# 容器安全卫士

## 用户使用指南

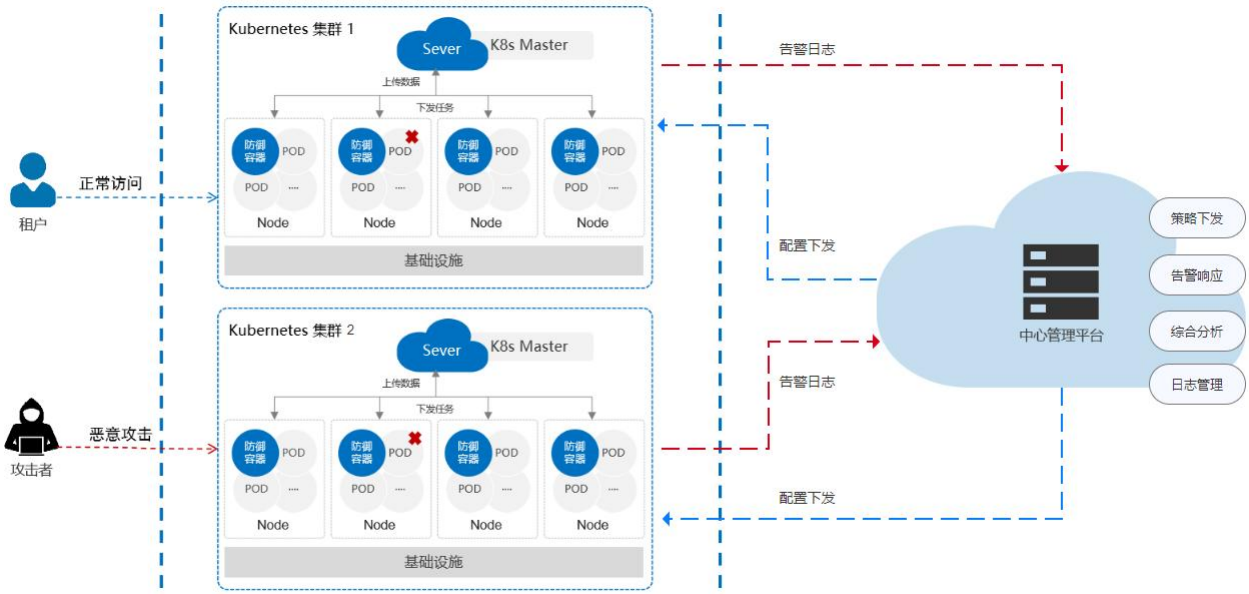
天翼云科技有限公司

# 目 录

# 1. 产品介绍

## 1.1. 产品定义

容器安全卫士是作用于容器集群的安全防护产品，提供了对容器环境下，业务动态及静态安全风险的事前发现、事中预警、事后溯源的安全闭环。可方便快捷的解决业务容器化后带来的安全问题。




容器安全卫士产品主要安全能力包括：深度资产清单、实时风险发现、快速安全防护、及时事后溯源：

- 深度资产清单

  对容器集群等基础资产可进行自动清点，在此基础上，还会进一步识别容器进程、容器挂载、容器端口、容器软件等深度资产信息，并会进行全资产的关联，便于分析。

- 实时风险发现

  针对静态风险，会识别漏洞、恶意文件、软件许可、风险软件、敏感信息等全面的风险。针对动态风险，采用触发式的方式，实时监测业务产生的所有行为，并进行智能研判，快速预警。

- 快速安全防护

  基于相关能力可快速定位风险影响范围，同时提供详细的风险信息，帮助用户对风险进行判断，确定风险后，可立即进行加白、隔离等快速安全防护处置。

- 及时事后溯源

由于容器特性，在容器消逝后，运行过程中的行为数据不再保留。容器安全卫士不但会记录正在运行业务的容器及相关信息，对已经消逝的容器也会对其详细行为信息进行保留，以防止事后发现安全事件无法溯源的问题。

## 1.1. 基本概念

- 容器：容器（Container）是一个视图隔离、资源可限制、独立文件系统的进程集合。它类似于虚拟机，但更轻量，可以在应用程序之间共享操作系统。“视图隔离”是指能够看到部分进程以及具有独立的主机名等；控制资源使用率则是可以对内存大小以及 CPU 使用个数等进行限制。常见的容器引擎包括 Docker、Containerd 等。
- 镜像：镜像（Image）是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源等文件外，还包含了一些为运行准备的配置参数（如环境变量）。镜像是容器的模板，而容器是镜像的实例。镜像是静态的，而容器是动态的。仓库镜像是指存储在镜像仓库内的镜像，节点镜像是指存储在集群节点上的镜像。
- 仓库：仓库（Repository）是集中存储和分发容器镜像文件的场所，分为公共仓库和私有仓库。
- 集群：集群特指容器集群，即 Kubernetes（简称 k8s）集群或基于 Kubernetes 衍生的企业定制版（例如 Openshift 集群），由一套 Kubernetes 系统管理的多台服务器形成一个集群。Kubernetes 是一个容器的编排和管理系统，提供服务发现、弹性伸缩、负载均衡、故障自愈等功能。Kubernetes 将集群中的服务器划分为 Master（控制节点）和 Node（计算节点）。其中，在 Master 节点运行着集群管理相关的一组进程，例如 etcd、kube-apiserver、kube-controller-manager 和 kube-scheduler，这些进程实现了整个集群的资源管理、Pod 调度、弹性伸缩、安全控制、系统监控和纠错等管理能力，并且都是全自动完成的。Node 作为集群中的计算节点，运行上层业务应用程序，在 Node 上 Kubernetes 管理的最小运行单元是 Pod。Node 上运行着 Kubernetes 的 kubelet、kube-proxy 服务进程，这些服务进程负责 Pod 的创建、启动、监控、重启、销毁以及实现软件模式的负载均衡器。
- 节点：节点是容器集群组成的基本元素。节点取决于业务，既可以是虚拟机，也可以是物理机。每个节点都包含运行 Pod 所需要的基本组件，包括 Kubelet、Kube-proxy 、Container Runtime 等。
- 命名空间：命名空间（Namespace）是 Kubernetes 提供的一种机制，可以将同一集群中的资源划分为相互隔离的组。同一命名空间内的资源名称要唯一，但跨命名空间时没有这个要求。在实际使用时可以为不同的用户、租户、环境或项目创建对应的命名空间，例如为 test、dev、pro 环境分别创建各自的命名空间。
- Pod：在 Kubernetes 中，Pod 是能够创建、调度和管理的最小部署单元，是一组容器的集合，而不是单独的应用容器。同一个 Pod 里的容器共享同一网络命名空间、IP 地址及端口空间。和一个个独立的应用容器一样，Pod 也被认为是相对临时性（而不是长期存在）的实体。Pod 会被创建、赋予一个

唯一的 ID（UID），并被调度到节点，并在终止或删除之前一直运行在该节点。如果一个节点失效，调度到该节点的 Pod 也会在给定超时期限后删除。

- 工作负载：工作负载是在 Kubernetes 上运行的应用程序。Kubernetes 提供 Deployment、StatefulSet、DaemonSet 等多种内置的工作负载资源类型。
- Service：Service 是 Kubernetes 中的一个重要概念，主要是提供负载均衡和服务自动发现。当一个 Service 资源被创建后，将会分配一个唯一的 IP（集群 IP），这个 IP 地址将存在于 Service 的整个生命资源，Service 一旦被创建，整个 IP 无法进行修改。
- Ingress：Ingress 资源对象用于对外暴露服务，实现从外部对 Kubernetes 集群中服务的访问，该资源对象定义了不同域名及 URL 和对应后端服务（Kubernetes Service）的绑定。
- Endpoint：Endpoint 是 Kubernetes 集群中的一个资源对象，存储在 ETCD 中，来记录一个 Service 对应的所有 Pod 的访问地址。
- Secrets：Kubernetes 中 Secrets 用于存储和管理一些敏感数据，比如密码、token、密钥等敏感信息。它把 Pod 想要访问的加密数据存放到 ETCD 中，然后用户可通过在 Pod 的容器里挂载 Volume 的方式或者环境变量的方式访问 Secret 里保存的信息。
- PV 和 PVC：Kubernetes 为了能更好地支持有状态应用的数据存储问题，还提供了 PV、PVC 和 StorageClass 资源对象来对存储进行管理。PV 的全称是 Persistent Volume（持久化卷），是对底层数据存储的抽象，PV 由管理员创建、维护以及配置。PVC 的全称是 Persistent Volume Claim（持久化卷声明），我们可以将 PV 比喻为接口，里面封装了我们底层的数据存储，PVC 就是调用接口实现数据存储操作，PVC 消耗的是 PV 的资源。
- 标签：标签 Label 是用于区分工作负载、Pod、Service、RC 等资源对象的 key/value 键值对，每个资源对象可以有多个 Label，但是每个 Label 的 key 只能对应一个 value。
- 软件包：软件包（SoftWare Package）是指具有特定功能，用来完成特定任务的一个程序或一组程序，可分为应用软件包和系统软件包两大类。
- 进程：进程（Process）是计算机中的程序关于某数据集合上的一次运行活动，是系统进行资源分配和调度的基本单位，是操作系统结构的基础。在当代面向线程设计的计算机结构中，进程是线程的容器。程序是指令、数据及其组织形式的描述，进程是程序的实体。
- 端口：“端口”是英文 port 的意译，可以认为是设备与外界通讯交流的出口。这里指的是虚拟的容器端口和节点端口，暴露这些端口以供外部访问，如容器的 80 端口。
- 运行应用：运行应用指的是运行在容器上的应用，包括 Web 服务、数据库、中间件等应用类别。
- 软件框架：软件框架（software framework），指的是为了实现某个业界标准或完成特定基本任务的软件组件规范，也指为了实现某个软件组件规范时，提供规范所要求之基础功能的软件产品。框架的功能类似于基础设施，与具体的软件应用无关，但是提供并实现最为基础的软件架构和体系。
- Web 站点：Web 站点是网站 Web 服务（Web Service），是基于 XML 和 HTTPS 的一种服务，其通信协议主要基于 SOAP，服务的描述通过 WSDL、通过 UDDI 来发现和获得服务的元数据。

- Web 服务：Web 服务是一种面向服务的架构的技术，通过标准的 Web 协议提供服务，目的是保证不同平台的应用服务可以互操作。
- Routes：Routes 是 OpenShift 中的推荐方式。它使用唯一的 URL 公开服务，是为了解决从集群外部（就是从除了集群节点以外的其它地方）访问服务的需求。Routes 路由匹配客户端的请求规则，匹配成功后分配到 Service 层。一个路由指向一个 Service，一个 Service 可以被多个不同规则的路由指向。
- Service Account：Service Account（服务账号）通常是指在计算机系统、云服务或网络中用于标识和管理服务实体的账户。

## 1.2. 功能特性

通过容器安全卫士服务，可以轻松应对各种云原生应用威胁和风险。功能特性如下：

### 仪表盘

仪表盘通过图标可视化方式展示了镜像、容器、节点、镜像仓库、集群这些重要资产的数量统计信息、部署安全信息、以及安全威胁分布情况。可以更直观地显示各资产信息统计、漏洞信息统计、报警信息。使客户能够更快速的识别和了解威胁情况。

- 趋势和历史记录

  提供可视化的界面和报告，以展示威胁情报的相关统计数据、趋势等信息，帮助决策者理解威胁情报的现状和趋势。

- 告警和事件管理

  集成告警和事件管理系统，将安全事件和告警信息汇总展示在大屏幕上，并提供快速的事件处理和跟踪功能。

- 资产管理

  展示每个资产的详细信息，包括集群资产、节点资产、命名空间、工作负载等资产，以帮助用户全面了解资产的特征和配置。

- 漏洞数据集成和可视化

  将漏洞扫描结果数据进行集成，以可视化的方式展示漏洞分布、统计信息，帮助用户全面了解漏洞态势。

## 告警响应中心

系统实时监控容器的运行情况，能够对可能出现的所有异常行为进行捕获和发出告警，并针对不同的入侵行为给出响应的安全处理建议，可在响应中心中查看所有入侵事件具体信息。并支持在响应中心对不同状态的容器进行相应的操作改变其状态，包括：解除隔离、启动容器、隔离容器、杀容器、暂停容器、一键封堵。

- 支持多种风险行为监测

  支持检测诸如启动特权容器、容器逃逸行为、读取敏感文件、启动恶意进程、挂载非法设备、映射敏感目录、反弹 SHELL 连接操作、修改命名空间等多种风险行为的检测。

- Pod 隔离

  支持对 Kubernetes 集群内 Pod 之间的通信进行网络隔离控制。

- ATT&CK 模型视角展示

  基于攻击者视角显示攻击各阶段信息，反映了攻击者攻击生命周期以及各个攻击阶段的目标。

- 一键封堵

  当生产环境内出现异常 IP 可通过一键封堵功对 IP 进行封堵，防止造成更大的损害。

## 镜像安全

镜像作为容器运行的基础，如果存在安全隐患、风险问题，将直接影响到容器环境的安全性。面对镜像中可能存在的安全问题，需要对业务环境主机中和镜像仓库中的镜像资产，进行自动扫描或手动扫描来识别风险，对危险镜像基于策略进行阻断，对高危镜像提供可写入 dockerfile 的修复建议。支持对容器镜像制作过程、镜像运行、镜像发布进行全方位的监控和检测。提供了自动获取节点和仓库中的镜像并从 CVE 漏洞、CNNVD 漏洞、木马病毒、可疑历史操作、敏感信息泄露、以及是否是可信任镜像等多个维度对镜像进行扫描。

- 镜像运行风险识别与处理

  能够设置镜像运行的安全策略，不符合安全策略的镜像将禁止运行，安全策略包括不允许以 root 用户启动、禁止镜像中存在木马病毒、阻止存在特定软件漏洞的镜像等。

- 支持多种镜像仓库的适配

  面对不同的客户使用场景，平台支持同步 Harbor、JForg、Huawei、Registry 等多种镜像仓库适配。

- 快速的镜像扫描

  镜像扫描速度快，结果准确，10G 镜像仅需 10 秒。

- 深入的镜像文件与软件包检测

在快速扫描的基础上增加扫描第三方依赖库、Web 框架库和病毒木马等恶意文件检测，更加深入地保证镜像资产的安全。

- 支持一键生成镜像报告

  镜像扫描完成后，用户可以一键生成镜像的合规检测报告，便于用户查看风险信息总览、风险镜像列表、漏洞列表、风险修复建议等信息。

- 安全溯源

  实时检测镜像历史中引入的安全风险信息，包括镜像层的构建命令、操作时间、引入的安全问题等信息。

## 容器安全

容器运行时的安全状况是容器安全管控的重中之重。目前传统的入侵检测方式主要针对于主机或者网络层面，现有手段无法快速发现针对容器层面的入侵行为。而传统云平台提供的管理平台虽可查看容器状态并进行容器隔离，但无法针对随时可能出现的异常行为进行持续监控与实时报警。若无法设置预警与实时报警，入侵者极有可能通过漏洞远程操作容器执行命令实现入侵，从而导致重要数据泄露。

支持对容器内行为进行检测。当发现容器逃逸行为、读取敏感信息、启动恶意进程、挂载非法设备、映射敏感目录、修改命名空间等恶意行为时，根据预设策略触发报警或阻断容器运行，并对发现异常的 Pod 进行隔离。

- 支持自定义策略设置

  根据用户的生产场景支持对集群、命名空间、节点等维度设置检测规则。

- 容器文件保护

  通过对容器内文件读写行为的学习，创建容器内文件读写行为的白名单，并以此识别所有异常读写容器内文件的行为，并及时发送报警。

- 数据取证

  对容器运行进程进行监控并记录，在追溯风险行为来源时能够快速查找攻击源头，及时排错。

- 容器运行时监控

  支持实时检测运行中的容器 CPU 占用、内存占用情况。

## 节点安全

集群部署后，运维人员需时刻关注集群内的 master 节点与 node 节点的在线情况，以及是否存在安全风险。针对存在安全风险的节点，需支持将风险信息生成报表，交由安全部门处理，保证节点上的资产安全运行。

- 节点入侵检测

支持对节点入侵事件的实时监测，包括主机反弹 Shell、高危系统调用等。

- 节点扫描

  支持设置扫描周期，按时扫描节点上的软件包是否存在漏洞，并给出修复建议。

- 支持自定义开启/关闭节点防护

  支持自定义开启或关闭对节点的防护，关闭防护后当前节点上的所有资产将不再受保护。

## 1.3. 产品优势

容器安全卫士对云原生应用进行多维度检测和防护，产品优势如下：

### 一键管理-便捷

贴合云原生特点，全组件采用容器化部署，实现客户端一键部署、一键卸载。安全能力随业务集群变动自动跟随防御，无需人工干预。

### 全面完整-专业

集成国际、国内、官方等多种漏洞源，基于小红伞、ClamAV、自研等多种病毒引擎，为您提供专业的安全风险检测。

### 动静结合-智能

采用静态动态双结合的检测方式，自动形成业务行为基线，基于学习引擎，实时发现未知安全风险，实现智能化防护。

### 全链加密-安全

容器安全卫士各个组件交互过程中，全链采用加密传输，敏感数据加密存储，客户端不暴漏任何端口，保护您的同时也注重自身安全。

# 1.4. 应用场景

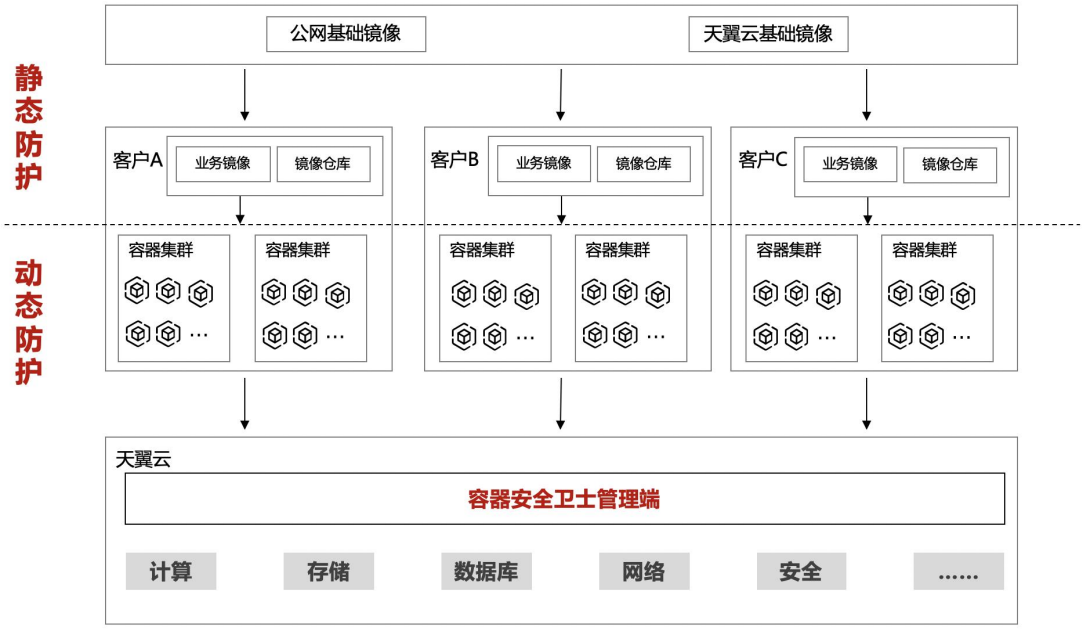
## 场景一：镜像安全防护

采用容器技术后，业务容器基于镜像启动。如何在业务上线前提前感知镜像安全风险，保障安全上线变得尤为重要。

**方案优势**

- 兼容性强：兼容市面主流镜像仓库，以及主流操作系统，包括国产化欧拉、麒麟等国产镜像 OS。
- 检测全面：基于多漏洞源以及病毒库，深入检测软件成分、漏洞、恶意文件、软件许可、敏感信息等安全风险。
- 风险阻断：针对风险镜像，可基于特权启动、漏洞、软件、文件、环境变量等多维度阻止其上线运行。

**场景示意图**



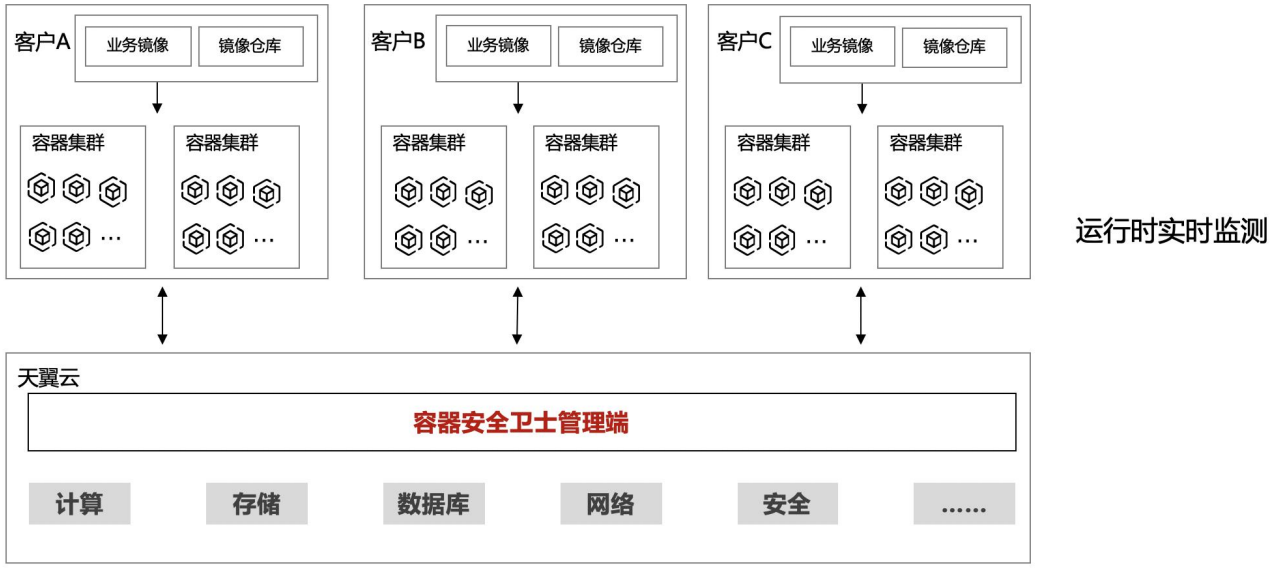

## 场景二：容器安全防护

容器内承载的即是业务进程，一旦容器被攻陷，或基于业务逻辑攻击进入容器，都将面临不可预估的风险，所以在享受容器带来便利的同时，也要加强关注容器及业务的安全性。

**方案优势**

- 覆盖 ATT&CK 全阶段：提供业务命令执行、文件读写、网络活动、主机风险等多个维度的安全检测策略，且可自定义。覆盖 ATT&CK 各个阶段，确保风险及时发现。
- 资产/风险联动性强：通过任一资产，都可查看其关联的其他资产，在发现风险时，也会提供攻击链条及详尽的关联数据，辅助判断。
- 确认风险极速处置：确认风险后，对存在风险的业务容器，可一键进行隔离、重启，或暂停容器。再通过历史信息对风险进行溯源。

**场景示意图**




# 1.5. 产品规格

| 分类 | 功能 | 标准版 |
| --- | --- | --- |
| 基础安全防护 | 仪表盘 | √ |
| | 运行态检测 | √ |
| | 镜像告警 | √ |
| | 响应中心 | √ |
| | 告警设置 | √ |

| 分类 | 功能 | 标准版 |
| --- | --- | --- |
| | 镜像管理 | √ |
| | 镜像策略 | √ |
| | 镜像设置 | √ |
| | 容器安全 | √ |
| | 容器策略 | √ |
| | 容器设置 | √ |
| | 节点安全 | √ |
| | 日志审计 | √ |
| | 安装配置 | √ |
| | 订单中心 | √ |
| | 消息中心 | √ |
| | 任务中心 | √ |

## 1.6. 支持的区域

容器安全卫士已支持的产品区域如下所示：

| 区域 | 一类节点 | 二类节点 |
| --- | --- | --- |
| 华东地区 | 华东 1 | - |

# 2. 计费说明

## 2.1. 计费模式

### 计费模式

容器安全卫士当前支持**包年/包月**计费模式。

支持续订，续订周期为 1 个月起。关于续订的更多信息请参见续订。

### 计费项

容器安全卫士根据**产品版本**、**防护节点数量**进行收费。

| 计费项 | 说明 |
| --- | --- |
| 产品版本 | 目前支持标准版，标准版支持的功能规格请参见产品规格。 |
| 防护节点数量 | 购买后若需要增加防护节点，可以扩容，详细操作请参见扩容。 |

说明：

一个账号支持购买一个包周期实例，实例必须绑定一个主套餐版本，可叠加购买节点。

### 产品价格

产品标准价格如下：

| 计费项 | 标准版（单节点） |
| --- | --- |
| 主套餐 | 290 元/月 |

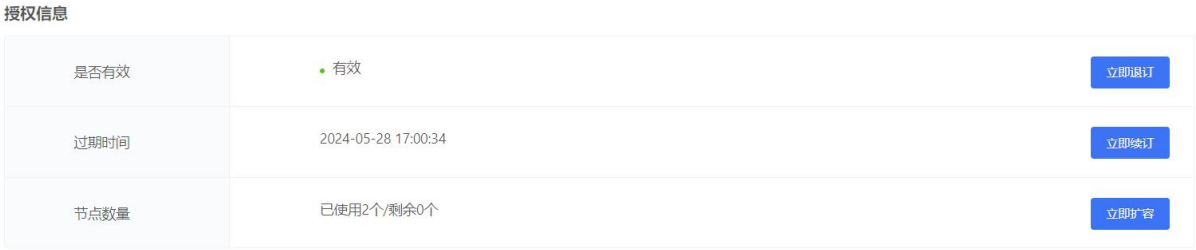
# 2.2. 续订

## 续订说明

订单到期后，若没有续订，将不能继续使用订单中的服务，建议您提前进行续订。更多详情请阅读天翼云续订规则说明。

## 手动续订

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“订单中心”，进入订单信息页面。




3. 单击“立即续订”，进入续订容器安全卫士页面。


4. 选择购买时长，支持 1 个月~5 年。
5. 阅读《天翼云容器安全卫士服务协议》后，勾选“我已阅读理解并同意《天翼云容器安全卫士服务协议》”，单击“立即购买”。
6. 进入付款页面，完成付款。

## 自动续订

方法一：在购买容器安全卫士时，同步开启“自动续订”。详细操作请参见购买云容器安全卫士。

方法二：若购买容器安全卫士时未开启“自动续订”，用户也可在购买后，通过天翼云“费用中心 > 订单管理 > 续订管理”页面，开通自动续订。详细操作请参见开通自动续订。

# 2.3. 退订

## 退订说明

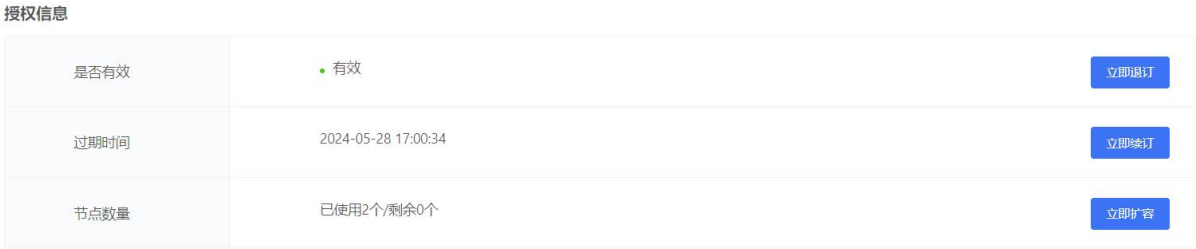
容器安全卫士支持退订，可通过容器安全卫士控制台界面、天翼云费用中心发起并完成退订操作。

- 容器安全卫士实例退订后，主套餐及扩容节点将一同退订；扩容节点不支持单独退订。
- 成功发起退订后，实例资源将转入冻结状态，冻结期 15 天。冻结期间，用户配置数据会保留 15 天，仍可以进行时安全防护，同时保留用户的配置数据，15 天后资源被释放，释放后无法恢复。

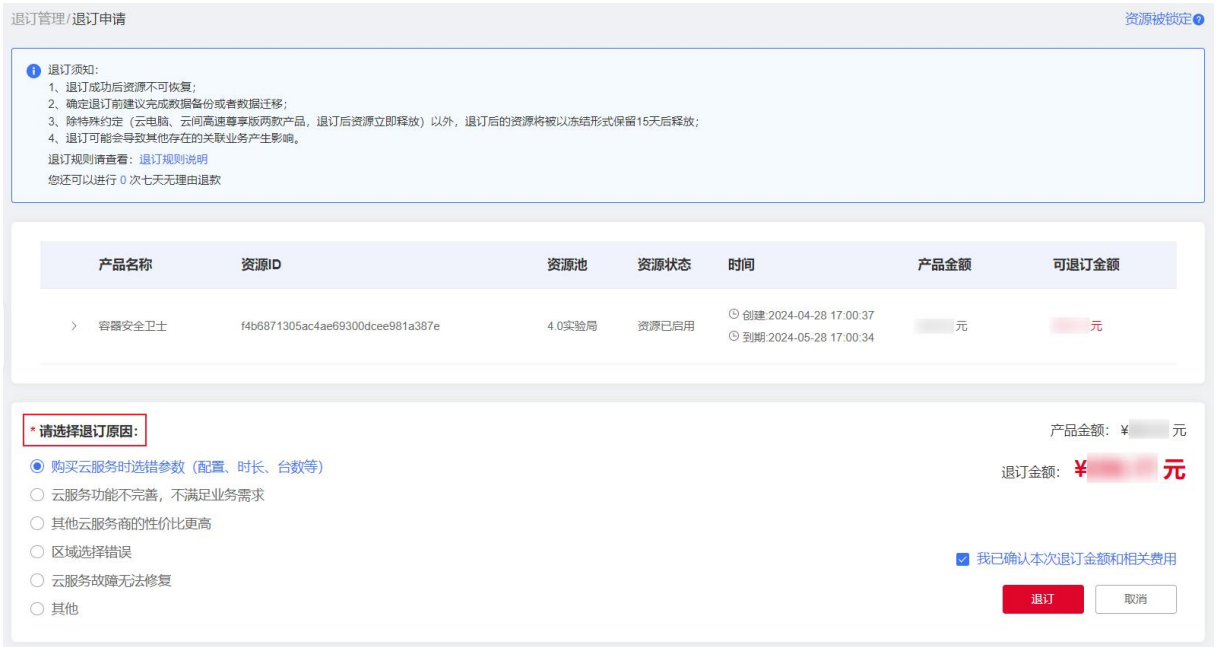
更多详情请参见退订规则说明。

## 退订步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“订单中心”，进入订单信息页面。




3. 单击“立即退订”，进入退订申请页面。



4. 确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，单击“退订”后即可进行退订。

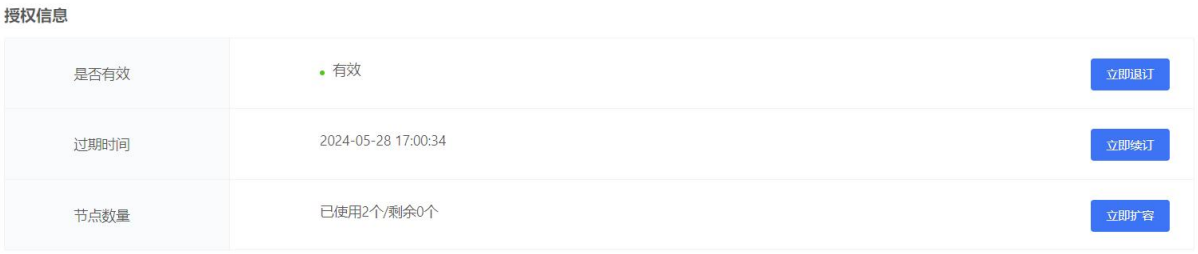
# 2.4. 扩容

## 扩容说明

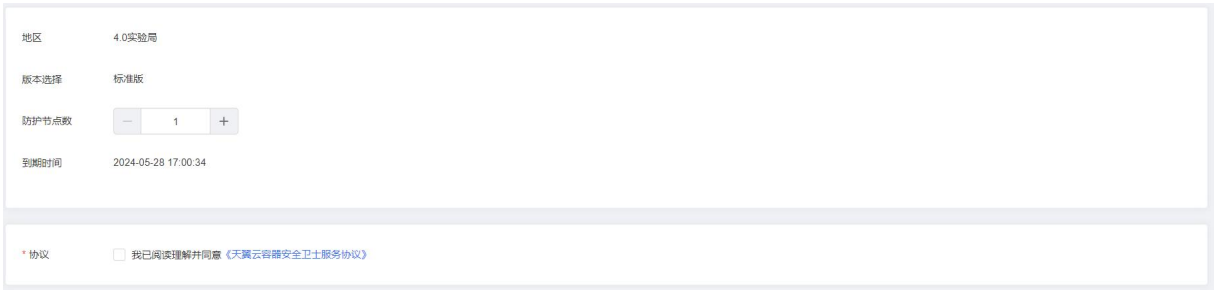
扩容节点不支持独立购买，必须在购买主套餐的基础上进行叠加购买；扩容的节点与主套餐绑定，资源到期时间与主套餐一致，不支持单独退订或单独续订。

## 扩容步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“订单中心”，进入订单信息页面。




3. 单击“立即扩容”，进入扩容页面。



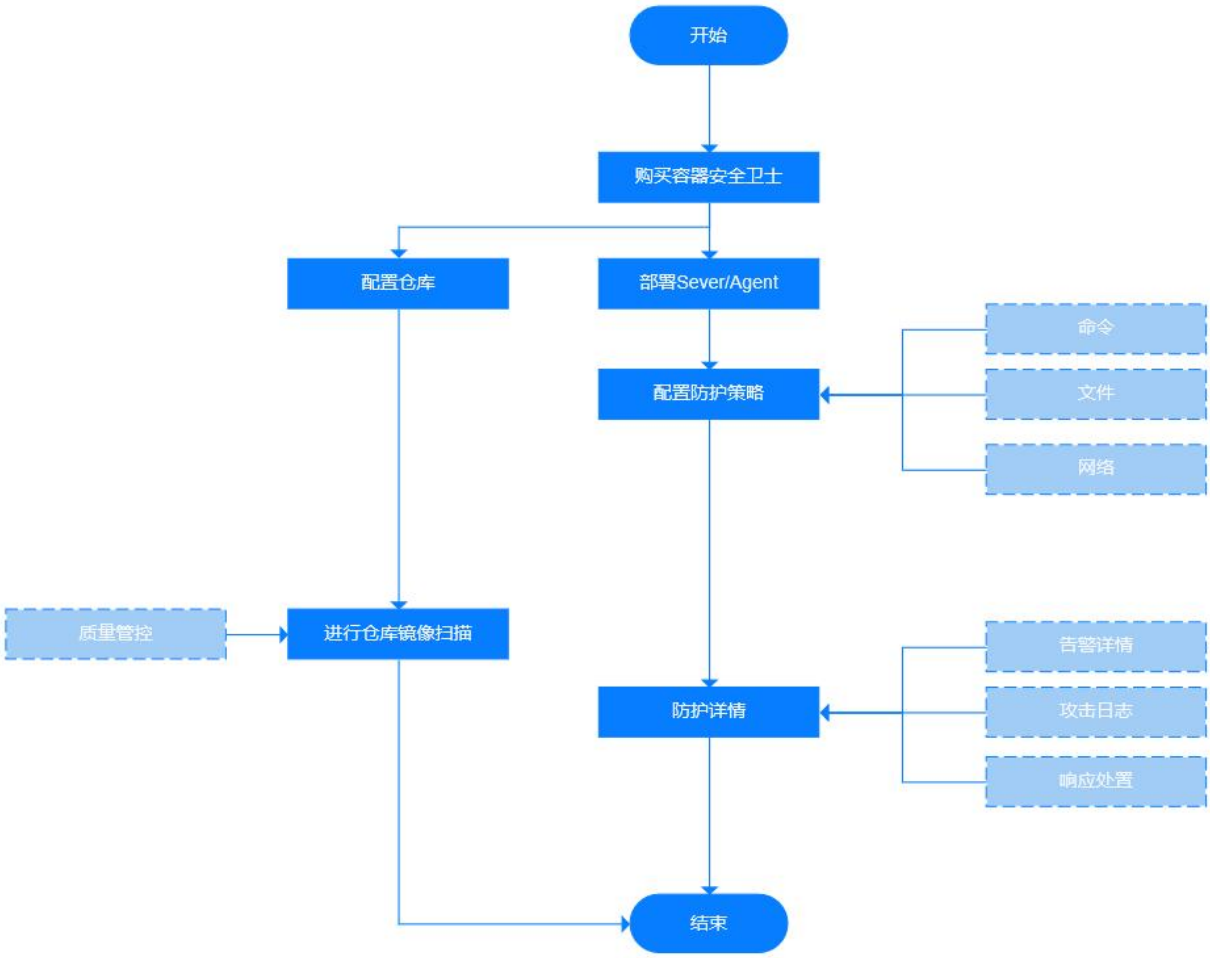

4. 选择扩容的防护节点数。到期时间为主套餐到期时间，扩容时不能更改。
5. 阅读《天翼云容器安全卫士服务协议》后，勾选“我已阅读理解并同意《天翼云容器安全卫士服务协议》”，单击“立即购买”。
6. 进入付款页面，完成付款。

# 3. 快速入门

## 3.1. 入门指引

容器安全卫士是作用于容器集群的安全防护产品，提供了对容器环境下，业务动态及静态安全风险的事前发现、事中预警、事后溯源的安全闭环。可方便快捷地解决业务容器化后带来的安全问题。

使用容器安全卫士防护云原生应用的流程如下：



# 3.2. 购买云容器安全卫士

容器安全卫士支持包年/包月计费模式，您可以根据业务规模选择容器安全卫士规格。

## 前提条件

已注册天翼云账号并完成实名认证。

## 约束限制

- 同一账号在同一个区域只能开通一个容器安全卫士实例，对应一个服务版本。

  说明：

  原则上，在任何一个区域购买的容器安全卫士实例支持防护所有区域的业务，但为了防护及转发效率，建议在购买容器安全卫士实例时，根据防护业务所在区域就近选择购买容器安全卫士实例区域。

- 开通容器安全卫士实例，必须购买主套餐，可以在主套餐基础上叠加购买节点。
- 容器安全卫士实例生效期间，支持扩容节点数量。扩容节点与主套餐绑定，到期时间与主套餐一致，不支持单独续订、退订。

## 适用场景

用户业务服务器部署在天翼云上、非天翼云或线下，防护对象为节点、容器、镜像。

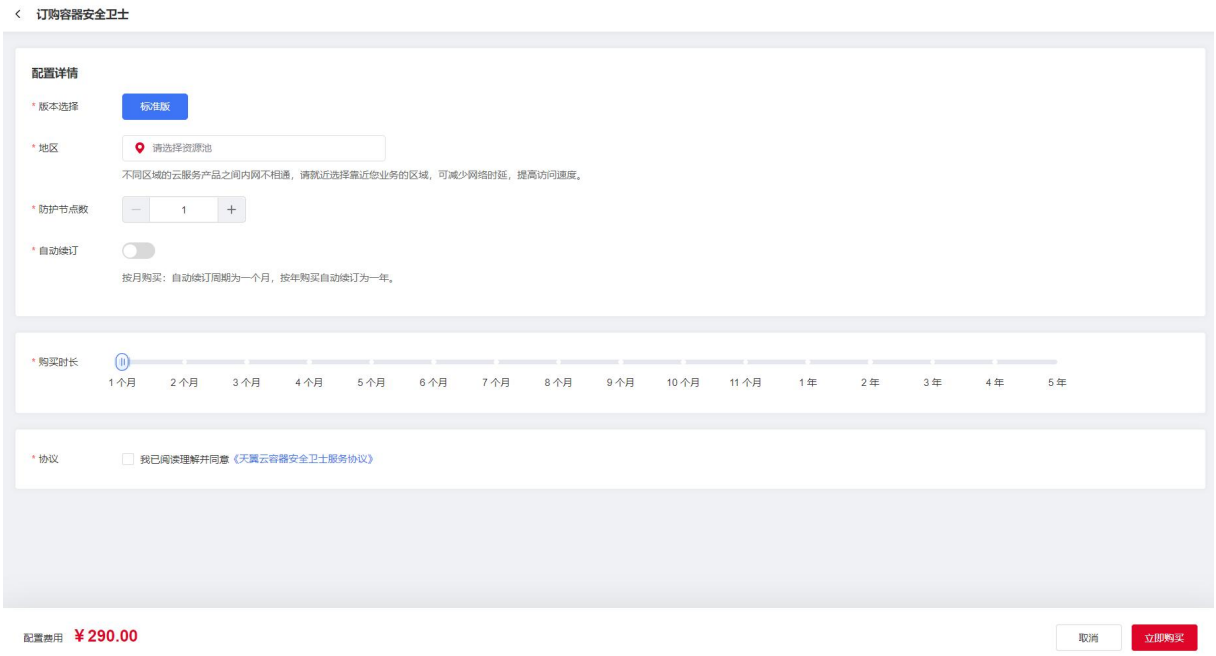
各服务版本推荐适用的场景说明如下：

- 标准版：适用云原生应用基本安全防护需求。

## 操作步骤

1. 登录天翼云控制中心。
2. 单击管理控制台上方的区域框，选择地域。
3. 在控制台列表页，选择“安全 > 容器安全卫士”，进入容器安全卫士欢迎页面。


4. 单击“立即订购”，进入产品订购页面。




5. 选择版本、地区、防护节点数，配置是否开启“自动续订”。

| 参数 | 说明 |
| --- | --- |
| 版本选择 | 当前仅支持标准版。版本规格详情请参见产品规格。 |
| 地区 | 若您需要切换区域，请在下拉框进行选择。<br>不同区域的云服务产品之间内网不相通，请就近选择靠近您业务的区域，可减 |

| 参数 | 说明 |
| --- | --- |
| | 少网络时延，提高访问速度。 |
| 防护节点数 | 配置防护节点数量，最多支持 10000 个防护节点。 |
| 自动续订 | 开启“自动续订”后，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。<br>• 按月购买，自动续费周期默认为 1 个月。<br>• 按年购买，自动续费周期默认为 1 年。<br>如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。 |

说明：

一个账号在一个区域仅支持购买一个包周期实例，实例必须绑定一个主套餐版本。

6. 选择“购买时长”，拖动时间轴设置购买时长，可以选择 1 个月~5 年的时长。
7. 确认配置参数和配置费用，阅读《天翼云容器安全卫士服务协议》并勾选“我已阅读并同意《天翼云容器安全卫士服务协议》”，单击“立即购买”。
8. 进入“付款”页面，完成付款。

## 3. 3. 安装 Sever/Agent

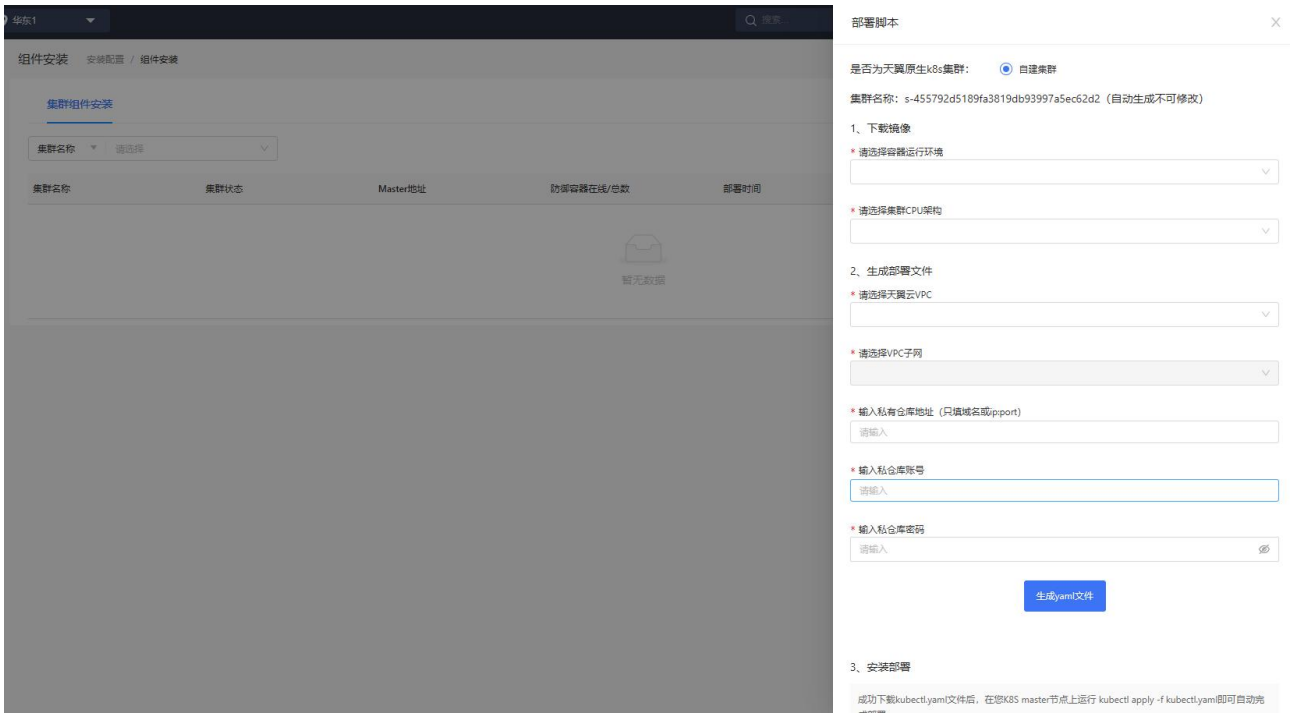
需要为容器集群安装 Sever/Agent，将容器集群纳管到容器安全卫士控制台后，才能对容器集群进行安全防护。

### 前提条件

已购买云容器安全卫士。

## 安装 Sever/Agent

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安装配置 > 组件安装”。
3. 单击“部署脚本”，进入部署脚本页面，获取集群组件部署脚本，并按页面提示进行集群安全组件的安装。




4. 在左侧导航栏选择“安装配置 > 运行状态”，更新并查看节点防护状态。

# 3.4. 扫描容器镜像

为了保障云原生供应链安全，您需要购买容器安全卫士实例，并进行安全扫描，通过仪表盘查看访问统计信息和攻击防护记录，掌握业务的安全状况。

## 步骤一：购买容器安全卫士实例

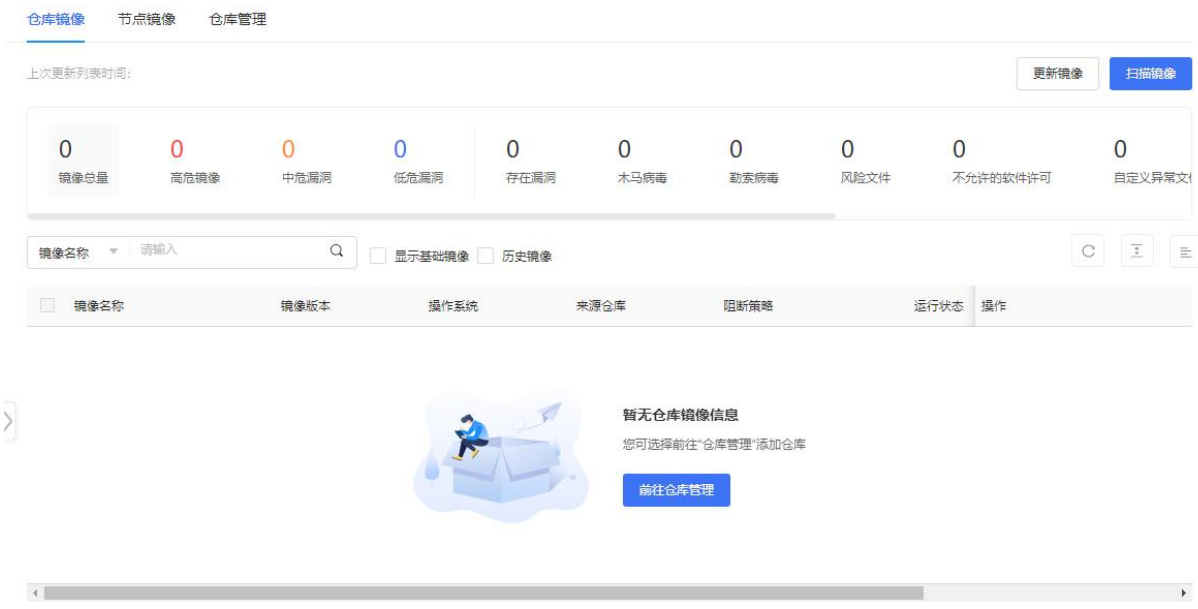
详细步骤请参见购买云容器安全卫士。

## 步骤二：安装 Sever/Agent

详细步骤请参见安装 Sever/Agent。

## 步骤三：扫描镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全 > 镜像管理”，在镜像管理页面可以对仓库镜像、节点镜像进行安全扫描。



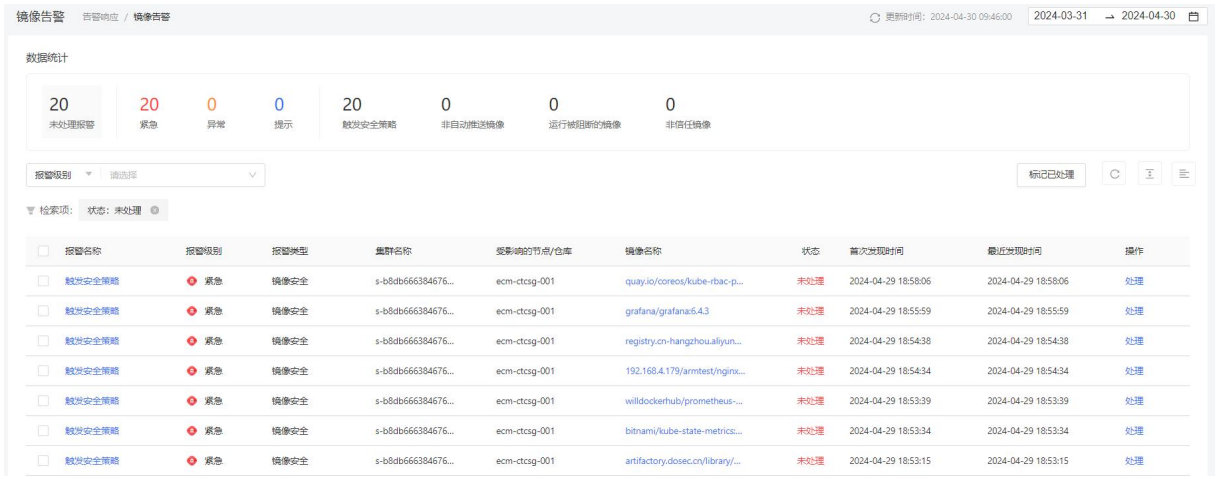

3. 进入“仓库管理”页面，单击“添加仓库”，添加镜像仓库。


4. 扫描节点镜像。
   a. 进入“节点镜像”页面，单击“更新镜像”，获取仓库镜像数据。
   b. 单击“扫描镜像”，对镜像进行安全扫描。
5. 扫描仓库镜像。
   a. 进入“仓库镜像”页面，单击“更新镜像”，获取仓库镜像数据。
   b. 单击“扫描镜像”，对镜像进行安全扫描。
6. 在左侧导航栏选择“镜像安全 > 镜像策略”，进入页面配置镜像策略，配置漏洞、文件、软件包规则，防止风险流入供应链。
7. 在左侧导航栏选择“镜像安全 > 镜像设置”，进入页面配置镜像扫描规则、历史镜像保留时长、及周期性扫描规则。

## 步骤四：查看事件报表

镜像配置防护策略后，会记录防护事件信息，包括报警名称、报警级别、报警类型、集群名称、受影响的节点/仓库、镜像名称、状态、首次发现时间、最近发现时间等。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“告警响应 > 镜像告警”。
3. 在告警列表可以查看镜像告警记录。

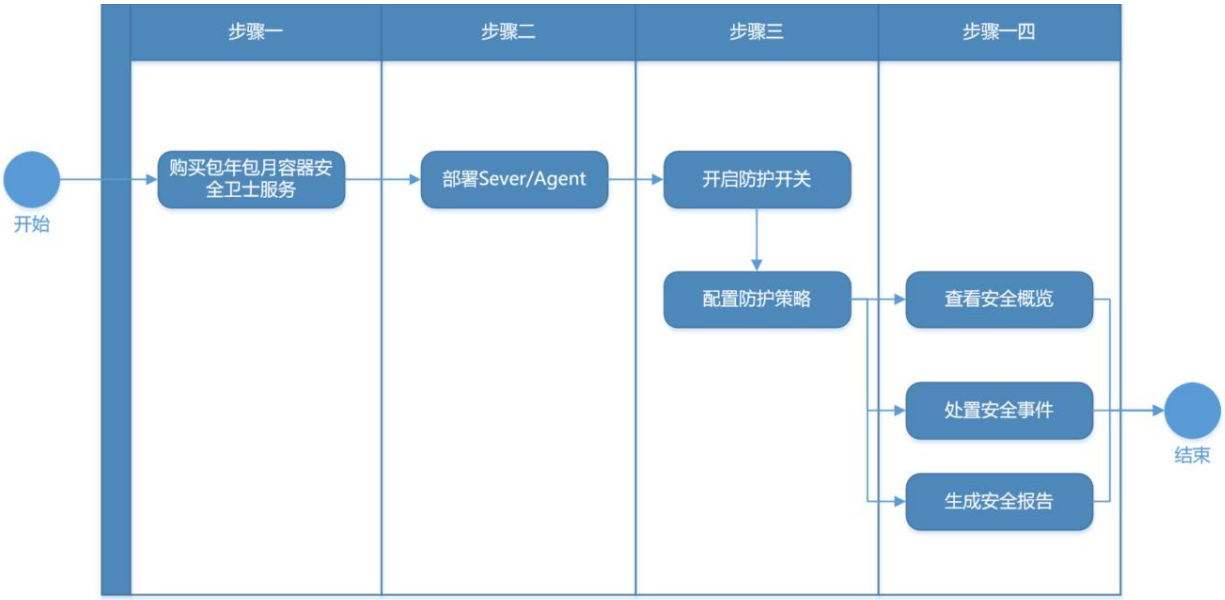


4. 单击列表操作列的“处理”，可对事件进行“标记为已处理”、“加入白名单”、“镜像阻断”等处置。单击列表右上方的“标记为已处理”，可以批量处置误报的告警。

## 3.5. 开启容器防护

为快速实现云原生应用防护，您需要购买容器安全卫士实例、配置防护策略。防护开启后，通过仪表盘查看访问统计信息和攻击防护记录，掌握业务的安全状况。

配置流程：




### 步骤一：购买容器安全卫士实例

详细步骤请参见购买云容器安全卫士。

### 步骤二：安装 Sever/Agent

详细步骤请参见安装 Sever/Agent。

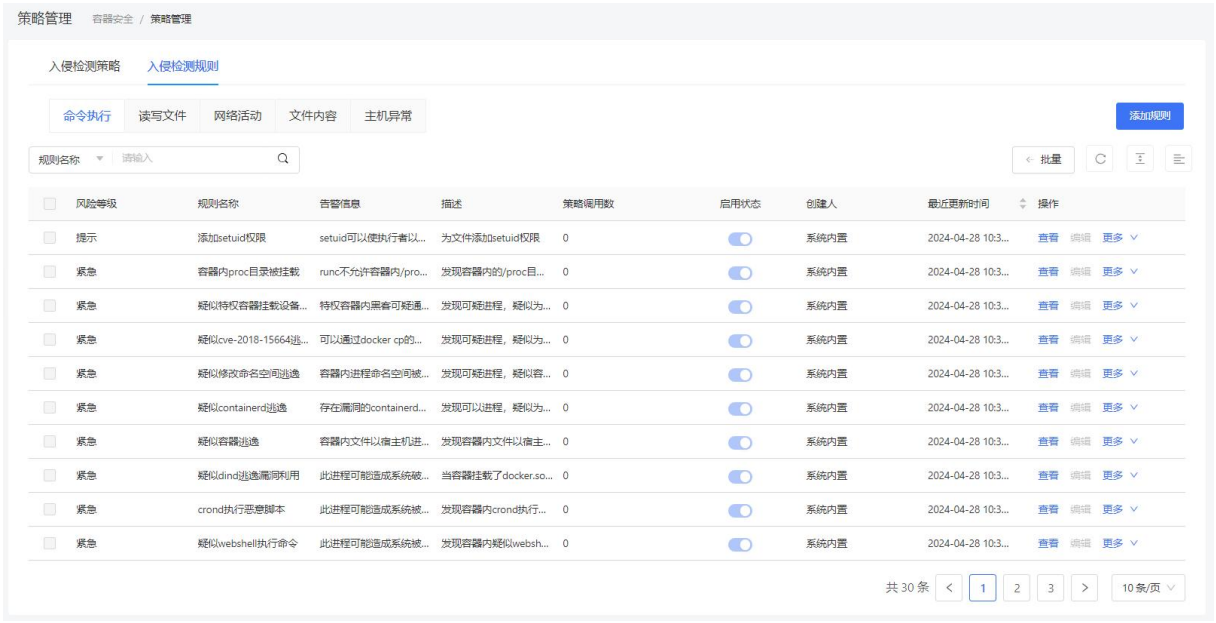
### 步骤三 配置防护策略

Server/Agent 安装完成后，系统默认使用“默认策略”防护所有容器，并将“状态”切换为开启。

用户也可以自定义防护策略，详细步骤如下：

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“容器安全 > 容器策略”，进入容器策略页面。

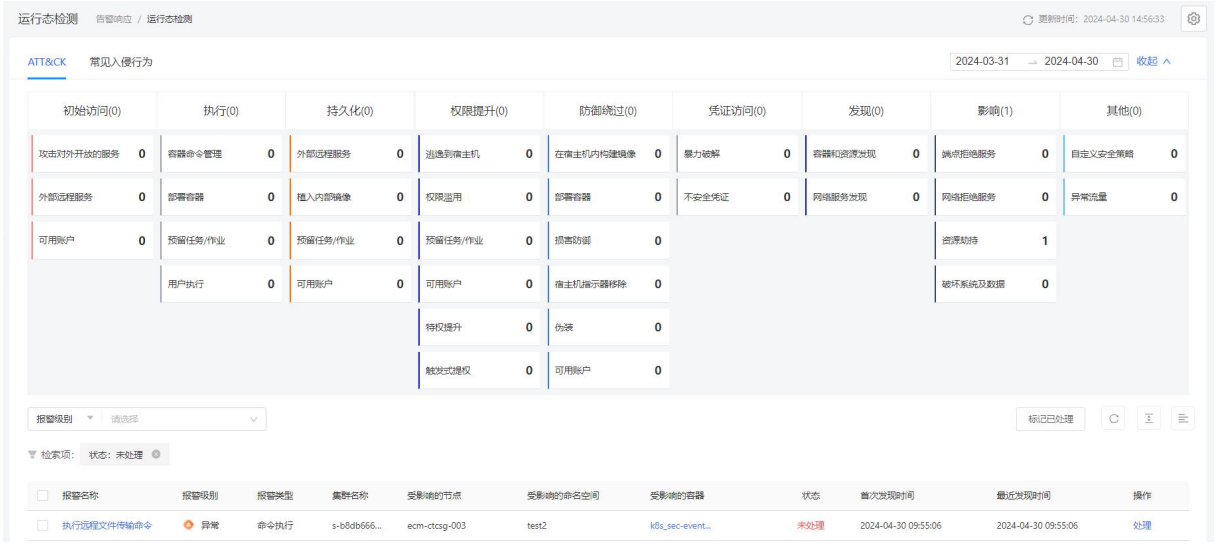

3. 在“入侵检测策略”页面，可以添加防护策略，并将策略的“启用状态”切换为开启。
4. 在“入侵检测规则”页面，可管理命令执行、读写文件、网络活动、文件内容等检测规则。




## 步骤四：查看事件报表

容器开启防护后，会记录防护事件信息，包括报警名称、报警级别、报警类型、集群名称、受影响节点、受影响命名空间、受影响容器、状态、首次发现时间、最近发现时间等。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“告警响应 > 运行态检测”。
3. 在防护告警列表可以查看容器的防护记录。




4. 单击列表操作列的“处理”，可对事件进行“标记为已处理”、“加入白名单”、“隔离 Pod”、“重启 Pod”、“暂停容器”等处置。

# 4. 用户指南

## 4.1. 组件安装

### 4.1.1. 租户集群为自建集群

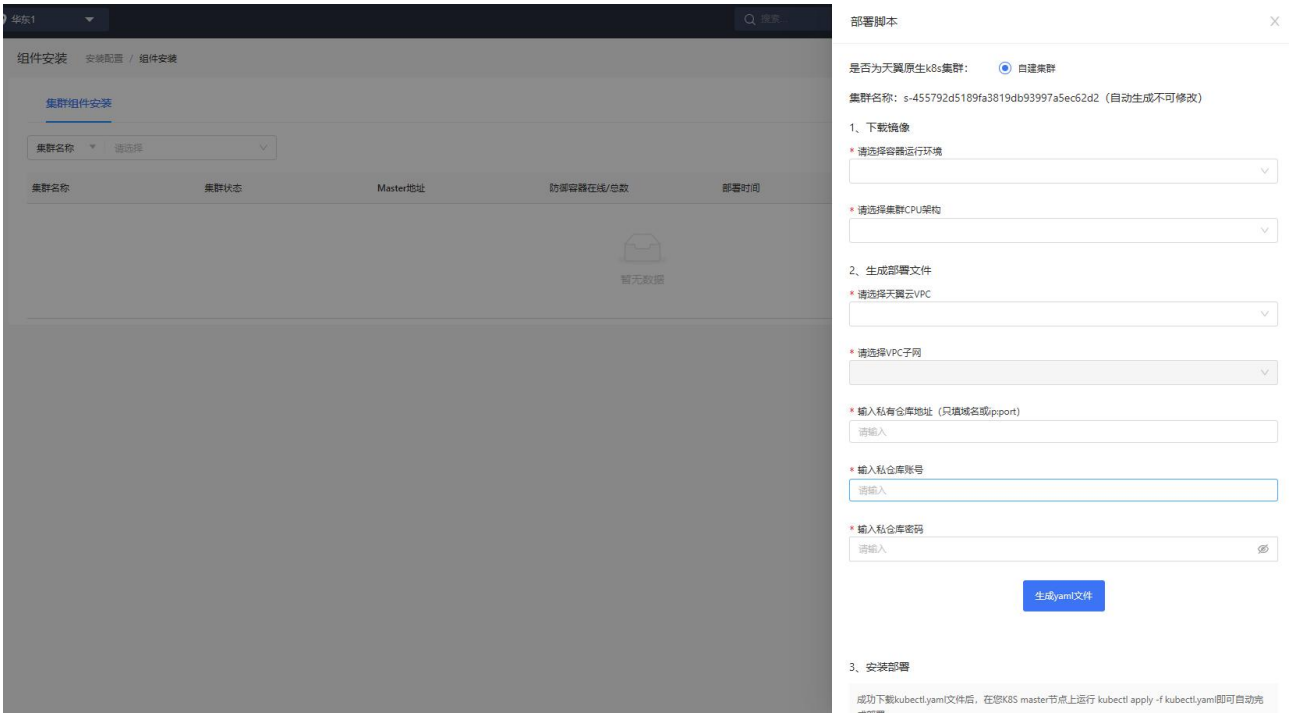
#### 注意事项

- 集群组件在运行时会挂载 k8s node 宿主机的/data（非 crio）和/root（crio）目录，请确保目录的权限正常。
- 请确保您的 k8s 集群允许出网策略 TCP 端口：31080、30432、32345。

#### 获取部署脚本

1. 进入容器安全卫士产品控制台。
2. 在左侧导航栏选择“安装配置 > 组件安装”，进入组件安装页面。


3. 单击“部署脚本”，进入部署脚本页面。




4. 选择“是否为天翼原生 k8s 集群”，此处选择“自建集群”。
5. 集群名称为系统自动生成，不可以修改。
6. 下载镜像。
   a. 选择容器运行环境（支持 docker、containerd、CRI-O）。
   b. 选择集群 CPU 架构（支持 X86、ARM 架构）。
   c. 单击“下载镜像 Tar 包”下载镜像 Tar 包到本地，然后加载至您的私有仓库中（请不要修改镜像名称）。

      Tar 包中包含 4 个镜像，分别为：

      - library/dosec-agent:2024-03-06T18.58.08V5.2.0_release_1e1cc2_f1e038c378,library
      - dosec-host-tool:alpineV3.8,library
      - dosec-scanner:2024-04-22T19.37.51V5.2.0_release_c60e9b_93f9a30a7b,library
      - dosec-server:2024-04-22T21.23.54V5.2.0_release_4933b2_523a6375b4
7. 生成部署脚本。
   a. 选择天翼云 VPC、VPC 子网，输入私有仓库的地址、账号、密码。
   b. 单击“生成 yaml 文件”，并将 yaml 文件保存到本地。

注意：

- 系统会根据您的输入自动生成 yaml。
- 容器安全卫士不会保存您的私有仓库用户名和密码以保证安全。
- 下载后的包，内容请勿进行修改。
- 下载的脚本仅能用于一个 k8s 集群使用，若在不同集群重复使用可能造成数据异常。

### 安装部署

成功下载 kubectl.yaml 文件后，执行以下步骤即可自动完成部署：

1. 登录集群 K8S Master 节点。
2. 执行 kubectl apply -f kubectl.yaml 命令。

### 部署成功

- 前往“安装配置 > 运行状态”查看具体部署情况。
- 部署成功后，sever 将租户信息上报至数据库，与项目信息进行关联展示。

## 4.1.2. 集群组件配置

1. 单击左侧导航栏中“安装配置 > 组件安装”，进入组件安装页面。
2. 查看集群列表。

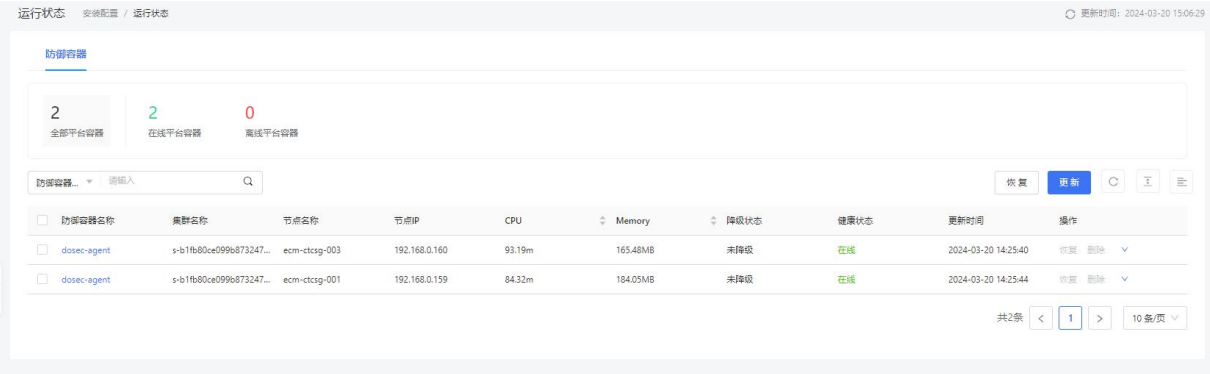

3. 单击集群列表操作列的“集群组件配置”按钮，可设置单个镜像扫描超时、节点扫描的并发数、仓库镜像扫描并发数、防御容器开启镜像阻断、开启入侵检测模块、开启容器审计功能等信息。


## 4.1.3. 查看运行状态

### 查看防御容器列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安装配置 > 运行状态”，进入运行状态页面。

3. 该页面显示平台内所有防御容器的运行状态。平台容器列表内，支持按照“防御容器名称”、“防御容器 IP”、“集群名称”、“节点名称”、“健康状态”、“降级状态”进行筛选查询。




| 参数 | 说明 |
| --- | --- |
| 防御容器名称 | 容器的名称。 |
| 所在集群 | 容器所属集群。 |
| 所在节点 | 容器运行所在节点。 |
| 节点 IP | 容器运行所在节点的 IP 地址。 |
| CPU | CPU 占用内核数量，单位 M：代表“千分之一核心”。例如，50M 的含义是指 50/1000 核心，即 5%。 |
| Memory | 防御容器占用的存储空间。 |
| 健康状态 | 健康状态分为“在线”状态和“离线”状态。 |
| 降级状态 | 降级状态分为已降级、未降级。<br>用户可查看防御容器降级状态，并且通过操作来恢复已降级的防御容器。<br>说明：<br>未降级或已离线的防御容器不支持恢复。 |
| 更新时间 | 容器状态更新的时间。 |

### 下载日志

在防御容器列表内，单击操作列中的“下载日志”，可直接将防御容器的日志下载至本地。

## 4. 2. 镜像安全

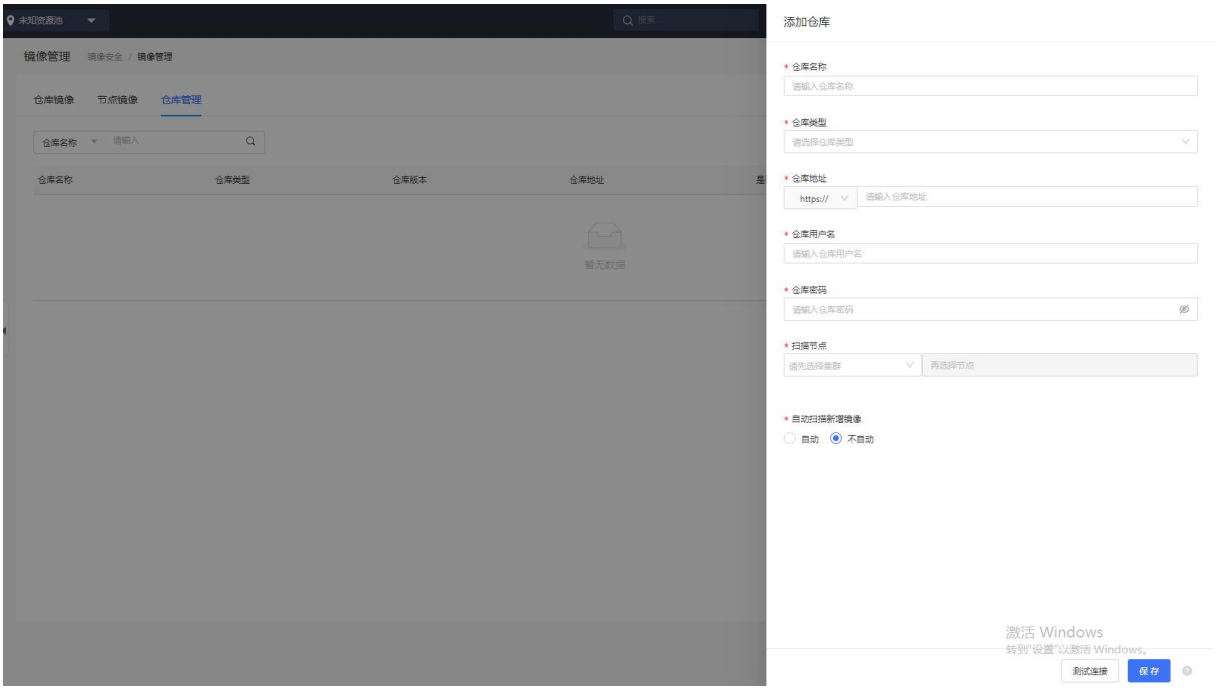
### 4.2.1. 配置镜像仓库

在没有添加镜像之前，页面会提示“暂无仓库镜像信息”。要获取新的仓库镜像列表，首先需要配置镜像仓库。

### 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全”，进入镜像安全页面。
3. 选择“仓库管理”页签，进入仓库管理页面，查看仓库配置列表。


4. 单击仓库配置列表右上角的“添加仓库”，页面右侧弹出添加仓库页面。




5. 填写仓库的相关参数。

| 参数 | 说明 |
| --- | --- |
| 仓库名称 | 输入仓库名称。 |
| 仓库类型 | 仓库类型支持 Harbor、Jfrog、Huawei、Huawei CCE Agile、Registry、Aliyun、AWS、Microsoft、金山云。 |
| 仓库地址 | 仓库地址支持 HTTP、HTTPS 两种协议。 |
| 仓库用户名 | 输入仓库的用户名。 |
| 仓库密码 | 输入仓库的密码。 |
| 扫描节点 | 选择扫描容器所在节点。 |
| 自动扫描新增镜像 | 选择是否自动扫描新增镜像。 |

| 参数 | 说明 |
| --- | --- |
| | 选择“自动”，仓库中每拉取一个新增的镜像后，系统就会自动进行扫描。 |

6. 填写完成后可单击“测试连接”，若提示“连接成功”，证明信息填写正确，单击“保存”完成添加。

## 4.2.2. 更新镜像列表

镜像列表会定期自动更新，也可以通过手动更新列表，来更新节点和仓库中存在的镜像资产。

### 前提条件

已添加镜像仓库，详细操作请参见配置镜像仓库。

### 更新仓库镜像列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全”，进入镜像安全页面。
3. 选择“仓库镜像”页签，单击仓库镜像列表右上角的“更新镜像”，可拉取仓库中的所有仓库镜像。


4. 选择更新范围：支持更新全部仓库镜像、单个仓库内的镜像、单个仓库项目内的镜像三种更新方式。

5. 单击“确定”，完成更新操作。

### 更新节点镜像列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全”，进入镜像安全页面。
3. 选择“节点镜像”页签，单击节点镜像列表右上角的“更新镜像”，可拉取集群中的所有节点镜像。


4. 选择更新范围：支持更新全部节点镜像、更新集群内的镜像两种更新方式。
5. 单击“确定”，完成更新操作。

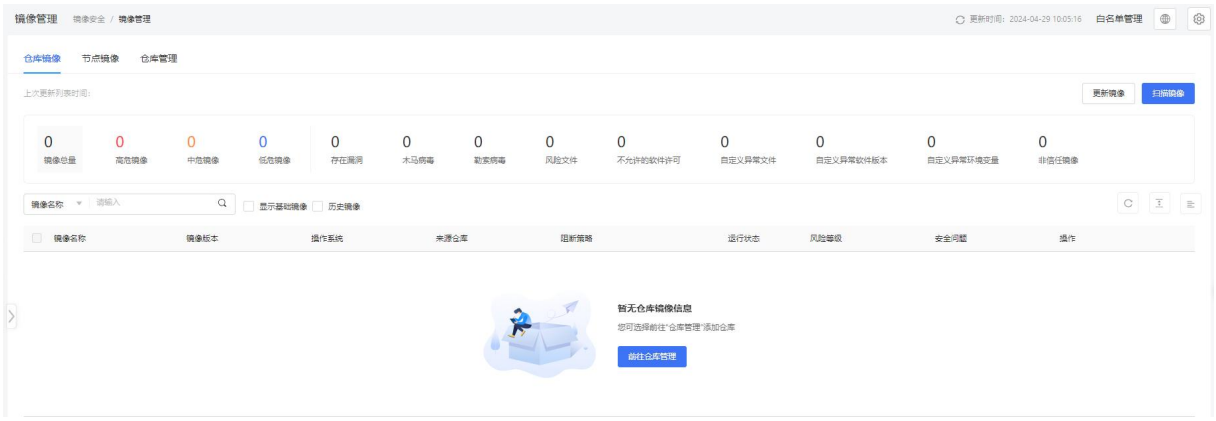
## 4.2.3. 扫描镜像

镜像扫描支持手动扫描、自动扫描、周期扫描三种方式。

### 4. 2. 3. 1. 手动扫描

#### 扫描仓库镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全”，进入镜像安全页面。
3. 查看仓库镜像列表，单击镜像列表中的“扫描”、“重新扫描”或者镜像列表右上角的“扫描镜像”，为未扫描的镜像或已经扫描完成的镜像建立扫描任务。

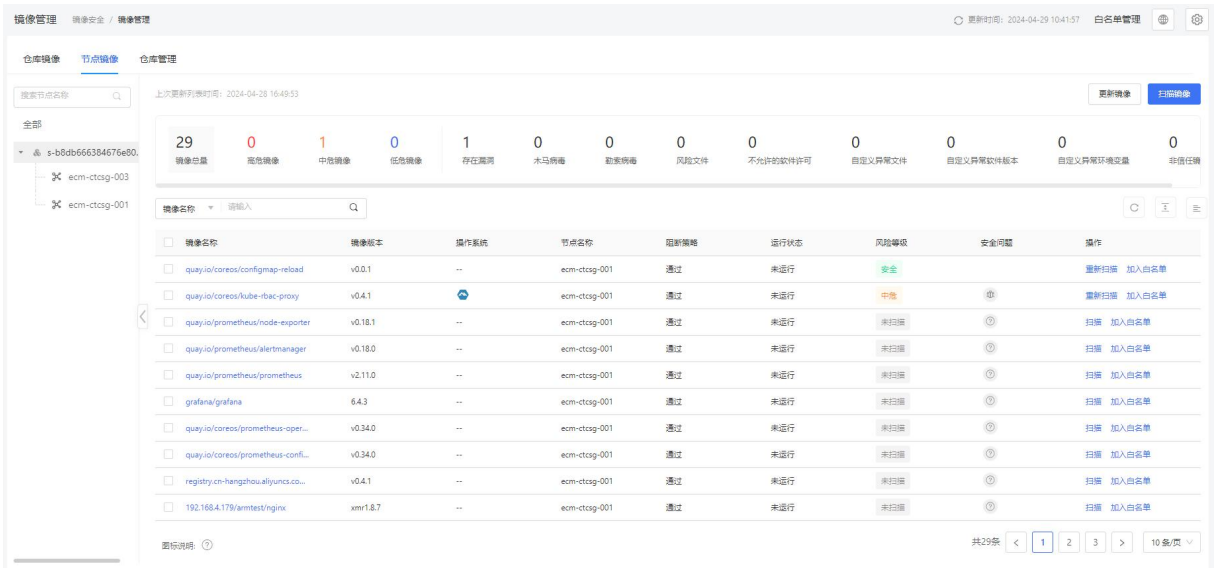



4. 在弹出的扫描仓库镜像对话框中，选择扫描范围。


5. 单击“确定”，即可开始扫描。

## 扫描节点镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全”，进入镜像安全页面。
3. 查看节点镜像列表，单击镜像列表中的“扫描”、“重新扫描”或者镜像列表右上角的“扫描镜像”，为未扫描的镜像或已经扫描完成的镜像建立扫描任务。




4. 在弹出的扫描节点镜像对话框中，选择扫描范围。

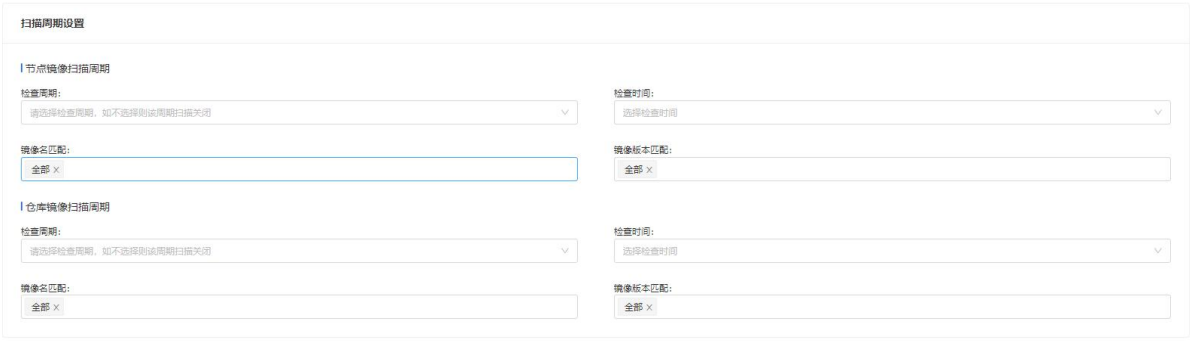

5. 单击“确定”，即可开始扫描。

## 4.2.3.2. 自动扫描

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全 > 镜像设置”，进入镜像设置页面。也可以在“镜像管理”页面，单击右上角的“设置”图标，进入设置页面。
3. 定位到“设置”中的“扫描设置”页面，打开“自动扫描节点新增镜像”开关，就会自动扫描节点新增的镜像。


### 4.2.3.3. 周期扫描

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“镜像安全 > 镜像设置”，进入镜像设置页面。也可以在“镜像管理”页面，单击右上角的“设置”图标，进入设置页面。
3. 定位到“设置”中的“扫描设置”页面，通过设置节点镜像、仓库镜像的“检查周期”和“检查时间”来对镜像进行周期性扫描，且支持输入限定周期扫描的镜像名称和版本，支持通配符，留空则默认为不限制，匹配全部镜像。




## 4.2.4. 查看扫描状态

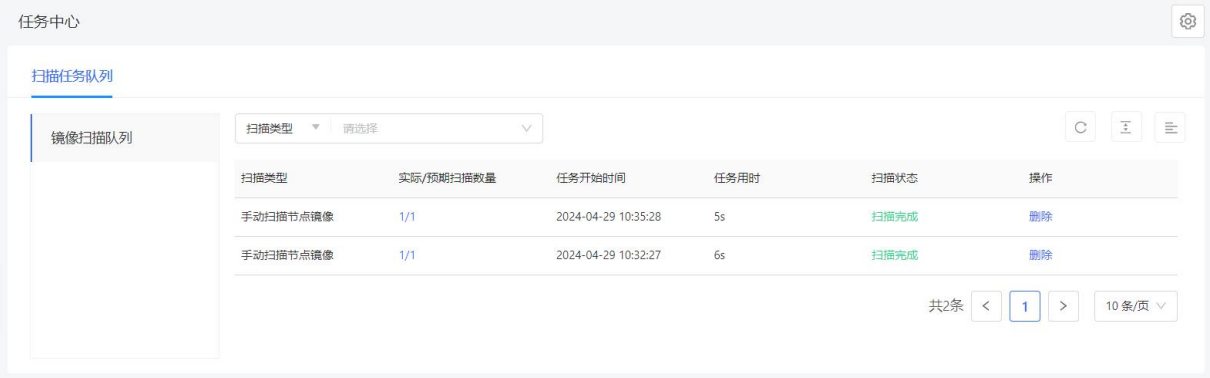
执行镜像扫描操作后，可通过“任务中心”查看镜像扫描任务的状态。

- 扫描状态包括扫描完成、待扫描、扫描中、创建中。
- 扫描类型分为手动扫描、自动扫描、周期扫描。

### 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“任务中心”，进入任务中心页面。

3. 定位到“扫描任务队列 > 镜像扫描队列”，可查看历史扫描任务和正在扫描任务中镜像的扫描状态。

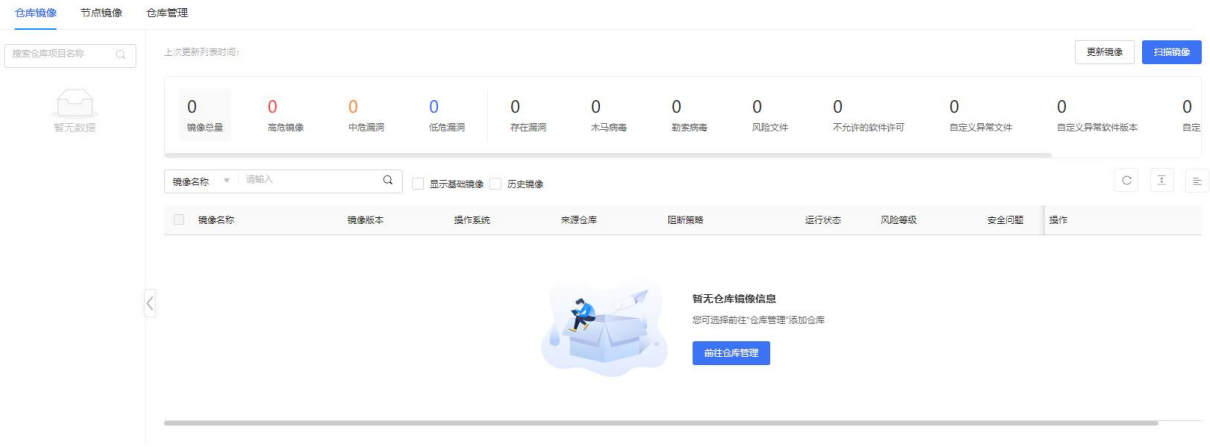



> 说明：
>
> 若扫描任务中扫描类型后带有“！”，则说明此任务中存在扫描失败的镜像。

## 4.2.5. 查看扫描结果

### 4. 2. 5. 1. 查看仓库镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。




3. 在仓库镜像页面左侧，可按照“仓库类别 > 项目名称”进行筛选查看，单击树形结构和镜像列表之间的“ < ”按钮，可以折叠树形结构。
4. 仓库镜像列表上方汇总展示了当前仓库或项目中存在的漏洞总量，又分别按照高、中、低危险级别和不同风险特征进行分类统计。随着在左侧树形结构中的选择改动，统计结果将响应式动态变化。单击想要查看的镜像类别，下方镜像列表会根据单击选择的条件进行筛选检索。

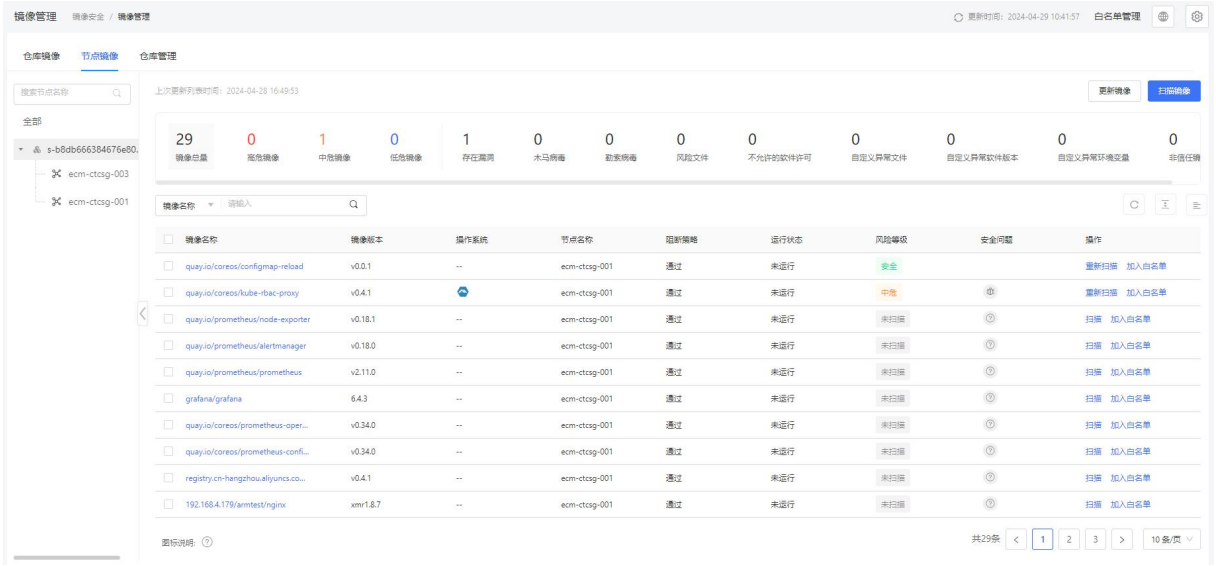
5. 仓库镜像列表内，支持按照“镜像名称”、“镜像 ID”、“镜像版本”、“软件名称”、“软件版本”、“漏洞编号”、“阻断策略”、“风险等级”、“安全问题”进行筛选查询。

   仓库镜像列表内各参数说明如下：

| 参数 | 说明 |
| --- | --- |
| 镜像名称 | 镜像的名称，命名通常为“[仓库名称]/[项目名称]/镜像名称”。 |
| 镜像版本 | 镜像的版本作为镜像的 tag 信息，可用来区分名称相同的镜像。 |
| 操作系统 | 构建该镜像使用的基础镜像的系统类型。 |
| 来源仓库 | 获取该镜像的来源仓库名称。 |
| 阻断策略 | 分为“阻断”和“通过”两种状态，用于显示镜像扫描后的处理结果。<br>当镜像存在风险问题时，可以通过阻断来处理风险。 |
| 风险等级 | 风险等级分为：高危、中危、低危、未知（扫描失败）、未扫描和安全。 |
| 安全问题 | 安全问题包括：存在漏洞、勒索病毒、重点关注漏洞、木马病毒、自定义异常文件、风险文件、自定义异常软件版本、不允许的软件许可、自定义异常环境变量、非信任镜像、未知、无安全问题、非自动推送镜像。 |
| 发现时间 | 系统初次拉取到该镜像的时间。 |

### 4.2.5.2. 查看节点镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“节点镜像”页签，进入节点镜像页面。



4. 在节点镜像页面左侧，可按照“集群名称 > 节点名称”进行筛选查看，单击树形结构和镜像列表之间的“<”按钮，可以折叠树形结构。
5. 节点镜像列表上方汇总展示了当前集群或节点中存在的漏洞总量，又分别按照高、中、低危险级别和不同风险特征进行分类统计。随着在左侧树形结构中的选择改动，统计结果将响应式动态变化。单击想要查看的镜像类别，下方镜像列表会根据单击选择的条件进行筛选检索。
6. 节点镜像列表内，支持按照“镜像名称”、“镜像 ID”、“镜像版本”、“软件名称”、“软件版本”、“漏洞编号”、“集群名称”、“节点名称”“阻断策略”、“运行状态”、“风险等级”、“安全问题”进行筛选查询。

   节点镜像列表内各字参数说明如下：

| 参数 | 说明 |
| --- | --- |
| 镜像名称 | 镜像的名称，命名通常为“[仓库名称]/[项目名称]/镜像名称”。 |
| 版本版本 | 镜像的版本作为镜像的 tag 信息，可用来区分名称相同的镜像。 |
| 操作系统 | 构建该镜像使用的基础镜像的系统类型。 |
| 集群名称 | 镜像所在集群的名称。 |
| 节点名称 | 镜像所在节点的名称。 |
| 阻断策略 | 分为“阻断”和“通过”两种状态，用于显示当前镜像扫描后的处理结果。<br>当镜像存在风险问题时，可以通过阻断来处理风险。 |

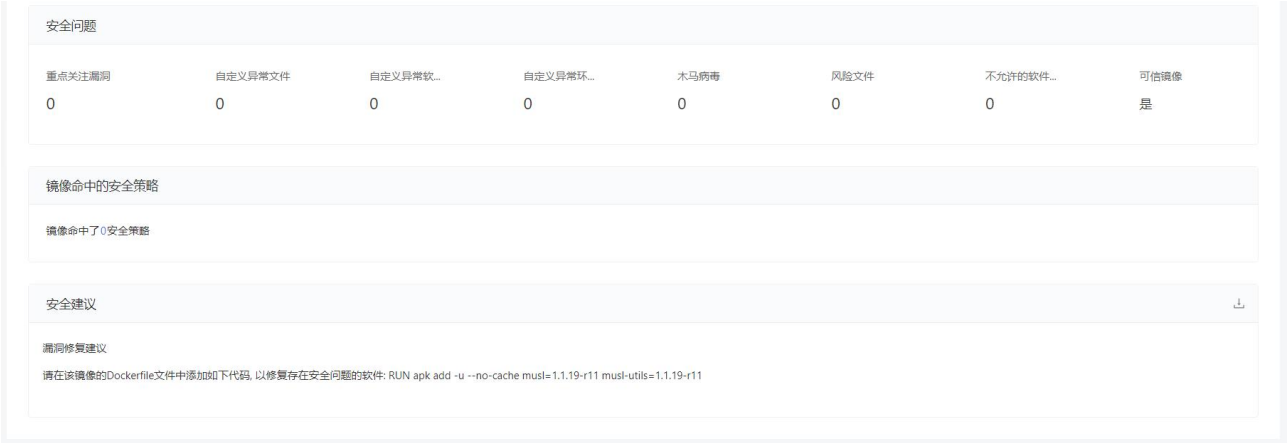
| 参数 | 说明 |
| --- | --- |
| 运行状态 | 运行状态指的是镜像关联容器的运行状态，分为：运行中、已停止、未运行。 |
| 风险等级 | 风险等级分为：高危、中危、低危、未知（扫描失败）、未扫描和安全。 |
| 安全问题 | 安全问题包括：存在漏洞、勒索病毒、重点关注漏洞、木马病毒、自定义异常文件、风险文件、自定义异常软件版本、不允许的软件许可、自定义异常环境变量、非信任镜像、未知、无安全问题。 |
| 发现时间 | 第一次更新出该镜像的时间。 |

## 4.2.5.3. 查看镜像详情

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“仓库镜像”或“节点镜像”页签，进入对应镜像列表页面。
4. 单击镜像列表中的“镜像名称”，进入镜像详情页面查看镜像的基本信息、关联信息、漏洞、软件、文件、环境变量、安全溯源等相关信息。

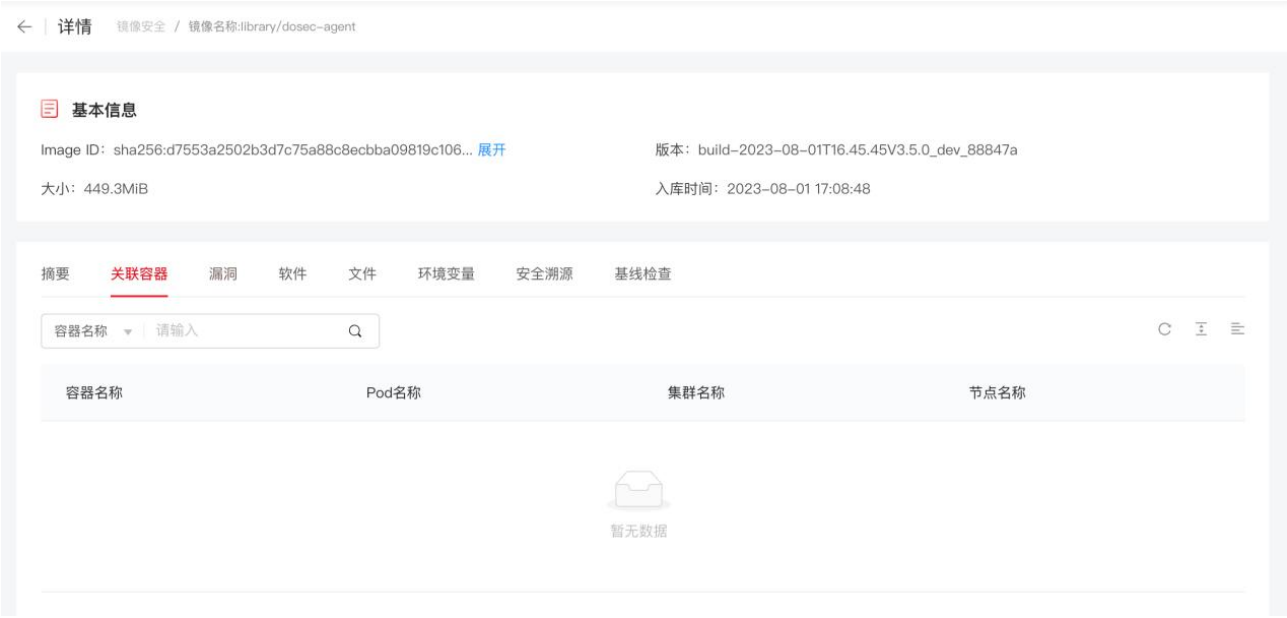
### 查看镜像安全概览

镜像安全概览页面可以查看镜像的基本信息、风险分数、安全问题、镜像命中的安全策略、安全建议等信息。



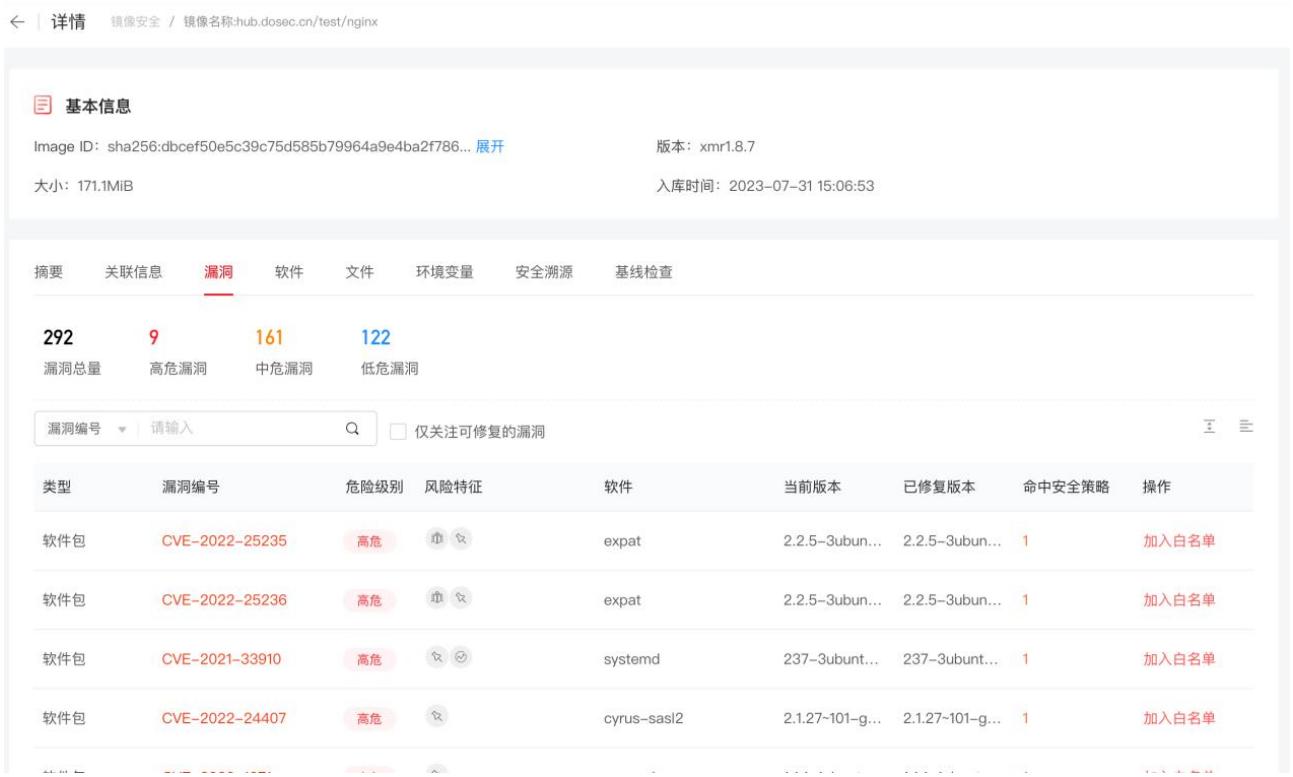

## 查看镜像关联容器

在“关联容器”页面，可查看与镜像相关联的容器的信息，包括容器名称、容器所在 Pod 名称、所属集群名称、运行所在节点的名称。

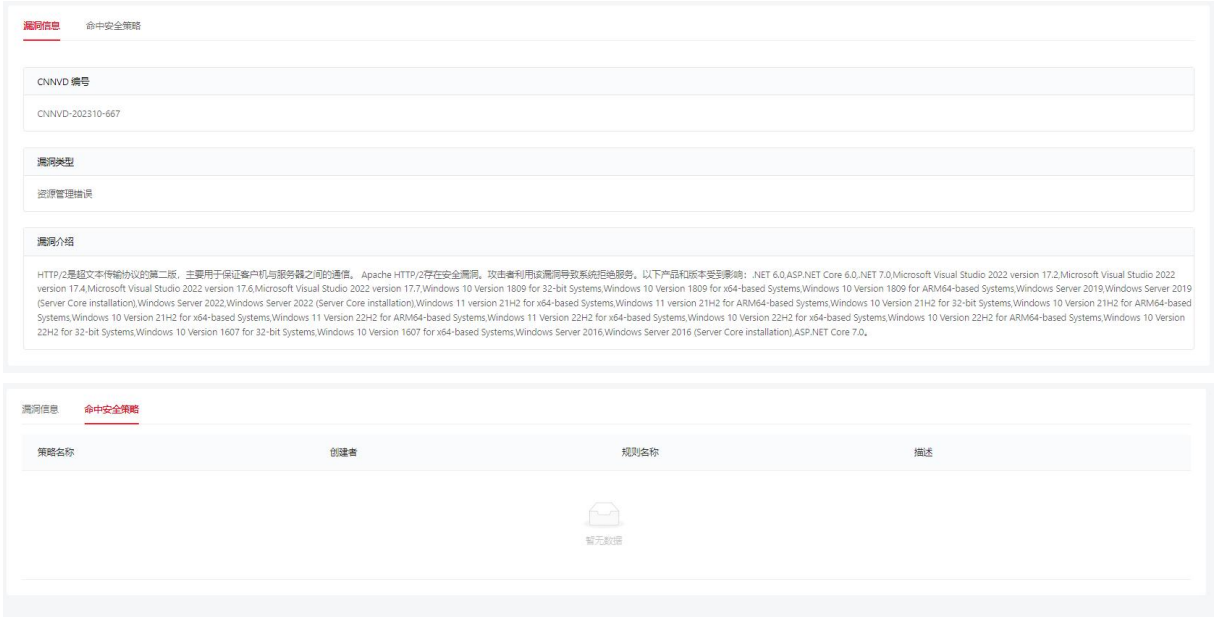



## 查看镜像漏洞详情

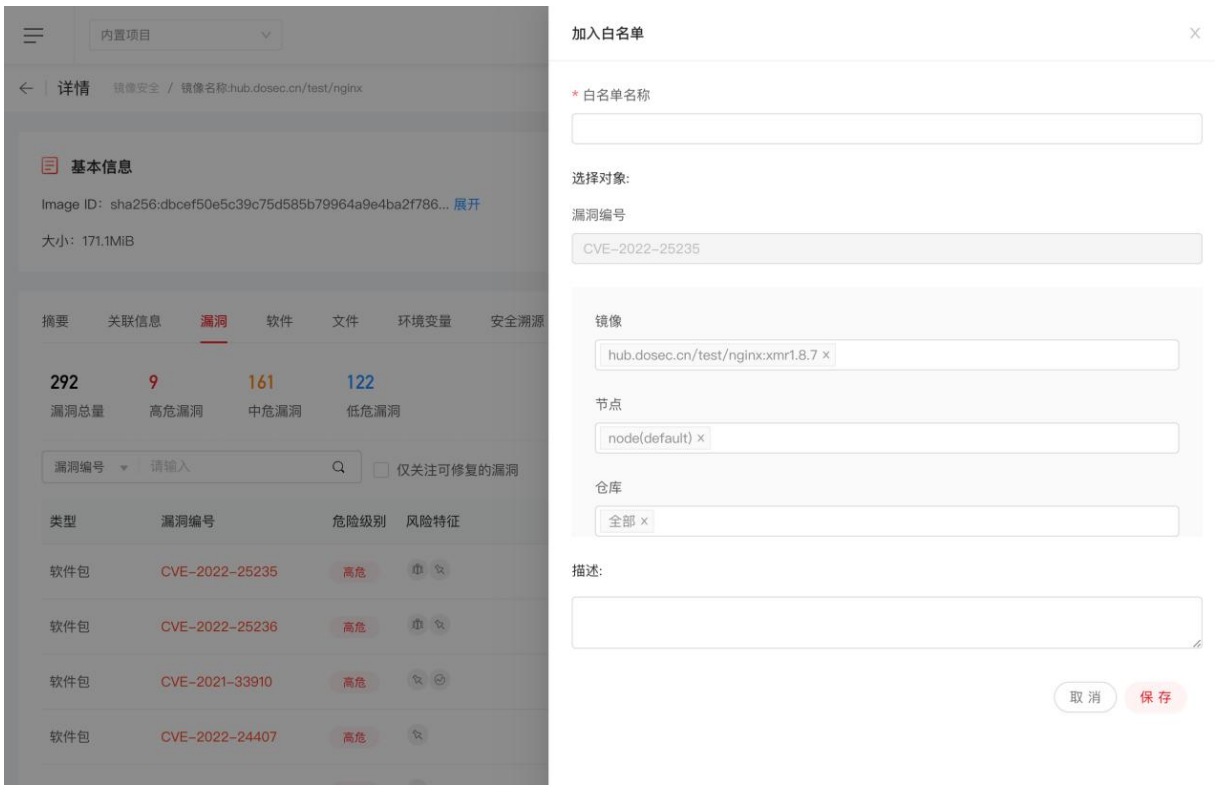
在“漏洞”页面，可查看该镜像中各个危险级别的漏洞统计情况，单击漏洞列表中的“漏洞编号”，可以查看漏洞的详细信息，包括漏洞介绍、漏洞评分、来源信息等。




- 单击漏洞详情中的“命中安全策略”，可以查看漏洞命中的安全策略。

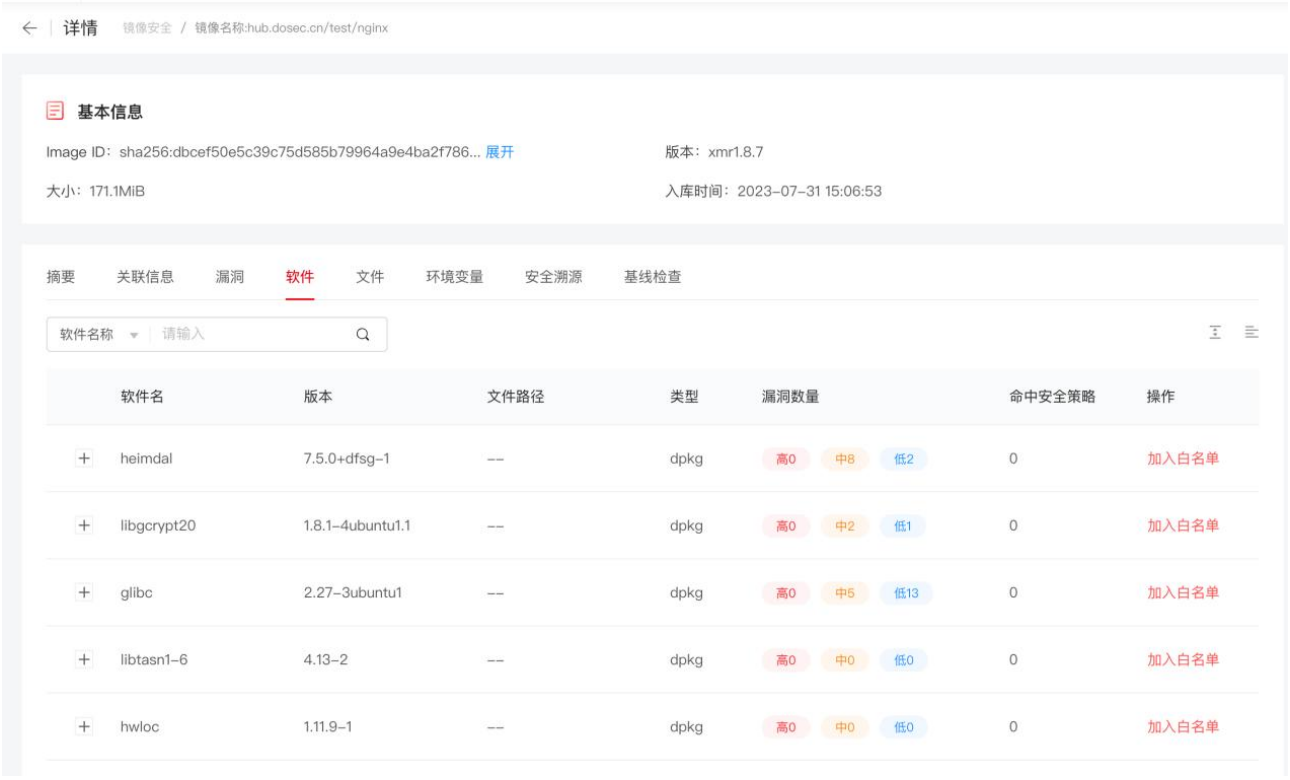



- 单击漏洞详情操作列的“加入白名单”可忽略此漏洞。添加完成后，扫描该镜像将不再展示已加入白名单的漏洞。

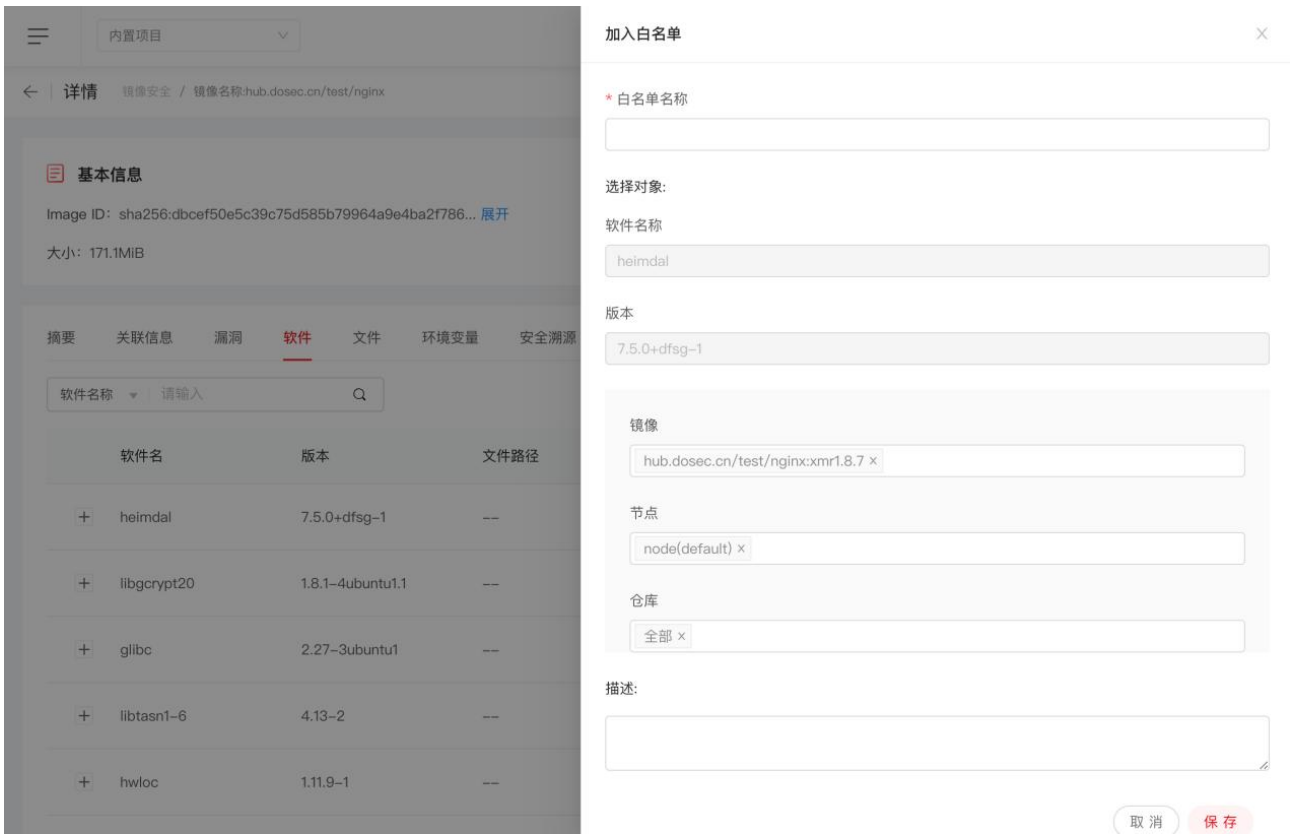



## 查看镜像软件信息

在“软件”页面，可查看当前镜像中软件的相关信息，可查看软件命中的策略，可将软件加入白名单。

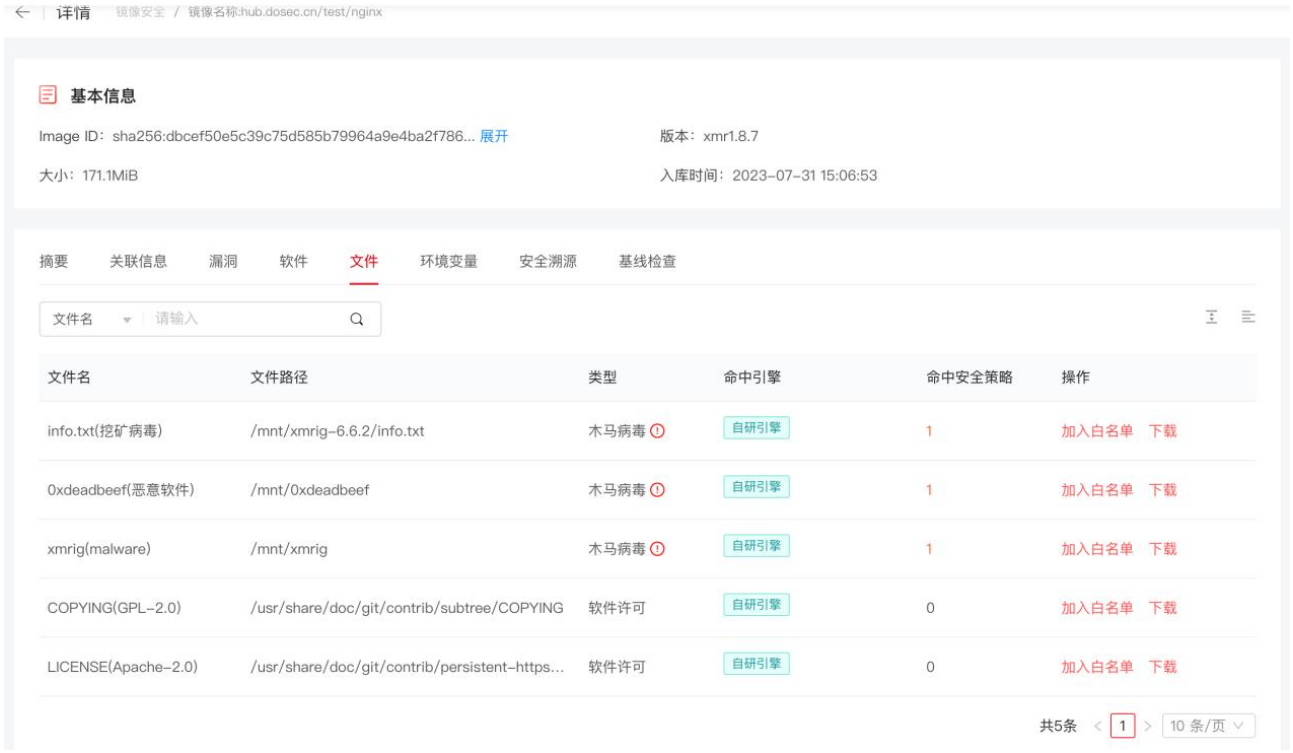


单击软件列表右侧的“加入白名单”，可屏蔽该软件的安全问题。添加完成后，此软件将不会命中安全策略。




## 查看镜像中文件信息

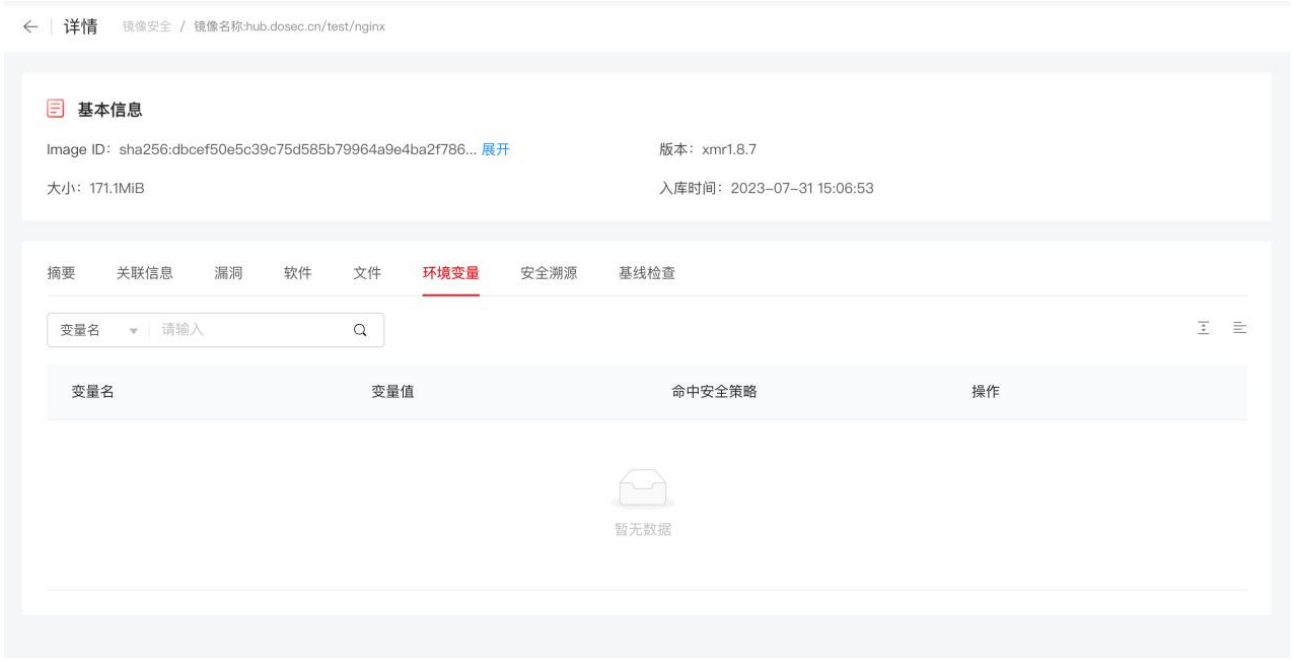
在“文件”页面，可以查看镜像中所有的文件信息，可查看文件命中的策略，可将文件加入白名单和下载到本地。




- 单击文件列表操作列的“加入白名单”，可屏蔽该文件的安全问题。
- 单击文件列表操作列的“下载”，可将文件下载到本地。
- 单击文件列表操作列的“文件预览”，方便用户不用下载也可查看文件内容。

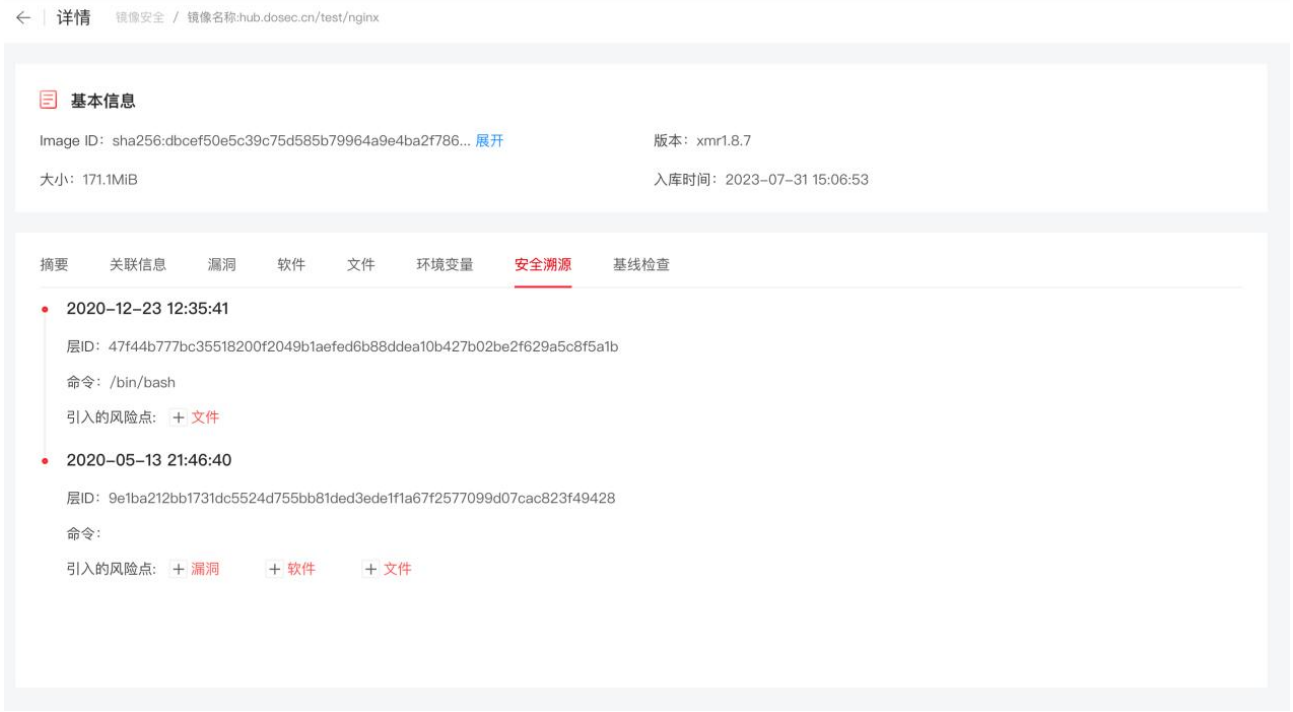

## 查看镜像环境变量

在“环境变量”页面，可以查看该镜像中所有的环境变量，可查看环境变量命中的安全策略。




## 安全溯源

在“安全溯源”页面，可以查看镜像构建历史中引入的安全风险及相关信息，包括镜像层的 ID、构建命令、引入风险点、操作时间。




# 4.2.6. 处置镜像

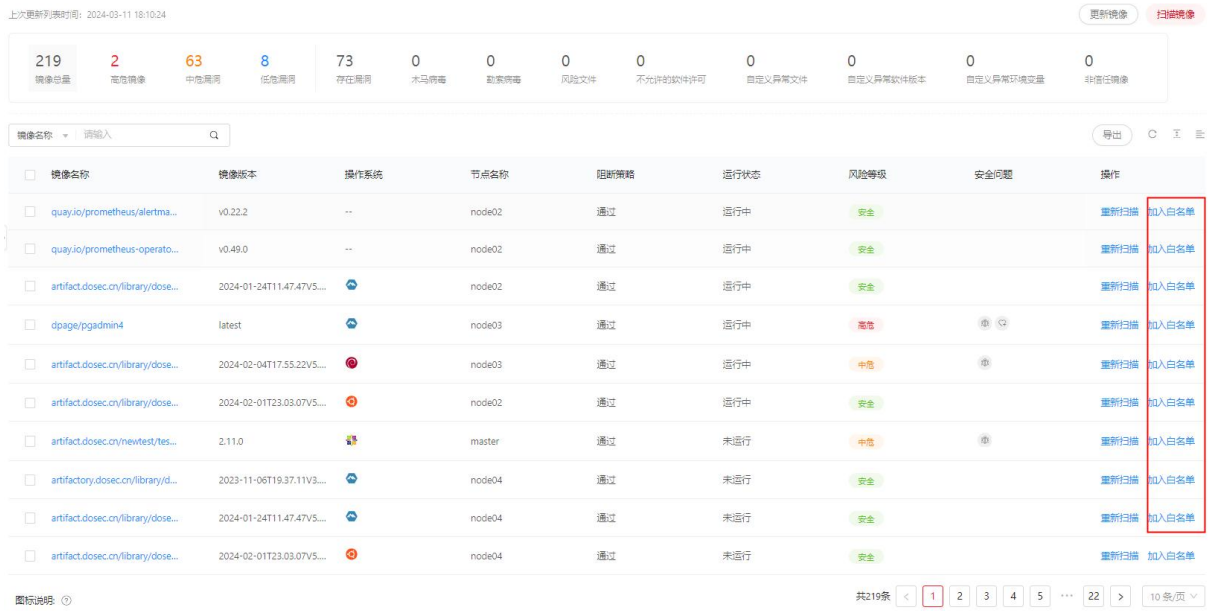
### 4.2.6.1. 修复漏洞

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“仓库镜像”或“节点镜像”页签，进入对应镜像列表页面。
4. 单击镜像列表中的“镜像名称”，进入镜像详情页面。
5. 在镜像详情页面的“摘要”页签底部，可以查看漏洞“安全建议”，为用户提供了漏洞的修复建议和异常文件处理建议，包括具体的做法和代码。

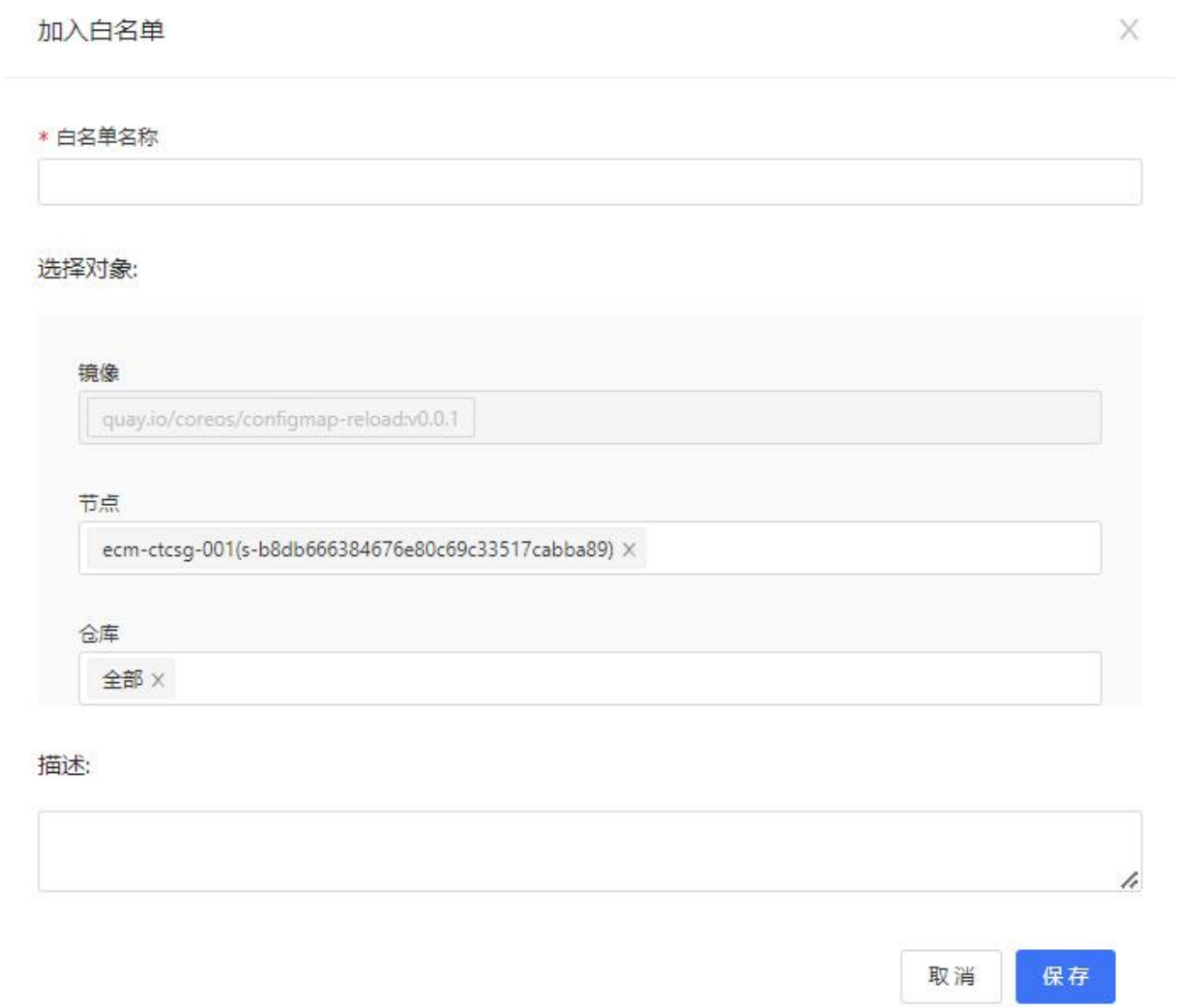

6. 单击安全建议右侧的“导出”图标，可将安全建议下载到本地，方便用户修改使用。

### 4.2.6.2. 加入白名单

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“仓库镜像”或“节点镜像”页签，进入对应镜像列表页面。
4. 单击镜像列表操作列中的“加入白名单”，进入加入白名单页面。




5. 输入白名单名称，选择应用于哪些节点和仓库，备注描述信息。




6. 单击“保存”，即可将该镜像加入白名单，之后在相应节点和仓库中扫描到该镜像时，将不会产生告警。

## 4.2.6.3. 设为基础镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“仓库镜像”页签，进入镜像列表页面。


4. 单击镜像列表操作列中的“设为基础镜像”，系统将提示操作成功。

5. 设为基础镜像后，需再次扫描镜像。
6. 扫描完成后，勾选列表上方的“显示基础镜像”，即可查看在当前仓库或项目中设置的所有基础镜像。

## 4.2.7. 管理白名单

### 新增白名单

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 单击镜像管理页面右上角的“白名单管理”，进入白名单管理页面。


4. 单击列表右上角的“新增白名单”，可以新增白名单。


5. 新增完成，可以在列表中看到刚才新增的白名单。
6. 白名单列表上方支持按照“白名单名称”、“内容”模糊搜索，按照“类型”定向筛选查询。


### 编辑白名单

单击操作列的“编辑”，即可查看或移除已添加到白名单中的镜像、漏洞、文件、软件、环境变量信息。

### 删除白名单

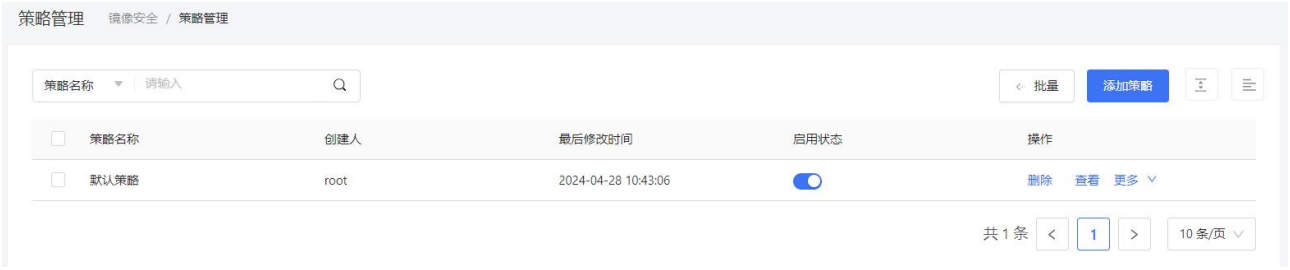
若不需要白名单时，可以单击操作列的“删除”，删除白名单。

> 注意：
>
> 删除白名单后不支持恢复，请谨慎操作。

## 4.2.8. 镜像策略管理

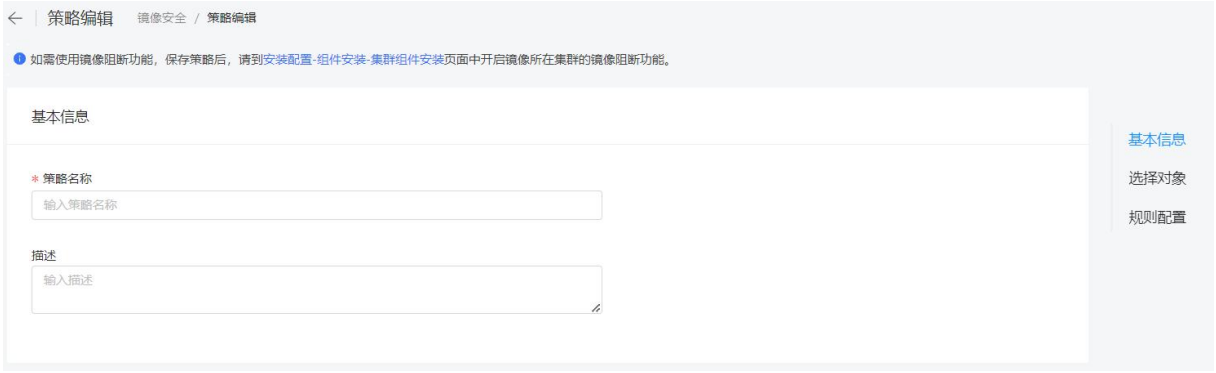
### 默认策略

有一个默认策略，默认为“启用”状态。默认策略应用对象为所有仓库、所有镜像，仅报警，不阻断。

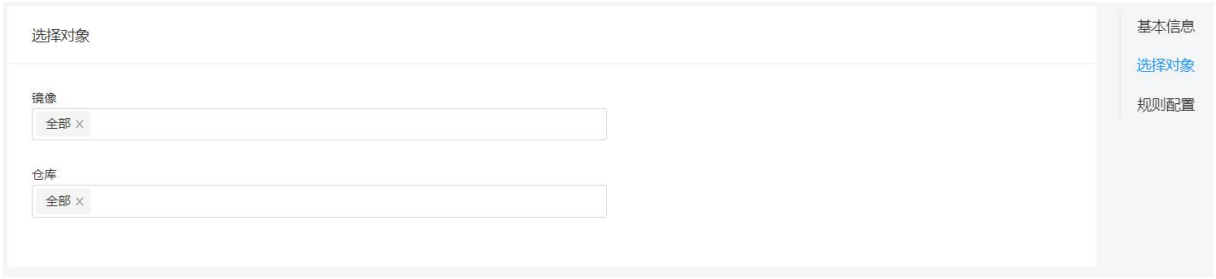



### 添加策略

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像策略”，进入镜像策略页面。
3. 单击“添加策略”，进入添加策略页面。
4. 输入策略的基本信息。




5. 选择策略对象，即指定该策略应用的镜像。




6. 对指定仓库中的镜像添加规则，通过添加这些规则来查看镜像、仓库中有哪些漏洞。

> 说明：
>
> 需要先输入策略的基本信息、选择策略对象后，才能添加具体规则。


7. 配置完成后单击“保存”，保存策略配置。

## 批量设置策略

还支持批量对策略进行处理，包括启用、禁用、删除。

1. 登录容器安全卫士控制台。

2. 在左侧导航栏选择“镜像安全 > 镜像策略”，进入镜像策略页面。
3. 勾选策略名称前的复选框，选择要操作的策略。


4. 单击选择列表上方的“批量”按钮，展开批量操作。
5. 根据需要选择执行的操作，支持批量启用、禁用、删除。

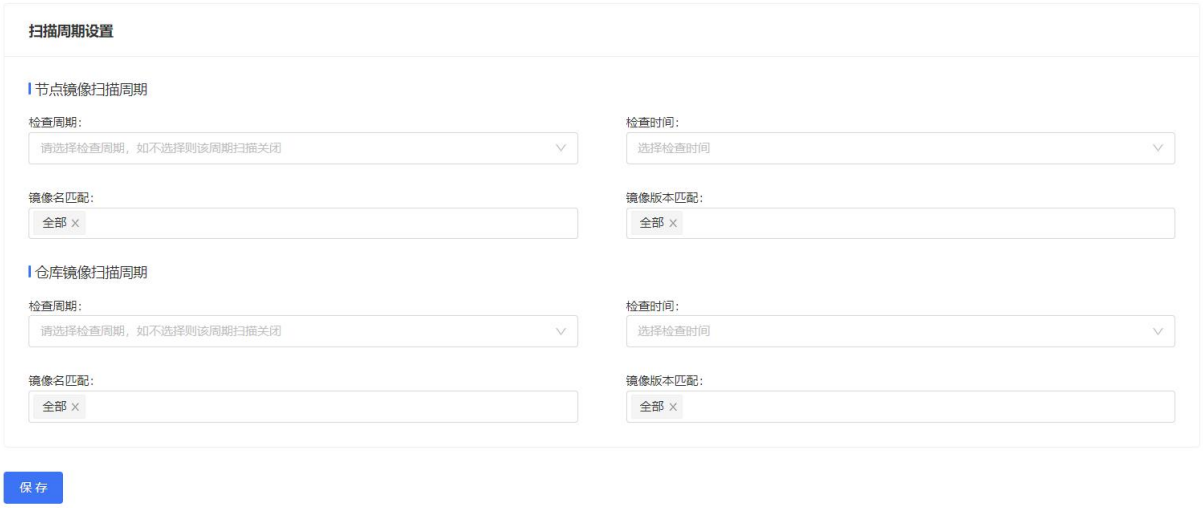
## 4.2.9. 镜像设置

### 4. 2. 9. 1. 扫描设置

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像设置”，进入镜像设置页面。
3. 选择“扫描设置”页签。设置扫描类型、自动扫描节点新增镜像和周期扫描等。

   扫描类型支持如下两种：

   - 快速扫描：只扫描包管理器安装的软件。
   - 深度扫描：在快速扫描的基础上增加扫描第三方依赖库、Web 框架库和病毒木马等恶意文件。

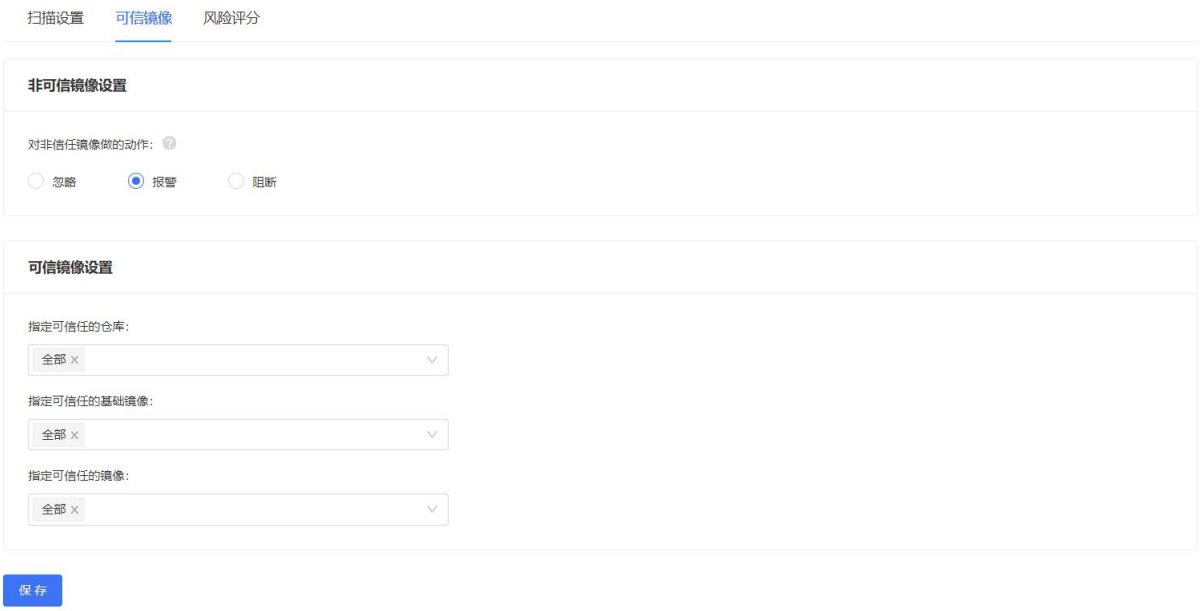



4. 配置完成后，单击“保存”。

## 4.2.9.2. 指定可信镜像

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像设置”，进入镜像设置页面。
3. 选择“可信镜像”页签。指定可信任的仓库、基础镜像、节点镜像，可对非信任的镜像进行忽略、报警、阻断的操作。

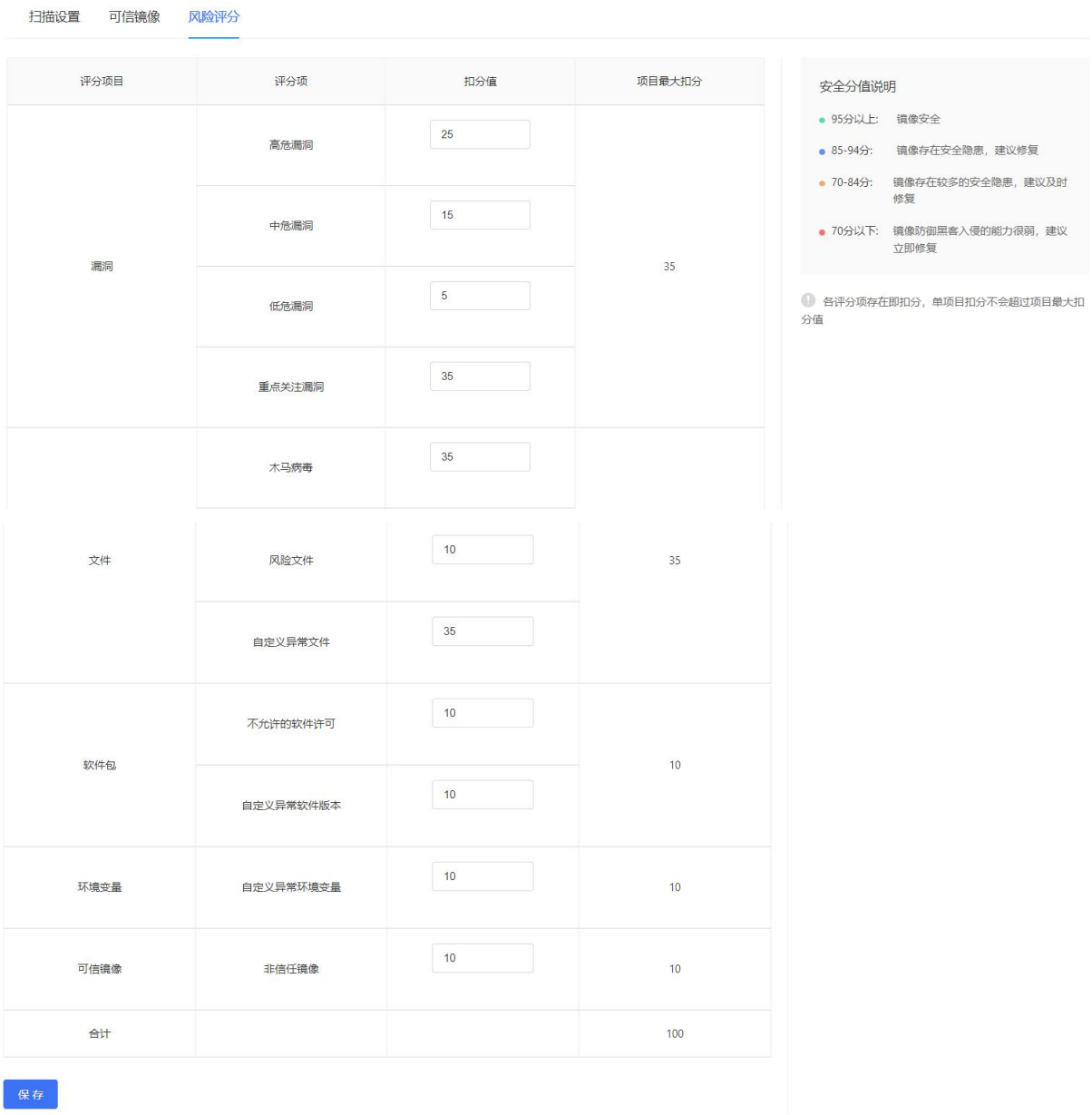
> 说明：
>
> 如需使用镜像阻断功能，请在“安装配置 > 组件安装”页面中开启镜像所在集群的镜像阻断功能，详细操作请参见集群组件配置。




4. 配置完成后，单击“保存”。

## 4.2.9.3. 查看风险评分

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像设置”，进入镜像设置页面。
3. 选择“风险评分”页签。可以自定义设置评分项。
   - 总分固定为 100，所有评分项目总和不得超过 100，所有子扣分项的分数不得超过对应评分项目的最大扣分值。
   - 扣分规则为发现即扣分，不考虑该风险项的数量，例如发现高危漏洞扣 25 分，则无论发现多少高危漏洞都只扣除 25 分。
   - 在风险评分表的右侧有各个分数段的安全分值说明。




4. 配置完成后，单击“保存”。

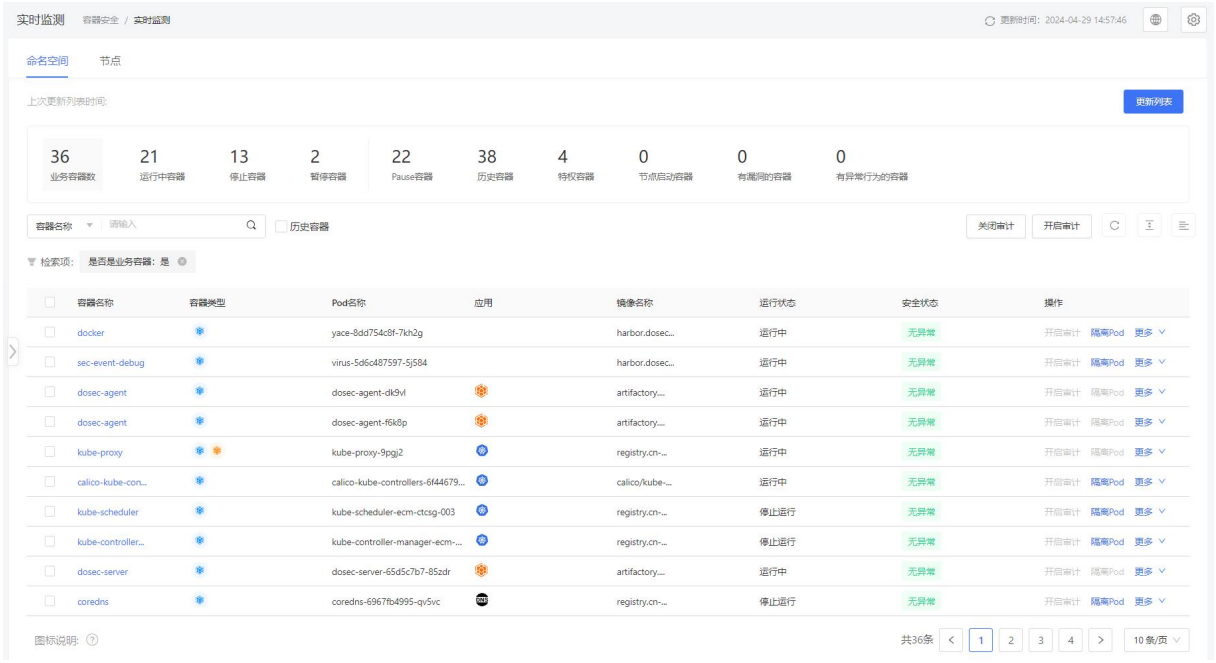
# 4. 3. 容器安全

## 4.3.1. 更新容器列表

容器运行时安全是容器安全管控的重中之重。目前传统的入侵检测方式主要针对于主机或者网络层面，现有防护手段无法发现针对容器层面的攻击行为。容器安全防护平台支持对容器内行为进行检测。当发现容器逃逸行为、反弹 shell、端口扫描、启动挖矿程序、启动远程木马程序时，根据预设策略对存在异常的容器进行报警或暂停，并支持对容器所在的 Pod 进行隔离或重启。

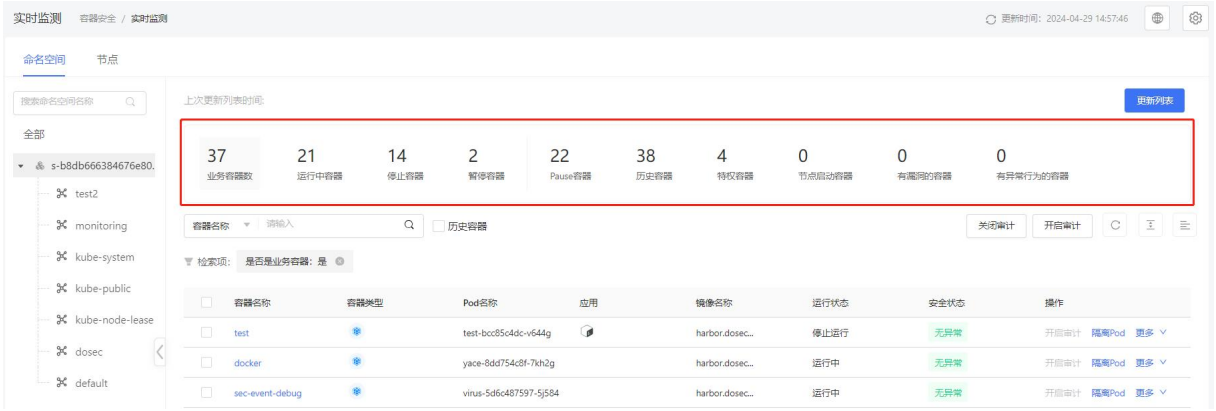
### 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 在该页面单击容器列表右侧的“更新列表”，实时获取集群内的容器信息。

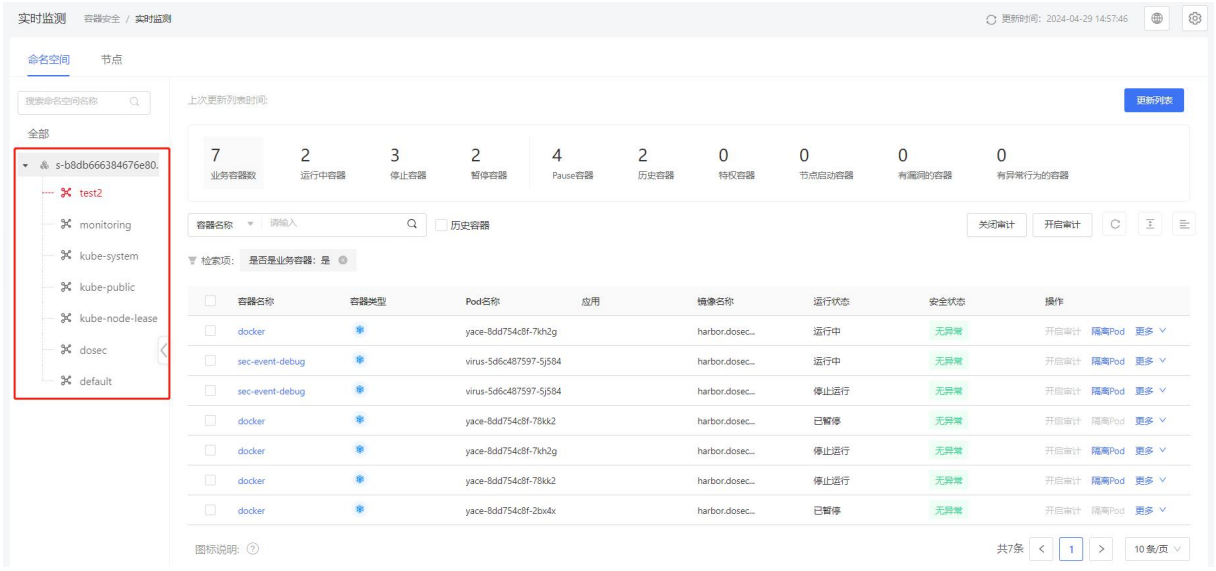



## 4.3.2. 查看容器列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 分类查看容器信息：选择“节点”和“命名空间”页签，可以更直观地分类查看集群中各个节点和各个命名空间上的容器信息。
4. 查看汇总统计信息：容器列表上方汇总展示了当前节点或命名空间中各类型的容器数量，包括运行中容器、特权容器、节点启动容器、有漏洞的容器和有异常行为的容器等，单击想要查看的容器类型，下方容器列表会根据单击选择的条件进行筛选。




5. 随着在左侧树形结构中的选择改动，右侧统计结果将响应式动态变化。



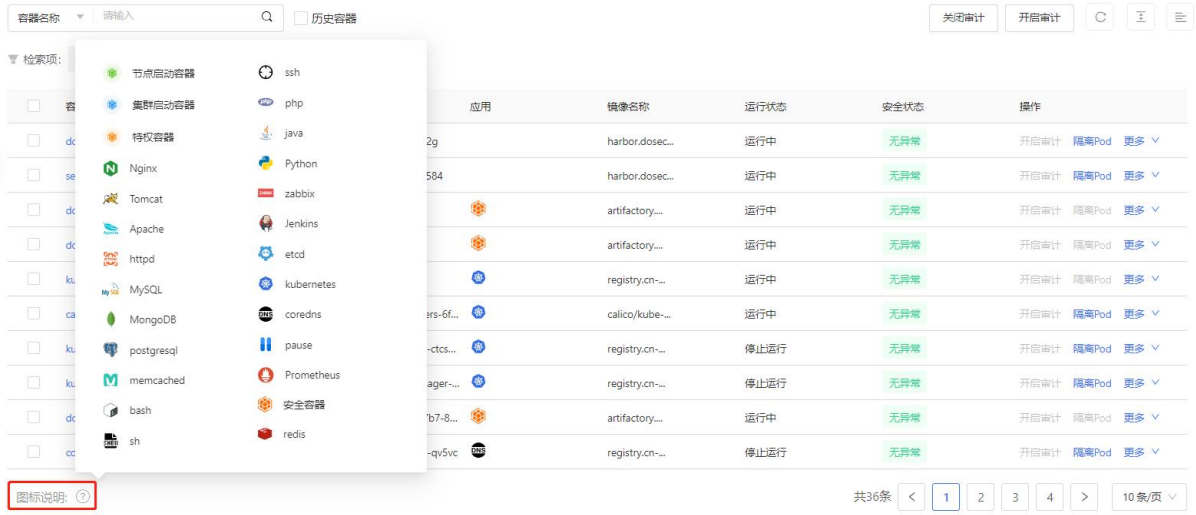

6. 查看容器列表：容器列表内，支持按照“容器名称”、“镜像名称”、“Pod 名称”、“容器标签”、“容器 IP”、“容器类型”、“运行状态”、“安全状态”等进行筛选查询。

容器列表内各参数说明如下：

| 参数 | 说明 |
| --- | --- |
| 容器名称 | 容器的名称。 |
| 容器类型 | 容器类型分为集群启动容器、节点启动容器和特权容器。 |
| Pod 名称 | 容器所属 Pod 的名称。 |
| 应用 | 容器所提供的应用服务，如 kubernetes、apache、nginx 等。 |

| 参数 | 说明 |
| --- | --- |
| 镜像名称 | 关联镜像是指该容器基于哪个镜像构建的。 |
| 运行状态 | 运行状态分为运行中、停止运行、已暂停、已删除。 |
| 安全状态 | 安全状分为“有异常”和“无异常”，有异常是指触发了安全策略产生告警的容器。 |

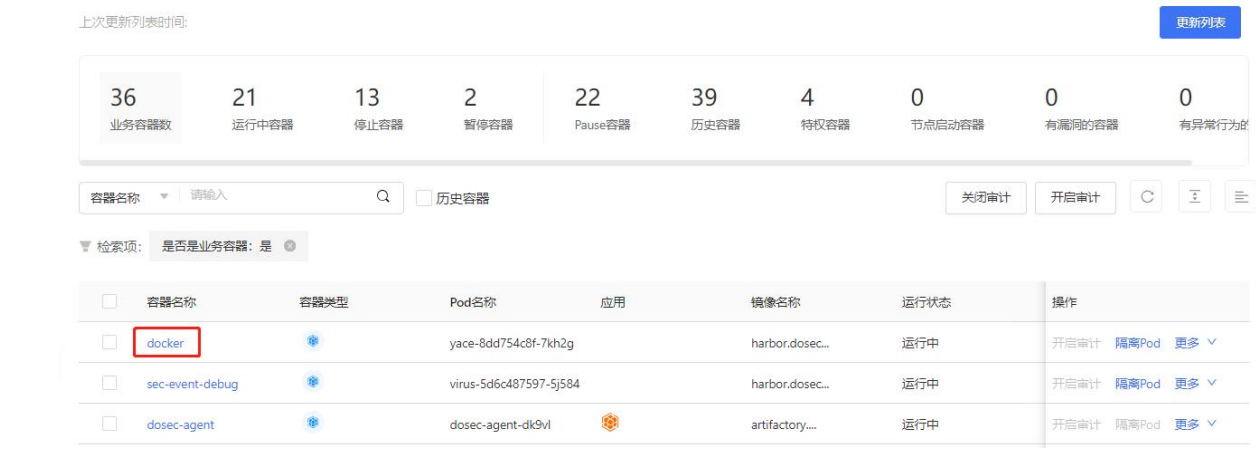
7. 查看图标说明：在容器列表左下角，可查看容器列表中图标的说明信息，前三个图标（节点启动容器、集群启动容器、特权容器）表示的是容器类型，其余图标表示的是容器列表中的应用。




## 4.3.3. 查看容器详情

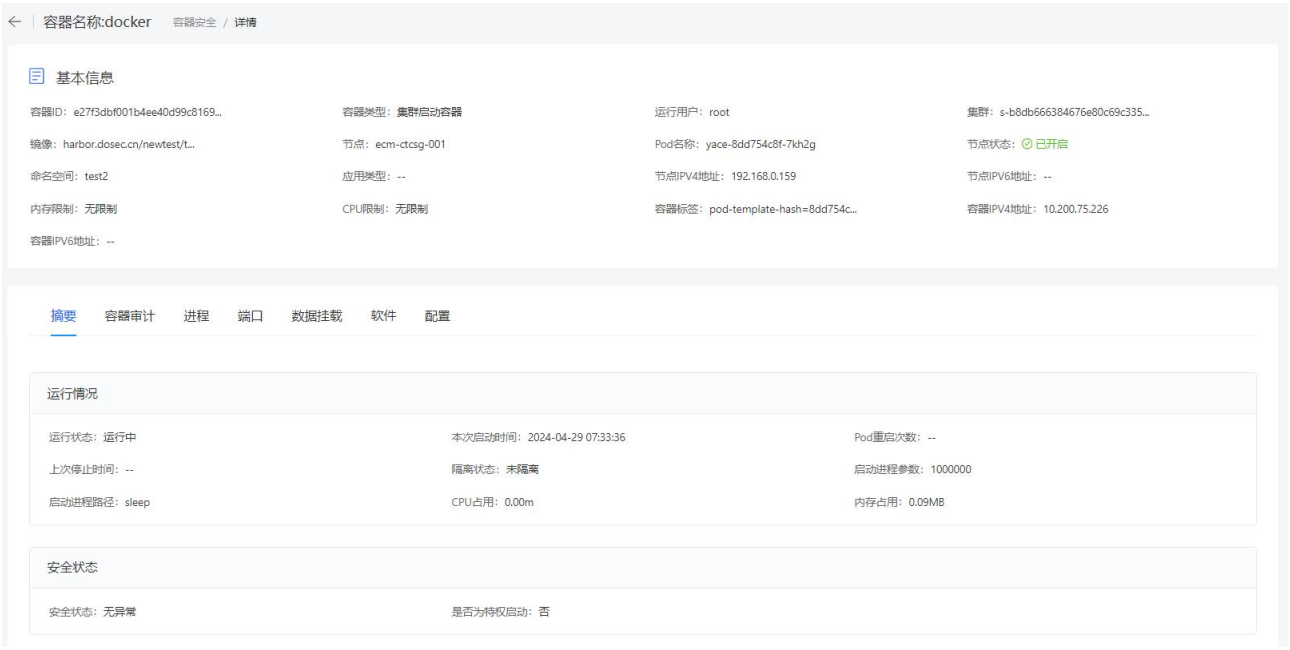
### 进入容器详情页面

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 单击容器列表中的容器名称，可以查看容器的基本信息、进程、端口、数据挂载、软件、配置等信息。



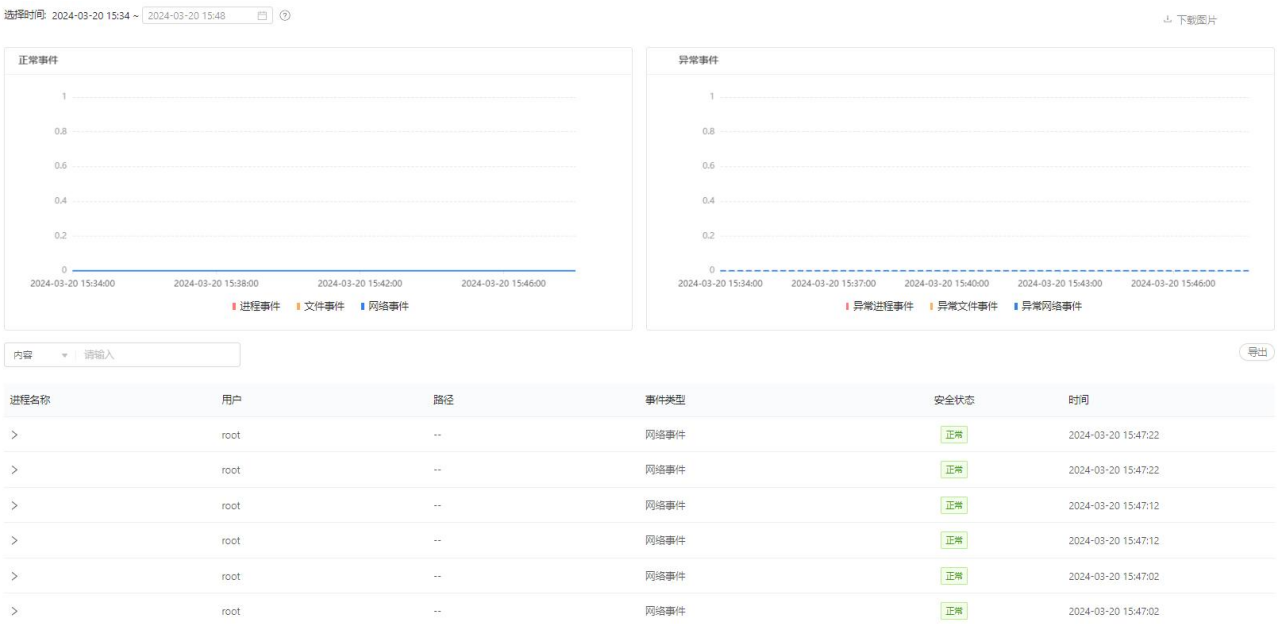

## 查看容器基本信息

容器信息页面展示了容器的基本信息、运行情况、安全状态等信息。



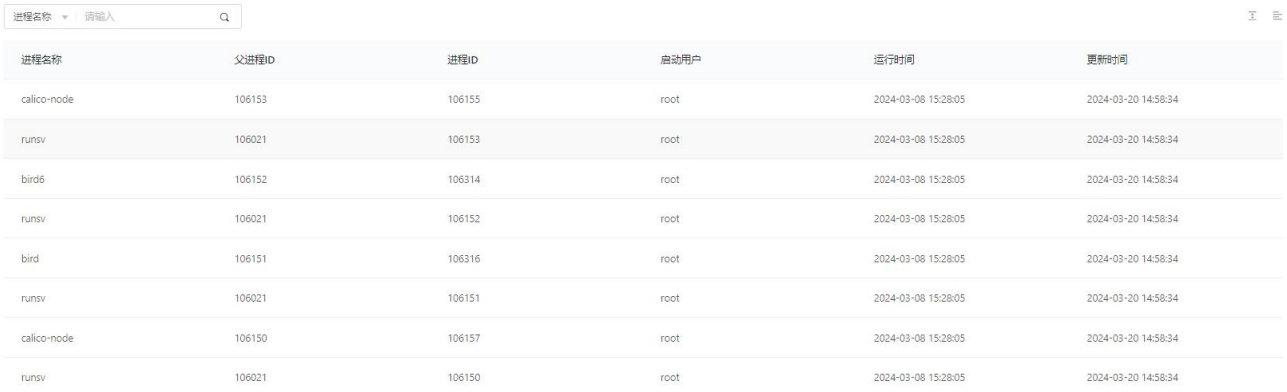

## 查看容器审计

容器审计页面统计展示了正常事件和异常事件的数量随时间变化的折线图。




## 查看容器进程信息

进程信息页面展示了容器内的进程名称、父进程 ID、进程 ID、启动用户、运行时间、更新时间等信息。

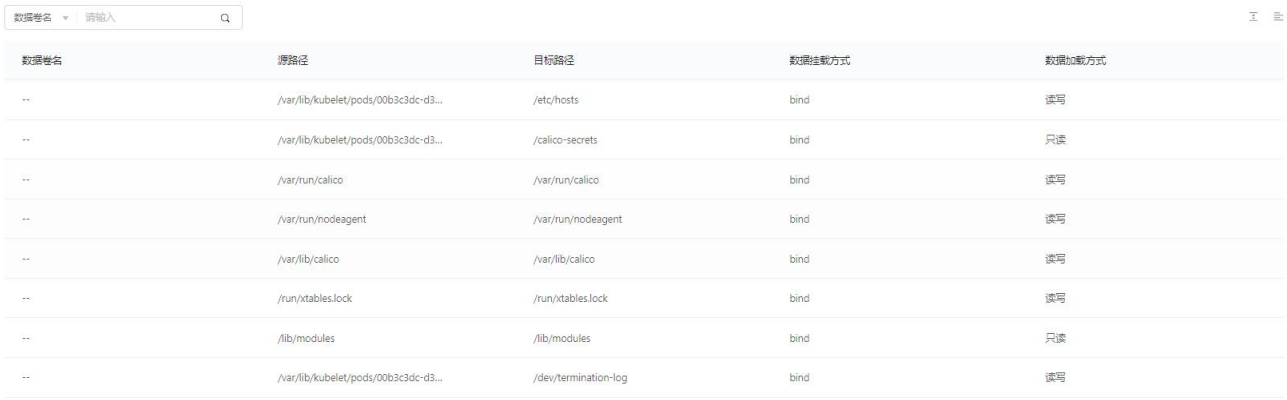



## 查看容器端口信息

端口页面展示了容器的端口信息，包括容器端口、进程、节点端口、IPv4、IPv6、绑定 IP、协议信息。


## 查看数据挂载

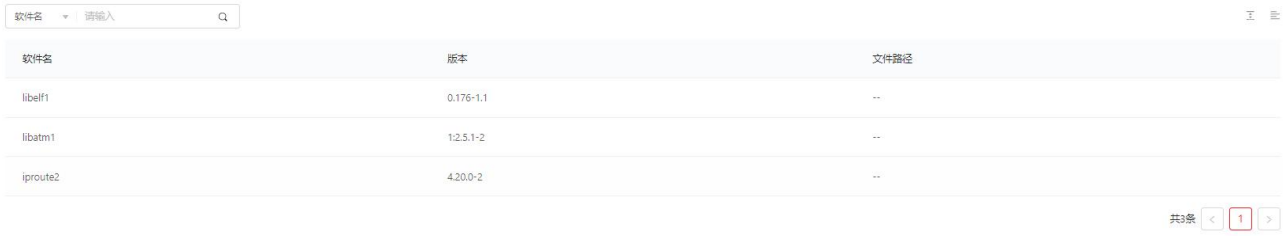
数据挂载页面展示了容器的数据挂载信息，包括数据卷名、源路径、目标路径、数据挂载方式、数据加载方式。



| 数据卷名 | 源路径 | 目标路径 | 数据挂载方式 | 数据加载方式 |
| --- | --- | --- | --- | --- |
| -- | /var/lib/kubelet/pods/00b3c3dc-d3... | /etc/hosts | bind | 读写 |
| -- | /var/lib/kubelet/pods/00b3c3dc-d3... | /calico-secrets | bind | 只读 |
| -- | /var/run/calico | /var/run/calico | bind | 读写 |
| -- | /var/run/nodeagent | /var/run/nodeagent | bind | 读写 |
| -- | /var/lib/calico | /var/lib/calico | bind | 读写 |
| -- | /run/xtables.lock | /run/xtables.lock | bind | 读写 |
| -- | /lib/modules | /lib/modules | bind | 只读 |
| -- | /var/lib/kubelet/pods/00b3c3dc-d3... | /dev/termination-log | bind | 读写 |

## 查看软件信息

软件页面展示了容器软件信息，包括软件名称、版本、文件路径等信息。



| 软件名 | 版本 | 文件路径 |
| --- | --- | --- |
| libelf1 | 0.176-1.1 | -- |
| libatm1 | 1:2.5.1-2 | -- |
| iproute2 | 4.20.0-2 | -- |

共3条 1

## 查看配置信息

配置页面展示了容器内的配置信息，包括配置项、值、安全建议等信息。

| 配置项 | 值 | 安全建议 |
| --- | --- | --- |
| Mounts.Source | /lib/modules | docker 容器挂载敏感目录，敏感目录包括"/，/root，/etc，/boot，/dev，/lib，/proc，/sys，/usr"，docker容器启动时挂载敏感目录到容器内，会造成敏感信息泄漏的风险，所以docker容器启动命令中应删除挂载的敏感目录，如：--volume(或者-v) /dev:/host/dev。 |
| PidsLimit | -- | 为防止容器内创建的进程数量过多，而导致内存、CPU消耗过快。在容器启动时使用--pids-limit参数，来限制容器在指定时间内创建进程的数量，减少内存、CPU消耗的资源。 |
| Health | -- | 如果容器镜像没有定义HEALTHCHECK指令，请在容器运行时使用--health-cmd参数来检查容器的健康状态。 |
| UsernsMode | -- | 无 |
| ReadonlyRootfs | false | 容器读写根文件系统，会造成根文件的损害。可以在容器启动时添加--read-only参数，将根文件系统设置为只读，来防止容器运行时写入数据到容器的根文件系统。 |
| UTSMode | host | 当容器共享主机的UTS namespace时，UIS命名空间会提供两个系统标识符主机名和NIS域名，用于设置在命名空间中运行的主机名和域名。如果不需要共享主机的UTS namespace，在启动时删除--uts=host参数。 |
| IpcMode | container:fb0a164eed5b011753daad0beebfd22027315f7dd6a95deed5add8fdc2025e88 | 无 |
| NetworkMode | container:fb0a164eed5b011753daad0beebfd22027315 | 无 |

# 4.3.4. 处置风险容器

## 4. 3. 4. 1. 隔离容器

支持将存在异常的 Pod 进行隔离，被隔离的 Pod 将不允许与其他资源进行通信。

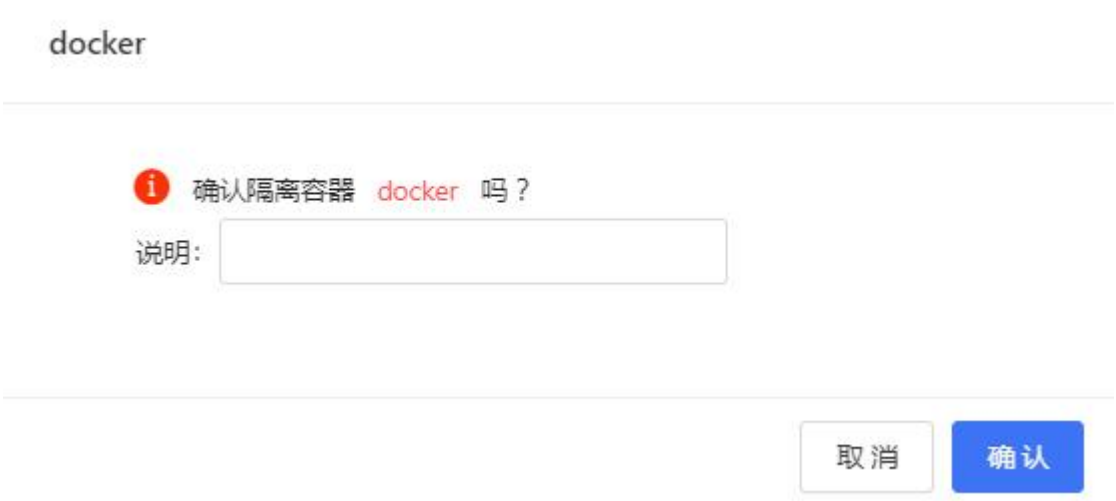
### 注意事项

特权容器、节点启动容器、安全容器、pause 应用类型容器暂不支持隔离。

## 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 单击容器列表右侧操作列中的“隔离 Pod”。


4. 在弹出的对话框中，输入说明信息。




5. 单击“确认”，隔离容器。

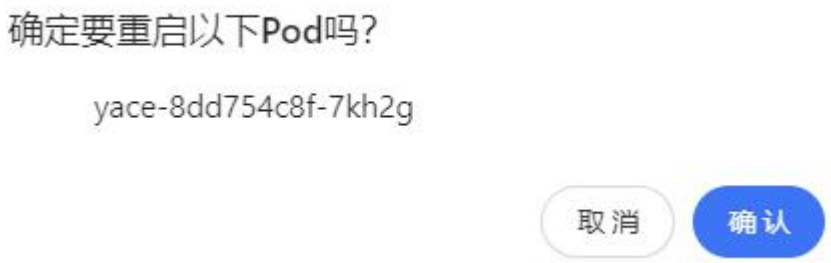
## 4. 3. 4. 2. 重启 Pod

通过重启 Pod，可以将存在异常的 Pod 进行杀死，通过 K8s 机制再重新启动一个新的 Pod。

## 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 单击容器列表右侧操作列中的“重启 Pod”。


4. 在弹出的提示框中单击“确认”。




## 4. 3. 4. 3. 暂停容器

### 注意事项

运行状态已停止的容器和历史容器不支持暂停操作。

### 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 单击容器列表右侧操作列中的“暂停”按钮，可以暂停存在异常的容器。


### 相关操作

恢复容器为“运行中”状态：暂停后的容器支持在操作列中单击“恢复”按钮，恢复容器运行状态。

## 4.3.5. 容器审计

## 4.3.5.1. 开启审计功能

在容器安全列表内，可以查看审计功能是否已开启。若操作列中开启审计字体为“灰色”，表示审计功能暂不可用，需要先开启该功能；若为“红色”，则表示审计功能可用。

### 集群开启审计功能

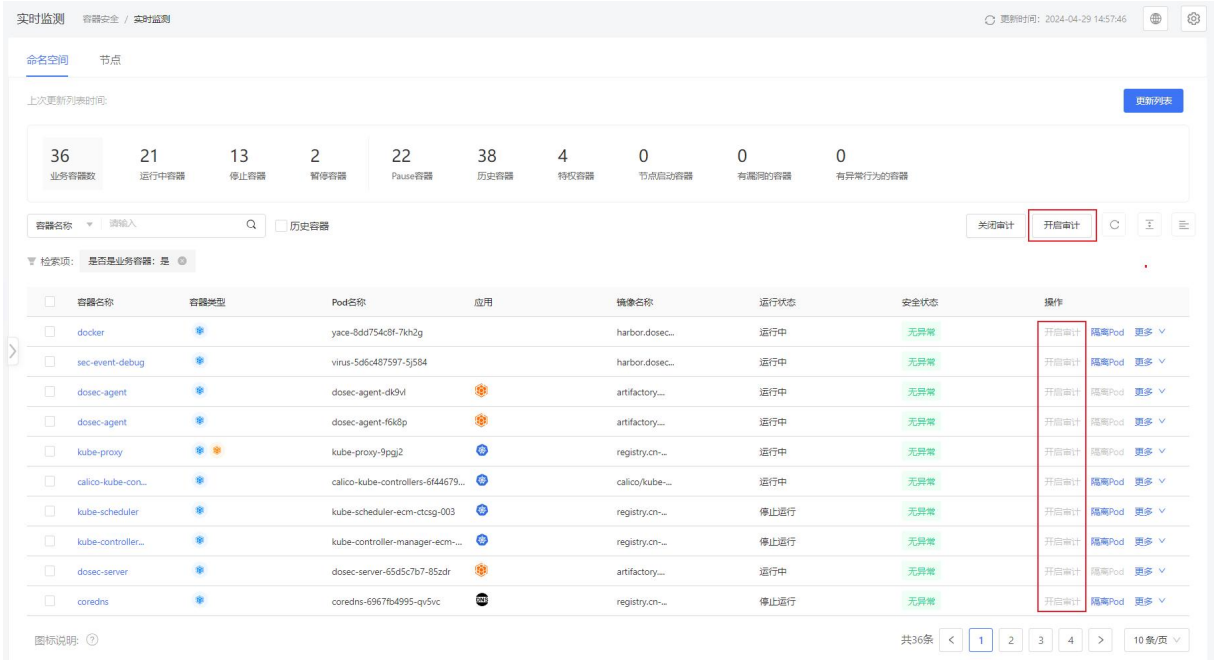
1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“安装配置 > 组件安装”，进入组件安装页面。


3. 单击集群列表操作列的“集群组件配置”，进入集群全局设置页面。


4. 开启容器审计功能，单击“保存”。

## 容器开启审计功能

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“容器安全 > 实时检测”，进入实时检测页面。




3. 在容器列表操作列单击“开启审计”，或勾选多个容器，单击列表右上方的“开启审计”，批量为容器开启审计功能。

## 配置容器审计

配置“容器调查审计信息保留时间”或“容器调查审计信息保留容量”。详细操作请参见容器设置。

# 4.3.5.2. 查看审计信息

容器审计提供正常和异常的容器事件统计，包括容器进程事件、文件事件、网络事件。

## 前提条件

容器集群已开启审计功能。

## 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 实时检测”，进入容器实时检测页面。
3. 单击容器列表内的容器名称，进入容器详情页面。
4. 选择“容器审计”页签，进入审计详情页面。可查看容器的正常事件和异常事件的数量随时间变化的折线图（默认统计最近 15 分钟内的事件），又分类统计了容器的进程事件、文件事件、网络事件的数量，可通过选择时间或拖拽下方进度条来查看不同时间段内，容器发生的事件信息。


5. 查看事件列表：在统计图下方以列表展示了容器中发生的事件信息，单击列表中某行，可展开查看对应事件的详细信息。


容器审计事件参数说明：

| 参数 | 说明 |
| --- | --- |
| 进程名称 | 进程的名称。 |
| 用户 | 执行用户。 |

| 参数 | 说明 |
| --- | --- |
| 路径 | 执行命令所在路径。 |
| 进程命令行 | 具体执行的命令行。 |
| 事件类型 | 容器的事件类型，分为进程事件、文件事件和网络事件。<br>• 进程事件：指在容器中运行进程的事件；<br>• 文件事件：指容器中对文件的读操作和写操作产生的事件；<br>• 网络事件：指访问、监听等网络活动产生的事件。 |
| 安全状态 | 安全状态分为“正常”和“异常”这两种状态。 |
| 时间 | 事件发生的时间，事件列表中以时间倒序的顺序进行展示。 |

## 4.3.6. 容器策略管理

### 4. 3. 6. 1. 入侵检测策略

容器的入侵行为主要是对命令执行、读写文件、网络活动、主机异常等类型进行监测。

平台支持多类检测规则，对黑客的攻击行为进行检测防护，且支持预设策略的方式，将入侵行为在事件发生的第一时间对容器进行暂停并支持对容器所在的 Pod 进行隔离或重启。

#### 默认策略

平台内置默认策略的启用状态默认为“启用”，且仅支持查看、编辑，不支持删除。

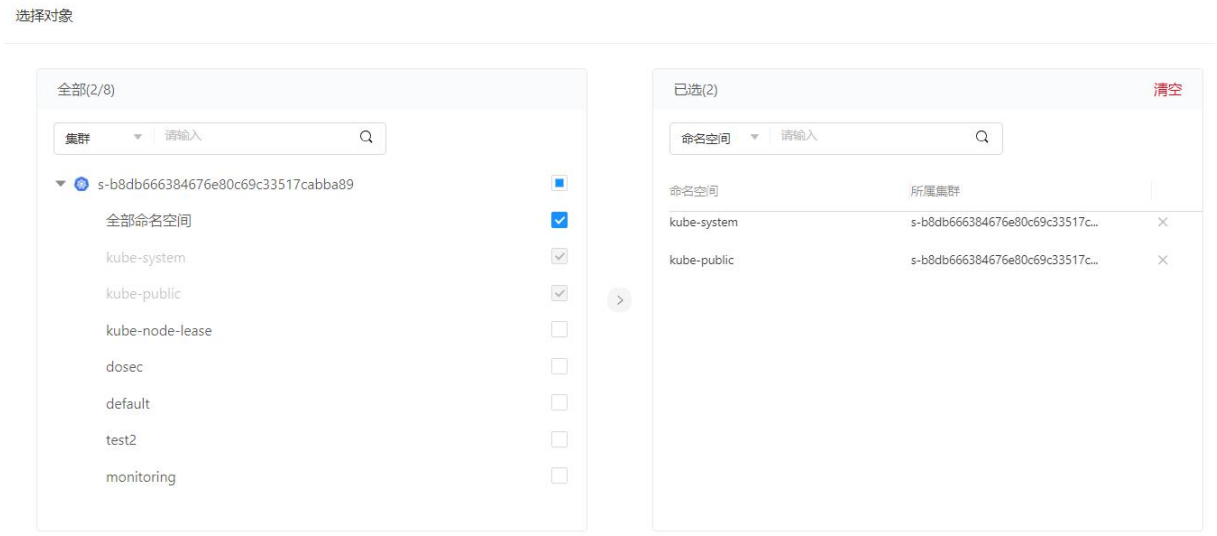
- 编辑默认策略时，支持选择应用对象、自定义规则等操作。
- 默认策略包含的检测规则请参见系统内置规则。


#### 添加策略

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 容器策略”，进入容器策略页面。

3. 在“入侵检测策略”页签，单击“添加策略”，进入添加策略页面。
4. 配置基本信息。


5. 选择策略应用的对象。




6. 配置策略规则，包括使用哪些规则，配置规则处置方式等。

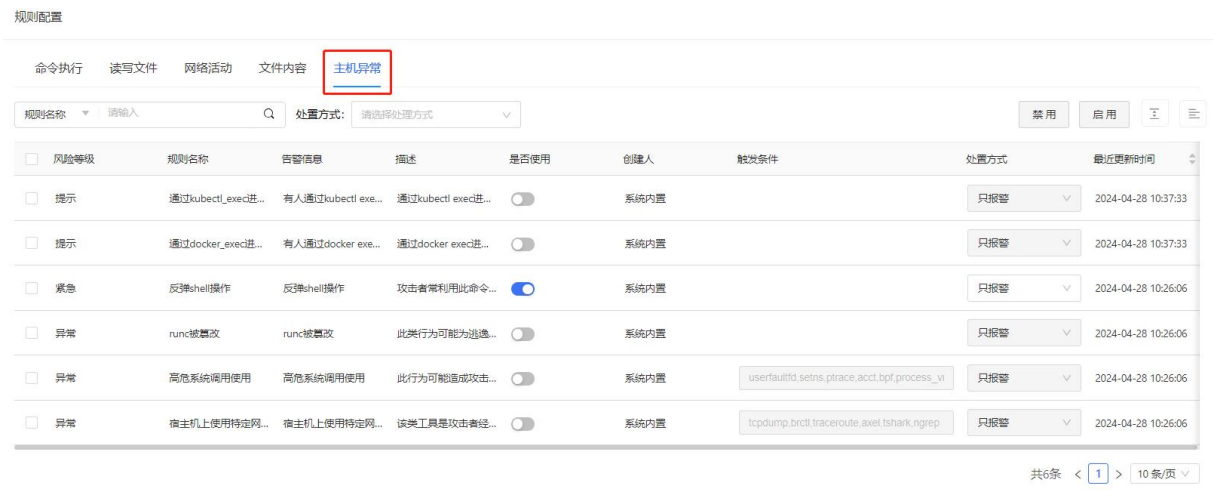
   每条入侵行为下，有相关的行为描述和开启建议，用户可进行参考设置。

说明：

可以为单个规则修改处置方式，也可以批量为规则修改处置方式：

- 单个规则：规则启用后才支持修改处置方式。
- 批量设置：勾选规则前的复选框，选择要启动报警的内置策略，在列表上方的报警“处置方式”下拉框中批量设置报警处理方式。
- 处置方式包含只报警、报警且隔离 Pod、报警且重启 Pod、报警且暂停容器这四种处理方式。


仅系统内置策略支持配置“主机异常”规则：




7. 参数配置完成后，单击“保存”。

## 复制策略

通过复制策略，可以快速添加一个和已有策略类似的策略。

1. 登录容器安全卫士控制台。

2. 在左侧导航栏选择“容器安全 > 容器策略”，进入容器策略页面。
3. 在“入侵检测策略”页签，在已有策略的操作列单击“复制策略”，进入复制策略页面。
4. 策略配置的详细说明请参考添加策略。

### 编辑策略

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 容器策略”，进入容器策略页面。
3. 在“入侵检测策略”页签，在已有策略的操作列单击“编辑”，进入编辑策略页面。
4. 在策略编辑界面，可以修改策略名称、策略应用的对象、检测规则配置对应的处理方式。策略配置的详细说明请参考添加策略。

### 批量管理策略

支持批量对策略进行管理，包括启用、禁用、删除。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“容器安全 > 容器策略”，进入容器策略页面。
3. 在“入侵检测策略”页签，勾选入侵行为名称前的复选框，选择要操作的策略。


4. 单击选择列表上方的“批量”按钮，展开批量操作。
5. 根据需要选择执行的操作，支持批量启用、禁用、删除。

## 4.3.6.2. 入侵检测规则

系统内置了丰富的检测规则，用户也可以根据需求自定义检测规则。

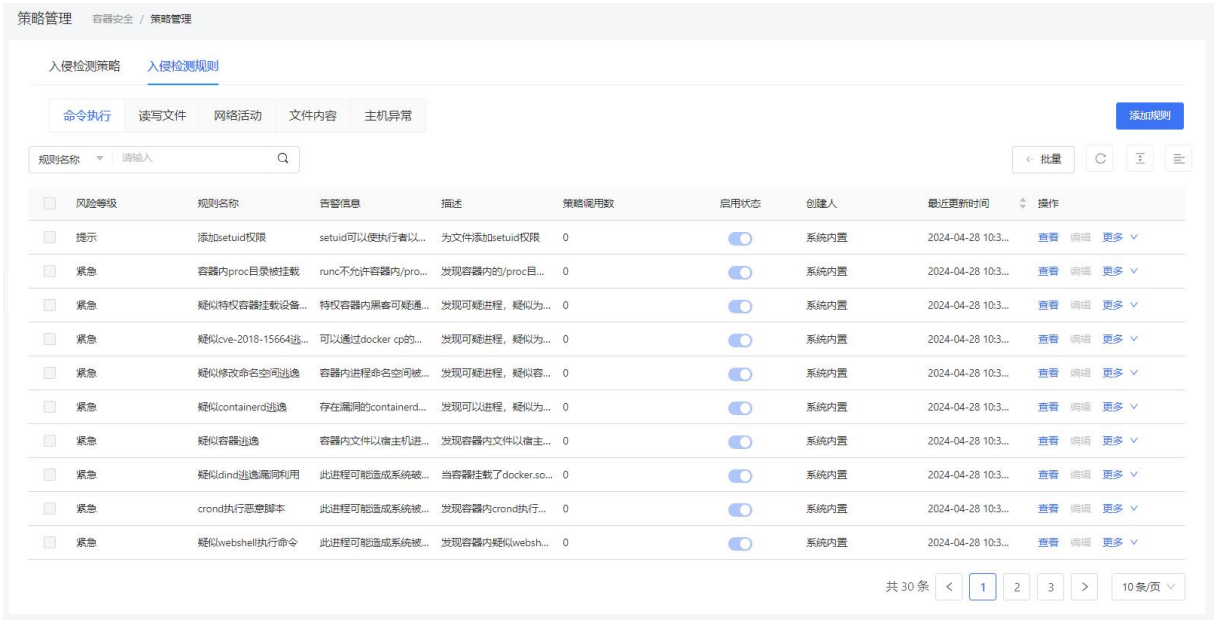
- 系统内置规则仅支持查看，不支持复制、编辑、删除等操作。
- 支持添加、编辑、删除自定义规则。

### 添加自定义规则

说明：

不支持添加“主机异常”类的自定义规则。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“容器安全 > 容器策略”，进入容器策略页面。
3. 选择“入侵检测规则”页签。




4. 单击“添加规则”，进入添加规则页面。

添加规则

* 规则名称

请输入规则名称

规则描述

请输入规则描述信息

是否启用

是 否

* 告警信息

请输入告警信息

* 规则类型

请选择规则类型

* Att&ck战术

请选择Att&ck战术

* Att&ck技术

请选择Att&ck技术

* 风险等级

请选择风险等级

* 规则内容（请参考模版格式编写规则内容）

请输入规则内容

修复建议

请输入修复建议

* 开启建议

建议开启

取消 保存

5. 在入侵检查规则页面输入规则名称（必填）和规则描述（非必填），选择是否启用，输入告警信息、选择规则类型（命令执行、网络活动、文件读写、文件内容）、Att&ck 战术、Att&ck 技术、风险等级、规则内容（DSL）、修复建议、开启建议。
6. 单击“保存”，生成一条新规则。

## 系统内置规则

| 类型 | 检测项 | 说明 |
| --- | --- | --- |
| 命令执行 | 启动特权容器 | 以特权模式启动容器相当于拥有服务器的管理员权限，可以操作服务器上的任何资源、执行任意命令。 |
| | 容器内使用 ncat 工具 | 该类工具是攻击者经常使用的工具，用于下载工具、探测信息、进一步渗透等，业务进程较少使用。 |
| | 容器内使用特定网络工具 | 该类工具是攻击者经常使用的工具，用于下载工具、探测信息、进一步渗透等，业务进程较少使用。 |
| | 执行敏感命令 | 此类通常为攻击者获得低权限 shell 后试图利用 setuid 获得高权限行为。 |
| | 搜索私钥行为 | 攻击者搜索可利用的私钥从而登录并攻陷对应的服务器。 |
| | 疑似 contanerd 逃逸 | 发现可以进程，疑似为利用 cve-2020-15257 进行逃逸，请确认是否为黑客行为 |
| | 疑似修改命名空间逃逸 | 发现可疑进程，疑似容器内获取宿主机权限后修改容器命名空间为宿主机命名空间以达成容器逃逸，请确认是否为黑客行为 |
| | 执行远程文件传输命令 | 攻击者常利用此命令来下载后门、上传敏感信息等。 |
| | 创建指向敏感文件的软连接 | 攻击者常利用此命令来提升权限，业务进程较少使用。 |
| | 脏牛漏洞提权 | 利用 Linux 系统的 Copy On Write 写时复制的竞争条件漏洞，达到权限提升的目的，攻击者可利用此漏洞提升为管理员权限从而控制服务器。 |
| | 容器内 sudo 漏洞利用 | 利用 CVE-2019-14287，可以进行提权行为。 |

| 类型 | 检测项 | 说明 |
| --- | --- | --- |
| | kubectl cp 漏洞利用 | 利用 CVE-2019-1002101，关于 kubectl cp 漏洞利用行为。 |
| | java 内存马 | 攻击者利用 java 的类缺陷，动态的修改 java 程序在内存中的代码段，注入远控后门程序，实现远程控制，具有隐蔽、不落盘等特点。 |
| | 启动挖矿程序 | 攻击者在服务器上植入挖矿程序，占用服务器大量计算资源挖矿，会导致业务进程缓慢、卡死等风险。 |
| | 启动远程木马程序 | 攻击者入侵成功后留下的远控后门，方便持续渗透。 |
| | 执行具有 setuid 位的命令 | 此类通常为攻击者获得低权限 shell 后试图利用 setuid 获得高权限行为。 |
| | 伪装 k8s 容器 | 此类通常为攻击者进行伪装的恶意容器。 |
| | 启动容器挂载目录 | 当容器挂载了一些风险目录时，容器内可以修改宿主机中的某些关键文件，将会有逃逸或者提权的风险 |
| | 启动具有敏感权限容器 | 此类行为容易增加逃逸风险。 |
| | 隧道利用 | 该方式是攻击者经常使用，用于下载数据、探测信息等。 |
| | 疑似 CVE-2021-3156 漏洞利用 | 利用 CVE-2021-3156，可以进行提权行为。 |
| | 疑似 CVE-2021-25741 漏洞利用 | 利用 CVE-2021-25741，可使攻击者使用软链接的方式在容器中挂载指定 subPath 配置的目录逃逸到主机敏感目录。 |
| | 疑似 CVE-2022-0492 漏洞利用 | 利用 CVE-2022-0492，可以绕过命名空间隔离，从而造成容器逃逸。 |
| | 执行恶意脚本 | 发现容器内部执行恶意脚本，请检查是否是黑客行为 |
| | 内存恶意代码执行 | 发现容器内部内存恶意代码执行，请检查是否是黑客行为 |
| | 疑似 webshell 执行命令 | 发现容器内疑似 webshell 执行命令 |

| 类型 | 检测项 | 说明 |
| --- | --- | --- |
| | crond 执行恶意脚本 | 发现容器内 crond 执行恶意脚本，请检查是否为黑客行为 |
| | 疑似 dind 逃逸漏洞利用 | 当容器挂载了 docker.sock 或者其根目录，容器内如果安装 docker,就可利用 docker 联系 docker.sock 创建新的容器并挂载宿主机敏感目录，以达到容器逃逸的目的 |
| | 疑似 cve-2018-15664 逃逸 | 发现可疑进程，疑似为利用 docker cp 进行逃逸，请确认是否为黑客行为 |
| | 疑似特权容器挂载设备逃逸 | 发现可疑进程，疑似为利用特权容器挂载设备逃逸，请确认是否为黑客行为 |
| | 疑似容器逃逸 | 发现容器内文件以宿主机进程执行，具有容器逃逸的风险，请确认是否为黑客行为 |
| | 从磁盘中删除大容量数据 | 此类行为通常为攻击者破坏数据、清除痕迹的操作，也有可能是业务进程清理日志，请根据详情进一步确认。 |
| | 执行恶意脚本 | 发现容器内部执行恶意脚本，请检查是否是黑客行为 |
| | crond 执行恶意脚本 | 发现容器内 crond 执行恶意脚本，请检查是否为黑客行为 |
| | 容器内 proc 目录被挂载 | 发现容器内的/proc 目录被挂载，请检查容器是否为黑客启动。 |
| | 添加 setuid 权限 | 为文件添加 setuid 权限 |
| 读写文件 | runc 逃逸漏洞利用 | 疑似利用 runc 逃逸漏洞 CVE-2019-5736 |
| | 容器内发现恶意文件 | 此类文件通常为病毒、木马等具有破坏行为的文件。 |
| | 篡改计划任务 | 此类通常为攻击者的恶意操作。 |
| | docker-cp 漏洞利用 | 利用 CVE-2019-14271，关于 docker cp 的提权漏洞。 |
| | 疑似 CVE-2021-4034 漏洞利用行为 | 利用 CVE-2021-4034，可以进行提取行为。 |

| 类型 | 检测项 | 说明 |
| --- | --- | --- |
| | 操作敏感文件 | 此类行为可将正常的可执行文件修改为具有破坏行为的文件。 |
| | 篡改容器内可执行文件 | 此类行为可将正常的可执行文件修改为具有破坏行为的文件。 |
| | 疑似 mount-procfs 容器逃逸 | /proc/sys/kernel/core_pattern 文件是负责进程奔溃时内存数据转储的，当第一个字符是管道符\|时， 后面的部分会以命令行的方式进行解析并运行 |
| | 疑似重写 devices.allow 逃逸 | 发现可疑进程，疑似为利用重写 devices.allow 进行逃逸，请确认是否为黑客行为 |
| 网络活动 | 反弹 shell 操作 | 攻击者常利用此命令来绕过防火墙规则，远程控制服务器。 |
| | 容器暴力破解 | 此类行为通常是攻击者在尝试获取目标服务的权限。 |
| 文件内容 | - | 支持自定义文件内容检测 |
| 主机异常 | 通过 docker exec 进入 pod | 通过 kubectl exec 进入 pod，某些情况不允许。 |
| | 通过 docker_exec 进入容器 | 通过 docker exec 进入 pod，某些情况不允许。 |
| | 反弹 shell 操作 | 攻击者常利用此命令来绕过防火墙规则，远程控制服务器。 |
| | runc 被篡改 | 此类行为可能为逃逸行为。 |
| | 高危系统调用使用 | 此行为可能造成攻击利用。 |
| | 宿主机上使用特定网络工具 | 该类工具是攻击者经常使用的工具，用于下载工具、探测信息、进一步渗透等，业务进程较少使用。 |

## 4.3.7. 容器设置

1. 登录容器安全卫士控制台。

2. 在左侧导航栏，选择“容器安全 > 容器设置”，进入容器设置页面。也可以在容器实时检测页面，单击右上角的“设置”按钮，进入容器设置页面。
3. 设置“容器调查审计信息保留时间”和“容器调查审计信息保留容量”。


| 参数 | 说明 |
| --- | --- |
| 历史容器保留时间 | 默认为 7，不支持修改。 |
| 存在报警的历史容器保留时间 | 默认为 7，不支持修改。 |
| 容器调查审计信息保留时间 | 最大值为“1095 天”。<br>容器审计信息会记录大量事件，占用较大的磁盘空间，请根据磁盘剩余空间大小酌情配置保存天数。 |
| 容器调查审计信息保留容量 | 最大值为“65535G”。<br>容器审计信息会记录大量事件，占用较大的磁盘空间，请根据磁盘剩余空间大小酌情配置保存容量。 |

说明：

“容器调查审计信息保留时间”和“容器调查审计信息保留容量”两个参数值均为 0 时，代表关闭审计功能。

# 4. 4. 节点安全

## 4.4.1. 扫描节点

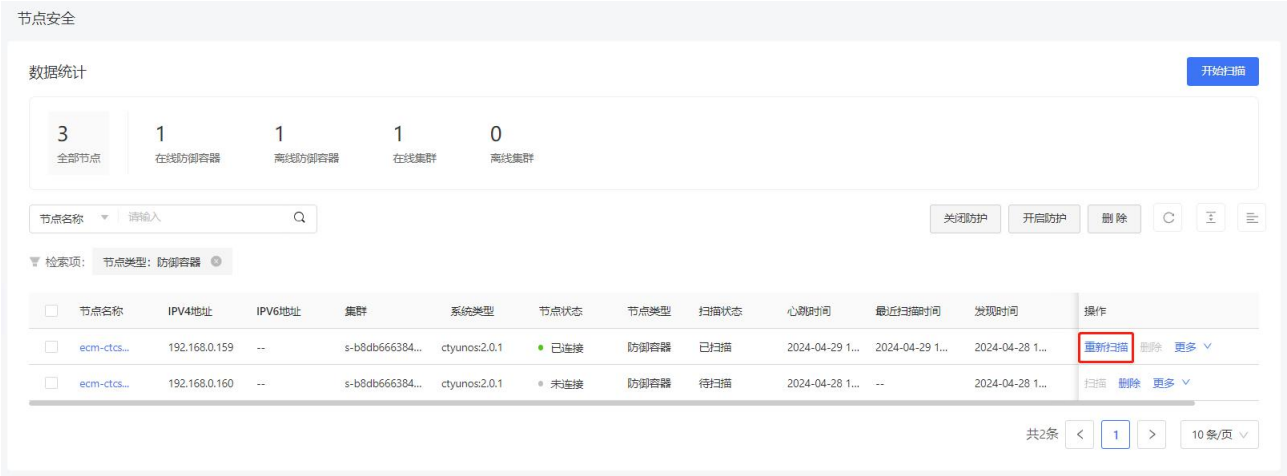
### 扫描节点

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“节点安全”，进入节点安全页面。
3. 单击节点列表右上方的“开始扫描”，可选择扫描全部节点或者仅扫描列表中勾选的节点。


4. 单击“确定”，立即开始扫描，扫描状态变为“扫描中”。


### 重新扫描

扫描完成后，可以单击操作列的“重新扫描”，重新对节点进行扫描。




## 4.4.2. 查看扫描结果

扫描完成后，在节点列表中可以查看扫描结果。

### 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“节点安全”，进入节点安全页面。
3. 节点状态列表上方，支持按照“节点名称”、“节点状态”、“防护状态”、“软件版本”、“软件名称”等进行筛选查询。系统默认筛选出节点类型为防御容器的节点。

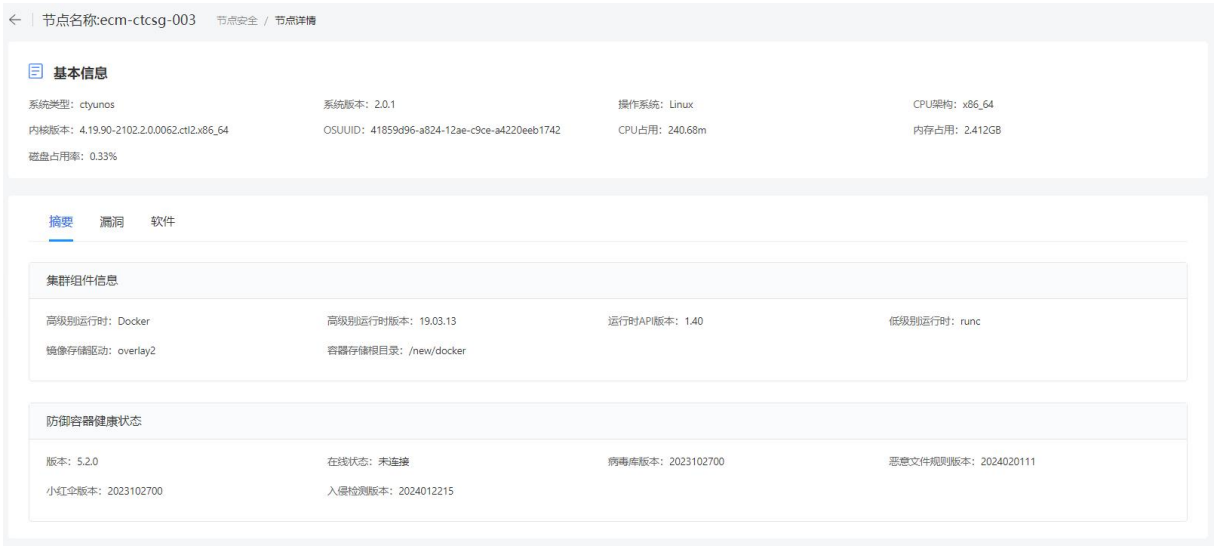
   节点列表参数说明如下：

| 参数 | 说明 |
| --- | --- |
| 节点名称 | 节点的名称。 |
| IPv4 地址 | 节点的 IPv4 地址。 |
| IPv6 地址 | 节点的 IPv6 地址。 |
| 集群 | 节点所属集群的名称。 |
| 系统类型 | 节点的操作系统类型。 |

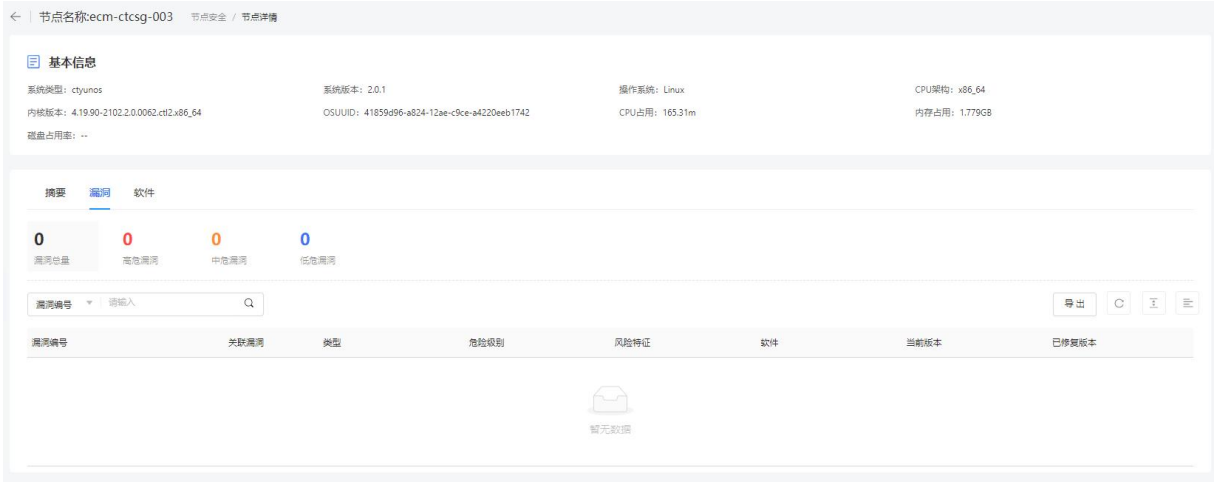
| 参数 | 说明 |
| --- | --- |
| 节点状态 | 指节点上防御容器的在线状态，分为已连接、未连接和已暂停三种状态。 |
| 节点类型 | 节点类型根据节点上运行的容器分为防御容器和扫描容器。 |
| 扫描状态 | 扫描状态分为待扫描、扫描中、已扫描、扫描失败这几种状态。 |
| 心跳时间 | 最近一次检查节点在线状态的时间。 |

## 4.4.3. 查看节点详情

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“节点安全”，进入节点安全页面
3. 单击节点列表中的“节点名称”，可以查看节点的详细信息。
4. 在节点信息页面可以查看节点信息、集群组件信息、防御容器健康状态，节点的 CPU 占用、内存占用、磁盘占用率资源使用情况等信息。




5. 查看软件漏洞：在软件漏洞页面，可以查看该节点扫描的漏洞统计信息，存在高危、中危和低危的漏洞数量，单击漏洞列表中的“漏洞编号”，可以查看漏洞的详细信息，包括漏洞介绍、漏洞评分、来源信息等。




6. 查看软件列表：软件列表页面展示当前节点中的软件包信息，包括软件名称、版本、文件路径、软件类型、漏洞数量等信息。单击软件前的“+”号，可查看该软件的漏洞详情，再单击漏洞编号前的“+”号，可查看该漏洞的介绍和参考网址等信息。


## 4.4.4. 其他操作

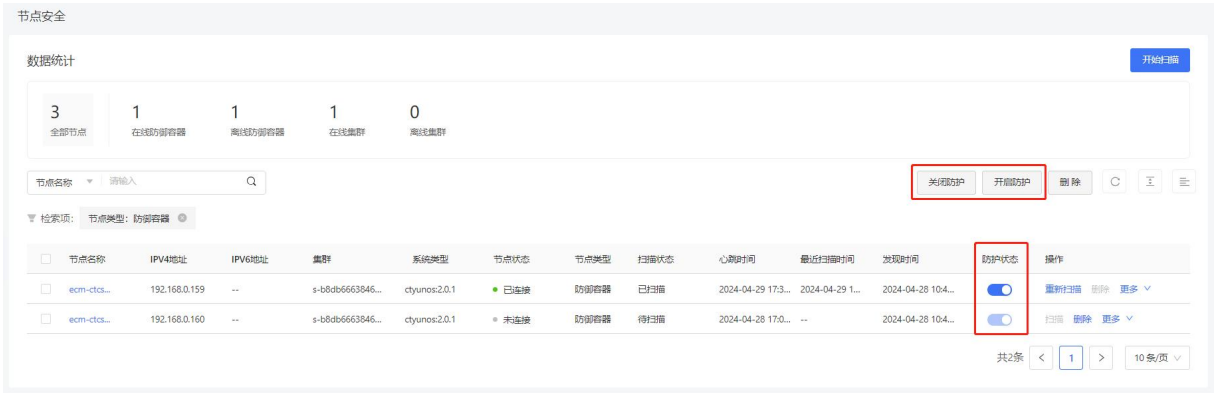
### 开启/关闭防护

注意：

关闭防护的节点不支持扫描操作。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“节点安全”。
3. 进入节点安全页面。
   - 关闭防护：单击节点列表上方的“关闭防护”，或者在列表中单击“防护状态”图标，可以关闭当前节点的防护容器。

- 开启防护：单击节点列表上方的“开启防护”，或者在列表中单击“防护状态”图标，可以恢复当前被关闭的节点防护容器。




## 删除节点

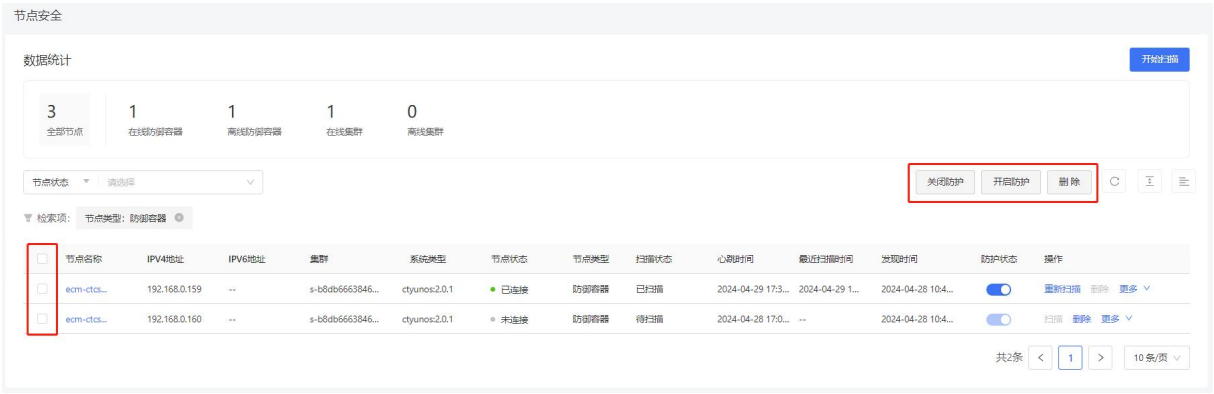
单击节点列表上方的“删除”，或者在列表中单击操作列的“删除”，可以删除节点的防护容器。

> 注意：
>
> 节点状态为“未连接”时，才可以删除。

## 批量操作

支持批量暂停、恢复或删除节点。

1. 先勾选节点列表中的“多选框”，支持多选。
2. 再对防护容器进行关闭防护、开启防护、删除操作。

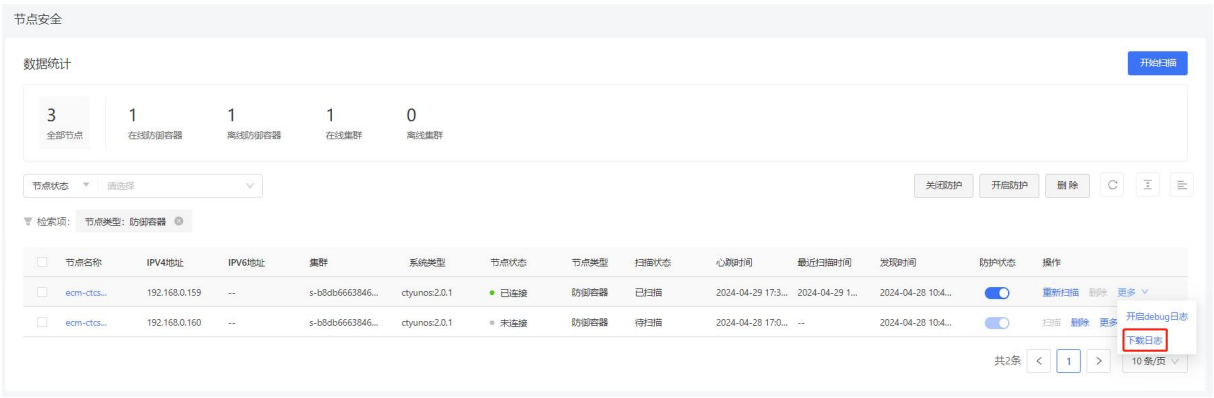


## 开启 debug 日志

单击节点列表操作列中的“开启 debug 日志”，可将防御容器日志开启 debug 模式。

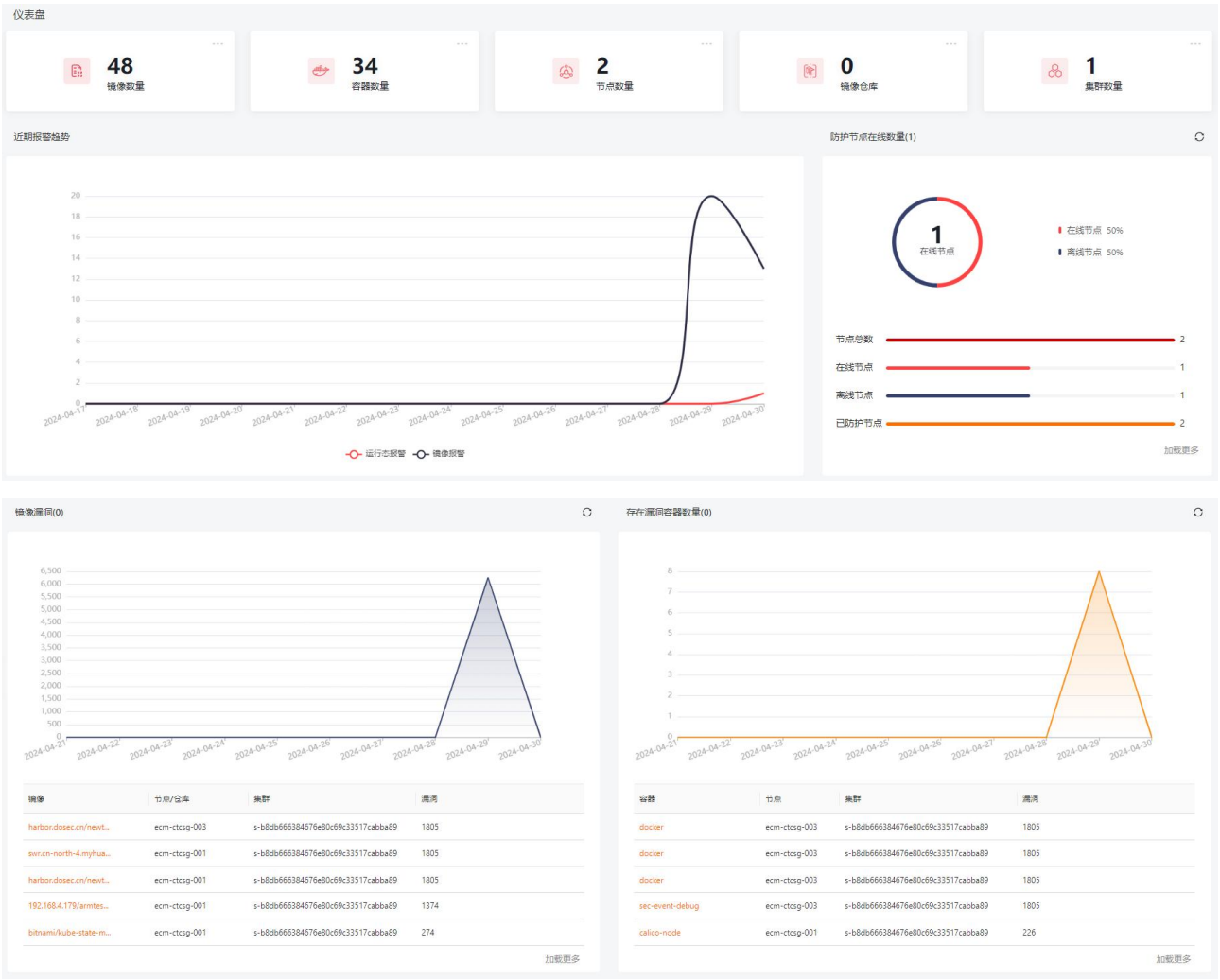

## 下载日志

单击节点列表操作列中的“下载日志”，可将防御容器日志以压缩包的形式下载到本地。




# 4.5. 仪表盘

购买容器安全卫士后，再次进入容器安全卫士控制台时，默认展示仪表盘页面。




## 数量统计

仪表盘页面上方展示了镜像、容器、节点、镜像仓库、集群这些重要资产的数量统计信息。

| 统计项 | 操作 |
| --- | --- |
| 镜像数量 | 单击镜像数量，可跳转至“镜像安全 > 镜像管理”页面，查看镜像详情。 |
| 容器数量 | 单击容器数量，可跳转至“容器安全 > 实时检测”页面，查看容器安全检测详情。 |
| 节点数量 | 单击节点数量，可跳转至“节点安全”页面，查看节点安全扫描详情。 |

| 统计项 | 操作 |
| --- | --- |
| 仓库数量 | 单击仓库数量，可跳转至“镜像安全 > 仓库配置”页面，管理配置镜像仓库。 |
| 集群数量 | 单击集群数量，可跳转至“安装配置 > 组件安装”页面，管理部署集群。 |

### 近期报警趋势

页面左侧显示近期报警趋势，统计了近 10 天内的运行态报警和镜像报警趋势，单击图例中的“镜像报警”，将隐藏“镜像报警”的曲线，只展示运行态告警变化趋势。

### 防护节点在线数量

页面右侧展示了防护节点的在线数量及在线率，并统计了节点总数、在线节点、离线节点以及已防护节点的数量。

### 镜像漏洞

仪表盘页面底部，展示了近 10 天内的镜像漏洞数量和存在漏洞的容器数量的变化趋势图，帮助您了解资产安全状态和存在的隐患。

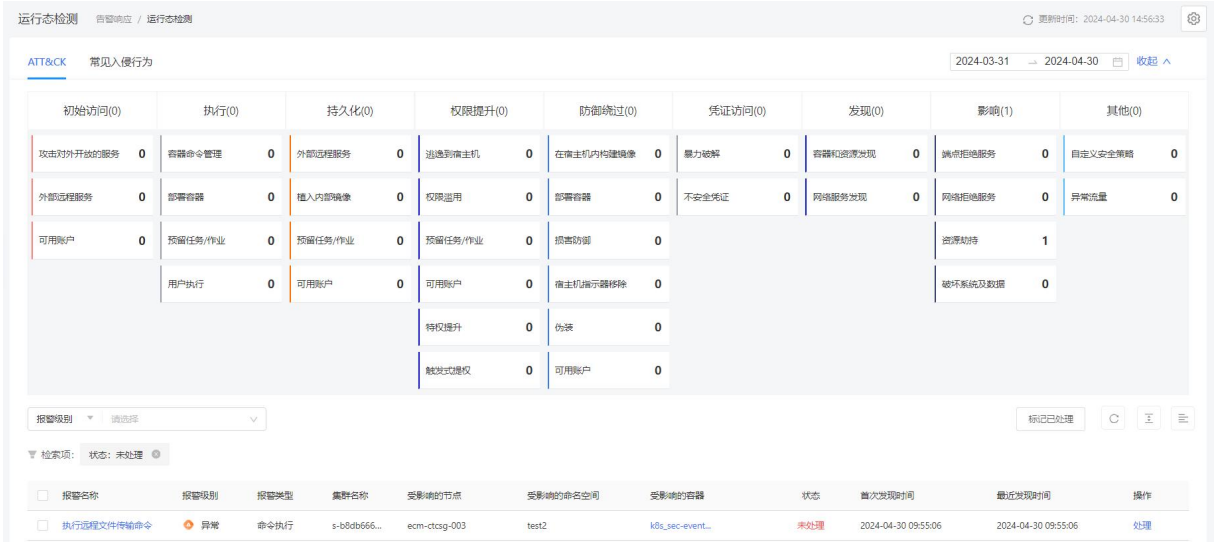
# 4. 6. 告警响应

## 4.6.1. 运行态检测告警

在运行态告警页面，用户可以查看已开启防护的容器的实时检测告警，并对告警进行处理。

### 查看运行态告警信息

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 运行态检测”，进入运行态检测页面。
3. “ATT&CK”告警视图采用 ATT&CK 的威胁分析框架，从攻击者初始访问到最后产生的影响进行全方位的分析。




4. “常见入侵行为”告警视图，支持反弹 shell、本地提权、暴力破解、恶意命令执行、病毒查杀、容器逃逸常见入侵行为视角。


5. 单击视图右上角的“收起”按钮或者向下滑动页面，可查看运行态告警列表。系统默认筛选出“未处理”的报警。

6. 运行态告警列表内，支持按照“报警级别”、“报警类型”、“报警名称”、“集群名称”、“受影响的节点”、“受影响的命名空间”、“受影响的容器”、“受影响的服务”、“状态”、“目的 IP”、“目的端口”、“源 IP”、“源端口”、“MD5”、“镜像名称”进行筛选查询，且“报警类型”、“报警名称”等筛选项支持模糊匹配。

   运行态告警信息参数说明：

| 参数 | 说明 |
| --- | --- |
| 报警名称 | 单击报警名称，进入告警详情页面，可以查看具体的报警原因。 |
| 报警级别 | 分为紧急、异常、提示这三种级别。 |

| 参数 | 说明 |
| --- | --- |
| 报警类型 | 分为命令执行、读写文件、网络活动、容器安全、集群异常、主机异常、文件内容这几种类型。 |
| 集群名称 | 发生报警的集群名称。 |
| 受影响的节点 | 受影响的节点名称。 |
| 受影响的命名空间 | 受影响的命名空间名称。 |
| 受影响的容器（服务） | 受影响的容器或服务的名称。 |
| 首次发现时间 | 首次发现报警事件的时间。 |
| 最近发现时间 | 最近一次发现报警事件的时间。 |
| 状态 | 状态分为已处理和未处理。 |

## 处理告警

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 运行态告警”，进入运行态告警页面。
3. 根据需要选择“ATT&CK”告警视图或“常见入侵行为”告警视图。
4. 单击告警列表操作列的“处理”，或单击报警名称进入告警详情页面后，单击“立即处理”按钮，进入处理告警页面，对本条告警进行处理。

   选择处理方式：

   - 若判断当前报警为误报，则可将其“加入白名单”或“标记为已处理”。
   - 非误报信息可以选择“隔离 Pod”、“重启 Pod”、“暂停容器”。

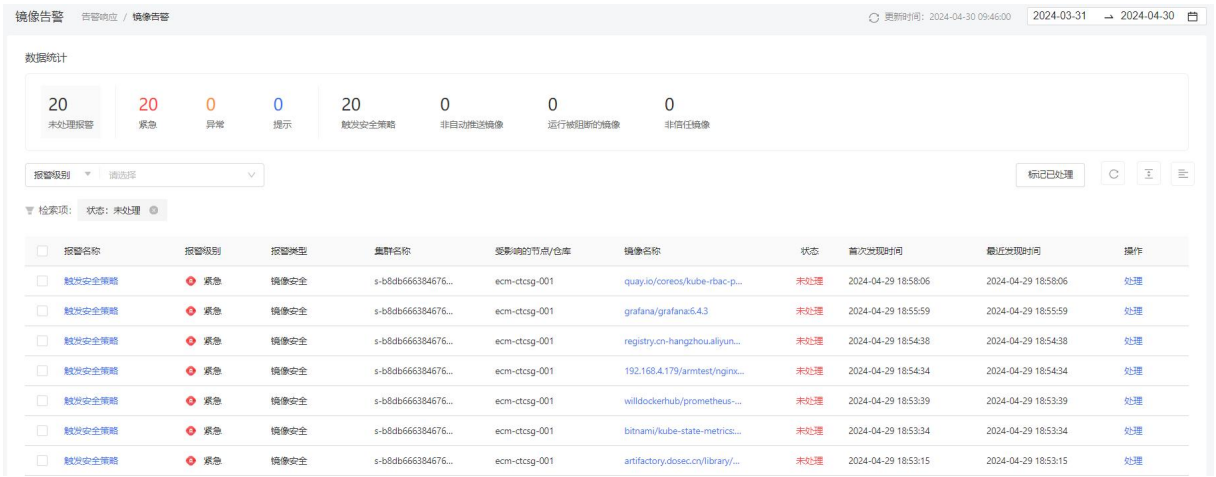

5. 选择处理方式后单击“保存”，即可完成告警处理。

## 4.6.2. 镜像告警

在镜像告警页面，用户可以查看已扫描镜像的告警信息，并对告警进行处理。

## 查看镜像告警信息

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 镜像告警”，进入镜像告警页面。




3. 查看镜像告警数据统计：镜像告警支持触发安全策略、非自动推动镜像、运行被阻断的镜像、非信任镜像四种检测类型的检测，显示不同类型报警的数量统计信息。
4. 单击数据统计中某一类型的镜像告警，下方报警列表将根据选择的类型进行筛选。
5. 镜像告警列表内，支持按照“报警级别”、“报警名称”、“镜像名称”、“策略名称”、“集群名称”、“受影响的节点”、“受影响的仓库”、“状态”进行筛选查询。

   镜像告警信息参数说明：

| 参数 | 说明 |
| --- | --- |
| 报警名称 | 报警的原因，包括触发安全策略、非自动推动镜像、运行被阻断的镜像和非信任镜像这四种。 |
| 报警级别 | 报警分为紧急、异常、提示这三种类型。 |
| 报警类型 | 镜像安全。 |
| 镜像名称 | 存在告警的镜像名称。 |
| 集群名称 | 存在报警的镜像所属集群的名称。 |

| 参数 | 说明 |
| --- | --- |
| 受影响的节点/仓库 | 受影响的节点名称或仓库名称（根据镜像所在位置区分）。 |
| 首次发现时间 | 首次发现报警事件的时间。 |
| 最近发现时间 | 最近一次发现报警事件的时间。 |
| 状态 | 状态分为已处理和未处理。 |

## 处理告警

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 镜像告警”，进入镜像告警页面。
3. 单击镜像告警列表操作列的“处理”，或单击报警名称进入告警详情页面后，单击“立即处理”按钮，进入处理告警页面，对本条告警进行处理。

   选择处理方式：

   - 若判断当前报警为误报，则可将其“加入白名单”或“标记为已处理”。
   - 非误报信息可以选择“镜像阻断”。


4. 选择处理方式后单击“保存”，即可完成告警处理。

## 4.6.3. 响应中心

响应中心展示“已隔离”、“已暂停”、“已重启”的容器，“已阻断”的镜像和已加入白名单的告警。

### 隔离 Pod 列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 响应中心”，进入响应中心页面。
3. 在隔离 Pod 列表，可以对已隔离的 Pod 进行恢复。


### 暂停容器列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 响应中心”，进入响应中心页面。
3. 在暂停容器列表，可以对已暂停的容器进行恢复。


### 重启 Pod 列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 响应中心”，进入响应中心页面。
3. 在重启 Pod 列表，可以查看重启过的 Pod。


## 镜像阻断列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 响应中心”，进入响应中心页面。
3. 在镜像阻断列表，可以对已阻断的镜像解除阻断。


## 白名单管理

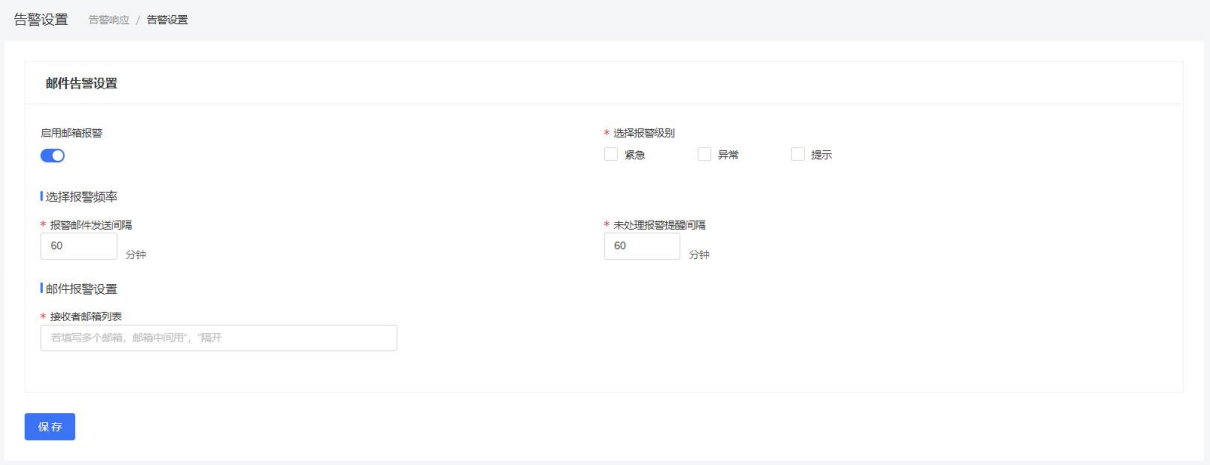
1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 响应中心”，进入响应中心页面。
3. 在白名单管理页面，可以查看已加入白名单的告警。支持对白名单进行管理，包括新增、查看、编辑、删除白名单。


# 4.6.4. 告警设置

系统默认未启用邮箱报警，您可以根据需要手动开启邮箱报警。开启邮箱报警通知功能后，您能接收到容器安全卫士发送的告警通知，及时了解容器、镜像的安全风险。否则，无论是否有风险，您都只能登录管理控制台自行查看，无法及时收到报警信息。

## 操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“告警响应 > 告警设置”，进入告警设置页面。




3. 将“启用邮箱报警”开关置为  ，开启邮箱报警功能。
4. 配置告警参数。

| 参数 | 说明 |
| --- | --- |
| 选择报警级别 | 勾选邮件通知的告警等级。 |
| 报警邮件发送间隔 | 配置邮件发送的时间间隔，例如配置为 60 分钟，表示每个小时发送一次告警邮件。 |
| 未处理报警提醒间隔 | 支持对未处理的报警单独进行邮件提醒，例如配置为 60 分钟，表示每个小时将筛选出的“未处理”报警发送一次告警邮件。 |
| 接收者邮箱列表 | 配置接收告警通知的邮箱地址。多个邮箱使用“,”隔开。 |

5. 配置完成后，单击“保存”。

# 4.7. 日志审计

日志审计会记录事件的操作时间、用户名、来源 IP、操作类型、所属模块、是否执行成功、操作行为等信息。

## 查看日志审计列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“日志审计”，进入日志审计页面。


3. 查看日志审计列表：日志列表上方支持按照“用户名”、“操作行为”、“来源 IP”、“操作类型”、“所属模块”、“是否执行成功”和操作时间段进行筛选查看。

   日志审计参数说明：

| 参数 | 说明 |
| --- | --- |
| 操作时间 | 记录的操作行为发生的时间。 |
| 用户名 | 操作用户的用户名。 |
| 来源 IP | 操作用户的 IP 地址。 |
| 操作类型 | 操作类型分为更新、查看、删除、登录/退出、未知这些类型。 |

| 参数 | 说明 |
| --- | --- |
| 所属模块 | 操作行为对应的功能模块，包括仪表盘、告警响应、镜像安全、容器安全、节点安全、平台管理、安装配置等模块。 |
| 是否执行成功 | 分为“执行成功”和“执行失败”两种类型。 |
| 操作行为 | 具体的操作行为信息。 |

## 日志设置

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“日志审计”，进入日志审计页面。
3. 单击页面右上角的“设置”图标，进入日志设置页面。


4. 可选择是否开启用户“查看类型的操作记录审计”，设置“操作审计保留时间”。
5. 单击“保存”，完成配置。

# 5. 常见问题

## 5.1. 计费购买类

### Q：同一个账号可以购买多个容器安全卫士实例吗？

同一个账号在同一个区域只能购买一个实例，对应一个主套餐版本。购买容器安全卫士实例后，您可以升级版本或扩容防护节点数。

### Q：实例到期后，还能防护节点吗？

购买的实例到期后如未按时续费，公有云平台会提供一定的保留期。

- 保留期内，平台会冻结服务，用户配置的各类防护策略将不再生效。
- 保留期满，用户若仍未续费，平台会清除实例资源，资源被释放，释放后无法恢复。

### Q：容器安全卫士实例可以降低版本和规格吗？

容器安全卫士实例不支持降级，同时已绑定的防护节点也不支持单独退订。

如您需要降低当前规格，您可以先退订当前实例，再重新购买较低版本的实例。

### Q：容器安全卫士是否支持自动续订？

支持。

您可以在购买套餐时勾选自动续订，也支持在使用过程中，在订单中心中设置自动续订。

### Q：容器安全卫士是如何计算并限制防护节点个数的？

根据购买防护节点数据量进行限制，若在线防护节点数超过购买防护节点数量时，将不允许开启防护。

### Q：若当前版本包含的防护节点个数不够用时，如何处理？

若当前版本包含的防护节点个数不够用时，您可以扩容购买节点。

### Q：续费时是否可同时变更容器安全卫士版本或规格？

续费时不能同时变更的规格。您只能为当前的容器安全卫士实例版本规格进行续费，增加使用时长。

您可以在续费完成后，对容器安全卫士实例版本进行升级。

### Q：防护节点购买上限是什么？

每个资源池最多支持购买 10000 个防护节点。

### Q：容器安全卫士是否支持按需计费？

当前容器安全卫士不支持按需计费。

### Q：在使用期间购买了防护节点，资源到期时间是何时？

扩容节点与主套餐绑定，资源到期时间与主套餐一致。

### Q：购买的扩容节点，支持单独退订吗？

不支持。扩容节点购买后与主套餐绑定，不支持单独退订。

### Q：退订重购后，原实例的配置数据可以保留吗？

用户退订后在 15 天内重新购买实例时，仅当新实例版本等于或高于旧实例时，可恢复原有配置。

当重新购买时距离退订已超过 15 天，原资源已释放且配置数据已删除，则无法恢复。

## 5.2. 防护配置类

### Q：标准版支持设置单条防护规则的防护状态吗？

支持。 标准版提供具体防护规则的防护开关。您可以根据业务需要选择开启或关闭规则的防护。

### Q：标准版支持对同一节点下发不同防护策略吗？

不支持。默认使用“默认策略”进行防护，创建策略时已生成防护策略的节点是不可重复选择的。若想重新配置策略，需要先解绑已有策略，然后再重新绑定。

### Q：标准版支持入侵检测规则自定义吗？

支持。可以在“容器安全 > 策略管理”中进行自定义，包括命令执行、网络活动、读写文件、文件内容。

### Q：标准版镜像安全扫描支不支持仓库镜像扫描？

支持。除了支持天翼云仓库以外，还支持 Harbor、JFrog、Huawei、Huawei CCE Agile、AWS、Aliyun、Registry、Microsoft。

## 5. 3. 管理类

### Q：容器安全卫士有哪些注意事项？

- 安全探针仅支持三种容器运行时，包括：docker、containerd、crio。
- 安全探针在运行时会挂载 k8s node 宿主机的 /data（非 crio）和 /root（crio）目录，请确保目录的权限正常。
- 安全探针需要跟中心通信，请确保您的 k8s 集群允许出网策略 TCP 端口：31080、30432、32345。

### Q：接入容器安全卫士对现有业务和服务器运行有影响吗？

接入容器安全卫士不需要中断现有业务，不会影响服务器的运行状态，即不需要对其进行任何操作（例如关机或重启）。

防护探针本身需要占用宿主机一定资源，可能会对宿主机产生一定影响。不过请放心，容器安全卫士对防护探针做了资源监控和降级处置，来保障业务稳定、安全。