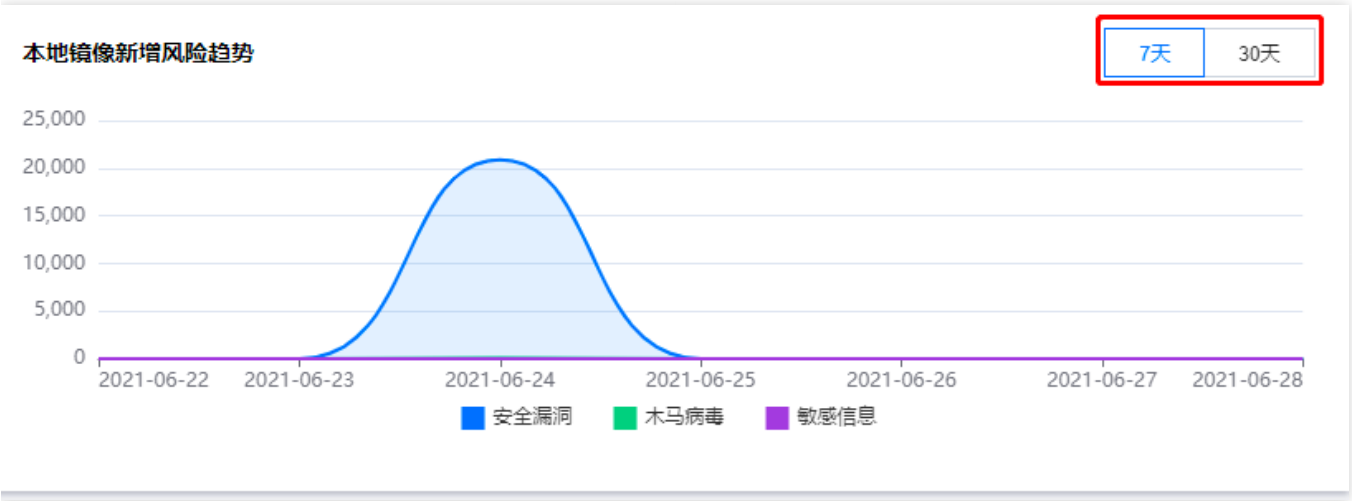
## 查看安全事件新增趋势

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。



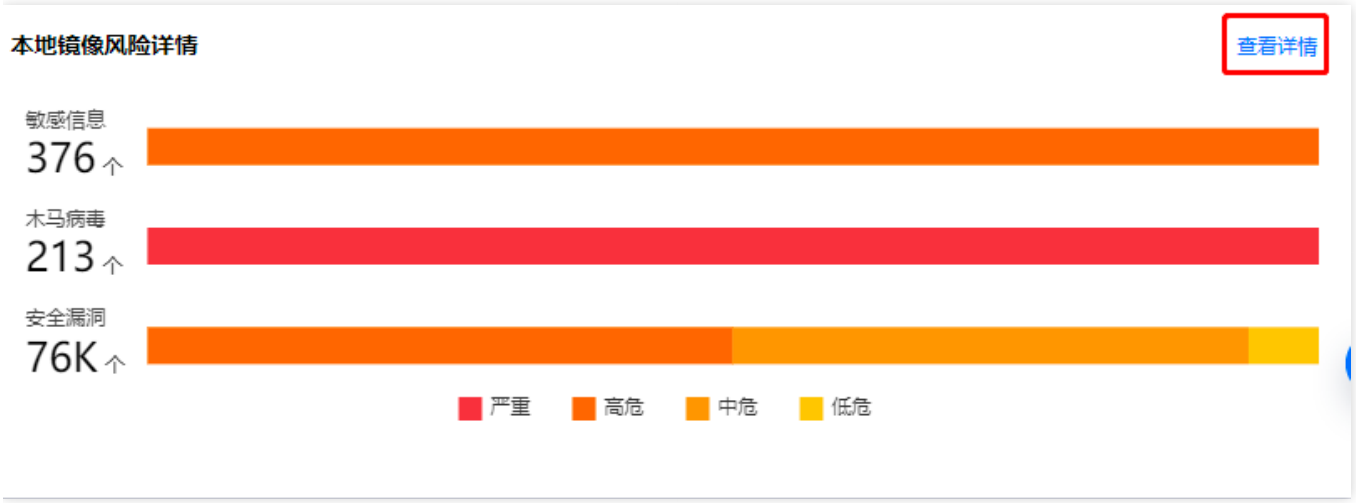

## 查看本地镜像新增风险趋势

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。


本地镜像风险详情
查看详情
敏感信息
376 个
木马病毒
213 个
安全漏洞
76K 个
严重
高危
中危
低危

# 资产管理
# 概述

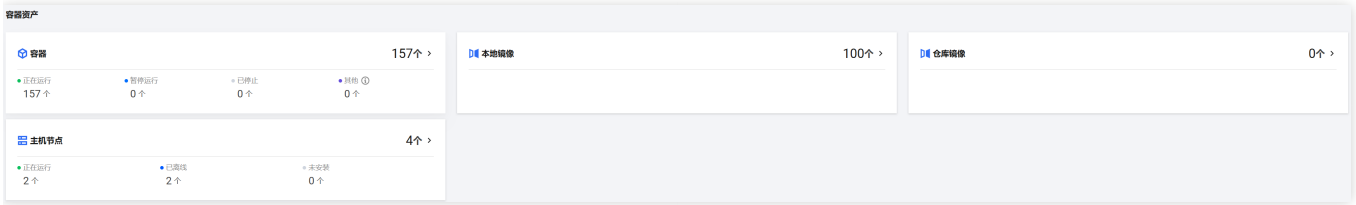
本文档为您介绍资产管理所提供的自动化资产清点功能，支持清点容器、镜像和镜像仓库等关键资产信息，帮助企业实现资产可视化。

- 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13种资产的信息：容器、本地镜像、仓库镜像、集群、主机节点、进程、端口、Web 服务、运行应用、数据库应用等。
- 目前支持识别的资产有：

| 资产类型 | 资产信息 |
| --- | --- |
| 容器资产 | 容器、本地镜像、仓库镜像、主机节点。 |
| 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

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、停止运行、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，进入资产管理页面。
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，进入资产管理页面。
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“主机名称”，右侧弹出抽屉展示主机详情，包括主机基本信息、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“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，单击设置图标，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，单击确定，即可完成设置自定义列表管理。



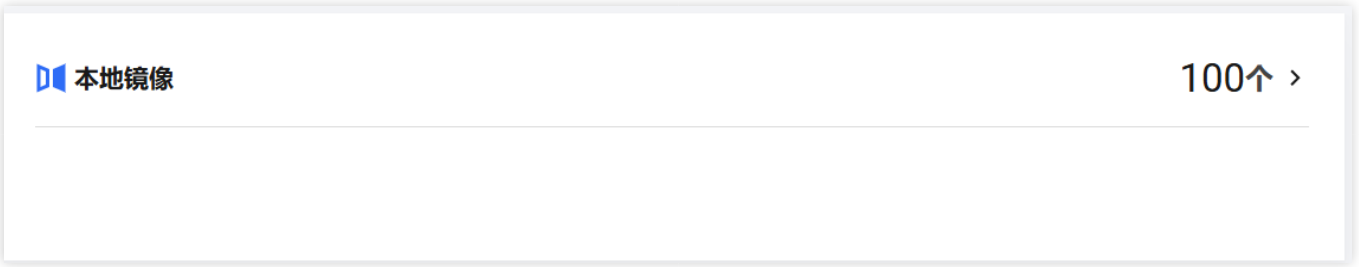

列表重点字段说明

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. POD名称/IP：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。

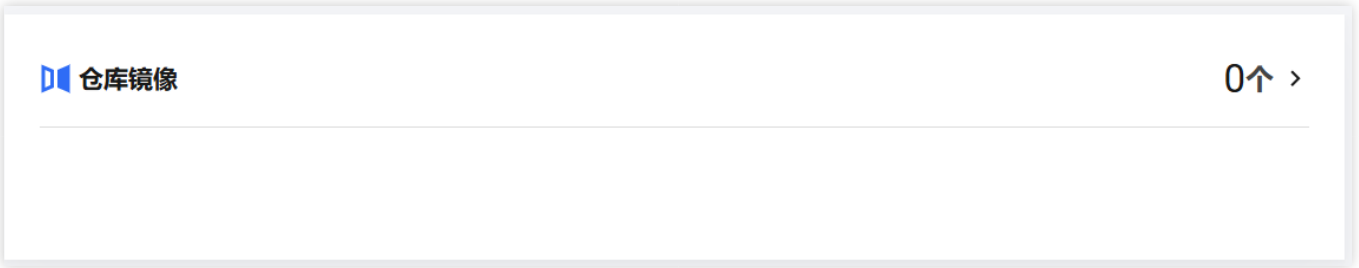
# 查看本地镜像模块

1. 登录容器安全服务控制台，在左侧导航中，单击资产管理，进入资产管理页面。
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。




# 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，进入资产管理页面。
2. 在资产管理页面，镜像仓库模块展示了仓库镜像资产总数。单击“仓库镜像总数”，可跳转镜像风险管理>仓库镜像页面查看仓库镜像详情。

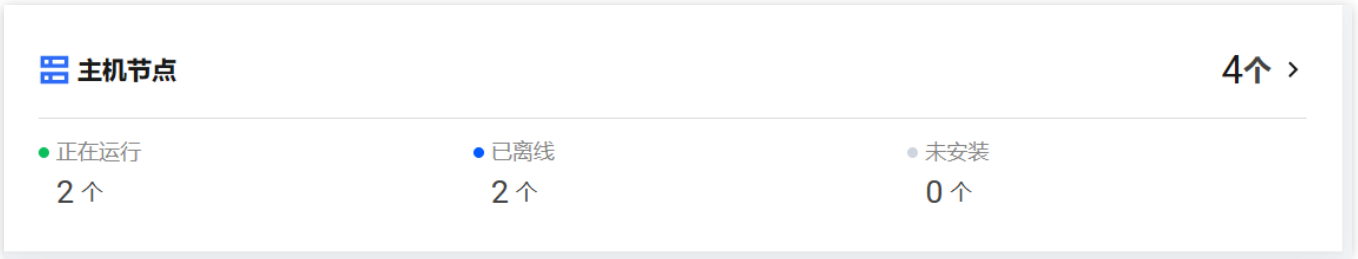



# 查看主机模块

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。

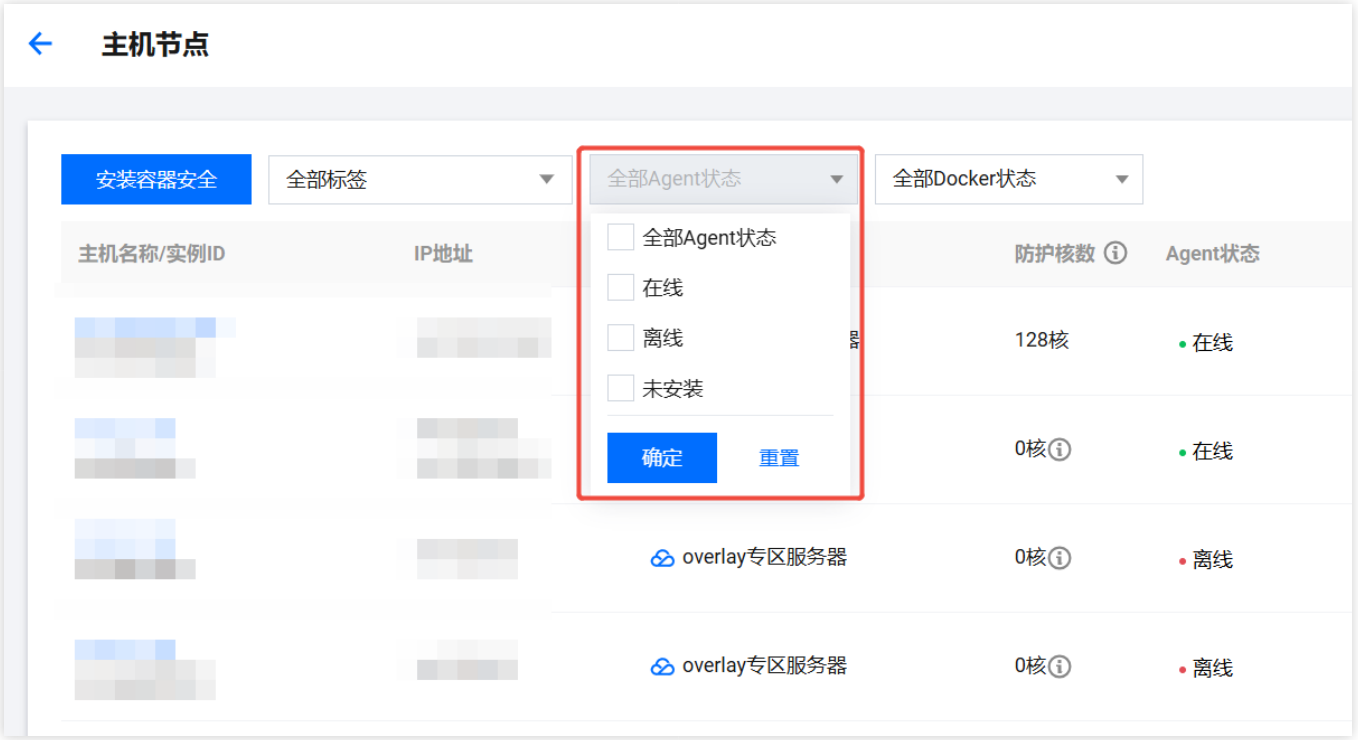
## 筛选主机列表

1. 登录容器安全服务控制台，在左侧导航中，单击资产管理，进入资产管理页面。
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。

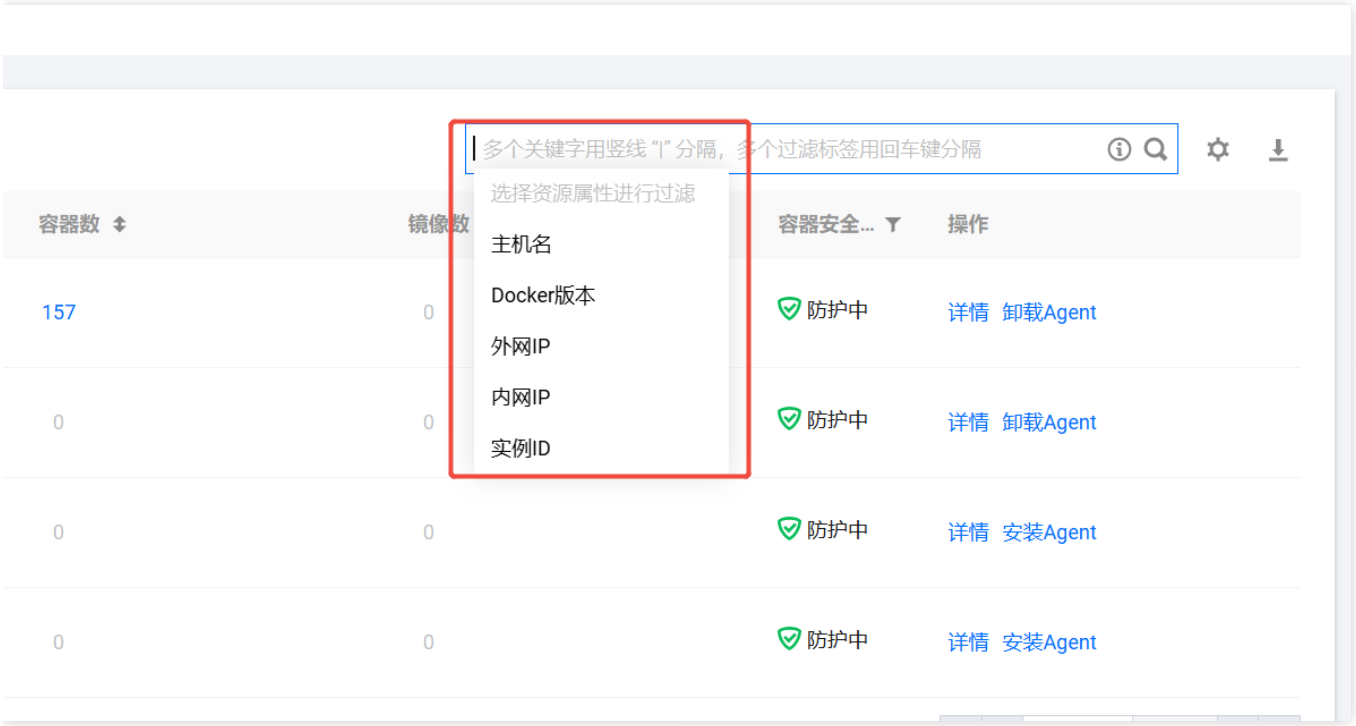



3. 在主机列表页面，可按主机状态对主机资产进行筛选，或搜索框通过"主机名、业务组、docker 版本、主机 IP"等关键字对主机进行查找。

- 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。

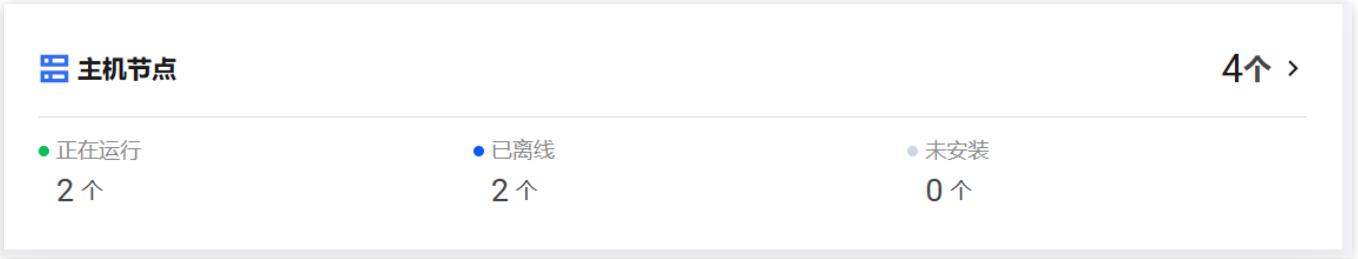



- 单击搜索框，通过"主机名、业务组、Docker 版本 、主机 IP"等关键字对主机进行查找。




## 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，进入资产管理页面。
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“主机名称”，右侧弹出抽屉展示主机详情，包括主机基本信息、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。




4. 在主机列表页面，单击“镜像数”，可查看关联镜像详情。



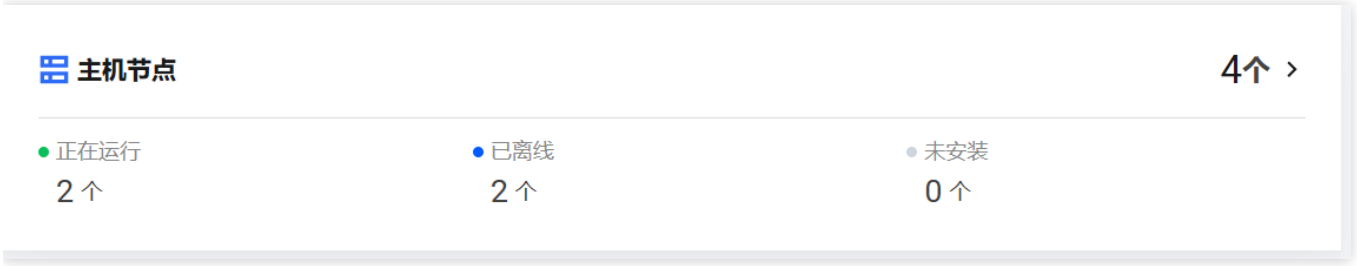

5. 在主机列表页面，单击“容器数”，可查看关联容器详情。




## 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，进入资产管理页面。

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，单击设置图标，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，单击确定，即可完成设置自定义列表管理。

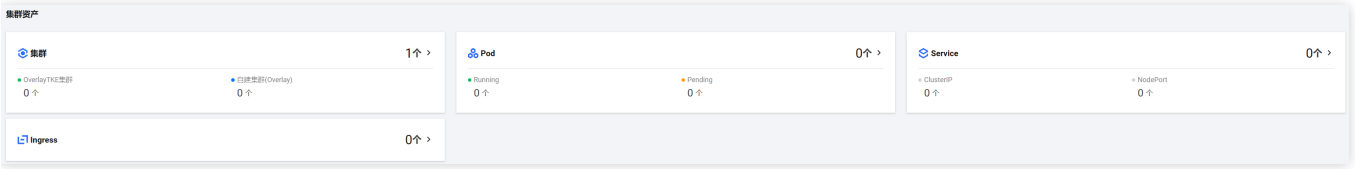



列表字段说明

1. 主机名称/实例ID：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、相关镜像数和相关容器数。
2. IP地址：主机的 IP 地址。
3. 标签：主机所标记的管理标签。
4. 主机来源：服务器所属 underlay 和 overlay 专区。
5. 防护核数：将根据您集群下已安装容器安全Agent的CVM节点/原生节点“配置”核数进行安全防护核数计算 。
6. Agent状态：在线、离线、未安装的三种状态。
7. 集群名称/ID/防护状态：标记接入所属集群或未接入状态。
8. Docker版本：展示 Docker 版本号，如未安装，则显示“未安装”。
9. Containerd版本：展示 Containerd 版本号，如未安装，则显示“未安装”。
10. 文件系统类型：展示主机的文件系统类型。
11. 镜像数：主机关联镜像数。单击“数字”可查看关联镜像详情。
12. 容器数：主机关联容器数。单击“数字”可查看关联容器详情。
13. 容器安全防护：展示容器防护状态，防护中或未防护。
14. 操作：查看主机详情的基本信息，关联容器数、关联镜像数，进行卸载Agent等操作。

# 集群资产

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。

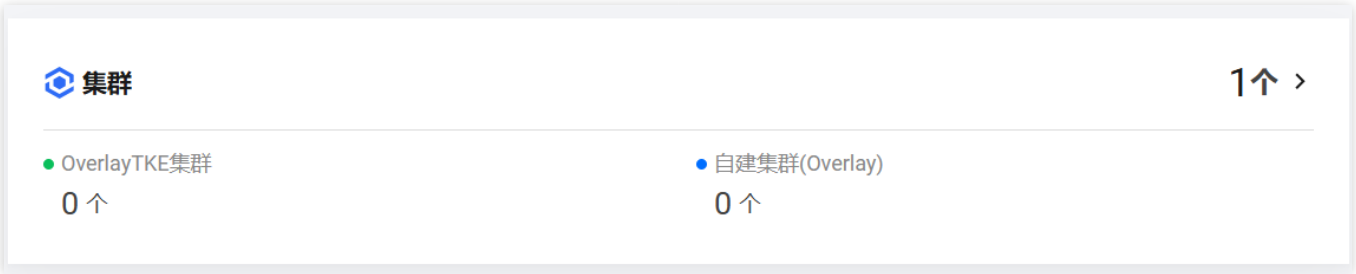



# 查看集群模块

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、集群类型、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，单击设置图标，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，单击确定，即可完成设置自定义列表。

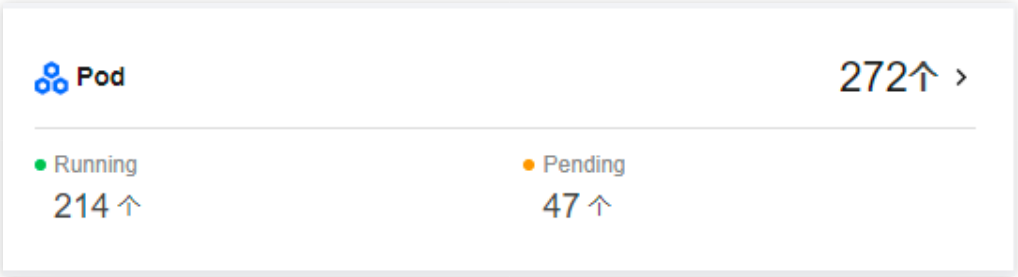



# 查看 Pod 模块

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”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，单击设置图标，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，单击确定，即可完成设置自定义列表。

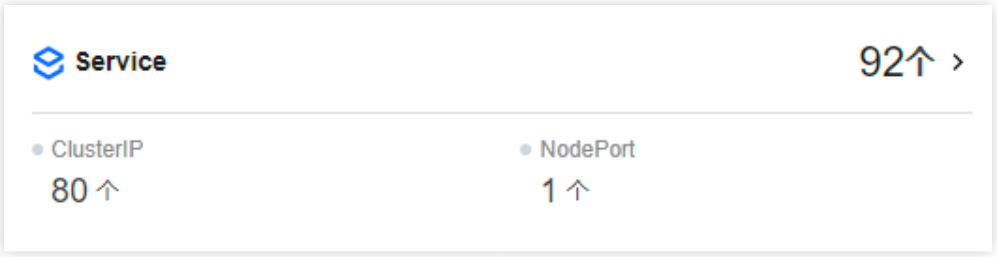


# 查看 Service 模块

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。



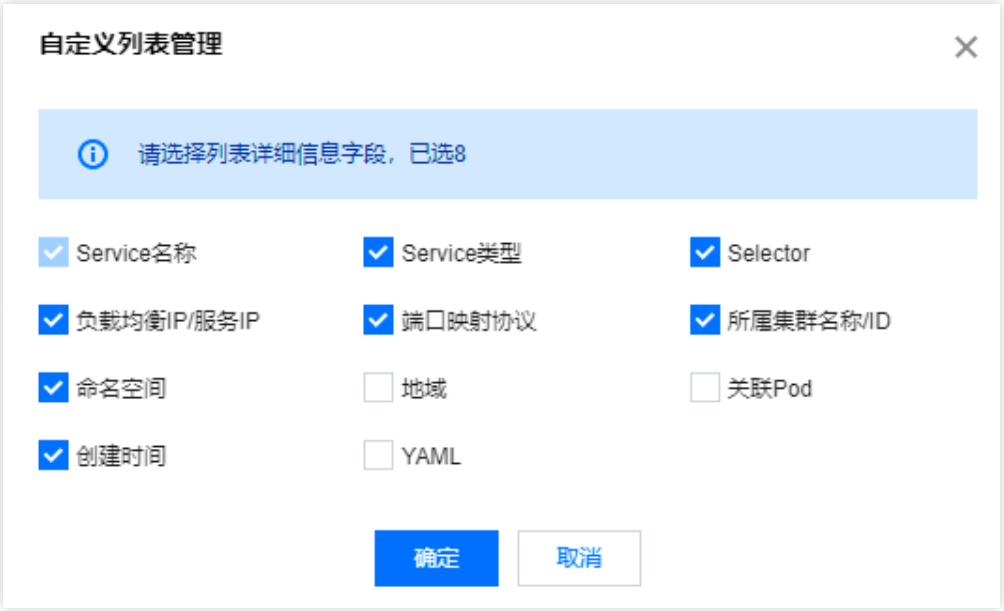

3. 找到目标 Service，单击**“Service 名称”**，右侧弹出抽屉展示该 Service 详情，页面可切换查看 Service 基本信息、Pod、YAML 和端口映射规则等信息。




## 自定义列表管理

1. 在 Service 列表页面，单击设置图标，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，单击确定，即可完成设置自定义列表。

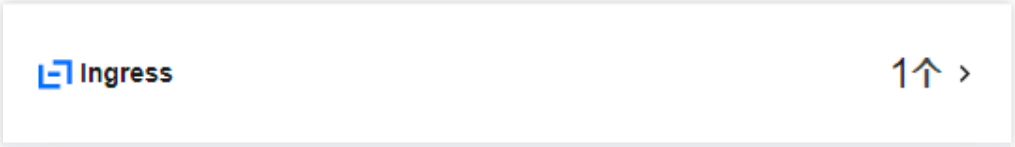



# 查看 Ingress 模块

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”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。



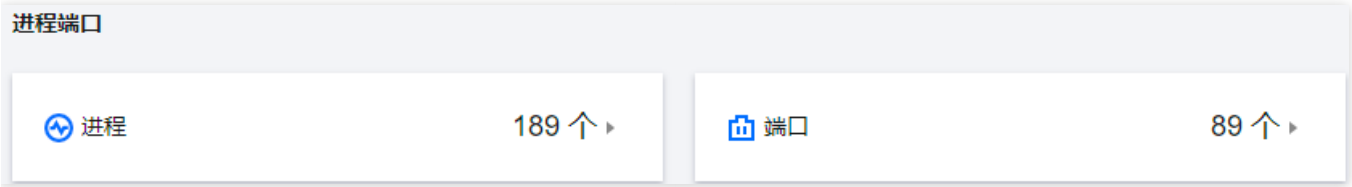

## 自定义列表管理

1. 在 Ingress 列表页面，单击设置图标，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，单击确定，即可完成设置自定义列表。



# 进程端口

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，进入资产管理页面。
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，进入资产管理页面。
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 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“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，单击设置图标，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，单击确定，即可完成设置自定义列表管理。

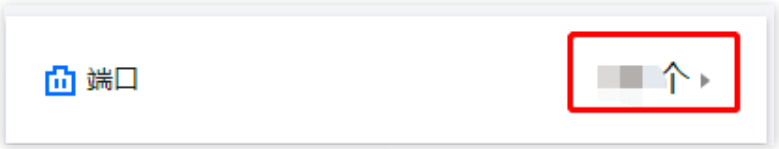



# 查看端口模块

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，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。

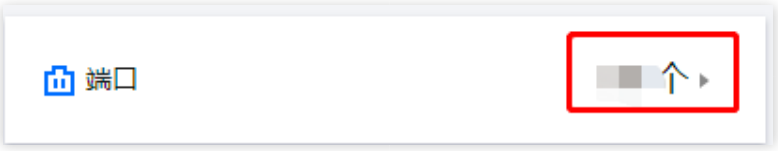



3. 在端口列表页面，单击搜索框，通过“主机 IP、进程名和宿主机端口”等关键字可对端口进行查找。




## 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，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。



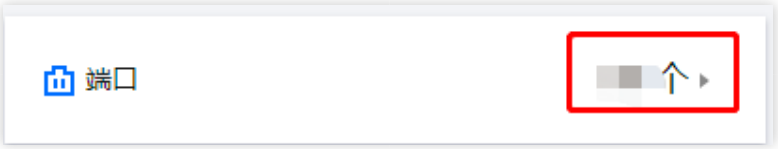

3. 在端口列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> 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。

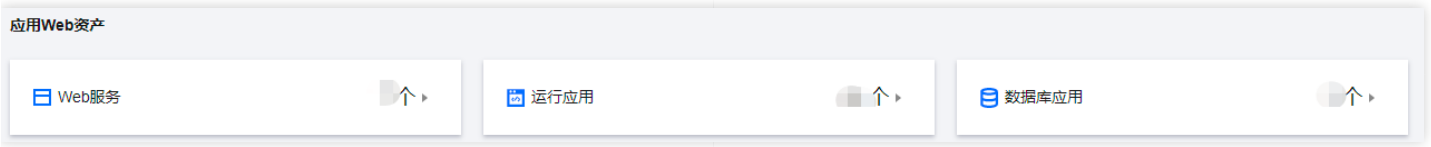



3. 在端口列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击确定，即可完成设置自定义列表管理。



# 应用Web资产

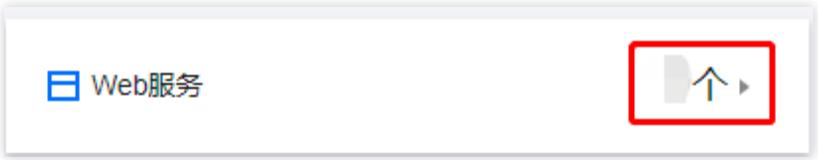
本文档为您介绍应用 Web 资产功能，以及如何查看 Web 服务、运行应用和数据库应用数量。




# 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，进入资产管理页面。
2. 在资产管理页面，单击“Web 服务总数”进入Web 服务列表页面，可查看全部进程资产列表。




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。

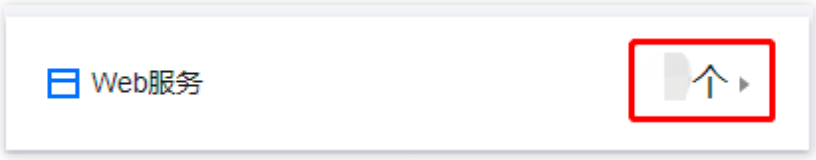



- 单击搜索框，可通过“容器名称、主机名、启动用户”等关键字对 Web 服务进行查找。



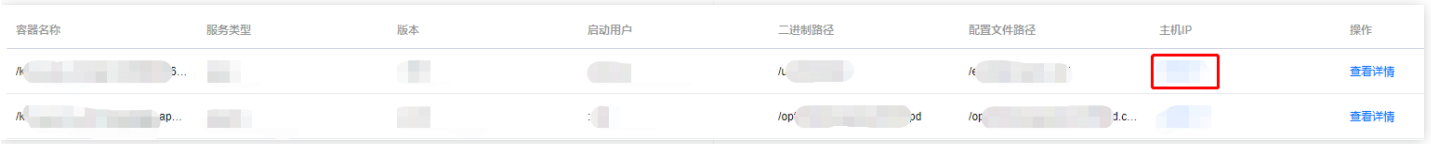

## 查看 Web 服务列表

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

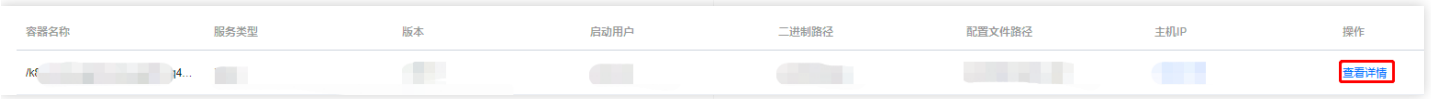



3. 在 Web 服务列表页面，单击“主机名称”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> 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。

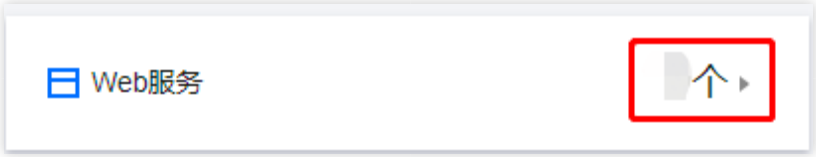



4. 在 Web 服务列表页面，单击查看详情，对话框展示 Web 应用服务详情，包括基本信息和关联进程列表。




## 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，进入资产管理页面。
2. 在资产管理页面，单击“Web 服务总数”进入Web 服务列表页面，可查看全部进程资产列表。



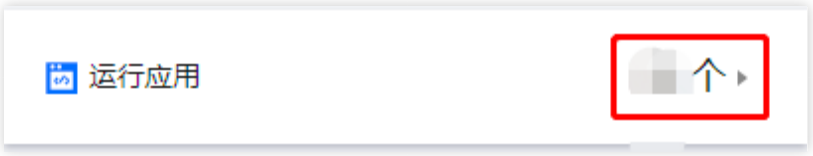

3. 在 Web 服务列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
4. 在自定义列表管理弹窗，选择所需的类型后，单击确定，即可完成设置自定义列表管理。




# 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，进入资产管理页面。
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。

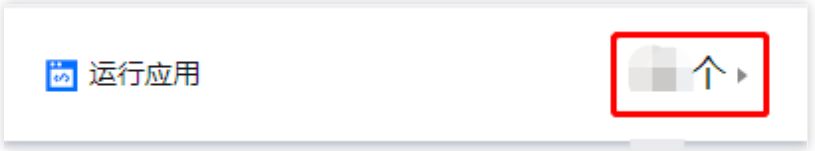



## 查看运行应用列表

1. 登录容器安全服务控制台，在左侧导航中，单击资产管理，进入资产管理页面。
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。
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。

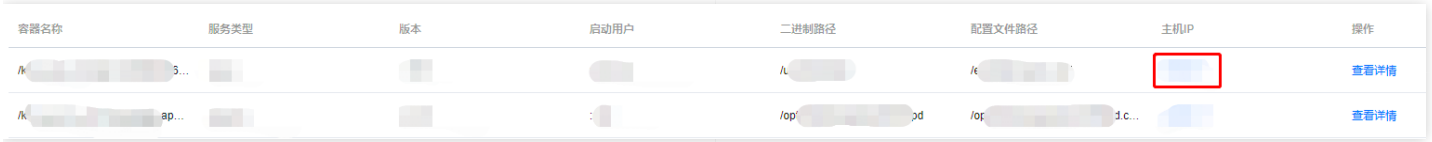
## 自定义列表管理

1. 登录容器安全服务控制台，在左侧导航中，单击资产管理，进入资产管理页面。
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。

> 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。



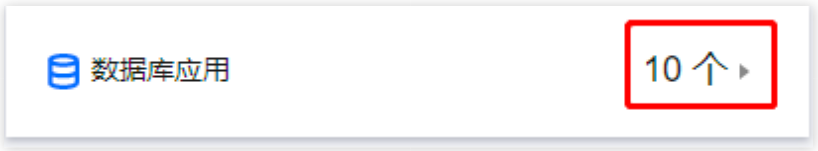

4. 在自定义列表管理弹窗，选择所需的类型后，单击确定，即可完成设置自定义列表管理。




# 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，进入资产管理页面。
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。

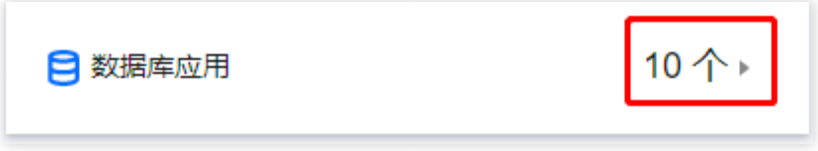



3. 在数据库应用资产列表页面，单击搜索框，通过“容器名称、主机IP和数据库类型”等关键字可对数据库应用进行查找。



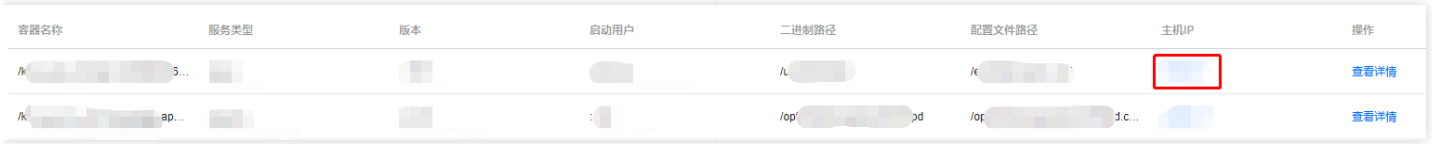

## 查看数据库应用列表

1. 登录容器安全服务控制台，在左侧导航中，单击资产管理，进入资产管理页面。
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。

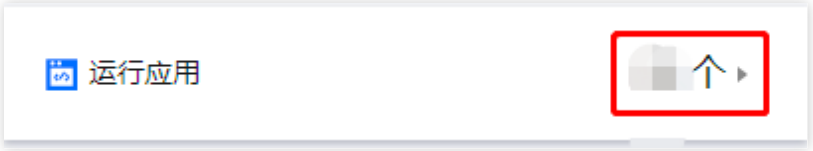



4. 在运行应用列表页面，单击查看详情，对话框展示数据库服详情，包括基本信息和关联进程列表。




## 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，进入资产管理页面。
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，单击设置图标，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，单击确定，即可完成设置自定义列表管理。



# 漏洞管理
# 漏洞检测

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。

## 前提条件

已开通容器安全服务专业版。

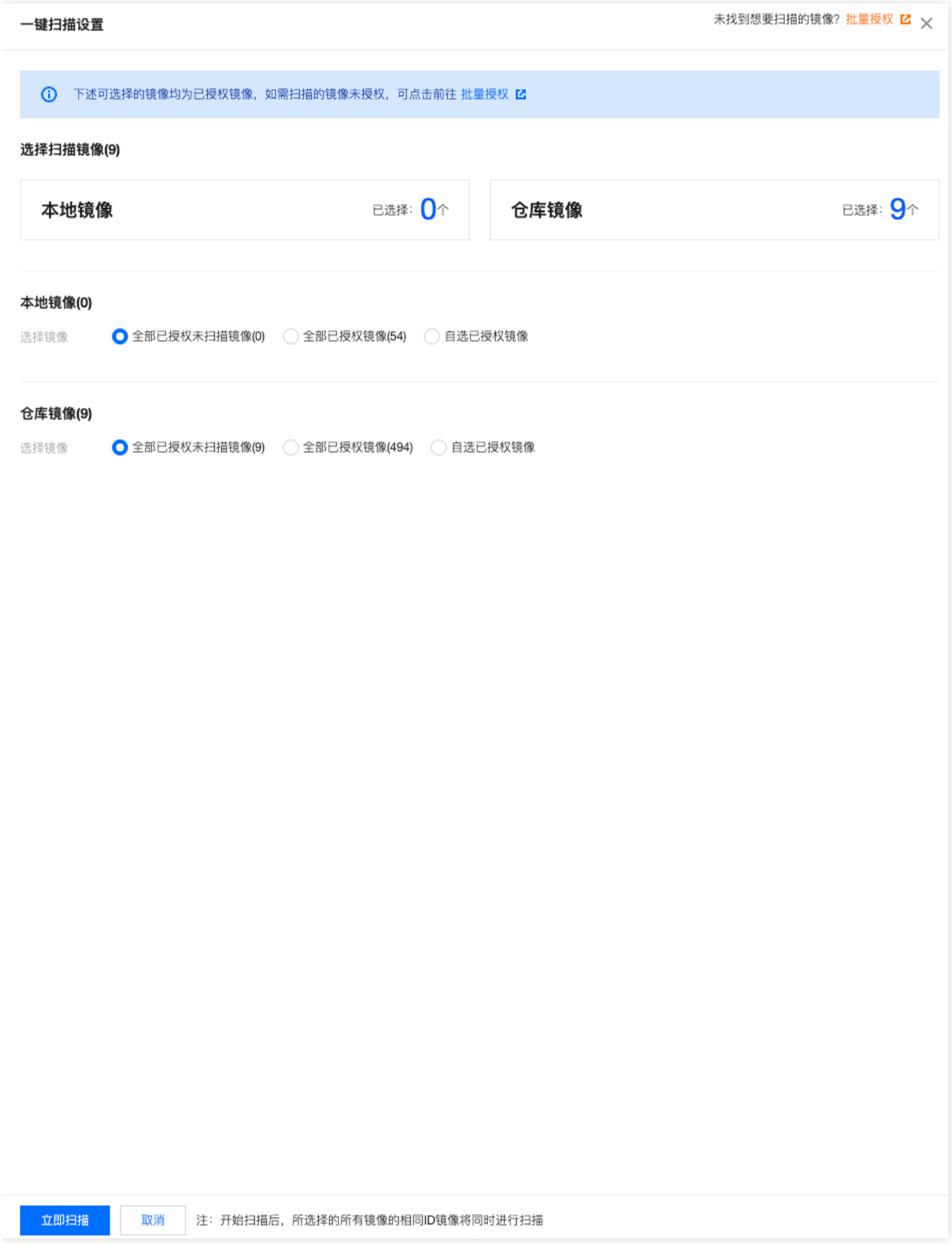
## 漏洞检测

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，单击立即检测，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。


一键扫描设置
未找到想要扫描的镜像？批量授权
下述可选择的镜像均为已授权镜像，如需扫描的镜像未授权，可点击前往 批量授权
选择扫描镜像(9)
本地镜像
已选择：0个
仓库镜像
已选择：9个
本地镜像(0)
选择镜像
全部已授权未扫描镜像(0)
全部已授权镜像(54)
自选已授权镜像
仓库镜像(9)
选择镜像
全部已授权未扫描镜像(9)
全部已授权镜像(494)
自选已授权镜像
立即扫描
取消
注：开始扫描后，所选择的所有镜像的相同ID镜像将同时进行扫描

# 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。



| 漏洞名称/标签 | 威胁等级 | CVSS | CVE编号 | 影响本地镜像 | 影响仓库镜像 | 影响容器 | 漏洞类型 | 首次发现时间 | 最近检出时间 | 操作 |
|---|---|---|---|---|---|---|---|---|---|---|
| A... | 高危 | | | 207 | 9 | 1 | 授权问题 | 2022-06-06 06:22:11 | 2022-06-07 14:53:47 | 查看详情 |
| A... | 高危 | | | 210 | 9 | 50 | 越界写入 | 2022-06-06 06:22:11 | 2022-06-07 14:53:47 | 查看详情 |
| ... 远程利用 | 严重 | | | 220 | 9 | 2 | 代码注入 | 2022-06-06 06:22:11 | 2022-06-07 14:53:47 | 查看详情 |

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关注紧急度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。
- 关注紧急度说明
  - 高危及严重：漏洞威胁等级为严重或高危。
  - 重点关注：重点关注漏洞是系统依据风险紧急程度等条件判断得出的，需要优先重点关注的漏洞，通常包含有需要高优紧急处理的风险。
  - 有 POC 或 EXP：漏洞风险标签存在有 EXP、有 POC、EXP/POC 的漏洞。
  - 远程 EXP：漏洞度量为 NetWork（远程利用）且存在 EXP 的漏洞。

4. 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。

# 镜像风险管理

# 概述

镜像风险管理可针对本地镜像、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

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。



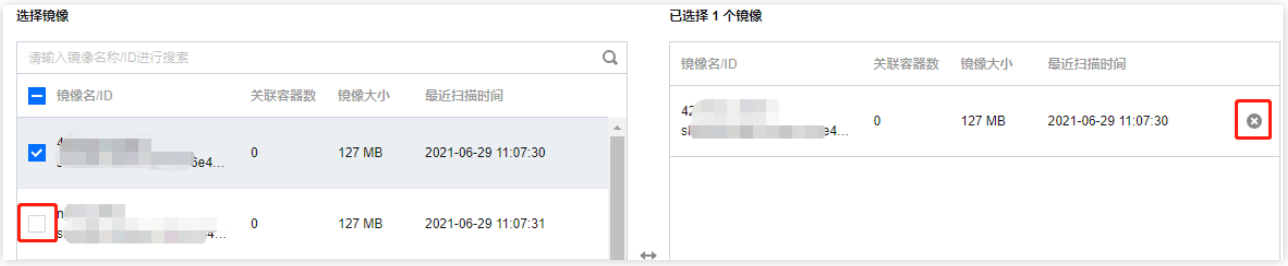

# 开启扫描数据

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. 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

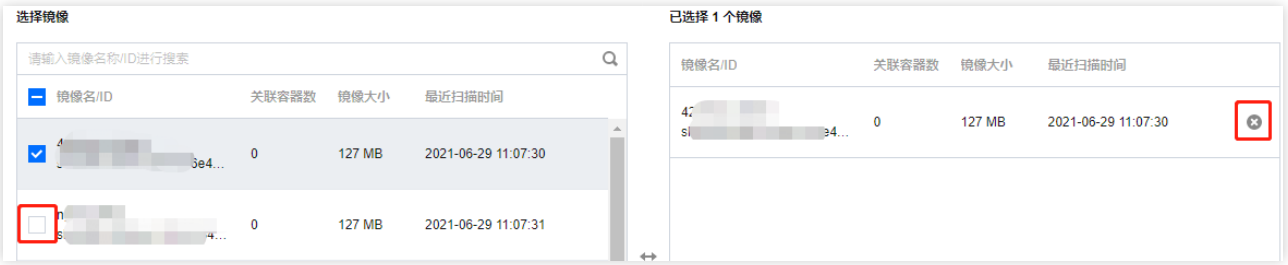
1. 在本地镜像页面，单击右侧定时扫描设置，可自定义设置是否开启定时扫描功能。




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。

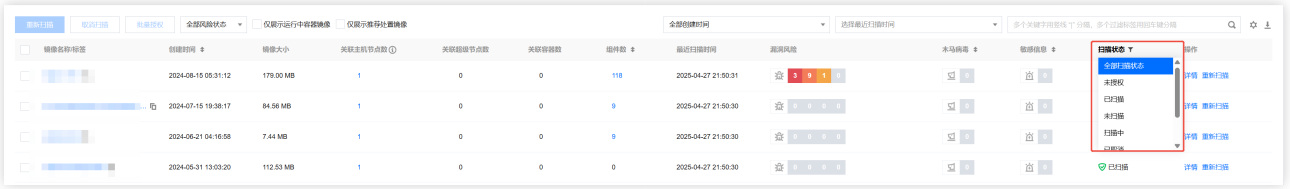
> 说明：
>
> 最长时间需要1~3分钟。

# 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：

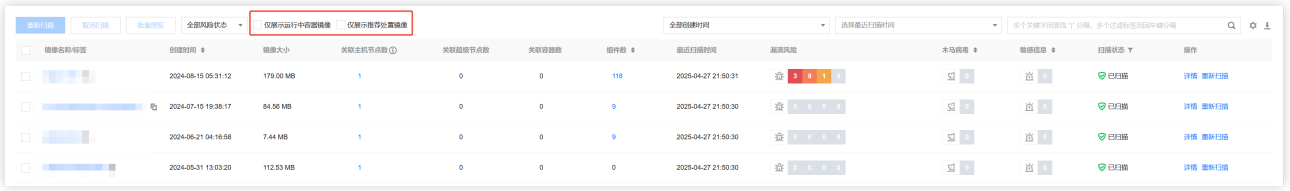
- 在本地镜像页面，单击扫描状态下拉框，按扫描状态对镜像资产进行筛选。



- 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。

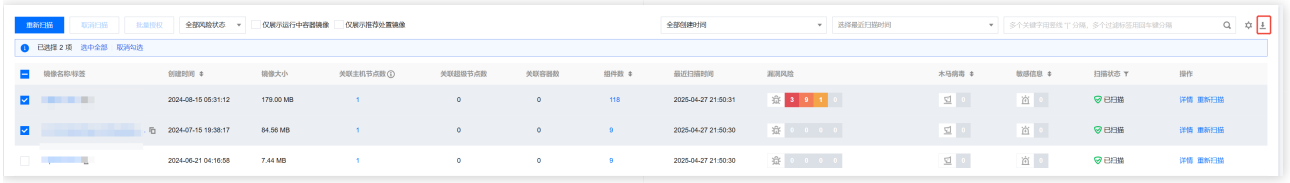


- 在本地镜像页面，单击搜索框通过“镜像名称、镜像 ID”等关键词对镜像资产进行查询。



## 导出镜像资产

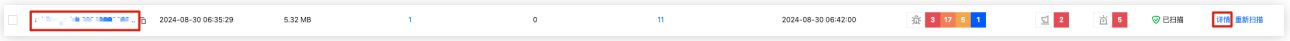
在本地镜像页面，单击 图标勾选所需的本地镜像后，单击 图标即可导出镜像资产。



## 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选主机：
>
> - 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。

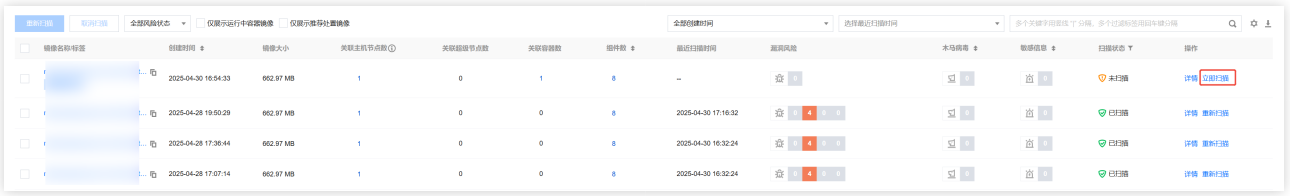
3. 在本地镜像页面，单击“关联容器数”，弹出关联的容器弹窗，展示了容器名称、容器 ID、容器运行状态、CMD、最近更新时间。

> 说明：
>
> 若关联多个容器，还可以通过以下操作筛选容器：
>
> - 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

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：
>
> 支持的镜像仓库类型：
>
> - 第三方镜像仓 Harbor。

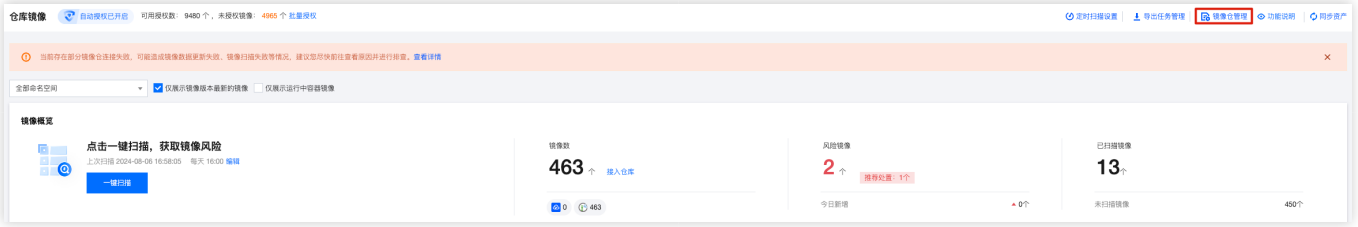
## 接入容器镜像服务

容器安全服务与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。
> - 首次使用时需手动进行仓库镜像资产数据更新，单击仓库镜像页面右上方的数据更新，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，单击新增镜像仓。
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：<br>- V1：镜像仓库版本为1.X.X。<br>- 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。 |

| 参数名称 | 说明 |
| --- | --- |
| 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、无限制 |
| 验证远程证书 | 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

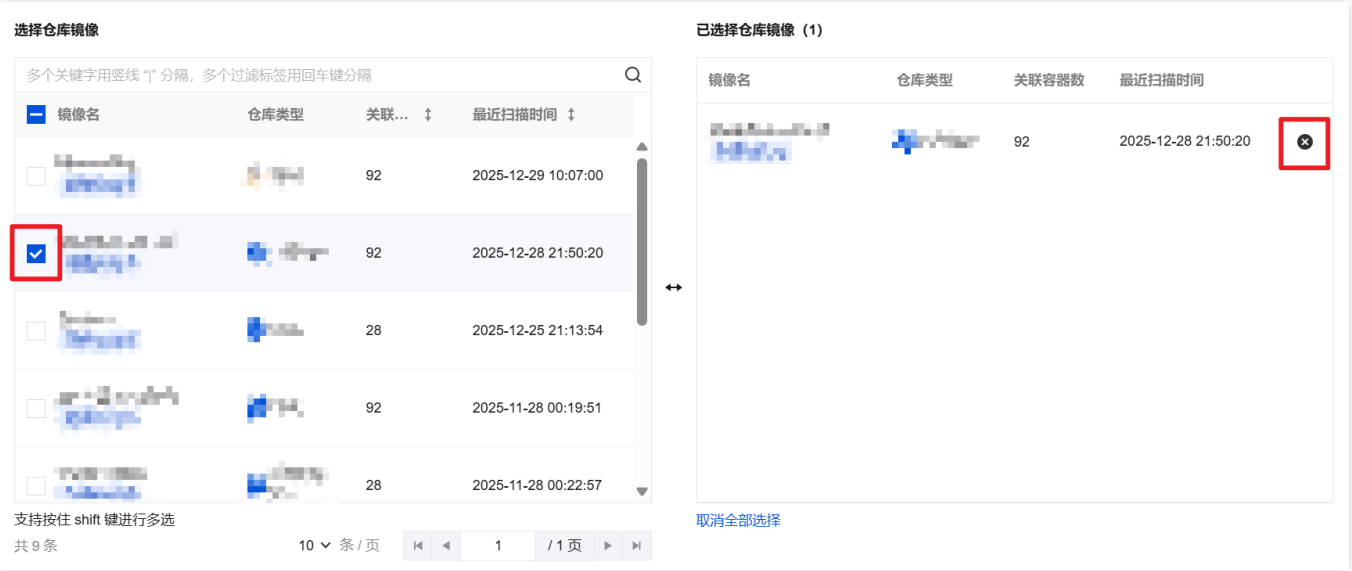
1. 在仓库镜像页面，单击右侧一键扫描，可获取最新镜像数据或镜像风险信息。




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：包含安全漏洞和敏感信息。
- 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：全部镜像和自选镜像。其中单击所需的自选镜像勾选图标，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

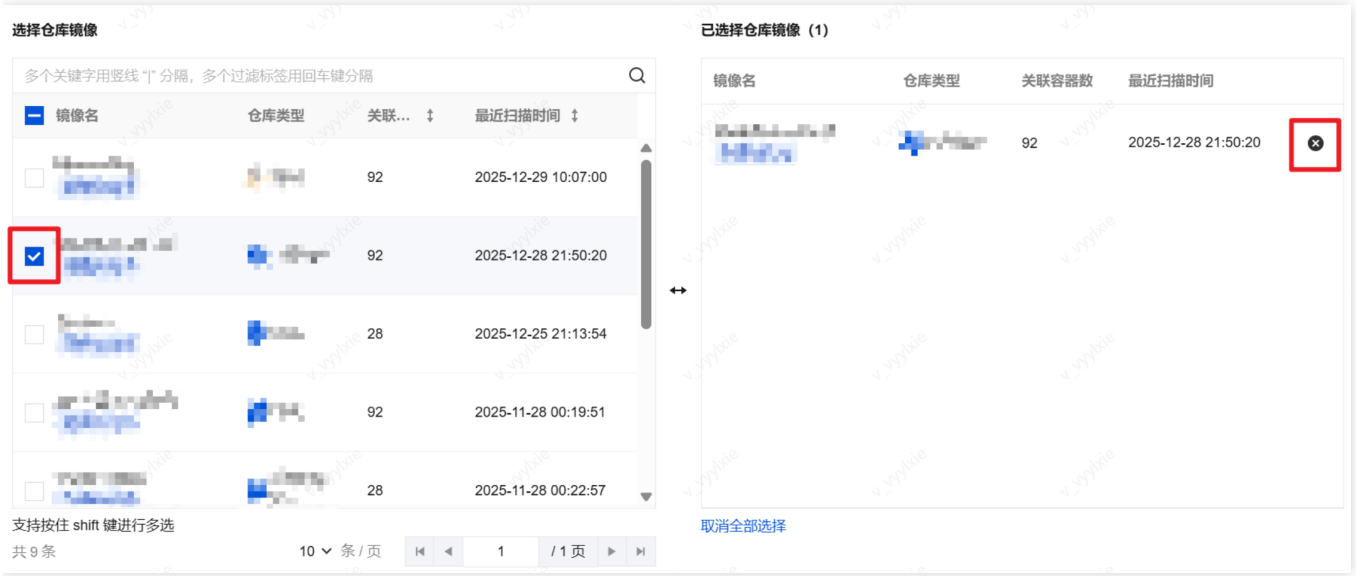
1. 在仓库镜像页面，单击右侧定时扫描设置，可自定义设置是否开启定时扫描功能。




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：单击选框图标、按需选择安全漏洞、敏感信息和木马病毒。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选或删除图标，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。

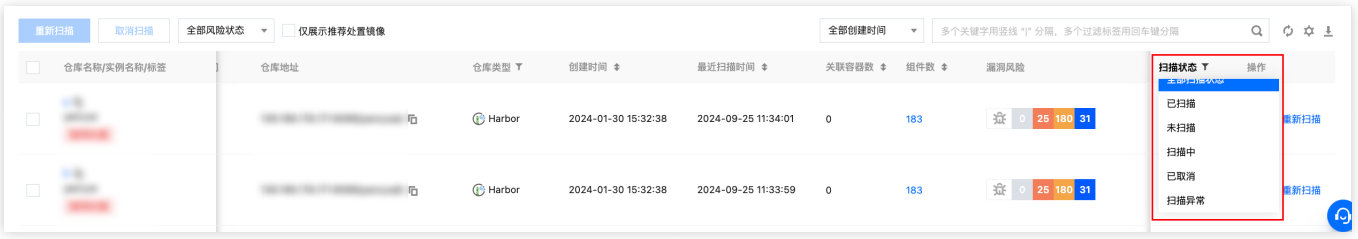
# 查看仓库镜像列表

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。

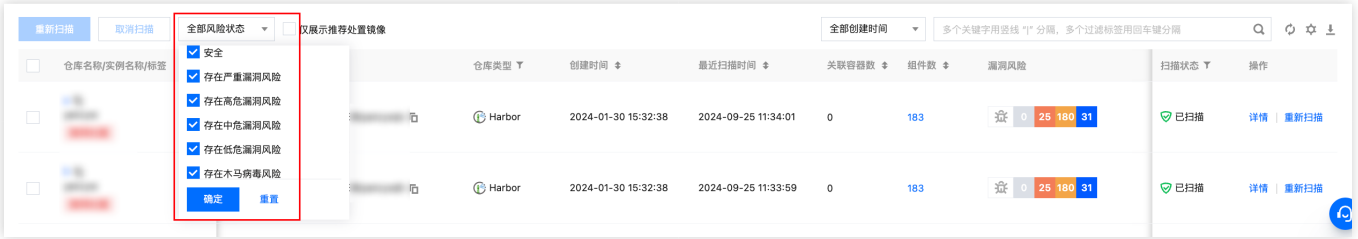
## 筛选镜像资产

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。

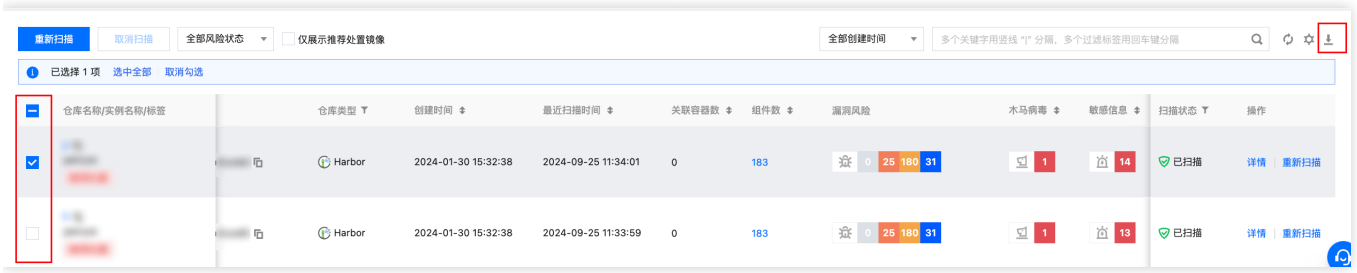



- 在仓库镜像页面，单击搜索框，可通过“镜像名称、镜像 Digest”等关键词对镜像资产进行查询。



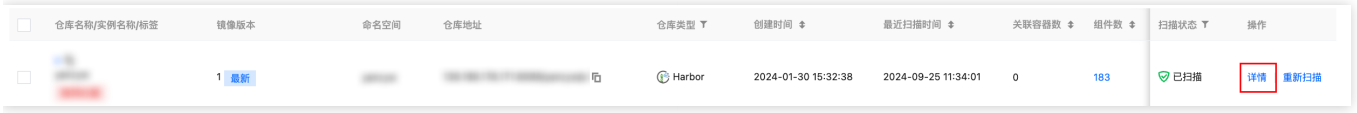

## 导出镜像资产

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。

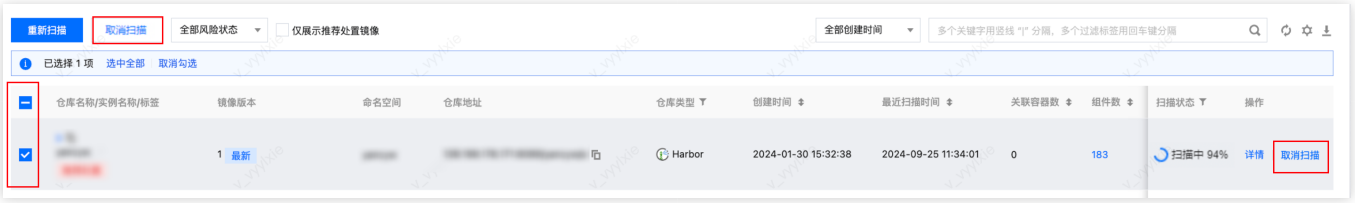
## 扫描镜像事件

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。



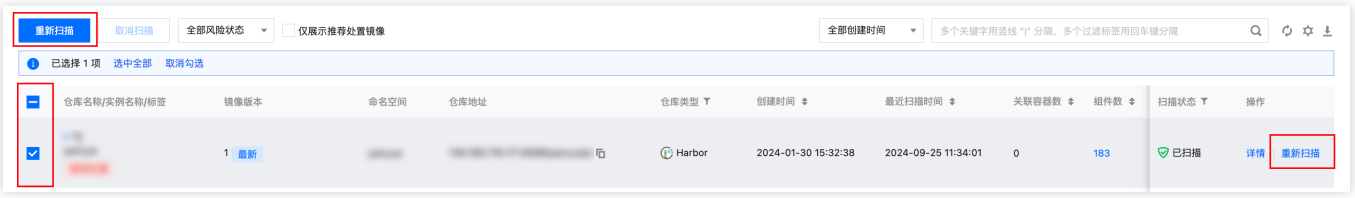

2. 在仓库镜像页面，镜像扫描状态为“扫描中”时，单击取消扫描，取消扫描镜像。

> 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。



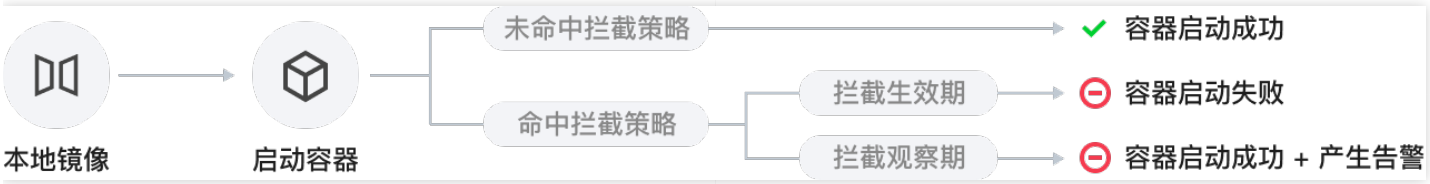

## 列表字段说明

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 CCR、Harbor。
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。

# 镜像拦截事件

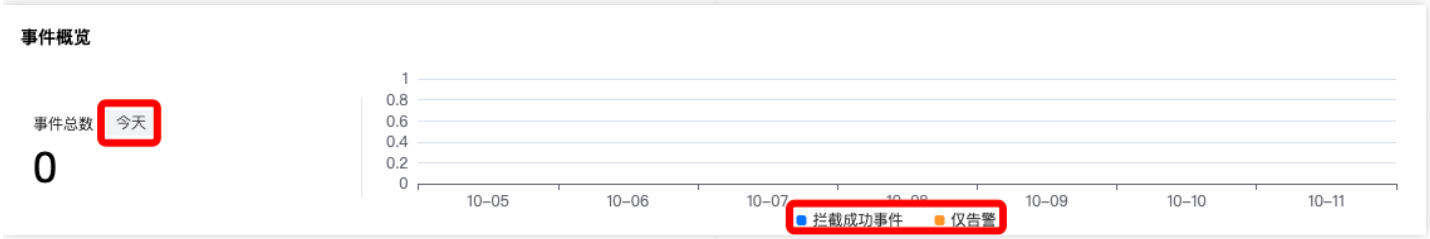
用户可在 [镜像拦截策略页面]配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。




- 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。

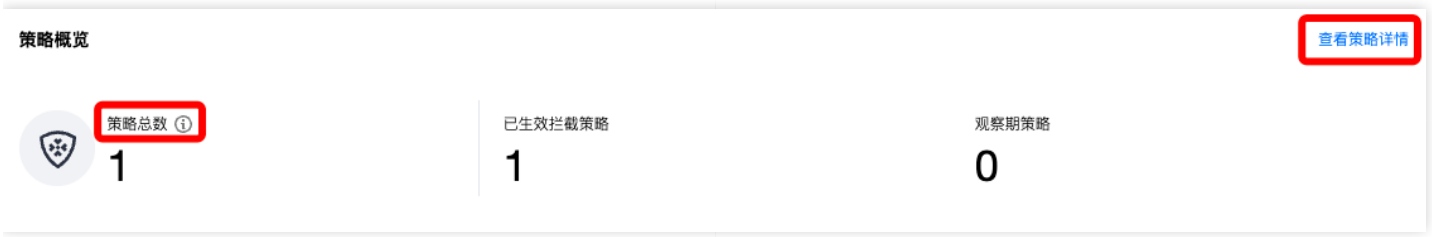
# 事件概览

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。
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。




# 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。可在此部分单击查看策略详情，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

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。此部分展示拦截或告警事件的事件类型、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

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 Overlay 自建集群 和 Overlay 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，支持接入单个集群或多个集群批量接入。

- 单个：选择所需集群 ID，单击接入集群，弹出安装容器安全窗口。
- 多个：选择多个集群 ID，单击安装组件批量接入集群，弹出安装容器安全窗口。




4. 在抽屉中，可选择 TKE 集群或自建集群进行接入。TKE 集群可直接操作列操作接入；自建集群需生成命令后进行手动接入。

## 执行集群检查

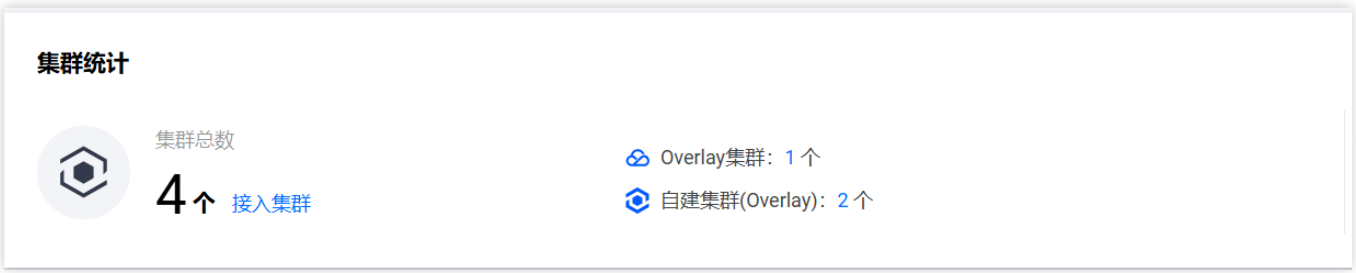
在集群检查页面，检查组件安装成功后系统会自动执行一次集群检查，您也可指定集群单击重新检查或指定多个集群单击批量检查执行集群检查。

> 说明：
>
> 集群检查组件默认为未安装状态，执行集群检查前需要先安装检查组件。

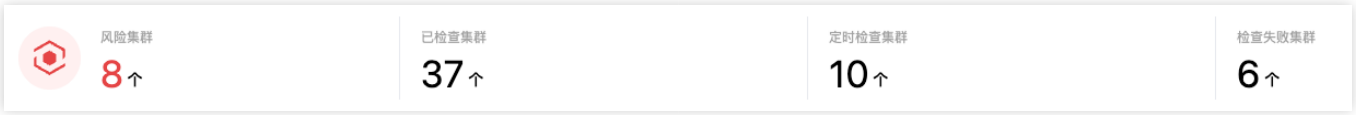


## 查看集群检查结果

1. 在集群检查页面，集群统计卡片展示集群总数、无风险集群数量以及未检查集群数量。




2. 集群风险卡片展示已检查集群中存在风险的风险集群数量、严重风险的集群数量、高危风险的集群数量、中危风险的集群数量和低危风险的集群数量。




3. 在集群检查页面，单击集群列表操作列的查看详情，进入“集群风险详情”页面。



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




5. 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。

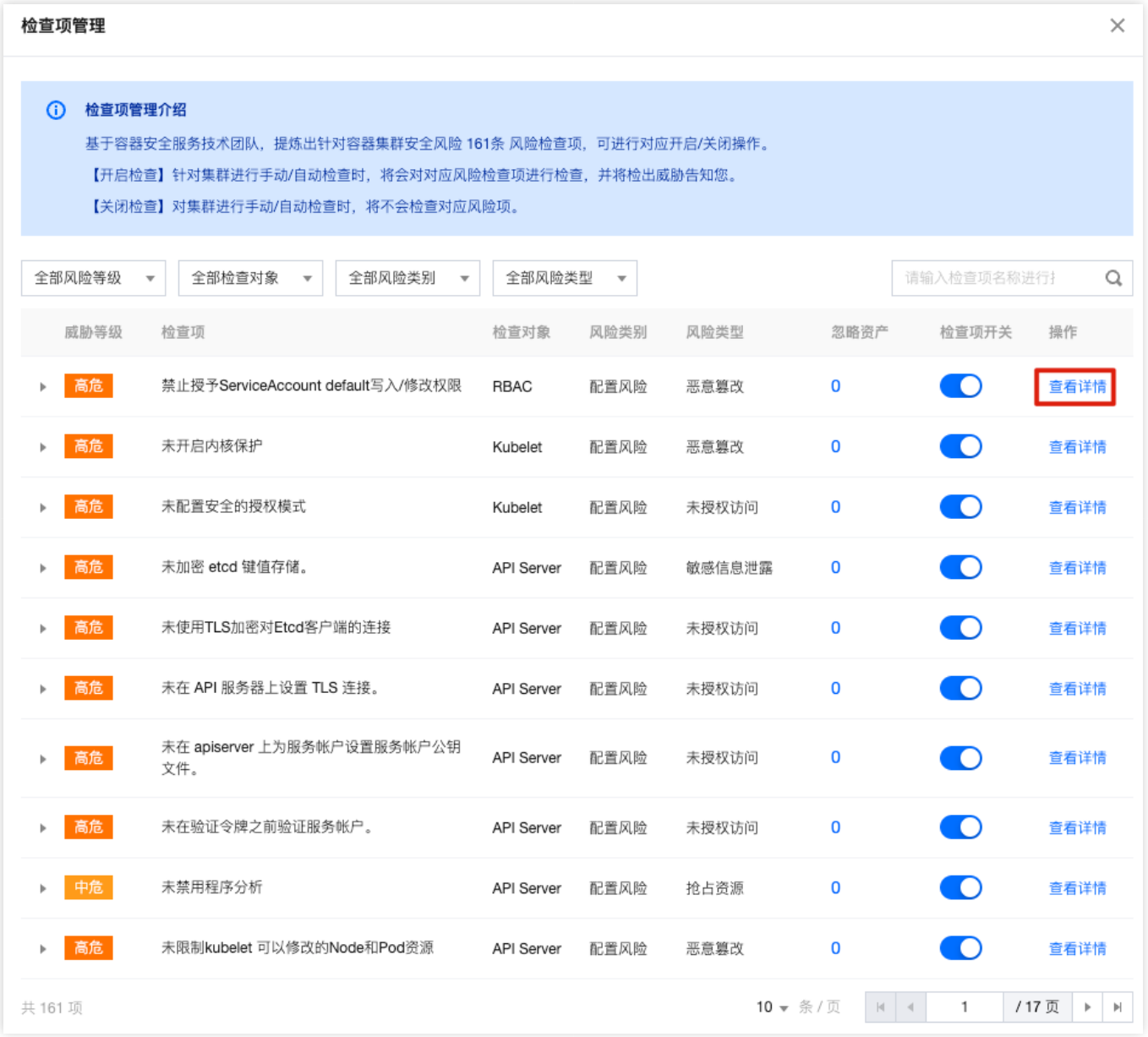



6. 在“风险检查项详情”页面，展示该风险检测项的风险详情、风险描述、解决方案以及当前集群的影响资产范围。
7. 点击“定时检查设置”，可配置定时任务对集群进行安全检查。


定时检查设置
定时检查
定时检查周期
检查周期
每天
15:00 ~ 18:00
(设置后会在周期选定的时间点开始定时检测)
检查项管理
检查项
已开启检查项 157 项 编辑
检查集群范围
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。
检查类型
全部集群
推荐
自选集群
选择集群
选择全部
已选择 10 个集群
取消全部选择
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
集群名称/ID
集群类型
腾讯云托管集群
自建集群(非腾讯云)
自建集群(腾讯云)
腾讯云独立集群
自建集群(腾讯云)
共 12 条
10 条 / 页
1
/ 2 页
支持按住 shift 键进行多选
保存
取消

# 管理集群检查项

1. 在集群检查页面，单击界面右上角的检测项管理，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。



# 自建集群

## 接入自建集群

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。

### 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. 在集群信息设置页面，配置相关参数，单击下一步。




参数说明：

| **参数组** | **参数** | **说明** | **可选项** |
| --- | --- | --- | --- |
| 基础信息设置 | 集群名称 | 输入自建集群的名称，64字符以内 | - |
| | 集群环境 | 选择自建集群的类型 | Kubernetes,Openshift |
| | 集群版本 | 选择集群环境的集群版本 | K8s 集群支持1.13以上版本 |
| 网络信息设置 | 网络类型 | 选择通过公网或通过 VPC 网络接入自建集群 | 公网、VPC |
| | 所在地域 | 选择自建集群所在的地域，公网类型无地域限制 | - |

| **参数组** | **参数** | **说明** | **可选项** |
| --- | --- | --- | --- |
| | VPC ID | 当网络类型使用 VPC 时，选择集群所在网络的 VPC 信息 | - |
| | API Server 地址 | 当网络类型使用 VPC 时，选择集群 API Server 后端服务类型 | 服务器、负载均衡 |
| 集群检查组件 | 安装检查组件 | 选择自动或者自行手动安装集群检查的组件 | ○ 自动安装检查组件并进行一次集群检查<br>○ 不安装检查组件，接入后自行安装组件并下发集群安装 |
| | 自动检查 | 是否开启集群的自动检查功能 | ○ 开启<br>○ 关闭 |

4. 在上传配置文件，单击选择文件，上传本地文件后，单击完成接入即可接入自建集群。

> 注意：
>
> ○ 公网方式接入自建集群，如果您的集群有设置访问控制策略，需单击 IP 白名单地址添加页面中的 IP 地址。
> ○ 您需要在服务器上生成 K8s 配置文件后，才能上传该配置文件。生成 K8s 配置文件的具体操作，请参见生成 K8S 配置文件。
> ○ 上传配置文件，大小需要在 1M 以内。

# 生成 K8s 配置文件

本文指导您生成容器安全需要的最小化权限 K8s 配置文件。您可参照文档步骤生成配置文件，或者参见 一键脚本。

## 前提条件

- 已在服务器上搭建 K8s 集群。具体操作，请参见 K8s 中文官方文档。
- 已安装 Docker 服务。

## 操作步骤

1. 以 Root 身份登录 K8s 集群 master 所在服务器。
2. 输入如下命令，创建命名空间和权限绑定。

```
# 1. 创建命名空间： tcss
# 2. 创建命名空间tcss下的管理角色： tcss-admin
# 3. 绑定角色tcss-admin和用户tcss
# 4. 创建秘钥并绑定服务账号： tcss-agent-secret，tcss-agent
# 5. 创建只读的集群角色： security-clusterrole
# 6. 绑定集群角色security-clusterrole到服务账号tcss-agent
```

```
---
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: User
  name: tcss
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: tcss-admin
  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: v1
kind: ServiceAccount
metadata:
  name: tcss-agent
  namespace: tcss
```

```
secrets:
  - name: tcss-agent-secret
    namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
  resources: ["namespaces", "pods", "nodes"]
  verbs: ["get", "list"]
- apiGroups: ["apps"]
  resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
  verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
  resources: ["networkpolicies"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
  resources: ["jobs", "cronjobs"]
  verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles", "clusterrolebindings"]
  verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
  resources: ["ingresses"]
  verbs: ["get", "list"]

---
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
```

> 说明：
>
> 执行上述命令，如果能显示 Pod 或者显示当前命名空间下没有相关资源，则表示该集群配置是可用的，上传该文件 /root/tcss.conf 即可。

## 一键脚本

在 mater 节点中，您可基于以下一键脚本代码一键快速生成集群配置文件：

> 说明：
>
> 环境需要提前安装 Openssl。

```
#!/bin/bash

set -e;

# API_SERVER 需要设置为公网可访问的地址和端口
# API_SERVER=https://xx.xx.xx.xx:xxxx

# 以下路径,用户根据集群实际情况设定
KUBECONFIG_TARGET=/root/tcss.conf
CA_FILE=/etc/kubernetes/ca.crt
CAKEY_FILE=/etc/kubernetes/ca.key
TCSS_TMPDIR=/tmp/tcss
# 如果是OpenShift环境，可以更换为 oc
KUBECTL_CMD=kubectl

if [ ! $API_SERVER ]; then
    echo "API_SERVER does not set.";
    exit 1;
fi
if ! which kubectl ; then
    echo "kubectl does not exist.";
    exit 1;
fi
if [ ! -f "$CA_FILE" ]; then
    echo "$CA_FILE does not exist.";
    exit 1;
fi
if [ ! -f "$CAKEY_FILE" ]; then
    echo "$CAKEY_FILE does not exist.";
    exit 1;
fi
if [ ! -d $TCSS_TMPDIR ]; then
    mkdir -p $TCSS_TMPDIR;
fi

cat <<EOF  > $TCSS_TMPDIR/tcss_res.yaml
---
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: User
  name: tcss
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: tcss-admin
  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: v1
kind: ServiceAccount
metadata:
  name: tcss-agent
  namespace: tcss
secrets:
  - name: tcss-agent-secret
    namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: ClusterRole
metadata:
  name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
  resources: ["namespaces", "pods", "nodes"]
  verbs: ["get", "list"]
- apiGroups: ["apps"]
  resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
  verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
  resources: ["networkpolicies"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
  resources: ["jobs", "cronjobs"]
  verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles", "clusterrolebindings"]
  verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
  resources: ["ingresses"]
  verbs: ["get", "list"]

---
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
EOF

# echo "generate tcss resource file ($TCSS_TMPDIR/tcss_res.yaml) success."

$KUBECTL_CMD apply -f $TCSS_TMPDIR/tcss_res.yaml;

# 创建User私钥 tcss.key。
openssl genrsa -out $TCSS_TMPDIR/tcss.key 2048
# 创建证书签署请求 tcss.csr
openssl req -new -key $TCSS_TMPDIR/tcss.key -out $TCSS_TMPDIR/tcss.csr -subj "/O=K8s/CN=tcss"
```

```
# 签署证书 生成 tcss.crt
openssl x509 -req -in $TCSS_TMPDIR/tcss.csr -CA $CA_FILE -CAkey $CAKEY_FILE -CAcreateserial -out $TCSS_TMPDIR/tcss.crt -days 365

# 创建并设置集群配置
$KUBECTL_CMD config set-cluster tcss --server=$API_SERVER --certificate-authority=$CA_FILE --embed-certs=true --kubeconfig=$KUBECONFIG_TARGET
# 创建并设置用户配置
$KUBECTL_CMD config set-credentials tcss --client-certificate=$TCSS_TMPDIR/tcss.crt --client-key=$TCSS_TMPDIR/tcss.key --embed-certs=true --kubeconfig=$KUBECONFIG_TARGET
# 设置context配置
$KUBECTL_CMD config set-context tcss@tcss --cluster=tcss --user=tcss --kubeconfig=$KUBECONFIG_TARGET
# 切换context配置
$KUBECTL_CMD config use-context tcss@tcss --kubeconfig=$KUBECONFIG_TARGET

echo "generate KUBECONFIG file success. $KUBECONFIG_TARGET"
```

# 生成 Openshift 配置文件

本文指导您生成容器安全需要的最小化权限 OpenShift 配置文件。您可参照文档步骤生成配置文件，或者参见 一键脚本。

## 前提条件

1. 已在服务器上搭建 K8s 集群。具体操作，请参见 K8s 中文官方文档。
2. 已安装 Docker 服务。
3. 暂仅支持 OpenShift3.0及以上版本接入，低于该版本可能存在不确定性问题。

## 操作步骤

> 说明：
>
> 整体接入思路和 Kubernetes 类似，只涉及相关路径和命令行工具区别，如果集群 master 节点上已经安装的 kubectl 工具，则可以完全同 Kubernetes 集群接入方式进行接入。

1. 以 Root 身份登录 OpenShift 集群 master 所在服务器。
2. 输入如下命令，创建命名空间和权限绑定。

```
# 1. 创建命名空间： tcss
# 2. 创建命名空间tcss下的管理角色： tcss-admin
# 3. 绑定角色tcss-admin和用户tcss
# 4. 创建秘钥并绑定服务账号： tcss-agent-secret，tcss-agent
# 5. 创建只读的集群角色： security-clusterrole
# 6. 绑定集群角色security-clusterrole到服务账号tcss-agent

---
```

```
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: User
  name: tcss
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: tcss-admin
  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: v1
kind: ServiceAccount
metadata:
  name: tcss-agent
  namespace: tcss
secrets:
  - name: tcss-agent-secret
```

```
    namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
  resources: ["namespaces", "pods", "nodes"]
  verbs: ["get", "list"]
- apiGroups: ["apps"]
  resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
  verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
  resources: ["networkpolicies"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
  resources: ["jobs", "cronjobs"]
  verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles", "clusterrolebindings"]
  verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
  resources: ["ingresses"]
  verbs: ["get", "list"]

---
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
```

3. 进入配置目录（/etc/origin/master/），输入如下命令，创建证书。

```
# 创建User私钥 tcss.key。
openssl genrsa -out tcss.key 2048
```

```
# 创建证书签署请求 tcss.csr
openssl req -new -key tcss.key -out tcss.csr -subj "/O=K8s/CN=tcss"

# 签署证书 生成 tcss.crt
openssl x509 -req -in tcss.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out tcss.crt -days 365
```

4. 输入如下命令，创建集群配置文件。

```
# 创建并设置集群配置, 其中需要主要 server 地址必须为公网可访问地址
KUBECONFIG=/root/tcss.conf oc config set-cluster tcss --server=https://xx.xx.xx.xx:60002 --certificate-author
ity=/etc/origin/master/ca.crt --embed-certs=true --kubeconfig=/root/tcss.conf

# 创建并设置用户配置
KUBECONFIG=/root/tcss.conf oc config set-credentials tcss --client-certificate=tcss.crt --client-key=tcss.key
--embed-certs=true --kubeconfig=/root/tcss.conf

# 设置context配置
KUBECONFIG=/root/tcss.conf oc config set-context tcss@tcss --cluster=tcss --user=tcss --kubeconfig=/root/
tcss.conf

# 切换context配置
KUBECONFIG=/root/tcss.conf oc config use-context tcss@tcss --kubeconfig=/root/tcss.conf
```

5. 输入如下命令，验证集群配置文件并上传配置。

```
KUBECONFIG=/root/tcss.conf oc -n tcss get pod
```

> 说明：
>
> 执行上述命令，如果能显示Pod或者显示当前命名空间下没有相关资源则表示该集群配置是可用的，上传该文件 /root/tcss.conf 即可。

## 一键脚本

在 mater 节点中，您可基于以下一键脚本代码一键快速生成集群配置文件：

> 说明：
>
> 环境需要提前安装 Openssl。

```
#!/bin/bash

set -e;

# API_SERVER 需要设置为公网可访问的地址和端口
# API_SERVER=https://xx.xx.xx.xx:xxxx
```

```
# 以下路径,用户根据集群实际情况设定
KUBECONFIG_TARGET=/root/tcss.conf
CA_FILE=/etc/kubernetes/ca.crt
CAKEY_FILE=/etc/kubernetes/ca.key
TCSS_TMPDIR=/tmp/tcss
KUBECTL_CMD=oc

if [ ! $API_SERVER ]; then
    echo "API_SERVER does not set.";
    exit 1;
fi
if ! which $KUBECTL_CMD ; then
    echo "$KUBECTL_CMD does not exist.";
    exit 1;
fi
if [ ! -f "$CA_FILE" ]; then
    echo "$CA_FILE does not exist.";
    exit 1;
fi
if [ ! -f "$CAKEY_FILE" ]; then
    echo "$CAKEY_FILE does not exist.";
    exit 1;
fi
if [ ! -d $TCSS_TMPDIR ]; then
    mkdir -p $TCSS_TMPDIR;
fi

cat <<EOF  > $TCSS_TMPDIR/tcss_res.yaml
---
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: User
  name: tcss
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: tcss-admin
  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: v1
kind: ServiceAccount
metadata:
  name: tcss-agent
  namespace: tcss
secrets:
  - name: tcss-agent-secret
    namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
  resources: ["namespaces", "pods", "nodes"]
  verbs: ["get", "list"]
- apiGroups: ["apps"]
  resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
  verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
  resources: ["networkpolicies"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
  resources: ["jobs", "cronjobs"]
```

```
  verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
  resources: ["clusterroles", "clusterrolebindings"]
  verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
  resources: ["ingresses"]
  verbs: ["get", "list"]

---
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
EOF

# echo "generate tcss resource file ($TCSS_TMPDIR/tcss_res.yaml) success."

$KUBECTL_CMD apply -f $TCSS_TMPDIR/tcss_res.yaml;
$KUBECTL_CMD adm policy add-scc-to-user privileged -n tcss -z tcss-agent;
$KUBECTL_CMD adm policy add-scc-to-user hostaccess -n tcss -z tcss-agent;
$KUBECTL_CMD adm policy add-scc-to-user privileged tcss;
$KUBECTL_CMD adm policy add-scc-to-user hostaccess tcss;
oc adm policy add-cluster-role-to-user cluster-reader tcss;

# 创建User私钥 tcss.key。
openssl genrsa -out $TCSS_TMPDIR/tcss.key 2048
# 创建证书签署请求 tcss.csr
openssl req -new -key $TCSS_TMPDIR/tcss.key -out $TCSS_TMPDIR/tcss.csr -subj "/O=K8s/CN=tcss"
# 签署证书 生成 tcss.crt
openssl x509 -req -in $TCSS_TMPDIR/tcss.csr -CA $CA_FILE -CAkey $CAKEY_FILE -CAcreateserial -out $TCSS_
TMPDIR/tcss.crt -days 365

# 创建并设置集群配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-cluster tcss --server=$API_SERVER --certifi
cate-authority=$CA_FILE --embed-certs=true --kubeconfig=$KUBECONFIG_TARGET
# 创建并设置用户配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-credentials tcss --client-certificate=$TCSS_
TMPDIR/tcss.crt --client-key=$TCSS_TMPDIR/tcss.key --embed-certs=true --kubeconfig=$KUBECONFIG_TAR
```

```
GET
# 设置context配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-context tcss@tcss --cluster=tcss --user=tc
ss --kubeconfig=$KUBECONFIG_TARGET
# 切换context配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config use-context tcss@tcss --kubeconfig=$KUBEC
ONFIG_TARGET

echo "generate KUBECONFIG file success. $KUBECONFIG_TARGET"
```

# 风险分析

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。

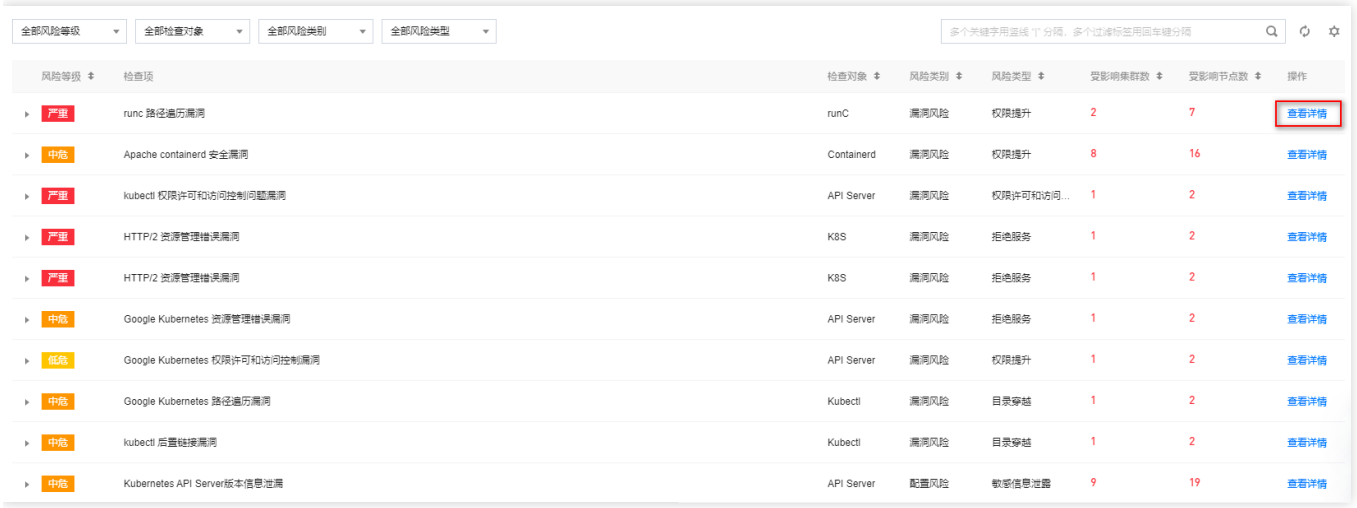
## 查看风险节点统计

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. 在风险分析页面的查案风险节点统计卡片，展示集群检查所发现的风险节点数量以及过去七天内风险节点的数量趋势，包括严重风险节点和趋势、高危风险节点和趋势、中危风险节点和趋势、低危风险节点和趋势。




## 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。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

安全基线支持 CIS Benchmark 标准并结合云鼎实验室最佳基线配置实践，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最佳基线配置，减少攻击面。

# 容器

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。

## 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、低危四个威胁等级的检测项数量。

> 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，单击百分比中的查看，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，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、检测耗时和自动检测周期配置。




3. 在容器页面，单击重新检测，可立即对容器资产进行一次基线检测。




4. 在容器页面，单击基线设置，可设置基线策略和基线忽略列表。



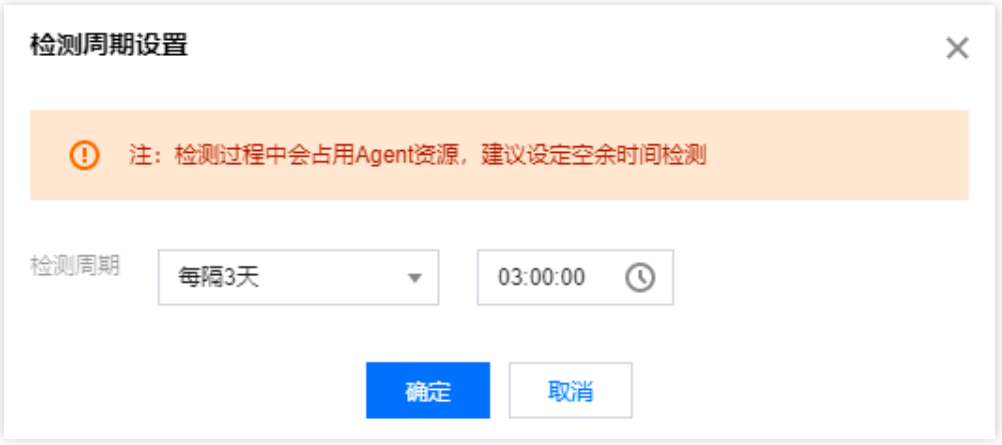

## 设置基线策略

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，可通过单击开关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，单击检测周期后的编辑按钮，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。
3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。




4. 单击确定，即可完成检测周期设置。

## 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"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。

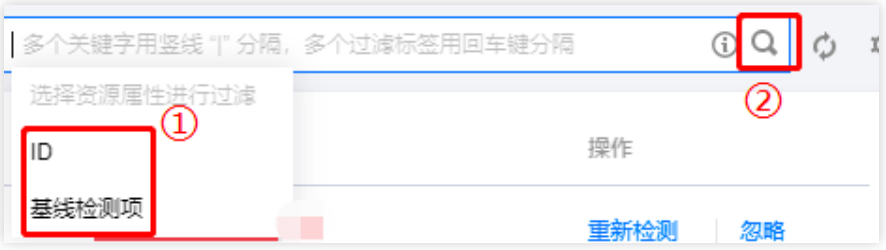
> 说明：

> 检测项取消忽略后，检测内容将恢复正常检测。

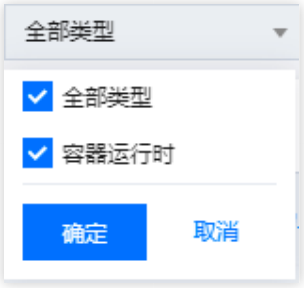
# 查看检测结果列表

## 筛选刷新基线检测项

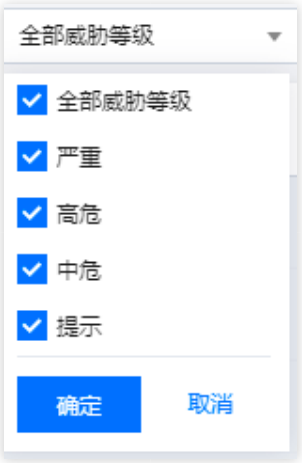
1. 登录容器安全服务控制台，在左侧导航中，单击基线管理 > 容器。
2. 在容器页面，单击搜索框，可通过“ID 和基线检测项”关键词对容器基线检测项进行查询。




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。




5.在容器页面，单击操作栏右侧刷新图标，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产进行重新检测。

> 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，单击设置图标，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

- 基线检测项：单击“基线检测项”，可查看检测项详情。
- 未通过检测项：未通过的检测项数量。
- 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。
- 最近检测时间：最近一次的检测时间。

# 镜像

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、低危四个威胁等级的检测项数量。

> 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，单击百分比中的查看，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、检测耗时和自动检测周期配置。




3. 在镜像页面，单击重新检测，可立即对镜像资产进行一次基线检测。



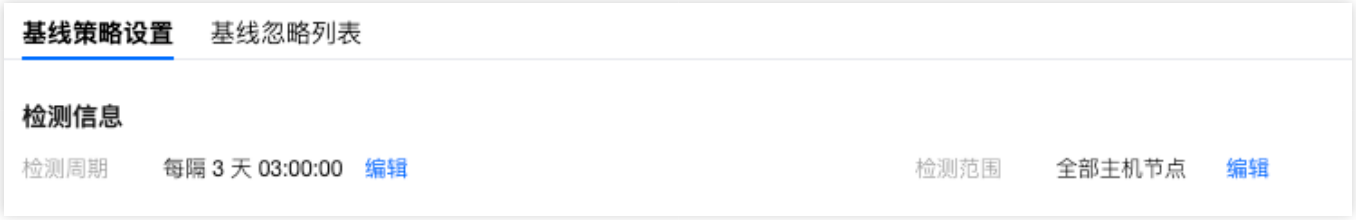

4. 在镜像页面，单击基线设置，可设置基线策略和基线忽略列表。




## 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，可通过单击开关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，单击检测周期后的编辑按钮，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。
3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。




4. 单击确定，即可完成检测周期设置。

## 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。



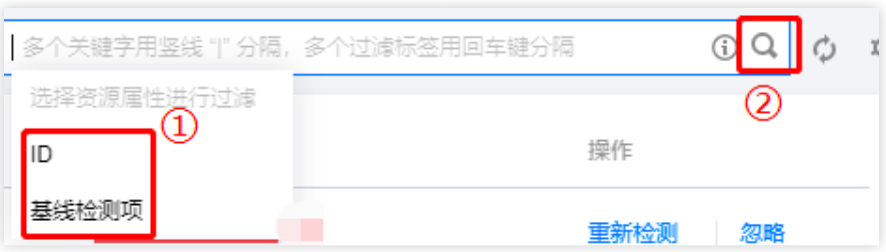

2. 在基线忽略列表页面，单击 图标勾选所需的镜像基线检测项后，单击取消忽略，将会对选中的镜像基线检测项取消忽略。

> 说明：
>
> 检测项取消忽略后，检测内容将恢复正常检测。

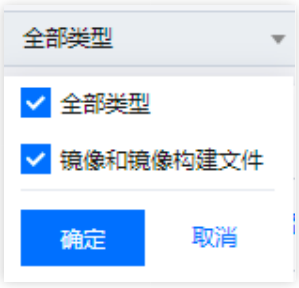
# 查看检测结果列表

## 筛选刷新基线检测项

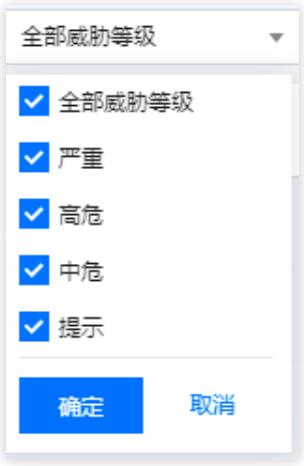
1. 登录容器安全服务控制台，在左侧导航中，单击基线管理 > 镜像。
2. 在镜像页面，单击搜索框，可通过"ID 和基线检测项"关键词对镜像基线检测项进行查询。




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，单击操作栏右侧刷新图标，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。

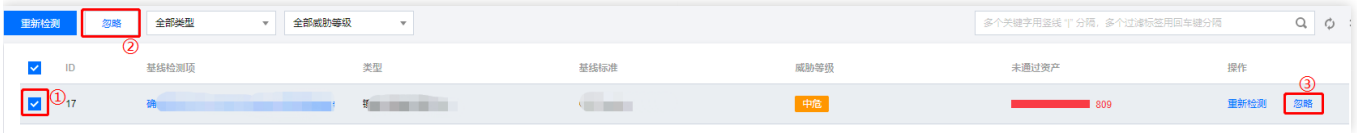
> 说明：
>
> 选定多个镜像基线检测项，单击②处的重新检测，可进行批量检测。




## 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，单击设置图标，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

- ID：检测项ID，该ID全局唯一。
- 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
- 类型：检测项的类型。
- 基线标准：检测项所属基线标准。
- 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。
- 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。
- 操作：重新检测和忽略。

# Docker主机

Docker 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。

## 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中严重、高危、中危、低危四个威胁等级的检测项数量。

> 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，单击百分比中的查看，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、检测耗时和自动检测周期配置。




2. 在 Docker 主机页面，单击重新检测，可立即对主机资产进行一次基线检测。



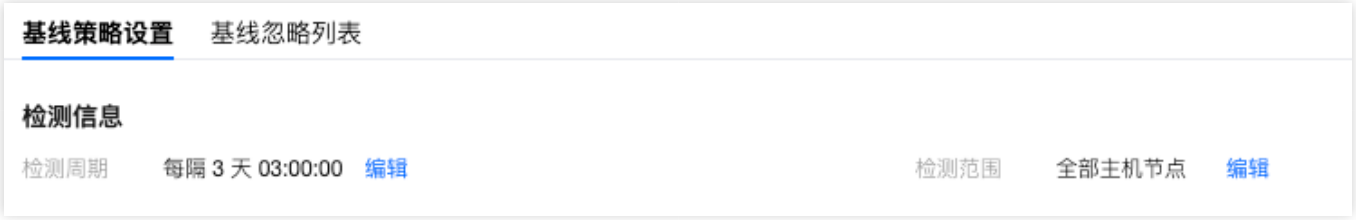

3. 在 Docker 主机页面，单击基线设置，可设置基线策略和基线忽略列表。




## 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，可通过单击开关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，单击检测周期的编辑，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。
3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。




4. 单击确定，即可完成检测周期设置。

## 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。



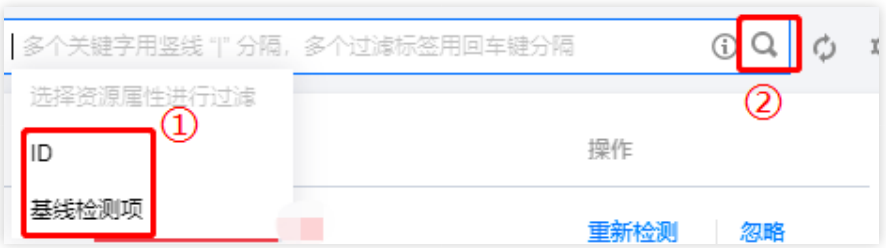

2. 在基线忽略列表页面，单击 图标勾选所需的主机基线检测项后，单击取消忽略，将会对选中的主机基线检测项取消忽略。

> 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

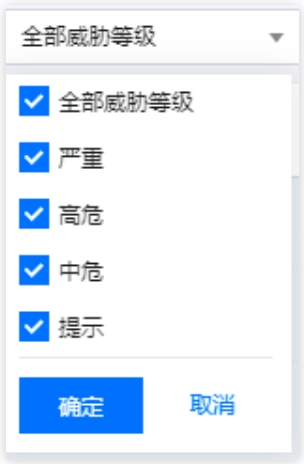
1. 在 Docker 主机页面，单击搜索框，可通过"ID 和基线检测项"关键词对 Docker 主机基线检测项进行查询。




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，单击操作栏右侧刷新图标，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

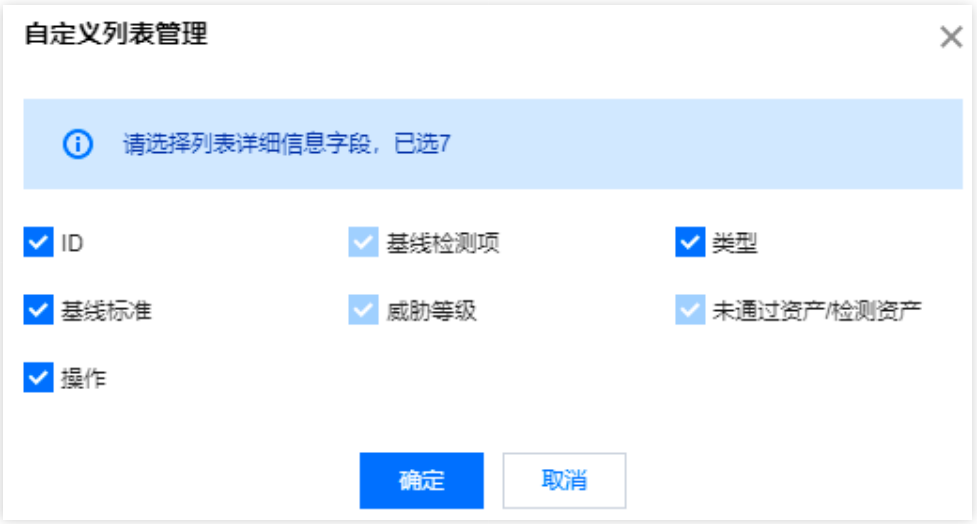
在 Docker 主机页面，单击勾选所需基线检测项后，单击忽略 > 确定，可对基线检测项进行忽略。

> 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，单击设置图标，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

- ID：检测项ID，该ID全局唯一。
- 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
- 类型：检测项的类型。
- 基线标准：检测项所属基线标准。
- 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。
- 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。
- 操作：重新检测和忽略。

# Kubernetes

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、低危四个威胁等级的检测项数量。

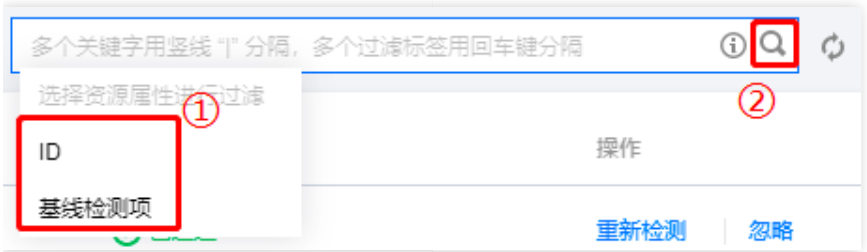
> 说明：
>
> 检测项通过率计算逻辑为：通过的检测项数量/检测项总数。




3. 在 Kubernetes 页面，单击百分比中的查看，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、检测耗时和自动检测周期配置。




3. 在 Kubernetes 页面，单击重新检测，可立即对 Kubernetes 基线检测项进行一次基线检测。



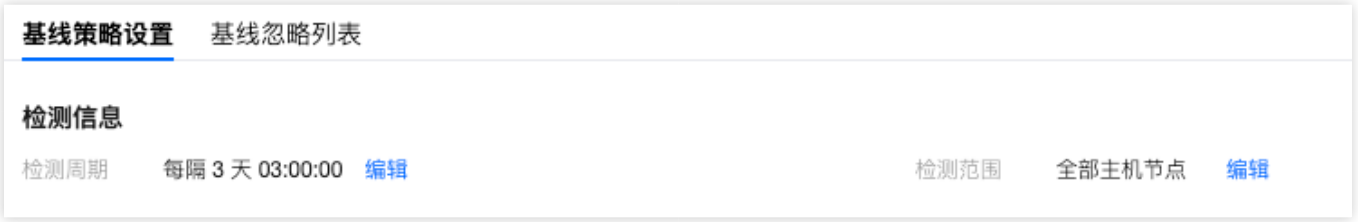

4. 在 Kubernetes 页面，单击基线设置，可设置基线策略和基线忽略列表。



## 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，可通过单击开关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，单击检测周期的编辑，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。




3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。




4. 单击确定，即可完成检测周期设置。

## 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。

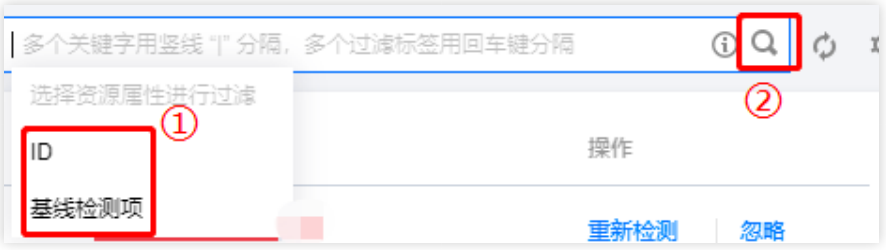
> 说明：

> 检测项取消忽略后，检测内容将恢复正常检测。

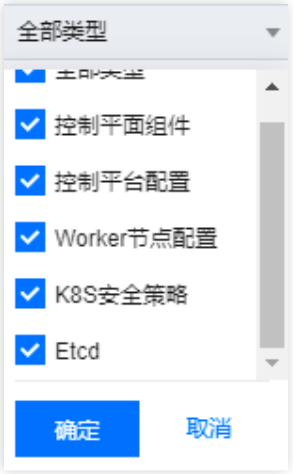
# 查看检测结果列表

## 筛选刷新基线检测项

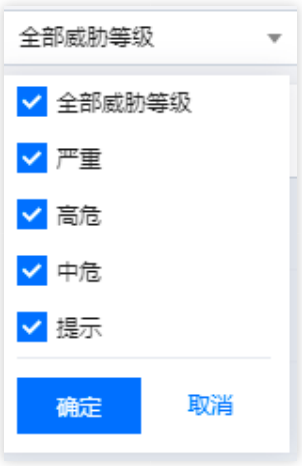
1. 登录容器安全服务控制台，在左侧导航中，单击基线管理 > Kubernetes。
2. 在 Kubernetes 页面，单击搜索框，可通过“基线检测项”关键词对 Kubernetes 基线检测项进行查询。




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，单击操作栏右侧刷新图标，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，单击刷新图标，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

- ID：检测项ID，该ID全局唯一。
- 基线检测项：检测内容，单击“ 基线检测项”，可查看检测项详情。
- 类型：检测项的类型。
- 基线标准：检测项所属基线标准。
- 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。
- 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。
- 操作：重新检测和忽略。

# 运行时安全
# 概述

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。

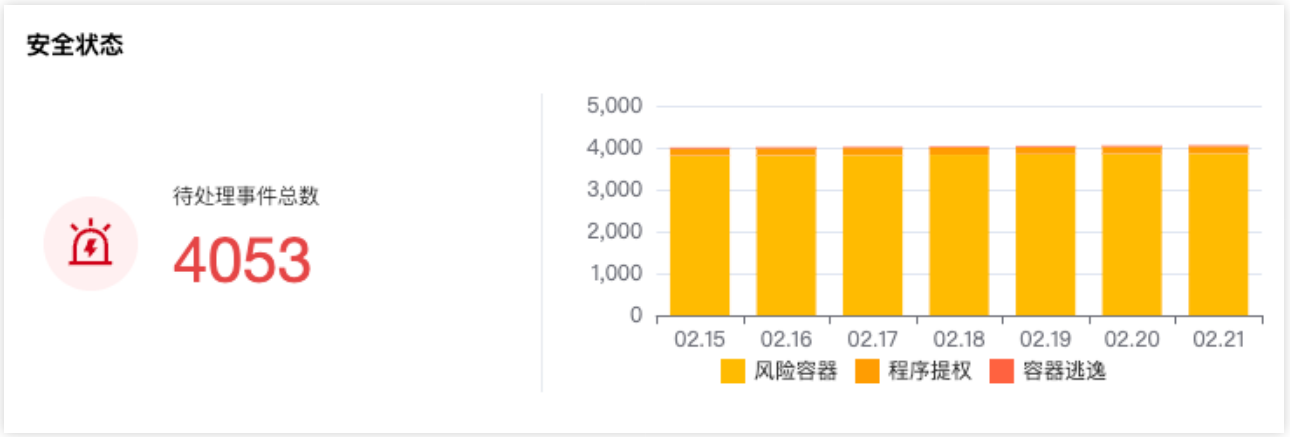
- 容器逃逸：指的是容器利用系统漏洞，“逃逸”出了其自身所拥有的权限，实现了对宿主机和宿主机上其他容器的访问。由于容器与宿主机共享操作系统内核，为了避免容器获取宿主机的 Root 权限，通常不允许采用特权模式运行容器。按照入侵者执行容器逃逸的顺序，容器安全服务将风险事件类型划分为三类，分别是：风险容器、程序提权、容器逃逸。
  - 风险容器：指当前容器存在部分潜在风险行为，可能会存在被提权或被逃逸的风险，包含敏感路径挂载、特权容器。
  - 程序提权：指当前容器出现了提权的风险行为，可能会进一步导致其逃逸，需要您进行关注。
  - 容器逃逸：指当前容器已经出现了逃逸行为，此时您应该立即对出现的风险事件进行关注，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。

# 容器逃逸

## 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

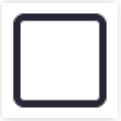
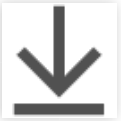
1. 在容器逃逸页面，单击搜索框，可通过“容器名称、镜像名称和节点名称”等关键词对容器逃逸事件进行查询。




2. 在容器逃逸页面，单击操作栏右侧刷新图标，即可刷新容器逃逸事件。

导出容器逃逸

在容器逃逸页面，单击勾选所需的容器逃逸事件后，单击导出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，单击事件类型左侧展开图标，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，单击设置图标，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

- 事件类型：容器逃逸告警事件类型，包括宿主机文件访问逃逸、MountNamespace 逃逸、程序提权逃逸、特权容器启动逃逸、敏感路径挂载和 Syscall 逃逸。
- 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。

- 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。
- 事件数量：聚合时间范围内该逃逸事件触发告警的总数量。
- 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。
-

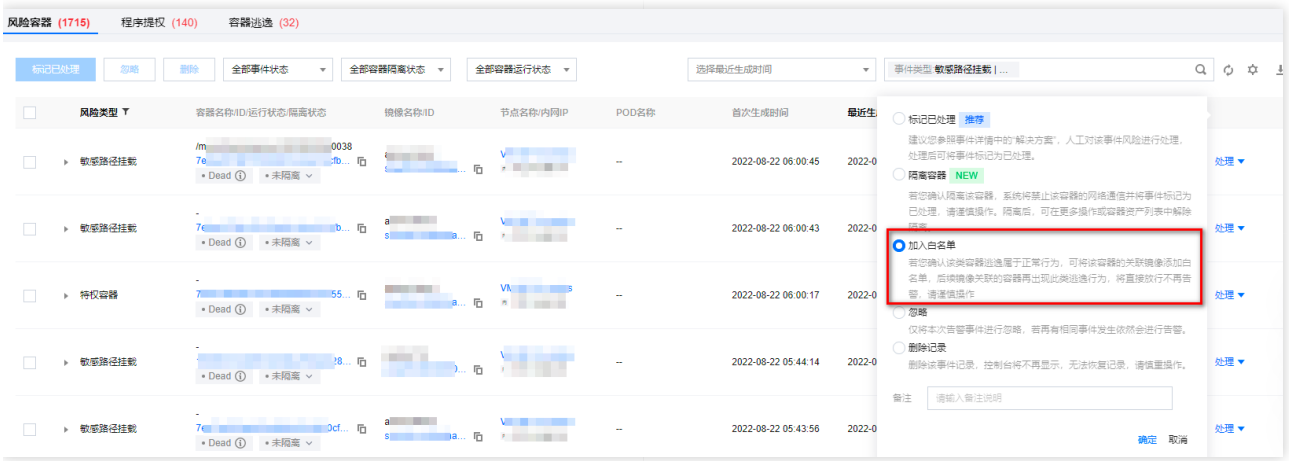
# 逃逸白名单

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

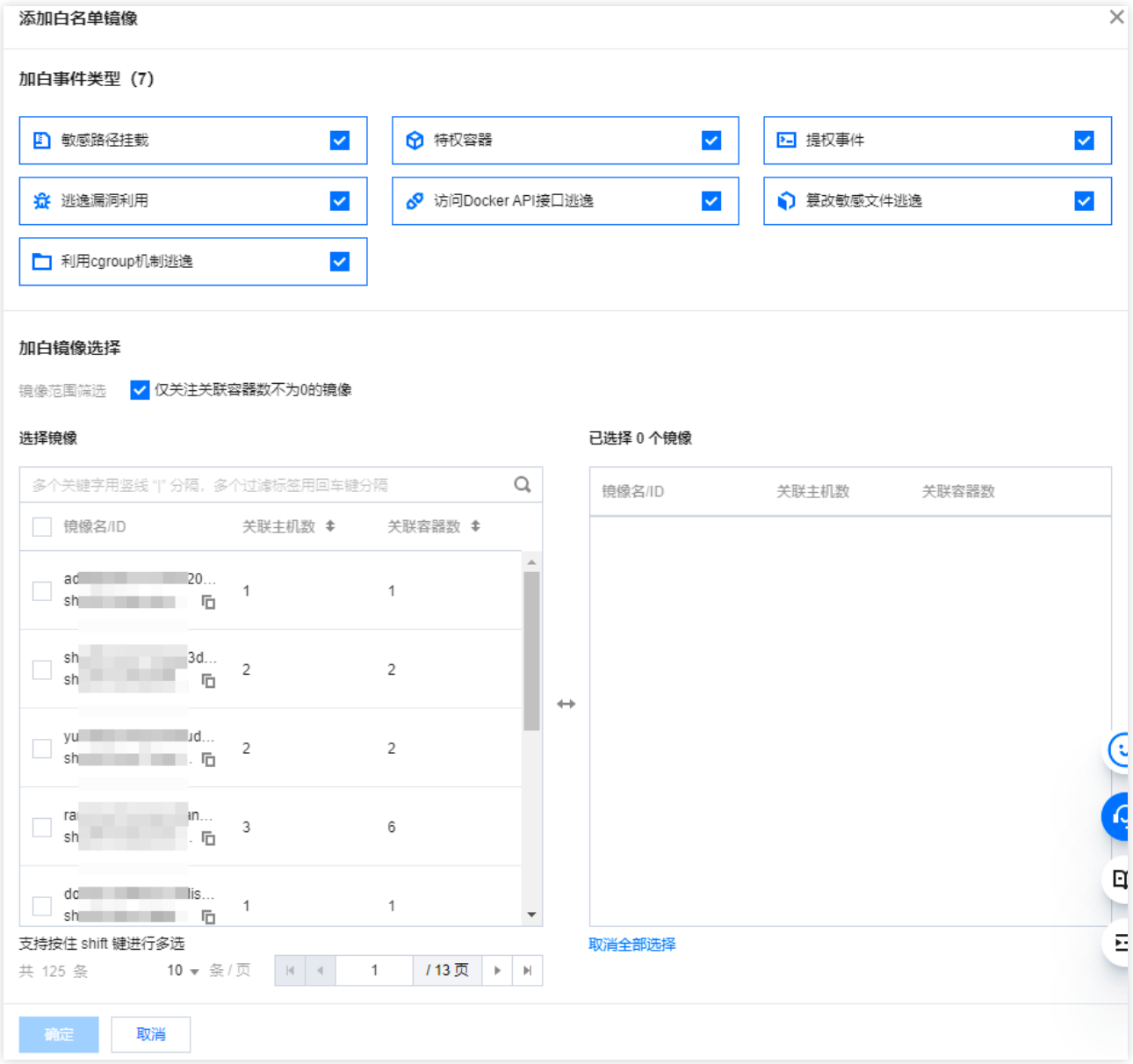
用户也可在白名单管理页面，批量新增白名单，避免后续产生告警。

### 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

1. 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。




2. 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。

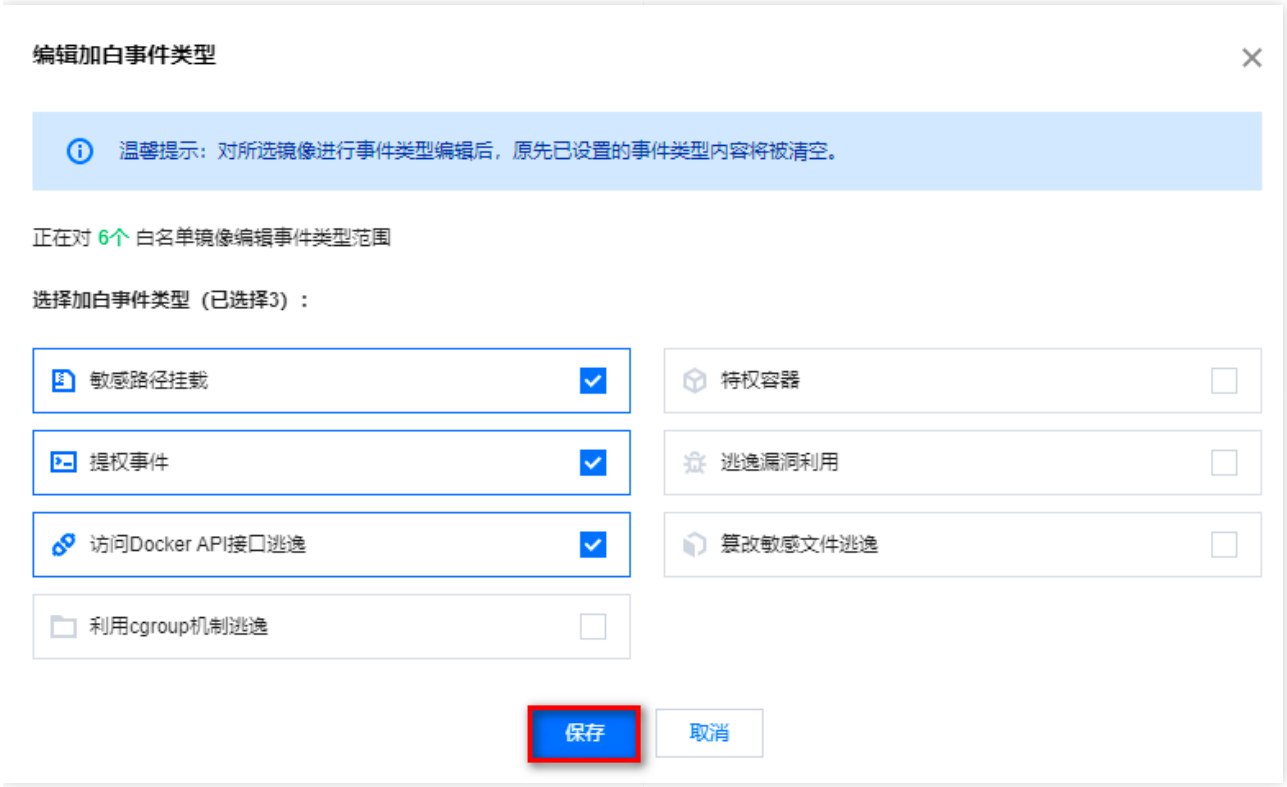



- 批量编辑白名单
  如需批量对多个镜像进行加白事件类型变更、且这些镜像需加白的类型一致，按照如下操作修改：
  - 在容器逃逸> 白名单管理页面，选择一个或多个镜像，单击左上角的编辑加白类型。




  - 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：
    >
    > 对所选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

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，单击操作栏右侧刷新图标，即可刷新反弹 Shell 事件列表。

## 导出事件列表

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

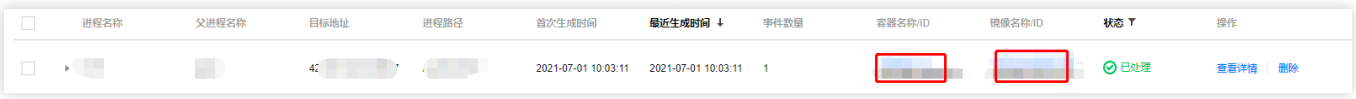
  > 注意：
  >
  > 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

# 查看列表详情

1. 在事件列表页面，单击事件类型左侧展开图标，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。




- 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。
- 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，单击设置图标，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

- 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。

- 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。

- 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。

- 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

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，单击操作栏右侧刷新图标，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，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。

- 单击目标地址左侧勾选图标，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）

- 单击连接进程左侧勾选图标，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勾选或删除图标，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。
5. 配置完成后，满足条件的目标地址和连接进程将直接放行不再告警。
6. 或选择正则加白，在正则表达式部分配置需要加白的匹配字段和匹配内容。




# 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，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。




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，单击设置图标，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

- 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。

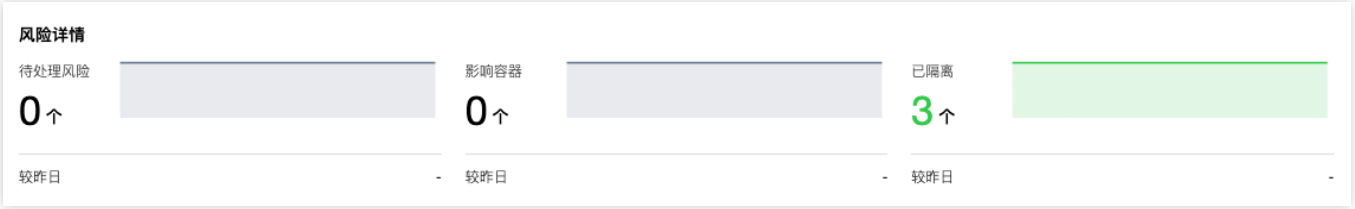
# 文件查杀

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。




## 设置风险检测

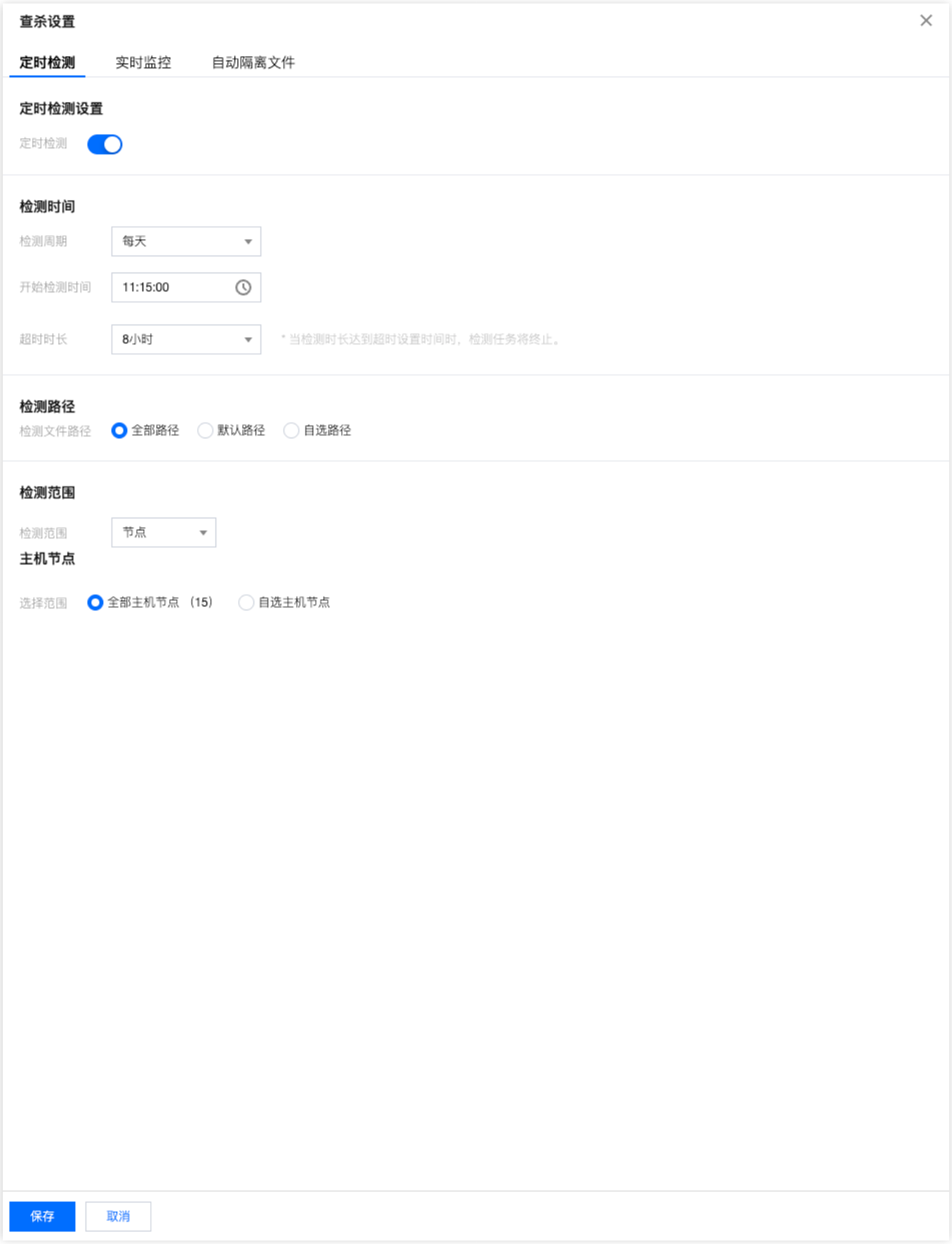
在文件查杀页面的风险检测模块，支持对定时检测和实时监控功能进行设置。

> 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，单击定时检测右侧设置按钮，进入定时检测设置页面。
2. 在定时检测设置页面，单击开启开关，开启定时检测，并依次设置检测时间、检测路径、检测范围。


查杀设置
定时检测
实时监控
自动隔离文件
定时检测设置
定时检测
检测时间
检测周期
每天
开始检测时间
11:15:00
超时时长
8小时
* 当检测时长达到超时设置时间时，检测任务将终止。
检测路径
检测文件路径
全部路径
默认路径
自选路径
检测范围
检测范围
节点
主机节点
选择范围
全部主机节点 （15）
自选主机节点
保存
取消

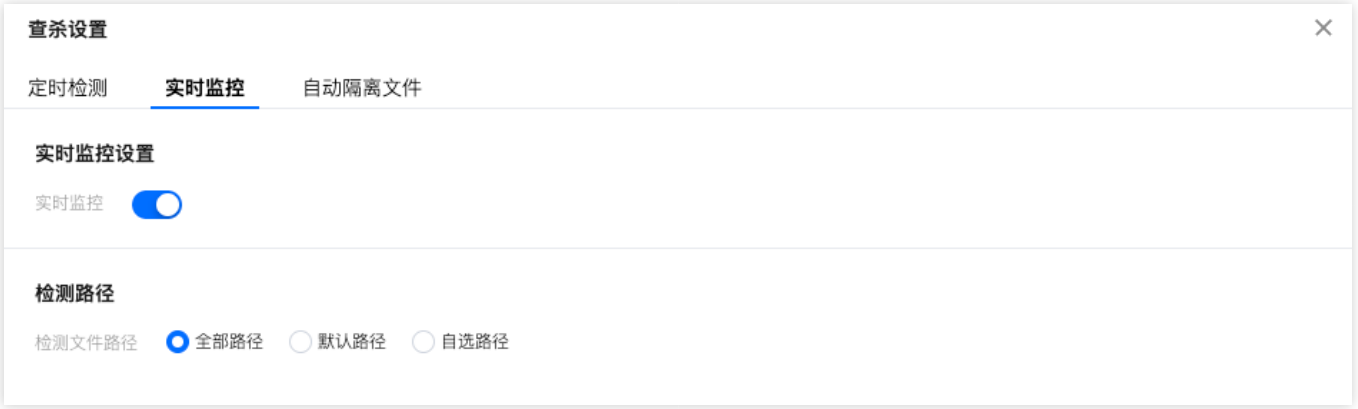
参数说明：

- 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
  - 主机节点：选择主机节点时，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编辑图标，进入实时监控设置页面。
2. 在实时监控设置页面，单击开启，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，并设置超时时间。




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。
  - 单击左侧展开图标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。

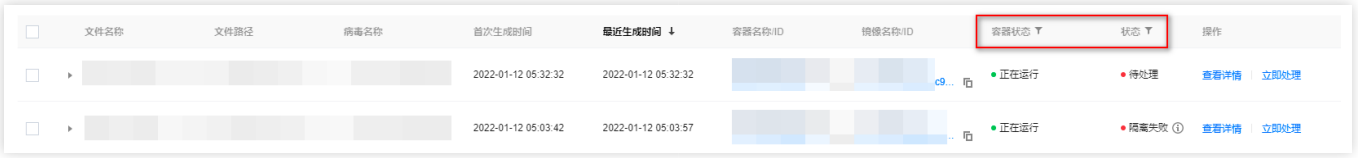
### 筛选事件

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。




- 单击容器状态或状态右侧的筛选图标，可以通过容器状态和事件状态对木马病毒事件进行查询。



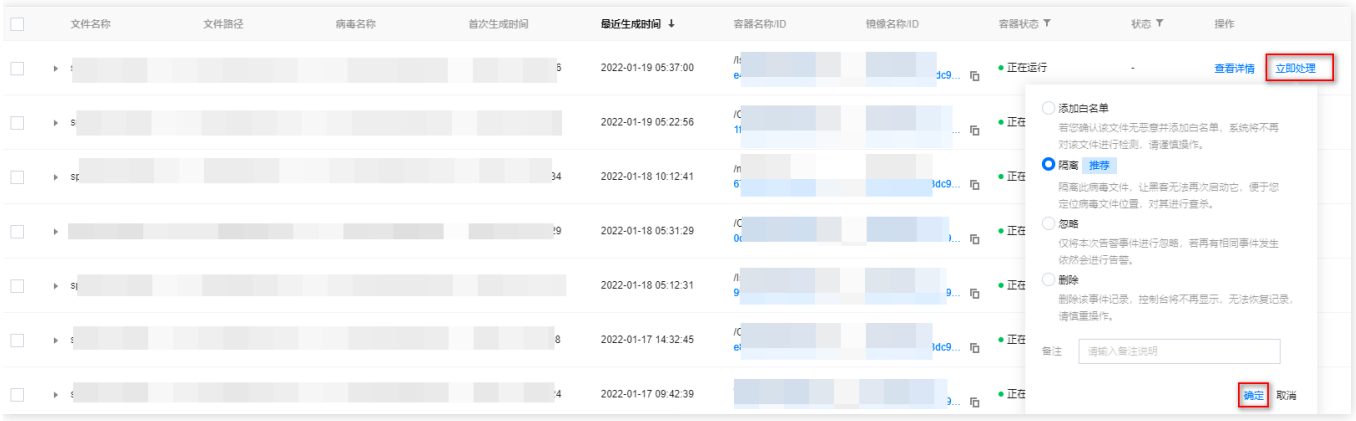

## 查看详情

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。

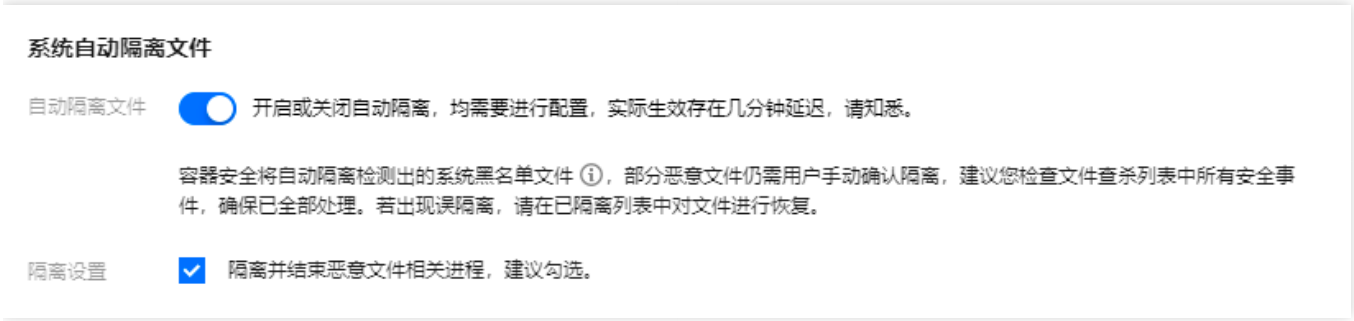
1. 登录容器安全服务控制台，在左侧导航中，单击运行时安全 > 文件查杀。
2. 在文件查杀页面，单击右上角的查杀设置。




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：容器安全运营专家与算法专家沉淀的文件名单，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。



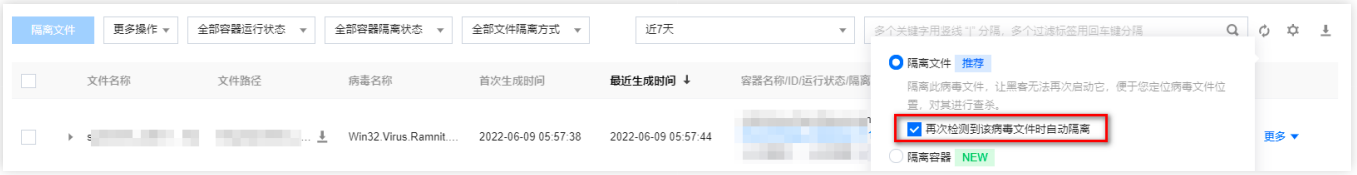

操作说明：

- 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

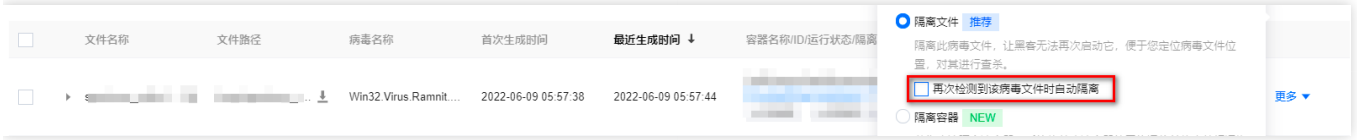
- 在文件查杀页面的事件列表中，手动隔离恶意文件时，如勾选“再次检测到该病毒文件时自动隔离”，该恶意文件的MD5值将记录在用户自定义隔离文件列表，自动隔离开关状态为开启。系统将对后续检出的同样文件进行自动隔离。当事件列表中手动隔离的恶意文件取消隔离后，用户自定义隔离文件列表中将删除该条记录，自动隔离配置也不再生

效。




- 在文件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

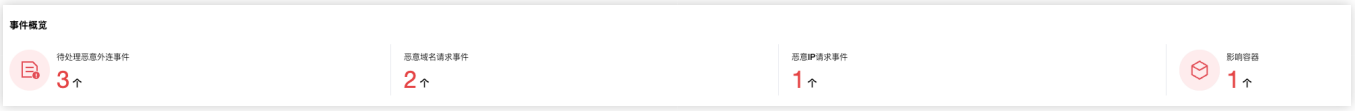
当容器向恶意域名或 IP 发起外连请求时，容器安全服务将检测此类行为，为您提供实时告警。当发现容器存在访问恶意域名/IP 的行为时，您的容器可能已经失陷，因为恶意域名/IP 可能是黑客的远控服务器、恶意软件下载源、矿池地址等。您需要及时进行如下排查：

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。 |

| 字段名称 | 字段详情 |
| --- | --- |
| 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。<br>- 单击处理对安全事件进行处理。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

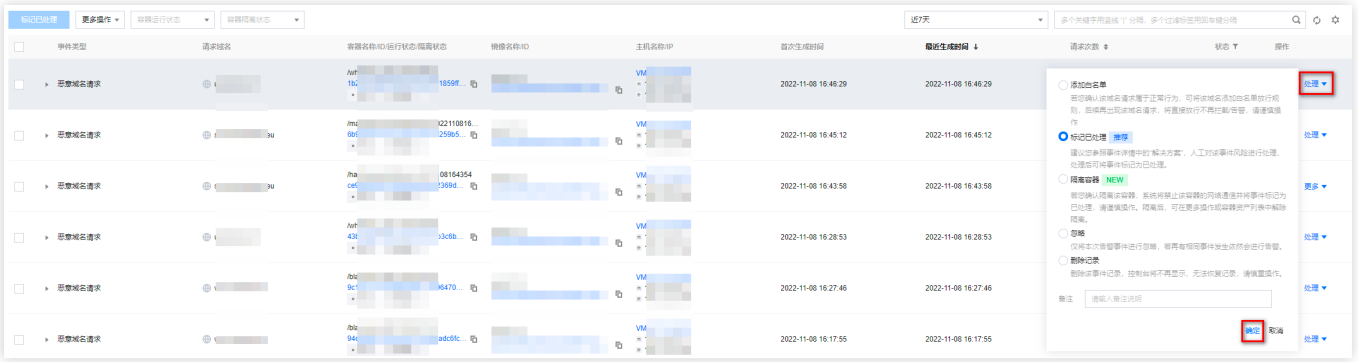
在事件列表中，单击详情，进入事件详情，展示事件详情，关联容器、镜像、主机等资产信息，风险描述，解决方案，请求域名详情和三层进程信息。


事件详情 • 待处理
标记已处理
隔离容器
更多操作
事件详情
事件类型
恶意域名请求
事件数量
1 个
首次生成时间 2022-11-02 15:20:15
最近生成时间 2022-11-02 15:20:15
容器名称/ID • 未隔离
镜像名称/ID
主机节点名称/IP
POD名称
风险描述
事件描述
发现容器存在访问恶意IP/域名的行为，您的容器可能已经失陷。
恶意IP/域名可能是黑客的远控服务器、恶意软件下载源、矿池地址等。
解决方案
建议方案
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.对容器所使用的的镜像进行加固，并替换运行中的容器。
事件详情
恶意请求域名
命中规则
用户自定义
标签特征
-
进程信息
进程权限
-rwxrwxrwx
进程MD5
进程用户
root:root
进程路径
/normal_test
进程树
进程命令行参数
-

父进程信息

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。

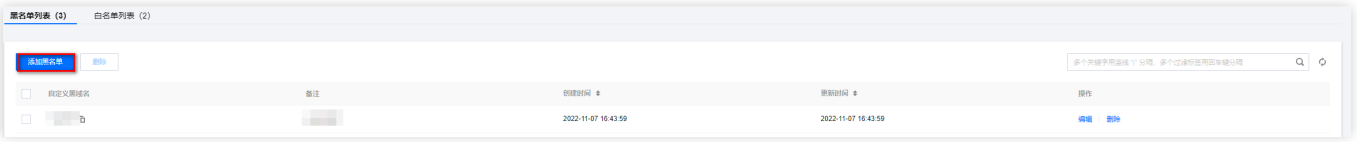
# 黑白名单管理

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 > 黑白名单管理，默认进入黑名单列表页签。
2. 在黑名单列表页签，单击添加黑名单。



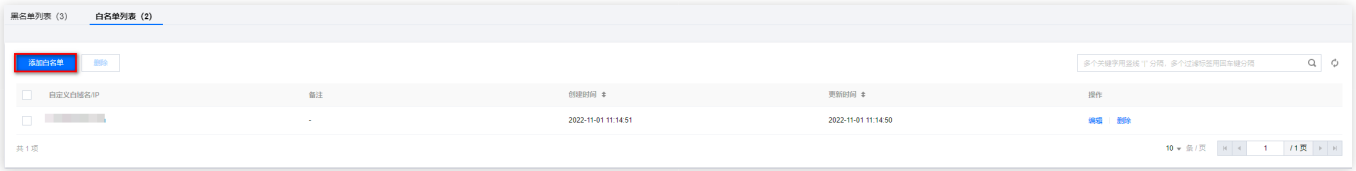

3. 在添加黑名单窗口中，可支持批量新增多个自定义黑域名；输入域名时，支持前缀置空的泛域名，例如 *.xxx.com； 泛域名下的子域名均会告警。




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 > 黑白名单管理 > 白名单列表。
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 *.xxx.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

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，包括系统规则和用户自定义规则两部分。
    - 系统规则：基于云服务商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。

# 异常进程
# 事件列表

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，单击操作栏右侧刷新图标，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，单击勾选所需的异常进程事件后，单击导出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 > 异常进程 > 事件列表，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧展开图标，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。

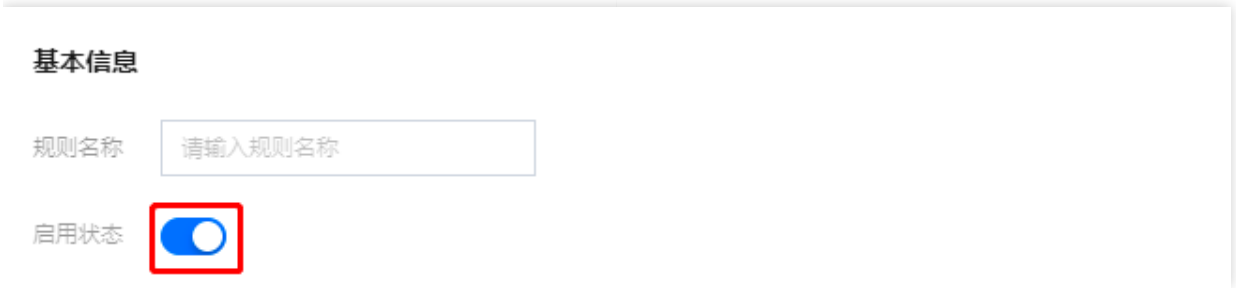
> 说明：
>
> 标记已处理、忽略和删除：相应操作处理请参考事件状态处理。

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勾选或删除图标，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，单击设置图标，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

- 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。

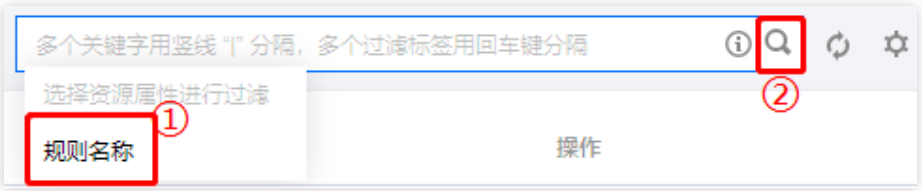
- 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。
- 事件数量：聚合时间范围内该异常进程事件触发告警的总数量。
- 动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。
- 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

# 规则配置

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。

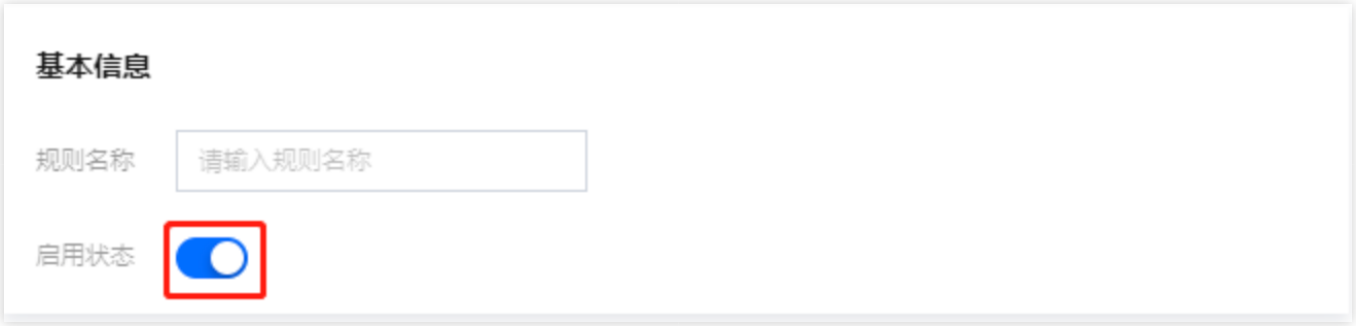



3. 在新增规则页面，需配置基本信息、配置规则和镜像生效范围。

- 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。

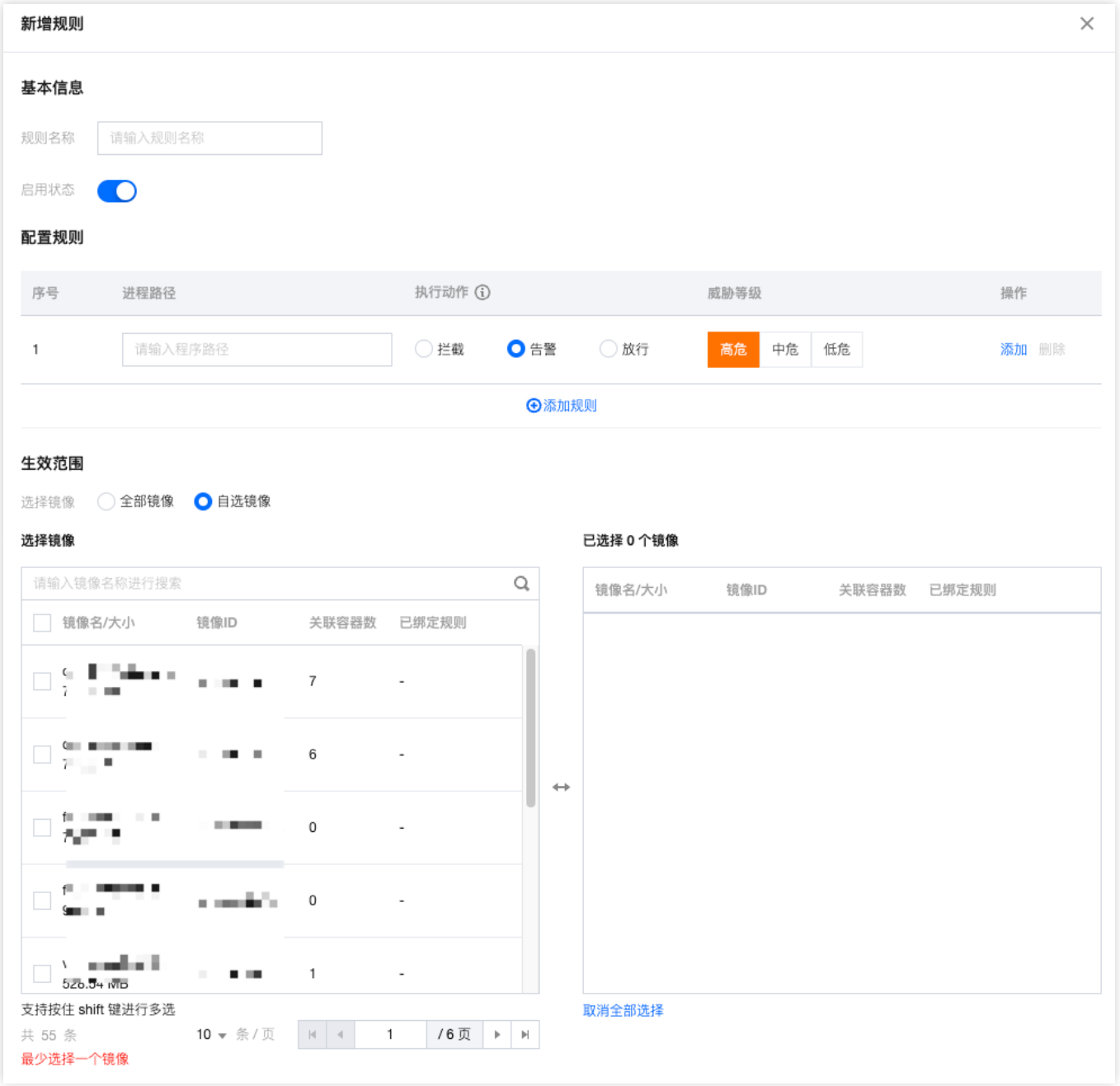
# 复制规则

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。

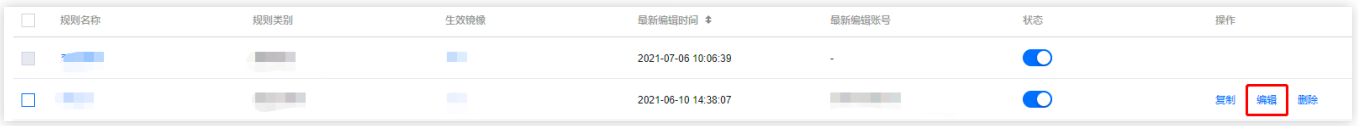



3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。
4. 选择所需内容后，单击确定或取消，即可完成或取消复制规则。




# 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。

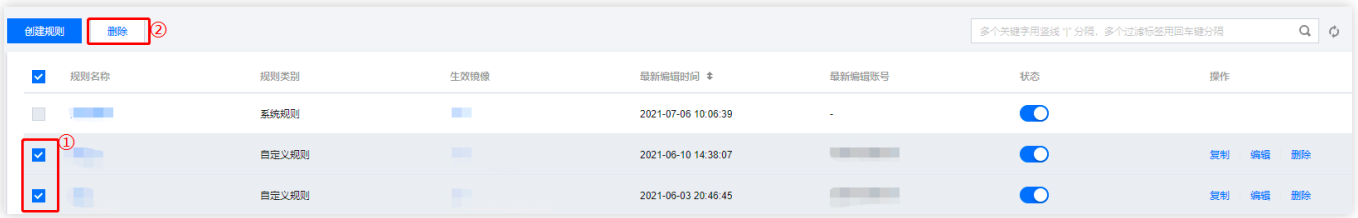



3. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。
4. 选择所需内容后，单击确定或取消，即可完成或取消修改规则。

# 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勾选图标，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。



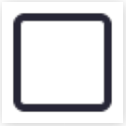

3. 在“确认删除”弹窗中，单击删除或取消，即可删除或取消删除规则。

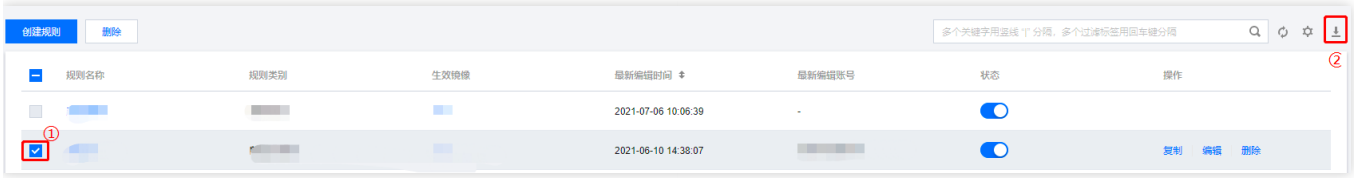
> 说明：
>
> 删除后，规则将无法恢复，该规则的关联镜像将自动关联系统默认规则。

# 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，单击勾选所需的异常进程规则后，单击导出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，单击设置图标，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

- 规则类别：系统规则或自定义规则。
- 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。




- 状态：启用/禁用。
- 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

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，单击操作栏右侧刷新图标，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，单击勾选所需的文件篡改检测事件后，单击导出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，单击进程路径左侧展开图标，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。

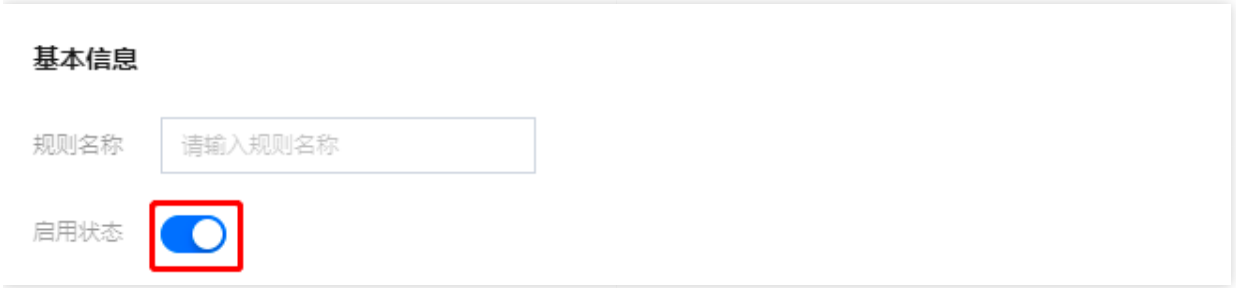
> 说明：
>
> 标记已处理、忽略和删除：相应操作处理请参考更改事件状态。

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，单击设置图标，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

- 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。
- 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。
- 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。
- 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。
- 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

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：
1、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。
2、仅支持以下指定的服务器操作系统和内核版本。

| 操作系统 | 系统版本号 | 内核版本号 |
| --- | --- | --- |
| TencentOS | 不作限制，以内核版本号为准 | 4.15.0-142-generic |
| | | 4.18.0-80.el8.x86 |
| | | 4.18.0-80.el8.x64 |
| | | 4.18.0-80.11.2.el8_0.x86 |
| | | 4.18.0-80.11.2.el8_0.x64 |
| | | 4.18.0-193.28.1.el8_2.x86 |
| | | 4.18.0-193.28.1.el8_2.x64 |
| | | 5.4.0-77-generic |
| | | 5.4.119-19.0009.56 |

## 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，单击操作栏右侧刷新图标，即可刷新规则列表。

## 新增规则

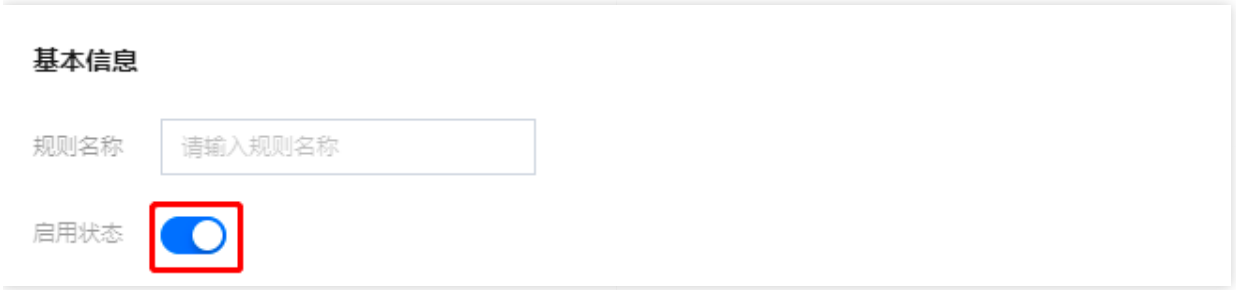
1. 登录容器安全服务控制台，在左侧导航中，单击高级防御 > 文件篡改 > 规则配置，进入规则配置页面。
2. 在规则配置页面，单击创建规则，右侧抽屉弹出新增规则页面。




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：需输入进程路径和被访问文件路径，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勾选或删除图标，即可选中或删除自选镜像。

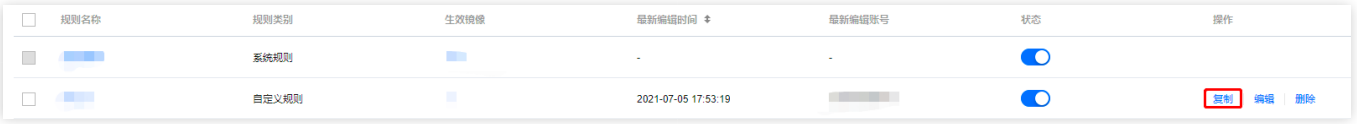
> 说明：
>
> 支持按住 Shift 键进行多选。



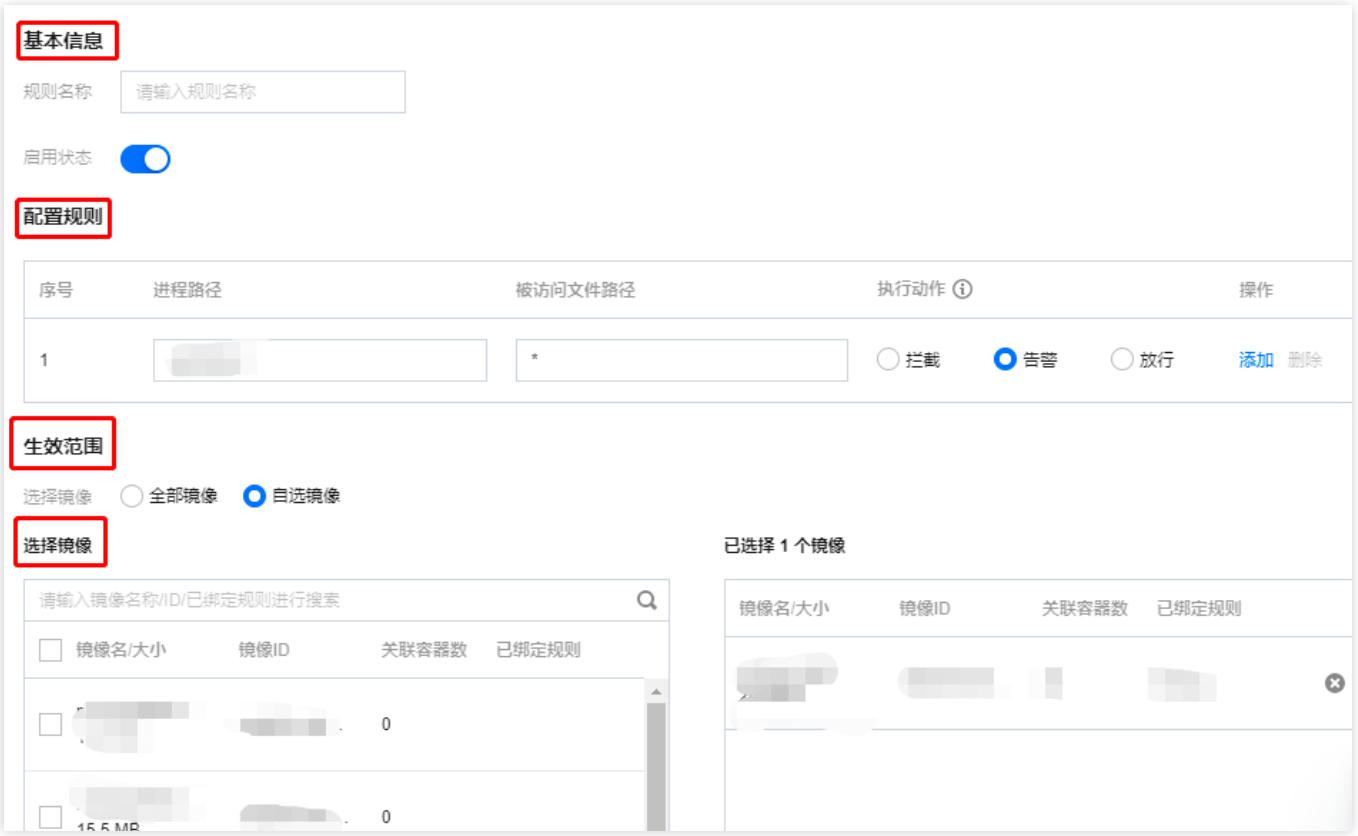

4. 选择所需内容后，单击设置或取消，即可完成或取消设置。

# 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，右侧弹出编复制规则页面。



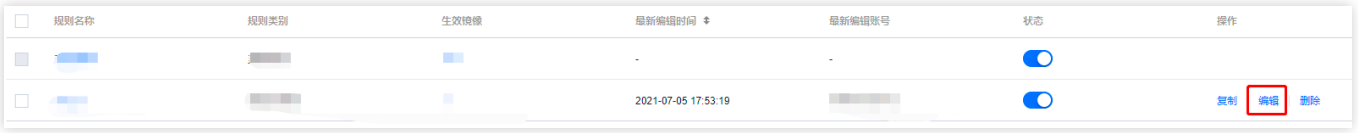

3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。



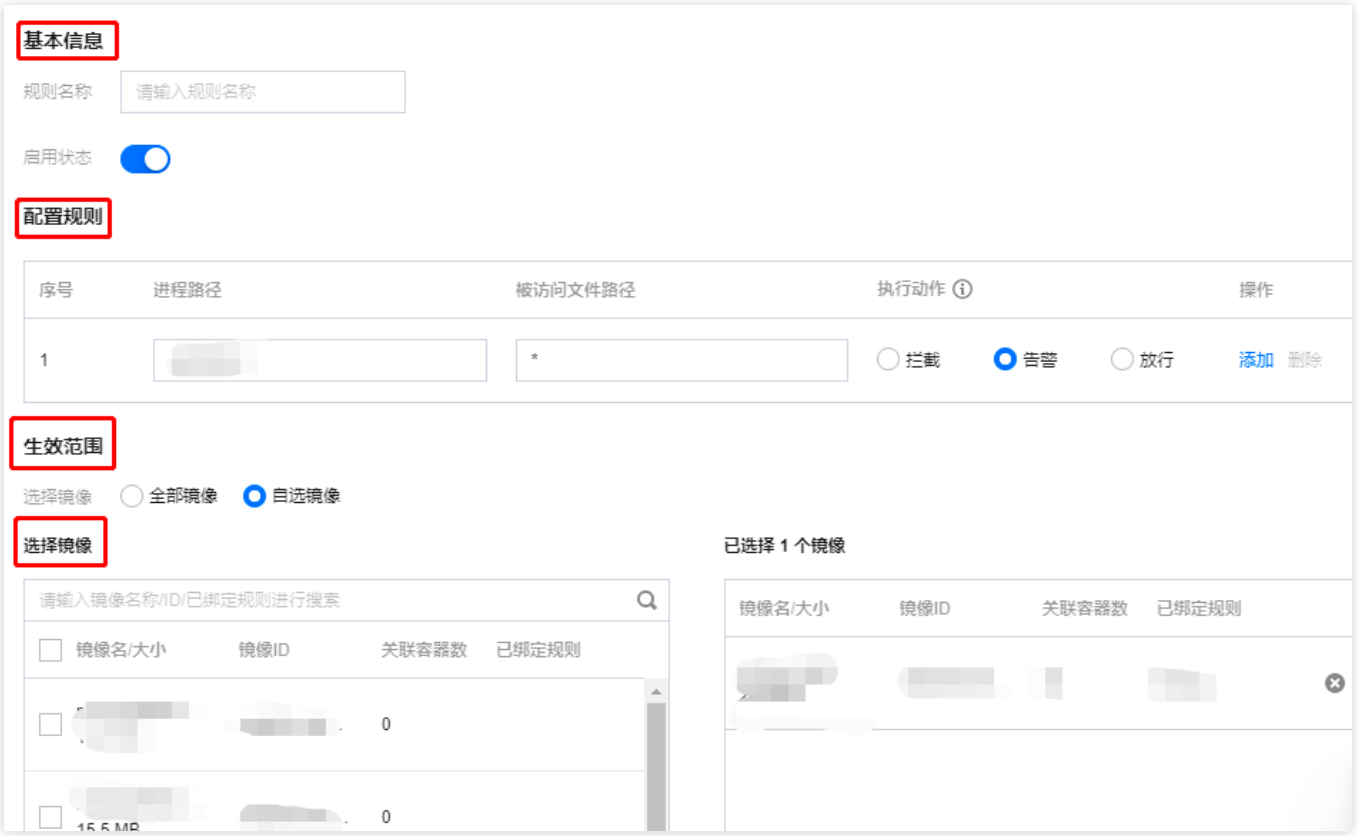

4. 选择所需内容后，单击确定或取消，即可完成或取消复制规则。

# 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勾选图标，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。

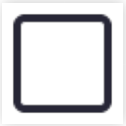


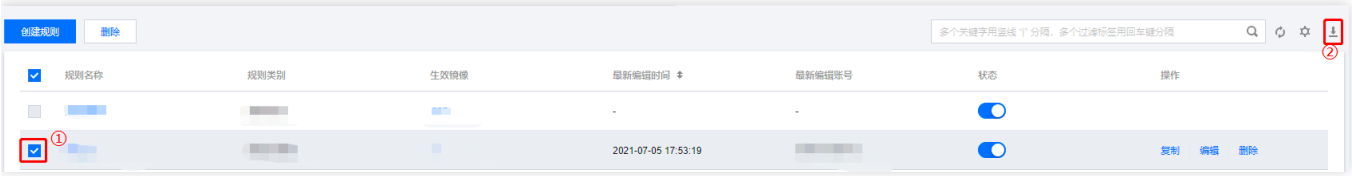

3. 在“确认删除”弹窗中，单击删除或取消，即可删除或取消删除规则。

> 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，单击勾选所需的文件篡改规则后，单击导出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，单击设置图标，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

- 规则类别：系统规则或自定义规则。
- 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。
- 状态：启用/禁用。
- 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

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，单击操作栏右侧刷新图标，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，单击勾选所需的高危系统调用事件后，单击导出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，单击进程路径左侧展开图标，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，单击设置图标，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

- 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。
- 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。
- 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。
- 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。
- 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

白名单管理展示模块中提供配置白名单接口和白名单管理列表。

## 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，单击操作栏右侧刷新图标，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勾选图标，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勾选或删除图标，即可选中或删除自选镜像。

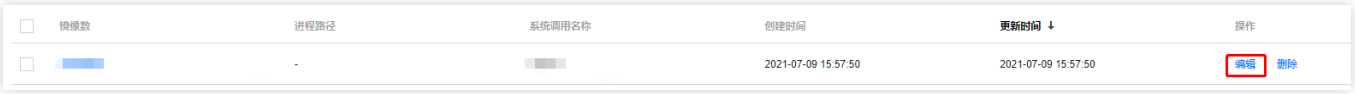
  > 说明：
  >
  > 支持按住 Shift 键进行多选。




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。



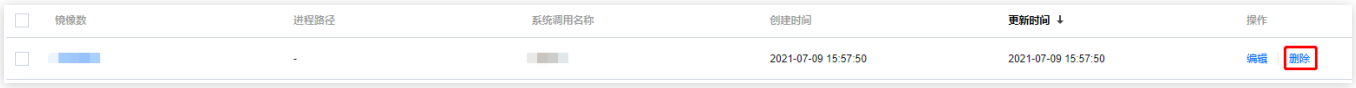

3. 在编辑白名单设置页面，可修改白名单生效的进程路径、系统调用名称和生效范围。




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。

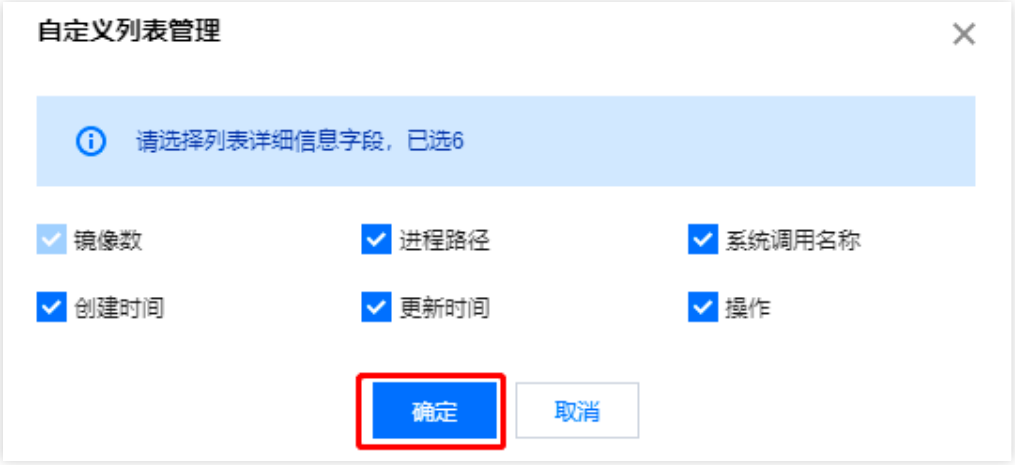



3. 在“确认删除”弹窗中，单击删除或取消，即可删除或取消删除白名单。

> 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，单击设置图标，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

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

# 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规则两部分。

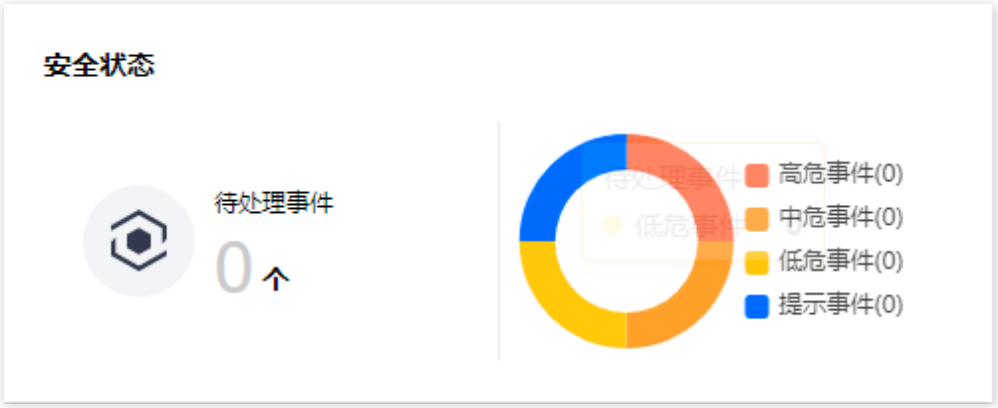
- 系统策略：基于云安全技术及多维度多种手段，通过匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 Pod 创建、可疑容器创建等共9个规则类型，对集群 API 异常请求行为进行监测。
- 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求。

## 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、提示来统计安全事件数量。




- 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。

事件详情 • 待处理

标记已处理 加白 更多操作

## 事件详情

事件类型 规则详情

**静态Pod创建**

系统规则

告警数量 356

威胁等级 低危

首次生成时间 2022-11-29 00:0...

最近生成时间 2022-11-29 15:4...

集群名称/ID • 运行中

ku

集群Master-IP

Kubernetes版本 v

运行时组件

### 风险描述

事件描述 检测到您的K8s API Server创建了静态pod，静态pod无法通过kube-apiserver进行管理，通常攻击者可利用创建静态pod的方式，运行指定的镜像。

### 解决方案

建议方案 请及时排查该创建静态pod的yaml文件是否为业务所需，非必要请勿使用静态pod。
如需删除静态pod，请直接删除静态pod的yaml文件，该文件通常与 API Server的yaml文件处于同一目录，
如：/etc/kubernetes/manifests。

异常请求信息 json日志

已为您自动高亮事件关联的异常请求信息：

操作类型verb patch

日志ID b9

Pod名称/IP




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，将直接放行不再告登，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。



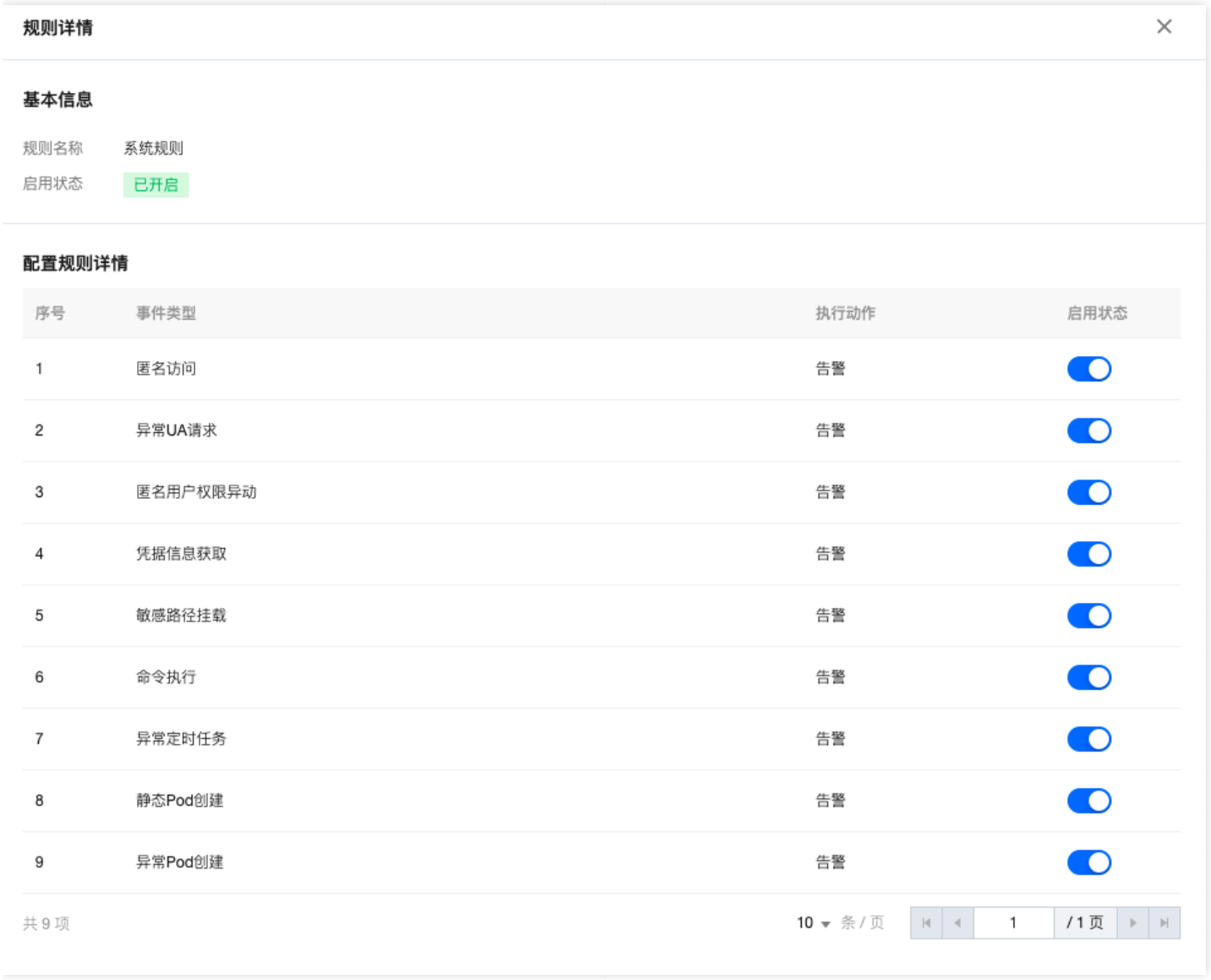

- 忽略：单击确定，仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。
- 删除记录：单击确定，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

# 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。

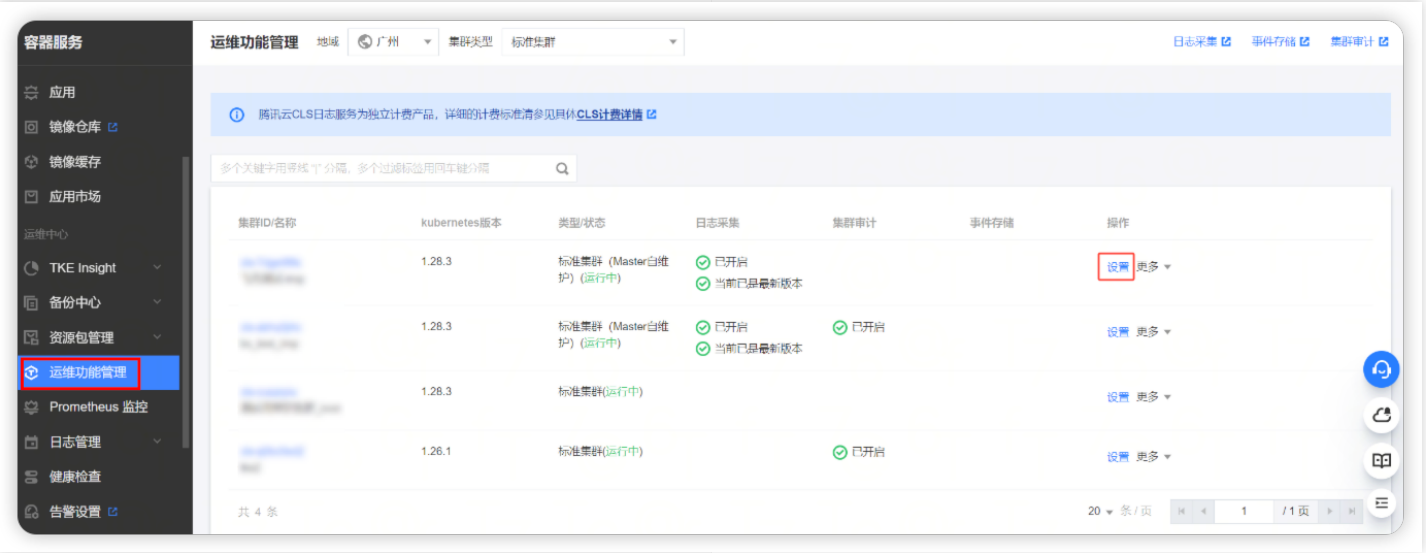

创建规则
基础设置
规则名称
请输入规则名称
启用状态
规则配置
K8s API异常请求的规则配置支持正则表达式，您可以在下方配置具体的规则匹配范围、执行动作及威胁等级。
序号
匹配范围
执行动作
威胁等级
操作
1
暂无匹配范围
告警
放行
高危
中危
低危
提示
删除
添加规则
生效范围
选择集群
全部集群
自选集群
选择集群
已选择 0 个集群
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
集群名称/ID
集群状态
已绑定规则
运行中
运行中
-
运行中
-
集群名称/ID
集群状态
已绑定规则
支持按住 shift 键进行多选
取消全部选择
共 3 条
10 条 / 页
1
/ 1 页
保存
取消

| 字段名称 | 字段详情 |
| --- | --- |

| 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。<br>- 当配置内容多条时，单击下方的添加规则即可。<br>- 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。<br>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audit流程

当集群audit未开启时，无法采集到K8s api审计日志进行风险检测。可按如下步骤进行开启。
进入容器服务控制台，在运维功能管理页面，选中需要开启audit的集群，点击设置按钮。




在设置功能页面，点击集群审计功能的编辑按钮。




勾选开启集群审计，点击确定即可。


设置功能
日志采集
编辑
日志采集
已开启
当前组件版本
1.1.15
当前已是最新版本
集群审计
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
开启集群审计
开启集群审计功能需要重启 Apiserver，建议不要频繁开关。独立集群会占用 Master 节点约1Gib 本地存储，请保证 Master 节点存储充足。
独立集群开启集群审计功能时会自动开启日志采集功能。
日志所在地域
广州
修改
日志集
自动创建日志集
选择已有日志集
日志服务CLS为TKE产生的所有审计/事件数据提供免费服务至2022年06月30日，请选择自动创建日志集，或在已有日志集中选择自动创建日志集。活动说明
确定
取消

# 策略管理
# 镜像拦截策略

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。

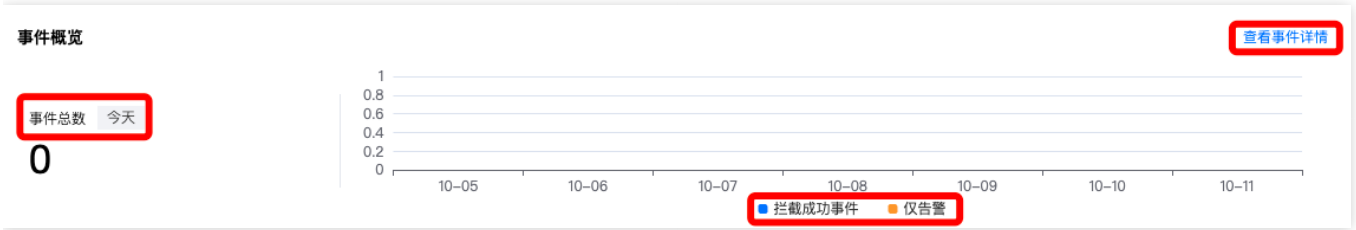
## 查看策略概览

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。单击查看事件详情，跳转镜像风险管理 > 镜像拦截事件页面查看镜像拦截事件详情。




# 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，单击确定。

> 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。

- 新建风险镜像拦截策略




| **参数类别** | **参数名称** | **参数详情** |
| --- | --- | --- |

| **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。<br>◦ 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。<br>◦ 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。<br>◦ 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。<br>◦ 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。<br>◦ 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** |
| --- | --- | --- |

| **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。<br>◦ 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。<br>◦ 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 | 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。

# 告警设置

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 | - |

## 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。

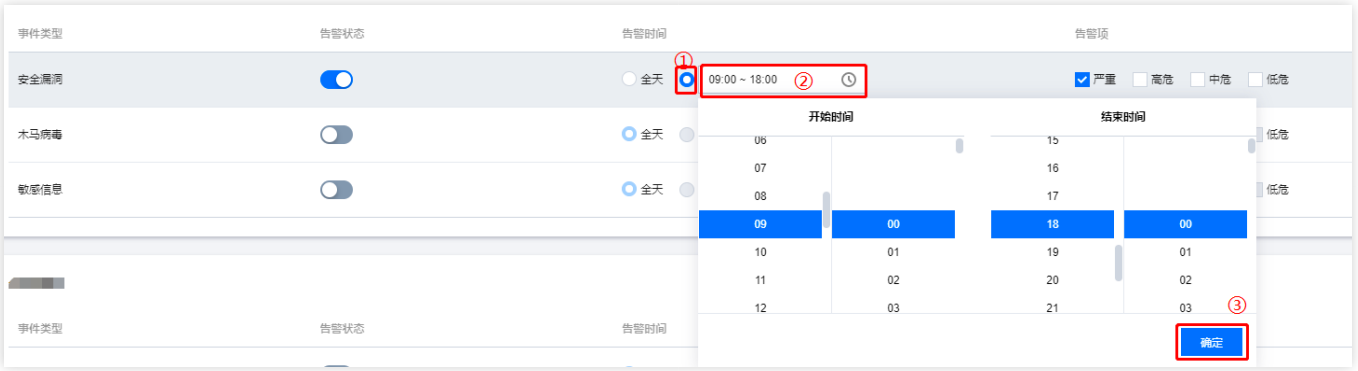



3. 开启告警设置模式后，告警时间可以单击选择全体或自定义时间。

- 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。



# 混合云安装指引
# 概述

## 背景信息

随着企业上云率提升，Overlay 云兼具公有云成本低、敏捷、灵活、使用方便及私有云可控、安全、高可用部署的优点。支持客户接入 Overlay 机器，支持接入 TKE 集群和自建集群帮助更好地用户统一管理和监控容器安全。

## 客户端支持版本说明

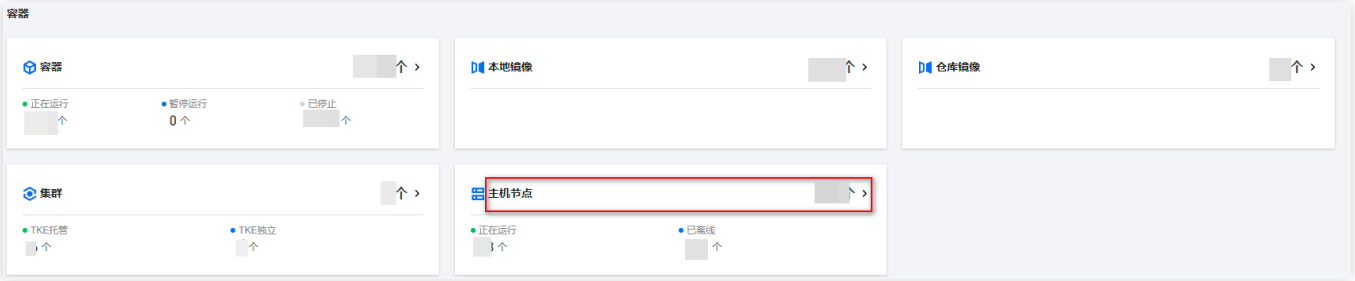
Linux 系统支持版本：

- 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Overlay云服务商机器

## 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 > 安装容器安全服务 Agent，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、服务器架构。



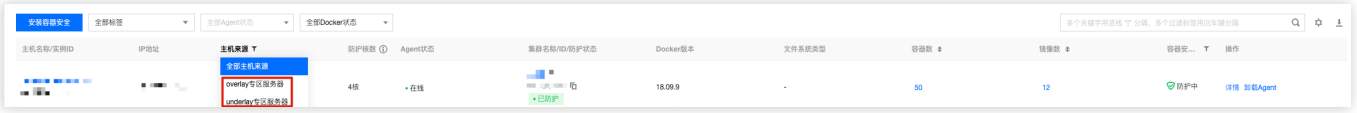

# 步骤2：确认是否安装成功

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 ，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。



# 热点问题

## 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云服务商机器？

整点自动开启新增机器的服务。

## 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云镜？

目前是的。

## Overlay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

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 | <br>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 | |
| 高危漏洞系统 | |
| 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 > 反弹Shell。
2. 在反弹Shell页面，选择所需容器，单击操作列的处理。

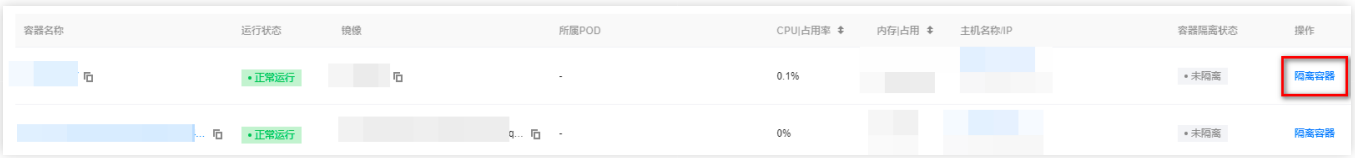


3. 选择隔离容器，并填写备注，单击确定。




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。

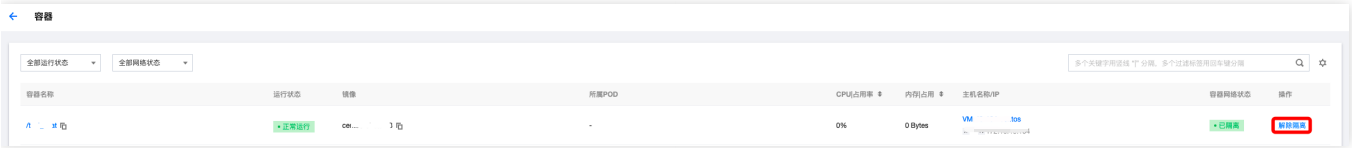



3. 在确认隔离弹窗中，单击确定，即可隔离该容器。

> 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 > 反弹Shell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，容器状态为已隔离。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筛选框，对不同隔离状态的容器事件进行筛选。



# 最佳实践
# 容器安全等保测评解读

容器安全服务（Container Security Service, TCSS）产品符合等级保护2.0标准体系主要标准。在一般测评实施过程中能够帮助企业满足容器、镜像、主机、Kubernetes 资产层面的杀毒、主动入侵防御、定期漏洞扫描等方面要求。

根据《网络安全等级保护基本要求》（GB/T 22239-2019），容器安全服务满足第三级及以下安全要求：

| 序号 | 等保标准章节 | 等保标准序号 | 等保标准内容 | 对应功能描述 |
| --- | --- | --- | --- | --- |
| 1 | 安全区域边界—入侵防范 | 8.1.3.3 b） | 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。 | 容器安全可实时监控容器内的攻击行为，对恶意命令、横向渗透、反弹 Shell 等类型的异常进程进行实时告警及拦截。 |
| 2 | 安全区域边界—入侵防范 | 8.1.3.3 c） | 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。 | 容器安全可对容器、镜像、Kubernetes 资产环境进行实时检测，对容器逃逸、集群漏洞、挖矿病毒等新型攻击行为和新型样本进行检测告警。 |
| 3 | 安全计算环境—安全审计 | 8.1.4.3 a） | 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。 | 容器安全支持对高危命令、高危操作进行审计，并支持对容器 bash 日志、容器启动日志和 K8s API 请求日志进行审计和记录。 |
| 4 | 安全计算环境—入侵防范 | 8.1.4.4 e） | 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 | 容器安全支持检测镜像及集群中存在的安全漏洞，评估风险级别并提供修复建议。 |
| 5 | 安全计算环境—入侵防范 | 8.1.4.4 f） | 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 容器安全支持检测容器内的入侵行为，主要包括容器逃逸、反弹 Shell、恶意文件、异常进程启动、文件篡改、高危系统调用等，提供告警及提高部分主动拦截能力。 |
| 6 | 安全计算环境—恶意代码防范 | 8.1.4.5 | 应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 容器安全支持恶意文件查杀功能，实时监测容器内木马病毒并支持隔离恶意文件。 |

# 镜像漏洞扫描和漏洞管理

镜像安全是容器稳定运行的必备条件，当镜像存在安全风险时，风险镜像运行的容器随时可能遭受攻击、影响线上运行业务稳定性。因此在业务上线之前，需对即将应用到的镜像进行安全风险评估，确认无风险后再投入使用。

镜像安全风险主要涉及漏洞、木马和敏感信息泄漏，其中涉及到的镜像漏洞及漏洞管理问题尤其重要。在对镜像漏洞进行扫描和管理时，主要分为两个阶段进行管理：上线前、上线后。

- 上线前：镜像存储在仓库，客户需要对仓库镜像的安全性进行保障。
- 上线后：拉取到云服务器的镜像称为本地镜像，业务方需及时评估最新漏洞、应急漏洞等是否影响到运行业务的镜像。

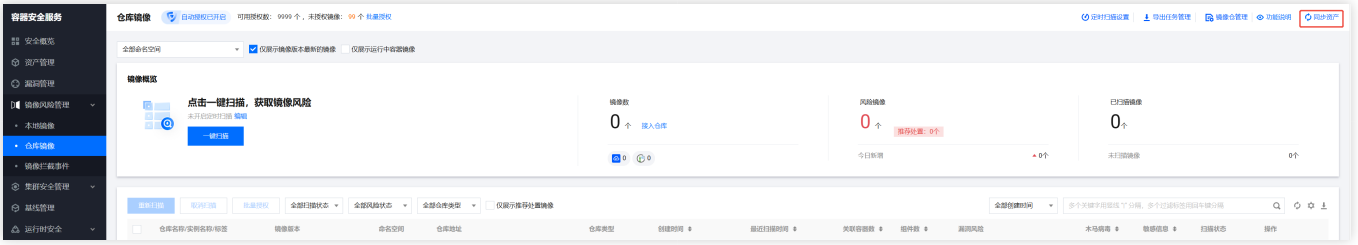
## 仓库存储阶段

镜像上线之前，客户将打包或下载好的镜像存储在仓库，入仓时需对新入仓的镜像进行整体安全评估，如存在安全问题，建议修复后再入仓管理。

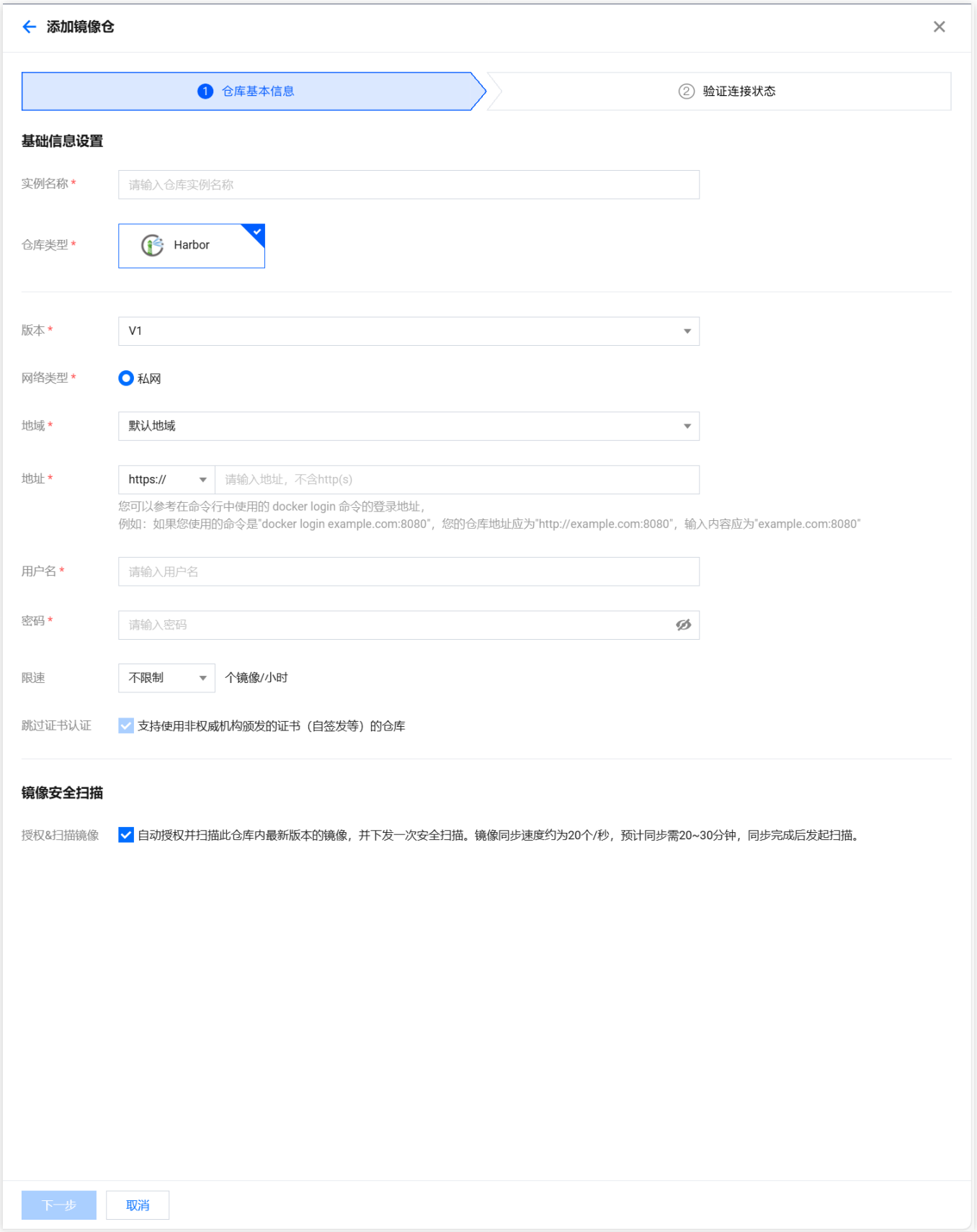
### 拉取仓库镜像

容器安全服务支持的仓库类型Harbor 镜像。

- 当有新镜像入仓时，在仓库镜像页面，单页右上角的同步资产即可更新资产。




- 当客户镜像存储在 Harbor 仓库时，客户需手动接入仓库再拉取镜像资产。在仓库镜像页面，单页右上角的镜像仓管理 > 添加镜像仓，按要求验证仓库基本信息、连接地址等即可。




## 扫描与查看仓库镜像漏洞

在仓库镜像页面，勾选自动授权并扫描此仓库内最新版本的镜像，并下发一次安全扫描。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。扫描完成，进入漏洞管理页面查看扫描出的漏洞。
如需查看全部漏洞，依次单击系统漏洞和应用漏洞，导出所有漏洞列表，在列表中查看影响仓库镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有 EXP、POC、远程利用、在野利用标签等。

- POC（Proof of Concept）：可通过一段描述或样例来证明漏洞确实存在。
- EXP（Exploit）：一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。
- 远程利用漏洞：指攻击者可以直接通过网络发起攻击并利用的软件漏洞。例如这类软件漏洞中的 RCE（远程代码执行）漏洞危害极大，攻击者能随心所欲地通过此漏洞对远端计算机进行远程控制，此类漏洞也是蠕虫病毒主要利用的漏洞。
- 本地利用漏洞：指攻击者必须在本机具有访问权限的前提下才能攻击并利用的软件漏洞。比较典型的是没有网络服务功能的本地软件漏洞，以及本地权限提升漏洞。例如本地提权漏洞能让普通用户获得最高管理员权限甚至系统内核的权限。
- 在野利用：该类漏洞存在在野利用或云平台上存在在野攻击（数据来源：we-detect 和 cisa）。

### 按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击导出图标，在列表中查看影响仓库镜像的漏洞，对存在应急漏洞的仓库镜像进行修复。

### 按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击导出图标，选择仅导出筛选结果，在列表中查看影响仓库镜像的漏洞，对存在这些标签的仓库镜像进行修复。



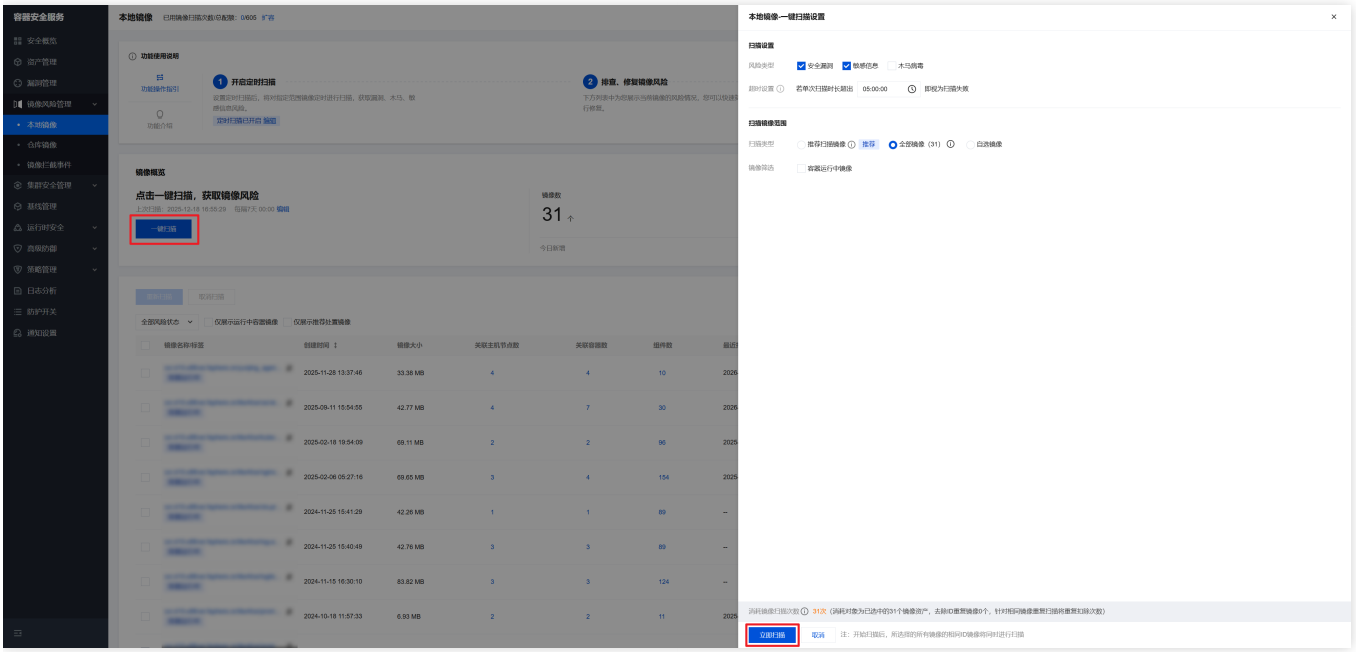

除了上述标签，客户在筛选仓库镜像漏洞时，也可利用“仅展示影响最新版本的镜像”、“威胁等级”、“CVSS”评分等条件进行综合筛选。

# 本地应用阶段

镜像安全风险问题在仓库存储阶段得到监控和修复后，在本地应用阶段则仅需关注新增漏洞的问题。本地镜像如存在严重的漏洞问题，可能直接影响线上业务。

### 扫描本地镜像

容器安全服务会在每天的资产自动更新时，默认更新云服务器上存在的镜像，无需客户手动拉取。具备足够镜像扫描次数配额即可在本地镜像页面执行扫描。



1. 在本地镜像页面，单击一键扫描，在右侧弹出的本地镜像-一键扫描设置面板中进行配置：
2. 扫描设置：选择风险类型（安全漏洞、敏感信息、木马病毒），并设置超时时间（若单次扫描时长超过设定时间则视为失败）。
3. 扫描镜像范围：推荐扫描镜像、全部镜像或自选镜像。
4. 查看面板底部显示的本次扫描将消耗的镜像扫描次数，确认无误后单击立即扫描。

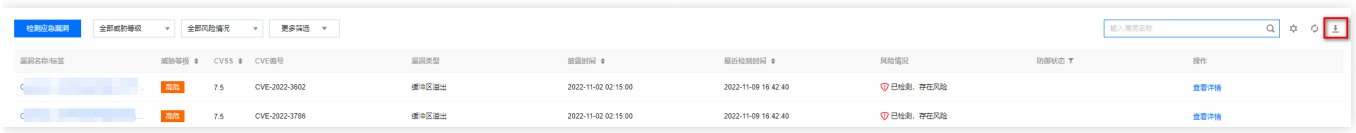
> 说明：
>
> - 本地镜像页面上方会显示当前已用镜像扫描次数/总配额，如配额不足可进行扩容。
> - 扫描即扣"镜像扫描次数"，针对相同镜像重复扫描将重复扣除次数。
> - 开始扫描后，所选择的所有镜像的相同ID的镜像将同时进行扫描。

## 查看本地镜像漏洞

扫描漏洞任务完成后，进入漏洞管理页面查看扫描出的漏洞。
如需查看全部漏洞，依次单击系统漏洞和应用漏洞，导出所有漏洞列表，在列表中查看影响本地镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有 EXP、POC、远程利用、在野利用标签等。

### 按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击导出图标，在列表中查看影响本地镜像的漏洞，对存在应急漏洞的本地镜像进行修复。



### 按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击导出图标，选择仅导出筛选结果，在列表中查看影响本地镜像的漏洞，对存在这些标签的本地镜像进行修复。




除了上述标签，客户在筛选本地镜像漏洞时，如只需查看运行容器的本地镜像漏洞时，可打开“仅展示影响容器的漏洞”开关，或在导出的漏洞列表中筛选关联容器大于0的镜像。同时也可以利用“威胁等级”、“CVSS”评分等条件进行综合筛选。

# 常见问题
常见问题

## 如何防护容器安全？

容器安全服务能通过对镜像及镜像仓库提供一键检测，支持对漏洞、木马病毒及敏感信息等多维度安全扫描，帮助用户解决防护镜像安全。同时容器安全提供容器逃逸、进程黑白名单、文件访问控制等安全功能，保护容器运行时安全，并提供安全运营日志，帮助企业实现容器安全可视化。

## 如何监控容器的健康状况？

通过容器安全服务的安全运营功能，可帮助企业实现容器安全可视化，并提供安全策略等功能，提高企业安全运营质量及效率。

## 容器安全服务和其他安全产品是否冲突？

不冲突，传统的主机安全产品仅仅对 OS（操作系统）一层有效，无法深入识别容器内的安全问题。传统防火墙主要是为了南北向业务模型所设计，无法细粒度管理到容器环境如此海量和复杂的业务。

## 容器安全服务的漏洞库多久更新一次？

容器安全服务的漏洞库，每天更新一次，容器安全服务会实时获取官方发布的漏洞信息，会在每天固定时刻将漏洞更新至漏洞库中。

## 容器安全服务支持线下及跨平台部署吗？

支持。详情请参见操作指南-混合云安装指引。

# 镜像与容器之间有什么关系？

- 镜像是一个包含程序运行必要依赖的环境和代码的只读文件，镜像是容器运行的基础。容器在启动或者创建时，依赖于镜像。不同的镜像可以构造出不同的容器，同一个镜像，我们也可以通过配置不同参数来构造出不同的容器。
- 容器是用镜像创建的运行实例。每个容器都可以被启动、开始、停止及删除，同时容器之间相互隔离，保证应用运行期间的安全。