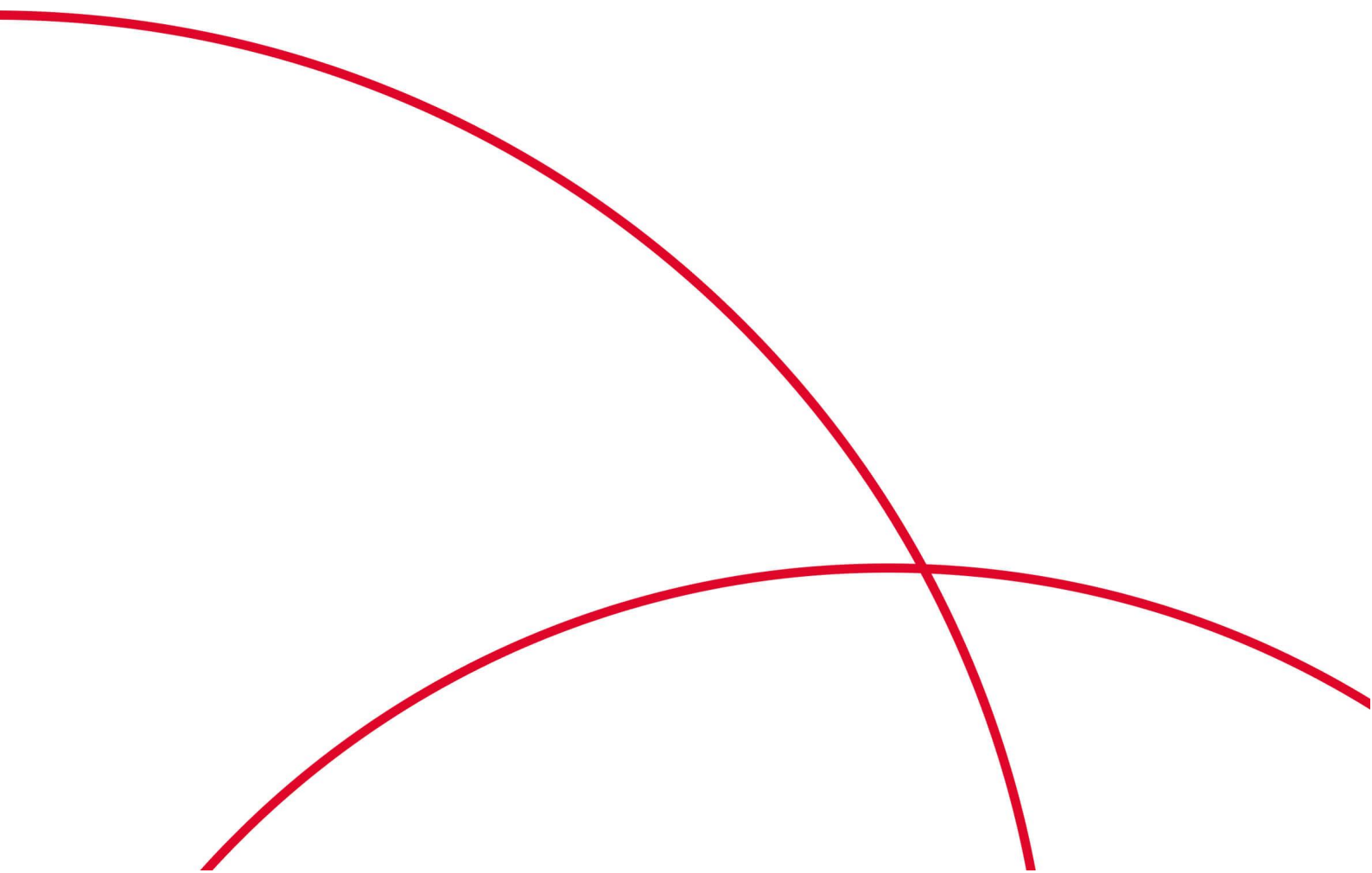




容器安全卫士

用户使用指南

天翼云科技有限公司



1. 产品介绍	1
1.1. 产品定义	1
1.2. 基本概念	2
1.3. 功能特性	4
1.3.1. 仪表盘	4
1.3.2. 网络可视化	4
1.3.3. 资产中心	5
1.3.4. 告警响应	6
1.3.5. 安全合规	6
1.3.6. IaC 安全	8
1.3.7. 镜像安全	8
1.3.8. 容器安全	9
1.3.9. 节点安全	10
1.3.10. 集群安全	10
1.4. 产品优势	11
1.5. 应用场景	12
1.6. 产品规格	13
1.7. 支持的区域	17
2. 计费说明	18
2.1. 计费模式	18
2.2. 续订	19
2.3. 扩容	20
2.4. 退订	20
3. 快速入门	22
3.1. 入门指引	22
3.2. 购买云容器安全卫士	23
3.3. 安装 Sever/Agent	25
3.4. 扫描容器镜像	26

3.5. 开启容器防护	28
4. 用户指南	31
4.1. 仪表盘	31
4.2. 网络雷达	32
4.2.1. 查看网络雷达图	32
4.2.2. 图例说明	33
4.2.3. 按访问类型查看	34
4.2.4. 查看命名空间之间的流量	35
4.2.5. 查看历史访问流量	35
4.2.6. 查看命名空间	36
4.2.7. 查看工作负载	37
4.2.8. 切换表格视图	45
4.3. 资产中心	46
4.3.1. 更新资产	47
4.3.2. 查看资产	48
4.4. 告警响应	101
4.4.1. 运行态检测告警	101
4.4.2. 镜像告警	105
4.4.3. IaC 告警	107
4.4.4. 响应中心	111
4.4.5. 告警设置	113
4.5. 安全合规	114
4.5.1. 查看基线检查列表	114
4.5.2. 选择并开启基线	116
4.5.3. 启动基线检查项	117
4.5.4. 扫描基线	117
4.5.5. 查看检查结果	119
4.6. IaC 安全	121
4.6.1. 上传文件	121
4.6.2. 扫描文件	122
4.6.3. 查看文件列表	123

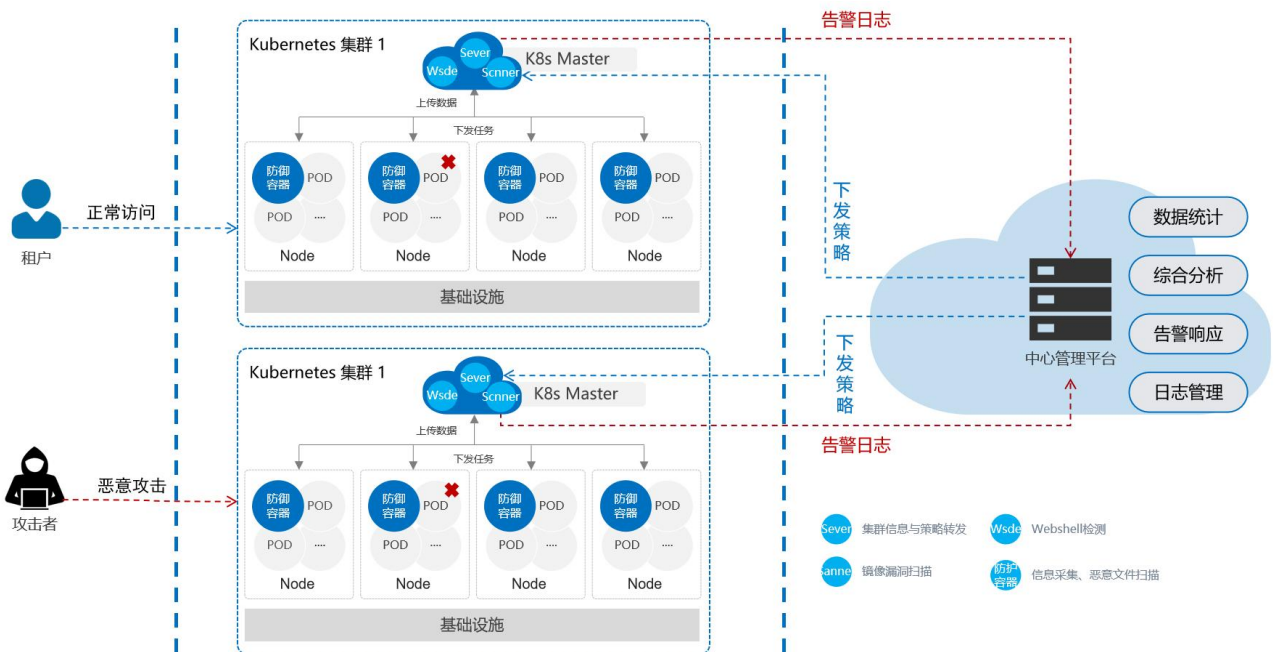
4.6.4. 查看文件详情	128
4.6.5. 下载扫描报告	129
4.6.6. 管理文件规则	130
4.6.7. 设置	134
4.7. 集群安全	135
4.7.1. 组件漏洞	135
4.7.2. 安全检查	138
4.7.3. 集群审计	140
4.7.4. 集群策略	144
4.7.5. 集群设置	145
4.8. 镜像安全	146
4.8.1. 配置镜像仓库	146
4.8.2. 更新镜像列表	147
4.8.3. 扫描镜像	149
4.8.4. 查看扫描状态	152
4.8.5. 查看扫描结果	153
4.8.6. 处置镜像	163
4.8.7. 管理白名单	165
4.8.8. 镜像策略管理	167
4.8.9. 镜像设置	169
4.9. 容器安全	172
4.9.1. 更新容器列表	172
4.9.2. 查看容器列表	173
4.9.3. 查看容器详情	175
4.9.4. 处置风险容器	178
4.9.5. 容器审计	180
4.9.6. 容器策略管理	184
4.9.7. 文件防篡改	193
4.9.8. 进程控制	195
4.9.9. 弱密码	196
4.9.10. 容器设置	198

4. 10. 网络安全	199
4. 10. 1. 选择策略类型	199
4. 10. 2. 添加策略	200
4. 10. 3. 发布策略	204
4. 10. 4. 查看网络雷达图	205
4. 11. 节点安全	206
4. 11. 1. 扫描节点	206
4. 11. 2. 查看扫描结果	208
4. 11. 3. 查看节点详情	209
4. 11. 4. 其他操作	210
4. 12. 平台管理	212
4. 12. 1. 日志审计	212
4.12.2. 外部集成	213
4. 13. 安装配置	215
4. 13. 1. 租户集群为天翼云原生集群	215
4. 13. 2. 租户集群为自建集群	216
4. 13. 3. 集群组件配置	218
4. 13. 4. 查看运行状态	220
4. 14. 任务中心	221
4. 15. 消息中心	222
5. 常见问题	224
5. 1. 计费购买类	224
5. 2. 防护配置类	226
5. 3. 管理类	226

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。

1.2. 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 的整个生命周期资源，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。

1.3. 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:

1.3.1. 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。

1.3.2. 网络可视化

对容器环境中网络流量进行绘图,打破网络黑洞,支持对进程、容器、pod、服务、主机级别的网络监测。通过对单个业务之间,业务组之间,以及租户之间的网络访问策略配置,实现业务之间隔离,来减小被入侵之后的影响范围;通过网络拓扑图,从网络层面判断入侵影响范围。

容器安全卫士自动检测发现 Kubernetes 集群内的运行容器，应用以及镜像，关联相应的安全风险进行汇总，展示安全风险的数量以及风险级别的分布。支持自动发现容器内进程之间、容器之间、POD 之间、服务之间、节点之间的网络连接状态，展示连接的原地址，目的地址以及端口。并对异常连接进行预警。支持对 Kubernetes 集群内 POD 之间的通信进行网络隔离控制、隔离策略支持配置 POD 的访问规则、阻断来自其他命名空间的所有流量、允许来自外部客户端的流量等。

- 支持租户隔离

支持对 Kubernetes 集群内租户进行隔离控制，租户之间默认禁止直接通信，可以通过配置 RBAC、POD 策略、网络策略等实现租户间的访问策略。

- 支持自定义网络策略

支持对 Kubernetes 集群内的隔离策略管理，展示各个 POD 已经配置的隔离策略并能进行配置和应用。

- 可视化的展示视角

通过雷达可视图的展示方式，用户可以查看到容器内进程之间、容器之间、POD 之间、服务之间、节点之间的网络进出站信息，对指定的网桥、网卡进行流量的 DPI 分析，有助于识别、阻断流向异常的流量。

- 多种类型策略支持

基于用户不同的使用环境与业务需求，支持多种策略类型，包括：

- IPtables 模式（可针对不同的资源之间设置网络访问策略）。
- OVS 模式（在 OpenShift 环境下，针对不同的资源之间设置网络访问策略）。
- NetworkPolicy 模式（为指定资源设置允许进出站访问）。

1.3.3. 资产中心

对镜像、仓库、容器、主机、微服务、kubernetes 配置信息等容器相关信息进行自动采集，统一可视化管理，对容器风险一目了然，时刻掌握容器资产变化，使安全不落后于业务。消除安全与运维之间的信息壁垒，使业务环境内各项资产对安全用户清晰可见。

细粒度、结构化的资产清点助力安全用户及时发现容器、集群环境中可能存在的风险隐患，提前进行预防、修复，并在入侵事件发生时帮助安全用户及时定位受损资产信息，快速进行响应处理以免恶意事件扩散使更多资产受到感染。

资产管理类型包括容器、镜像、仓库、主机、POD 等，为用户提供容器内资产的分类视图，支持对每一类资产进行数据分级聚合展示，实现容器资产的全面可视化，帮助用户更直观地了解当前系统内的资产情况。

- 资产管理

系统资产数据持续更新，每日及时、自动上报资产数据。基于历史清点的数据，每次只清点新启动的进程信息，极大降低对服务性能的消费。

- 资产可视化

系统支持清点的资产种类包括容器、镜像、Registry、POD 等，为用户提供容器内资产的分类视图，支持对每一类资产进行数据分级聚合展示，实现容器资产的全面可视化。

- 资产更新

用户可根据使用场景设置资产的更新周期，包括资产的范围。

1.3.4. 告警响应

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。

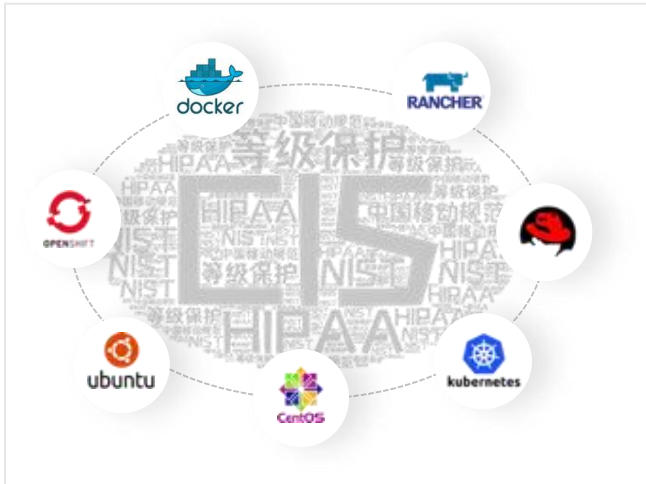
- 一键封堵

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。

1.3.5. 安全合规

在业务系统上线运行之前，应对业务系统所在容器、集群以及容器原镜像进行合规检测，以防止不安全的配置导致容器逃逸或者集群入侵事件。

提供了对容器及集群进行合规审计，支持主流的 CIS 安全检测标准。基于产品提供可视化的基线检测结果和修复建议，用户可以自行修复不合规的检测项。根据用户的生产场景支持自定义合规检测项。



- 支持多种系统合规 CIS 检测

支持 Docker CIS、Kubernetes CIS 合规、Centos CIS、Ubuntu CIS、OpenShift 合规等多种系统合规项检测，并支持快速扩展，满足不同场景的需求。

- 支持多种自定义检测项

用户可根据各行业安全标准，自定义配置安全合规检测项。灵活适应组织或行业的安全合规需求，提供高度个性化的定制选择。

- 支持一键导出合规检测结果

系统基线检测扫描后，用户快速一键生成基线的合规检测报告。

- 深入可视化的结果展示

合规基线检测结果可视化列表呈现，用户可以清晰看到每一个检查项的说明、通过情况以及检测详情信息。帮助用户快速了解基线检测未通过的原因，及时对容器相关配置进行修改更新。

- 多视角合规审计

合规基线支持多视角查看包括资产视角、合规视角，用户可在镜像、容器、节点、资产内查看当前资产的基线检测项，也可以在合规视角内查当前合规项内存在哪些不合规的资产。

- 持续安全检查

系统提供持续安全检查功能，通过自动扫描、监控机制。系统实时检测云原生环境的合规性，确保符合 CIS 基准和最佳实践。

1.3.6. IaC 安全

在 kubernetes 系统中，各类资源均需要通过编排文件构建，编排文件编写是否规范，将直接影响到构建资源的安全性、规范性与可用性。对于部署资源所编写的编排文件，系统支持自动接入，自动扫描，根据扫描结果指出编排文件中存在风险或不规范的配置项，并给出修复建议，保障资源合规且安全地创建。

- 编排文件审计

支持对编排文件内的扫描结果进行分类展示，并对不合规的检查支持所在行数显示。

- 自定义规则

内置 K8S manifests 文件与 Dockerfile 文件的自定义设计规则，并支持用户根据使用场景进行开启或关闭检测项。

1.3.7. 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。

1.3.8. 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。

- 容器文件防篡改

通过对容器内重要路径（多路径之间若存在包含关系，将自动去重后保存，默认防护路径及其下所有子路径）下的重要文件进行备份，并识别所有异常篡改文件的行为，及时发送报警并恢复文件。

- 弱口令检测

支持对包括但不限于 mysql8、ssh、redis、tomcat、容器 env 等应用弱口令检测。

- 进程访问控制

通过进程访问控制策略对一个或多个容器进行进程监控，并通过配置进程名称、Url 等信息来识别异常进程，及时告警或阻断。

- 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。

1.3.9. 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。

1.3.10. 集群安全

针对不同的项目情况、支持对 Kubernetes、OpenShift、Rancher 等集群的不同版本进行安全风险扫描。如：

Kubernetes 版本信息披露、匿名身份验证、可能遭受 Ping Flood 攻击等。对于部署资源所编写的编排文件，支持一键同步并扫描编写内容是否存在风险以及是否符合编写规范。并支持对集群内的组件进行检查和对集群的审计通过多方位的检测方式保证集群的安全。

- 组件漏洞

支持对集群内的组件进行检查，并给出该组件内的漏洞信息包括漏洞介绍、参考地址、受影响版本等信息。

- Kubernetes 安全检查

支持对 Kubernetes 环境进行安全性扫描，检查是否存在诸如信息泄露、特权升级、远程代码执行、危险访问等安全风险，列出各种风险所影响的资产范围，并输出解决方法。

- 插件管理

支持针对 0day 或特殊漏洞生成专业的安全插件，运行后能快速发现受影响资产，确定影响面。

- 集群审计

记录了对 APIServer 的访问事件，通过查看、分析日志，可以了解集群的运行状况、排查异常，发现集群潜在的安全、性能等风险。

- 集群策略

可配置集群审计类型包括 get 类型审计、watch 类型审计、list 类型审计、update 类型审计、create 类型审计、patch 类型审计、delete 类型审计。

默认内置针对日常运营模式、重保模式、高级防护模式的告警策略；同时也支持自定义告警策略。

支持告警规则自定义。

- 集群设置

支持对新增集群自动扫描、周期扫描的设置。

1.4. 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，客户端不暴露任何端口，保护您的同时也注重自身安全。

1.5. 应用场景

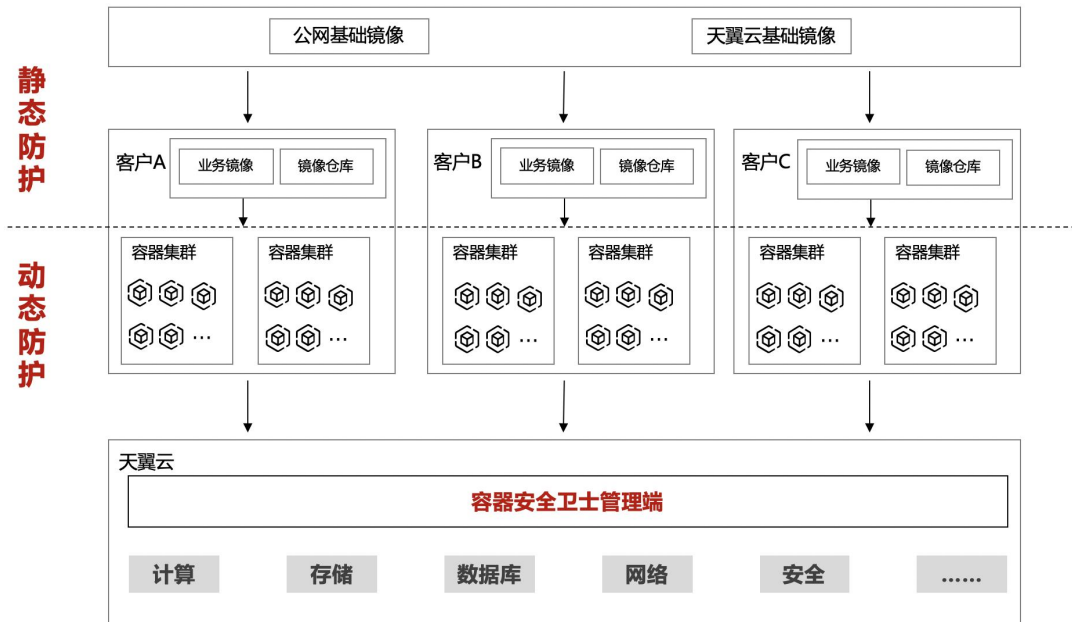
场景一：镜像安全防护

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



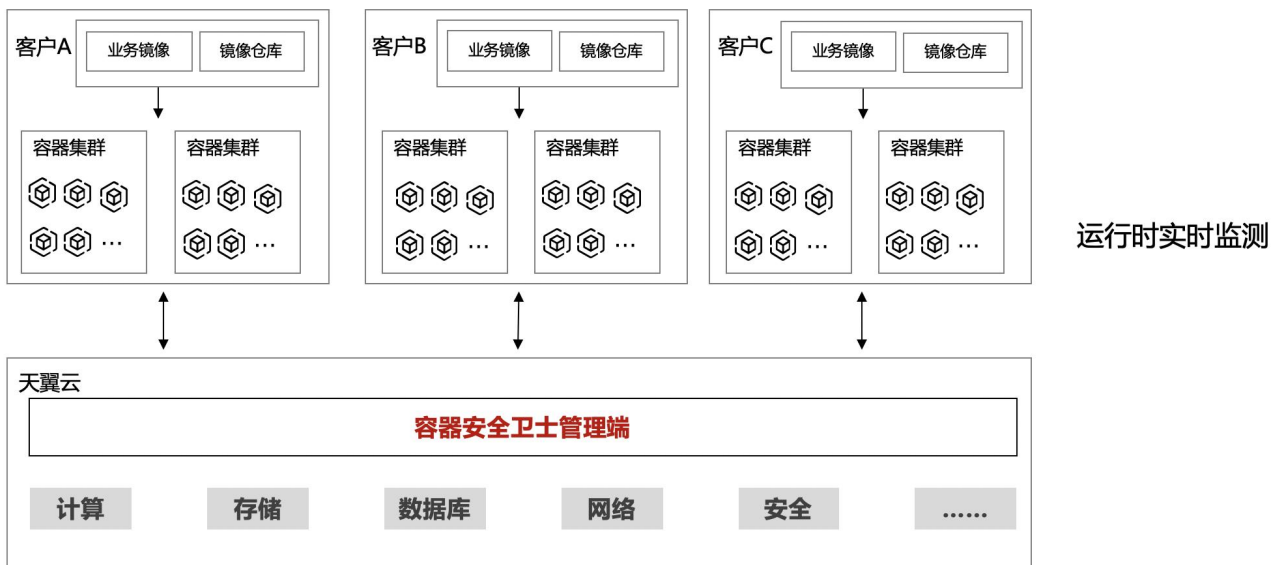
场景二：容器安全防护

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



1.6. 产品规格

一级功能	二级功能	功能描述	标准版	高级版
仪表盘	-	从全局视角统计重要资产、防护情况、告警趋势、及安全情况，便于用户更好的进行安全响应处置，提升运营	✓	✓

一级功能	二级功能	功能描述	标准版	高级版
		效率。		
资产中心	-	查看集群资产、镜像资产、主机节点资产、应用服务资产、K8S 配置详细信息。	✓	✓
告警响应	运行态检测	查看所有容器、主机、K8S 入侵告警事件，并对其进行响应处置。	✓	✓
	镜像告警	查看所有触发安全策略的镜像告警事件，并对其进行响应处置。	✓	✓
	IaC 告警	查看存在未通过高危检查的文件。	×	✓
	响应中心	查看告警处置记录，包括隔离 Pod 列表、暂停容器列表、重启 Pod 列表、镜像阻断列表，并进行白名单管理、一键封堵。	✓	✓
安全合规	基线管理	对各版本的 Linux 系统按照等保、CIS 的基线要求检测，覆盖主流操作系统的检测。 对各版本的 kubernetes 按照 CIS 基线要求检测。 对各个版本容器运行环境按照 CIS 基线要求检测。	✓	✓
	基线配置	自定义配置基线扫描周期、安全合规达标率等。	✓	✓
镜像安全	镜像管理	对业务环境主机中和镜像仓库中的镜像资产统一管理、安全扫描，并提供可写入 dockerfile 的修复建议。	✓	✓
	镜像策略	通过漏洞规则、文件规则、软件包规则、及其他规则设置来对风险制品镜像进行告警或阻断管控。	✓	✓

一级功能	二级功能	功能描述	标准版	高级版
	镜像设置	配置节点镜像和仓库镜像扫描周期。	✓	✓
容器安全	实时检测	从命名空间或节点的视角实时检测容器安全状态，对容器进行基线检查、容器审计等。	✓	✓
	容器策略	创建并管理容器入侵检测策略及入侵检测规则。	✓	✓
	文件防篡改	创建并管理容器防篡改策略。	×	✓
	进程访问控制	创建并管理容器进程访问策略，支持进程阻断/放行。	×	✓
	弱口令	弱口令字典管理及弱口令检测。	×	✓
	容器设置	设置容器保留时长、容器审计信息保留时长，及容器扫描周期。	✓	✓
节点安全	节点安全	查看节点信息、集群组件信息、防御容器健康状态，对节点实时入侵监测，扫描节点漏洞，开启节点 debug 日志。	✓	✓
	节点设置	自定扫描新增节点，设置节点更新周期。	✓	✓
IaC 安全	IaC 检查	对于部署资源所编写的编排文件，支持扫描编写内容是否存在风险以及是否符合编写规范。	×	✓
	规则管理	统一管理 K8S manifests/helmchart 文件规则、Dockerfile 文件规则、ConfigMap 文件规则等。	×	✓
	IaC 设置	配置自动扫描、周期扫描策略。	×	✓

一级功能	二级功能	功能描述	标准版	高级版
集群安全	组件漏洞	扫描 Kubernetes 内的 kubelet、calico、etcd 等组件漏洞信息。	×	✓
	安全检查	对集群进行安全检查，发现未通过检查项及影响范围，提供解决方案及参考链接。	×	✓
	插件管理	可通过提供插件的形式，帮助用户验证 1day 漏洞信息。	×	✓
	集群审计	记录了对 APIServer 的访问事件，通过查看、分析日志，可以了解集群的运行状况、排查异常，发现集群潜在的安全、性能等风险对异常事件支持报警。	×	✓
	集群策略	配置集群审计策略，管理集群审计规则，管理集群告警规则。	×	✓
	集群设置	配置自动扫描新增集群及集群扫描周期。	×	✓
网络安全	网络策略	通过对单个业务之间，业务组之间，以及租户之间的网络访问策略配置，实现业务之间隔离，来减小被入侵之后的影响范围。	×	✓
网络雷达	-	对容器环境中网络流量进行绘图，打破网络黑洞，支持对命名空间、Pod、主机、集群、外网级别的网络监测。通过对单个业务之间、业务组之间以及多租户之间的网络访问策略配置，通过对业务之间的隔离，来减小被入侵之后的影响范围。通过网络拓扑图从网络层判断入侵的影响范围。	×	✓
平台管理	日志审计	对系统操作日志进行统计及报表输出。	✓	✓

一级功能	二级功能	功能描述	标准版	高级版
安装配置	-	支持天翼云原生集群或非原生集群部署方式。	✓	✓
订单中心	-	查看用户订单情况，可以进行退订、扩容、续订等操作。	✓	✓
任务中心	-	查看任务执行情况，可以进行终止、删除、查看详情等操作。	✓	✓
消息中心	-	查收系统内部消息。	✓	✓

1.7. 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	-
华南地区	华南 2	-
西南地区	西南 1	-
北方地区	华北 2	-

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）	高级版（单节点）
主套餐	290 元/月	500 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。

授权信息

是否有效	● 有效	立即退订
过期时间	2024-11-12 11:27:01	立即续订
节点数量	已使用1个/剩余0个	立即扩容

3. 单击“立即续订”，进入续订容器安全卫士页面。

套餐产品配套

产品名称	资源ID	版本	数量
容器安全卫士	f4b6871305ac4ae69300dcee981a387e	标准版	1

购买时长:

* 协议 我已阅读理解并同意《天翼云容器安全卫士服务协议》

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. 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。

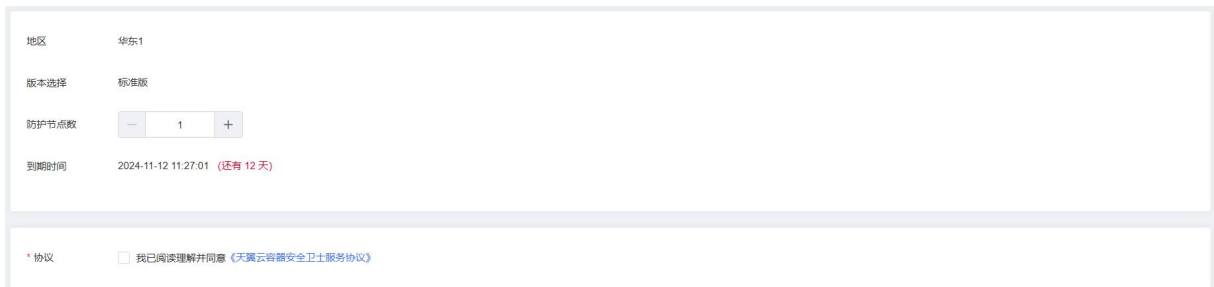
扩容步骤

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。

授权信息

是否有效	● 有效	立即退订
过期时间	2024-11-12 11:27:01	立即续订
节点数量	已使用1个/剩余0个	立即扩容

3. 单击“立即扩容”，进入扩容页面。



扩容配置界面截图，显示以下信息：

- 地区：华东1
- 版本选择：标准版
- 防护节点数：1 (可调整)
- 到期时间：2024-11-12 11:27:01 (还有 12 天)
- 协议：我已阅读理解并同意《天翼云容器安全卫士服务协议》

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。

2.4. 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

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

授权信息

是否有效	● 有效	立即退订
过期时间	2024-11-12 11:27:01	立即续订
节点数量	已使用1个/剩余0个	立即扩容

- 单击“立即退订”，进入退订申请页面。

退订管理/退订申请 资源被锁定

退订须知：

- 退订成功后资源不可恢复；
- 确定退订前建议完成数据备份或者数据迁移；
- 除特殊约定（云电脑、云间高速尊享版两款产品，退订后资源立即释放）以外，退订后的资源将被以冻结形式保留15天后释放；
- 退订可能会导致其他存在的关联业务产生影响。

退订规则请查看：[退订规则说明](#)
您还可以进行 0 次/七天无理由退款

产品名称	资源ID	资源池	资源状态	时间	产品金额	可退订金额
> 容器安全卫士	f4b6871305ac4ae69300dcee981a387e	4.0实验局	资源已启用	创建: 2024-04-28 17:00:37 到期: 2024-05-28 17:00:34	元	元

*** 请选择退订原因：**

产品金额：¥ 元
退订金额：¥ 元

购买云服务时选错参数（配置、时长、台数等）

云服务功能不完善，不满足业务需求

其他云服务商的性价比更高

区域选择错误

云服务故障无法修复

其他

我已确认本次退订金额和相关费用

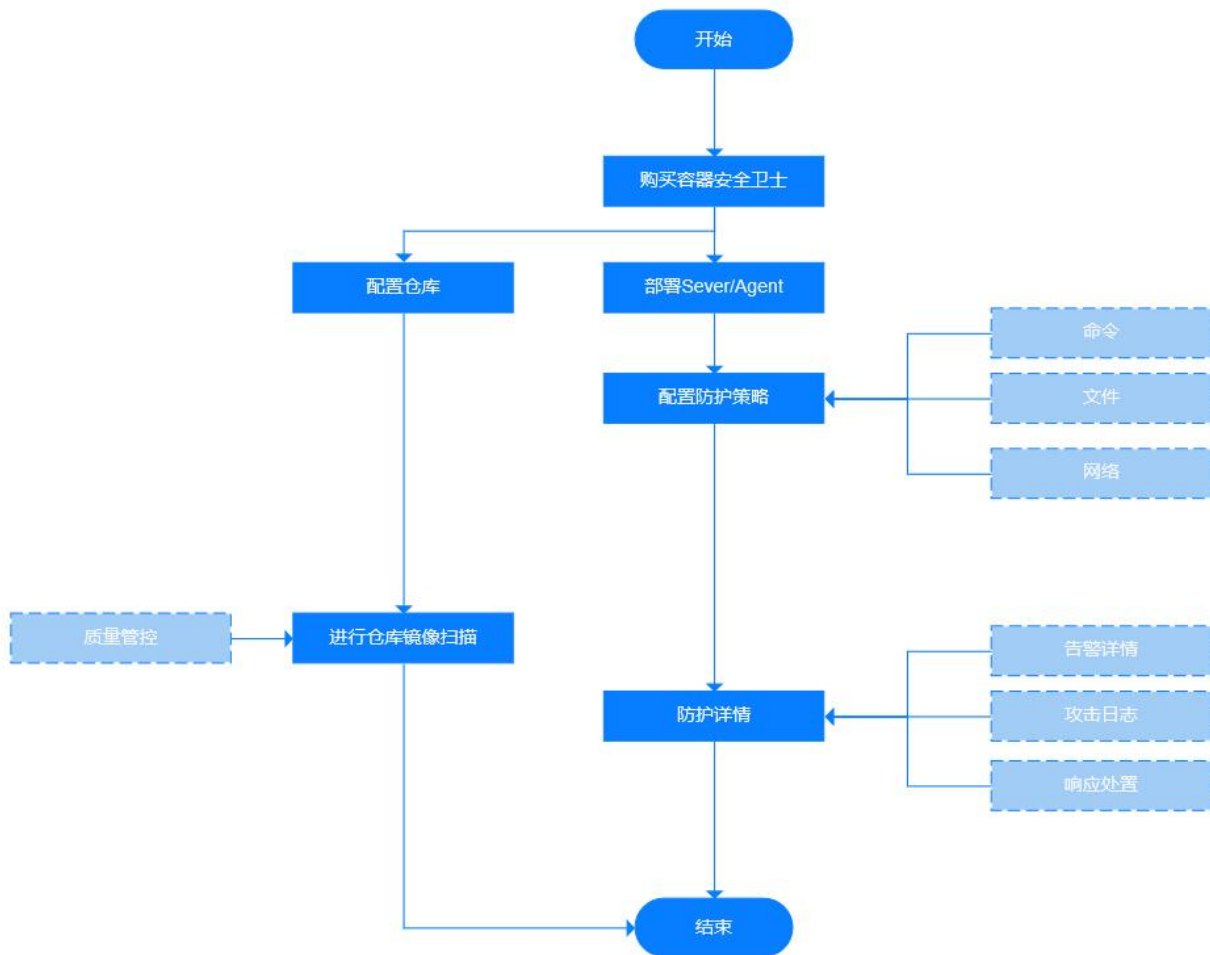
- 确认退订信息，信息确认无误后选择退订原因，勾选“我已确认本次退订金额和相关费用”后，单击“退订”后即可进行退订。

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，支持升级购买的服务版本以及扩增节点数量，但不支持降级。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

- 登录天翼云控制中心。
- 单击管理控制台上方的区域框，选择地域。
- 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。
- 单击“立即订购”，进入产品订购页面。

< 订购容器安全卫士

配置详情

* 版本选择 标准版 高级版

* 地区 请选择资源池

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，可减少网络时延，提高访问速度。

* 防护节点数 - 1 +

* 自动续订

按月购买：自动续订周期为 3 个月；按年购买：自动续订周期为 1 年

* 购买时长 1 个月

1 个月 2 个月 3 个月 4 个月 5 个月 6 个月 7 个月 8 个月 9 个月 10 个月 11 个月 1 年 2 年 3 年 4 年 5 年

* 协议 我已阅读理解并同意 [《天翼云容器安全卫士服务协议》](#)

配置费用 **¥290.00**

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	提供标准版、高级版。不同版本差异请参见 产品规格 。
地区	若您需要切换区域，请在下拉框进行选择。 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	<p>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。</p> <ul style="list-style-type: none"> 按月购买，自动续费周期默认为 3 个月。 按年购买，自动续费周期默认为 1 年。 <p>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。</p>

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

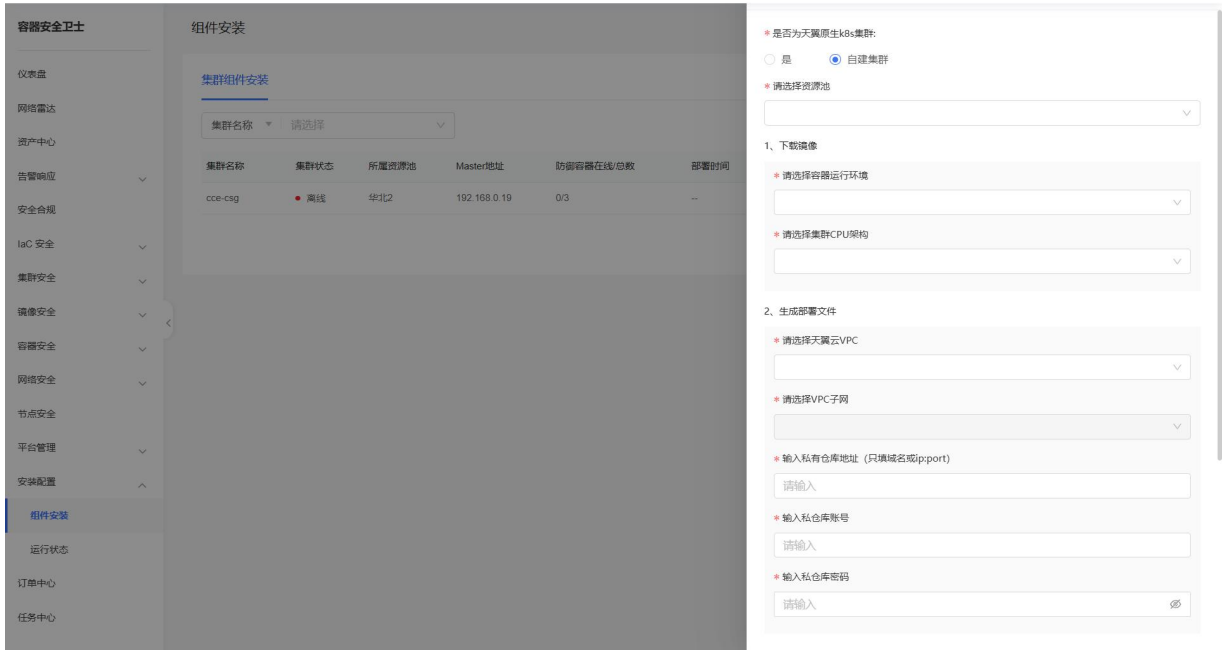
需要为容器集群安装 Sever/Agent，将容器集群纳管到容器安全卫士控制台后，才能对容器集群进行安全防护。

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“集群组件部署”，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

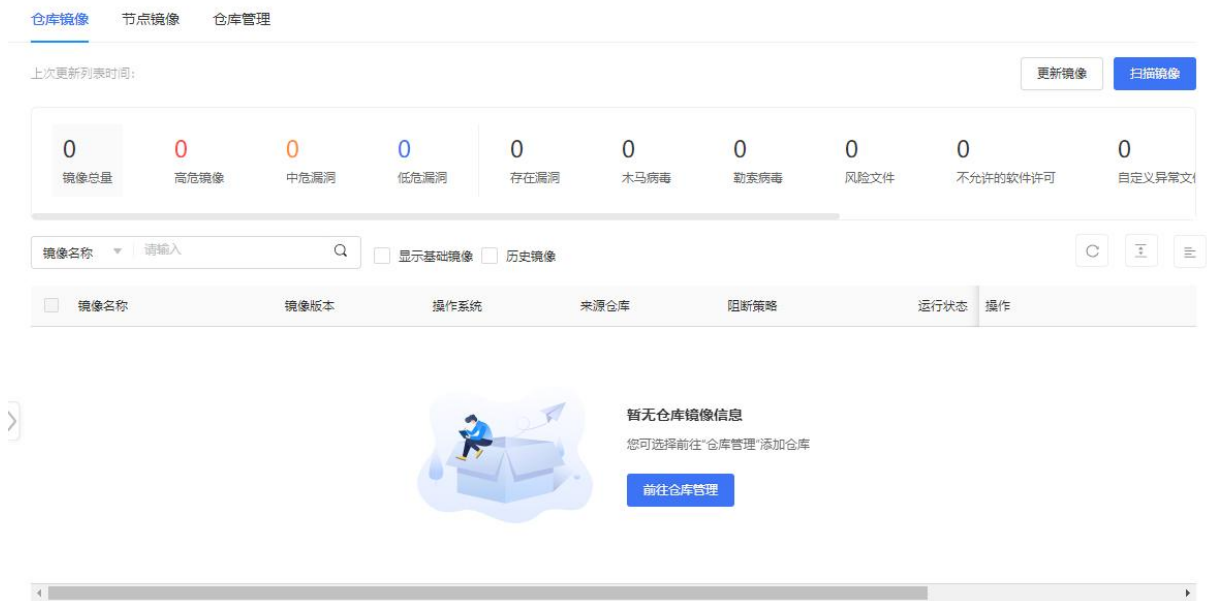
详细步骤请参见[购买云容器安全卫士](#)。

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。



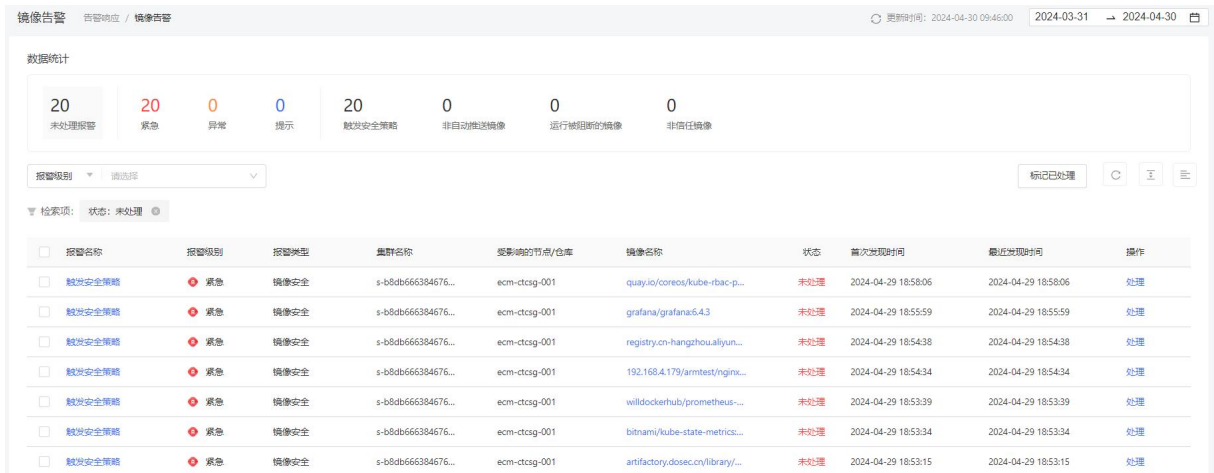
4. 扫描节点镜像。
 - a. 进入“节点镜像”页面，单击“更新镜像”，获取仓库镜像数据。
 - b. 单击“扫描镜像”，对镜像进行安全扫描。
5. 扫描仓库镜像。
 - a. 进入“仓库镜像”页面，单击“更新镜像”，获取仓库镜像数据。
 - b. 单击“扫描镜像”，对镜像进行安全扫描。

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。

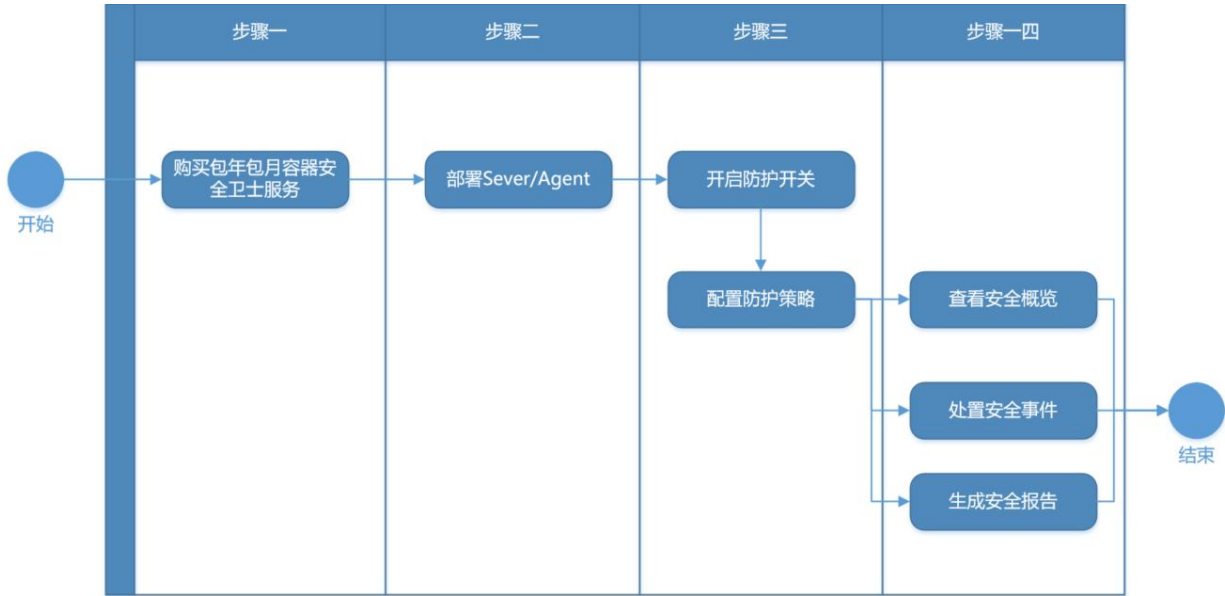


4. 单击列表操作列的“处理”，可对事件进行“标记为已处理”、“加入白名单”、“镜像阻断”等处置。单击列表右上方的“标记为已处理”，可以批量处置误报的告警。

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。

策略管理 容器安全 / 策略管理

入侵检测策略 入侵检测规则

命令执行 读写文件 网络活动 文件内容 主机异常 添加规则

规则名称 请输入 批量 刷新 重置 列表

<input type="checkbox"/>	风险等级	规则名称	告警信息	描述	策略调用数	启用状态	创建人	最近更新时间	操作
<input type="checkbox"/>	提示	添加setuid权限	setuid可以使执行者以...	为文件添加setuid权限	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	容器内proc目录被挂载	runc不允许容器内/pro...	发现容器内的proc目录...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似特权容器挂载设备...	特权容器内黑客可能通...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似cve-2018-15664逃...	可以通过docker cp的...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似修改命名空间逃逸	容器内进程命名空间被...	发现可疑进程，疑似容...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似containerd逃逸	存在漏洞的containerd...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似容器逃逸	容器内文件以宿主主机进...	发现容器内文件以宿主...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似dind逃逸漏洞利用	此进程可能造成系统破...	当容器挂载了docker.sock...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	crond执行恶意指令	此进程可能造成系统破...	发现容器内crond执行...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似webshell执行命令	此进程可能造成系统破...	发现容器内疑似websh...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多

共 30 条 < 1 2 3 > 10条/页

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。

运行态检测 告警响应 / 运行态检测 更新时间: 2024-04-30 14:56:33

ATT&CK 常见入侵行为 2024-03-31 - 2024-04-30 收起

初始访问(0)	执行(0)	持久化(0)	权限提升(0)	防御绕过(0)	凭证访问(0)	发现(0)	影响(1)	其他(0)
攻击对外开放的服务	容器命令管理	外部进程服务	逃逸到宿主主机	在宿主主机内构建镜像	暴力破解	容器和宿主机发现	端口拒绝服务	自定义安全策略
外部进程服务	部署容器	植入内部镜像	权限滥用	部署容器	不安全凭证	网络服务发现	网络拒绝服务	异常流量
可用账户	预留任务/作业	预留任务/作业	预留任务/作业	预留任务/作业	隔离防护		资源劫持	
	用户执行	可用账户	可用账户	可用账户	宿主主机指示器移除		破坏系统及数据	
			特权提升	伪装				
			触发式提权	可用账户				

报警级别 请选择 标记已处理 刷新 重置 列表

搜索项: 状态: 未处理

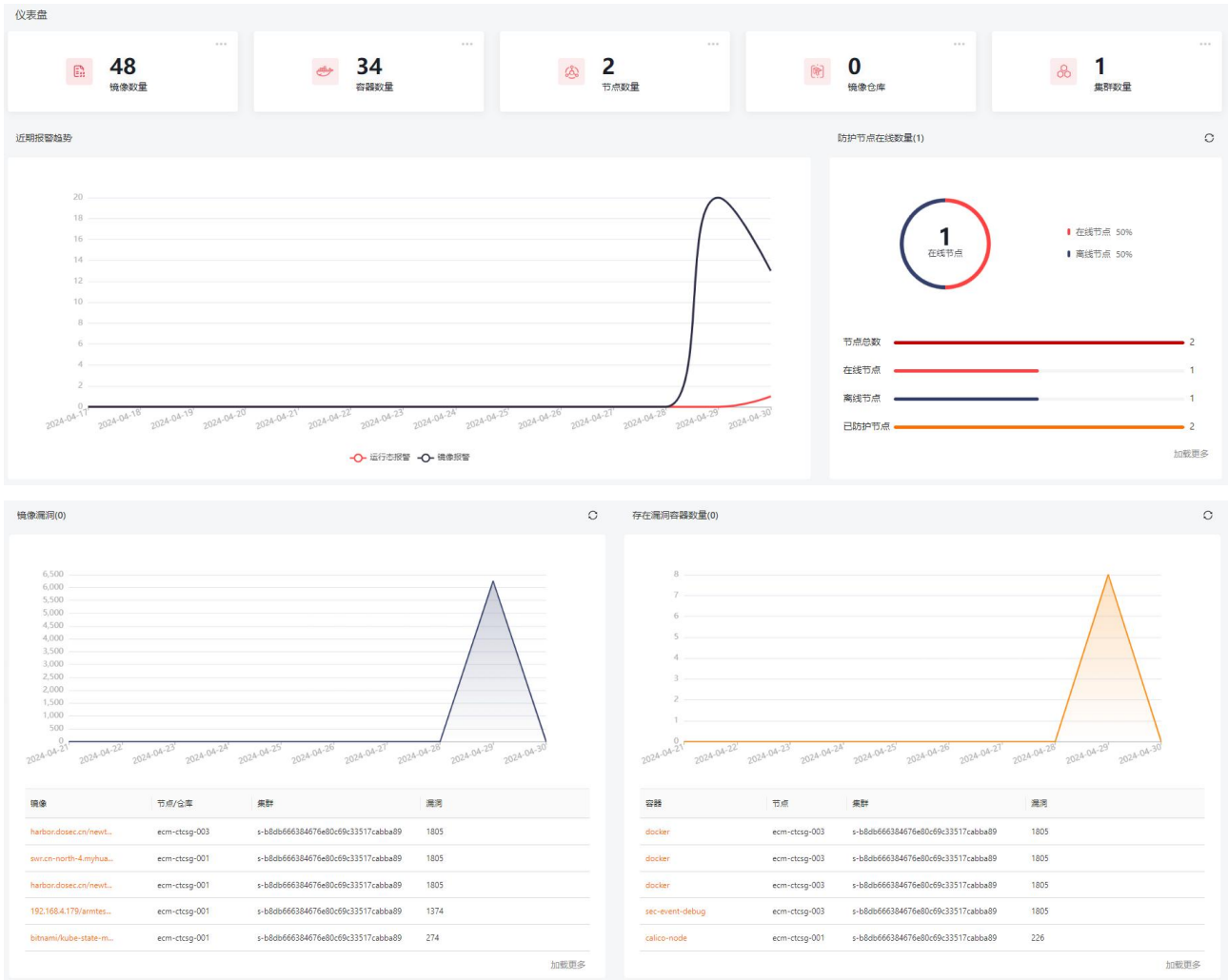
<input type="checkbox"/>	报警名称	报警级别	报警类型	集群名称	受影响的节点	受影响的命名空间	受影响的容器	状态	首次发现时间	最近发现时间	操作
<input type="checkbox"/>	执行远程文件传输命令	异常	命令执行	s-b8db666...	ecm-ctag-003	test2	k8s_sec-event...	未处理	2024-04-30 09:55:06	2024-04-30 09:55:06	处理

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. 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

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。
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。

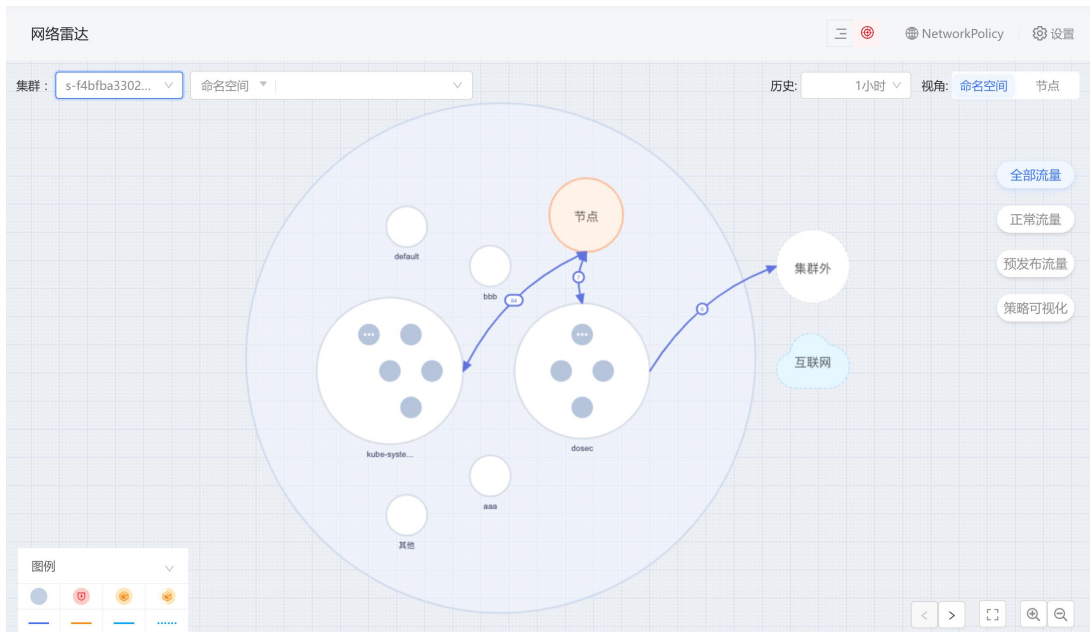
镜像漏洞

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。

4.2. 网络雷达

4.2.1. 查看网络雷达图

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。

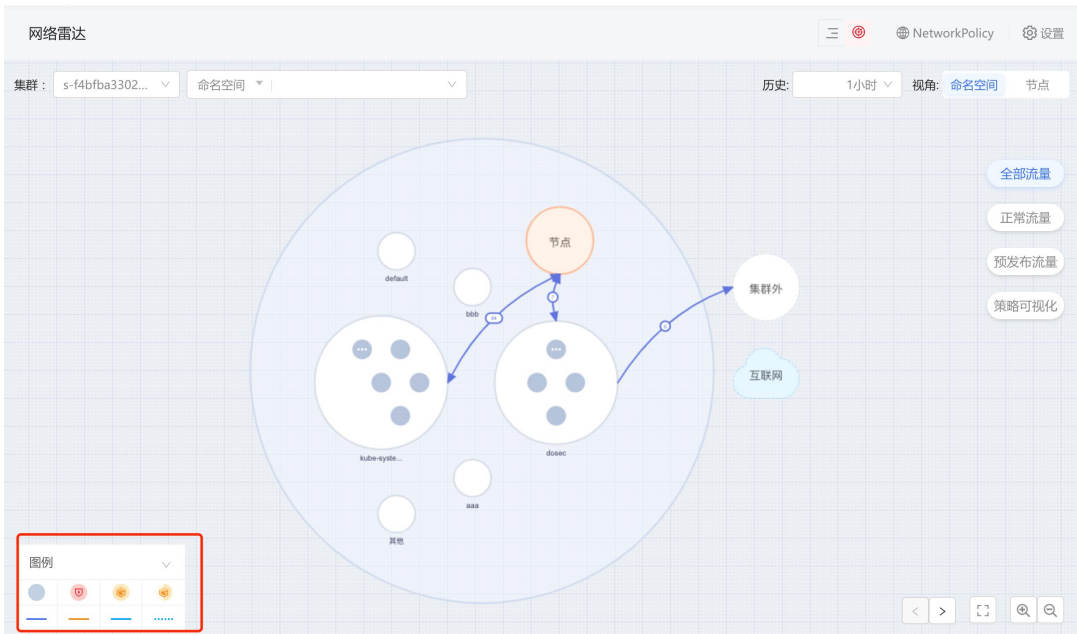


3. 在网络雷达图上方，支持按照“集群名称”、“命名空间名称”筛选查询，按照“工作负载名称”、“IP地址”、“工作负载标签”模糊查询。
 - 选择“集群名称”，将切换至相应集群的网络雷达图页面，可查看该集群中的所有命名空间、工作负载、Pods 的网络图。
 - 按照“命名空间名称”筛选查询，按照“工作负载名称”、“IP地址”、“工作负载标签”等条件搜索后，拓扑图将高亮显示相应资源。
4. 查看网络雷达图。
 - 整个视图以“集群 > 命名空间 > 工作负载”的级别区分各类资源。
 - “集群外”代表了非本集群内部的访问关系。
 - “互联网”代表了与公网 IP 的访问关系。
 - 页面默认根据全部流量、正常流量、异常流量展示命名空间最多的流量。
 - 每个命名空间内展示 9 个工作负载，点击跳转到当前命名空间下的工作负载视角。下方支持翻页。

4.2.2. 图例说明

在网络雷达图的左下方，展示网络雷达图的图例。

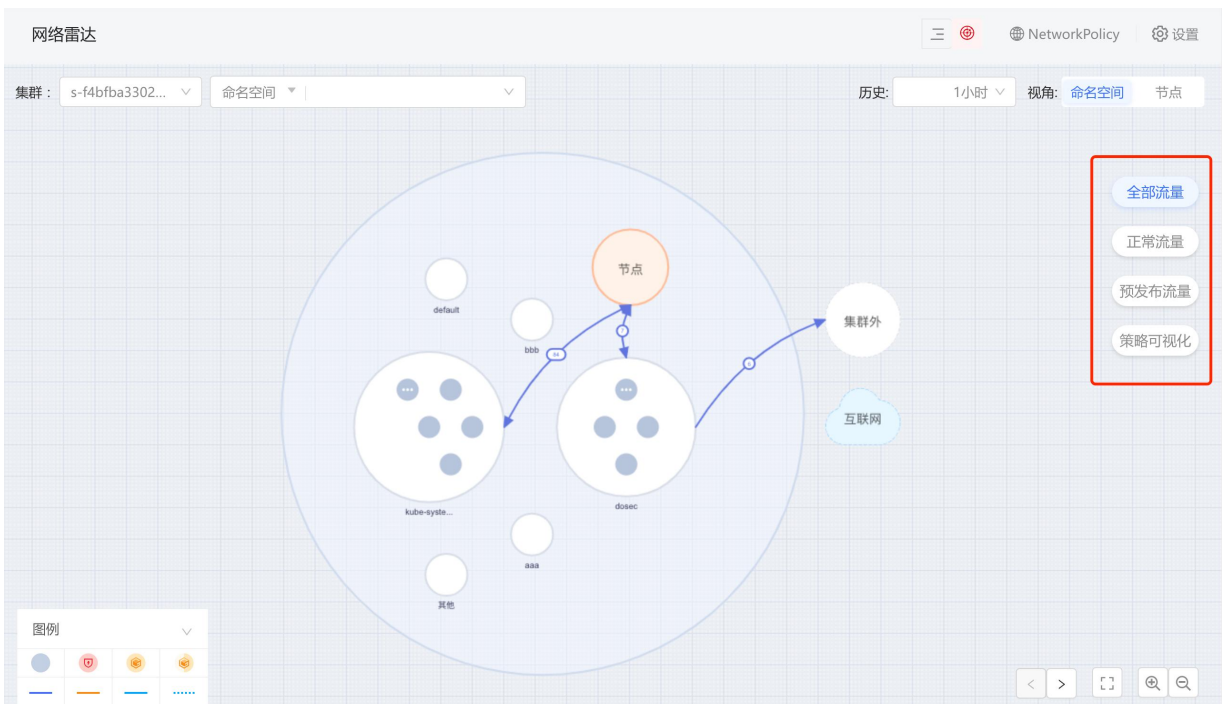
- 第一行展示了 4 种不同的工作负载。
- 第二行展示了不同访问类型的 4 种流量。用三种不同颜色的实线分别表示全部流量、正常流量、触发预发布策略的异常流量，用一种不同颜色的虚线表示预发布策略流量。



4.2.3. 按访问类型查看

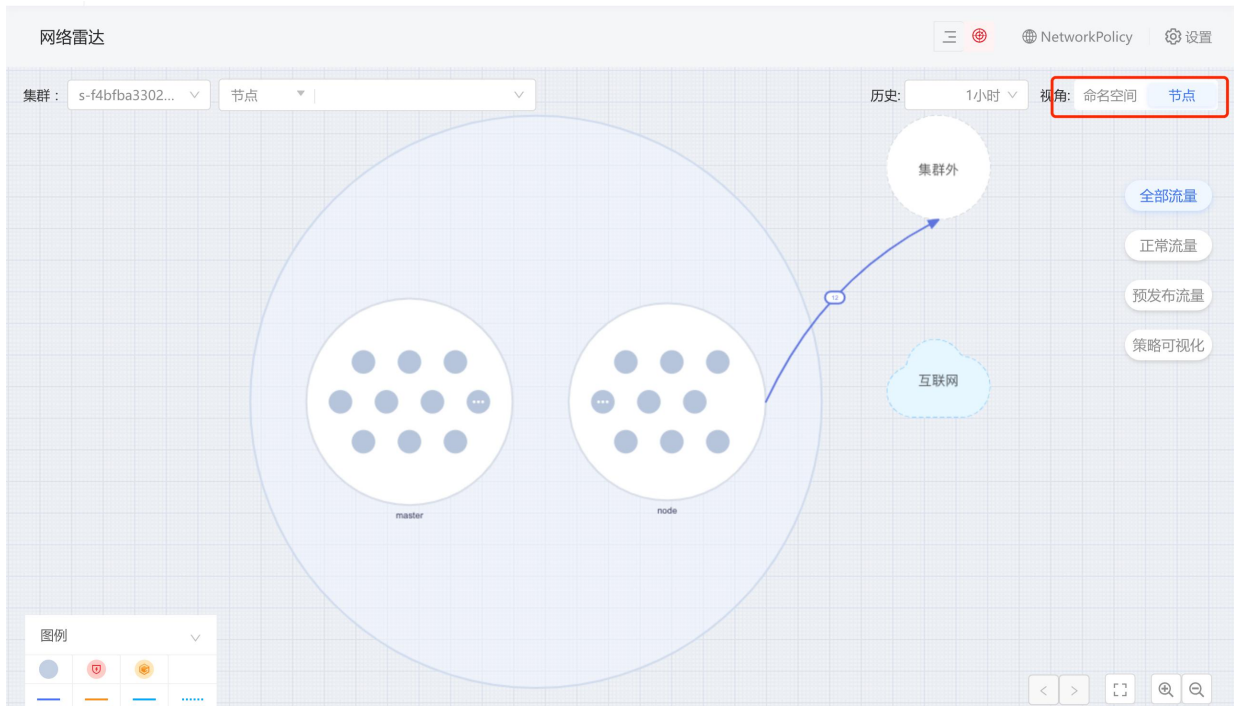
在网络雷达图右侧的访问类型中，包含全部流量、正常流量、预发布流量、策略可视化。系统默认展示全部流量，单击其他类型即可切换查看不同类型的流量。

预发布流量指的是触发预发布策略的流量将会产生报警的情况。



4.2.4. 查看命名空间之间的流量

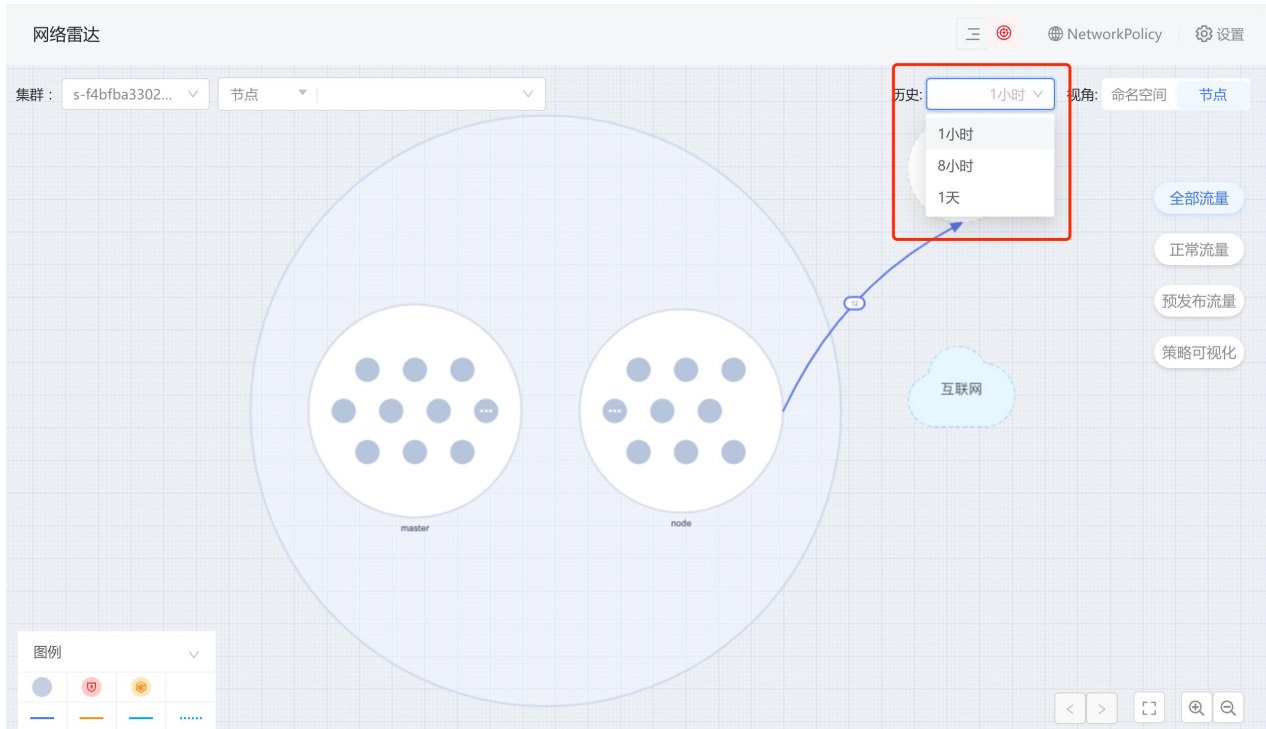
系统默认隐藏命名空间之间的流量。点击网络雷达图右上方的视角切换按钮“命名空间”或“节点”，可清晰地了解到整个链路中跨命名空间和节点的访问信息。



4.2.5. 查看历史访问流量

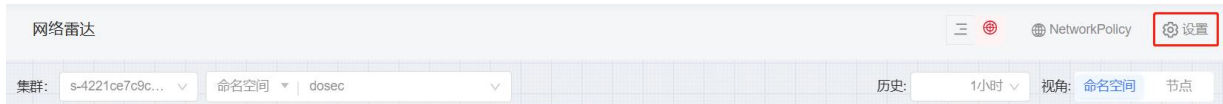
系统提供访问关系保留的功能，支持查看所选时间范围内的历史访问流量。支持选择的时间范围包括 1 小时、8 小时、1 天、7 天、30 天，可参照“设置历史时间”设置可选时间范围。

系统默认显示 1 小时内的访问流量，选择时间范围后，拓扑图中的访问连接关系将按选择的时间范围显示。



设置历史时间

1. 点击网络雷达图右上方的设置按钮。



2. 进入配置页面。支持选择 1 小时、8 小时、1 天、7 天、30 天的时间。



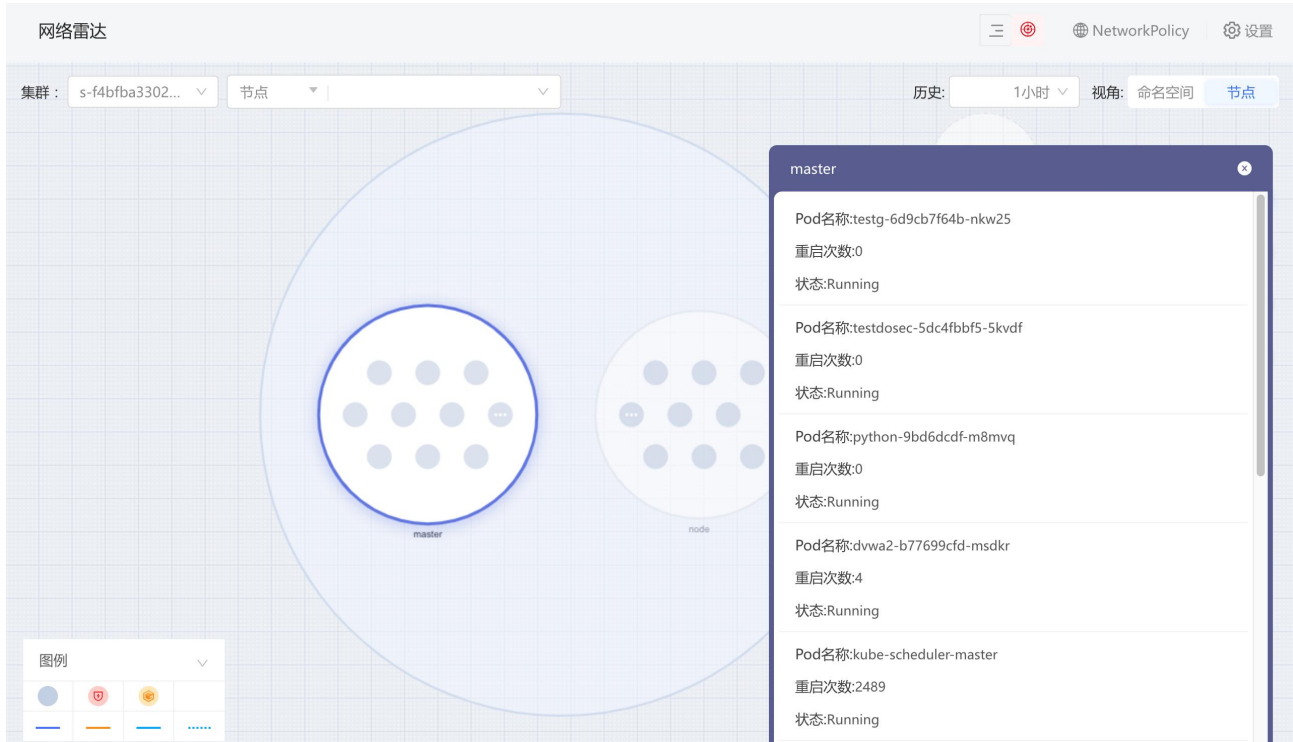
3. 单击“确定”，完成配置。

4.2.6. 查看命名空间

单击某个命名空间内空白区域，即可查看该命名空间中工作负载的分布情况，包含工作负载名称、副本数、创建时间、工作负载个数（工作负载名称个数即为命名空间关联的工作负载个数）。

参数	解释说明
----	------

参数	解释说明
工作负载名称	命名空间关联的工作负载的名称。
副本数	该工作负载 创建 Pod 副本的个数（由 replicas 字段标明）。
创建时间	该工作负载的创建时间。



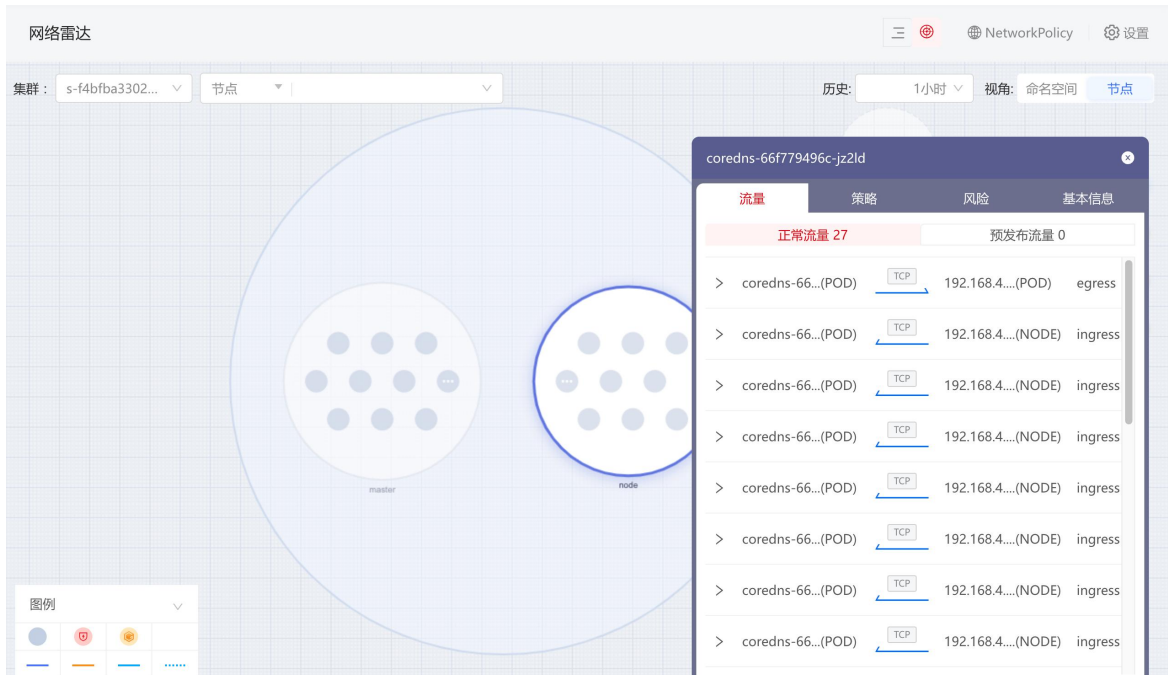
4.2.7. 查看工作负载

在工作负载的详情页面，可查看该工作负载的流量信息、触发的隔离策略、存在的风险信息和工作负载其他基本信息。

查看访问流量

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。
3. 单击某个工作负载，进入该工作负载的详情页面。
4. 在“流量”页签，查看访问流量。
5. 流量包括正常流量和异常流量，默认显示正常流量。

- 在“正常流量”中，可查看该工作负载所有的入站与出站访问信息。



■ 工作负载流量列表说明

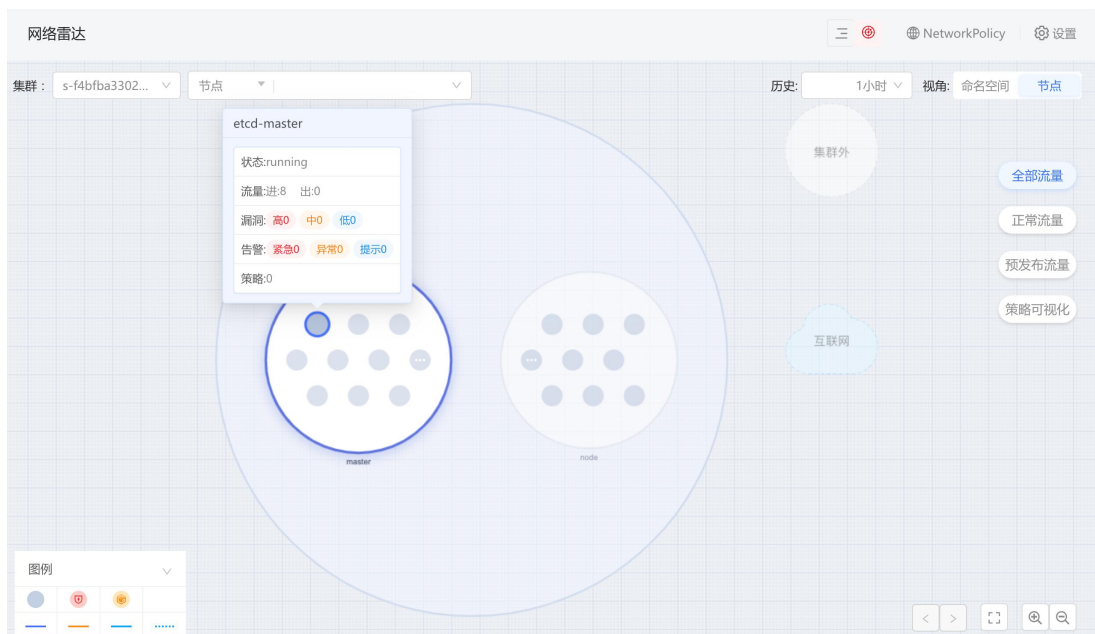
列数	解释说明
第一列	<p>访问源→访问目标。</p> <ul style="list-style-type: none"> ● 访问源和访问目标显示的内容为：源/目标命名空间、源/目标工作负载、源/目标端口、源/目标 IP、源/目标容器、源/目标服务、源/目标进程等。 ● 括号中的类型包括 POD、NODE、OUT 这三种类型。POD 类型表示与集群内部其他 Pod 之间的访问流量，NODE 类型表示集群内部 IP，OUT 类型表示与集群外部之间的访问流量。
第二列	使用的访问协议，TCP 或 UDP 协议。
第三列	<p>访问的类型，ingress 或 egress。</p> <ul style="list-style-type: none"> ● ingress 用于指定 Pod 的入口流量的网络策略，公开了从集群外部到集群内服务的 HTTP 和 HTTPS 路由。 ● egress 用于指定 Pod 的出口流量的网络策略，让服务访问集群外部的 HTTP、HTTPS、TCP 相关的服务。

- 单击下拉展开可查看访问流量的源对象和目标对象的详细信息。默认为收起状态。

访问流量信息参数说明：

参数	解释说明
源命名空间	访问源来自哪个命名空间，“--”表示可能是 OUT 或 NODE 类型的访问流量。OUT 表示来自集群外部的访问流量。
源对象	源对象的名称，Pod 名称或 IP 地址。
所属 deployment	源对象所属 Deployment 名称
源端口	源对象开放的流量输出端口
目标命名空间	访问目标对象所属命名空间
目标对象	目标对象的名称——Pod 名称或 IP 地址
所属 deployment	目标对象所属 Deployment 的名称
目的端口	目标对象开放的流量输入端口

- 查看工作负载内部的访问流量：在正常流量中会展示两条 ingress 类型的源对象所属 deployment 与目标对象所属 deployment 相同的访问流量。在网络雷达图中呈现出一个蓝色箭头指向工作负载自身。



- 切换至“预发布流量”页面，可查看与该 deployment 相关的所有触发了网络安全预发布策略的流量访问请求，显示内容信息与“正常流量”一致。



查看策略信息

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。
3. 单击某个工作负载，进入该工作负载的详情页面。
4. 选择“策略”页签，查看策略信息。

按照策略状态分为“已发布策略”和“预发布策略”页面。可查看与该 deployment 包含的所有 IP、pod 相关的所有网络安全策略（或预发布策略）的信息，包括策略名称、策略描述、策略类型这些信息。

5. 单击“前往策略管理”按钮后，跳转到“策略管理”页面，并搜索出对应策略。

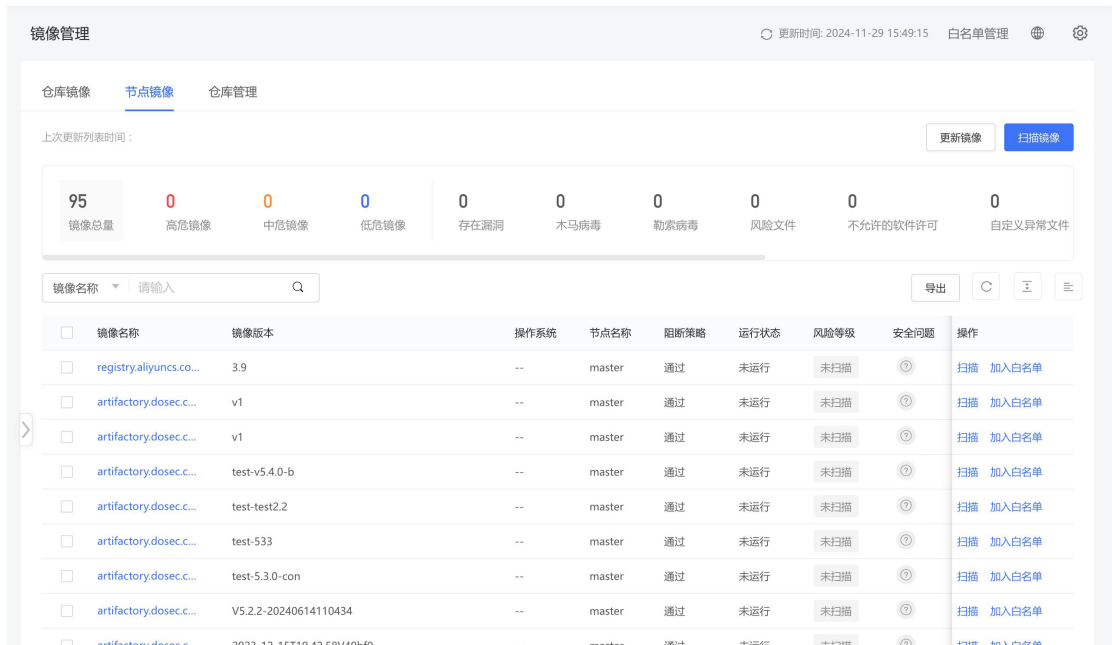


查看风险信息

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。
3. 单击某个工作负载，进入该工作负载的详情页面。
4. 定位到“风险”页面，可查看其风险来源，是存在漏洞还是报警提示。
 - 如果存在漏洞
 - a. 在“风险 > 漏洞”页面可查看该 deployment 构建 pod 时指定镜像的名称、版本和漏洞统计信息。



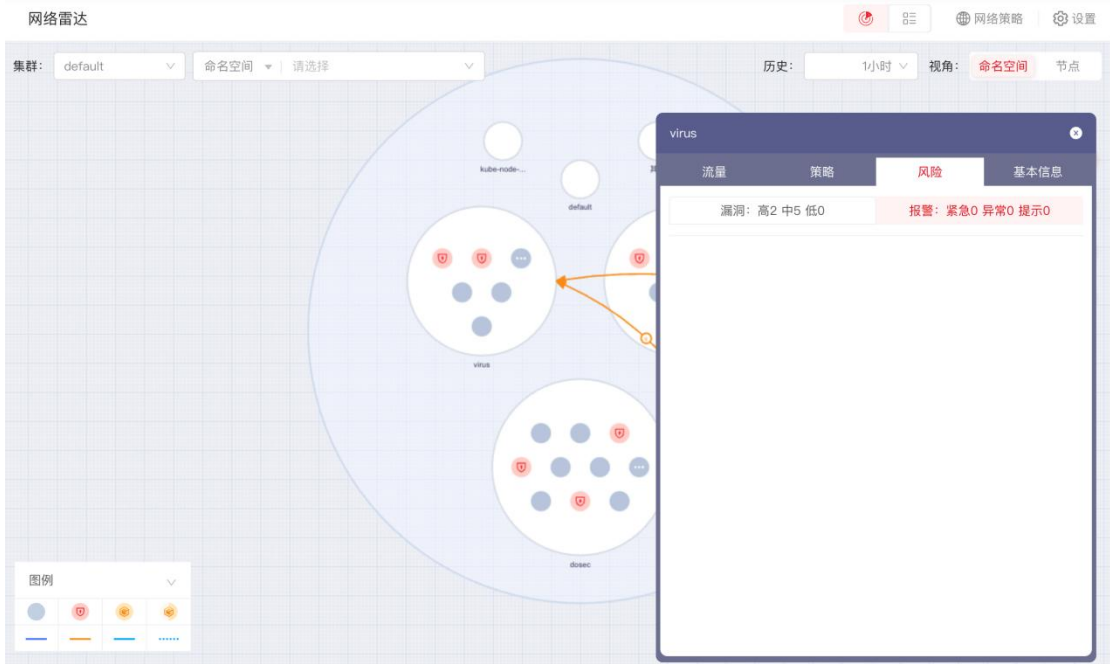
- b. 再单击“前往镜像安全”，跳转到“镜像安全 > 节点镜像”页面，可查看该镜像的漏洞风险详情。在“镜像安全”页面，系统将自动按照刚刚查看的镜像名称进行检索，自动筛选出该镜像。



- c. 单击“镜像名称”即可查看镜像安全概览、关联信息、漏洞详情、软件、文件、环境变量、安全溯源等详细信息。

– 如果有报警提示

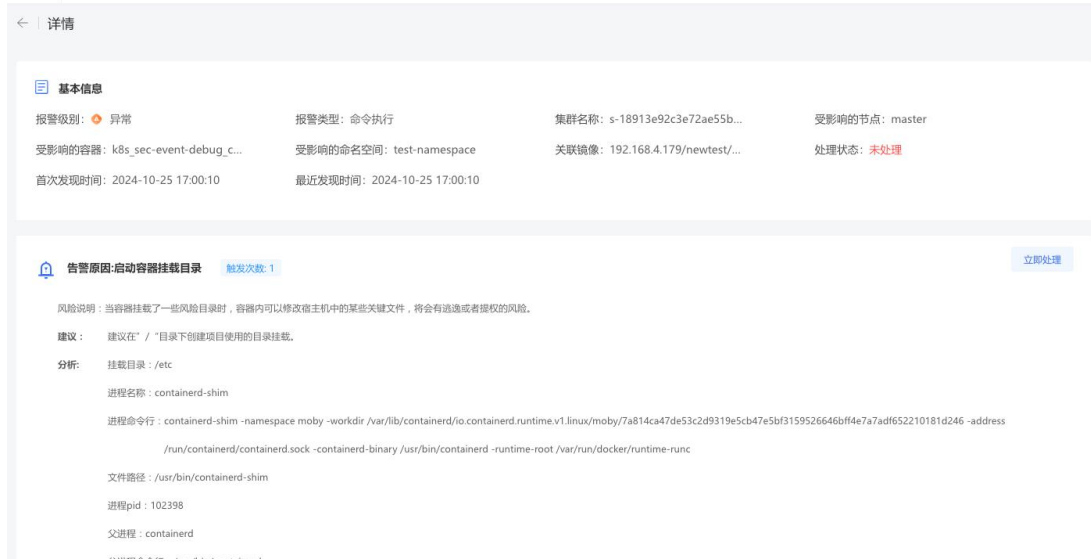
- a. 在“风险 > 报警”页面可查看该 deployment 中包含的容器存在的未处理报警信息，包括容器的名称、所在节点、报警数量统计信息。



- b. 再单击“前往运行态检测”，跳转到“告警响应 > 运行态检测”页面，可查看该容器的未处理报警信息。在“告警响应 > 运行态检测”页面，系统将自动按照刚刚查看的报警信息进行检索，自动筛选出该报警信息。



- c. 单击操作列中的“详情”可查看攻击链条、告警原因、风险说明、建议等信息，并立即进行处理。



← | 详情

基本信息

报警级别: 异常	报警类型: 命令执行	集群名称: s-18913e92c3e72ae55b...	受影响的节点: master
受影响的容器: k8s_sec-event-debug_c...	受影响的命名空间: test-namespace	关联镜像: 192.168.4.179/newtest/...	处理状态: 未处理
首次发现时间: 2024-10-25 17:00:10	最近发现时间: 2024-10-25 17:00:10		

告警原因: 启动容器挂载目录 触发次数: 1 [立即处理](#)

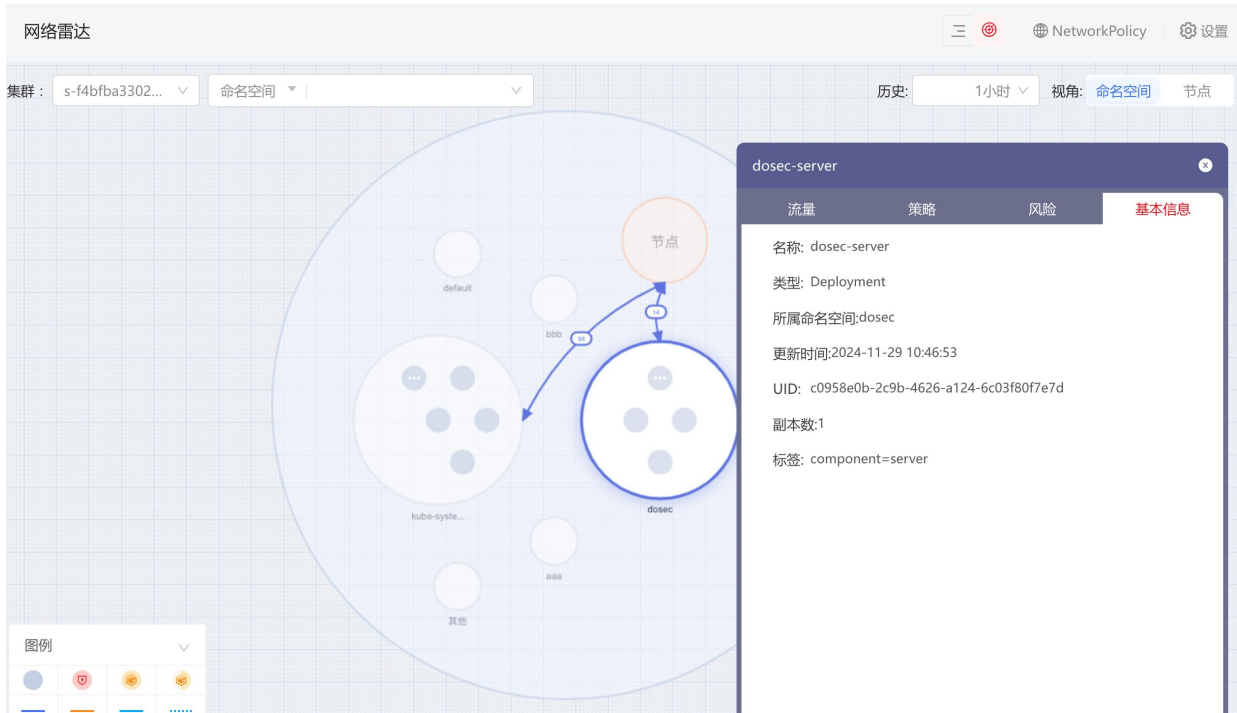
风险说明: 当容器挂载了一些风险目录时, 容器内可以修改宿主机中的某些关键文件, 将会有逃逸或者提权的风险。

建议: 建议在 / 目录下创建项目使用的目录挂载。

分析: 挂载目录: /etc
进程名称: containerd-shim
进程命令行: containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1.linux/moby/7a814ca47de53c2d9319e5cb47e5bf3159526646bf4e7a7ad652210181d246 -address /run/containerd/containerd.sock -containerd-binary /usr/bin/containerd -runtime-root /var/run/docker/runtime-runc
文件路径: /usr/bin/containerd-shim
进程pid: 102398
父进程: containerd
容器ID: /var/lib/containerd

查看基本信息

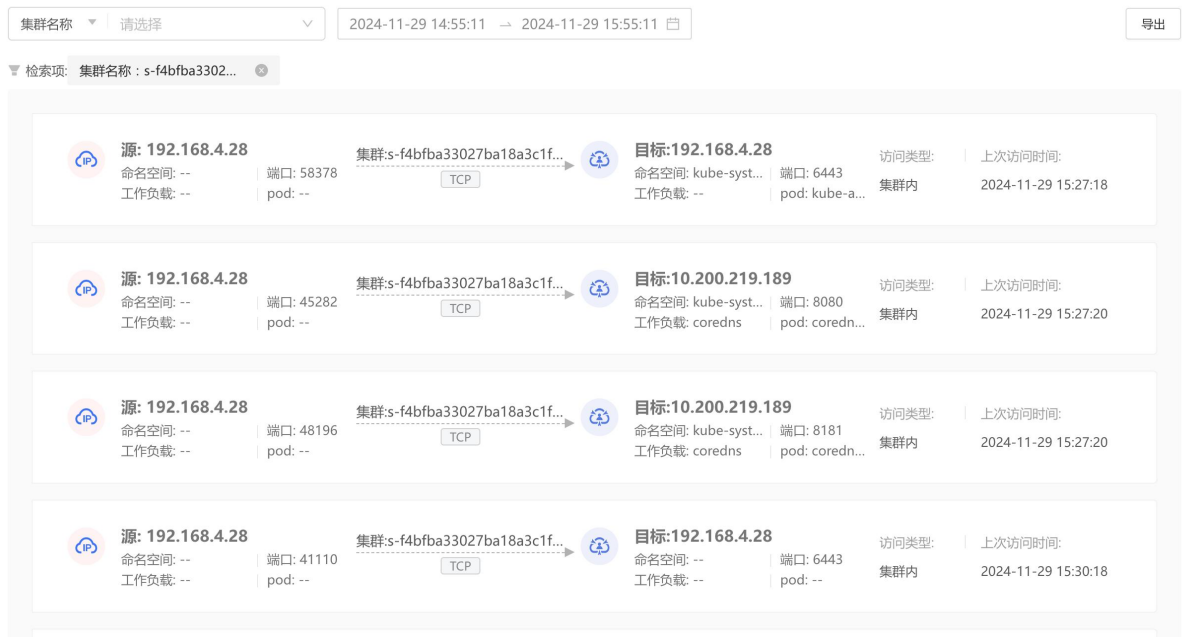
1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。
3. 单击某个工作负载，进入该工作负载的详情页面。
4. 在详情中的“基本信息”页面，可查看该工作负载的名称、类型、所属命名空间、UID、副本数、标签等基本信息。



4.2.8. 切换表格视图

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络雷达”，进入网络雷达可视图页面。
3. 单击雷达网络图的右上角的 按钮，即可切换至表格视图。

在表格视图内，支持按照“源命名空间”、“源端口”、“目标命名空间”、“目标端口”、“集群名称”筛选查看。



4. 单击雷达网络图的左上角的 按钮，可切换回雷达网络图视角。

导出列表

1. 单击列表右上角的“导出”按钮，选择导出范围，导出全部访问信息或当前列表筛选结果中的访问信息。



2. 单击“确认”，可将导出任务添加至“任务中心”，开始生成网络雷达流量记录报表。

3. 在“任务中心 > 下载任务管理”中，找到对应下载任务，待下载文件生成完毕后，单击“下载”按钮即可下载至本地。

4.3. 资产中心

“资产中心”是汇集所有功能模块的入口，旨在提高资源的利用率和管理效率，同时提升用户的使用体验。

4.3.1. 更新资产

设置更新范围

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“资产中心”，进入资产中心页面。
3. 单击资产中心页面右上角的“设置”图标。



4. 进入资产设置页面，对更新范围进行选择。

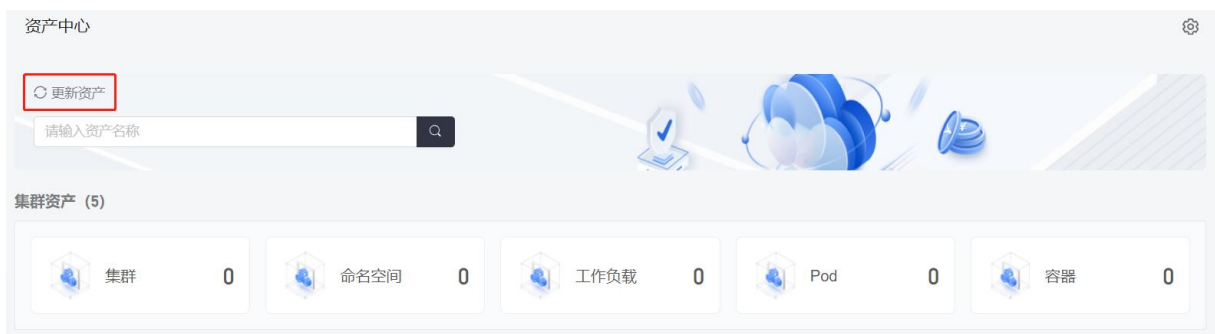
更新范围支持全部资产和集群资产：

- 全部资产：更新慢，更新所有资产。
- 集群资产：更新快，更新除仓库镜像外的资产。仓库镜像可通过在“镜像安全 > 镜像设置 > 扫描设置”设置“仓库镜像更新周期”定期自动更新。具体操作请参见镜像设置。



手动更新资产

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“资产中心”，进入资产中心页面。
3. 单击资产中心页面左上角的“更新资产”，系统将按照已设置的更新范围更新资产。



4.3.2. 查看资产

资产按照不同板块进行了5大类，分别为集群资产、镜像资产、节点资产、应用服务以及配置相关，也可通过搜索资产名称定位到你想要的资产。

4.3.2.1. 集群

4.3.2.1.1. 查看集群列表

1. 点击【集群名称】，跳转至 Kubernetes 集群列表。
2. 集群列表页面，支持按照“集群状态”、“集群名称”、“Master 地址”进行筛选查询。



参数	解释说明
集群名称	<p>集群名称是在部署安装容器安全平台的 server 组件和 agent 组件时设定。如果是图形化安装上述组件，则可以在【安装配置】-【组件安装】-【防御容器安装】-【新建集群】页面设定“集群名称”。</p> <p>如果是后台 yaml 文件部署上述组件，则“集群名称”是在编排文件中设定。</p>
集群版本	Kubernetes 的版本号，由 server 组件读取信息。
集群状态	在线与离线两种状态。离线指的是该集群与容器安全平台无法正常通信，并不代表集群本身一定存在故障。
Master 地址	Kubernetes 集群的节点存在两种角色，Master（控制节点）和 Node（计算节点）。此参数展示控制节点的 IP 地址，数量可能为 1 个或多个（通常为奇数）。
Node 数量	Kubernetes 集群内计算节点的数量。
漏洞数量	该集群包含的组件的漏洞统计，按高中低级别进行汇总。

4.3.2.1.2. 查看集群详情

1. 查看集群列表；
2. 单击【集群名称】，进入集群详情页面；
3. 在集群详情页面，可查看该集群的关联节点、关联命名空间和组件信息；

← 集群-s-18913e92c3e7...352

关联节点 关联命名空间

节点名称 请输入 Q

跳转至节点安全

节点名称	IP	类型	状态
master	192.168.4.80	防护容器	已连接
node02	192.168.4.82	防护容器	已连接
node03	192.168.4.83	防护容器	已连接
node02	192.168.4.82	扫描容器	已连接
node01	192.168.4.81	防护容器	已连接

共5条 < 1 > 10 条/页

← 集群-s-18913e92c3e7...352

关联节点 关联命名空间

名称 请输入 Q

跳转至命名空间

名称	工作负载数量	内存限制	CPU限制	状态
wanghy	2	无限制	无限制	Active
test2	8	无限制	无限制	Active
test-namespace	2	无限制	无限制	Active
kube-system	6	无限制	无限制	Active
kube-public	0	无限制	无限制	Active
kube-node-lease	0	无限制	无限制	Active
dosec	5	无限制	无限制	Active
default	0	无限制	无限制	Active
custom-namespace	0	无限制	无限制	Active

共9条 < 1 > 10 条/页

- 单击关联节点页面的【跳转至节点安全】，可跳转至【节点状态】页面，查看该集群节点的安全状况；
- 单击关联命名空间页面的【跳转至命名空间】，可跳转至【资产中心】-【命名空间】页面，管理命名空间标签；

数据统计
开始扫描

5
全部节点

4
在线防御容器

0
离线防御容器

1
在线集群

0
离线集群

请输入

▼ 检索项: 节点类型: 防御容器

<input type="checkbox"/>	节点名称	IPv4地址	IPv6地址	集群	系统类型	节点状态	扫描状态	最近扫描时间	发现时间	操作
<input type="checkbox"/>	master	192.168.4.80	--	s-18913e92c3e72ae55b32abef8a0633...		已连接	待扫描	--	2024-10-23 15:05:24	扫描 删除 ...
<input type="checkbox"/>	node02	192.168.4.82	--	s-18913e92c3e72ae55b32abef8a0633...		已连接	待扫描	--	2024-10-23 15:05:00	扫描 删除 ...
<input type="checkbox"/>	node03	192.168.4.83	--	s-18913e92c3e72ae55b32abef8a0633...		已连接	待扫描	--	2024-10-23 15:04:26	扫描 删除 ...
<input type="checkbox"/>	node01	192.168.4.81	--	s-18913e92c3e72ae55b32abef8a0633...		已连接	待扫描	--	2024-10-23 15:04:03	扫描 删除 ...

共4条 < 1 > 10条/页

命名空间
开始扫描

请输入

名称	所属集群	更新时间	操作
wanghy	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
test2	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
test-namespace	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
kube-system	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
kube-public	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
kube-node-lease	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
dosec	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
default	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签
custom-namespace	s-18913e92c3e72ae55b32abef8a0633...	2024-10-23 15:37:37	管理标签

共9条 < 1 > 10条/页

4.3.2.2. 命名空间

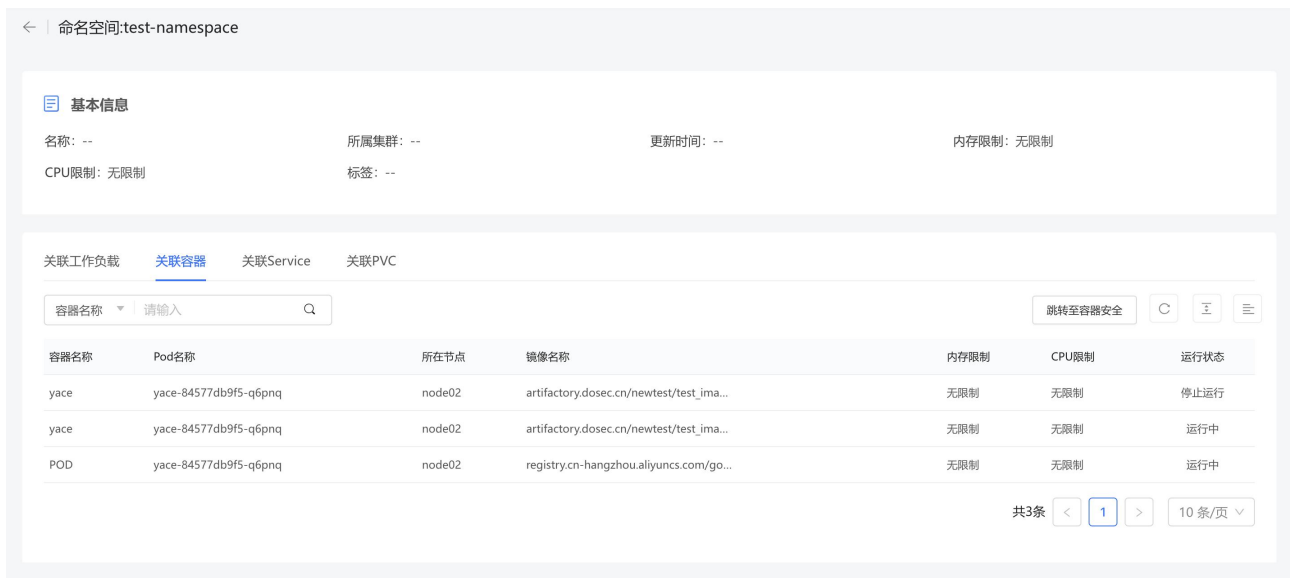
4.3.2.2.1. 查看命名空间列表

1. 单击【命名空间名称】，跳转至命名空间列表。
2. 命名空间列表页面，支持按照“名称”、“所属集群”进行筛选查询。

参数	解释说明
名称	命名空间的名称
所属集群	命名空间所属集群的名称
更新时间	命名空间更新的时间
管理标签	标签用来标记命名空间，于【网络安全】-【策略管理】中选择策略应用对象时使用。在管理标签页面，可以查看或删除该命名空间的标签键、标签值信息。

4.3.2.2.2. 查看命名空间详情

1. 查看命名空间列表；
2. 单击命名空间列表中的【名称】，进入命名空间详情页面；
3. 查看基本信息：在详情中的基本信息页面，可查看该命名空间的其他基本信息：内存限制和 CPU 限制，用来展示该命名空间占用资源限额，“无限制”表示没有为其设置资源限额。
4. 查看关联工作负载：在详情中的关联工作负载页面，可查看该命名空间关联的工作负载信息。点击“跳转至工作负载”，可跳跃至资产中心-工作负载页面，查看工作负载更多详细信息。
5. 查看关联容器：在详情中的关联容器页面，可查看镜像关联的容器信息。点击“跳转至容器安全”，可跳跃至容器安全-实时监测页面，查看容器安全检测信息。
6. 查看关联 Service：在详情中的关联 Service 页面，可查看该命名空间关联的 Service 信息。点击“跳转至 Service”，可跳跃至资产中心-Service 页面，查看关联 Service 更多详细信息。
7. 查看关联 PVC：在详情中的关联 PVC 页面，可查看该命名空间关联的 PVC 信息。点击“跳转至 PVC”，可跳跃至资产中心-PVC 页面，查看关联 PVC 更多详细信息。



命名空间:test-namespace

基本信息

名称: -- 所属集群: -- 更新时间: -- 内存限制: 无限制
CPU限制: 无限制 标签: --

关联工作负载 关联容器 关联Service 关联PVC

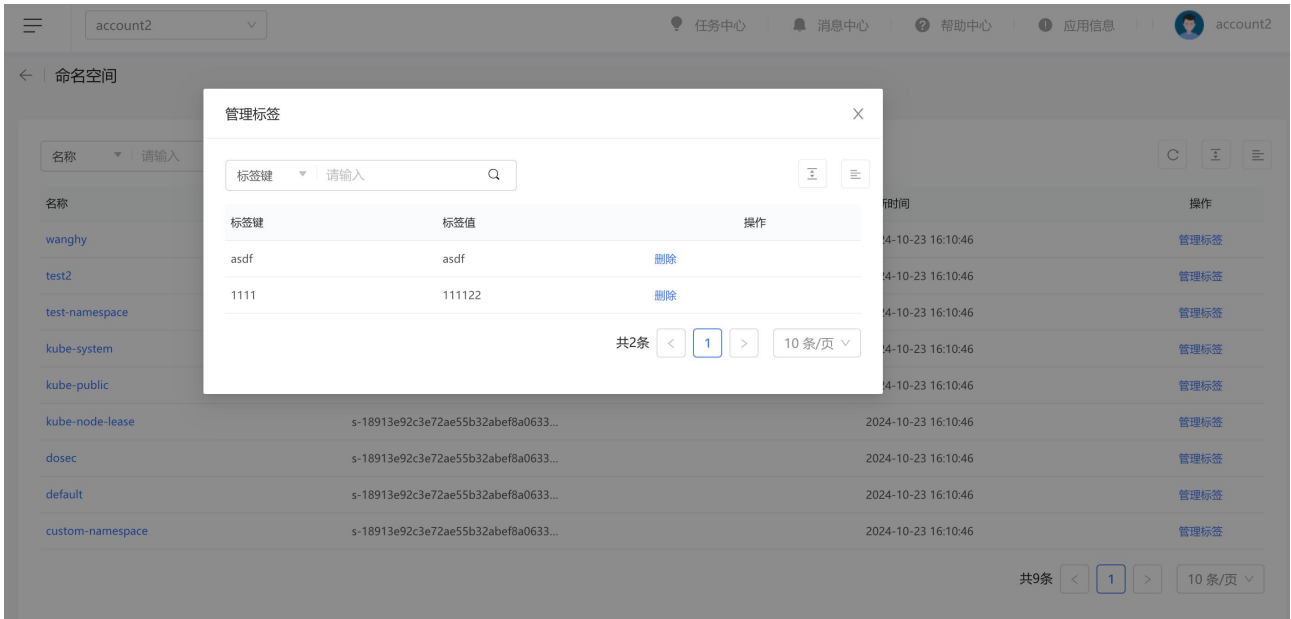
容器名称 请输入 Q 跳转至容器安全 C 三

容器名称	Pod名称	所在节点	镜像名称	内存限制	CPU限制	运行状态
yace	yace-84577db9f5-q6pnq	node02	artifactory.dosec.cn/newtest/test_jma...	无限制	无限制	停止运行
yace	yace-84577db9f5-q6pnq	node02	artifactory.dosec.cn/newtest/test_jma...	无限制	无限制	运行中
POD	yace-84577db9f5-q6pnq	node02	registry.cn-hangzhou.aliyuncs.com/go...	无限制	无限制	运行中

共3条 < 1 > 10条/页

4.3.2.2.3. 管理标签

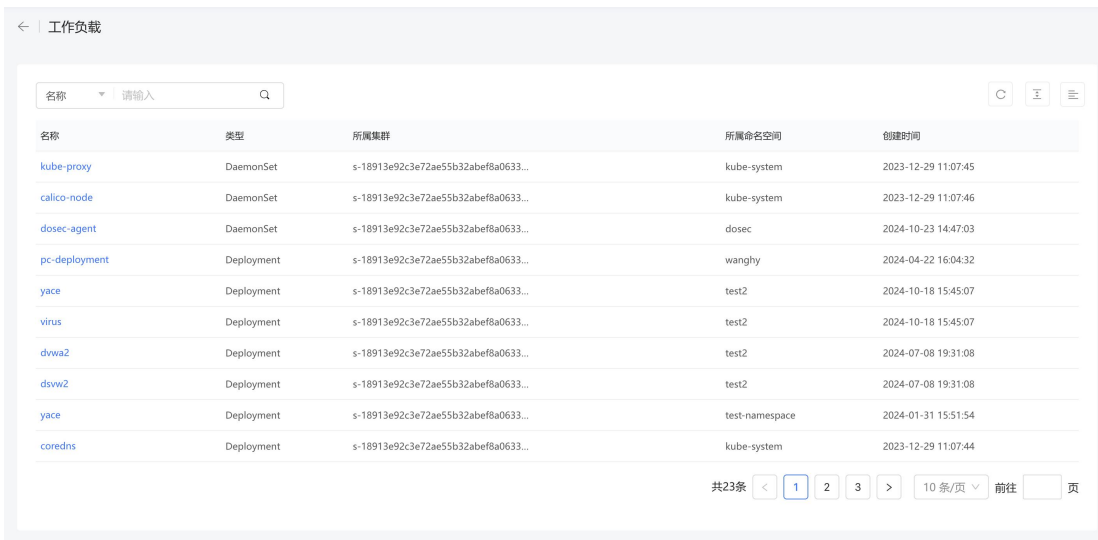
进入命名空间列表页，点击操作栏的【管理标签】，弹出弹窗后，可对标签键和标签值进行删除



4.3.2.3. 工作负载

4.3.2.3.1. 查看工作负载列表

单击【工作负载】，跳转至工作负载列表。工作负载列表页面，支持按照“名称”、“所属集群”、“所属命名空间”、“类型”进行筛选查询。



参数	解释说明
名称	工作负载的名称，在创建时通过 yaml 文件定义，对应于 yaml 文件中“metadata.name”字段
类型	工作负载的类型，主要包含 Deployment、ReplicaSet、StatefulSet、DaemonSet、

参数	解释说明
	CronJob、Job、ReplicationController 这七种不同类型，对应于 yaml 文件中的“kind” 字段值
所属命名空间	说明该工作负载是包含在哪个命名空间之中的，可在 yaml 文件中定义所属命名空间，不写明表示默认 default 命名空间
所属集群	工作负载所属集群的名称
创建时间	工作负载创建的时间

4.3.2.3.2. 查看工作负载详情

1. 查看工作负载列表；
2. 单击工作负载列表中的【名称】，进入工作负载详情页面；在工作负载详情页面，可查看该工作负载的其他基本信息：关联容器和关联 Pod，关联容器可跳转至容器安全的详情页，关联 Pod 可跳转至 Pod 列表

← | 工作负载:kube-proxy

基本信息

名称: kube-proxy 类型: DaemonSet 所属命名空间: kube-system 更新时间: 2024-10-23 15:37:23

UID: bd44d4db-323d-43b9-b3db-32423df5a0df 副本数: 1 标签: k8s-app=kube-proxy

关联容器 关联Pod

容器名称

容器名称	Pod名称	所在节点	镜像名称	内存限制	CPU限制	运行状态
kube-proxy	kube-proxy-jwkt2	master	registry.cn-hangzhou.aliyuncs.com/go...	无限制	无限制	运行中
kube-proxy	kube-proxy-tbzb9	node02	registry.cn-hangzhou.aliyuncs.com/go...	无限制	无限制	运行中
kube-proxy	kube-proxy-rx5xp	node03	registry.cn-hangzhou.aliyuncs.com/go...	无限制	无限制	运行中
kube-proxy	kube-proxy-h445h	node01	registry.cn-hangzhou.aliyuncs.com/go...	无限制	无限制	运行中

共4条 < 1 > 10条/页 ▾

← | 工作负载:kube-proxy

基本信息

名称: kube-proxy 类型: DaemonSet 所属命名空间: kube-system 更新时间: 2024-10-23 15:37:23

UID: bd44d4db-323d-43b9-b3db-32423df5a0df 副本数: 1 标签: k8s-app=kube-proxy

关联容器 **关联Pod**

Pod名称 请输入

Pod名称	所属集群	所属命名空间	运行状态	IP	更新时间
kube-proxy-tbzip9	s-18913e92c3e72ae55b32abef8a0633...	kube-system	Running	192.168.4.82	2024-10-23 15:37:25
kube-proxy-rx5xp	s-18913e92c3e72ae55b32abef8a0633...	kube-system	Running	192.168.4.83	2024-10-23 15:37:25
kube-proxy-jwkt2	s-18913e92c3e72ae55b32abef8a0633...	kube-system	Running	192.168.4.80	2024-10-23 15:37:25
kube-proxy-h445h	s-18913e92c3e72ae55b32abef8a0633...	kube-system	Running	192.168.4.81	2024-10-23 15:37:25

共4条 < 1 > 10条/页 ▾

4.3.2.4. Pod

4.3.2.4.1. 查看 Pod 列表

1. 单击【Pod】名称，跳转至 Pod 列表。
2. Pod 列表页面，支持按照“名称”、“所属集群”、“所属命名空间”、“IP”进行筛选查询。

← | Pod

Pod名称 请输入

Pod名称	所属集群	所属命名空间	重启次数	状态	IP
pc-deployment-5ff...	s-18913e92c3e72ae55b32abef8a0633...	wanghy	0	Running	10.233.140.116
yace-84fc849dd...	s-18913e92c3e72ae55b32abef8a0633...	test2	0	Running	10.233.219.68
virus-d68767447-s...	s-18913e92c3e72ae55b32abef8a0633...	test2	0	Running	10.233.219.122
dwaa2-56fc45cdf...	s-18913e92c3e72ae55b32abef8a0633...	test2	0	Running	10.233.186.225
dsvw2-6b67cd549...	s-18913e92c3e72ae55b32abef8a0633...	test2	1	Running	10.233.140.117
yace-84577db9f5...	s-18913e92c3e72ae55b32abef8a0633...	test-namespace	1	Running	10.233.140.84
kube-scheduler-m...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	9	Running	192.168.4.80
kube-proxy-tbzip9	s-18913e92c3e72ae55b32abef8a0633...	kube-system	1	Running	192.168.4.82
kube-proxy-rx5xp	s-18913e92c3e72ae55b32abef8a0633...	kube-system	1	Running	192.168.4.83
kube-proxy-jwkt2	s-18913e92c3e72ae55b32abef8a0633...	kube-system	7	Running	192.168.4.80

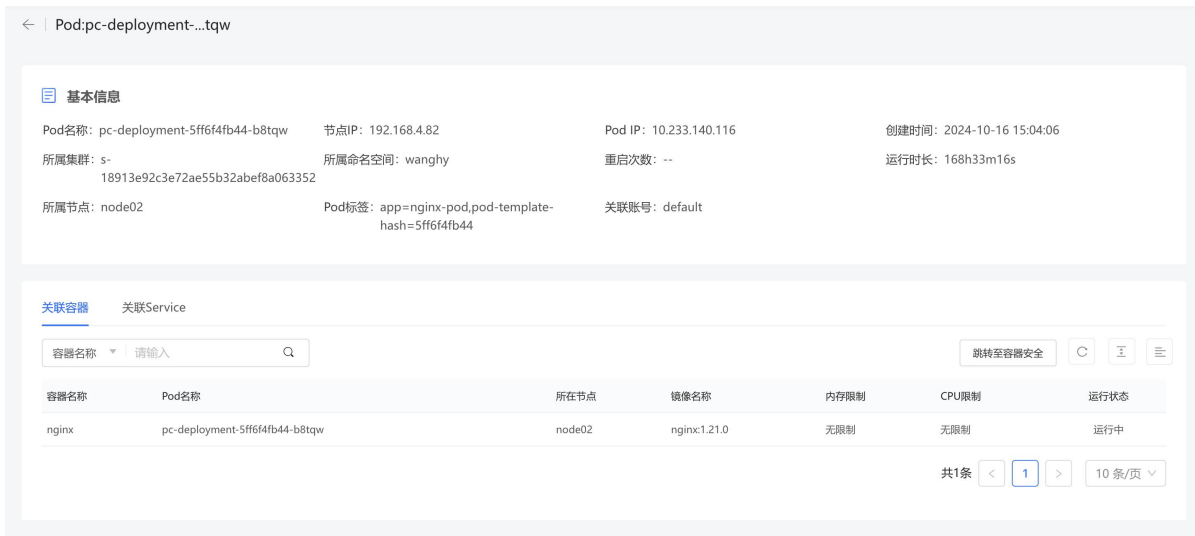
共29条 < 1 2 3 > 10条/页 ▾ 前往 页

参数	解释说明
Pod 名称	Pod 的名称
所属集群	Pod 所属集群的名称

参数	解释说明
所属命名空间	Pod 所属命名空间的名称
重启次数	重启 Pod 的次数。 对于静态 Pod 而言，kubelet 直接监控每个 Pod，并在其失效时重启之。
IP	Pod 的 IP 地址。 每个 Pod 都在每个地址族中获得一个唯一的 IP 地址。Pod 内的容器可以使用 localhost 互相通信。当 Pod 中的容器与 Pod 之外的实体通信时，它们必须协调如何使用共享的网络资源（例如端口）。

4.3.2.4.2. 查看 Pod 详情

1. 查看 Pod 列表；
2. 单击 Pod 列表中的【名称】，进入 Pod 详情页面；



3. 查看基本信息：在详情中的基本信息页面，可查看 Pod 的其他基本信息：节点 IP、运行时长、所属节点和 Pod 标签信息。每个 Pod 都绑定到调度它的节点，并一直保持到终止（根据重启策略）或删除为止。
4. 查看关联容器：在详情中的关联容器页面，可查看该 Pod 关联的容器信息，关联容器表示该 Pod 中包含的容器。
5. 查看关联 Service：在详情中的关联 Service 页面，可查看该 Pod 关联的容器信息，Service 通过标签关联一组 Pod。

4.3.2.5. 容器

4.3.2.5.1. 查看容器列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【容器】，跳转至容器列表。
3. 容器列表页面，支持按照“容器名称”、“镜像名称”、“Pod 名称”、“容器类型”、“学习状态”、“运行状态”、“安全状态”进行筛选查询。

参数	解释说明
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。
命名空间	容器所属命名空间的名称
节点	容器运行所在节点的名称
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
所属集群	该容器所属集群的名称
镜像	关联镜像是指该容器基于哪个镜像构建的
学习状态	学习状态是指根据容器行为模型学习的状态，分为未学习、学习中、学习成功和学习异常这四种类型
运行状态	运行状态分为运行中、停止运行、暂停运行、已删除这四种类型
安全状态	安全状态分为有异常和无异常两种类型，有异常是指触发了安全策略产生告警的容器。

4.3.2.5.2. 查看容器详情

1. 查看容器列表；
2. 单击容器列表中的【名称】，进入容器详情页面；
3. 查看容器信息：在详情中的容器信息页面，可查看容器的详细信息包括基本信息、运行状况、安全状态和学习状态。

参数		解释说明
基本信息	容器 ID	容器的唯一标识 ID
	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。
	运行用户	运行镜像启动容器的用户
	集群	容器所在集群的名称
	镜像	说明该容器是基于哪个镜像构建的
	节点	容器运行所在节点的名称
	Pod 名称	容器所属 Pod 的名称
	节点状态	节点状态分为已连接和未连接状态
	命名空间	容器所属命名空间的名称
	应用类型	容器所提供的应用服务类型，如 kubernetes、apache、nginx 等类型
	节点 IP	容器运行所在节点的 IP 地址
	内存限制	限制该容器占用的内存大小
	CPU 限制	限制该容器占用的 CPU 大小
	容器标签	容器标签用于标记容器，于【网络安全】-【策略管理】中选择策略应用对象时使用
运行状况	容器 IP	容器的 IP 地址
	运行状态	运行状态分为运行中、停止运行、暂停运行、已删除这四种类型
	本次启动时间	最近一次启动的日期和时间
	Pod 重启次数	<p>容器所在 Pod 的重启次数。Pod 的重启策略（RestartPolicy）应用于 Pod 内的所有容器，并且仅在 Pod 所处的 Node 上由 kubelet 进行判断和重启操作。</p> <p>当某个容器异常退出或者健康检查失败时，kubelet 将根据 RestartPolicy 的</p>

		设置来进行相应的操作。
	上次停止时间	最近一次被暂停容器的暂停时间
	隔离状态	隔离状态分为隔离、未隔离、禁止隔离这三种类型。当容器出现异常行为时，可能会采用隔离容器的措施来减少损失。特权容器、节点启动容器、安全容器暂不支持隔离。
	启动进程参数	容器启动时添加的参数
	启动进程路径	容器启动时进程的文件路径
	CPU 占用	容器运行时程序占用的 CPU 资源
	内存占用	容器运行时占用内存资源的情况
安全状态	安全状态	安全状态分为有异常和无异常这两种，有异常是指存在异常告警的容器，这里备注的告警次数为未处理告警的次数，单击有异常(报警次数:X)可跳转至【告警响应】-【运行态检测】中查看告警详情并处理。
	是否为特权启动	特权启动容器是指使用--privileged 标志启动的容器。让 docker 运行在--privileged 特权模式会有一些安全风险。这种模式下运行容器对 docker 宿主主机拥有 root 访问权限，就是说容器可以完成主机可以做的几乎所有事情。存在此标志是为了允许特殊用例，例如在 Docker 中运行 Docker。
学习状态	上次学习时间	根据行为模型学习过的容器的学习时间
	学习策略	进行行为学习时设置的策略

4. 查看应用层漏洞：在详情中的应用层漏洞页面，可以查看容器上运行的应用是否存在漏洞。

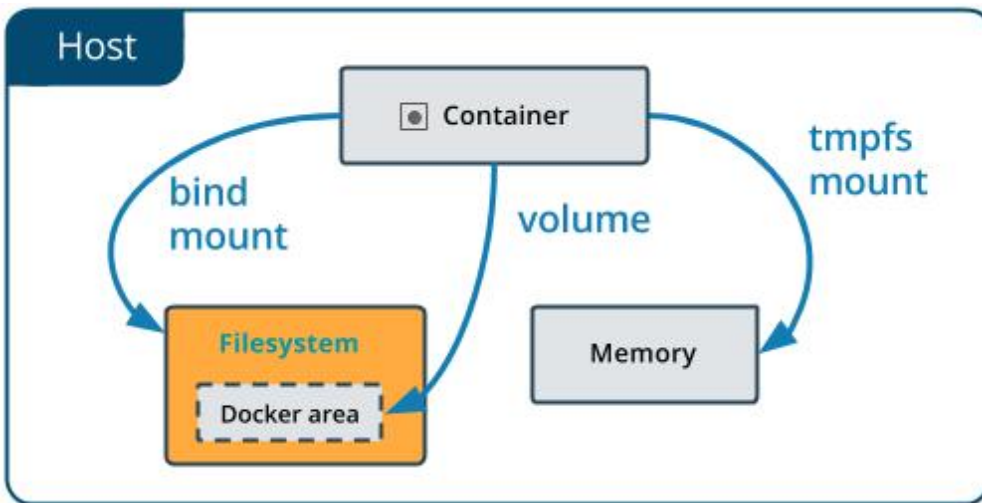
参数	解释说明
漏洞类型	漏洞包括 XSS 漏洞、SQL 注入、命令/代码注入、目录枚举、路径穿越、XML 实体注入、poc、文件上传、弱口令、jsonp、ssrf、基线检查、任意跳转、CRLF 注入等多种类型。
URL	检测出漏洞的所在网址
参数	API 所能够接收的参数类型

参数	解释说明
危险级别	危险级别分为高危、中危和低危这三种类型
测试方法	测试是否存在漏洞的方法

- 查看进程信息：在详情中的进程页面，可以查看容器上运行的进程信息，具体各字段意义详见 6.2.17 查看进程。
- 查看端口信息：在详情中的端口页面，可以查看容器的端口信息，具体各字段意义详见 6.2.18 查看端口。
- 查看数据挂载信息：容器重启或发生故障后，数据将不会持续存在，数据很难从容器中取出，影响用户使用，因此需要额外的存储工具来进行数据挂载，以保存数据信息。把宿主机的某个目录（或文件）挂载到容器的指定目录（或文件）下，比如 mysql 的数据，即使容器意外宕机或者被删除的话，只要数据还在，我们就可以启动一个新的 mysql 容器。

【名词解释-数据挂载】

操作系统中将存储定义为 Volume（卷），这是对物理存储的逻辑抽象，以达到对物理存储提供有弹性的分割方式。另外，将外部存储关联到操作系统的动作定义为 Mount（挂载）。



参数	解释说明
数据卷名	通过采用外接数据卷的方式来保存数据时，定义的数据卷名称
源路径	数据存储路径
目标路径	容器中临时存储数据信息的路径

数据挂载方式	<p>数据挂载分为 Bind、Volume、tmpfs 这三种方式。</p> <p>通过 Bind mount 方式，可以将你主机上的任何文件或目录（绝对路径）挂载到容器中。</p> <p>Volume 方式是 docker 中数据持久化的最佳方式。docker 默认在主机上会有一个特定的区域（/var/lib/docker/volumes），该区域用来存放 Volume。tmpfs 方式仅将数据存储在主机的内存中，不会写入主机的文件系统，使用情况一般是对安全比较重视以及不需要持久化数据。</p>
数据加载方式	<p>数据加载分为读写和只读两种方式：只读方式只支持读操作，读写方式既支持读操作，也支持写操作。</p>

查看网络信息：在详情中的网络页面，可以查看容器网络采用的网络模式等信息。

参数	解释说明
网络模式	<p>docker 主要使用四种网络模式：Bridge、Host、Container 和 None。启动容器时默认是桥接模式，也可以使用 <code>--net</code> 参数指定。</p> <p>Bridge 模式下的容器没有一个公有 ip，只有宿主机可以直接访问，外部主机是不可见的，但容器通过宿主机的 NAT 规则后可以访问外网。</p> <p>Host 模式是 Bridge 桥接模式很好的补充。Host 模式可以让容器共享宿主机网络栈，这样的好处是外部主机与容器直接通信，但是容器的网络缺少隔离性。</p> <p>Container 模式下的 Docker 容器会共享一个网络栈，这样两个容器之间可以使用 localhost 高效快速通信。</p> <p>None 网络模式不为 Docker 容器创建任何的网络环境。一旦 Docker 容器采用了 None 网络模式，那么容器内部就只能使用 loopback 网络设备，不会再有其他的网络资源。不过在这种情况下，Docker 开发者能在这基础做其他无限多可能的网络定制开发。</p>
网络名	网络名称
网络 ID	网络 ID 即网络号
端口 ID	容器网络的端口 ID
网关	<p>网关（Gateway）又称网间连接器、协议转换器，就是一个网络连接到另一个网络的“关口”，也就是网络关卡。</p>

参数	解释说明
IPv4 地址	容器网络的 IPv4 地址
IPv6 地址	容器网络的 IPv6 地址
MAC 地址	容器网络的 MAC 地址，用来确认网络设备位置

查看软件信息：在详情中的软件页面，可以查看容器上运行软件的详细信息。

参数	解释说明
软件名	容器上软件的名称
软件版本	软件的版本号
文件路径	软件的文件存储路径

查看配置信息：在详情中的配置页面，可以查看容器的配置项信息。

参数	解释说明
配置项	容器配置项名称
值	配置值
安全建议	平台针对容器配置提出的安全建议

4.3.2.5.3. 跳转至容器安全

1. 查看容器列表；
2. 单击列表右上方的【跳转至容器安全】按钮。

容器

容器名称 请输入 跳转至容器安全

容器名称	容器类型	命名空间	节点	Pod名称	应用	所属集群	镜像名称	学习状态	运行状态	安全状态
dosec-server		dosec	master	dosec-server-7f5c884796-m5xq8		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	运行中	无异常
dosec-chowner		dosec	master	dosec-server-7f5c884796-m5xq8		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	停止运行	无异常
naughty_noether		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	停止运行	无异常
nervous_swanson		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	停止运行	无异常
calico-kube-contro...		kube-system	master	calico-kube-controllers-6f44679d5b-f...		s-18913e92c3e72ae55b32abef8a0633...	calico/kube...	未学习	运行中	无异常
calico-node		kube-system	master	calico-node-bc6vs		s-18913e92c3e72ae55b32abef8a0633...	calico/node...	未学习	运行中	无异常
youthful_hugle		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	运行中	无异常
happy_goldberg		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	停止运行	无异常
my-registry		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	registry.lat...	未学习	停止运行	无异常
keen_knuth		--	master	--		s-18913e92c3e72ae55b32abef8a0633...	artifactory...	未学习	停止运行	无异常

图标说明: 共100条 1 2 3 4 5 ... 10 10 条/页 前往 页

3. 页面将跳转至【容器安全】-【实时监测】页面，即可查看容器的详细安全信息。

容器名称: naughty_noether

基本信息

容器ID: b8587fadd4572b01d...	容器类型: 节点启动容器	运行用户: --	集群: s-18913e92c3e72ae55b32abe...
镜像: artifactory.dosec....	节点: master	Pod名称: --	节点状态: 已开启
命名空间: --	应用类型: --	节点IPV4地址: 192.168.4.80	节点IPV6地址: --
内存限制: 无限制	CPU限制: 无限制	容器标签: --	容器IPV4: --
容器IPV6: --			

摘要 容器审计 进程 端口 数据挂载 软件 配置

运行情况

运行状态: 停止运行	本次启动时间: 2024-08-19 12:01:26	Pod重启次数: --
上次停止时间: 2024-08-19 12:01:26	隔离状态: 禁止隔离	启动进程参数: /bin/bash
启动进程路径: /dosec/bin/dosec_controll...	CPU占用: --	内存占用: --

安全状态

4.3.2.6. 仓库

4.3.2.6.1. 查看仓库列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【仓库】，跳转至仓库列表。
3. 仓库列表页面，支持按照“仓库名称”、“仓库地址”、“仓库类型”、“是否自动扫描”、“连接状态”进行筛选查询

参数	解释说明
仓库名称	仓库的名称。仓库名称前有红色感叹号表示该仓库中存在漏洞
仓库类型	仓库类型分为 Harbor、JFrog、Huawei、Registry、Aliyun 等多种类型。
仓库地址	仓库的网络地址
是否自动扫描	是否设置了周期自动扫描
连接状态	连接状态分为已连接和未连接

4.3.2.6.2. 查看仓库详情

1. 查看仓库列表；
2. 单击仓库列表中的【仓库名称】，进入仓库详情页面；
3. 在仓库详情页面，可以查看仓库的版本号、登录仓库的用户名、仓库扫描节点等详细信息。

4.3.2.7. 仓库镜像

4.3.2.7.1. 查看仓库镜像列表

1. 登录容器安全管理平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【仓库镜像】，跳转至仓库镜像列表。
3. 仓库镜像列表页面，支持按照“镜像名称”、“版本”、“阻断策略”、“风险等级”、“安全策略”进行筛选查询。



参数	解释说明
镜像名称	镜像的名称
版本	镜像的版本号，可用来区分名称相同的镜像
基础镜像	该镜像是在哪个基础镜像的基础上构建的
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，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、未扫描和安全这几种状态
安全问题	安全问题包括存在漏洞、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、非可信镜像、未知、无安全问题，这些情况
发现时间	第一次更新出该镜像的时间

4.3.2.7.2. 查看仓库镜像详情

1. 查看仓库镜像列表；
2. 单击仓库镜像列表中的【名称】，进入仓库镜像详情页面；
3. 查看镜像安全概览：在详情中的安全概览页面，可查看镜像的详细信息包括风险系数、安全问题、命中的安全策略、基本信息、安全建议和阻断结果。

参数		解释说明
风险说明	风险系数	风险系数包括风险等级和风险的具体评分。
	风险评分项目	风险系数右侧展示了所有的评分项，评分项后面展示扣分值。当镜像未扫描或分数为 100 时，所有扣分项的扣分为 0。扣分项目列表：按漏洞、文件、软件包、环境变量、可信镜像评分项目进行扣分。鼠标移入扣分项目后的问号，可查看该项目最大扣分值的提示信息。 具体扣分规则见【镜像安全】-【设置】-【风险评分】。
安全问题	重点关注漏洞	检测出该镜像存在的重点关注漏洞的数量。 在【镜像安全】-【设置】-【镜像安全策略】的策略编辑页面的【漏洞规

参数		解释说明
		则】中可自定义添加重点关注漏洞。
	自定义异常文件	<p>检测出该镜像存在的自定义异常文件的数量。</p> <p>在【镜像安全】-【设置】-【镜像安全策略】的策略编辑页面的【文件规则】中可自定义添加重点关注漏洞。</p>
	自定义异常软件版本	<p>检测出该镜像存在的自定义异常软件版本的数量。</p> <p>在【镜像安全】-【设置】-【镜像安全策略】的策略编辑页面的【软件包规则】中可自定义添加异常文件。</p>
安全问题	自定义异常环境变量	<p>检测出该镜像存在的自定义异常环境变量的数量。</p> <p>在【镜像安全】-【设置】-【镜像安全策略】的策略编辑页面的【其他规则】中可自定义添加异常文件。</p>
	木马病毒	<p>检测出该镜像存在的木马病毒的数量。木马病毒是指隐藏在正常程序中一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击 Dos 等特殊功能的后门程序。</p>
	风险文件	<p>检测出该镜像存在的风险文件的数量。</p> <p>一般有危险的文件类型如下：</p> <p>exe 文件：可执行文件（可能包含危险代码）</p> <p>com 文件：MS-DOS 可执行文件（可能包含危险代码）</p> <p>pif 文件：指向 com 文件的快捷方式（可能引发病毒）</p> <p>bat 文件：MS-DOS 批处理文件（可能执行对电脑有危害的 cmd 命令）</p> <p>scr 文件：屏幕保护程序（可能包含恶意脚本）</p> <p>如果文件关联被更改了，那么任何文件几乎都可以是病毒。</p>
	不允许授权许可	<p>检测出该镜像出现不允许授权许可软件的数量。</p> <p>在【镜像安全】-【设置】-【镜像安全策略】的策略编辑页面【软件包规则】中可自定义选择不允许的软件许可。</p>
	可信镜像	<p>设置该镜像是否可以信任的镜像。</p> <p>在【镜像安全】-【设置】-【可信镜像】页面中可自定义指定可信任的镜像，并对非信任镜像采取动作。</p>

参数		解释说明
安全策略	镜像命中的安全策略	介绍该镜像命中安全策略的个数，以及命中的安全策略名称 在【镜像安全】-【设置】-【镜像安全策略】页面中可自定义添加、编辑或删除安全策略
基本信息	ImageID	镜像的 ID 编号
	版本	镜像的版本
	大小	镜像文件大小
	入库时间	镜像入仓库的时间
安全建议	漏洞修复建议	对于存在漏洞的镜像，平台将提供漏洞修复建议，请在该镜像的 Dockerfile 文件中添加提示代码，以修复漏洞
	异常文件处理建议	对于存在异常文件的镜像，平台将提供文件处理建议，请确认相关文件是否存在风险，确认后删除异常的文件
阻断结果	阻断结果	镜像是否被阻断处理的结果

4. 查看关联容器：在详情中的关联容器页面，可查看镜像关联的容器信息。

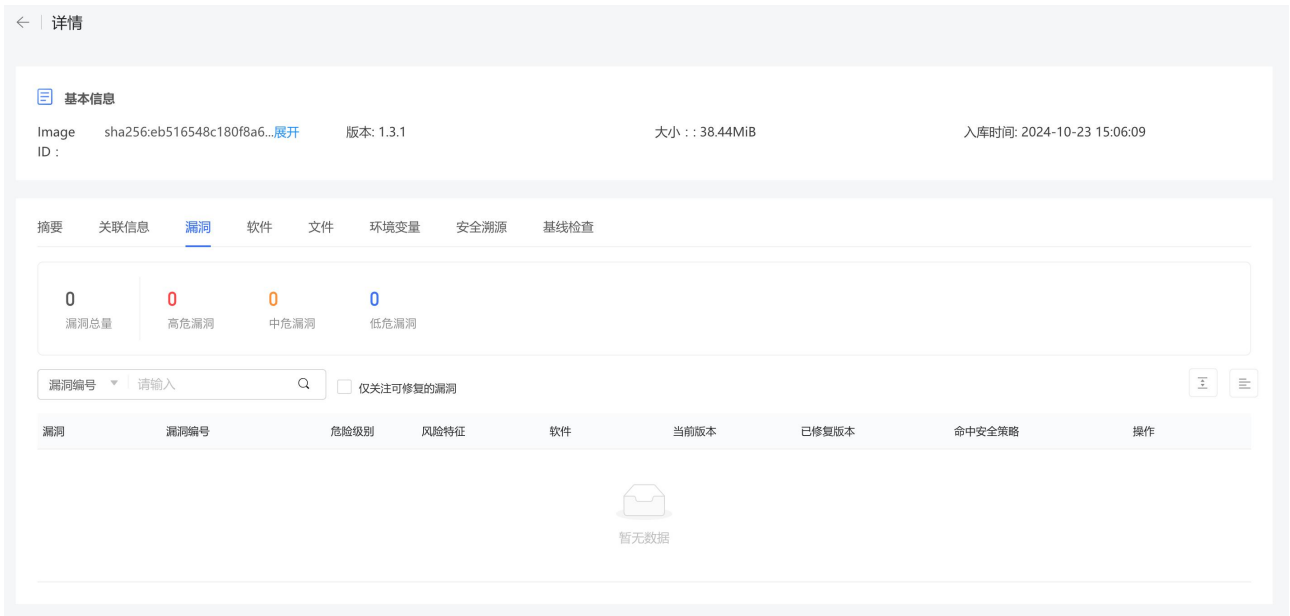
参数	解释说明
容器名称	镜像关联容器的名称
Pod 名称	镜像关联容器所属 Pod 的名称
集群名称	镜像关联容器所属集群的名称
节点名称	镜像关联容器运行所在节点的名称

5. 查看漏洞详情：在详情中的漏洞详情页面，可查看镜像的漏洞统计信息，在下方还可以查看漏洞详情。

参数	解释说明
----	------

参数	解释说明
类型	文件类型，包括软件包和语言包两种类型
漏洞编号	漏洞的编号
危险级别	漏洞的危险等级，包括高、中、低这三种等级
风险特征	风险特征包括重点关注、高分漏洞、有补丁、有 exp、可远程攻击这集中风险特征类型
软件	漏洞所在软件名称
当前版本	当前版本号
已修复版本	漏洞是否存在可修复的版本，如果存在则展示已修复版本号，如果不存在则为空
命中安全策略	镜像中文件包命中的安全策略个数，单击展开可查看策略名称、创建者、规则名称及描述信息
操作	单击操作列中的【加入白名单】，可将该镜像中的漏洞加入白名单

打开【软件-漏洞视角】按钮，能够以镜像中的软件为视角查看该软件上存在的漏洞状态，单击软件名前的“+”号，可以展开查看该软件漏洞信息，又单击漏洞编号前的“+”号，可以展开查看漏洞介绍和参考网址。



6. 查看软件信息：在详情中的软件页面，可查看镜像中软件的详细信息。

参数	解释说明
软件名	镜像中软件的名称
版本	软件版本
文件路径	镜像中软件存放的文件路径
类型	软件包括 Debian 软件包管理器 dpkg、rpm、Android 应用程序包 apk、python、java、ruby、node、二进制文件 binary 等多种类型
命中安全策略	镜像中软件命中的安全策略个数，单击展开可查看策略名称、创建者、规则名称及描述信息
操作	单击操作列中的【加入白名单】，可将该软件加入白名单

7. 查看文件信息：再详情中的文件页面，可以查看镜像中文件的详细信息。

参数	解释说明
文件名	镜像中文件的名称
文件路径	镜像中文件存放的文件路径
类型	文件包括木马病毒、风险文件、自定义异常文件、不允许授权许可软件这几种类型
命中引擎	镜像中文件命中的引擎，分为自研的 YARA 引擎和小红帽引擎，系统默认内置 YARA 引擎。 在【安装配置】-【组件安装】-【防御容器配置】中，单击【开启节点深度扫描】，即开启了小红伞引擎，在深度扫描节点镜像时会同时使用小红伞引擎扫描，但会增大防御容器的内存使用量。
命中安全策略	镜像中文件命中的安全策略个数，单击展开可查看策略名称、创建者、规则名称及描述信息
操作	单击操作列中的【加入白名单】，可将该文件加入白名单； 单击操作列中的【下载】，可将该软件直接下载至本地

8. 查看环境变量：在详情中的安全概览页面，可查看镜像的环境变量信息。

参数	解释说明
变量名	镜像环境变量名称
变量值	镜像环境变量值
命中安全策略	镜像环境变量命中的安全策略（其他规则中）个数，单击展开可查看策略名称、创建者、规则名称及描述信息
操作	单击操作列中的【加入白名单】，可将该环境变量加入白名单

9. 安全溯源：在详情中的安全溯源页面，可查看镜像中的风险信息是在何时引入的。由于镜像是分层构建的，可以通过每一层的构建时间和操作进行溯源。

参数	解释说明
时间	镜像层的构建时间
层 ID	层 ID 编号
命令	写入的命令
引入风险点	可能引入的风险点包括漏洞、软件、文件等多个风险点

10. 查看基线检查：在详情中的基线检查页面，可查看镜像在基线检查时是否通过。

参数	解释说明
基线 ID	基线检查项的 ID 编号，一般为“X.XX”形式
基线检查项类别	基线检查项类别随着基线类型的不同而不同，详见 9.8.不同基线检查项类别
基线检查项	基线检查项的具体描述信息
检查结果	该镜像对应基线检查项的检查结果，分为通过和未通过
操作	单击操作列中的【查看详情】，可以查看检查项的描述信息、检查方法、未通过原因及修复建议等详细信息。

< | 详情

基本信息

Image sha256:eb516548c180f8a6...**展开** 版本: 1.3.1 大小 : : 38.44MiB 入库时间: 2024-10-23 15:06:09

ID :

摘要 关联信息 漏洞 软件 文件 环境变量 安全溯源 **基线检查**

Docker 18.09 CIS 基线检查项名称 请输入 Q C 三 三

基线检查项类别	基线检查项名称	检查结果	类型	动作
容器镜像和构建文件	将 HEALTHCHECK 说明添加到容器镜像	不通过	镜像	查看详情
容器镜像和构建文件	不在 Dockerfile 中单独使用更新命令	通过	镜像	查看详情

共2条 < 1 > 10条/页

4.3.2.8. 节点镜像

4.3.2.8.1. 查看节点镜像列表

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【节点镜像】，跳转至节点镜像列表。

节点镜像列表页面，支持按照“镜像名称”、“版本”、“集群名称”、“节点名称”“阻断策略”、“风险等级”、“安全策略”进行筛选查询。

< | 节点镜像

镜像名称 请输入 Q C 三 三

镜像名称	镜像版本	操作系统	集群名称	节点名称	阻断策略	运行状态	风险等级	安全问题	发现时间
tomcat	8.5.31		s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	中危		2024-10-23 15:06:09
registry.cn-hangzh...	1.3.1	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	1.0	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-01-24T11.47.47V5.2_release_076...	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-01-26T18.46.44V2.0	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-01-26T18.30.17V	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-02-05T11.16.42V	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-02-01T20.57.46V5.1.2_release_b...	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-02-01T23.03.07V5.2.0_release_f3...	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09
artifactory.dosec.c...	2024-02-02T14.28.09V5.1.2_release_d...	--	s-18913e92c3e72ae55b32abef8a0633...	node02	通过	未运行	未扫描		2024-10-23 15:06:09

图标说明:

共337条 < 1 2 3 4 5 ... 34 > 10条/页 前往 页

参数	解释说明
镜像名称	镜像的名称

参数	解释说明
版本	镜像的版本号，可用来区分名称相同的镜像
基础镜像	该镜像是在哪个基础镜像的基础上构建的
集群	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，当镜像存在风险问题时，可以通过阻断来处理风险
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、未运行这几种状态
风险等级	风险等级分为高危、中危、低危、未知、未扫描和安全这些状态
安全问题	安全问题包括存在漏洞、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、非可信镜像、未知、无安全问题，这些情况
发现时间	第一次更新出该镜像的时间

4.3.2.8.2. 查看节点镜像详情

1. 查看节点镜像列表；
2. 单击节点镜像列表中的【名称】，进入节点镜像详情页面；
3. 在镜像详情页面，可查看镜像安全概览、关联信息、漏洞详情、软件、文件、环境变量、安全溯源及基线检查信息。

< 详情

基本信息

Image sha256:e7429d8429dcf670...[展开](#) 版本: 1.0 大小: 271.7MiB 入库时间: 2024-10-23 15:06:09

ID:

摘要 关联信息 漏洞 软件 文件 环境变量 安全溯源 基线检查

风险评分

未知

漏洞	0
文件	0
软件包	0
环境变量	0
可信镜像	0

安全问题

重点关注漏洞	0	自定义异常文件	0	自定义异常软...	0	自定义异常环...	0	木马病毒	0	风险文件	0	不允许的软件...	0	可信镜像	是
--------	---	---------	---	-----------	---	-----------	---	------	---	------	---	-----------	---	------	---

4.3.2.9. 软件包

4.3.2.9.1. 查看软件包列表

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【软件包】，跳转至软件包列表。
软件包列表页面，支持按照“软件包名称”、“版本”进行筛选查询。

< 软件包

软件包名称 请输入

[跳转到镜像安全](#)

软件包名称	版本	关联镜像
	3.4-1build4	1
cronie-anacron	1.4.11	15
fontconfig	2.11.0-6.7+b1	1
libsmartcols1	2.33.1-0.1	5
libcurl4	7.74.0-1.3+deb11u1	4
diffutils	1.3.7-3	5
libudev1	241-7~deb10u4	4
libpython3-stdlib	3.9.2-3	2
libldap-common	2.4.44+dfsg-5+deb9u2	1
perl-libs	5.16.3	16

共1478条 < 1 2 3 4 5 ... 148 > 10条/页 前往 页

参数	解释说明
-----------	-------------

参数	解释说明
软件包名称	软件包的名称
版本	软件包的版本号，用来区分名称相同的软件包
关联镜像	该软件包关联镜像的个数

4.3.2.9.2. 查看软件包详情

1. 查看软件包列表；
2. 单击软件包列表中的【软件包名称】，进入详情页面。在软件包详情页面，可查看软件包关联镜像的详细信息，包括镜像名称、镜像版本、基础镜像、所在节点名称、集群名称、文件路径、类型及发现时间。

← 软件包: cronie-anacron

关联镜像

镜像名称	版本	操作系统	节点/仓库名称	集群名称	文件路径	类型	发现时间
artifactory.dosec.cn/newtest/test_ima...	2.11.0		node02	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
harbor.dosec.cn/newtest/test_images	2.11.0		node02	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
192.168.4.179/newtest/test_images	2.11.0		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
artifactory.dosec.cn/newtest/test_ima...	2.11.0		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	1		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	10		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	2		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	3		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	4		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23
aaa	5		master	s-18913e92c3e72ae55b32abef8a0633...	--	rpm	2024-10-23

图标说明: ⓘ

共15条 < 1 2 > 10条/页 前往 页

4.3.2.9.3. 跳转至镜像安全

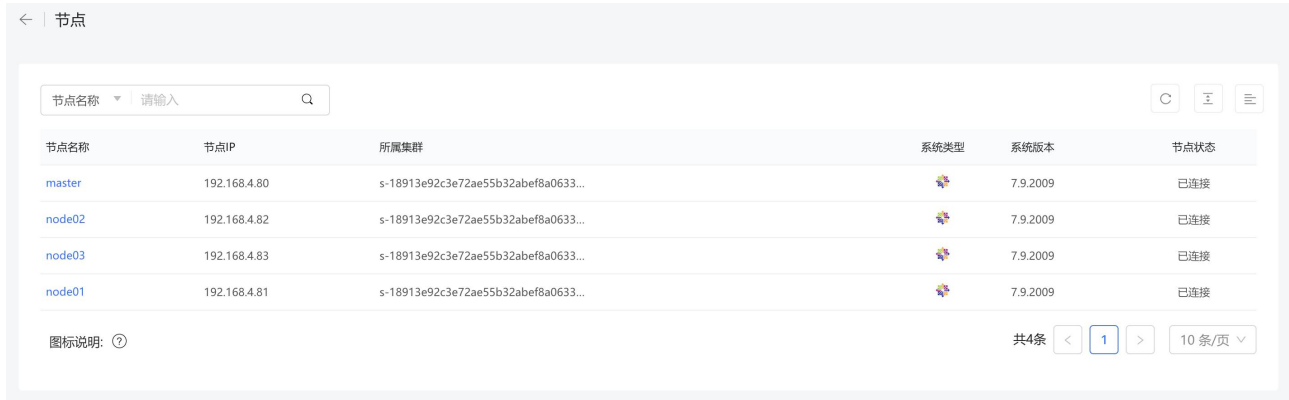
1. 查看软件包列表；
2. 单击列表右上方的【跳转至镜像安全】按钮。
3. 页面将跳转至【镜像安全】页面，即可查看镜像的详细安全信息。以镜像为视角，查看镜像中软件是否命中安全策略。

4.3.2.10. 节点

4.3.2.10.1. 查看节点列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【节点】，跳转至节点列表。

节点列表页面，支持按照“节点名称”、“集群名称”、“IP 地址”、“节点状态”进行筛选查询。



参数	解释说明
节点名称	节点的名称
IP	节点的 IP 地址
所属集群	节点所在集群的名称
系统类型	节点使用的操作系统类型
Docker 版本	节点使用的 Docker 容器版本
节点状态	节点状态指的是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

4.3.2.10.2. 查看节点详情

1. 查看节点列表；
2. 单击节点列表中的【节点名称】，进入详情页面；

← 节点名称: master

基本信息

系统类型: CentOS Linux	系统版本: 7.9.2009	操作系统: Linux
CPU架构: x86_64	内核版本: 5.4.262-1.el7.elrepo.x86_64	OSUUID: d64321a8-cad2-3632...
CPU占用: 645.49m	内存占用: 4.01GB	磁盘占用率: 50.92%

摘要 漏洞 软件 基线检查

集群组件信息

高级别运行时: Docker	高级别运行时版本: 19.03.9	运行时API版本: 1.40	低级别运行时: runc
镜像存储驱动: overlay2	容器存储根目录: /var/lib/docker		

防御容器健康状态

版本: 5.2.0	在线状态: 在线	病毒库版本: 2024042406	恶意文件规则版本: 2024050911
小红伞版本: 2024042406	入侵检测版本: 2024022216		

3. 查看基本信息：在节点详情页面，可查看节点的其他详细信息。

参数		解释说明
节点信息	系统类型	节点使用的操作系统类型
	系统版本	节点使用的操作系统版本
	操作系统	节点操作系统，主要为 Linux 操作系统
	CPU 架构	目前有两大主流的 CPU 架构：X86、ARM。X86 架构使用的是 CISC 复杂指令集。ARM 架构采用了 RISC 精简指令集，架构上非常灵活，可以根据面向应用场景不同使用不同设计的内核，具有低成本、高性能和低耗电的特性。
	内核版本	操作系统内核版本
	OSUUID	操作系统的通用唯一识别码 (Universally Unique Identifier, UUID)
	CPU 占用	节点运行程序占用的 CPU 资源
	内存占用	节点占用内存资源的情况
	磁盘占用率	Docker 安装目录下，磁盘占用空间与全部可用空间的百分比
集群组件信息	Docker 版本	节点使用的 Docker 容器版本号
	Docker API 版本	节点上 Docker 容器的 API 版本号

参数		解释说明
	容器运行时	容器运行时使用的命令，如-runc
	镜像存储驱动	docker 提供了多种存储驱动来实现不同的方式存储镜像，常用的几种存储驱动：AUFS、OverlayFS、Devicemapper、Btrfs、ZFS。其中 Overlay 性能相对要强。Overlay 是一种 Union FS，但只有两层：一个 upper 文件系统和一个 lower 文件系统，分别代表 Docker 的镜像层和容器层。当需要修改一个文件时，使用 CoW 将文件从只读的 lower 复制到可写的 upper 进行修改，结果也保存在 upper 层。在 Docker 中，底下的只读层就是 image，可写层就是 Container。目前最新的 OverlayFS 为 Overlay2。
	Docker 根目录	Docker 的根目录
防御容器健康状态	版本	节点上防御容器的版本
	在线状态	防御容器的在线状态
	YARA 规则库版本	防御容器扫描使用的 YARA 规则库版本
	病毒库版本	防御容器扫描病毒使用的病毒库版本

4. 查看软件漏洞：在节点详情中的软件漏洞页面，可查看节点上软件存在的漏洞统计情况，及下方列表中节点上存在的漏洞详情（各字段意义见 7.1.7.2 查看仓库镜像详情中漏洞详情）。

< | 节点名称: master

基本信息

系统类型: CentOS Linux

CPU架构: x86_64

CPU占用: 645.49m

系统版本: 7.9.2009

内核版本: 5.4.262-1.el7.elrepo.x86_64

内存占用: 4.01GB

操作系统: Linux

OSUID: d64321a8-cad2-3632...

磁盘占用率: 50.92%

摘要
漏洞
软件
基线检查


0
漏洞总量

0
高危漏洞

0
中危漏洞

0
低危漏洞

|

漏洞编号	关联漏洞	类型	危险级别	风险特征	软件	当前版本	已修复版本
 暂无数据							

- 查看基线检查结果：在节点详情中的基线检查页面，可查看节点对应的基线检查项及检查结果。单击操作列表中的【查看详情】按钮，可以查看相应检查项的描述信息、检查方法、未通过原因、修复建议、参考地址。

基本信息

系统类型: CentOS Linux
CPU架构: x86_64
CPU占用: 645.49m

系统版本: 7.9.2009
内核版本: 5.4.262-1.el7.elrepo.x86_64
内存占用: 4.01GB

操作系统: Linux
OSUID: d64321a8-cad2-3632...

摘要 漏洞 软件 **基线检查**

CentOS 7 CIS

基线检查项名称

基线检查项类别	基线检查项名称	检查结果	类型	动作
初始设置	确保/var/tmp分区包含nosuid选项	● 不通过	节点	查看详情
初始设置	确保在/dev/shm分区上设置noexec选项	● 不通过	节点	查看详情
初始设置	确保在/dev/shm分区上设置nosuid选项	● 通过	节点	查看详情
服务	确保IMAP和POP3服务器未安装	● 通过	节点	查看详情
日志与审计	确保已安装 auditd	● 通过	节点	查看详情
日志与审计	确保安装了 rsyslog	● 通过	节点	查看详情
访问、认证和授权	确保配置了SSHMax启动程序	● 不通过	节点	查看详情
访问、认证和授权	确保配置 SSH 公共主机密钥文件的权限	● 通过	节点	查看详情

4.3.2.11. 进程

4.3.2.11.1. 查看进程列表

- 登录容器安全平台管理界面；
- 选择【资产中心】-【全部资产】，单击【进程】，跳转至进程列表。

进程列表页面，支持按照“容器名称”、“进程名称”、“进程 PID”进行筛选查询。

← 进程

进程名称

进程名称	进程PID	父进程PID	所属集群	所在节点	容器名称	更新时间
bash	78310	78293	s-18913e92c3e72ae55b32abef8a0633...	master	priceless_wing	2024-10-25 14:58:41
pause	105563	105534	s-18913e92c3e72ae55b32abef8a0633...	master	POD	2024-10-25 14:58:41
sleep	63272	62041	s-18913e92c3e72ae55b32abef8a0633...	master	friendly_kare	2024-10-25 14:58:41
bash	62041	61354	s-18913e92c3e72ae55b32abef8a0633...	master	friendly_kare	2024-10-25 14:58:41
bash	61354	50260	s-18913e92c3e72ae55b32abef8a0633...	master	friendly_kare	2024-10-25 14:58:41
bash	50260	50146	s-18913e92c3e72ae55b32abef8a0633...	master	friendly_kare	2024-10-25 14:58:41
boot	50146	50051	s-18913e92c3e72ae55b32abef8a0633...	master	friendly_kare	2024-10-25 14:58:41
doberman	63421	63152	s-18913e92c3e72ae55b32abef8a0633...	master	dosec-agent	2024-10-25 14:58:41
dosec_hades	63152	54577	s-18913e92c3e72ae55b32abef8a0633...	master	dosec-agent	2024-10-25 14:58:41
dosec_hades	54577	54567	s-18913e92c3e72ae55b32abef8a0633...	master	dosec-agent	2024-10-25 14:58:41

共180条 ... 页

4.3.2.11.2. 查看进程详情

1. 查看进程列表；
2. 单击进程列表中的【进程名称】，进入详情页面；
3. 在进程详情页面，可查看进程的其他详细信息，包括节点名称、节点 IP 和进程 TTY 等。



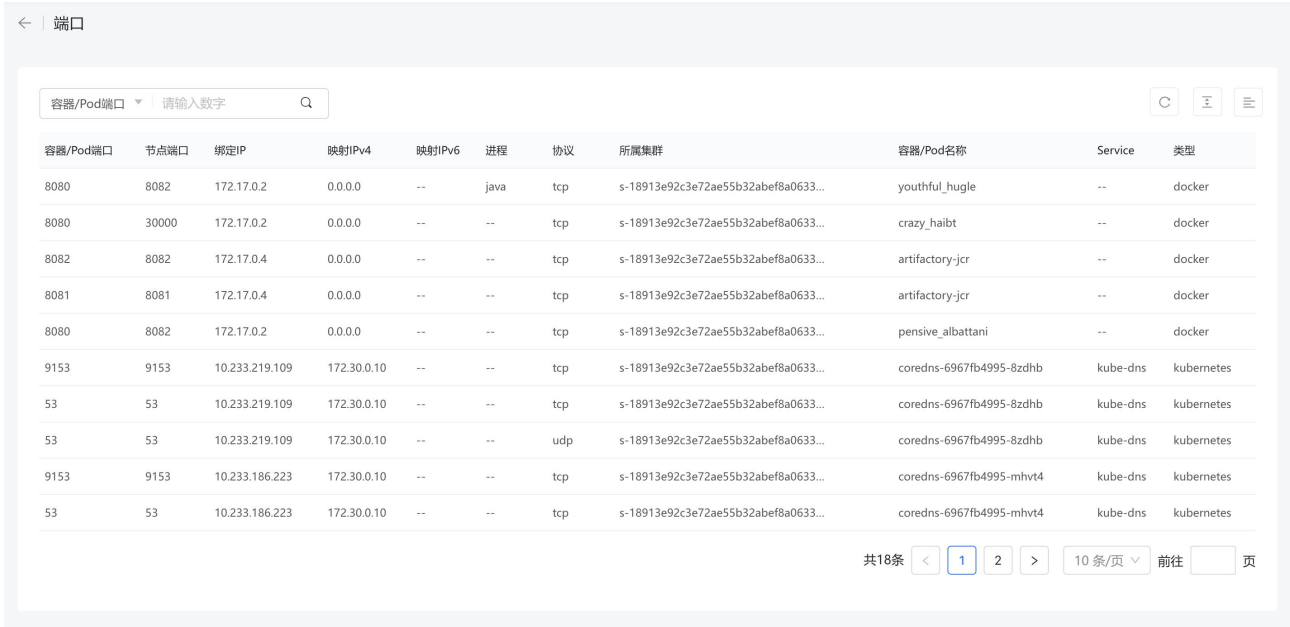
参数	解释说明
进程名	进程的名称
进程 PID	本进程的编号 PID，作为进程的唯一标识
容器名称	进程所属容器的名称
容器名称	进程所属容器的 ID 编号
父进程 PID	父进程的进程编号 PID，也被称为 PPID
节点 ID	进程运行所在节点的 ID
节点名称	进程运行所在节点的名称
进程 TTY	TTY 是“Teletype”的简写，进程 TTY 是指进程的控制终端

4.3.2.12. 端口

4.3.2.12.1. 查看端口列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【端口】，跳转至端口列表。

端口列表页面，支持按照“容器/Pod 名称”、“容器/Pod 端口”、“进程”、“节点端口”、“映射 IPv4”、“映射 IPv6”、“绑定 IP”、“所属集群”、“Service”、“协议”、“类型”进行筛选查询。



容器/Pod端口	节点端口	绑定IP	映射IPv4	映射IPv6	进程	协议	所属集群	容器/Pod名称	Service	类型
8080	8082	172.17.0.2	0.0.0.0	--	java	tcp	s-18913e92c3e72ae55b32abef8a0633...	youthful_hugle	--	docker
8080	30000	172.17.0.2	0.0.0.0	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	crazy_haibt	--	docker
8082	8082	172.17.0.4	0.0.0.0	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	artifactory-jcr	--	docker
8081	8081	172.17.0.4	0.0.0.0	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	artifactory-jcr	--	docker
8080	8082	172.17.0.2	0.0.0.0	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	pensive_albattani	--	docker
9153	9153	10.233.219.109	172.30.0.10	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	coredns-6967fb4995-8zdhb	kube-dns	kubernetes
53	53	10.233.219.109	172.30.0.10	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	coredns-6967fb4995-8zdhb	kube-dns	kubernetes
53	53	10.233.219.109	172.30.0.10	--	--	udp	s-18913e92c3e72ae55b32abef8a0633...	coredns-6967fb4995-8zdhb	kube-dns	kubernetes
9153	9153	10.233.186.223	172.30.0.10	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	coredns-6967fb4995-mhvt4	kube-dns	kubernetes
53	53	10.233.186.223	172.30.0.10	--	--	tcp	s-18913e92c3e72ae55b32abef8a0633...	coredns-6967fb4995-mhvt4	kube-dns	kubernetes

参数	解释说明
容器/Pod 端口	容器或 Pod 开放的端口号
节点端口	容器或 Pod 所在节点的端口
绑定 IP	容器内部网卡的 IP 地址
映射 IPv4	节点的 IPv4 地址
映射 IPv6	节点的 IPv6 地址
进程	容器或 Pod 上运行的进程
协议	<p>端口采用的协议，根据协议类型可分为 TCP 端口和 UDP 端口。</p> <p>TCP：全称 Transmission Control Protocol 传输控制协议，是一种面向连接的、可靠的、基于字节流的传输层（Transport layer）通信协议。在简化的计算机网络 OSI 模型中，它完成第四层传输层所指定的功能，UDP 是同一层内另一个重要的传输协议。</p> <p>UDP：全称 User Datagram Protocol 用户数据报协议，是 OSI 参考模型中一种无连</p>

	接的传输层协议，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是 IP 协议与上层协议的接口。UDP 协议适用端口分别运行在同一台设备上的多个应用程序。
所属集群	容器或 Pod 所属集群的名称
容器/Pod 名称	容器或 Pod 的名称
Service	关联 Service 的名称
类型	分为 kubernetes 和 docker

4.3.2.13. Ingress

4.3.2.13.1. 查看 Ingress 列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【Ingress】，跳转至 Ingress 列表。

Ingress 列表页面，支持按照 “Ingress 名称”、“所属命名空间” 进行筛选查询。

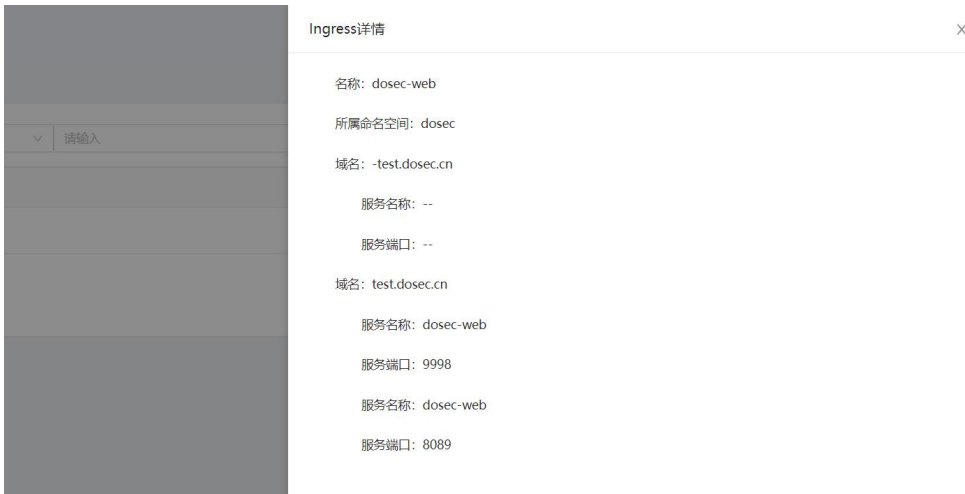


参数	解释说明
Ingress 名称	Ingress 的名称
所属命名空间	Ingress 所属命名空间的名称

4.3.2.13.2. 查看 Ingress 详情

1. 查看 Ingress 列表；

- 单击 Ingress 列表中的【Ingress 名称】，进入详情页面。在 Ingress 详情页面，可查看 Ingress 的其他详细信息，包括域名、服务名称和服务端口。



参数	解释说明
Ingress 名称	Ingress 的名称
所属命名空间	Ingress 所属命名空间的名称
域名	域名用于对外暴露服务，从而实现从外部对 k8s 集群中服务的访问
服务名称	不同域名对应后端服务 Service 的名称
服务端口	用于对外服务的 Service 端口号

4.3.2.14. Service

4.3.2.14.1. 查看 Service 列表

- 登录容器安全平台管理界面；
- 选择【资产中心】-【全部资产】，单击【Service】，跳转至 Service 列表。

Service 列表页面，支持按照“应用名称”、“所属命名空间”、“端口”进行筛选查询。

← | Service

Service名称 请输入

Service名称	所属集群	命名空间	类型	ClusterIP	端口
	s-18913e92c3e72ae55b32abef8a0633...	test2	NodePort	172.30.242.96	80:30922/TCP
	s-18913e92c3e72ae55b32abef8a0633...	test2	NodePort	172.30.61.120	80:30003/TCP
dsww2-svc	s-18913e92c3e72ae55b32abef8a0633...	test2	NodePort	172.30.237.9	80:30268/TCP
kube-dns	s-18913e92c3e72ae55b32abef8a0633...	kube-system	ClusterIP	172.30.0.10	53/UDP53/TCP9153/TCP
dosec-wsde	s-18913e92c3e72ae55b32abef8a0633...	dosec	NodePort	172.30.67.137	30666:30666/TCP
dosec-webhook-b...	s-18913e92c3e72ae55b32abef8a0633...	dosec	NodePort	172.30.129.10	1236:31236/TCP
dosec-server	s-18913e92c3e72ae55b32abef8a0633...	dosec	NodePort	172.30.210.219	1234:31234/TCP:30078:30078/TCP
kubernetes	s-18913e92c3e72ae55b32abef8a0633...	default	ClusterIP	172.30.0.1	443/TCP

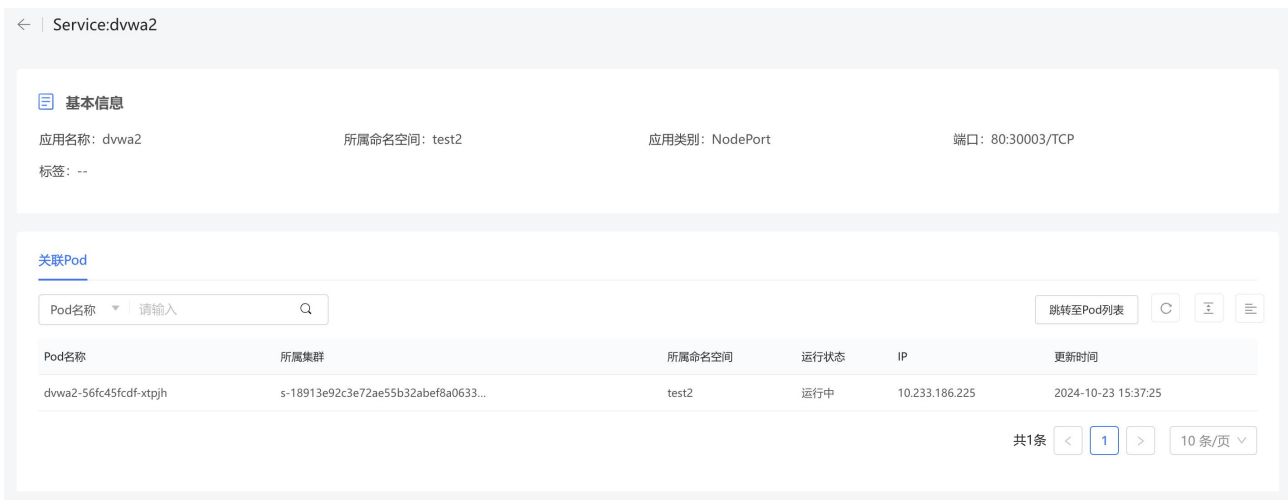
共8条 < 1 > 10条/页

参数	解释说明
Service 名称	Service 的名称
所属命名空间	Service 所属命名空间的名称
类型	<p>K8s 中 Service 主要包含以下四种类型：ClusterIP、NodePort、LoadBalance、ExternalName。</p> <p>ClusterIP 为默认类型，每个 Node 分配一个集群内部的 IP，内部可以互相访问，外部无法访问集群内部。</p> <p>NodePort 通过每个节点上的 IP 和静态端口（NodePort）暴露服务。NodePort 服务会路由到自动创建的 ClusterIP 服务。通过请求 <节点 IP-节点端口>，你可以从集群的外部访问一个 NodePort 服务。</p> <p>LoadBalancer：使用云提供商的负载均衡器向外部暴露服务。外部负载均衡器可以将流量路由到自动创建的 NodePort 服务和 ClusterIP 服务上。</p> <p>ExternalName：通过返回 CNAME 和对应值，可以将服务映射到 externalName 字段的内容（例如 foo.bar.example.com）。无需 创建任何类型代理。类型为 ExternalName 的服务将服务映射到 DNS 名称，而不是典型的选择器。你可以使用 spec.externalName 参数指定这些服务。</p>
ClusterIP	Service 的 ClusterIP 地址。有时不需要负载均衡，以及单独的 Service IP，这种情况下可以通过指定 Cluster IP（spec.clusterIP）的值为 "None" 来创建 Headless Service。

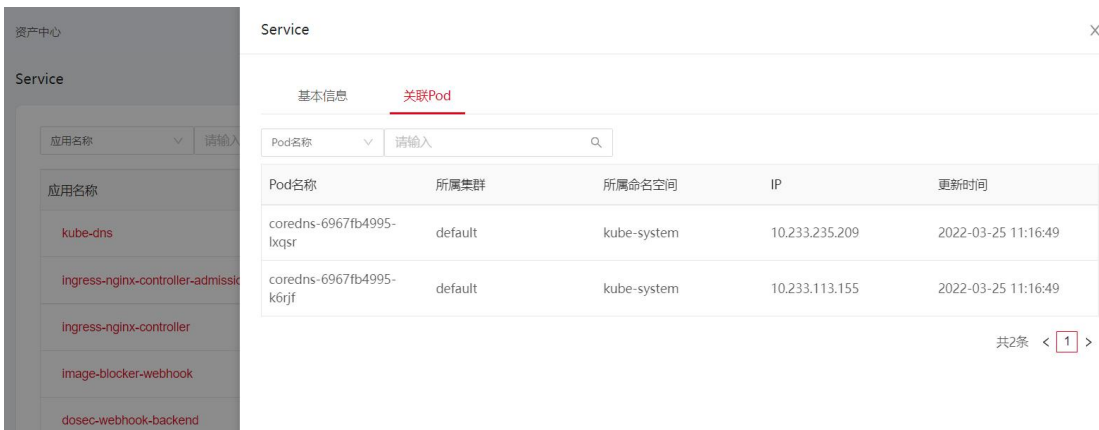
参数	解释说明
端口	节点 Node 暴露的端口号和采用的协议（如 UDP 协议、TCP 协议）

4.3.2.14.2. 查看 Service 详情

1. 查看 Service 列表；
2. 单击 Service 列表中的【Service 名称】，进入详情页面。
3. 在基本信息页面，可查看 Service 的其他详细信息如标签，被 Service 用来匹配 Pod。



4. 在关联 Pod 页面，可查看 Service 所关联 Pod 的信息，一个 Service 可能对应多个 Pod，并可以跳转至 Pod 列表。

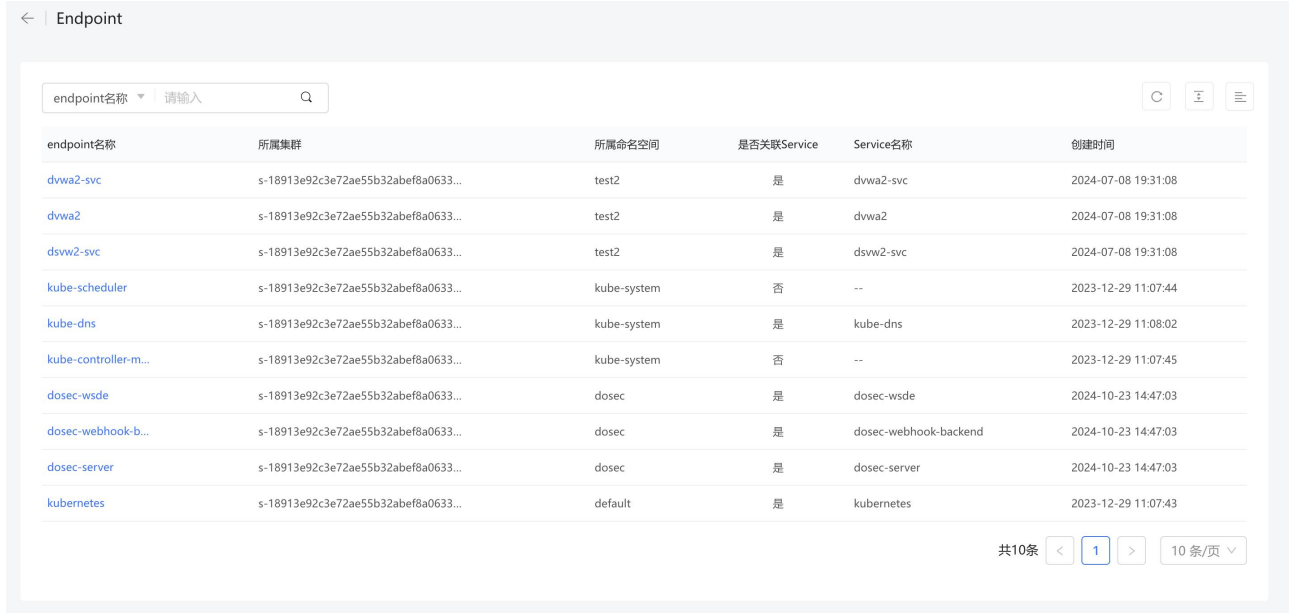


4.3.2.15. Endpoint

4.3.2.15.1. 查看 Endpoint 列表

1. 登录容器安全平台管理界面；

2. 选择【资产中心】-【全部资产】，单击【Endpoint】，跳转至 Endpoint 列表。
3. Endpoint 列表页面，支持按照“名称”、“所属集群”、“所属命名空间”、“关联 Service”进行筛选查询。



endpoint名称	所属集群	所属命名空间	是否关联Service	Service名称	创建时间
dvwa2-svc	s-18913e92c3e72ae55b32abef8a0633...	test2	是	dvwa2-svc	2024-07-08 19:31:08
dvwa2	s-18913e92c3e72ae55b32abef8a0633...	test2	是	dvwa2	2024-07-08 19:31:08
dsvw2-svc	s-18913e92c3e72ae55b32abef8a0633...	test2	是	dsvw2-svc	2024-07-08 19:31:08
kube-scheduler	s-18913e92c3e72ae55b32abef8a0633...	kube-system	否	--	2023-12-29 11:07:44
kube-dns	s-18913e92c3e72ae55b32abef8a0633...	kube-system	是	kube-dns	2023-12-29 11:08:02
kube-controller-m...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	否	--	2023-12-29 11:07:45
dosec-wsde	s-18913e92c3e72ae55b32abef8a0633...	dosec	是	dosec-wsde	2024-10-23 14:47:03
dosec-webhook-b...	s-18913e92c3e72ae55b32abef8a0633...	dosec	是	dosec-webhook-backend	2024-10-23 14:47:03
dosec-server	s-18913e92c3e72ae55b32abef8a0633...	dosec	是	dosec-server	2024-10-23 14:47:03
kubernetes	s-18913e92c3e72ae55b32abef8a0633...	default	是	kubernetes	2023-12-29 11:07:43

参数	解释说明
名称	Endpoint 的名称
所属命名空间	Endpoint 所属命名空间的名称
所属集群	Endpoint 所属集群的名称
是否关联 Service	该 Endpoint 是否关联了服务 Service
服务名称	如果关联了 Service，则显示服务 Service 的名称；否则为空
创建时间	Endpoint 的创建时间

4.3.2.15.2. Endpoint 信息

1. 查看 Endpoint 列表；
2. 单击【Endpoint 名称】，跳转至 Endpoint 详情，可查看 Endpoint 基本信息

Endpoint: dvwa2-svc

基本信息

endpoint名称: dvwa2-svc 所属集群: s-18913e92c3e72ae55b32abef8a063352 所属命名空间: test2 Service名称: dvwa2-svc

创建时间: 2024-07-08 19:31:08 IP: 10.233.186.225 端口: 80/TCP 标签: --

4.3.2.16. 运行应用

4.3.2.16.1. 查看运行应用列表

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【运行应用】，跳转至运行应用列表。

运行应用列表页面，支持按照“容器名称”、“应用类别”、“应用名称”、“运行用户”进行筛选查询。

运行应用

容器名称 请输入

容器名称	应用类别	应用名称	版本号	运行用户	程序路径	配置文件
youthful_hugle	web服务	tomcat	10.0.14	root	/usr/local/openjdk-11/bin/java	/usr/local/tomcat/conf/server.xml
etcd	中间件	etcd	3.3.1	root	/usr/local/bin/etcd	/opt/bitnami/etcd/conf
sweet_diffie	数据库	postgres	2024-0	root	/usr/local/bin/postgres	/etc/postgresql
nginx	web服务	nginx	1.21.0	root	/usr/sbin/nginx	/etc/nginx/nginx.conf
beautiful_moore	web服务	nginx	1.21.5	root	/usr/sbin/nginx	/etc/nginx/nginx.conf

共5条 < 1 > 10条/页

参数	解释说明
容器名称	运行应用所在的容器
应用类别	应用的类别，包括 web 服务、数据库、中间件和监控这四种类型
应用名称	应用的名称
版本号	应用的版本号
运行用户	运行该应用的用户
程序路径	运行程序所在路径
配置文件	应用配置文件的路径（可能存在多个配置文件，这里仅列主配置文件）

4.3.2.16.2. 查看运行应用详情

1. 查看运行应用列表；
2. 单击运行应用列表中的【容器名称】，进入详情页面。
3. 在运行应用详情中的基本信息页面，可查看运行应用的其他详细信息；
4. 在详情中的关联进程页面，可查看容器运行了多少个进程，进程的名称以及节点 PID；

参数	解释说明
主进程 PID	应用中运行的主进程的进程编号 PID
所属用户组	运行应用的用户所属用户组
日志路径	应用的日志存储路径

运行应用:tomcat

基本信息

应用名称: tomcat 版本: 10.0.14 主进程PID: 15109 启动用户: root
 所属用户组: root 程序路径: /usr/local/openjdk-11/bin/java 配置文件路径: /usr/local/tomcat/conf/server.xml 日志路径: /var/lib/docker/containers/df1cd3866d0d7d38cc8f8cec07f34eee63b705199ed9a2c2c663ee0233681275/df1cd3866d0d7d38cc8f8cec07f34eee63b705199ed9a2c2c663ee0233681275-json.log

关联进程 关联端口

进程名称

进程名称	节点PID
java	15109

共1条 10条/页

5. 在详情中的关联端口页面，可查看容器对外服务的端口信息。

关联进程 **关联端口**

容器端口

容器端口	进程	IPv4	IPv6	绑定IP	协议
8080	java	0.0.0.0	--	172.17.0.2	tcp

共1条 10条/页

4.3.2.17. 软件框架

4.3.2.17.1. 查看软件框架列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【软件框架】，跳转至软件框架列表。

软件框架列表页面，支持按照“容器名称”、“框架类别”、“应用名称”、“框架语言”、“框架名称”进行筛选查询。



参数	解释说明
容器名称	运行软件框架的容器名称
框架类别	软件框架的类别，如 web
应用名称	软件框架对应的应用名称，如 tomcat
框架语言	软件框架编写语言，如 java 语言
框架名称	框架的名称
版本号	软件框架的版本号
框架路径	软件框架所在路径
节点 IP	软件框架运行所在节点的 IP 地址

4.3.2.18. web 站点

4.3.2.18.1. 查看 Web 站点列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【Web 站点】，跳转至 Web 站点列表。

Web 站点列表页面，支持按照“应用名称”、“容器名称”、“域名”进行筛选查询。



参数	解释说明
容器名称	站点上挂载的容器名称
域名	站点上挂载的域名（通过解析配置文件获取）
应用名称	容器上运行应用名称
启动用户	启动容器的用户
主目录	Web 站点映射的主目录（容器内部）
所有者权限	<p>第一个字符代表文件类型。[d]-目录、[-]-文件、[l]-链接、[b]-可储存周边设备、[c]-序列设备、[s]-套接字。</p> <p>接下来每三个字符为一组权限，分为三组，依次代表所有者权限，同组用户权限，其它用户权限。</p> <p>每组权限的三个字符依次代表是否可读，是否可写，是否可执行，[r]-可读、[w]-可写、[x]-可执行、[-]-相应的权限还没有被授予。例如，所有者权限为 drwxr-xr-x，解读如下：</p> <p>第一组 rwx：表示拥有人（user）所有者的权限（这里 rwx:代表拥有者有可读，可写，可执行的权限）；</p> <p>第二组 r-x：表示同组群（group）使用者权限（这里 r-x 代表同组群使用者有可读，可执行权限）；</p> <p>第三组 r-x：表示其他（other）使用者权限（这里 r-x 代表其他使用者有可读，可执行权限）。</p>

4.3.2.18.2. 查看 Web 站点详情

1. 查看 Web 站点列表;
2. 单击 Web 站点列表中的【容器名称】，进入详情页面;
3. 在 Web 站点详情中的基本信息页面，可查看 Web 站点的目录信息。

参数	解释说明
域名	站点上挂载的域名
应用名称	容器上运行应用的名称
绑定 IP	Web 站点绑定的 IP 地址
协议	WEB 服务器提供各种网络服务的协议类型，主要为 HTTP 协议。HTTP 协议 (HyperText Transfer Protocol, 超文本传输协议) 是用于从 Web 服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示 (如文本先于图形) 等。
容器端口	容器对外开放的端口
节点端口	容器所在节点的端口
主目录	挂载的主目录地址
主目录持有者	主目录的持有者


← | 网站.youthful_hugle

基本信息

域名: localhost	应用名称: tomcat	绑定IP: 192.168.4.80	协议: http
用户: root	容器端口: 8080	节点端口: 8082	主目录: /usr/local/tomcat
主目录持有者: root	所有者权限: drwxr-xr-x		

目录信息

虚拟路径 C E 三

虚拟路径	物理路径	文件所有者	文件权限
 暂无数据			

参数	解释说明
虚拟路径	虚拟目录是网站的访问路径
物理路径	web 站点的目录指的是网站的物理目录，就是真实目录
文件所有者	目录文件的所有者

4.3.2.19. Routes

4.3.2.19.1. 查看 Routes 列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【Routes】，跳转至 Routes 列表。

Routes 列表页面，支持按照“名称”、“所属命名空间”模糊查询，按照“所属集群”、“状态”定向筛选。

参数	解释说明
名称	Routes 名称
所属集群	Routes 所属集群的名称
所属命名空间	Routes 所属命名空间的名称
状态	状态包括允许 (Accepted)、拒绝 (Rejected)、待定 (Pending) 这三种状态。
URL	Routes 映射控制的 URL 地址
关联 Service	Routes 关联 Service 的名称
创建时间	Routes 被创建的时间



4.3.2.19.2. 查看 Routes 详情

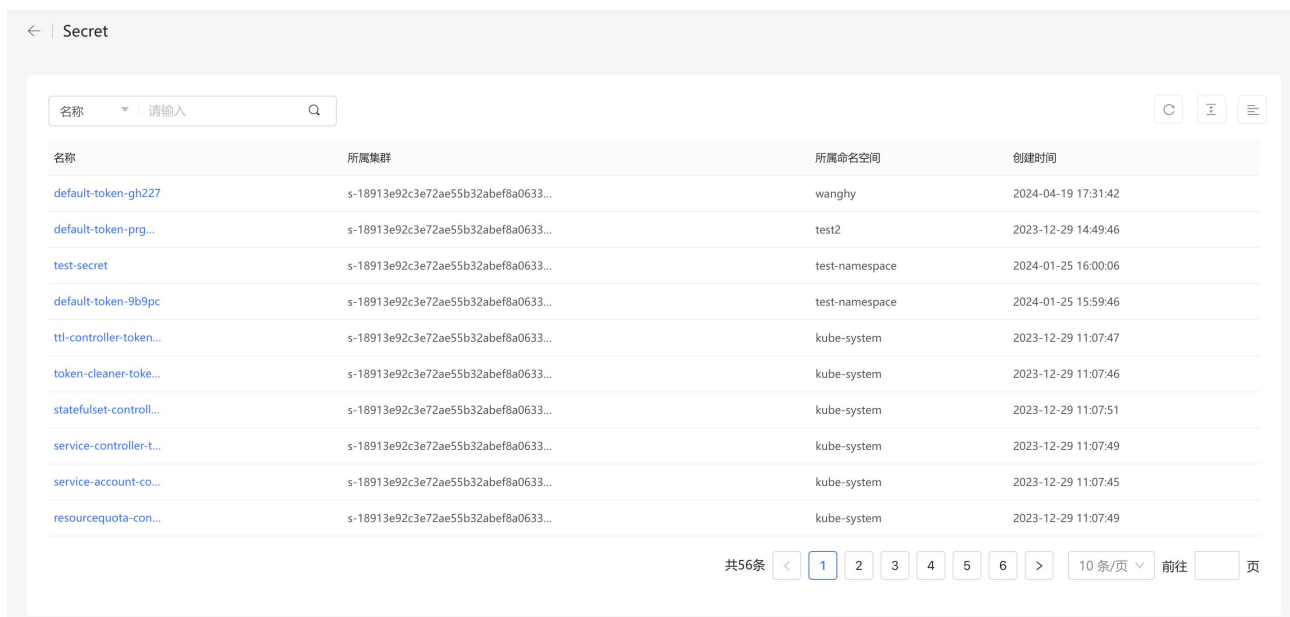
1. 查看 Routes 列表；
2. 单击 Routes 列表中的【容器名称】，进入详情页面；
3. 在 Routes 详情中的基本信息页面，可查看其他详细信息，包括主机、路径、真实主机名、标签、目的端口等信息。

4.3.2.20. Secret

4.3.2.20.1. 查看 Secret 列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【Secret】，跳转至 Secret 列表。

Secret 列表页面，支持按照“名称”、“所属命名空间”进行筛选查询。

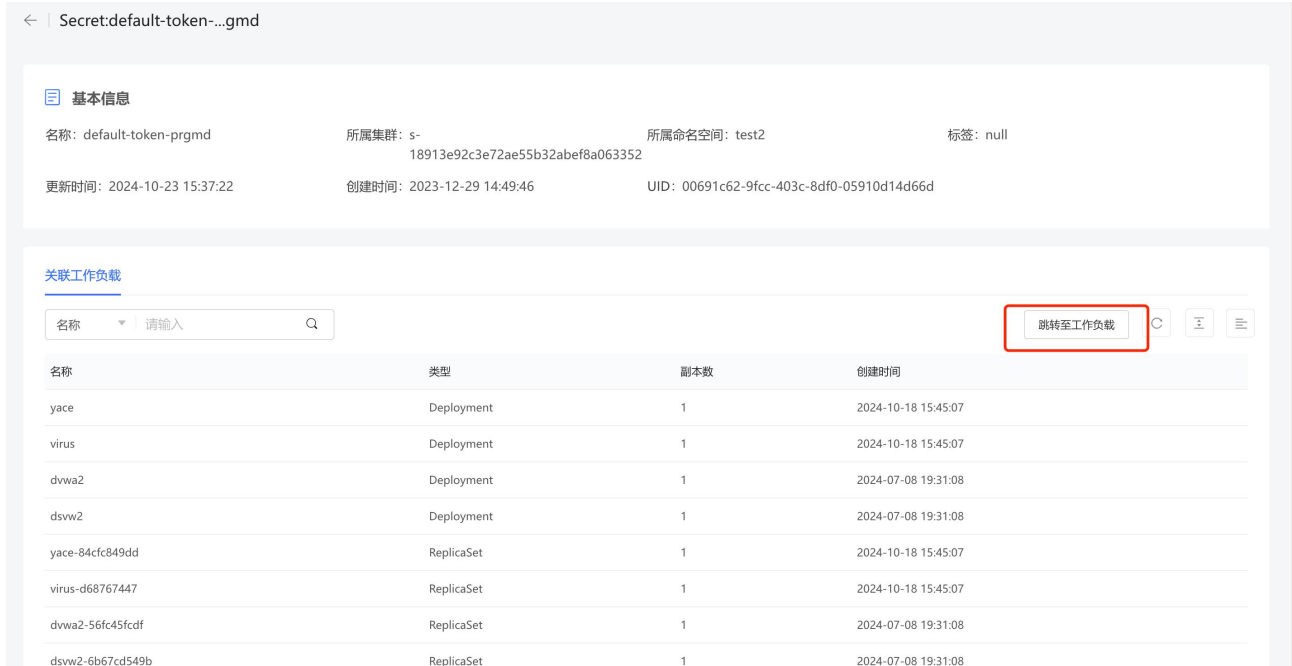


名称	所属集群	所属命名空间	创建时间
default-token-gh227	s-18913e92c3e72ae55b32abef8a0633...	wanghy	2024-04-19 17:31:42
default-token-prg...	s-18913e92c3e72ae55b32abef8a0633...	test2	2023-12-29 14:49:46
test-secret	s-18913e92c3e72ae55b32abef8a0633...	test-namespace	2024-01-25 16:00:06
default-token-9b9pc	s-18913e92c3e72ae55b32abef8a0633...	test-namespace	2024-01-25 15:59:46
t1-controller-token...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:47
token-cleaner-toke...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:46
statefulset-controll...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:51
service-controller-t...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:49
service-account-co...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:45
resourcequota-con...	s-18913e92c3e72ae55b32abef8a0633...	kube-system	2023-12-29 11:07:49

参数	解释说明
名称	Secret 的名称
所属命名空间	Secret 被包含的命名空间
创建时间	Secret 创建时间

4.3.2.20.2. 查看 Secret 详情

1. 查看 Secret 列表;
2. 单击 Secret 列表中的【Secret 名称】，进入详情页面。
3. 在 Secret 详情页面，可查看 Secret 的基本信息，也可查看关联工作负载的列表。



Secret:default-token-...gmd

基本信息

名称: default-token-prgmd 所属集群: s-18913e92c3e72ae55b32abef8a063352 所属命名空间: test2 标签: null

更新时间: 2024-10-23 15:37:22 创建时间: 2023-12-29 14:49:46 UID: 00691c62-9fcc-403c-8df0-05910d14d66d

关联工作负载

名称

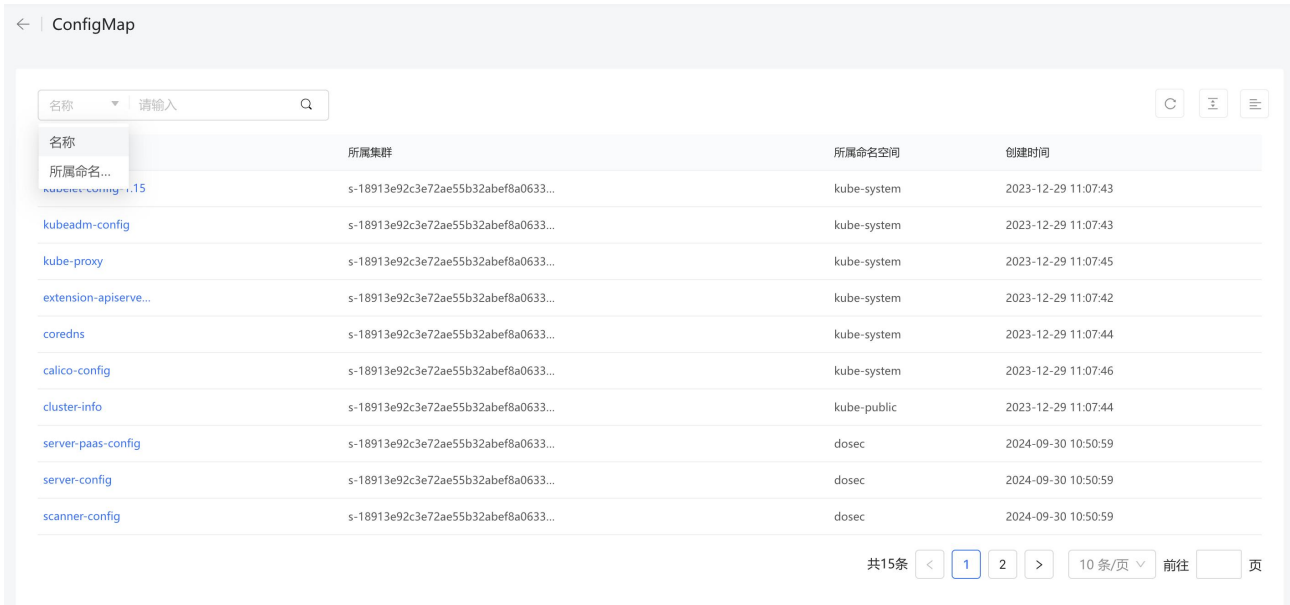
名称	类型	副本数	创建时间
yace	Deployment	1	2024-10-18 15:45:07
virus	Deployment	1	2024-10-18 15:45:07
dvwa2	Deployment	1	2024-07-08 19:31:08
dsvw2	Deployment	1	2024-07-08 19:31:08
yace-84fc849dd	ReplicaSet	1	2024-10-18 15:45:07
virus-d68767447	ReplicaSet	1	2024-10-18 15:45:07
dvwa2-56fc45fcdf	ReplicaSet	1	2024-07-08 19:31:08
dsvw2-6b67cd549b	ReplicaSet	1	2024-07-08 19:31:08

4.3.2.21. ConfigMap

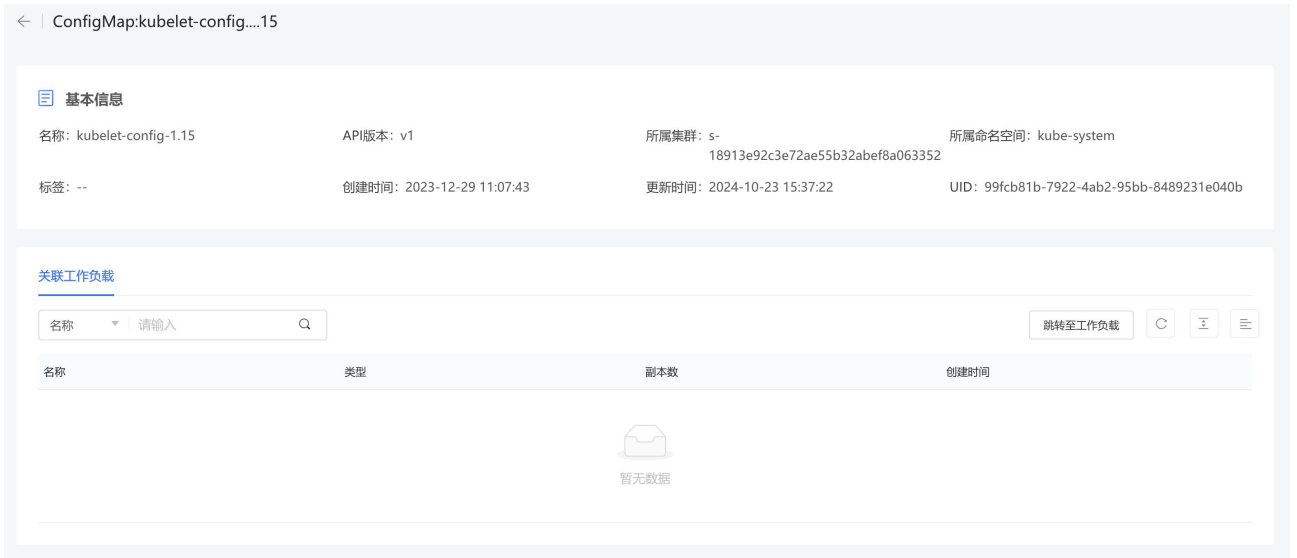
4.3.2.21.1. 查看 ConfigMap 列表及详情

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【ConfigMap】，跳转至 ConfigMap 列表。

ConfigMap 列表页面，支持按照“名称”“所属命名空间”进行筛选查询。



3. 单击【ConfigMap 名称】，跳转至 ConfigMap 详情页，可查看基本信息以及关联的工作负载列表，并也可以跳转至工作负载页面。



4. 3. 2. 22. PV

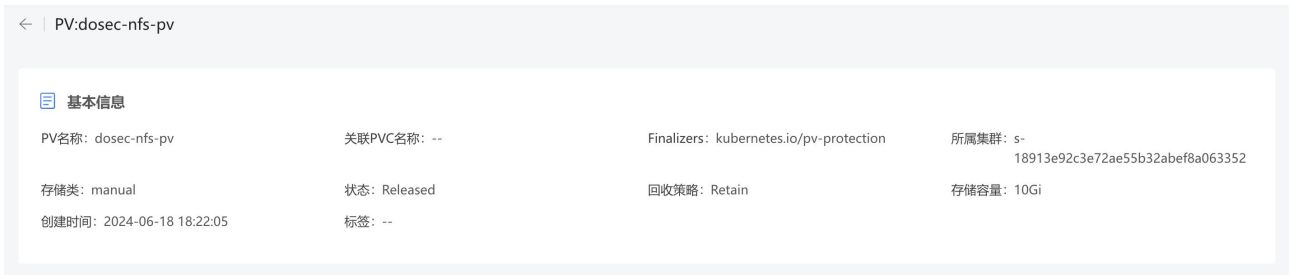
4. 3. 2. 22. 1. 查看 PV 列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【PV】，跳转至 PV 列表。

PV 列表页面，支持按照“PV 名称”、“关联 PVC 名称”、“所属集群”、“状态”、“回收策略”进行筛选查询。



3. 单击【PV 名称】，跳转至 PV 详情页，可查看基本信息。



参数	解释说明
名称	PV 的名称
Finalizers	Finalizer 是带有命名空间的键，告诉 Kubernetes 等到特定的条件被满足后，再完全删除被标记为删除的资源。Finalizer 提醒控制器清理被删除的对象拥有的资源。
存储类	持久卷（PersistentVolume，PV）是集群中的一块存储，可以由管理员事先供应，或者使用存储类（Storage Class）来动态供应。 申领可以通过为 storageClassName 属性设置 StorageClass 的名称来请求特定的存储类。如果 PVC 申领指定存储类为 ""，则相当于为自身禁止使用动态供应的卷。
状态	PV 卷可以处于以下的某种状态： Available（可用）——是一块空闲资源还没有被任何声明绑定 Bound（已绑定）——卷已经被声明绑定 Released（已释放）——声明被删除，卷处于释放状态，但是资源还未被集群重新声明
回收策略	PV 可以设置三种回收策略：保留（Retain），回收（Recycle）和删除（Delete）。 保留策略 Retain：允许用户手动回收资源。

	<p>删除策略：将删除 pv 和外部关联的存储资源，需要插件支持。</p> <p>回收策略：会在卷上执行一些基本的擦除（rm -rf /thevolume/*）操作，之后允许该卷用于新的 PVC 申领。Recycle 策略已被废弃。取而代之的建议方案是使用动态供应。</p>
存储容量	PV 的存储能力大小
创建时间	PV 的创建时间

4.3.2.23. PVC

4.3.2.23.1. 查看 PVC 列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【PVC】，跳转至 PVC 列表。

PVC 列表页面，支持按照“名称”、“所属命名空间”进行筛选查询。

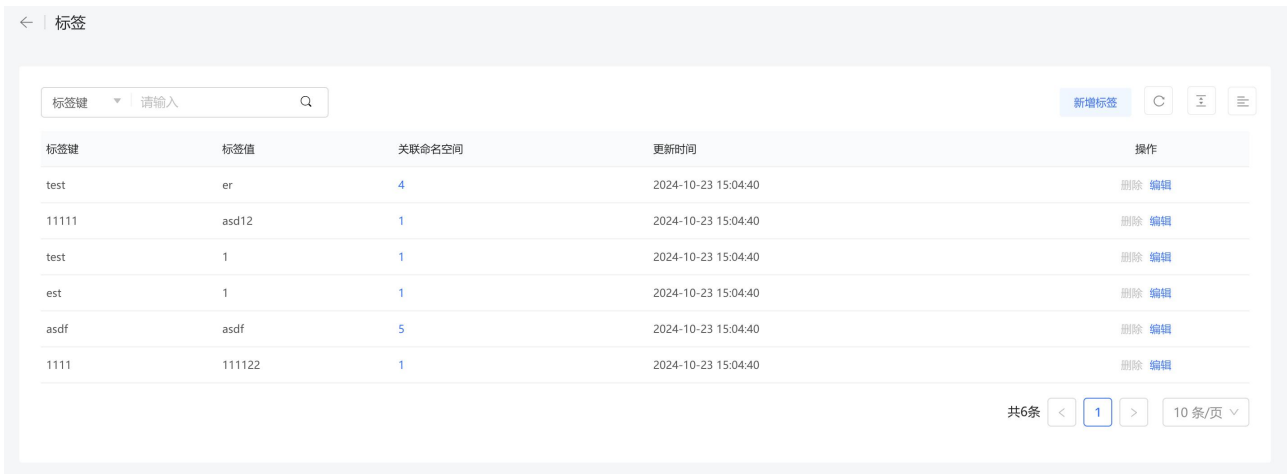
参数	解释说明
名称	PVC 的名称
命名空间	PVC 所属命名空间
存储卷模式	<p>Kubernetes 支持两种卷模式（volumeModes）：Filesystem（文件系统）和 Block（块）。VolumeMode 是一个可选的 API 参数，如果该参数被省略，默认的卷模式是 Filesystem。</p> <p>VolumeMode 属性设置为 Filesystem 的卷会被 Pod 挂载（Mount）到某个目录。</p> <p>VolumeMode 设置为 Block，以便将卷作为原始块设备来使用。这类卷以块设备的方式交给 Pod 使用，其上没有任何文件系统，对于为 Pod 提供一种使用最快可能方式来访问卷而言很有帮助。</p>
创建时间	PV 的创建时间

4.3.2.24. 标签

4.3.2.24.1. 查看标签列表

1. 登录容器安全平台管理界面；
2. 选择【资产中心】-【全部资产】，单击【标签】，跳转至标签列表。

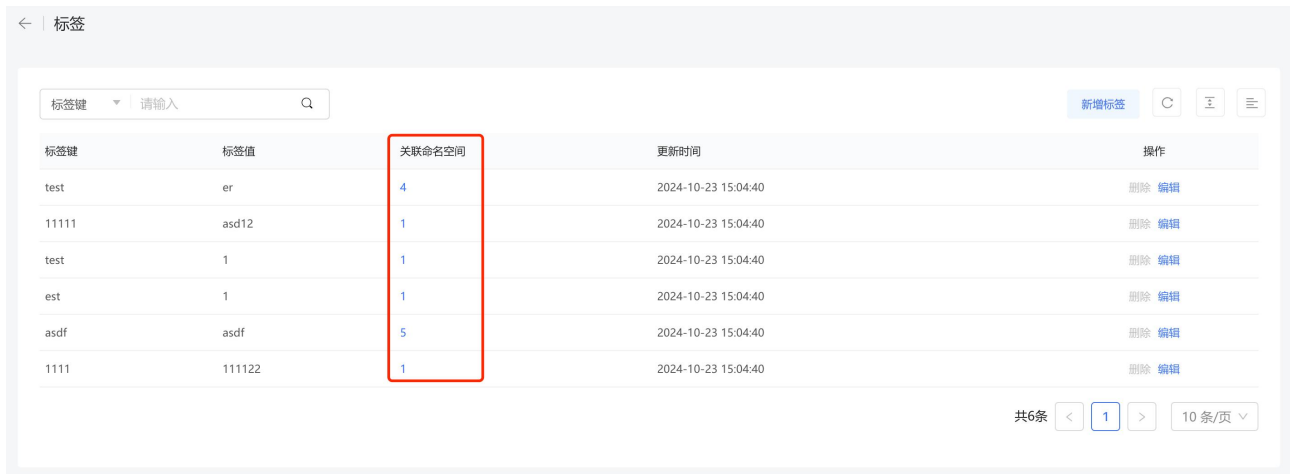
标签列表页面，支持按照“标签键”、“标签值”进行筛选查询。



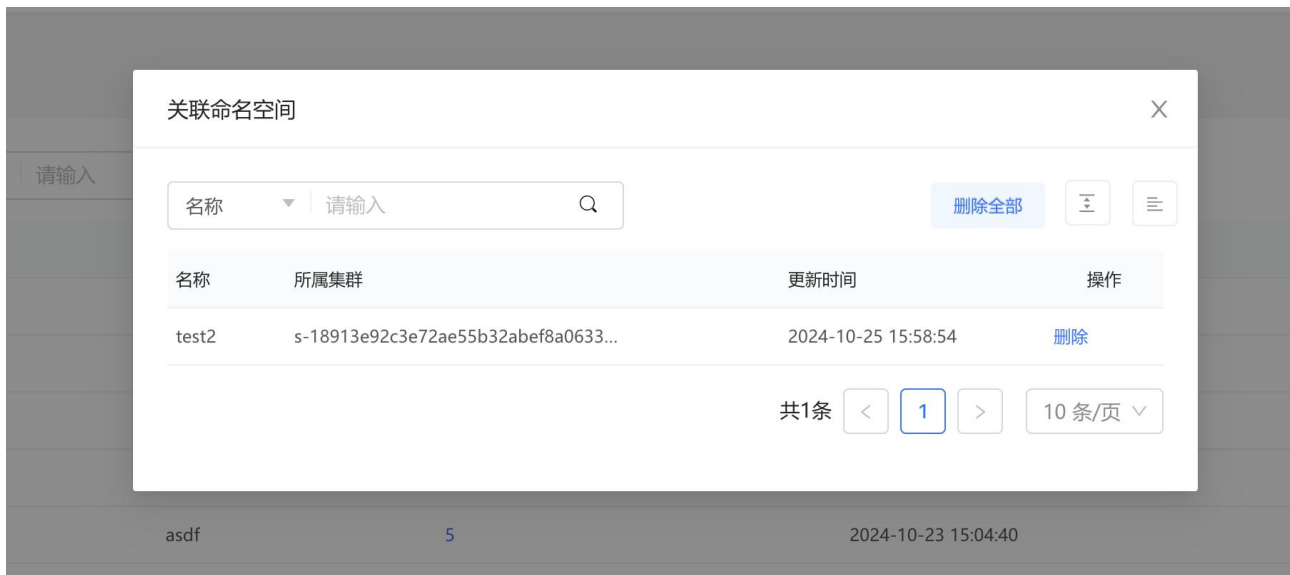
参数	解释说明
标签键	标签键
标签值	标签键对应的值
命名空间	标签键值对的应用对象——命名空间的个数
更新时间	标签的更新时间
操作	<p>单击操作列中的“删除”按钮，可删除该键值对信息。注意事项：命名空间个数不为零时，需先清除关联命名空间才可删除标签。</p> <p>单击操作列中的“编辑”按钮，可进入编辑页面修改键值对信息。</p>

4.3.2.24.2. 查看标签关联命名空间

1. 查看标签列表；
2. 单击标签列表中的【命名空间】，进入标签关联命名空间的详情页面。

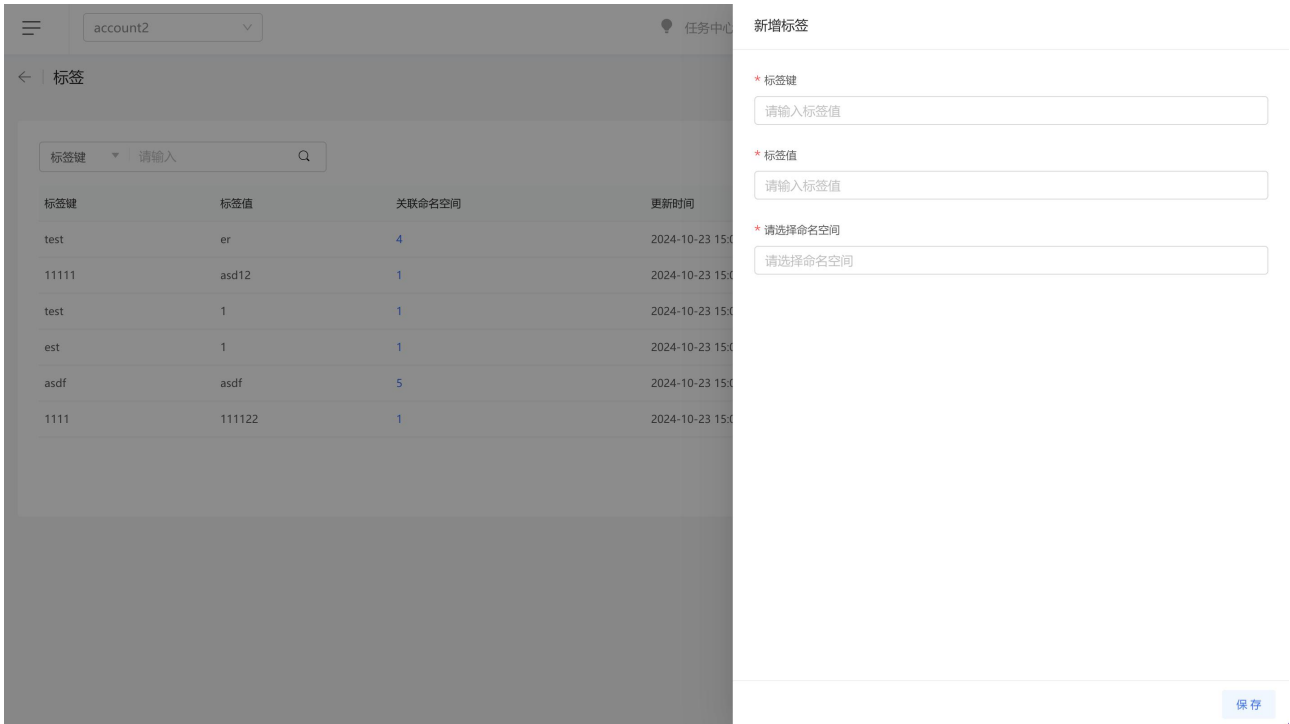


3. 在标签详情页面，可查看标签所关联的所有命名空间名称、命名空间所属集群及更新时间。
4. 单击关联命名空间列表操作列中的“删除”按钮，可删除关联的某个命名空间，单击右上角的“删除全部”按钮，可清除所有关联的命名空间。



4.3.2.24.3. 新建标签

1. 查看标签列表；
2. 单击标签列表右上角的【新建标签】按钮，进入新建标签页面。
3. 输入标签键和标签值信息，选择键值对应用的命名空间对象（可选多个）。
4. 单击“保存”按钮，即可新建成功。

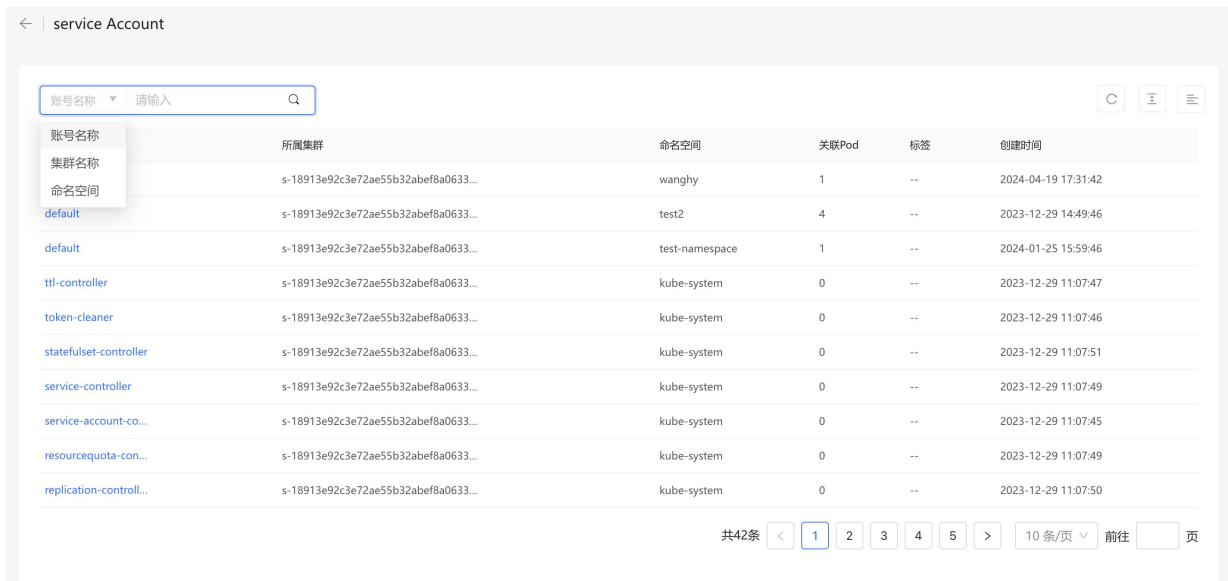


4.3.2.25. Service Account

4.3.2.25.1. 查看 service Account 列表

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【Service Account】，跳转至标签列表。

标签列表页面，支持按照“账号名称”、“集群名称”、“命名空间”进行筛选查询。



3. 单击【service Account 名称】，跳转至 service Account 详情页，可查看基本信息，关联 Pod 列表，可跳转至 Pod 列表。

← | service Account:default

基本信息

账号名称: default 所属命名空间: wanghy 所属集群: s-18913e92c3e72ae55b32abef8a063352 创建时间: 2024-04-19 17:31:42

标签: --

Object :

1 []

关联Pod

Pod名称: 请输入 Q 跳转至Pod列表 C ≡ ☰

Pod名称	所属集群	所属命名空间	运行状态	IP	更新时间
pc-deployment-5ff6f4fb44-b8tqw	s-18913e92c3e72ae55b32abef8a0633...	wanghy	Running	10.233.140.116	2024-10-23 15:37:25

共1条 < 1 > 10条/页 ∨

4.3.2.26. Role

4.3.2.26.1. 查看 role 列表及详情

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【role】，跳转至 role 列表。role 列表页面，支持按照“角色名称”、“角色类型”、“所属集群”、“命名空间”进行筛选查询。

← | role

角色名称: 请输入 Q C ≡ ☰

角色名称	角色类型	所属集群	命名空间	标签	创建时间
角色名称	角色类型	所属集群	命名空间	标签	创建时间
角色名称	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
角色类型	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
所属集群	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
命名空间	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:public-info...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:persistent-v...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:node-proxier	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:node-probl...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:node-boot...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:node	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:kubelet-api...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42
system:kube-sched...	ClusterRole	s-18913e92c3e72ae55b32abef8a0633...	--	kubernetes.io/bootstrapping.rbac-def...	2023-12-29 11:07:42

共70条 < 1 2 3 4 5 6 7 > 10条/页 前往 页

3. 单击【role 名称】，跳转至 role 详情页，可查看基本信息。

role:system:volume-...ler

基本信息

角色名称: system:volume-scheduler 所属命名空间: -- 所属集群: s-18913e92c3e72ae55b32abef8a063352 创建时间: 2023-12-29 11:07:42

标签: kubernetes.io/bootstrapping.rb...

Object :

```

1  [
2  {
3    "verbs": [
4      "get",
5      "list",
6      "patch",
7      "update",
8      "watch"
9    ],
10   "apiGroups": [
11     ""
12   ],

```

4.3.2.27. Role binding

4.3.2.27.1. 查看 Role binding 列表及详情

1. 登录容器安全平台管理界面;
2. 选择【资产中心】-【全部资产】，单击【Role binding】，跳转至 Role binding 列表。

Role binding

规则名称 请输入

规则名称	角色名称	角色类型	关联账号	所属集群	命名空间	创建时间
system:volume-scheduler	system:volume-scheduler	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:public-info-viewer	system:public-info-viewer	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:node-proxier	system:node-proxier	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:node	system:node	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:kube-scheduler	system:kube-scheduler	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:kube-dns	system:kube-dns	ClusterRole	kube-dns	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:kube-controller-manager	system:kube-controller-manager	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:discovery	system:discovery	ClusterRole	--	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43
system:coredns	system:coredns	ClusterRole	coredns	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:44
system:controller:ttl-controller	system:controller:ttl-controller	ClusterRole	ttl-controller	s-18913e92c3e72ae55b32abef8a0633...	--	2023-12-29 11:07:43

共57条 < 1 2 3 4 5 6 > 10条/页 前往 页

4.4. 告警响应

4.4.1. 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。

初始访问(0)	执行(0)	持久化(0)	权限提升(0)	防御绕过(0)	凭证访问(0)	发现(0)	影响(1)	其他(0)
攻击对外开放的服务	容器命令管理	外部远程服务	逃逸到宿主主机	在宿主主机内构建镜像	暴力破解	容器和资源发现	端口拒绝服务	自定义安全策略
外部远程服务	部署容器	植入内部镜像	权限滥用	部署容器	不安全凭证	网络服务发现	网络拒绝服务	异常流量
可用账户	预留任务/作业	预留任务/作业	预留任务/作业	预留任务/作业	损害防御		密潭劫持	1
	用户执行	可用账户	可用账户	可用账户	宿主主机指示器移除		破坏系统及数据	0
			特权提升	0	伪装	0		
			触发式提权	0	可用账户	0		

报警名称	报警级别	报警类型	集群名称	受影响的节点	受影响的命名空间	受影响的容器	状态	首次发现时间	最近发现时间	操作
执行远程文件传输命令	异常	命令执行	s-b8db666...	ecm-ctcsg-003	test2	k8s_sec-event...	未处理	2024-04-30 09:55:06	2024-04-30 09:55:06	处理

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。

反弹shell操作	本地提权	暴力破解	恶意命令执行	病毒查杀	挖矿行为	容器逃逸
0	0	0	0	0	0	0

报警名称	报警级别	报警类型	集群名称	受影响的节点	受影响的命名空间	受影响的容器	状态	首次发现时间	最近发现时间	操作
执行远程文件传输命令	异常	命令执行	s-b8db666...	ecm-ctcsg-003	test2	k8s_sec-event...	未处理	2024-04-30 09:55:06	2024-04-30 09:55:06	处理

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”、“受影响的节点”、“受影响的节点”、“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。
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”。

命令执行-执行远程文件传输命令



处理方式：?

标记为已处理

选择标记为已处理后，该告警状态将更新为已处理。

加入白名单

选择加入白名单后，该事件将不再报警，可在【响应中心】查看白名单规则详情。

隔离Pod

选择隔离Pod后，会阻止Pod的外出流量，但不会影响Pod的进入流量，不会影响业务访问。可在【响应中心】解除隔离。隔离Pod该告警状态标记为已处理。

重启Pod

选择重启Pod后，该Pod将被杀死运行。可在【响应中心】查看已重启的Pod。重启Pod后该告警状态标记为已处理。

暂停容器

选择暂停容器后，该容器将暂停运行。可在【响应中心】恢复容器。暂停容器后该告警状态标记为已处理。

查看详情

取消

保存

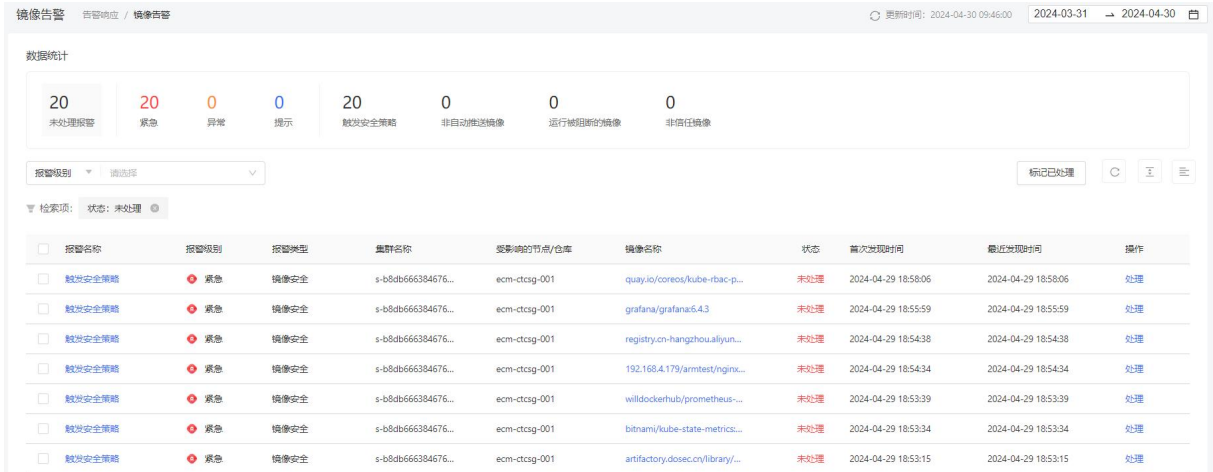
5. 选择处理方式后单击“保存”，即可完成告警处理。

4.4.2. 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”。

① 如需使用镜像阻断功能，请到[安装配置-组件安装-防御容器安装](#)页面中开启镜像所在集群的镜像阻断功能。

处理方式: ?

标记为已处理

选择标记为已处理后，该告警状态将更新为已处理。

加入白名单

选择加入白名单后，该事件将不再报警，可在【响应中心】查看白名单规则详情。

* 白名单名称

规则

* 报警类型

镜像安全-触发安全策略

匹配规则

节点名称

相等

ecm-ctcsg-001



镜像名称

相等

quay.io/coreos/kube-rbac-proxy:v0.4.1



镜像阻断

选择阻断镜像后，该镜像将不允许启动容器。可在【响应中心】解除阻断镜像。阻断镜像后该告警状态标记为已处理。

查看详情

取消

保存

4. 选择处理方式后单击“保存”，即可完成告警处理。

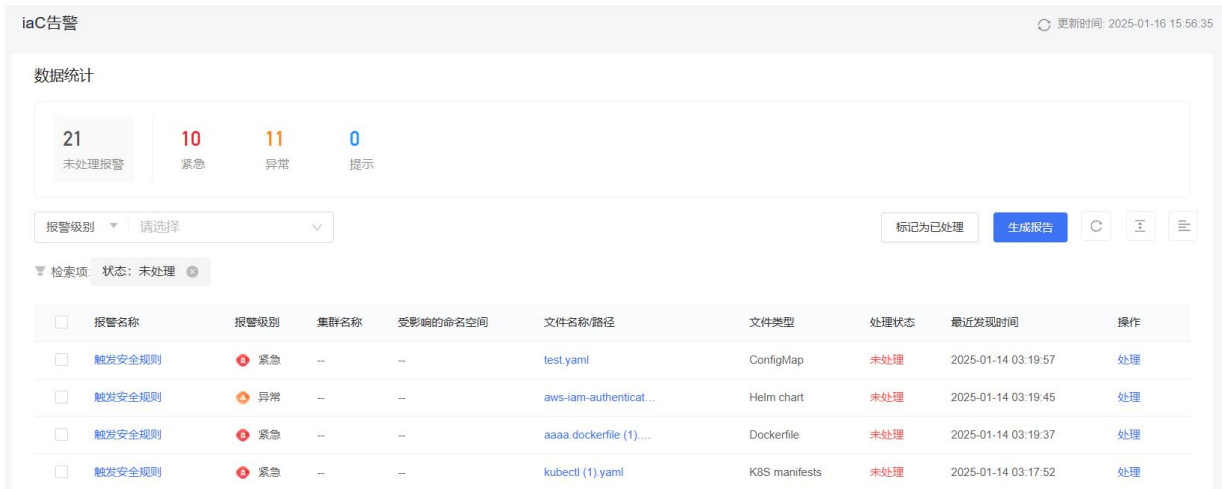
4.4.3. IaC 告警

在 IaC 告警页面，用户可以查看 IaC 告警信息，并对告警进行处理。

4.4.3.1. 查看告警列表

1. 登录容器安全卫士控制台。

- 在左侧导航栏，选择“告警响应 > IaC 告警”，进入 IaC 告警页面。



- 查看告警数据统计：显示未处理的告警数量，并分别按不同级别进行数量统计。
- 单击数据统计中某一级别的告警，下方报警列表将根据选择的级别进行筛选。
- 告警列表内，支持按照“报警级别”、“文件名称/路径”、“文件类型”、“集群名称”、“命名空间”、“状态”进行筛选查询。

告警信息参数说明：

参数	说明
报警名称	报警的原因。单击报警名称可查看报警详情。
报警级别	报警分为紧急、异常、提示这三种类型。
集群名称	存在报警的镜像所属集群的名称。
受影响的命名空间	受影响的命名空间名称。
文件名称/路径	告警的文件名称。单击可查看文件详情及文件告警详情。
文件类型	告警的文件类型。
处理状态	状态分为已处理和未处理。
最近发现时间	最近一次发现报警事件的时间。

4.4.3.2. 查看告警详情

- 登录容器安全卫士控制台。
- 在左侧导航栏，选择“告警响应 > IaC 告警”，进入 IaC 告警页面。

3. 点击告警列表“报警名称”，可查看报警详情。

数据统计

13 未处理报警 7 紧急 6 异常 0 提示

报警级别 请选择

搜索项: 状态: 未处理

报警名称	报警级别	集群名称	受影响的命名空间	文件名/路径	文件类型	处理状态	最近发现时间	操作
触发安全规则	异常	s-94bfeb44de8a04fab56a18c969557c5	test2	intrusion.yaml	K8S manifests	未处理	2024-12-23 14:17:59	处理
触发安全规则	异常	s-94bfeb44de8a04fab56a18c969557c5	test2	yace.yaml	K8S manifests	未处理	2024-12-23 14:17:58	处理
触发安全规则	紧急	s-94bfeb44de8a04fab56a18c969557c5	kube-system	kube-proxy.yaml	K8S manifests	未处理	2024-12-23 14:17:58	处理
触发安全规则	异常	s-94bfeb44de8a04fab56a18c969557c5	kube-system	calico-kube-contro...	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	异常	s-94bfeb44de8a04fab56a18c969557c5	kube-system	coredns.yaml	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	紧急	s-94bfeb44de8a04fab56a18c969557c5	dosec	dosec-server.yaml	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	紧急	s-94bfeb44de8a04fab56a18c969557c5	dosec	dosec-scanner.yaml	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	异常	s-94bfeb44de8a04fab56a18c969557c5	test2	virus.yaml	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	紧急	s-94bfeb44de8a04fab56a18c969557c5	kube-system	calico-node.yaml	K8S manifests	未处理	2024-12-23 14:17:57	处理
触发安全规则	异常	aws-iam-authentic...	Helm chart	未处理	2024-12-23 14:17:56	处理

共13条 < 1 2 > 10条/页 前往 页

4. 在报警详情页面，可查看该告警的基本信息、告警命中规则、处置建议等信息。

报警名称: 触发安全规则

基本信息

文件名/路径: [dwa2.yaml](#) 资源名称: dwa2 资源类型: Deployment 集群名称: s-ced90c0ae27aa6fd7742876718dbbbc1
 命名空间: test2 文件来源: 自动发现 文件添加时间: 2024-12-23 10:30:36 首次发现时间: 2024-12-23 11:41:00
 最近发现时间: 2024-12-23 11:41:00

报警名称: 触发安全规则 触发次数: 1 立即处理

告警说明: K8S manifest文件安全检查存在安全风险

命中规则: 高风险: 0 中风险: 5 低风险: 2

处置建议: 请根据关联信息确认风险

4.4.3.3. 处理告警

处理单个告警

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 > IaC 告警”，进入IaC告警页面。
3. 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。
4. 进入处理告警页面，对本条告警进行处理。

若您已手动处理该选择处理方式后单击“确认”，即可完成告警处理。告警，或判断当前报警为误报，可以将其“标记为已处理”。

处理方式:

标记为已处理

选择标记为已处理后, 该告警状态将更新为已处理。

5. 选择处理方式后单击“确认”，即可完成告警处理。

批量处理告警

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 > IaC 告警”, 进入 IaC 告警页面。
3. 筛选告警, 并勾选需要标记为已处理的告警, 单击列表页右上方的“标记已处理”按钮。



报警名称	报警级别	集群名称	受影响的命名空间	文件名称/路径	文件类型	处理状态	最近发现时间	操作
<input checked="" type="checkbox"/> 触发安全规则	异常	--	--	aws-iam-authenticat...	Helm chart	未处理	2025-01-14 03:19:45	处理
<input checked="" type="checkbox"/> 触发安全规则	异常	--	kube-system	calico-kube-controll...	K8S manifests	未处理	2025-01-14 03:17:46	处理
<input type="checkbox"/> 触发安全规则	异常	--	dosec	dosec-server.yaml	K8S manifests	未处理	2025-01-14 03:17:46	处理

4. 在“标记为已处理”窗口, 选择标记范围。



5. 选择标记范围后, 单击“确认”。

4.4.3.4. 导出告警

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 > IaC 告警”, 进入 IaC 告警页面。
3. 筛选告警, 并勾选需要导出的告警, 单击列表页右上方的“生成报告”按钮。



4. 在“导出”窗口，选择导出范围。



5. 选择导出范围后，单击“确认”。

4.4.4. 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。




4.4.5. 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”。

4.5. 安全合规

4.5.1. 查看基线检查列表

1. 登录容器安全卫士产品控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 在安全合规页面单击“基线名称”，进入基线详情页面。

安全合规 更新时间: 2024-10-31 15:35:53

基线管理

基线名称 扫描基线

<input type="checkbox"/>	基线名称	适用版本	基线版本	检查项	基线类型	创建人	是否达标	检测通过率	最近检查时间	最近更新
<input type="checkbox"/>	Ubuntu 20.04 CIS	适用于 Ubuntu 20.04 版本	1.1.0	243	CIS基线	内置	未达标	0.00%	--	2024-09-29 04:37:40
<input type="checkbox"/>	Ubuntu 18.04 CIS	适用于 Ubuntu 18.04 版本	2.1.0	242	CIS基线	内置	未达标	0.00%	--	2024-09-29 04:37:36

4. 筛选检查项：支持按照“集群”、“检查项名称”、“类型”、“启用状态”进行筛选查询。

基线名称: Ubuntu 18.04 CIS

集群: 检查项名称 导出 扫描

<input type="checkbox"/>	检查项名称	检查项类型	检查对象类型	来源	检测通过率	检查未通过	检查通过	启用状态	最近检查时间	最近更新
<input type="checkbox"/>	确保禁用 cramfs 文件系统的挂载 (自动)	自动	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用挂载 freevxfs 文件系统 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 jffs2 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 hfs 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 hfsplus 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 udf 文件系统的挂载被禁用 (自动)	初始设置	--	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	--	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 分区包含 nodev 选项 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 分区包含 nosuid 选项 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42

共242条 1 2 3 4 5 ... 25 > 10条/页 前往 页

“集群”筛选通过左上角“集群”下拉列表选择，支持选择全部集群或单个集群，集群改变时，检查通过率、检查未通过、检查通过数量和详情会随之更新。

基线名称: Ubuntu 18.04 CIS

集群: 检查项名称 导出 扫描

<input type="checkbox"/>	基线检查项类别	检查对象类型	来源	检测通过率	检查未通过	检查通过	启用状态	最近检查时间	最近更新	
<input type="checkbox"/>	全部									
<input type="checkbox"/>	s-87dd947942cfea6b7c...	(自动)	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	s-2c404ba3d5758d1791...	(自动)	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	s-6253b4c21c26d0618b...	(自动)	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 jffs2 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 hfs 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保禁用 hfsplus 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 udf 文件系统的挂载被禁用 (自动)	初始设置	--	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	--	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 分区包含 nodev 选项 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42
<input type="checkbox"/>	确保 /var/tmp 分区包含 nosuid 选项 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:42

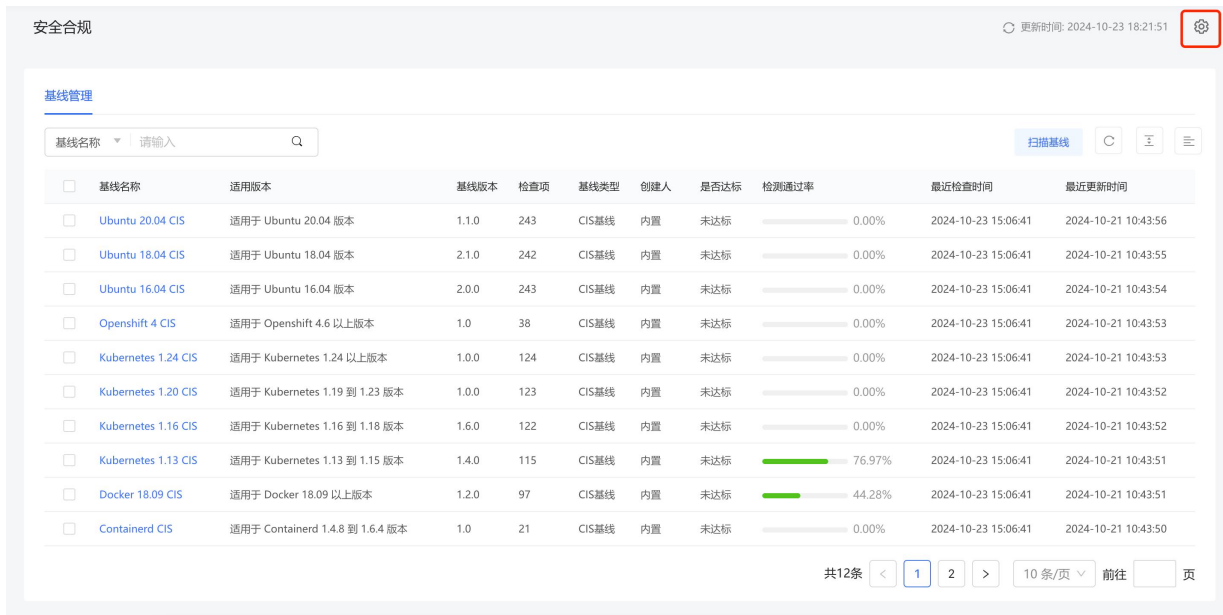
共242条 1 2 3 4 5 ... 25 > 10条/页 前往 页

5. 基线合规信息参数说明。

参数	说明
检查项名称	基线检查项的名称。
基线检查项类别	基线检查项类别随着基线类型的不同而不同。
检查对象类型	类型指的是基线检查项检测对象的类型，分为容器、镜像和节点。
来源	基线检查项的来源。
检测通过率	该基线检测项在相应对象类型（容器或镜像或节点）中的检查通过率，通过用绿色线条表示，不通过用红色线条表示。
检查未通过	未通过该基线检测项的容器（或镜像、或节点）数量。
检查通过	通过该基线检测项的容器（或镜像、或节点）数量。
启用状态	是否启用该基线检查项。

4.5.2. 选择并开启基线

1. 登录容器安全卫士产品控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 在该页面单击右上角的“设置”按钮，进入设置页面。



安全合规 更新时间: 2024-10-23 18:21:51 ⚙️

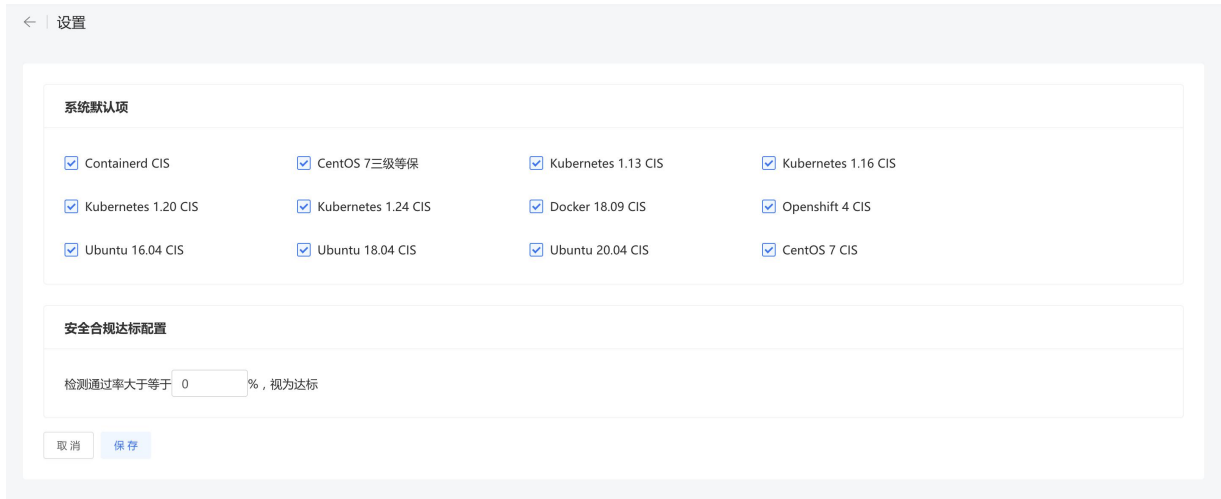
基线管理

基线名称 请输入 扫描基线

<input type="checkbox"/>	基线名称	适用版本	基线版本	检查项	基线类型	创建人	是否达标	检测通过率	最近检查时间	最近更新时间
<input type="checkbox"/>	Ubuntu 20.04 CIS	适用于 Ubuntu 20.04 版本	1.1.0	243	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:56
<input type="checkbox"/>	Ubuntu 18.04 CIS	适用于 Ubuntu 18.04 版本	2.1.0	242	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:55
<input type="checkbox"/>	Ubuntu 16.04 CIS	适用于 Ubuntu 16.04 版本	2.0.0	243	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:54
<input type="checkbox"/>	OpenShift 4 CIS	适用于 OpenShift 4.6 以上版本	1.0	38	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:53
<input type="checkbox"/>	Kubernetes 1.24 CIS	适用于 Kubernetes 1.24 以上版本	1.0.0	124	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:53
<input type="checkbox"/>	Kubernetes 1.20 CIS	适用于 Kubernetes 1.19 到 1.23 版本	1.0.0	123	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:52
<input type="checkbox"/>	Kubernetes 1.16 CIS	适用于 Kubernetes 1.16 到 1.18 版本	1.6.0	122	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:52
<input type="checkbox"/>	Kubernetes 1.13 CIS	适用于 Kubernetes 1.13 到 1.15 版本	1.4.0	115	CIS基线	内置	未达标	76.97%	2024-10-23 15:06:41	2024-10-21 10:43:51
<input type="checkbox"/>	Docker 18.09 CIS	适用于 Docker 18.09 以上版本	1.2.0	97	CIS基线	内置	未达标	44.28%	2024-10-23 15:06:41	2024-10-21 10:43:51
<input type="checkbox"/>	Containerd CIS	适用于 Containerd 1.4.8 到 1.6.4 版本	1.0	21	CIS基线	内置	未达标	0.00%	2024-10-23 15:06:41	2024-10-21 10:43:50

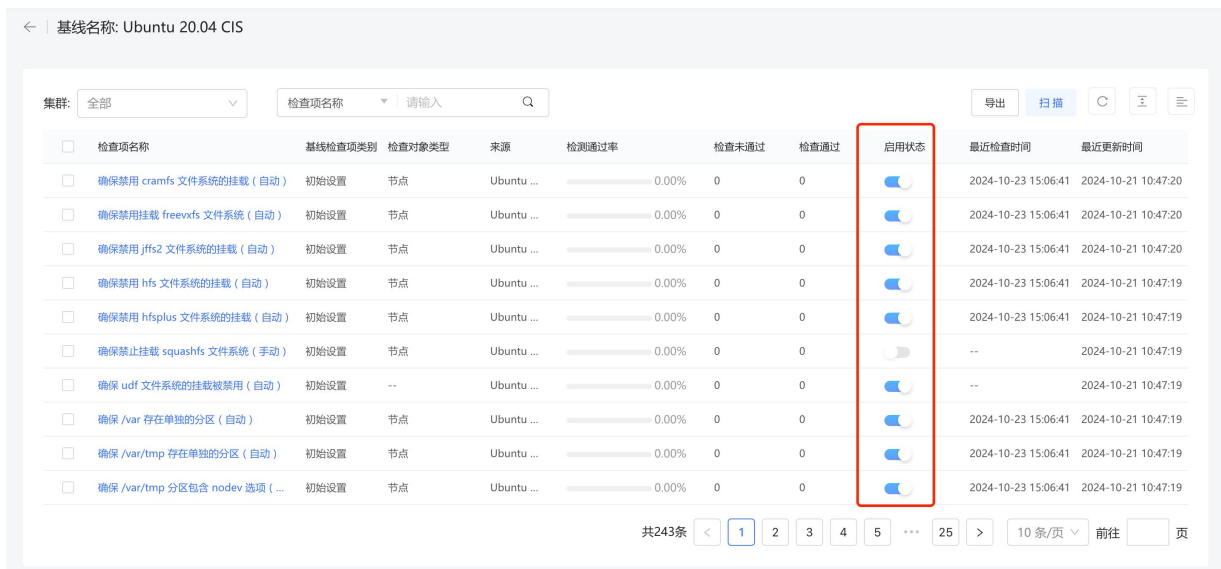
共12条 < 1 2 > 10 条/页 前往 页

- 在设置页面，可见系统默认支持 Docker CIS 基线、Kubernetes CIS 基线（1.3 版本和 1.6 版本）、OpenShift 基线、Ubuntu CIS 基线、Centos CIS 基线这五种合规检查项，选择并开启要进行扫描检测的合规项，单击保存按钮即可添加成功。



4.5.3. 启动基线检查项

- 登录容器安全卫士产品控制台。
- 在左侧导航栏选择“安全合规”，进入安全合规页面。
- 在安全合规页面单击“基线名称”，进入基线详情页面。
- 在“启用状态”这一列，可自定义选择是否启用某项基线检查项。



4.5.4. 扫描基线

支持扫描全部、部分基线，也支持对基线中的部分检查项进行扫描。

扫描基线

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 单击列表右上角的“扫描基线”。



4. 在弹出的扫描窗口中设置基线范围和扫描对象。



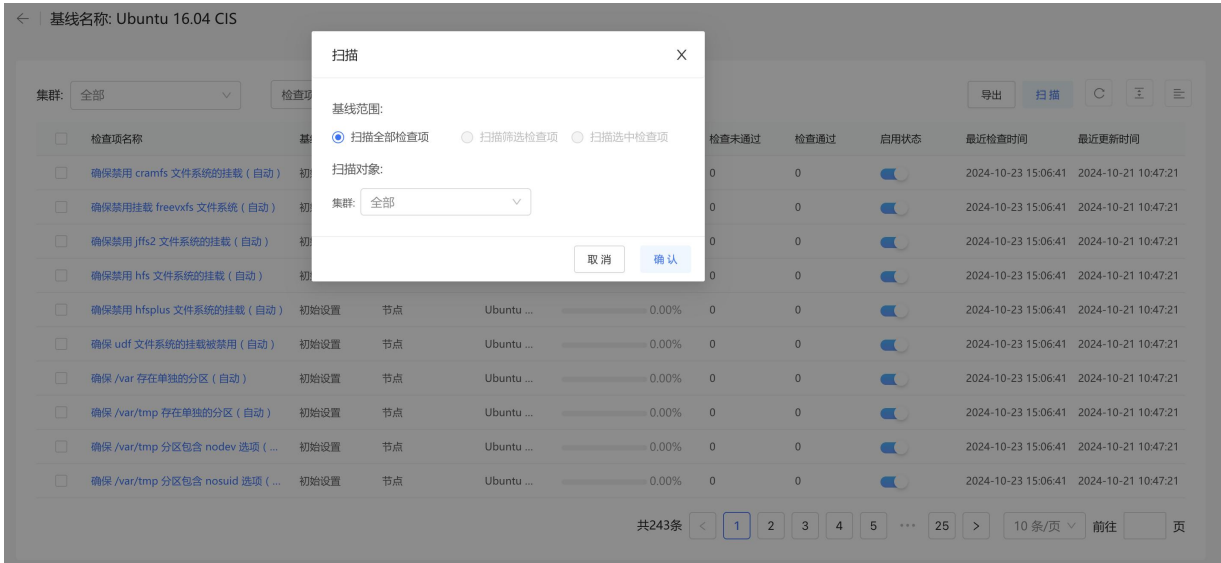
5. 设置完成后，单击“确认”即可开始扫描。

扫描基线检查项

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 在安全合规页面单击“基线名称”，进入基线详情页面。



4. 单击列表右上角的“扫描”，即可开始扫描检查相应容器、镜像和节点是否符合该基线的安全规则。



4.5.5. 查看检查结果

4.5.5.1. 查看基线整体检查通过率

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 查看基线管理列表，包括基线名称、适用版本、基线版本、基线检查项数量和检查结果等，可通过检测率的条形图查看检查通过率的百分比。

安全合规 更新时间: 2024-10-30 10:32:39

基线管理

基线名称 请输入 扫描基线

<input type="checkbox"/>	基线名称	适用版本	基线版本	检查项	基线类型	创建人	是否达标	检测通过率	最近检查时间	最近更新时间
<input type="checkbox"/>	Ubuntu 20.04 CIS	适用于 Ubuntu 20.04 版本	1.1.0	243	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:59
<input type="checkbox"/>	Ubuntu 18.04 CIS	适用于 Ubuntu 18.04 版本	2.1.0	242	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:59
<input type="checkbox"/>	Ubuntu 16.04 CIS	适用于 Ubuntu 16.04 版本	2.0.0	243	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:58
<input type="checkbox"/>	Openshift 4 CIS	适用于 Openshift 4.6 以上版本	1.0	38	CIS基线	内置	未达标	<div style="width: 76.67%;"></div> 76.67%	2024-10-29 18:48:54	2024-10-28 15:38:58
<input type="checkbox"/>	Kubernetes 1.24 CIS	适用于 Kubernetes 1.24 以上版本	1.0.0	124	CIS基线	内置	未达标	<div style="width: 68.75%;"></div> 68.75%	2024-10-29 18:48:54	2024-10-28 15:38:58
<input type="checkbox"/>	Kubernetes 1.20 CIS	适用于 Kubernetes 1.19 到 1.23 版本	1.0.0	123	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:58
<input type="checkbox"/>	Kubernetes 1.16 CIS	适用于 Kubernetes 1.16 到 1.18 版本	1.6.0	122	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:57
<input type="checkbox"/>	Kubernetes 1.13 CIS	适用于 Kubernetes 1.13 到 1.15 版本	1.4.0	115	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:57
<input type="checkbox"/>	Docker 18.09 CIS	适用于 Docker 18.09 以上版本	1.2.0	97	CIS基线	内置	未达标	<div style="width: 0%;"></div> 0.00%	2024-10-29 18:48:54	2024-10-28 15:38:57
<input type="checkbox"/>	Containerd CIS	适用于 Containerd 1.4.8 到 1.6.4 版本	1.0	21	CIS基线	内置	未达标	<div style="width: 78.79%;"></div> 78.79%	2024-10-29 19:54:29	2024-10-28 15:38:57

共12条 前往 页

4.5.5.2. 查看单个检查项通过结果

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 在安全合规页面单击“基线名称”，进入基线详情页面，可查看单个基线检测项是否通过检查。

← 基线名称: Openshift 4 CIS

集群: 导出 扫描

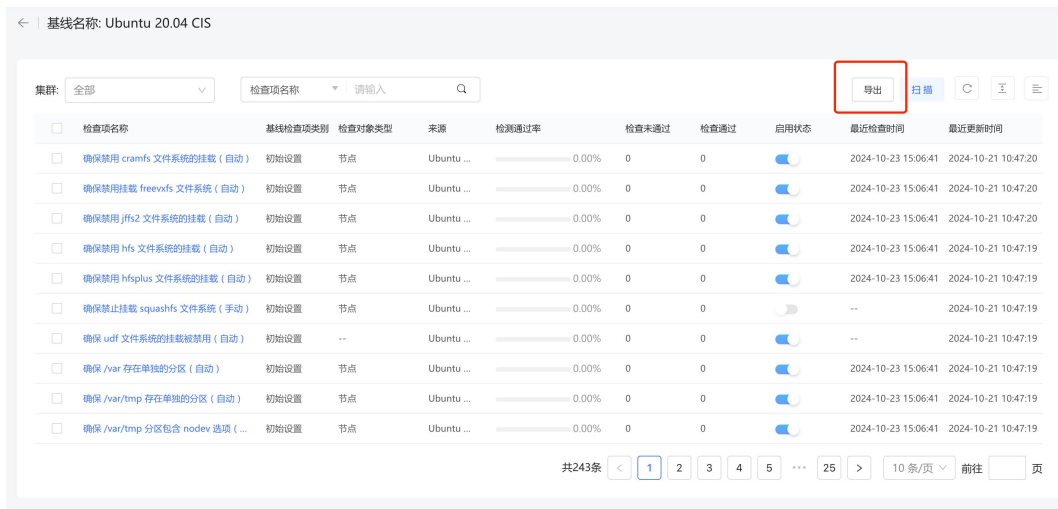
<input type="checkbox"/>	检查项名称	基线检查项类别	检查对象类型	来源	检测通过率	检查未通过	检查通过	启用状态	最近检查时间	最近更新时间
<input type="checkbox"/>	确保设置了准入控制插件 NodeRestriction	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	尽量减少希望共享主机 IPC 名称空间的容...	openshift	master检查项	Openshi...	<div style="width: 100.00%;"></div> 100.00%	0	3	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保未设置准入控制插件 SecurityConte...	openshift	master检查项	Openshi...	<div style="width: 100.00%;"></div> 100.00%	0	3	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保没有设置 --insecure-bind-address ...	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保没有设置 --basic-auth-file 参数	openshift	master检查项	Openshi...	<div style="width: 100.00%;"></div> 100.00%	0	3	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保 --authorization-mode 参数没有设...	openshift	master检查项	Openshi...	<div style="width: 100.00%;"></div> 100.00%	0	3	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保准入控制插件 AlwaysPullimages 没...	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保 --service-account-private-key-file...	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保准入控制插件 ServiceAccount 已设置	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43
<input type="checkbox"/>	确保准入控制插件 SecurityContextCons...	openshift	master检查项	Openshi...	<div style="width: 66.67%;"></div> 66.67%	1	2	<input checked="" type="checkbox"/>	2024-10-29 18:48:54	2024-10-28 15:40:43

共38条 前往 页

4.5.5.3. 导出检查结果

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“安全合规”，进入安全合规页面。
3. 在安全合规页面单击“基线名称”，进入基线详情页面。

4. 点击列表右上方的“导出”按钮，该导出任务会添加至“任务中心 > 下载任务管理”，开始生成 Excel 格式的基线合规检查结果报表。



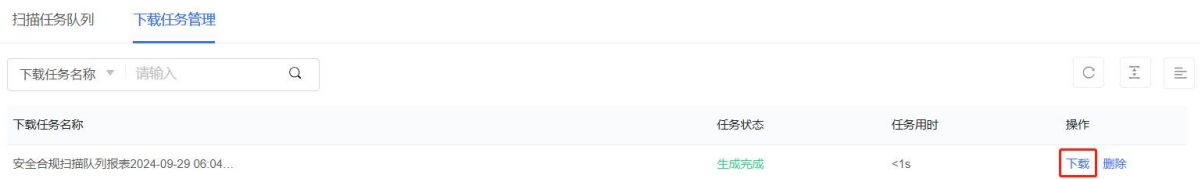
基线名称: Ubuntu 20.04 CIS

集群: 全部 检查项名称 请输入

检查项名称	基线检查项类别	检查对象类型	来源	检测通过率	检查未通过	检查通过	启用状态	最近检查时间	最近更新时间
确保禁用 cramfs 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:20
确保禁用挂载 freevxfs 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:20
确保禁用 jifs2 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:20
确保禁用 hfs 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:19
确保禁用 hfsplus 文件系统的挂载 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:19
确保禁止挂载 squashfs 文件系统 (手动)	初始设置	节点	Ubuntu ...	0.00%	0	0	关闭	--	2024-10-21 10:47:19
确保 udf 文件系统的挂载被禁用 (自动)	初始设置	--	Ubuntu ...	0.00%	0	0	开启	--	2024-10-21 10:47:19
确保 /var 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:19
确保 /var/tmp 存在单独的分区 (自动)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:19
确保 /var/tmp 分区包含 nodev 选项 (...)	初始设置	节点	Ubuntu ...	0.00%	0	0	开启	2024-10-23 15:06:41	2024-10-21 10:47:19

共243条 < 1 2 3 4 5 ... 25 > 10条/页 前往 页

5. 在“任务中心 > 下载任务管理”中，找到对应下载任务，待下载文件生成完毕后，单击“下载”按钮即可下载至本地。



扫描任务队列 下载任务管理

下载任务名称 请输入

下载任务名称	任务状态	任务用时	操作
安全合规扫描队列报表2024-09-29 06:04...	生成完成	<1s	下载 删除

4.6. IaC 安全

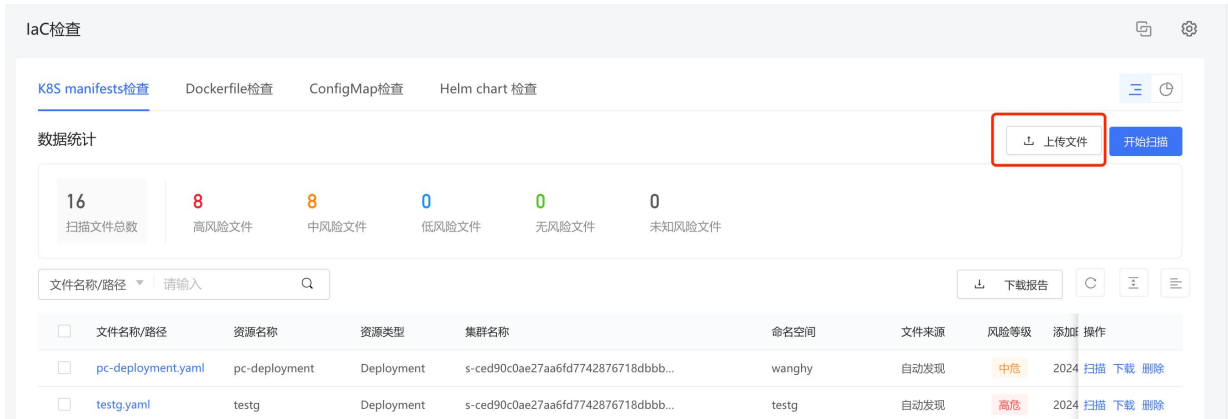
在 kubernetes 系统中，各类资源均需要通过编排文件构建，编排文件编写是否规范，将直接影响到构建资源的安全性、规范性与可用性。系统支持通过本地上传、自动发现或通过对接第三方平台的方式同步 K8S manifests、dockerfile、Configmap，并根据扫描结果指出编排文件中存在风险或不规范的配置项，给出修复建议，保障资源合规且安全的创建。

4.6.1. 上传文件

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“IaC 安全 > IaC 检查”，进入 IaC 检查页面。
3. 选择检查的文件类型。



4. 单击“上传文件”。



5. 可将本地需要扫描检查的 K8S manifests、dockerfile、Configmap，文件上传到系统内进行检查。



4.6.2. 扫描文件

前提条件

已上传需要检测的 K8S manifests、dockerfile、Configmap 文件。

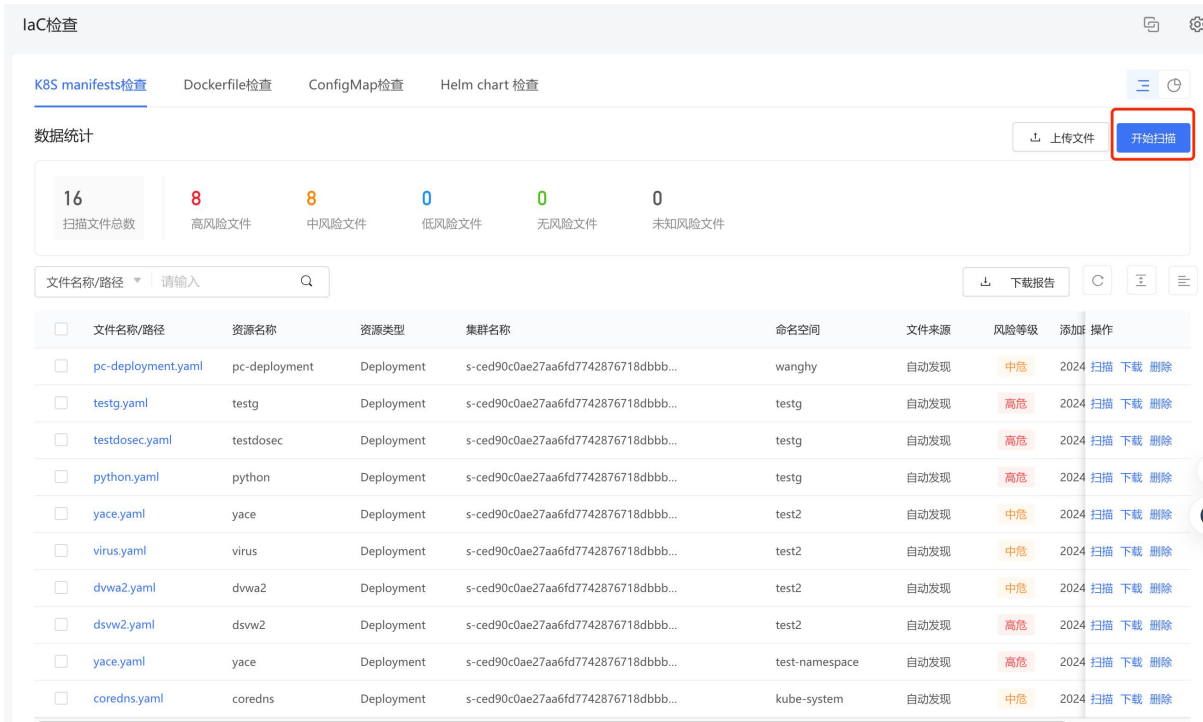
操作步骤

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“IaC 安全 > IaC 检查”，进入 IaC 检查页面。

3. 选择检查的文件类型。



4. 单击检查列表操作列的“扫描”按钮或者列表右上角的“开始扫描”，可对已上传的文件进行检测。



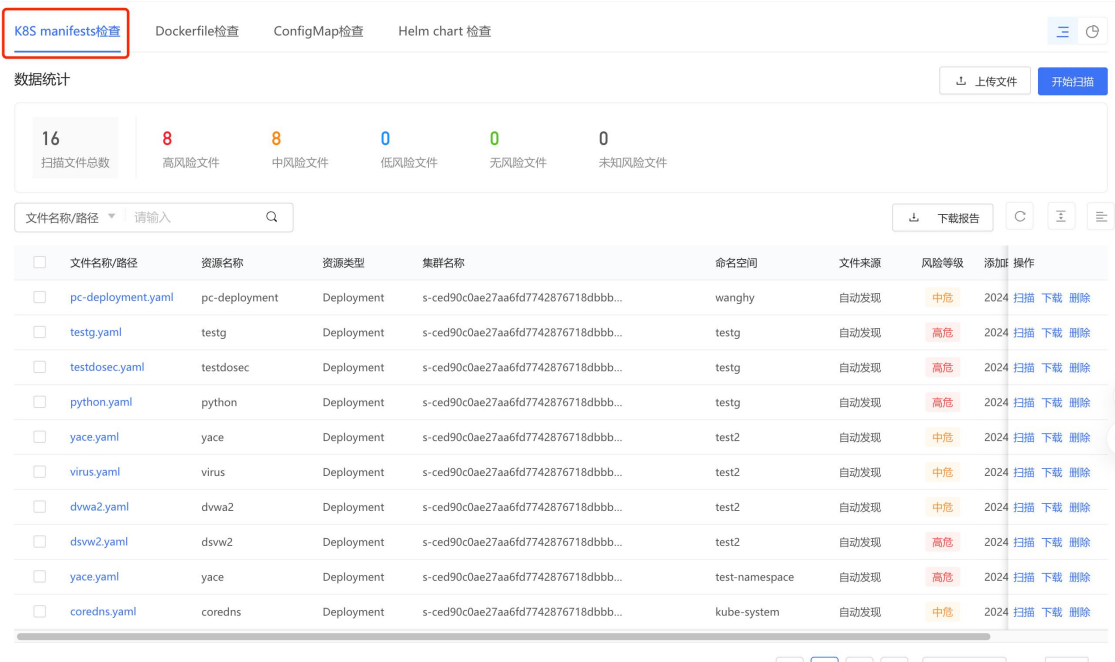
5. 扫描后，到“任务中心 > 扫描任务队列 > IaC 安全扫描队列”中查看扫描状态及生成扫描结果。

4.6.3. 查看文件列表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“IaC 安全 > IaC 检查”，进入 IaC 检查页面。
3. 支持 K8S manifests、Dockerfile、ConfigMap、Helm chart 文件进行检查。



4.6.3.1. 查看 K8S manifests 文件



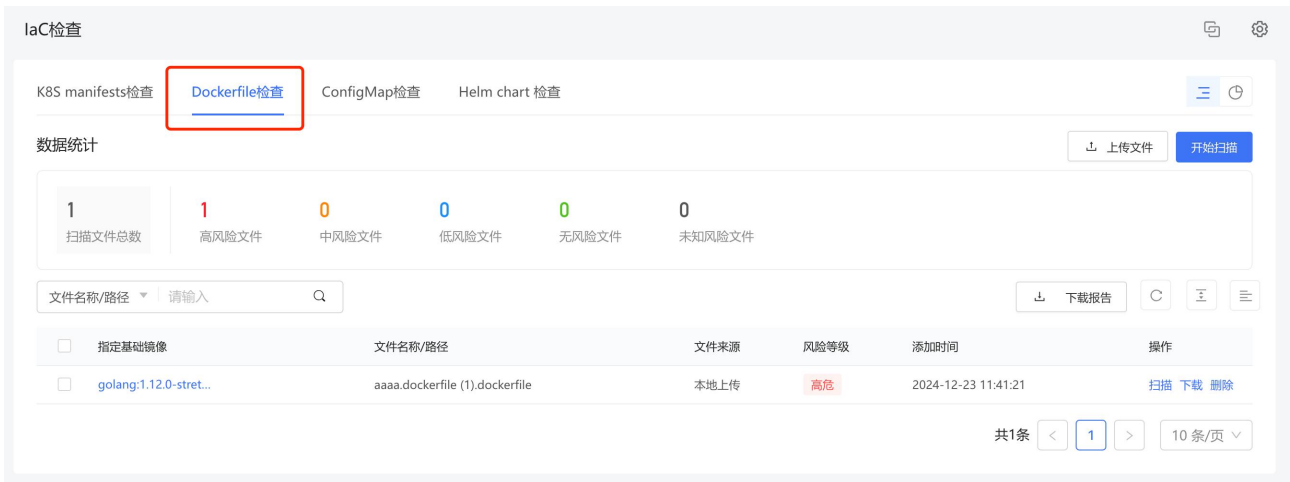
K8S manifests 文件列表内，支持按照“文件名称/路径”、“资源名称”、“资源类型”、“集群名称”、“命名空间”、“文件来源”、“扫描状态”、“风险等级”进行筛选查询。

K8S manifests 文件列表内各字段意义说明如下：

参数	解释说明
文件名称/路径	K8S Manifests 文件名称，以.yaml 为后缀。 K8S Manifests 是指用于定义、创建和管理 Kubernetes 资源的配置文件。这些配置文件以 YAML 或 JSON 格式编写，描述了应用程序、服务、存储等在 Kubernetes 集群上的部署和配置。
资源名称	K8S Manifests 文件所属资源的名称。
资源类型	K8S Manifests 文件所属资源的类型。

参数	解释说明
集群名称	K8S Manifests 文件所属集群。
命名空间	K8S Manifests 文件所属命名空间。
文件来源	文件分为本地上传、自动发现和 GitLab 同步。
扫描状态	扫描状态分为待扫描、扫描中、扫描完成和扫描失败。
风险等级	风险等级分为未知、高风险、中风险、低风险、无风险，未知代表该文件未经过扫描。
添加时间	添加或发现该 K8S Manifests 文件的时间。

4.6.3.2. 查看 dockerfile 文件



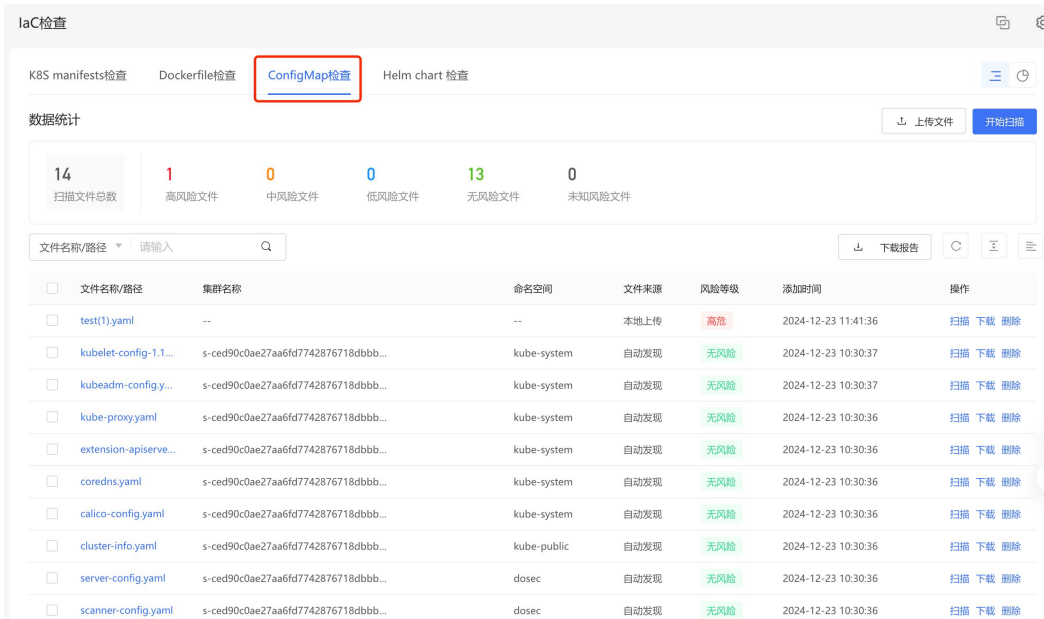
Dockerfile 文件列表内，支持按照“文件名称/路径”、“文件来源”、“扫描状态”、“风险等级”进行筛选查询。

Dockerfile 文件列表内各字段意义说明如下：

参数	解释说明
指定基础镜像	指定构建新 Image 时使用的基础镜像，通常在 Dockerfile 文件中第一个有效指令 FROM 中指定。
文件名称/路径	以.txt 为后缀名的文件名称。 Dockerfile 是一个文本文件，文件内包含了用于构建镜像的指令（Instruction）。
文件来源	文件分为本地上传、GitLab 同步。

扫描状态	扫描状态分为待扫描、扫描中、扫描完成和扫描失败。
风险等级	风险等级分为未知、高风险、中风险、低风险、无风险，未知代表该文件未经过扫描。
添加时间	添加或发现该 Dockerfile 文件的时间。

4.6.3.3. 查看 ConfigMap 文件



The screenshot shows the 'laC检查' interface. At the top, there are tabs for 'K8S manifests检查', 'Dockerfile检查', 'ConfigMap检查' (highlighted with a red box), and 'Helm chart 检查'. Below the tabs is a '数据统计' (Data Statistics) section with a bar chart showing: 14 扫描文件总数 (Total scanned files), 1 高风险文件 (High risk files), 0 中风险文件 (Medium risk files), 0 低风险文件 (Low risk files), 13 无风险文件 (No risk files), and 0 未知风险文件 (Unknown risk files). Below the statistics is a search bar and a table of files. The table has columns: 文件名称/路径 (File name/path), 集群名称 (Cluster name), 命名空间 (Namespace), 文件来源 (File source), 风险等级 (Risk level), 添加时间 (Add time), and 操作 (Action). The first row shows 'test(1).yaml' with a '高危' (High risk) status. Other rows show various ConfigMap files with '无风险' (No risk) status.

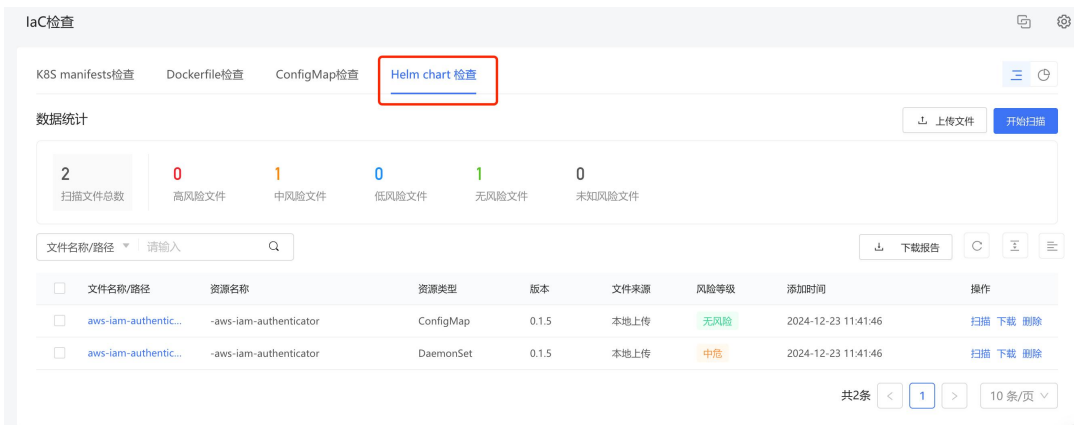
ConfigMap 文件列表内，支持按照“文件名称/路径”、“集群名称”、“命名空间”、“文件来源”、“扫描状态”、“风险等级”进行筛选查询。

ConfigMap 文件列表内各字段意义说明如下：

参数	解释说明
文件名称/路径	ConfigMap 文件名称，以.yaml 为后缀。 ConfigMap 是一种用于存储非机密的配置数据的资源对象。它允许将配置数据从应用程序的 Pod 中分离出来，以便更灵活地管理和更新配置，而不需要重新构建镜像。
集群名称	ConfigMap 文件所属集群。
命名空间	ConfigMap 文件所属命名空间。
文件来源	文件分为本地上传、自动发现。

扫描状态	扫描状态分为待扫描、扫描中、扫描完成和扫描失败。
风险等级	风险等级分为未知、高风险、中风险、低风险、无风险，未知代表该文件未经过扫描。
添加时间	添加或发现该 ConfigMap 文件的时间。

4.6.3.4. 查看 Helm chart 文件



Helm chart 文件列表内，支持按照“文件名称/路径”、“资源名称”、“资源类型”、“版本”、“文件来源”、“扫描状态”、“风险等级”进行筛选查询。

Helm chart 文件列表内各字段意义说明如下：

参数	解释说明
文件名称/路径	Helm chart 文件名称，以.yaml 为后缀。 Helm 是一个 Kubernetes 包管理工具，它允许你定义、安装和升级 Kubernetes 应用程序。Helm 使用一种被称为 Helm Charts 的打包格式，它包含了在 Kubernetes 中部署应用程序所需的所有资源和配置信息。
资源名称	Helm chart 文件所属资源的名称。
资源类型	Helm chart 文件所属资源的类型。
版本	Helm chart 文件的版本。
文件来源	文件分为本地上传、Helm 同步。
扫描状态	扫描状态分为待扫描、扫描中、扫描完成和扫描失败。

风险等级	风险等级分为未知、高风险、中风险、低风险、无风险，未知代表该文件未经过扫描。
添加时间	添加或发现该 Helm chart 文件的时间。

4.6.4. 查看文件详情

前提条件

已上传需要检测的 K8S manifests、dockerfile、Configmap 文件。

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“laC 安全 > laC 检查”，进入 laC 检查页面。
3. 选择需要查看详情的文件所属文件类型。

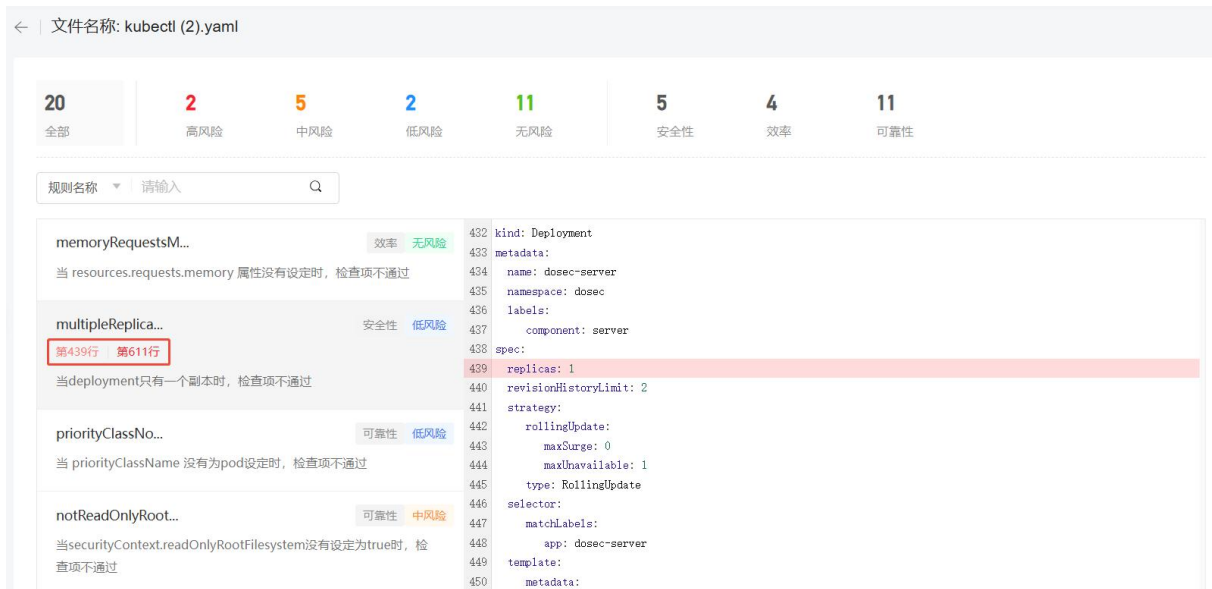


4. 查找目标文件：点击数据统计模块的风险等级数字可以进行快速筛选，或根据列表上方的筛选条件框对文件列表进行精细筛选。
5. 单击“文件名称/路径”链接，可查看当前文件的扫描结果和具体内容。

<input type="checkbox"/>	文件名称/路径	资源名称	资源类型	集群名称	命名空间	文件来源	扫描状态	风险等级	添加时间	操作
<input type="checkbox"/>	kubectf (2).yaml	dosec,dosec-sa,dosec-cr,dosec-crb,regi...	Namespace,ServiceAccount,ClusterRole...	--	--	本地上传	扫描完成	高危	2025-01-14 03:08	扫描 下载 删除
<input type="checkbox"/>	kubectf (1).yaml	dosec,dosec-sa,dosec-cr,dosec-crb,regi...	Namespace,ServiceAccount,ClusterRole...	--	--	本地上传	扫描完成	高危	2025-01-14 03:03	扫描 下载 删除

6. 针对有风险的检查项，单击检查项的“行数”可快速定位到有风险的配置，方便用户查找并修改文件。

注：当检查项提示缺少某项设定时，不会提供定位所在行功能，在文件中添加相关设定即可。



4.6.5. 下载扫描报告

前提条件

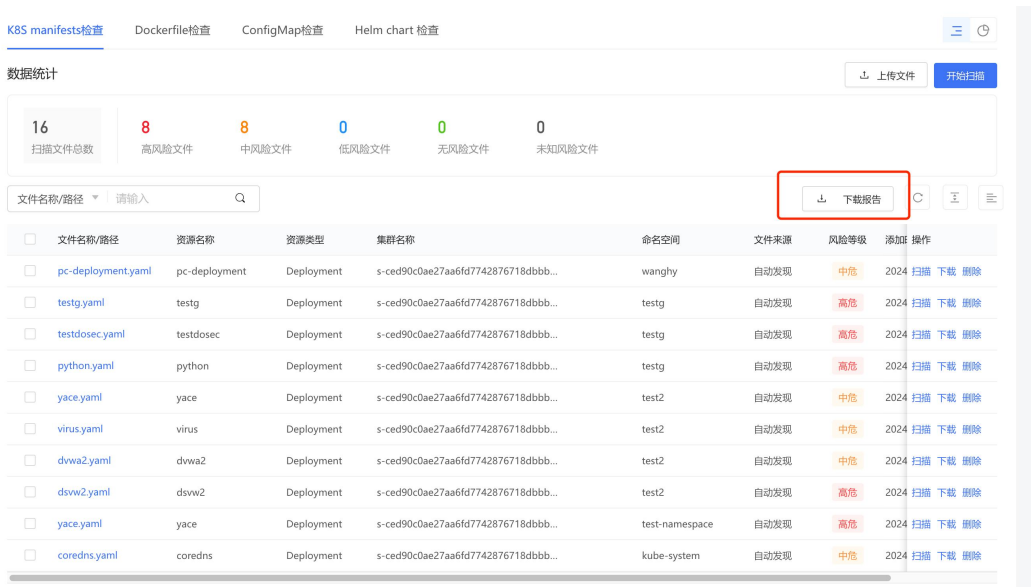
已上传需要检测的 K8S manifests、dockerfile、Configmap 文件。

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“**laC 安全 > laC 检查**”，进入 laC 检查页面。
3. 选择需要下载报告的文件所属文件类型。



4. 单击文件列表右上角的“**下载报告**”，可生成当前选择的编排文件扫描报告。



5. 到“任务中心 > 下载任务管理”中查看任务状态，当任务状态为“生成完成”时，单击任务操作列的“下载”，可以下载已生成的报表。



4.6.6. 管理文件规则

在规则管理页面，可查看并管理 K8S manifests/Helm chart、Dockerfile、ConfigMap 文件的检查规则。

系统内置检查规则，用户也可以按照实际业务需求自定义开启或禁用检查项、自定义添加新的文件检查规则。

4.6.6.1. 添加自定义规则

若系统内置规则不满足需求，用户可根据实际情况，添加自定义检查规则。

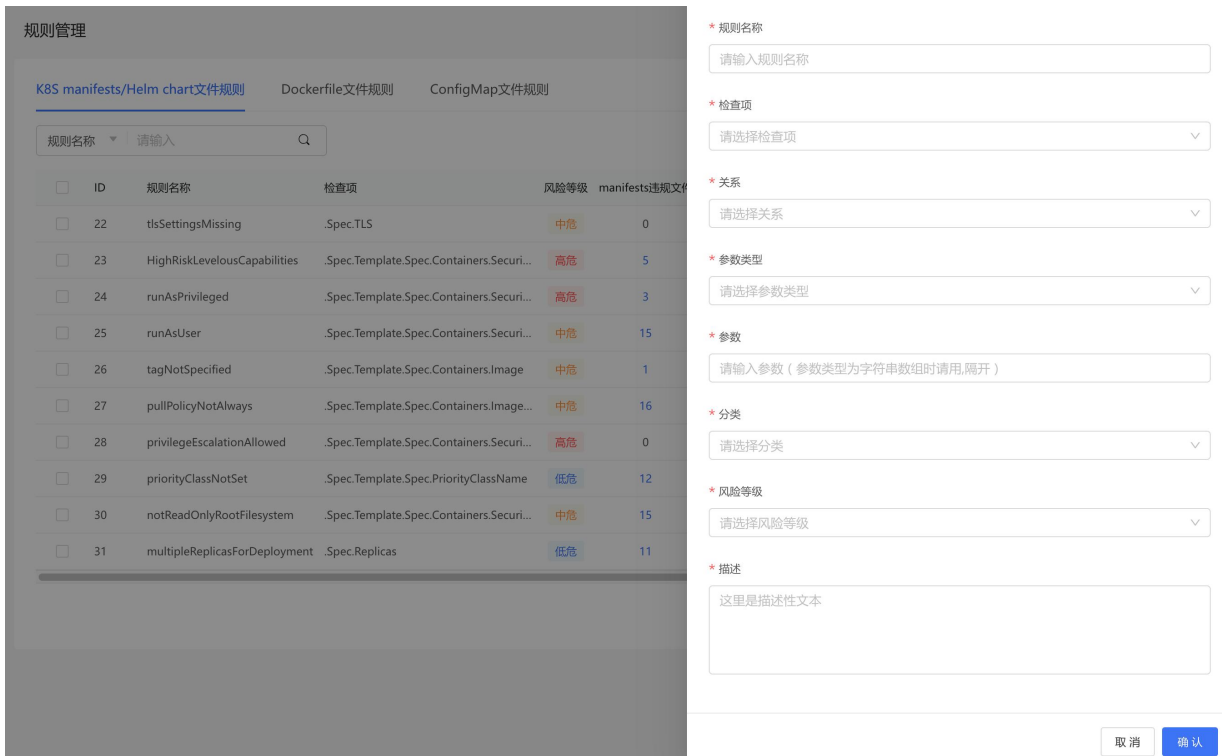
1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“laC 安全 > 规则管理”，进入规则管理页面。
3. 选择需要添加规则的类型。



4. 单击“添加规则”，根据业务需求添加检查项。



5. 在弹出的窗口中，配置规则参数。



参数说明如下：

参数	说明
规则名称	自定义规则名称。
检查项	通过下拉框选择检查项。

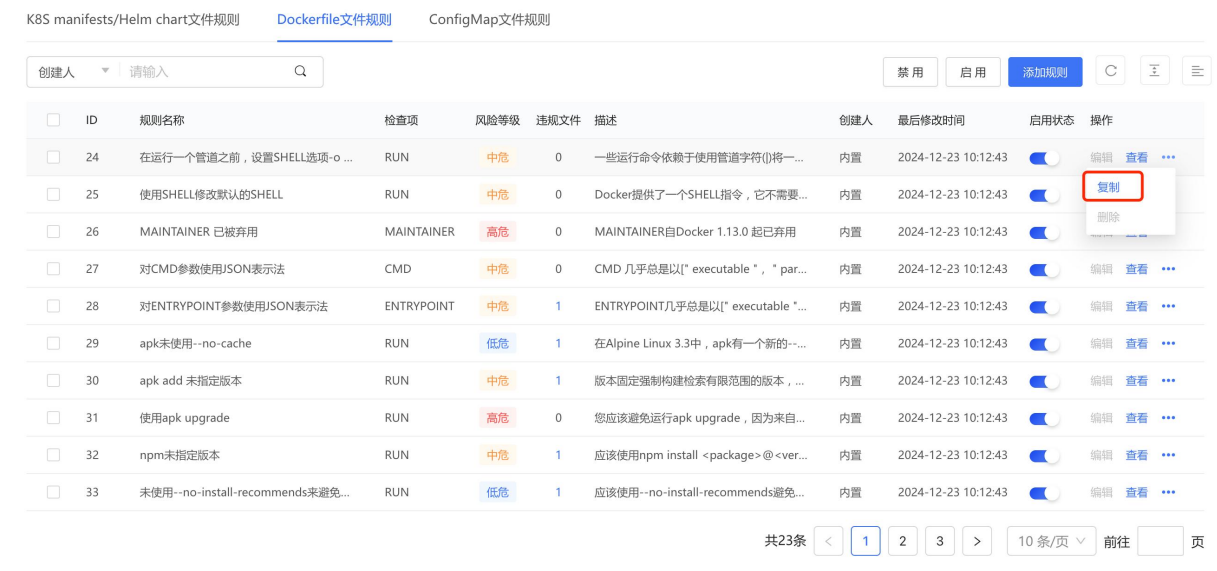
参数	说明
关系	可选等于、不等于、大于、小于、在...之间、不包括、包括这 7 种关系。
参数类型	可选整数、字符串、布尔、字符串数组、空值这 5 种类型。
参数	当参数类型为非空时，必须输入相应类型的参数。
分类	分类包括安全性、效率、可靠性。 根据选择的检查项自动更新，可根据实际情况进行修改。
风险等级	通过下拉框选择添加的检查规则的告警级别，包括高危、中危、低危。
描述	自定义规则描述信息。

6. 参数配置完成后，单击“确认”，添加完成。

4.6.6.2. 复制规则

通过复制规则，只需修改少量配置参数，用户即可快速创建一个和已有规则类似的规则。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“**IaC 安全 > 规则管理**”，进入规则管理页面。
3. 选择需要添加规则的类型。
4. 在规则列表中找到目标规则，单击操作列的“复制”。



The screenshot shows the '规则管理' (Rule Management) page for 'Dockerfile文件规则' (Dockerfile File Rules). It features a search bar, a filter menu, and a table of rules. The table columns include ID, Rule Name, Check Item, Risk Level, Violation Count, Description, Creator, Last Modified Time, and Action. Rule ID 25, '使用SHELL修改默认的SHELL', is highlighted, and its '复制' (Copy) button is visible in the action column.

ID	规则名称	检查项	风险等级	违规文件	描述	创建人	最后修改时间	启用状态	操作
24	在运行一个管道之前，设置SHELL选项-o ...	RUN	中危	0	一些运行命令依赖于使用管道符号()将一...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
25	使用SHELL修改默认的SHELL	RUN	中危	0	Docker提供了一个SHELL指令，它不需要...	内置	2024-12-23 10:12:43	启用	复制
26	MAINTAINER 已被弃用	MAINTAINER	高危	0	MAINTAINER自Docker 1.13.0 起已弃用	内置	2024-12-23 10:12:43	启用	删除
27	对CMD参数使用JSON表示法	CMD	中危	0	CMD 几乎总是以" executable " , " par...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
28	对ENTRYPOINT参数使用JSON表示法	ENTRYPOINT	中危	1	ENTRYPOINT几乎总是以" executable *...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
29	apk未使用--no-cache	RUN	低危	1	在Alpine Linux 3.3中，apk有一个新的--...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
30	apk add 未指定版本	RUN	中危	1	版本固定强制构建检索有限范围的版本，...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
31	使用apk upgrade	RUN	高危	0	您应该避免运行apk upgrade，因为来自...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
32	npm未指定版本	RUN	中危	1	应该使用npm install <package> @<ver...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...
33	未使用--no-install-recommends来避免...	RUN	低危	1	应该使用--no-install-recommends避免...	内置	2024-12-23 10:12:43	启用	编辑 查看 ...

5. 在弹出的窗口中，修改规则参数。参数说明请参见添加自定义规则。
6. 参数修改完成后，单击“确认”。

4.6.6.3. 启用/禁用规则

为了控制检查规则“误报”和“漏报”之间的均衡关系，系统提供规则开关，用户可自定义开启或关闭文件规则检查项。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“laC 安全 > 规则管理”，进入规则管理页面。
3. 选择要操作的规则类型。
4. 在规则列表的启用状态列，可以打开或关闭某一规则。

ID	规则名称	检查项	风险等级	manifests违规文件	chart违规文件	描述	创建人	最后修改时间	启用状态	操作
1...	ItsSettingsMissing	.Spec.TLS	中危	0	0	当securityContext.runAsUser没有设定非...	内置	2025-01-14 01:28:33	<input checked="" type="checkbox"/>	编辑 查看 ...
1...	HighRiskLevelousCapabilities	.Spec.Template.Spec.Containers.Securit...	高危	2	0	当镜像的拉取策略设定不是Always时，...	内置	2025-01-14 01:28:33	<input checked="" type="checkbox"/>	编辑 查看 ...

或勾选多个规则，单击规则列表右上方的“禁用”、“启用”按钮，可以批量启用/禁用规则。

ID	规则名称	检查项	风险等级	manifests违规文件	chart违规文件	描述	创建人	最后修改时间	启用状态	操作	
<input checked="" type="checkbox"/>	1...	ItsSettingsMissing	.Spec.TLS	中危	0	0	当securityContext.runAsUser没有设定非...	内置	2025-01-14 01:28:33	<input type="checkbox"/>	编辑 查看 ...
<input checked="" type="checkbox"/>	1...	HighRiskLevelousCapabilities	.Spec.Template.Spec.Containers.Securit...	高危	2	0	当镜像的拉取策略设定不是Always时，...	内置	2025-01-14 01:28:33	<input type="checkbox"/>	编辑 查看 ...
<input type="checkbox"/>	1...	runAsPrivileged	.Spec.Template.Spec.Containers.Securit...	高危	0	0	当Ingress缺少TLS设定时，检查项不通过	内置	2025-01-14 01:28:33	<input type="checkbox"/>	编辑 查看 ...

4.6.6.4. 编辑规则

说明：

仅支持对自定义规则进行编辑，系统内置规则（创建人为“内置”）不可编辑。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“laC 安全 > 规则管理”，进入规则管理页面。
3. 选择需要添加规则的类型。
4. 在规则列表中找到目标规则，单击操作列的“编辑”。

ID	规则名称	检查项	风险等级	manifests违规文件	chart违规文件	描述	创建人	最后修改时间	启用状态	操作
1...	hostPIDSet	.Spec.Template.Spec.HostPID	高危	2	0	当hostPID属性配置设定时，检查项不...	内置	2025-01-14 01:28:33	<input type="checkbox"/>	编辑 查看 ...
211	test	.Spec.TLS	中危	0	0	当securityContext.runAsUser没有设定非...	c07960e2659b486e8d48ab7e6022645d	2025-01-20 15:55:08	<input checked="" type="checkbox"/>	编辑 查看 ...

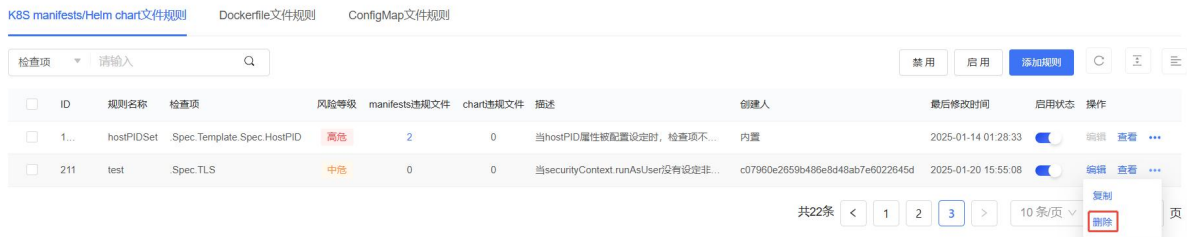
5. 在弹出的窗口中，修改规则参数。参数说明请参见[添加自定义规则](#)。
6. 参数修改完成后，单击“确认”。

4.6.6.5. 删除规则

说明：

仅支持删除自定义规则，系统内置规则（创建人为“内置”）不允许删除。

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“[IaC 安全 > 规则管理](#)”，进入规则管理页面。
3. 选择需要添加规则的类型。
4. 在规则列表中找到目标规则，单击操作列的“删除”。



ID	规则名称	检查项	风险等级	manifests违规文件	chart违规文件	描述	创建人	最后修改时间	启用状态	操作
1...	hostPIDSet	.Spec.Template.Spec.HostPID	高危	2	0	当hostPID属性被配置设定时，检查项不...	内置	2025-01-14 01:28:33	<input checked="" type="checkbox"/>	编辑 查看 ...
211	test	.Spec.TLS	中危	0	0	当securityContext.runAsUser没有设置非...	c07960e2659b486e8d48ab7e6022645d	2025-01-20 15:55:08	<input checked="" type="checkbox"/>	编辑 查看 ...

共22条 < 1 2 3 > 10条/页

5. 在弹出的提示框中，单击“确认”。

4.6.7. 设置

在 IaC 安全的设置管理页面，支持设置是否自动扫描新增的 K8S manifests、Dockerfile、ConfigMap、Helm chart 文件。

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“[IaC 安全 > 设置管理](#)”，进入设置管理页面。
3. 在基本设置页面，打开或关闭自动扫描开关。

设置管理

基本设置

自动扫描

自动扫描新增yaml文件



自动扫描新增dockerfile文件



自动扫描新增configMap文件



自动扫描新增Helm chart文件



保存

4.7. 集群安全

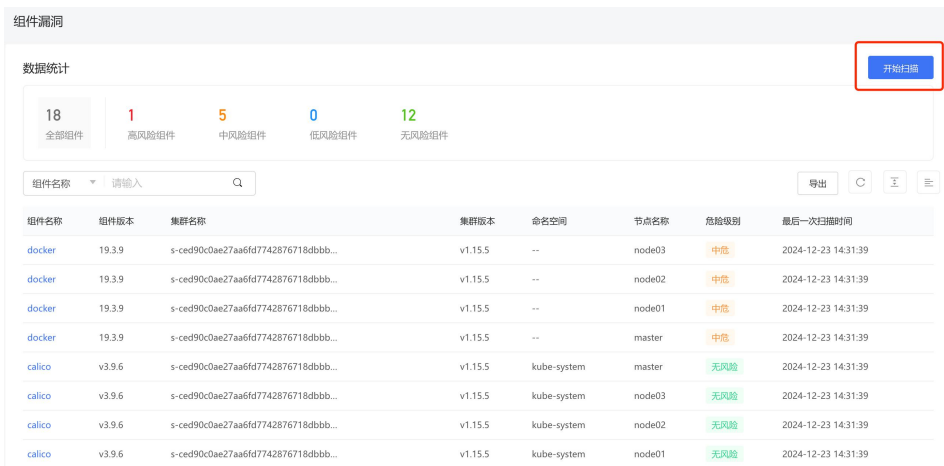
集群安全页面主要对集群的扫描和检查，包括集群内的组件漏洞扫描、集群安全检查、插件管理、集群审计等功能。

4.7.1. 组件漏洞

4.7.1.1. 扫描组件

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“集群安全 > 组件漏洞”，进入组件漏洞页面。
3. 单击组件漏洞列表右上角的“开始扫描”，对集群内的组件进行扫描，获取全部组件漏洞信息。



组件漏洞

数据统计

18 全部组件 | 1 高风险组件 | 5 中风险组件 | 0 低风险组件 | 12 无风险组件

开始扫描

组件名称	组件版本	集群名称	集群版本	命名空间	节点名称	危险级别	最后一次扫描时间
docker	19.3.9	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node03	中危	2024-12-23 14:31:39
docker	19.3.9	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node02	中危	2024-12-23 14:31:39
docker	19.3.9	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node01	中危	2024-12-23 14:31:39
docker	19.3.9	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	master	中危	2024-12-23 14:31:39
calico	v3.9.6	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	master	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node03	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node02	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ces90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node01	无风险	2024-12-23 14:31:39

4. 扫描完成后，即可查看组件漏洞列表。

组件漏洞列表内，支持按照“组件名称”“组件版本”“集群名称”“集群版本”“命名空间”“节点名称”“漏洞编号”进行筛选查询。

组件信息参数说明：

参数	解释说明
组件名称	<p>Kubernetes 集群中的组件主要有以下几类：</p> <ul style="list-style-type: none"> ● 控制平面组件（Control Plane Components）：控制平面的组件对集群做出全局决策(比如调度)，以及检测和响应集群事件。包括 kube-apiserver、etcd、kube-scheduler、kube-controller-manager、cloud-controller-manager 等组件。 ● Node 组件：节点组件在每个节点上运行，维护运行的 Pod 并提供 Kubernetes 运行环境。包括 kubelet、kube-proxy 等组件。 ● 容器运行时（Container Runtime）组件：容器运行时组件是负责运行容器的软件。 ● 第三方插件：插件使用 Kubernetes 资源（DaemonSet、Deployment 等）实现集群功能。因为这些插件提供集群级别的功能，插件中命名空间域的资源属于 kube-system 命名空间。包括 DNS、Dashboard 等组件。
组件版本	组件的版本。
集群名称	组件所属集群的名称。
集群版本	组件所属集群的版本。
命名空间	组件所属命名空间。
节点名称	组件运行所在节点的名称。
漏洞数量	显示组件内存在的不同风险等级的漏洞数量统计信息。
最后一次扫描时间	该组件最后一次被扫描的时间。

4.7.1.2. 查看组件详情

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 组件漏洞”，进入组件漏洞页面。
3. 单击组件列表内的“组件名称”，可查看组件内存在的漏洞信息。

组件名称	组件版本	集群名称	集群版本	命名空间	节点名称	危险级别	最后一次扫描时间
docker	19.3.9	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node03	中危	2024-12-23 14:31:39
docker	19.3.9	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node02	中危	2024-12-23 14:31:39
docker	19.3.9	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	node01	中危	2024-12-23 14:31:39
docker	19.3.9	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	--	master	中危	2024-12-23 14:31:39
calico	v3.9.6	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	master	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node03	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node02	无风险	2024-12-23 14:31:39
calico	v3.9.6	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	node01	无风险	2024-12-23 14:31:39
etcd	3.3.10	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	master	高危	2024-12-23 14:31:39
coredns	1.3.1	s-ced90c0ae27aa6fd7742876718dbbb...	v1.15.5	kube-system	master	无风险	2024-12-23 14:31:39

共18条 < 1 2 > 10条/页 前往 页

4. 进入漏洞信息页面，可查看不同危险等级漏洞的数量统计结果，漏洞详情展示了漏洞类型、漏洞编号、危险级别、软件、受影响的版本等信息。

< 组件名称: docker

2	0	2	0
漏洞总量	高危漏洞	中危漏洞	低危漏洞

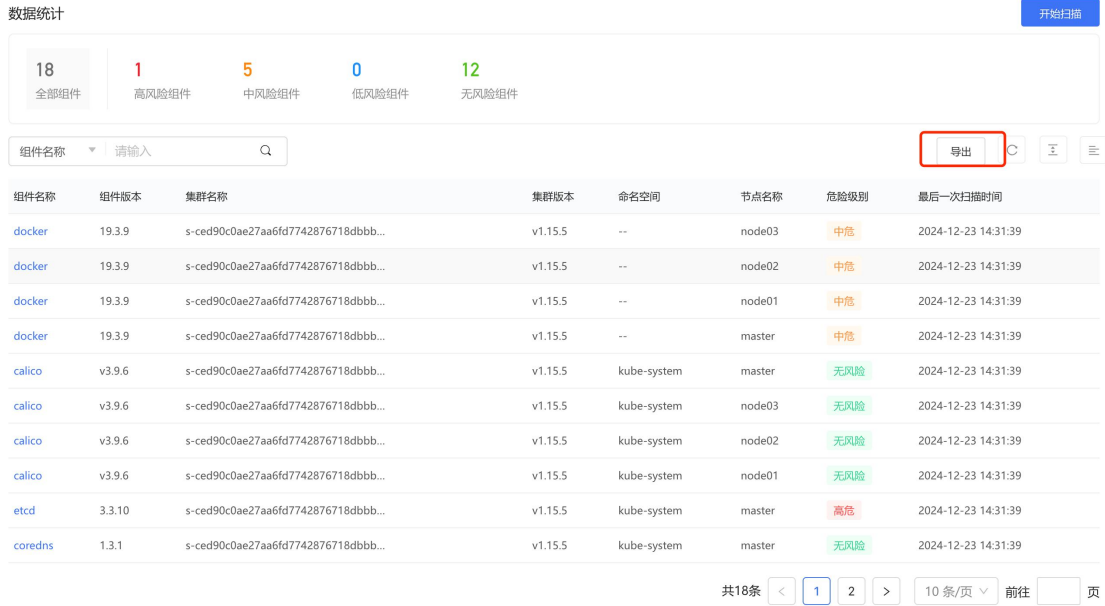
漏洞编号	类型	危险级别	软件	版本
CVE-2021-21285	软件包	中危	docker	<19.03.15;20.0.0<=V<20.10.3;
CVE-2021-21284	软件包	中危	docker	<19.03.15;20.0.0<=V<20.10.3;

共2条 < 1 > 10条/页

5. 单击漏洞详情中的漏洞编号可查看漏洞介绍和参考地址等信息。

4.7.1.3. 生成组件漏洞报表

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 组件漏洞”，进入组件漏洞页面。
3. 单击组件漏洞列表右上角的“导出”按钮，可生成当前集群组件漏洞报表。



4. 到“任务中心 > 下载任务管理”中查看任务状态，当任务状态为“生成完成”时，单击任务操作列的“下载”，可以下载已生成的报表至本地。

4.7.2. 安全检查


4.7.2.1. 集群扫描

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 安全检查”，进入安全检查页面。
3. 单击安全检查列表右上角的“开始扫描”按钮，可对所有集群进行扫描检测。



4.7.2.2. 查看检查结果

查看统计信息

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 安全检查”，进入安全检查页面。
3. 点击数据统计切换按钮 ，可分别查看个检查项的数据统计图和环形图占比。



查看检查结果

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 安全检查”，进入安全检查页面。
3. 在安全检查页面下方，可查看各项检查项的检查结果。

检查项	分类	描述	危害级别	影响节点数量	检查是否通过
Kubernetes版本信息披露	信息披露	您的基础架构正在使用Kubernetes，并...	中危	1	● 不通过
Pod挂载系统日志目录	特权升级	Kubernetes在节点上使用/var/log/pods...	高危	0	● 通过
Etcd远程写访问事件	远程代码执行	Etcd (Kubernetes的数据库)是可写的，...	高危	0	● 通过
存在CVE-2019-11246漏洞	远程代码执行	KubectI被发现容易受到CVE-2019-1124...	高危	0	● 通过
存在CVE-2019-1002101漏洞	远程代码执行	KubectI容易受到CVE-2019-1002101的...	高危	0	● 通过
暴露附加容器	远程代码执行	攻击者可以通过kubelet'/attach'端点上...	高危	0	● 通过
容器内执行任意命令	远程代码执行	攻击者可以通过kubelet的'/run'端点在...	高危	0	● 通过
匿名身份验证	远程代码执行	kubelet被配置为允许对其HTTP api的匿...	高危	0	● 通过
仪表盘暴露	远程代码执行	检测到一个打开的Kubernetes仪表盘。...	高危	0	● 通过
对集群范围内资源的任意访问	特权升级	集群容易受到CVE-2019-11247的漏洞攻...	高危	0	● 通过

共26条 < 1 2 3 > 10条/页 前往

安全检查信息参数说明：

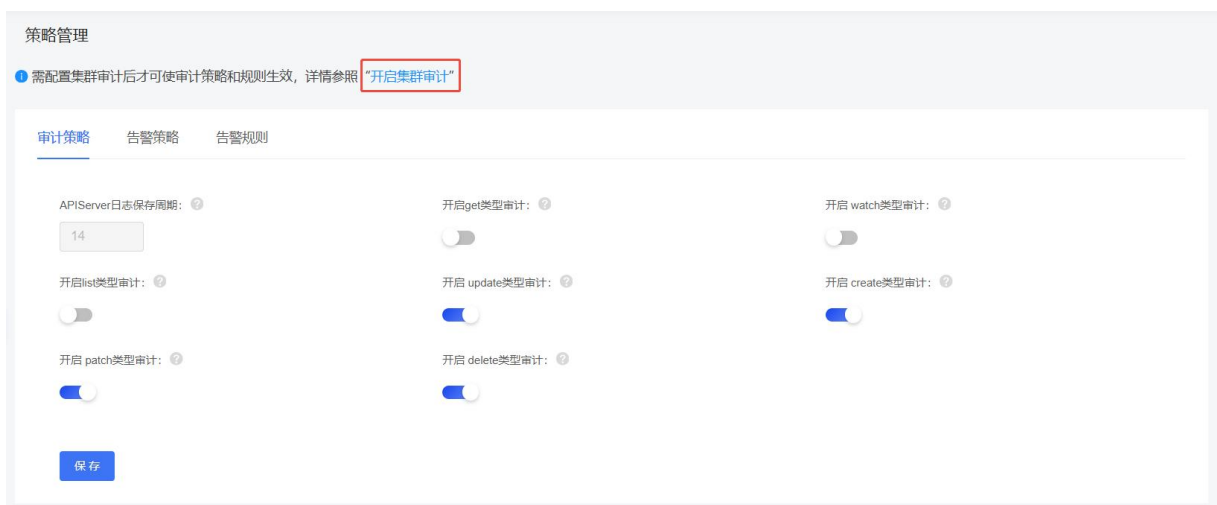
参数	解释说明
检查项	检查项的名称。
分类	检查项所属类型，包括信息泄露、危险访问、远程代码执行、特权升级、拒绝服务等多种类型。
描述	检查项的描述信息。
危害级别	危害级别分为高危、中危、低危。
影响节点数量	受该安全漏洞影响的节点数量。 点击数量，可查看受影响的节点名称。
检查是否通过	集群在该项安全检查中是否通过。

4.7.3. 集群审计

集群审计可以帮助集群管理人员记录或追溯不同用户的日常操作，通过查看、分析审计日志，可以了解集群状态的变更和集群运行状况，排查异常，进而发现集群潜在的安全、性能风险等，及时采取安全防范措施，更好地为集群安全保驾护航。

4.7.3.1. 开启集群审计

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 集群策略”，进入集群策略页面。
3. 单击“开启集群审计”，查看具体的配置方法。



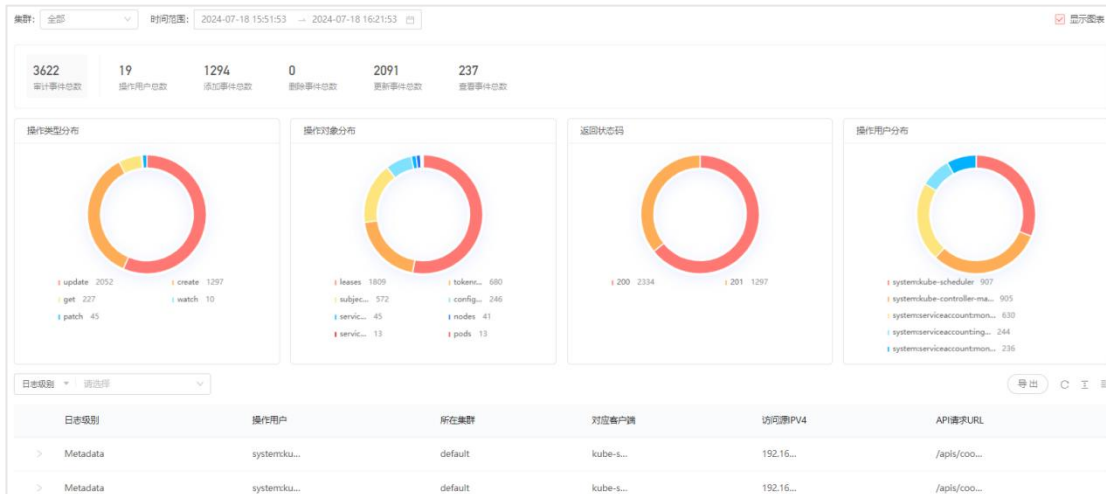
- 选择配置方式，单击对应方式的“查看配置说明”，根据配置说明开启集群审计功能。



4.7.3.2. 查看日志列表

查看事件统计

- 登录容器安全卫士控制台。
- 在左侧导航栏选择“集群安全 > 集群审计”，进入集群审计页面。
- 查看事件统计信息：统计信息分为审计事件总数、操作用户总数、添加事件总数、删除事件总数、更新事件总数、查看事件总数、操作类型分布、资源操作分布、返回状态码、操作用户分布，帮助用户更直观的查看集群内的异常事件分布。



查看日志列表

- 登录容器安全卫士控制台。
- 在左侧导航栏选择“集群安全 > 集群审计”，进入集群审计页面。
- 查看页面下方的审计日志列表，方便用户溯源事件。

日志列表内，支持按照“安全状态”、“日志级别”、“日志所属阶段”、“操作对象”、“操作类型”、“对应客户端”、“客户端节点 IP”、“API 响应状态”进行筛选查询。

日志级别	操作用户	所在集群	对应客户端	访问源IPV4	API请求URL
> Request	system.servi...	s-94bfe...	coredns...	192.168....	/api/v1/serv...
> Metadata	system.apis...	s-94bfe...	kube-ap...	127.0.0.1	/apis/coordi...
> Metadata	system.ano...	s-94bfe...	kube-pr...	192.168....	/readyz
> Metadata	system.ano...	s-94bfe...	kube-pr...	192.168....	/livez
> Metadata	system.servi...	s-94bfe...	Go-http...	192.168....	/apis/crd.pr...
> Metadata	system.kub...	s-94bfe...	kube-sc...	192.168....	/api/v1/na...
> Metadata	system.kub...	s-94bfe...	kube-sc...	192.168....	/apis/coordi...
> Metadata	system.kub...	s-94bfe...	kube-sc...	192.168....	/apis/coordi...
> Metadata	system.kub...	s-94bfe...	kube-co...	192.168....	/apis/coordi...
> Metadata	system.kub...	s-94bfe...	kube-co...	192.168....	/apis/coordi...

共6336条 < 1 2 3 4 5 ... 634 > 10 条/页 前往 页

日志信息参数说明：

参数	解释说明
日志级别	<p>审计日志根据日志策略可以选择事件保存的等级，根据等级不同，APIServer 记录日志的详细程度也不同。目前支持的日志等级有：</p> <p>None：不记录日志。</p> <p>Metadata：只记录 Request 的一些 metadata (例如 user, timestamp, resource, verb 等)，但不记录 Request 或 Response 的 body。</p> <p>Request：记录 Request 的 metadata 和 body。</p> <p>RequestResponse：最全记录方式，会记录所有的 metadata、Request 和 Response 的 Body。</p>
日志所属阶段	<p>审计日志根据日志策略可以选择在事件执行的某个阶段记录，目前支持的事件阶段有：</p> <p>RequestReceived：接收到事件且在分配给对应 handler 前记录。</p> <p>ResponseStarted：开始响应数据的 Header 但在响应数据 Body 发送前记录，这种一般应用在持续很长的操作事件，例如 watch 操作。</p> <p>ResponseComplete：事件响应完毕后记录。</p> <p>Panic：内部出现 panic 时记录。</p>

参数	解释说明
操作对象	操作的资源类型
所在集群	操作对象所属集群
操作类型	<p>操作类型分为 get 获取、watch 监控、list 获取、update 更新、create 创建、patch 修改、delete 删除这些类型。</p> <p>update 和 patch 的区别：update 请求需要将整个修改后的对象提交给 k8s；而 patch 请求只需要将对象中某些字段的修改提交给 k8s。</p>
对应客户端	事件服务的客户端名称（在 userAgent 中定义）。
访问源 IPv6/IPv4	事件服务的客户端所在节点的 IP 地址。
API 响应状态	<p>API 响应状态码分为以下几类：</p> <p>“1XX” 为信息性状态码（informational）。</p> <p>“2XX” 为成功状态码（Success）。</p> <p>“3XX” 为重定向状态码（Redirection）。</p> <p>“4XX” 为客户端错误状态码（Client Error）。</p> <p>“5XX” 为服务端错误状态码。</p> <p>常用的状态码解释说明如下：</p> <p>200：OK，请求成功，具体意义根据请求所使用的方法不同而不同。</p> <p>201：Created，请求成功并创建了资源；</p> <p>403：Forbidden，表示身份认证通过了，但是对服务器请求资源的访问被拒绝了；</p> <p>404：Not Found，表示服务器找不到你请求的资源；</p> <p>409：Conflict，表示请求与服务器当前状态冲突。通常发生在更新资源时，主要是处理并发问题的状态码。</p> <p>500：Internal Server Error，表示服务器执行请求的时候出错了。</p>
API 请求 URL	API 请求 URL 的地址
安全状态	安全状态分为正常和异常这两种，异常是指触发了内置策略的事件
请求时间	事件的请求时间

4. 单击日志列表内的下拉按钮，可展开查看事件的 json 格式详情。

日志级别	操作用户	所在集群	对应客户端	访问源IPV4	API请求URL
Request	system:servi...	s-94bfe...	coredns...	192.168...	/api/v1/serv...
<pre> 1 { 2 "level": "Request", 3 "auditID": "20a99d84-022f-45e1-019f-1b8837dbfd13", 4 "stage": "ResponseStarted", 5 "requestURI": "/api/v1/services?allowWatchBookmarks=true\u0026resourceVersion=2621044\u0026timeout=5m12s\u0026timeoutSeconds=312\u0026watch=true", 6 "verb": "watch", 7 "user": { 8 "username": "system:serviceaccount:kube-system:coredns", 9 "uid": "68d4efde-4994-4e3b-9ac2-39956407234f", 10 "groups": [11 "system:serviceaccounts", 12 "system:serviceaccounts:kube-system", 13 "system:authenticated" 14], 15 "extra": { 16 "authentication.kubernetes.io/nod-name": [</pre>					
Metadata	system:apis...	s-94bfe...	kube-ap...	127.0.0.1	/apis/coordi...
Metadata	system:ano...	s-94bfe...	kube-pr...	192.168...	/readyz
Metadata	system:ano...	s-94bfe...	kube-pr...	192.168...	/livez

4.7.4. 集群策略

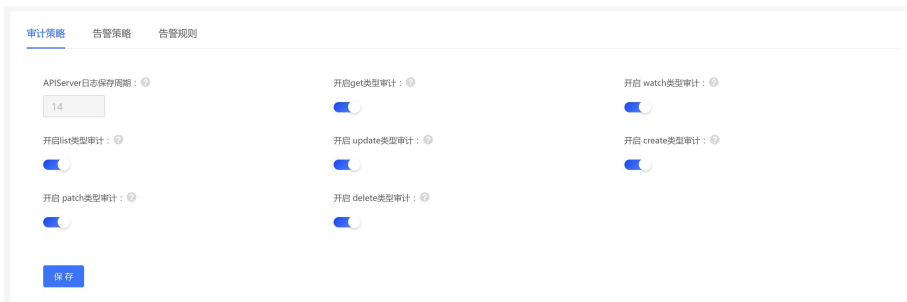
在集群策略页面内，支持配置集群审计策略、告警策略、告警规则。

前提条件

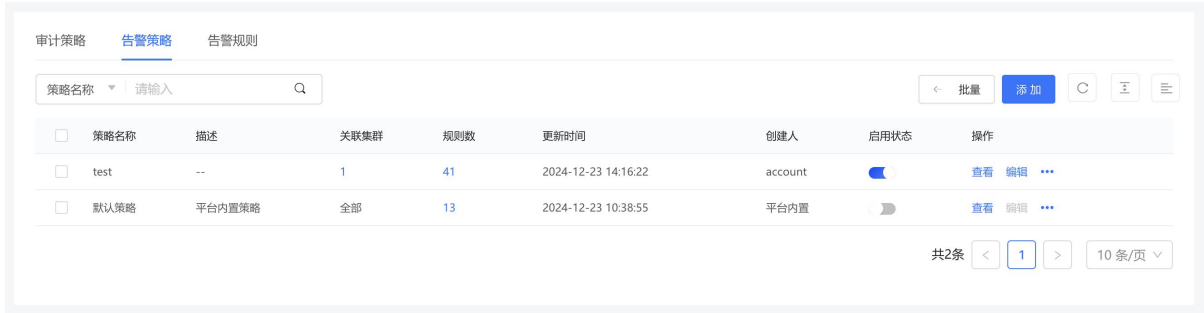
已开启集群审计功能。

操作步骤

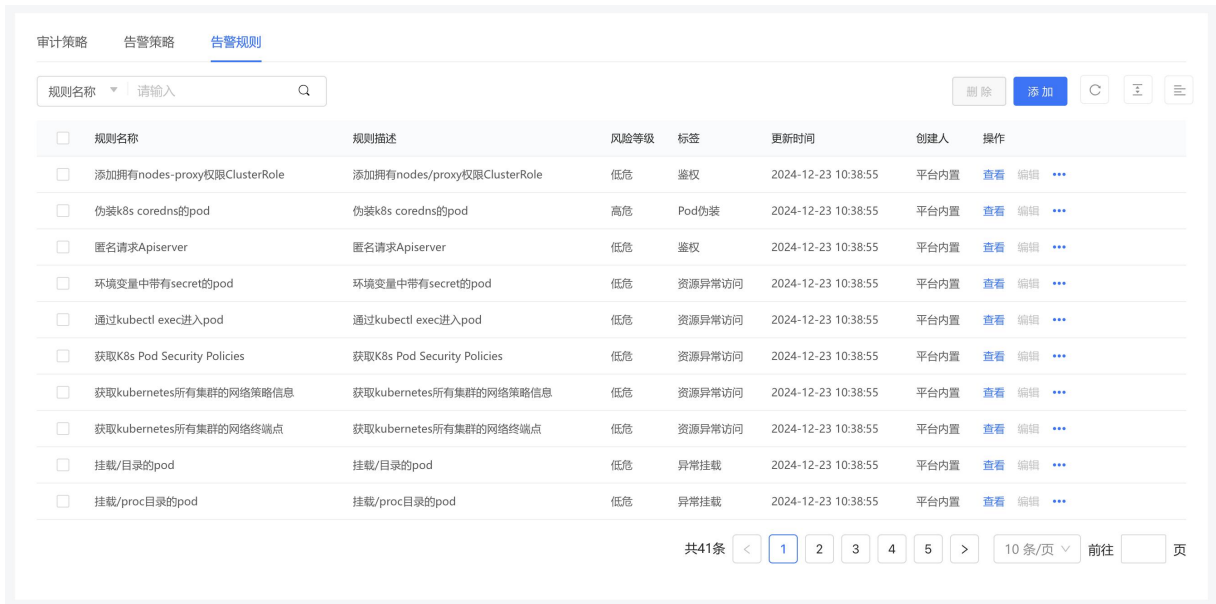
1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“集群安全 > 集群策略”，进入集群策略页面。
3. 配置审计策略：进入“审计策略”页面，可配置审计事件保留周期、审计事件类型。



4. 配置告警策略：进入“告警策略”页面，默认内置日常运营、重保模式、高级防护对应策略。
 点击添加按钮，进入策略添加页面，输入策略名称（必填）、策略描述（非必填）、选择对象、开启规则，点击保存。

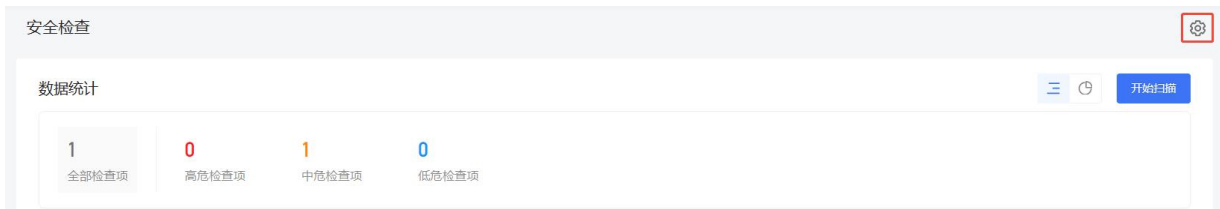


- 配置告警规则：进入“告警规则”页面，点添加按钮，进入规则添加页面，输入规则名称（必填）、规则描述（非必填）、风险等级、att&ck 战术、att&ck 技术、标签、配置规则组，点击保存。

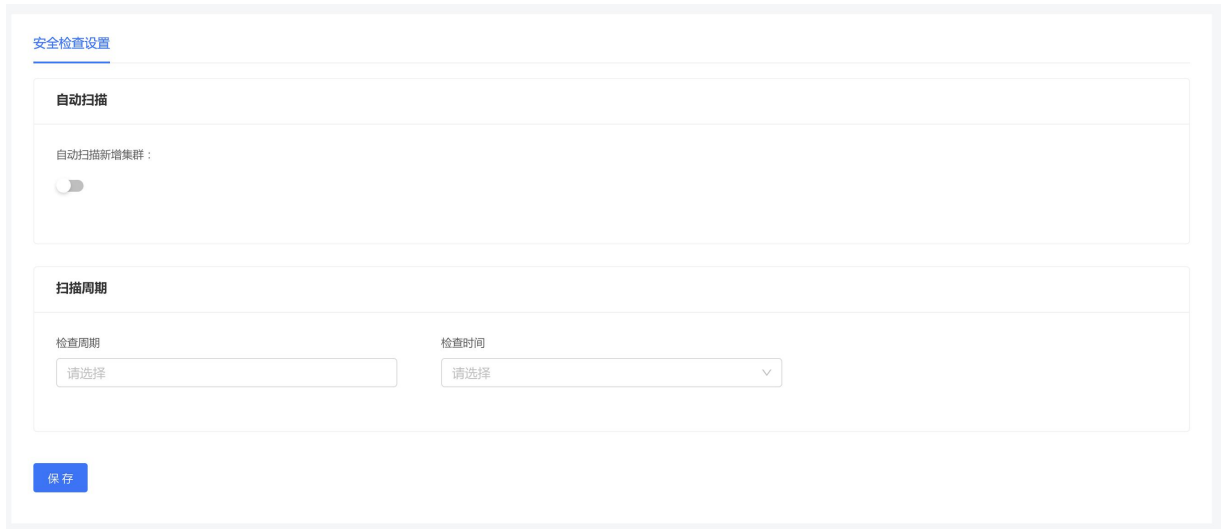


4.7.5. 集群设置

- 登录容器安全卫士控制台。
- 在左侧导航栏选择“集群安全 > 安全检查”，进入安全检查页面。
- 单击页面右上角的设置图标，进入集群设置页面。



- 在基本设置页面内，可以设置自动扫描新增集群、扫描周期。



4.8. 镜像安全

4.8.1. 配置镜像仓库

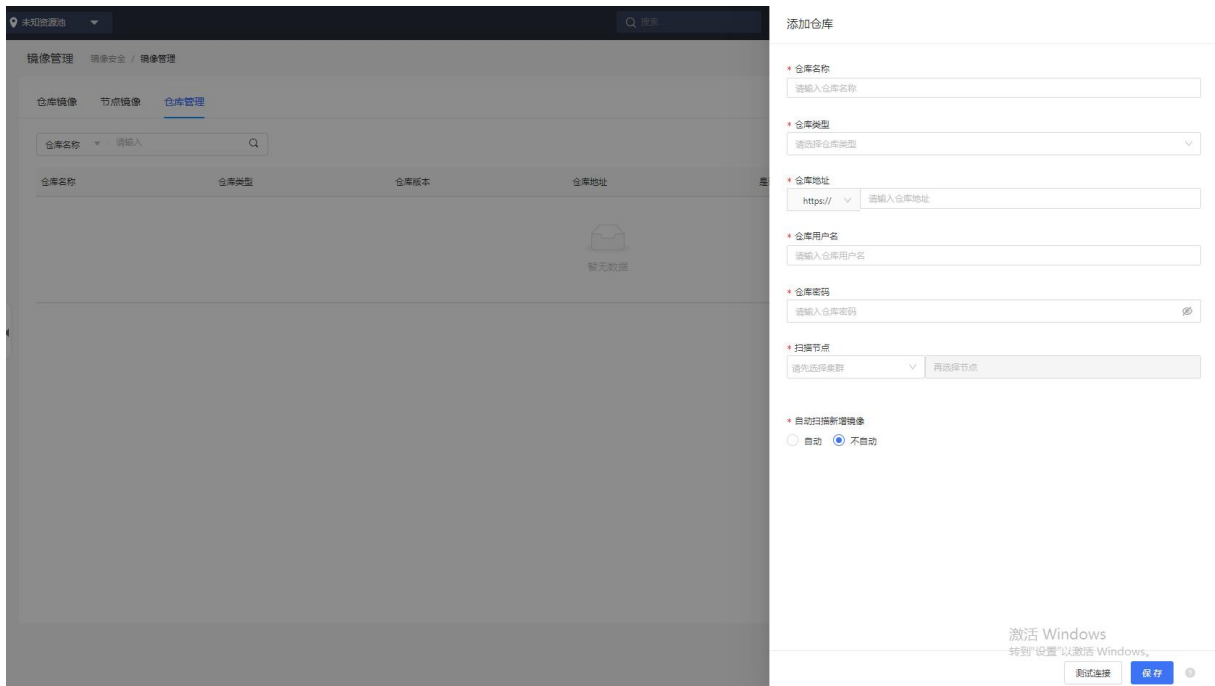
在没有添加镜像之前，页面会提示“暂无仓库镜像信息”。要获取新的仓库镜像列表，首先需要配置镜像仓库。

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。 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。

4.8.2. 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。



更新仓库镜像

请选择仓库镜像更新范围

更新全部仓库镜像

更新单个仓库内的镜像

更新单个仓库项目内的镜像

取消 确定

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。

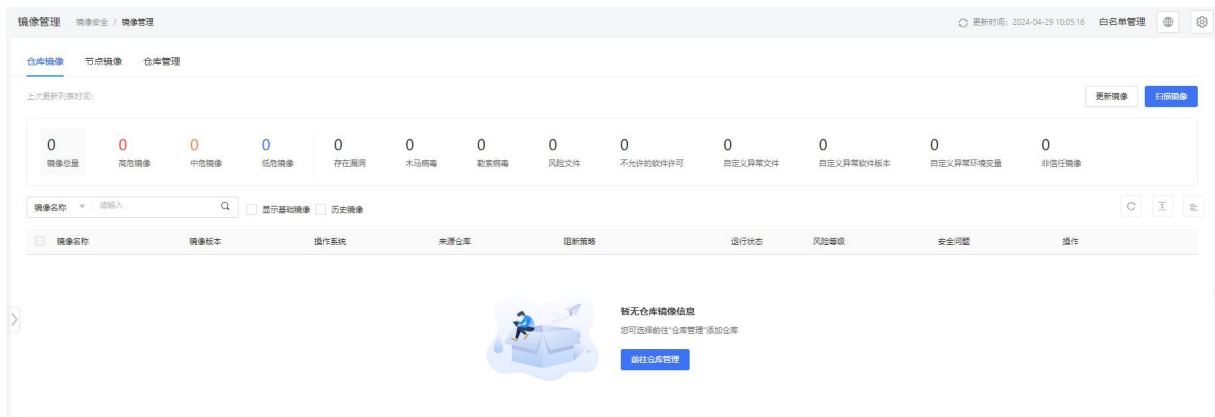
4.8.3. 扫描镜像

镜像扫描支持手动扫描、自动扫描、周期扫描三种方式。

4.8.3.1. 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。

扫描仓库镜像✕

请选择扫描范围处于待扫描状态的镜像不会重复加到队列中

扫描全部仓库镜像

扫描当前筛选仓库镜像

扫描选择项仓库镜像

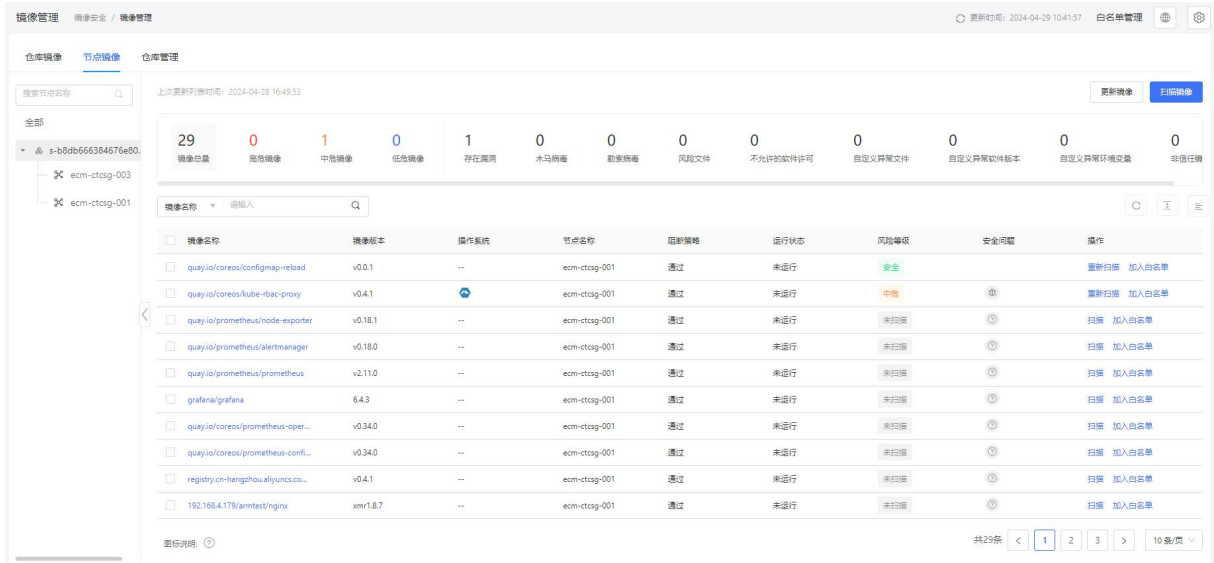
扫描单个仓库内的镜像

扫描单个仓库项目内的镜像

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。

4.8.3.2. 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。



4.8.3.3. 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。



4.8.4. 查看扫描状态

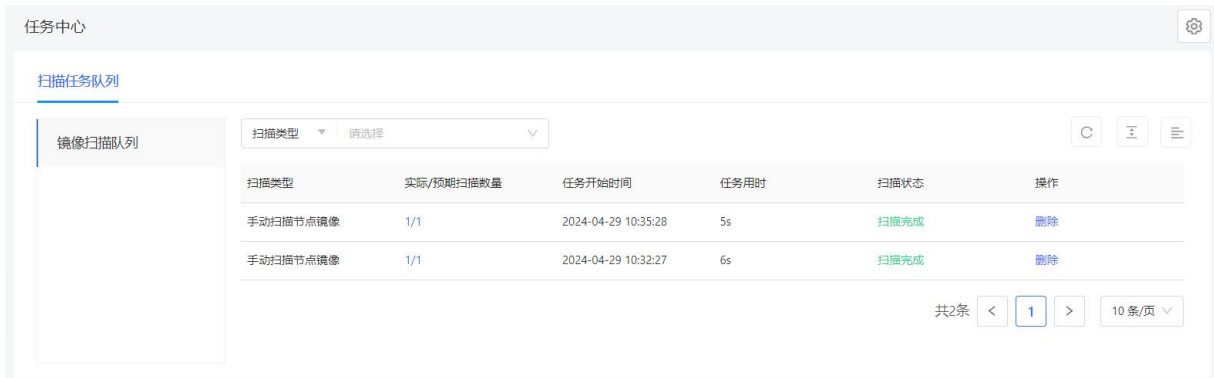
执行镜像扫描操作后，可通过“任务中心”查看镜像扫描任务的状态。

- 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。



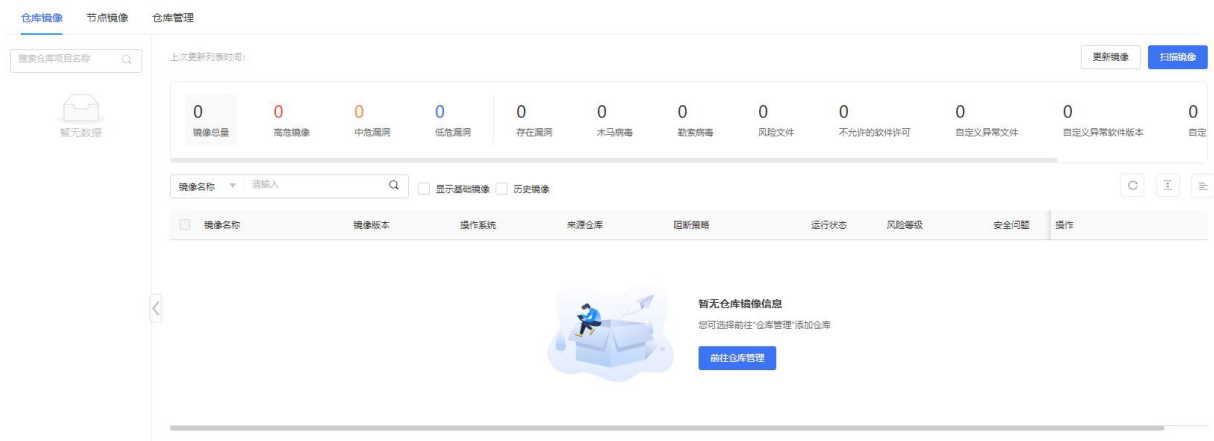
说明：

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。

4.8.5. 查看扫描结果

4.8.5.1. 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。

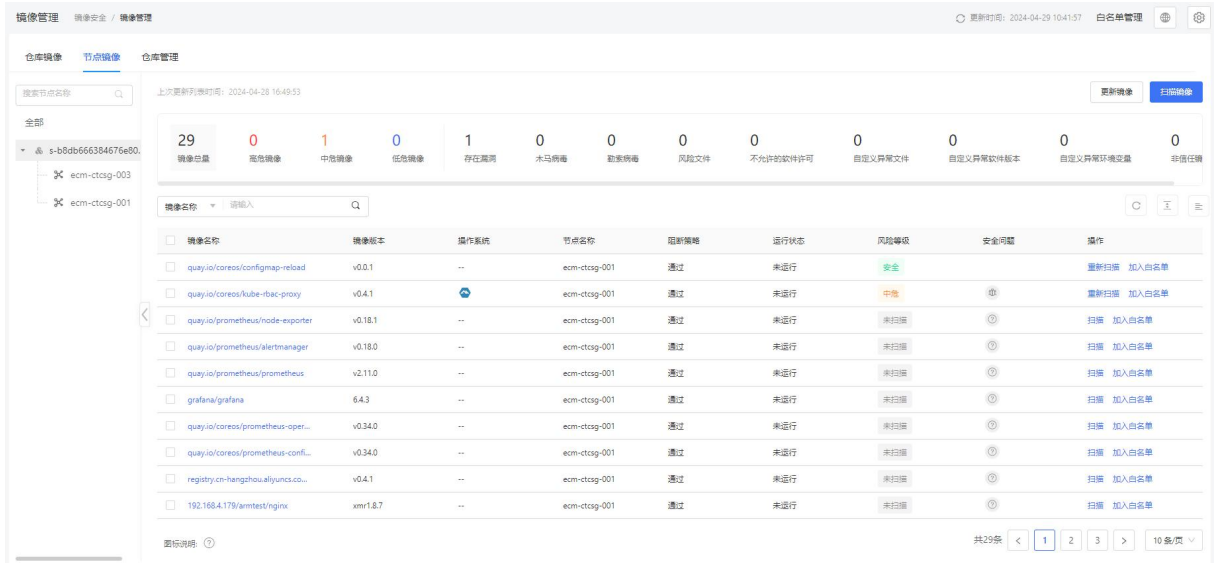
5. 仓库镜像列表内，支持按照“镜像名称”、“镜像 ID”、“镜像版本”、“软件名称”、“软件版本”、“漏洞编号”、“阻断策略”、“风险等级”、“安全问题”进行筛选查询。

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，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。 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。

4.8.5.2. 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。 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。

4.8.5.3. 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。

📄 基本信息

Image ID: sha256:70eeaa7791f218b7... [展开](#)

版本: v0.4.1

大小: 39.4MiB

入库时间: 2024-04-28 16:49:56

[摘要](#) [关联信息](#) [漏洞](#) [软件](#) [文件](#) [环境变量](#) [安全溯源](#)

风险评分



75分

中危

漏洞 🔍	-25
文件 🔍	0
软件包 🔍	0
环境变量 🔍	0
可信镜像 🔍	0

安全问题							
重点关注漏洞	自定义异常文件	自定义异常软...	自定义异常环...	木马病毒	风险文件	不允许的软件...	可信镜像
0	0	0	0	0	0	0	是

镜像命中的安全策略
镜像命中了0安全策略

安全建议
漏洞修复建议
请在该镜像的Dockerfile文件中添加如下代码,以修复存在安全问题的软件: RUN apk add -u --no-cache musl=1.1.19-r11 musl-utils=1.1.19-r11

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。

← | 详情 镜像安全 / 镜像名称:library/dosec-agent

基本信息

Image ID: sha256:d7553a2502b3d7c75a88c8ecbba09819c106... [展开](#) 版本: build-2023-08-01T16.45.45V3.5.0_dev_88847a

大小: 449.3MiB 入库时间: 2023-08-01 17:08:48

摘要 **关联容器** 漏洞 软件 文件 环境变量 安全溯源 基线检查

容器名称 ▾ | 请输入 🔍 🔄 📄 ☰

容器名称	Pod名称	集群名称	节点名称
暂无数据			

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。

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... [展开](#)

大小: 171.1MiB

版本: xmr1.8.7

入库时间: 2023-07-31 15:06:53

摘要
关联信息
漏洞
软件
文件
环境变量
安全溯源
基线检查

292

漏洞总量

9

高危漏洞

161

中危漏洞

122

低危漏洞

漏洞编号

▼

请输入

🔍

仅关注可修复的漏洞

☰

类型	漏洞编号	危险级别	风险特征	软件	当前版本	已修复版本	命中安全策略	操作
软件包	CVE-2022-25235	高危	🔒 🗑️	expat	2.2.5-3ubun...	2.2.5-3ubun...	1	加入白名单
软件包	CVE-2022-25236	高危	🔒 🗑️	expat	2.2.5-3ubun...	2.2.5-3ubun...	1	加入白名单
软件包	CVE-2021-33910	高危	🗑️ 🛡️	systemd	237-3ubunt...	237-3ubunt...	1	加入白名单
软件包	CVE-2022-24407	高危	🗑️	cyrus-sasl2	2.1.27-101-g...	2.1.27-101-g...	1	加入白名单

- 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。

漏洞信息 命中安全策略

CVND 编号

CVND-202310-667

漏洞类型

逆序管理错误

漏洞介绍

HTTP/2是超文本传输协议的第二版，主要用于保证客户端与服务端之间的通信。Apache HTTP/2存在安全漏洞，攻击者利用该漏洞导致系统的拒绝服务。以下产品和版本受到影响：.NET 6.0,ASP.NET Core 6.0,.NET 7.0,Microsoft Visual Studio 2022 version 17.2,Microsoft Visual Studio 2022 version 17.6,Microsoft Visual Studio 2022 version 17.7,Windows 10 Version 1809 for 32-bit Systems,Windows 10 Version 1809 for x64-based Systems,Windows 10 Version 1809 for ARM64-based Systems,Windows Server 2019 (Server Core installation),Windows Server 2022 (Server Core installation),Windows 11 version 21H2 for x64-based Systems,Windows 11 version 21H2 for ARM64-based Systems,Windows 10 Version 21H2 for 32-bit Systems,Windows 10 Version 21H2 for ARM64-based Systems,Windows 10 Version 21H2 for x64-based Systems,Windows 11 Version 22H2 for ARM64-based Systems,Windows 10 Version 22H2 for x64-based Systems,Windows 10 Version 22H2 for ARM64-based Systems,Windows 10 Version 22H2 for 32-bit Systems,Windows 10 Version 1607 for 32-bit Systems,Windows 10 Version 1607 for x64-based Systems,Windows Server 2016,Windows Server 2016 (Server Core installation),ASP.NET Core 7.0.

漏洞信息 命中安全策略

策略名称	创建者	规则名称	描述
<div style="border: 1px solid #ccc; width: 40px; height: 40px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> </div> <p>暂无数据</p>			

- 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。

内置项目

详情 镜像安全 / 镜像名称:hub.dosec.cn/test/nginx

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... 展开

大小: 171.1MiB

摘要 关联信息 **漏洞** 软件 文件 环境变量 安全溯源

292 漏洞总量 9 高危漏洞 161 中危漏洞 122 低危漏洞

漏洞编号 请输入 仅关注可修复的漏洞

类型	漏洞编号	危险级别	风险特征
软件包	CVE-2022-25235	高危	<input type="checkbox"/>
软件包	CVE-2022-25236	高危	<input type="checkbox"/>
软件包	CVE-2021-33910	高危	<input type="checkbox"/>
软件包	CVE-2022-24407	高危	<input type="checkbox"/>

加入白名单

* 白名单名称

选择对象:

漏洞编号

镜像

节点

仓库

描述:

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。

详情 镜像安全 / 镜像名称:hub.dosec.cn/test/nginx

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... 展开 版本: xmr1.8.7

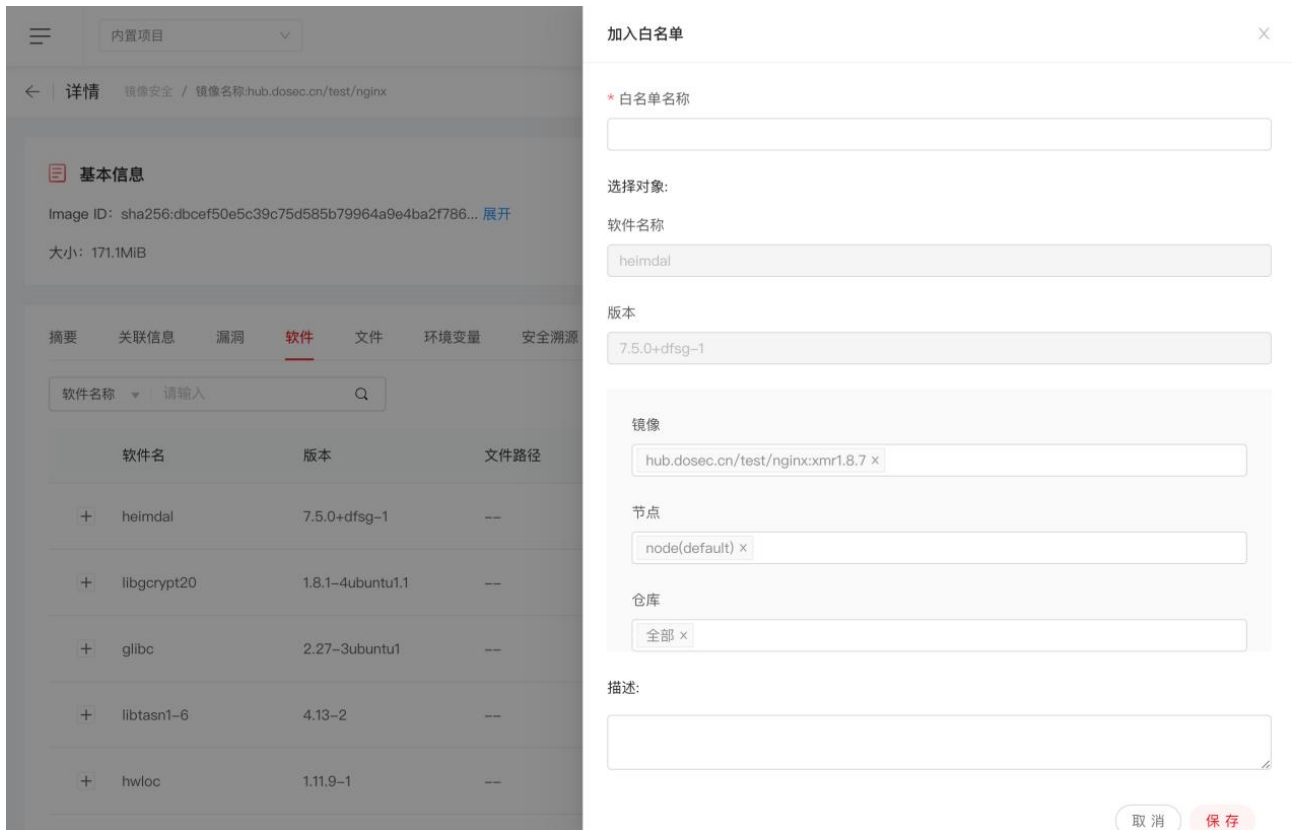
大小: 171.1MiB 入库时间: 2023-07-31 15:06:53

摘要 关联信息 漏洞 **软件** 文件 环境变量 安全溯源 基线检查

软件名称 请输入

软件名	版本	文件路径	类型	漏洞数量	命中安全策略	操作	
+	heimdal	7.5.0+dfsg-1	--	dpkg	高0 中8 低2	0	加入白名单
+	libcrypt20	1.8.1-4ubuntu1.1	--	dpkg	高0 中2 低1	0	加入白名单
+	glibc	2.27-3ubuntu1	--	dpkg	高0 中5 低13	0	加入白名单
+	libtasn1-6	4.13-2	--	dpkg	高0 中0 低0	0	加入白名单
+	hwloc	1.11.9-1	--	dpkg	高0 中0 低0	0	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。

← 详情 镜像安全 / 镜像名称:hub.dosec.cn/test/nginx

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... [展开](#) 版本: xmr1.8.7
大小: 171.1MiB 入库时间: 2023-07-31 15:06:53

摘要 关联信息 漏洞 软件 **文件** 环境变量 安全溯源 基线检查

文件名

文件名	文件路径	类型	命中引擎	命中安全策略	操作
info.txt(挖矿病毒)	/mnt/xmrig-6.6.2/info.txt	木马病毒 🚫	自研引擎	1	加入白名单 下载
Oxdeadbeef(恶意软件)	/mnt/Oxdeadbeef	木马病毒 🚫	自研引擎	1	加入白名单 下载
xmrig(malware)	/mnt/xmrig	木马病毒 🚫	自研引擎	1	加入白名单 下载
COPYING(GPL-2.0)	/usr/share/doc/git/contrib/subtree/COPYING	软件许可	自研引擎	0	加入白名单 下载
LICENSE(Apache-2.0)	/usr/share/doc/git/contrib/persistent-https...	软件许可	自研引擎	0	加入白名单 下载

共5条 < 1 > 10条/页

- 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。

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... [展开](#) 版本: xmr1.8.7
大小: 171.1MiB 入库时间: 2023-07-31 15:06:53

摘要 关联信息 漏洞 软件 文件 **环境变量** 安全溯源 基线检查

变量名

变量名	变量值	命中安全策略	操作
暂无数据			

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。

基本信息

Image ID: sha256:dbcef50e5c39c75d585b79964a9e4ba2f786... [展开](#) 版本: xmr1.8.7
大小: 171.1MiB 入库时间: 2023-07-31 15:06:53

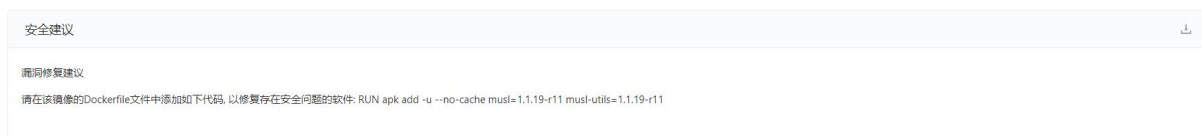
摘要 关联信息 漏洞 软件 文件 环境变量 **安全溯源** 基线检查


- 2020-12-23 12:35:41
层ID: 47f44b777bc35518200f2049b1aefed6b88ddea10b427b02be2f629a5c8f5a1b
命令: /bin/bash
引入的风险点: [+ 文件](#)
- 2020-05-13 21:46:40
层ID: 9e1ba212bb1731dc5524d755bb81ded3ede1f1a67f2577099d07cac823f49428
命令:
引入的风险点: [+ 漏洞](#) [+ 软件](#) [+ 文件](#)

4.8.6. 处置镜像

4.8.6.1. 修复漏洞

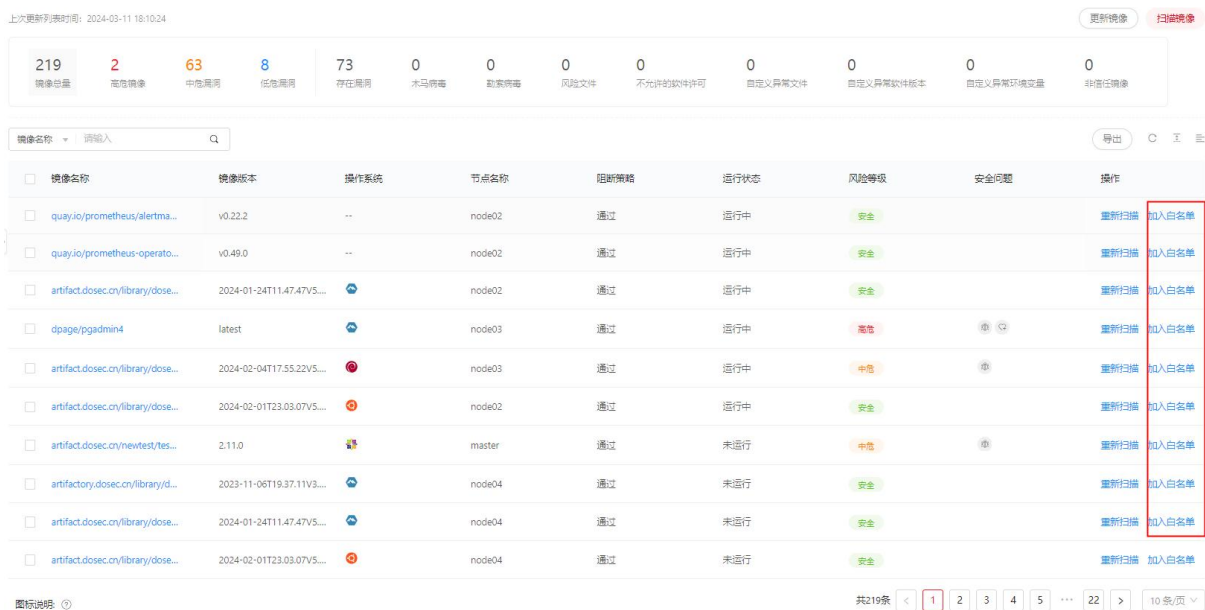
1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“镜像安全 > 镜像管理”，进入镜像管理页面。
3. 选择“仓库镜像”或“节点镜像”页签，进入对应镜像列表页面。
4. 单击镜像列表中的“镜像名称”，进入镜像详情页面。
5. 在镜像详情页面的“摘要”页签底部，可以查看漏洞“安全建议”，为用户提供了漏洞的修复建议和异常文件处理建议，包括具体的做法和代码。



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。

4.8.6.2. 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。

加入白名单
✕

*** 白名单名称**

选择对象:

镜像

quay.io/coreos/configmap-reload:v0.0.1

节点

ecm-ctcsg-001(s-b8db666384676e80c69c33517cabba89) ✕

仓库

全部 ✕

描述:

取消

保存

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。

4.8.6.3. 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。

镜像名称	镜像版本	操作系统	来源仓库	阻断策略	运行状态	风险等级	安全问题	操作
<input type="checkbox"/> web/mono	slim	--	4.99-harbor	通过	未知	未扫描	🔍	扫描 加入白名单 更多 ▾
<input type="checkbox"/> web/mono	latest	--	4.99-harbor	通过	未知	未扫描	🔍	扫描 加入白名单 更多 ▾
<input type="checkbox"/> web/mono	6.8.0.96-slim	--	4.99-harbor	通过	未知	未扫描	🔍	扫描 加入白名单 更多 ▾
<input type="checkbox"/> web/mono	6.8.0.96	--	4.99-harbor	通过	未知	未扫描	🔍	扫描 加入白名单 更多 ▾ 设为基础镜像

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。

4.8.7. 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。

加入白名单 X

*** 白名单名称**

*** 白名单类型**

镜像 v

选择对象

镜像 v

节点 v

仓库 v

描述

取消 保存

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。

4.8.8. 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。



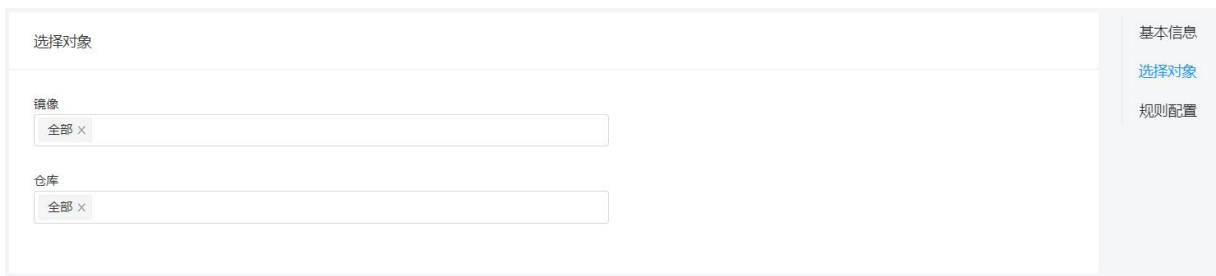
添加策略

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。

4.8.9. 镜像设置

4.8.9.1. 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。



扫描周期设置

节点镜像扫描周期

检查周期:

检查时间:

镜像名匹配:

镜像版本匹配:

仓库镜像扫描周期

检查周期:

检查时间:

镜像名匹配:

镜像版本匹配:

4. 配置完成后，单击“保存”。

4.8.9.2. 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](#)。

扫描设置 **可信镜像** 风险评分

非可信镜像设置

对非信任镜像做的动作: ?

忽略 报警 阻断

可信镜像设置

指定可信任的仓库:

全部 x v

指定可信任的基础镜像:

全部 x v

指定可信任的镜像:

全部 x v

保存

4. 配置完成后，单击“保存”。

4.8.9.3. 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。

评分项目	评分项	扣分值	项目最大扣分
漏洞	高危漏洞	<input type="text" value="25"/>	35
	中危漏洞	<input type="text" value="15"/>	
	低危漏洞	<input type="text" value="5"/>	
	重点关注漏洞	<input type="text" value="35"/>	
文件	木马病毒	<input type="text" value="35"/>	35
	风险文件	<input type="text" value="10"/>	
软件包	自定义异常文件	<input type="text" value="35"/>	10
	不允许的软件许可	<input type="text" value="10"/>	
环境变量	自定义异常软件版本	<input type="text" value="10"/>	10
	自定义异常环境变量	<input type="text" value="10"/>	
可信镜像	非信任镜像	<input type="text" value="10"/>	10
合计			100

安全分值说明

- 95分以上: 镜像安全
- 85-94分: 镜像存在安全隐患, 建议修复
- 70-84分: 镜像存在较多的安全隐患, 建议及时修复
- 70分以下: 镜像防御黑客入侵的能力很弱, 建议立即修复

① 各评分项存在即扣分, 单项目扣分不会超过项目最大扣分值

保存

4. 配置完成后, 单击“保存”。

4.9. 容器安全

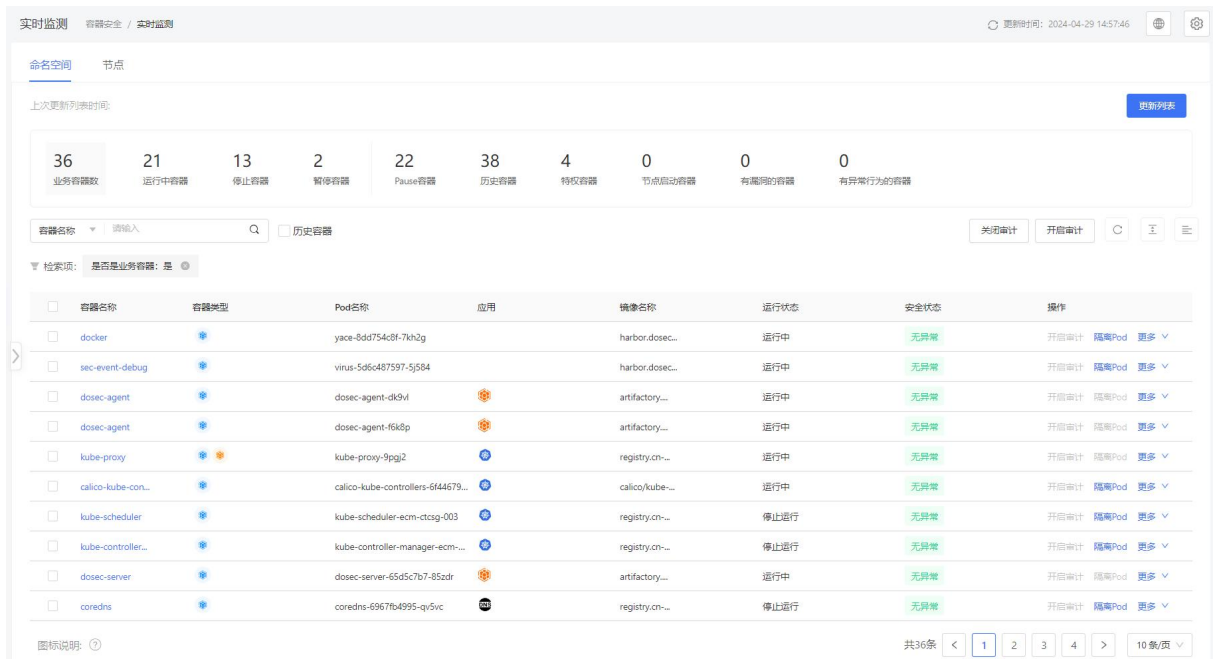
4.9.1. 更新容器列表

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。

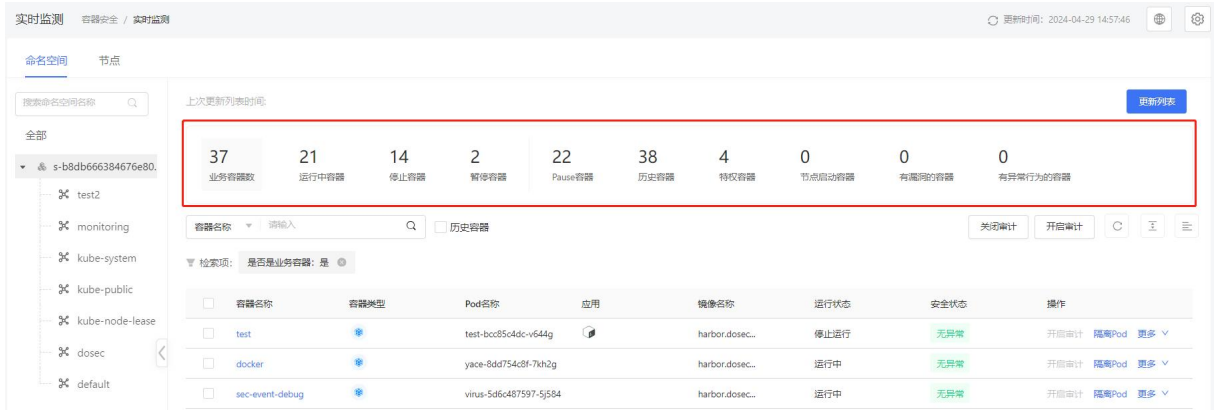
操作步骤

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。

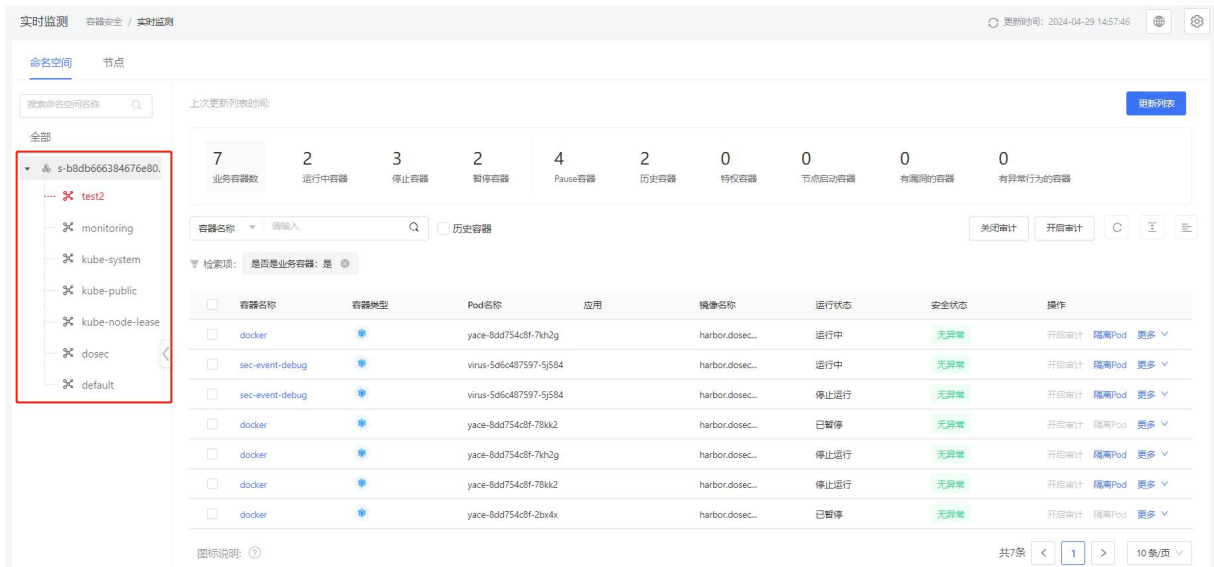


4.9.2. 查看容器列表

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。



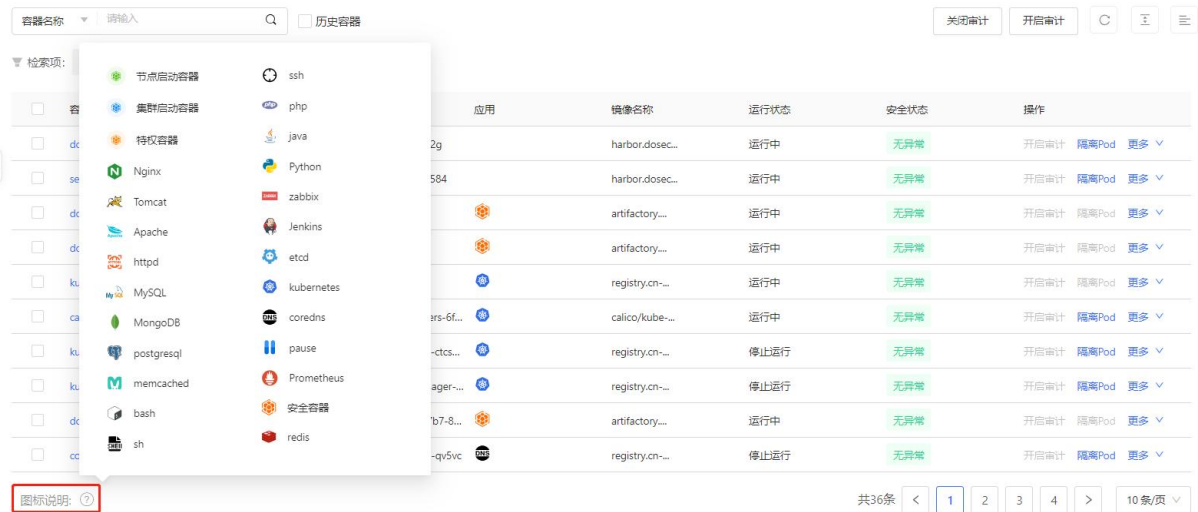
6. 查看容器列表：容器列表内，支持按照“容器名称”、“镜像名称”、“Pod 名称”、“容器标签”、“容器 IP”、“容器类型”、“运行状态”、“安全状态”等进行筛选查询。

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	安全状态分为“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。

- 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。



4.9.3. 查看容器详情

进入容器详情页面

- 登录容器安全卫士控制台。
- 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。
- 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。

上次更新列表时间:

更新列表

36	21	13	2	22	39	4	0	0	0
业务容器数	运行中容器	停止容器	暂停容器	Pause容器	历史容器	特权容器	节点启动容器	有漏洞的容器	有异常行为的

容器名称 请输入 历史容器

检索项: 是否是业务容器: 是

<input type="checkbox"/>	容器名称	容器类型	Pod名称	应用	镜像名称	运行状态	操作
<input type="checkbox"/>	docker		yace-8dd754c8f-7kh2g		harbor.dosec...	运行中	开启审计 隔离Pod 更多
<input type="checkbox"/>	sec-event-debug		virus-5d6c487597-5j584		harbor.dosec...	运行中	开启审计 隔离Pod 更多
<input type="checkbox"/>	dosec-agent		dosec-agent-dk9vl		artifactory...	运行中	开启审计 隔离Pod 更多

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。

← 容器名称:docker 容器安全 / 详情

基本信息

容器ID: e27f3dbf001b4ee40d99c8169...	容器类型: 集群启动容器	运行用户: root	集群: s-b8db666384676e90c69c335...
镜像: harbor.dosec.cn/newtest/...	节点: ecm-ctcsg-001	Pod名称: yace-8dd754c8f-7kh2g	节点状态: 已开启
命名空间: test2	应用类型: --	节点PV4地址: 192.168.0.159	节点PV6地址: --
内存限制: 无限制	CPU限制: 无限制	容器标签: pod-template-hash=8dd754c...	容器PV4地址: 10.200.75.226
容器PV6地址: --			

摘要 容器审计 进程 端口 数据挂载 软件 配置

运行情况

运行状态: 运行中	本次启动时间: 2024-04-29 07:33:36	Pod重启次数: --
上次停止时间: --	隔离状态: 未隔离	启动进程参数: 1000000
启动进程路径: sleep	CPU占用: 0.00m	内存占用: 0.09MB

安全状态

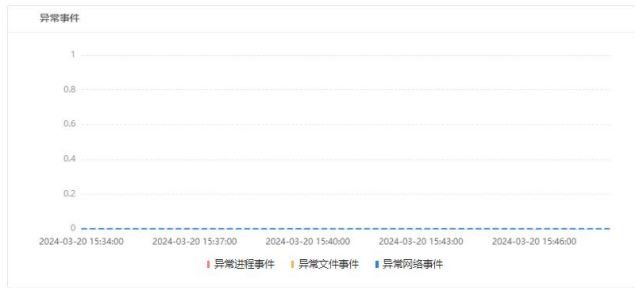
安全状态: 无异常	是否为特权启动: 否
-----------	------------

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。

选择时间: 2024-03-20 15:34 ~ 2024-03-20 15:48

下载图片



内容 请输入

导出

进程名称	用户	路径	事件类型	安全状态	时间
>	root	--	网络事件	正常	2024-03-20 15:47:22
>	root	--	网络事件	正常	2024-03-20 15:47:22
>	root	--	网络事件	正常	2024-03-20 15:47:12
>	root	--	网络事件	正常	2024-03-20 15:47:12
>	root	--	网络事件	正常	2024-03-20 15:47:02
>	root	--	网络事件	正常	2024-03-20 15:47:02

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。

进程名称 请输入

导出

进程名称	父进程ID	进程ID	启动用户	运行时间	更新时间
calico-node	106153	106155	root	2024-03-08 15:28:05	2024-03-20 14:58:34
runsv	106021	106153	root	2024-03-08 15:28:05	2024-03-20 14:58:34
bird6	106152	106314	root	2024-03-08 15:28:05	2024-03-20 14:58:34
runsv	106021	106152	root	2024-03-08 15:28:05	2024-03-20 14:58:34
bird	106151	106316	root	2024-03-08 15:28:05	2024-03-20 14:58:34
runsv	106021	106151	root	2024-03-08 15:28:05	2024-03-20 14:58:34
calico-node	106150	106157	root	2024-03-08 15:28:05	2024-03-20 14:58:34
runsv	106021	106150	root	2024-03-08 15:28:05	2024-03-20 14:58:34

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。

进程 请输入

导出

容器端口	进程	节点端口	IPv4	IPv6	绑定IP	协议	PID	运行用户
------	----	------	------	------	------	----	-----	------



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，会造成敏感信息泄露的风险，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。
UsersMode	--	无
ReadOnlyRootfs	false	容器读写根文件系统，会造成根文件的损坏，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:fb0a164eed5b011753daad0beebfd2202731517d06a95deed5add8fd2025e88	无
NetworkMode	container:fb0a164eed5b011753daad0beebfd2202731517d06a95deed5add8fd2025e88	无

4.9.4. 处置风险容器

4.9.4.1. 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

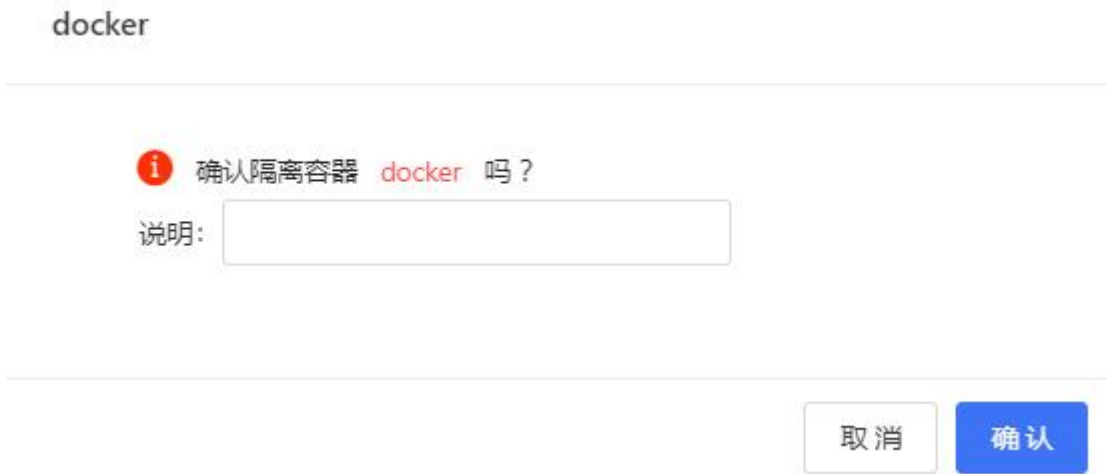
特权容器、节点启动容器、安全容器、pause 应用类型容器暂不支持隔离。

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。

4.9.4.2. 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”。

4.9.4.3. 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。

4.9.5. 容器审计

4.9.5.1. 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。

组件安装 安装配置 / 组件安装 更新时间: 2024-04-29 11:25:35

集群组件安装

集群名称: 部署脚本 C 刷新 更多

集群名称	集群状态	Master地址	防御容器在线/总数	部署时间	部署状态	操作
s-b8db666384676...	● 在线	192.168.0.160	1/2	--	后台部署	集群组件配置 下载日志 更多

共1条 < 1 > 10条/页

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。

集群名称: s-b8db666384676e80c69c33517cabba89 ×

全局设置

单个镜像扫描超时 分钟
单个镜像扫描超时默认为10分钟

节点扫描的并发数 ↑
各节点镜像并发扫描数量默认为1, 不可配置

仓库镜像扫描并发数 ↑
各仓库镜像并发扫描数量默认为1且最高数量不超过3个

防御容器设置

开启镜像阻断
开启镜像阻断功能, 才能对异常镜像进行阻断

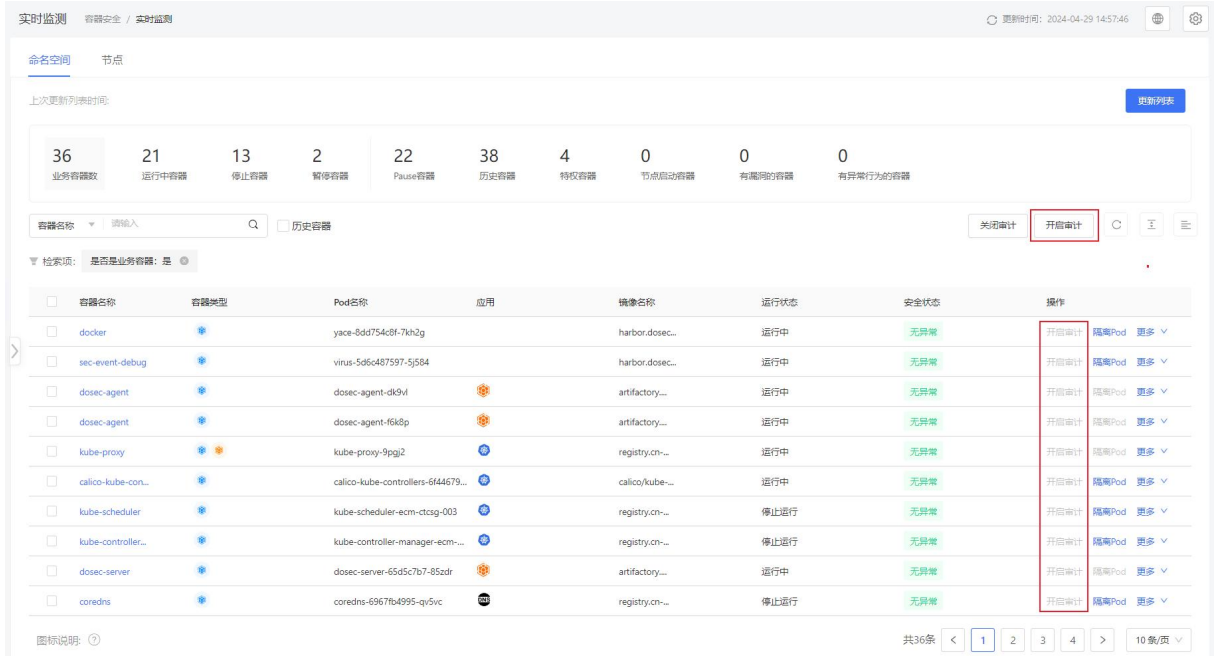
开启入侵检测模块
开启入侵检测模块, 才能对容器的入侵检测行为进行报警

开启容器审计功能
开启容器审计功能后, 会记录大量事件, 占用较大的磁盘空间。

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](#)。

4.9.5.2. 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。

内容	用户	路径	事件类型	安全状态	时间
> awk	dosec	/usr/bin/mawk	进程事件	正常	2023-08-01 18:34:07
详情					
类型：进程事件	用户：dosec	时间：2023-08-01 18:34:07			
进程名称：awk	进程路径：/usr/bin/mawk	进程命令行：awk {print \$1,\$2}			
> tail	dosec	/usr/bin/tail	进程事件	正常	2023-08-01 18:33:37
> ps	dosec	/usr/bin/ps	进程事件	正常	2023-08-01 18:33:36

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。 <ul style="list-style-type: none"> 进程事件：指在容器中运行进程的事件； 文件事件：指容器中对文件的读操作和写操作产生的事件； 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。

4.9.6. 容器策略管理

4.9.6.1. 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。

基本信息

* 策略名称

请输入

描述

请输入

* 策略标签

请输入

* 是否启用

是 否

5. 选择策略应用的对象。

选择对象

全部(2/8)

集群 请输入 Q

- s-b8db666384676e80c69c33517cabba89
 - 全部命名空间
 - kube-system
 - kube-public
 - kube-node-lease
 - dosec
 - default
 - test2
 - monitoring

已选(2) 清空

命名空间	所属集群	
kube-system	s-b8db666384676e80c69c33517c...	×
kube-public	s-b8db666384676e80c69c33517c...	×

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。

规则配置

命令执行 | 读写文件 | 网络活动 | 文件内容

规则名称 请输入 处置方式: 请选择处置方式

<input type="checkbox"/>	风险等级	规则名称	告警信息	描述	是否使用	创建人	自定义对象	处置方式
<input type="checkbox"/>	提示	添加setuid权限	setuid可以使执行者...	为文件添加setuid权限	<input checked="" type="checkbox"/>	系统内置		只报警
<input type="checkbox"/>	紧急	容器内proc目录被挂...	runc不允许容器内/p...	发现容器内的/proc...	<input type="checkbox"/>	系统内置		只报警
<input type="checkbox"/>	紧急	疑似特权容器挂载设...	特权容器内黑客可疑...	发现可疑进程，疑似...	<input type="checkbox"/>	系统内置		只报警

仅系统内置策略支持配置“主机异常”规则：

规则配置

命令执行 | 读写文件 | 网络活动 | 文件内容 | **主机异常**

规则名称 请输入 处置方式: 请选择处置方式

<input type="checkbox"/>	风险等级	规则名称	告警信息	描述	是否使用	创建人	触发条件	处置方式	最近更新时间
<input type="checkbox"/>	提示	通过kubectl_exec进...	有人通过kubectl exe...	通过kubectl_exec进...	<input type="checkbox"/>	系统内置		只报警	2024-04-28 10:37:33
<input type="checkbox"/>	提示	通过docker_exec进...	有人通过docker exe...	通过docker_exec进...	<input type="checkbox"/>	系统内置		只报警	2024-04-28 10:37:33
<input type="checkbox"/>	紧急	反弹shell操作	反弹shell操作	攻击者常利用此命令...	<input checked="" type="checkbox"/>	系统内置		只报警	2024-04-28 10:26:06
<input type="checkbox"/>	异常	runc被篡改	runc被篡改	此类行为可能为逃逸...	<input type="checkbox"/>	系统内置		只报警	2024-04-28 10:26:06
<input type="checkbox"/>	异常	高危系统调用使用	高危系统调用使用	此行为可能造成攻击...	<input type="checkbox"/>	系统内置	userfaultfd, setns, ptrace, acct, bpf, process_vi	只报警	2024-04-28 10:26:06
<input type="checkbox"/>	异常	宿主机上使用特定网...	宿主机上使用特定网...	该类工具是攻击者经...	<input type="checkbox"/>	系统内置	tcpdump, brctl, traceroute, axel, tshark, ngrep	只报警	2024-04-28 10:26:06

共6条 < 1 > | 10条/页

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。

4.9.6.2. 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。

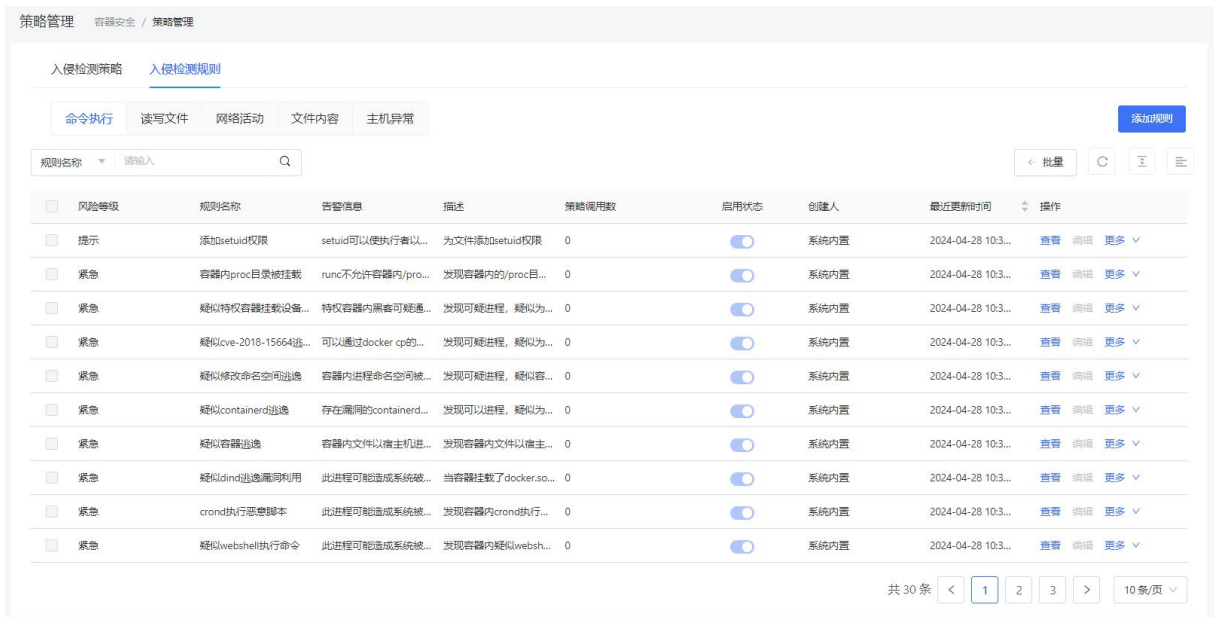
- 系统内置规则仅支持查看，不支持复制、编辑、删除等操作。
- 支持添加、编辑、删除自定义规则。

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。



策略管理 容器安全 / 策略管理

入侵检测策略 入侵检测规则

命令执行 读写文件 网络活动 文件内容 主机异常 添加规则

规则名称 请输入

<input type="checkbox"/>	风险等级	规则名称	告警信息	描述	策略调用数	启用状态	创建人	最近更新时间	操作
<input type="checkbox"/>	提示	添加setuid权限	setuid可以使执行者以...	为文件添加setuid权限	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	容器内proc目录被挂载	runc不允许容器内的/pro...	发现容器内的/proc目...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似特权容器挂载设备	特权容器内黑客可能通...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似CVE-2018-15664逃...	可以通过docker cp的...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似修改命名空间逃逸	容器内进程命名空间可被...	发现可疑进程，疑似容...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似containerd逃逸	存在漏洞的containerd...	发现可疑进程，疑似为...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似容器逃逸	容器内文件以宿主机进...	发现容器内文件以宿主...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似dind逃逸漏洞利用	此进程可能造成系统被...	当容器挂载了docker.so...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	crond执行恶意图本	此进程可能造成系统被...	发现容器内crond执行...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多
<input type="checkbox"/>	紧急	疑似webshell执行命令	此进程可能造成系统被...	发现容器内疑似websh...	0	<input checked="" type="checkbox"/>	系统内置	2024-04-28 10:3...	查看 编辑 更多

共 30 条 < 1 2 3 > 10 条/页

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 containerd 逃逸	发现可疑进程，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
	cron 执行恶意脚本	发现容器内 cron 执行恶意脚本，请检查是否为黑客行为

类型	检测项	说明
	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。
	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。

类型	检测项	说明
	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。

4.9.7. 文件防篡改

4.9.7.1. 添加文件防篡改策略

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 > 文件防篡改”，进入文件防篡改页面。

- 单击“添加策略”，进入添加策略页面。



- 在新建策略页面输入策略名称（必填）和描述信息（非必填），选择或输入目标对象（支持通配符），设置监控路径。
- 单击“保存”按钮，系统提示保存成功，安全策略设置完毕。

4.9.7.2. 管理文件防篡改策略

- 登录容器安全卫士控制台。
- 在左侧导航栏选择“容器安全 > 文件防篡改”，进入文件防篡改页面。

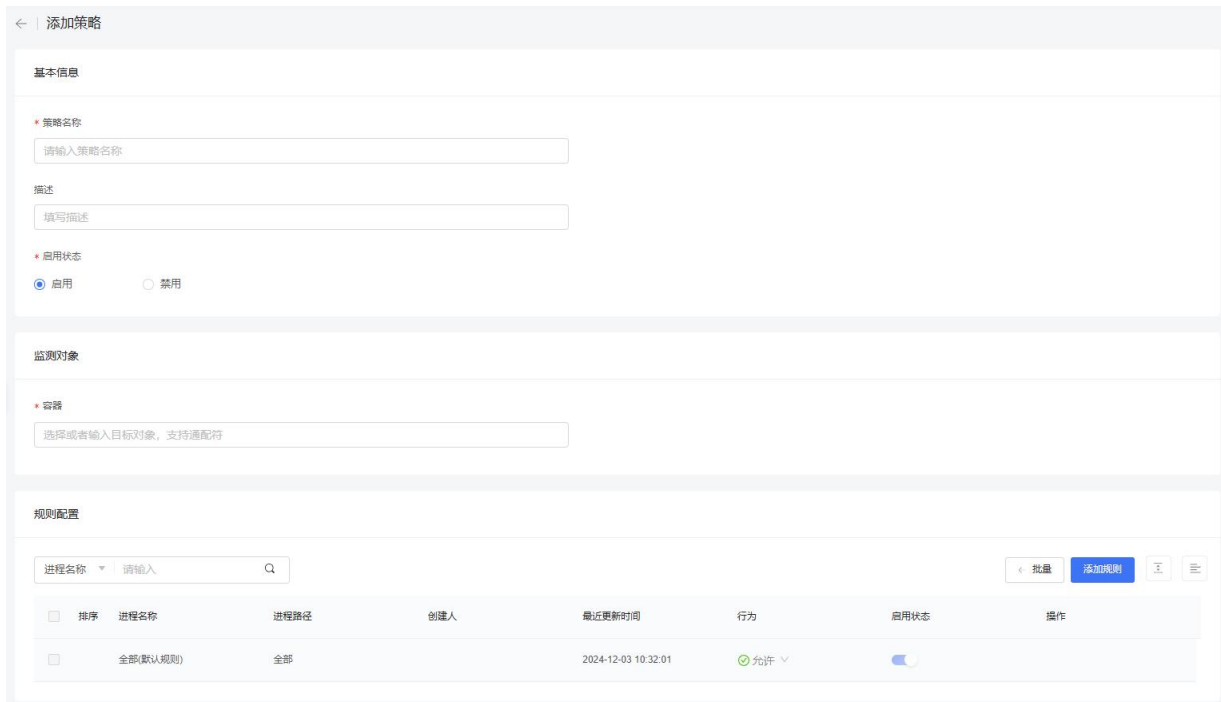


3. 查找策略：搜索框支持按策略名称、启用状态查找目的策略。
4. 策略管理：在策略列表内，支持对已添加策略进行查看、编辑、删除、开启、关闭。

4.9.8. 进程控制

4.9.8.1. 添加进程阻断策略

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 > 进程控制”，进入进程控制页面。
3. 单击“添加策略”，进入添加策略页面。



4. 在添加策略页面输入策略名称（必填）和描述信息（非必填），选择或输入目标对象（支持通配符），选择策略规则。
5. 单击“保存”按钮，系统提示保存成功，安全策略设置完毕。

4.9.8.2. 管理进程阻断策略

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 > 进程控制”，进入进程控制页面。



3. 查找策略：搜索框支持按策略名称、启用状态查找目的策略。
4. 策略管理：在策略列表内，支持对已添加策略进行编辑、删除、开启、关闭。

4.9.9. 弱密码

4.9.9.1. 添加弱口令字典

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 > 弱口令”，进入弱口令页面。
3. 单击“添加弱密码”，进入添加弱密码页面。

添加弱密码 X

* 字典名称

描述

* 标签

* 是否启用

启用 禁用

弱口令

- 在添加弱密码页面输入字典名称（必填）、描述信息（非必填）、标签（必填）、是否启用，输入弱口令信息。
- 单击“保存”按钮，系统提示保存成功，弱口令字典创建成功。

4.9.9.2. 管理弱口令字典

- 登录容器安全卫士控制台。
- 在左侧导航栏选择“容器安全 > 弱口令”，进入弱口令页面。

弱密码

字典名称

← 批量 添加弱密码 🗑️ 🔍 ☰

<input type="checkbox"/>	字典名称	描述	弱口令数	标签	创建人	启用状态	最近更新时间	操作
<input type="checkbox"/>	默认弱口令字典	用于弱口令检测	904	弱口令	--	🔵	2024-11-28 16:33:05	编辑 复制 ...

共1条 ⏪ 1 ⏩ 10条/页

3. 查找字典：搜索框支持按字典名称、启用状态查找目的弱口令字典。
4. 字典管理：在字典列表内，支持对已添加的字典进行编辑、删除、开启、关闭。

4.9.10. 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”。

实时监测设置

基本设置

历史容器保留时间: ? <input style="width: 80%;" type="text" value="7"/> 天	存在报警的历史容器保留时间: ? <input style="width: 80%;" type="text" value="7"/> 天
容器调查审计信息保留时间: ? <input style="width: 80%;" type="text" value="1"/> 天	容器调查审计信息保留容量: ? <input style="width: 80%;" type="text" value="3"/> G

[保存](#)

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”。 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”。 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。

4.10. 网络安全

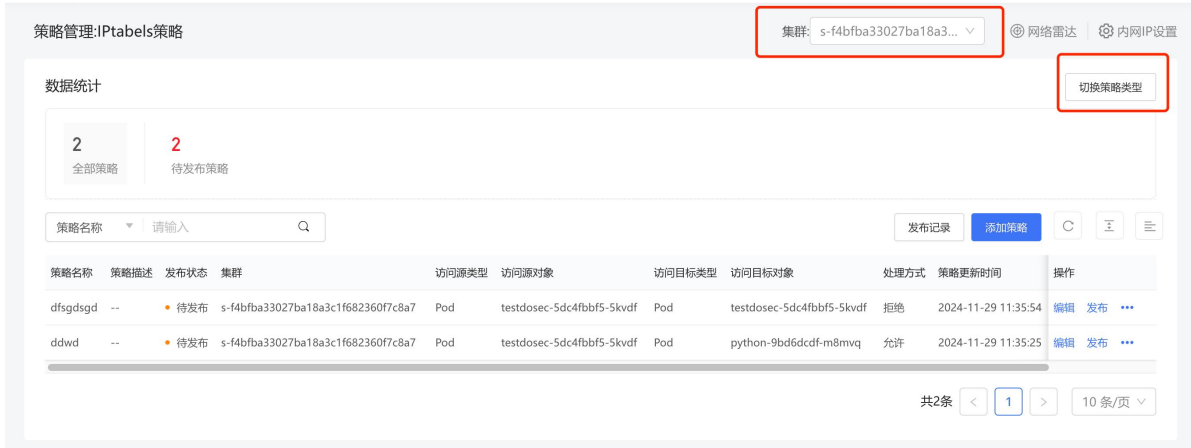
4.10.1. 选择策略类型

策略介绍

- NetworkPolicy 适用于为指定资源设置允许进出站访问的场景。
- OVS 模式仅限于 OpenShift 环境，可为指定的访问源与访问目标设置拒绝规则。
- IPtables 模式可为指定的访问源与访问目标设置访问规则，由策略优先级决定允许或拒绝。

选择策略类型

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络安全 > 策略管理”，进入策略管理页面。
 - 当首次添加集群时，系统会要求用户选择一种策略类型。在完成策略类型的选择后，点击“确定”按钮，系统会跳转至“策略管理”页面。
 - 当再次进入“策略管理”页面时（非初次进入），系统将会默认显示上次选择的策略类型。在“策略管理”页面中，可以查看当前所选策略类型的相关信息，还可以对集群和策略类型进行切换。
3. 在“策略管理”页面中，可以查看当前所选策略类型的相关信息，还可以对集群和策略类型进行切换。



4. 在弹出的对话框中，选择策略类型，单击“确定”。



4.10.2. 添加策略

4.10.2.1. 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“网络安全 > 策略管理”，进入策略管理页面。

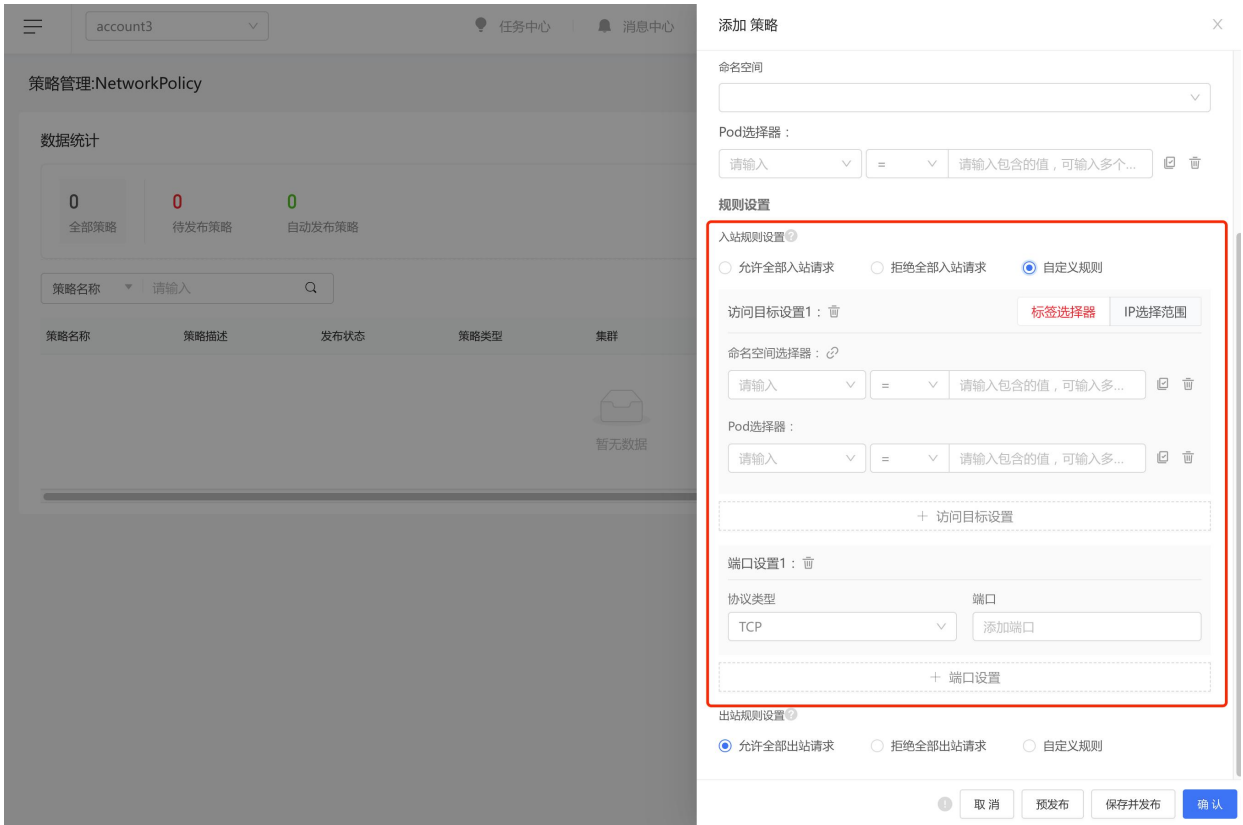


3. 单击策略列表右上方的“添加策略”，即可进入添加访问策略页面。

4. 10. 2. 1. 1. Networkpolicy

Networkpolicy 适用于为指定资源设置允许进出站访问的场景。

- 基本信息：策略名称（必填）、描述。
- 策略执行对象：命名空间、Pod 选择器（可新增或删除）。
- 规则设置：出/入站规则设置里，允许、拒绝和自定义三种选项，自定义规则可对访问目标和端口进行设置，也可对访问目标和端口进行添加和删除。



4. 10. 2. 1. 2. OVS 策略

OVS 模式仅限于 OpenShift 环境，可为指定的访问源与访问目标设置拒绝规则。

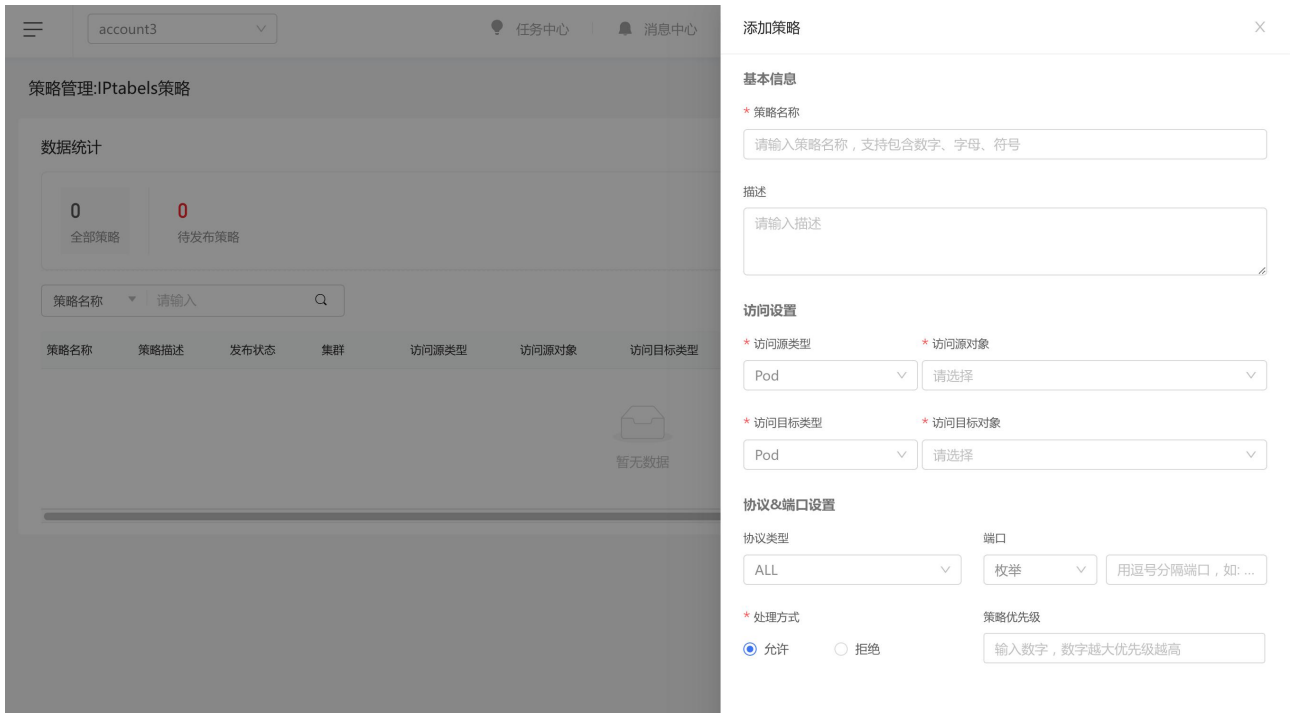
- 基本信息：策略名称（必填）、描述。
- 访问设置：访问源/目标类型，访问源/目标对象。
- 协议&端口设置：协议类型和端口。



4. 10. 2. 1. 3. Iptables 策略

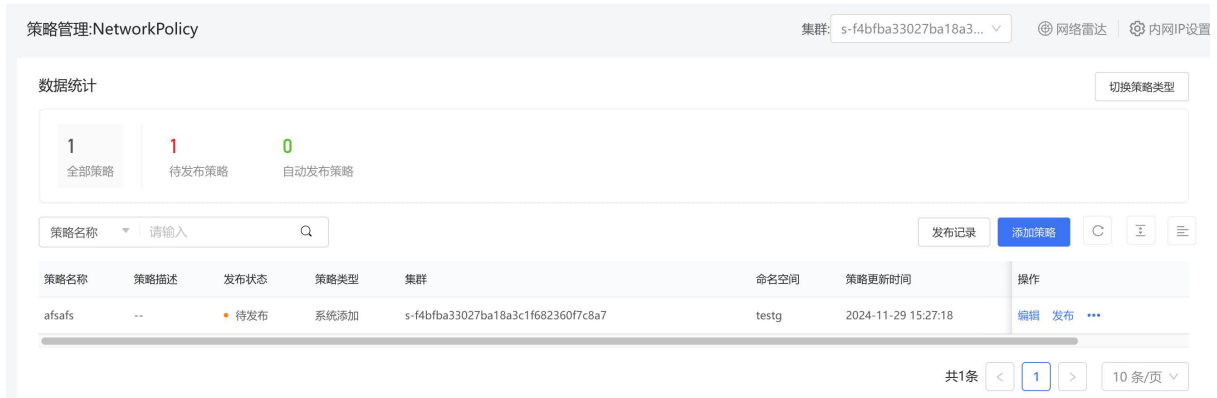
Iptables 模式可为指定的访问源与访问目标设置访问规则，由策略优先级决定允许或拒绝。

- 基本信息：策略名称（必填）、描述。
- 访问设置：访问源/目标类型，访问源/目标对象。
- 协议&端口设置：协议类型、端口、处理方式、策略优先级（数字越大优先级越高，最小优先级为 1）。



4. 10. 2. 2. 预发布策略

1. 相关的访问策略配置完成后，单击页面右下方的“预发布”按钮来测试发布情况。
触发预发布策略的访问请求不会直接被阻断，系统将自动发送报警，避免直接保存并发布策略可能会影响到正在运行的业务。
2. 单击“预发布”按钮完成添加后，返回至策略列表，可见新添加的策略的发布状态。



4.10.3. 发布策略

在预发布策略确认无误后，可以选择正式发布策略。

发布策略

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络安全 > 策略管理”，进入策略管理页面。
3. 单击策略列表操作列内的“发布”按钮，可以将预发布的策略改为正式发布。



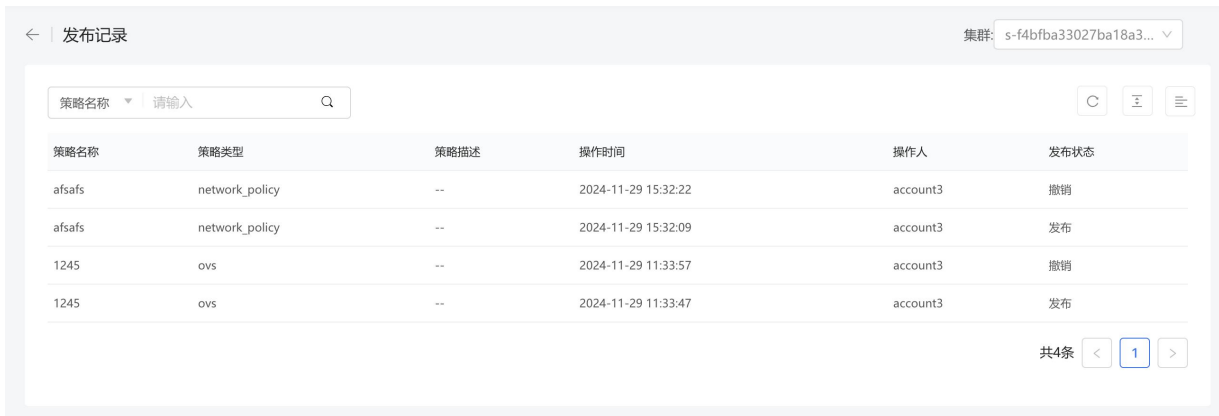
4. 修改后，发布状态将改变为“已发布”状态。

若要修改已经发布的策略，需要先单击策略列表操作列内的“撤销”按钮撤回已发布的策略，撤回后才支持进行编辑操作。



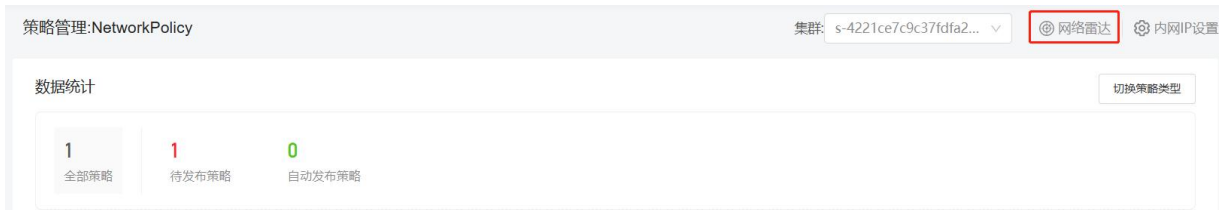
查看发布记录

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络安全 > 策略管理”，进入策略管理页面。
3. 单击策略列表右上方的“发布记录”按钮，即可查看策略发布记录。



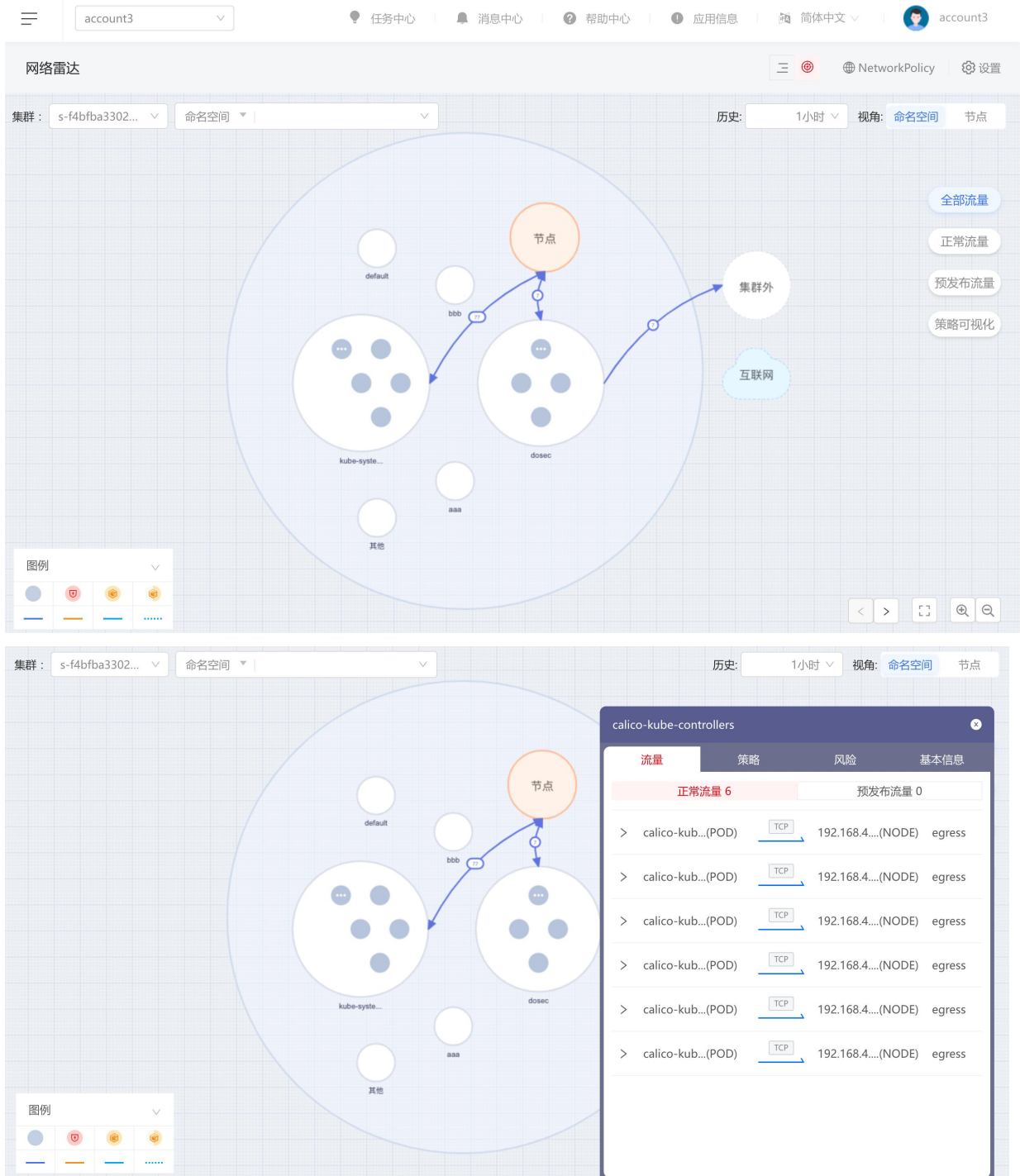
4.10.4. 查看网络雷达图

1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“网络安全 > 策略管理”，进入策略管理页面。
3. 单击页面右上角“网络雷达”。



4. 进入网络雷达图页面，在工作负载详情中的“策略”页面，可查看正常流量和预发布流量。

关于网络雷达的更多详细信息，请参见[网络雷达](#)。



4.11. 节点安全

4.11.1. 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”。

数据统计 开始扫描

3	1	1	1	0
全部节点	在线防御容器	离线防御容器	在线集群	离线集群

节点名称: 请输入 关闭防护 开启防护 删除 C 刷新 列表

检索项: 节点类型: 防御容器

<input type="checkbox"/>	节点名称	IPv4地址	IPv6地址	集群	系统类型	节点状态	扫描状态	最近扫描时间	发现时间	防护状态	操作
<input type="checkbox"/>	ecm-ctcs...	192.168.0.159	--	s-b8db666384676e8...	ctyunos.2.0.1	已连接	扫描中	2024-04-29 1...	2024-04-28 10:47:55	<input checked="" type="checkbox"/>	重新扫描 删除 更多
<input type="checkbox"/>	ecm-ctcs...	192.168.0.160	--	s-b8db666384676e8...	ctyunos.2.0.1	未连接	待扫描	--	2024-04-28 10:47:55	<input type="checkbox"/>	扫描 删除 更多

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。

节点安全

数据统计 开始扫描

3	1	1	1	0
全部节点	在线防御容器	离线防御容器	在线集群	离线集群

节点名称: 请输入 关闭防护 开启防护 删除 C 刷新 列表

检索项: 节点类型: 防御容器

<input type="checkbox"/>	节点名称	IPv4地址	IPv6地址	集群	系统类型	节点状态	节点类型	扫描状态	心跳时间	最近扫描时间	发现时间	操作
<input type="checkbox"/>	ecm-ctcs...	192.168.0.159	--	s-b8db666384...	ctyunos.2.0.1	已连接	防御容器	已扫描	2024-04-29 1...	2024-04-29 1...	2024-04-28 1...	重新扫描 删除 更多
<input type="checkbox"/>	ecm-ctcs...	192.168.0.160	--	s-b8db666384...	ctyunos.2.0.1	未连接	防御容器	待扫描	2024-04-28 1...	--	2024-04-28 1...	扫描 删除 更多

共2条 < 1 > 10条/页

4.11.2. 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

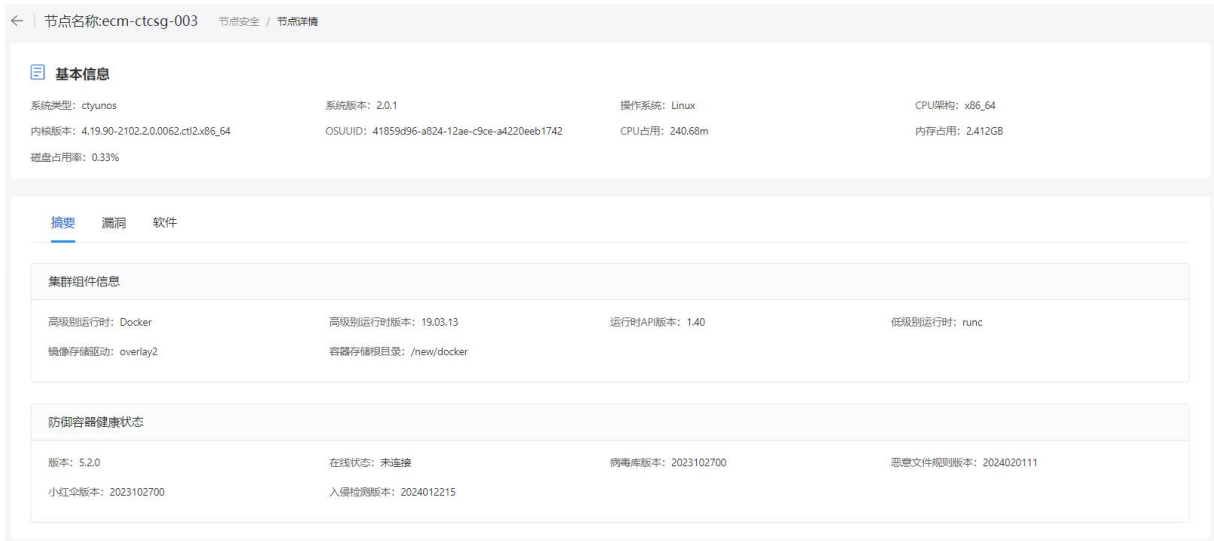
1. 登录容器安全卫士控制台。
2. 在左侧导航栏选择“节点安全”，进入节点安全页面。
3. 节点状态列表上方，支持按照“节点名称”、“节点状态”、“防护状态”、“软件版本”、“软件名称”等进行筛选查询。系统默认筛选出节点类型为防御容器的节点。

节点列表参数说明如下：

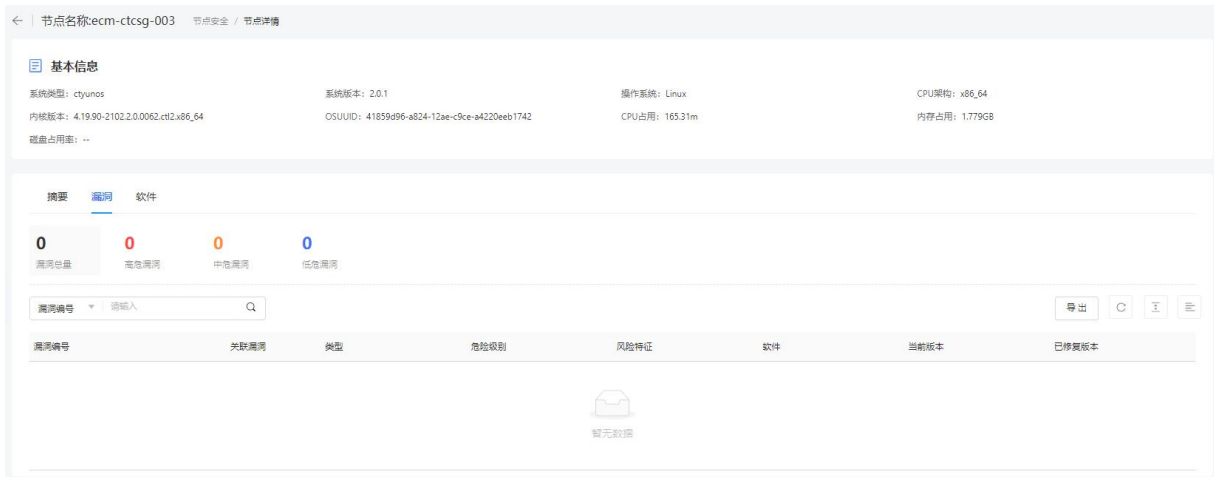
参数	说明
节点名称	节点的名称。
IPv4 地址	节点的 IPv4 地址。
IPv6 地址	节点的 IPv6 地址。
集群	节点所属集群的名称。
系统类型	节点的操作系统类型。
节点状态	指节点上防御容器的在线状态，分为已连接、未连接和已暂停三种状态。
节点类型	节点类型根据节点上运行的容器分为防御容器和扫描容器。
扫描状态	扫描状态分为待扫描、扫描中、已扫描、扫描失败这几种状态。
心跳时间	最近一次检查节点在线状态的时间。

4.11.3. 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。

摘要 漏洞 软件

软件名称 请输入

软件名称	版本	文件路径	类型	漏洞数量
+ ModemManager-glib	--	--	rpm	高 0 中 0 低 0
+ NetworkManager	--	--	rpm	高 0 中 0 低 0
+ NetworkManager-config-server	--	--	rpm	高 0 中 0 低 0

4.11.4. 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。

节点安全

数据统计 开始扫描

3 全部节点 | 1 在线防护容器 | 1 离线防护容器 | 1 在线集群 | 0 离线集群

节点名称 请输入

关闭防护 开启防护 删除

搜索项: 节点类型: 防护容器

<input type="checkbox"/>	节点名称	IPv4地址	IPv6地址	集群	系统类型	节点状态	节点类型	扫描状态	心跳时间	最近扫描时间	发现时间	防护状态	操作
<input type="checkbox"/>	ecm-ctcs...	192.168.0.159	--	s-b8ab6663846...	ctyunos2.0.1	已连接	防护容器	已扫描	2024-04-29 17:3...	2024-04-29 1...	2024-04-28 10:4...	<input checked="" type="checkbox"/>	重新扫描 删除 更多
<input type="checkbox"/>	ecm-ctcs...	192.168.0.160	--	s-b8ab6663846...	ctyunos2.0.1	未连接	防护容器	待扫描	2024-04-28 17:0...	--	2024-04-28 10:4...	<input type="checkbox"/>	扫描 删除 更多

共2条 < 1 > 10条/页

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

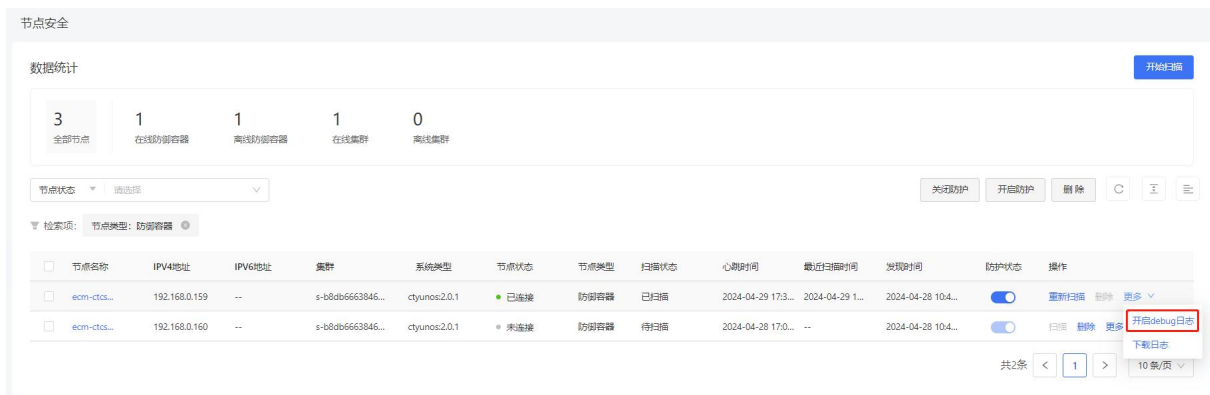
支持批量暂停、恢复或删除节点。

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。



4.12. 平台管理

4.12.1. 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。


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
2024-04-29 14:32:09	27618268ad77...	192.168.0.163	更新	其他	执行成功	Agent降级恢复
2024-04-29 14:32:03	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表
2024-04-29 14:32:03	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表
2024-04-29 14:26:26	27618268ad77...	192.168.0.163	更新	其他	执行成功	手动获取 agent 资源
2024-04-29 14:21:44	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表
2024-04-29 14:21:44	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表
2024-04-29 14:21:31	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表
2024-04-29 14:21:31	27618268ad77...	192.168.0.163	更新	其他	执行成功	查看集群安全-集群列表

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。
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。

基础设置

查看类型的操作记录审计

操作审计保留时间

6 月

[保存](#)

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。

4.12.2. 外部集成

外部集成页面提供了系统数据同步的集成方式，用户可通过该页面功能与外部数据库同步数据。

目前支持 Syslog 集成配置，Syslog 服务器可以对多个设备的 Syslog 消息进行统一的存储，解析其中的内容做相应的处理。

添加 syslog 集成设置

1. 登录容器安全卫士控制台。
2. 在左侧导航栏，选择“平台管理 > 外部集成”，进入外部集成页面。

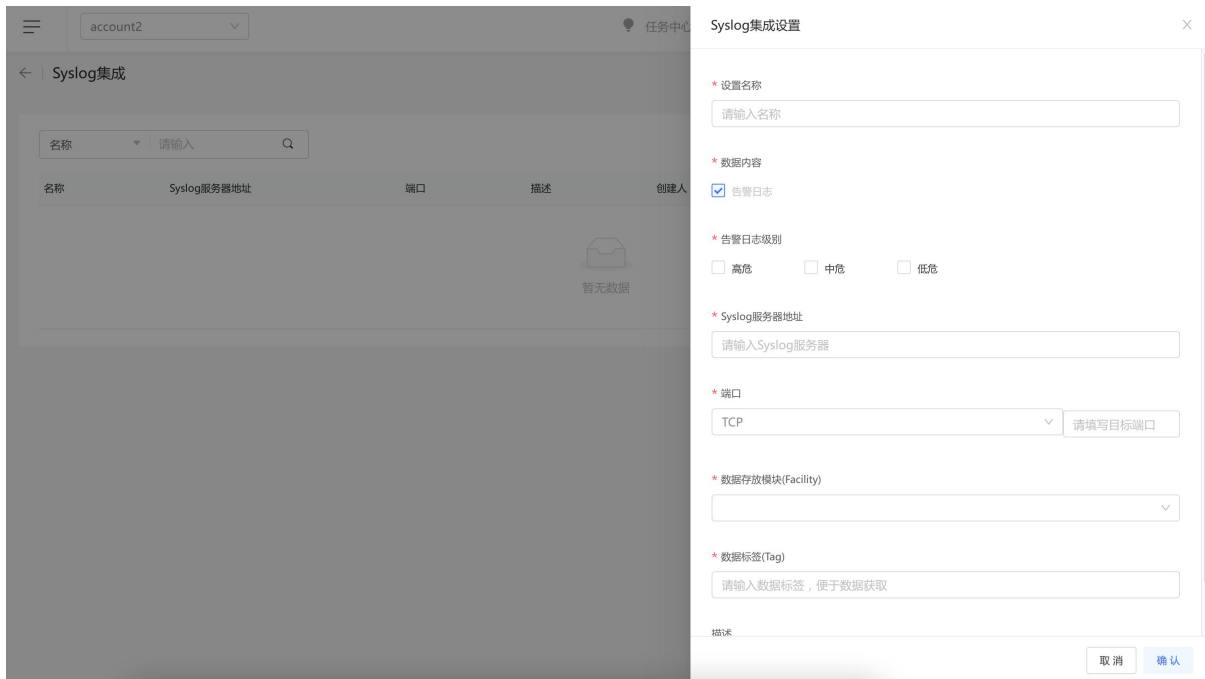


3. 单击 Syslog 卡片，进入 Syslog 集成列表页面。



4. 单击右上方的“添加集成设置”，进入 Syslog 集成设置页面，可添加新的 Syslog 集成设置。

输入名称，选择需要的告警日志级别，配置 Syslog 服务器地址和端口号，选择数据存放模块，配置数据标签（数据标签的设置便于数据获取），还可输入描述信息便于管理查看。



5. 配置完成后，单击“确认”，回到 Syslog 集成列表页面，查看已经配置的 Syslog 集成列表。

相关操作

在 Syslog 集成列表页面，单击操作列的编辑按钮，可查看并修改所选集成设置。

4.13. 安装配置

4.13.1. 租户集群为天翼云原生集群

开通容器安全卫士实例后，需要通过安装 Sever/Agent 将您要防护的集群、节点接入到平台中，用来采集集群、节点、容器等资产信息，包运行状态、命令、文件、网络等，进行安全检测和防护。

注意事项

- 集群组件在运行时挂载 k8s node 宿主机的 /data（非 cri-o）和 /root（cri-o）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。

前提条件

已购买容器安全卫士。

操作步骤

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“集群组件部署”，进入集群组件部署页面。



4. 选择集群类型，天翼云原生集群选择“是”；选择集群所在的区域；选择集群。

* 是否为天翼原生k8s集群:

是 自建集群

* 请选择区域

请选择区域

* 请选择集群

请选择集群

5. 单击“立即部署”。

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。

4.13.2. 租户集群为自建集群

注意事项

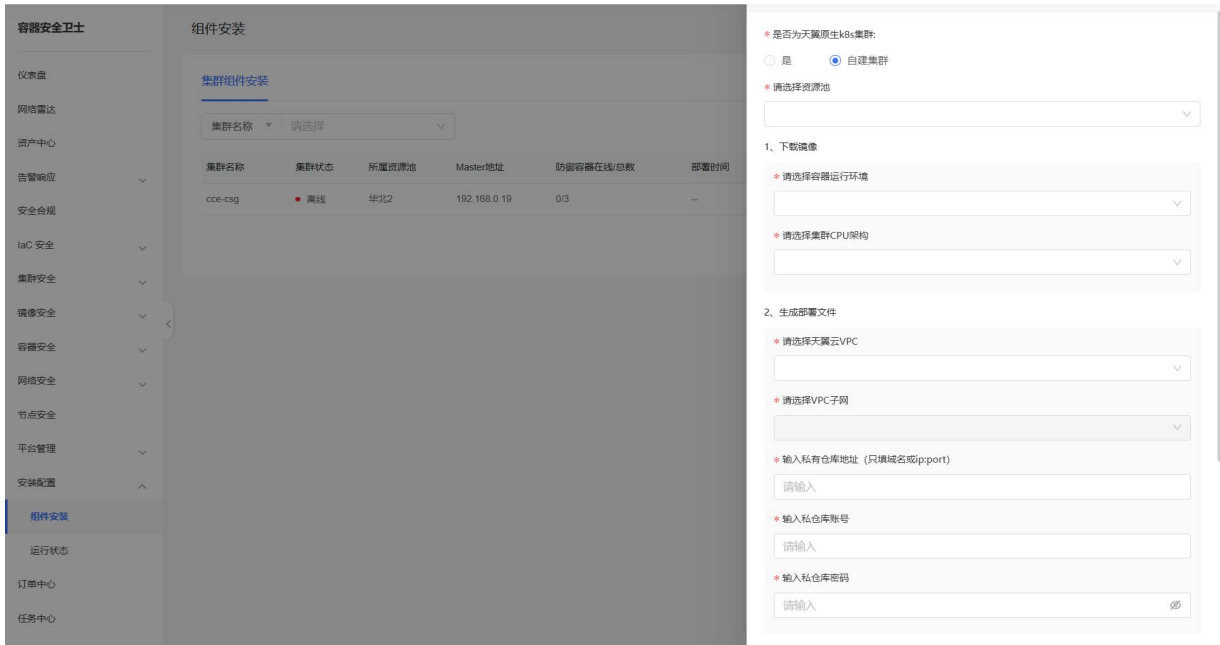
- 集群组件在运行时会挂载 k8s node 宿主机的 /data (非 cri-o) 和 /root (cri-o) 目录, 请确保目录的权限正常。
- 请确保您的 k8s 集群允许出网策略 TCP 端口: 31080、30432、32345。

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“集群组件部署”, 进入集群组件部署页面。



4. 选择“是否为天翼原生 k8s 集群”, 此处选择“自建集群”; 选择集群所在的资源池。



5. 选择“是否为天翼原生 k8s 集群”, 此处选择“自建集群”。
6. 集群名称为系统自动生成, 不可以修改。

7. 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:2024-12-24T19.31.05V5.2.0_release_298e83_b85cc6c5bc,library
- dosec-host-tool:alpineV3.8,library
- dosec-scanner:2025-01-06T17.38.12V5.2.0_release_bd003d_d3e87a1881,library
- dosec-server:2025-01-07T11.36.00V5.2.1-sp89-1.1_release_287a57_d168109d92

8. 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。

4.13.3. 集群组件配置

1. 登录容器安全卫士控制台。
2. 单击左侧导航栏中“安装配置 > 组件安装”，进入组件安装页面。
3. 查看集群列表。



4. 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。

全局设置

单个镜像扫描超时 分钟
单个镜像扫描超时默认为10分钟

节点扫描的并发数 个
各节点镜像并发扫描数量默认为1个且最高数量不超过3个

仓库镜像扫描并发数 个
各仓库镜像并发扫描数量默认为1个且最高数量不超过3个

防御容器设置

开启镜像阻断
开启镜像阻断功能，才能对异常镜像进行阻断

开启入侵检测模块
开启入侵检测模块，才能对容器的入侵检测行为进行报警

开启容器审计功能
开启容器审计功能后，会记录大量事件，占用较大的磁盘空间。

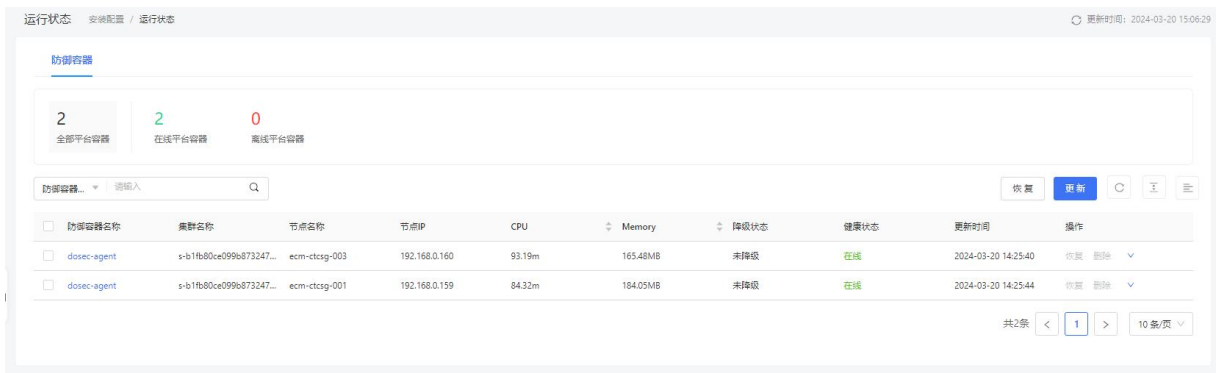
文件防篡改存储阈值设置 G
备份文件占用主机资源超出最大限制阈值时，将不再备份相关文件并进行告警通知。最多备份支持10000个文件，超出限制时，将不再备份相关文件并进行告警通知。

5. 配置完成后，单击“保存”。

4.13.4. 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。



防御容器名称	集群名称	节点名称	节点IP	CPU	Memory	降级状态	健康状态	更新时间	操作
dosec-agent	s-b1fb80ce999b873247...	ecm-ctcsg-003	192.168.0.160	93.19m	165.48MB	未降级	在线	2024-03-20 14:25:40	恢复 删除
dosec-agent	s-b1fb80ce999b873247...	ecm-ctcsg-001	192.168.0.159	84.32m	184.05MB	未降级	在线	2024-03-20 14:25:44	恢复 删除

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。

参数	说明
	<p>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。</p> <p>说明： 未降级或已离线的防御容器不支持恢复。</p>
更新时间	容器状态更新的时间。

下载日志

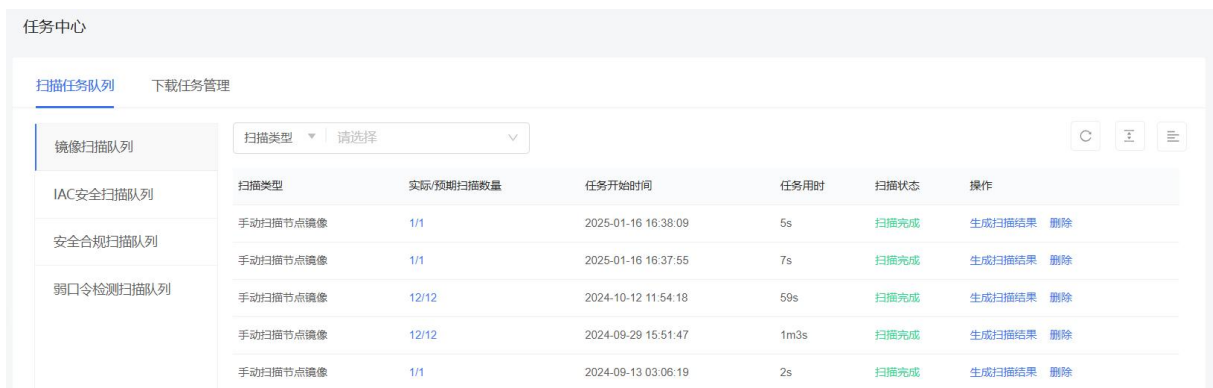
在防御容器列表内，单击操作列中的“下载日志”，可直接将防御容器的日志下载至本地。

4.14. 任务中心

任务中心页面提供统一的任务管理窗口，包括扫描任务队列和下载任务管理，在该页面可以查看各项任务的扫描状态或下载生成状态，并且在下载任务管理页面可将报表下载到本地。

查看扫描任务

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. 在“扫描任务队列”页面，可以查看镜像扫描任务、IaC 安全扫描任务、安全合规扫描任务、弱口令检测扫描任务。



任务中心

扫描任务队列 下载任务管理

扫描类型 请选择

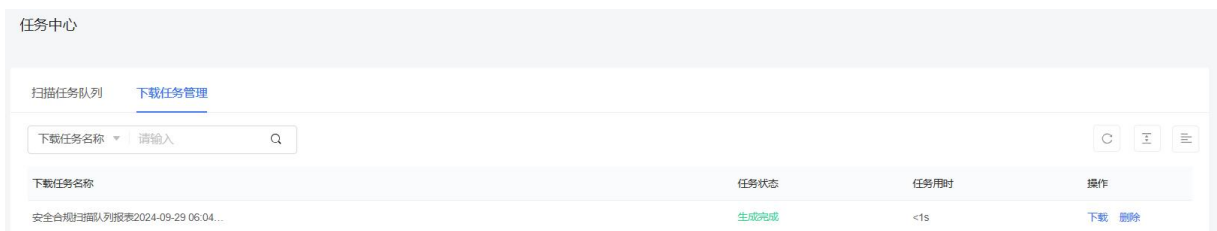
扫描类型	实际/预期扫描数量	任务开始时间	任务用时	扫描状态	操作
手动扫描节点镜像	1/1	2025-01-16 16:38:09	5s	扫描完成	生成扫描结果 删除
手动扫描节点镜像	1/1	2025-01-16 16:37:55	7s	扫描完成	生成扫描结果 删除
手动扫描节点镜像	12/12	2024-10-12 11:54:18	59s	扫描完成	生成扫描结果 删除
手动扫描节点镜像	12/12	2024-09-29 15:51:47	1m3s	扫描完成	生成扫描结果 删除
手动扫描节点镜像	1/1	2024-09-13 03:06:19	2s	扫描完成	生成扫描结果 删除

- 扫描完成后，单击操作列的“生成扫描结果”，开始生成对应的报表任务。可在“下载任务管理”页签，查看任务状态并下载报表。

相关操作：单击任务操作列的“删除”，可以删除扫描任务。

查看并下载报表

- 登录容器安全卫士控制台。
- 在左侧导航栏，选择“任务中心”，进入任务中心页面。
- 选择“下载任务管理”页签，可以查看下载任务状态。



- 当任务状态为“生成完成”时，单击任务操作列的“下载”，可以下载已生成的报表。

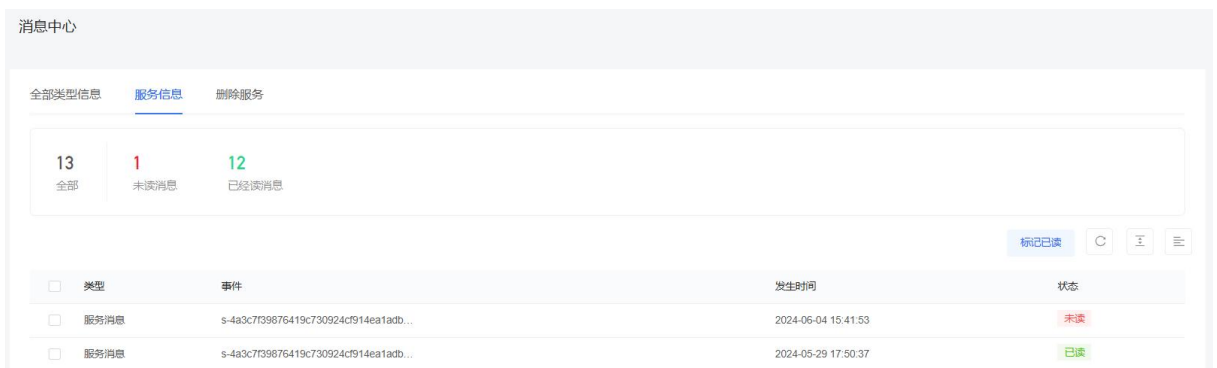
相关操作：单击任务操作列的“删除”，可以删除下载任务。

4.15. 消息中心

消息中心页面提供防护容器的下线通知和删除服务通知，以便用户及时恢复防护容器。

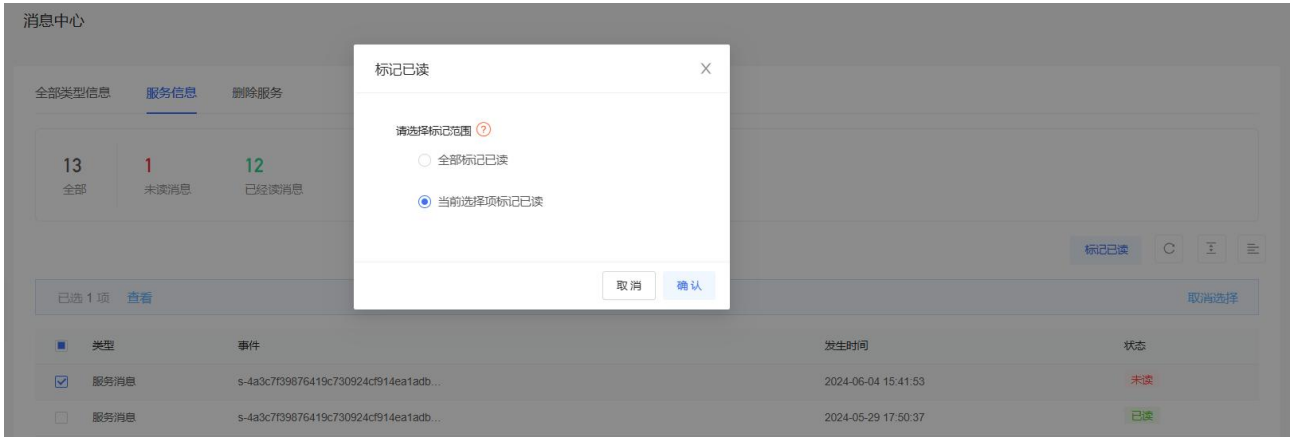
查看消息

- 登录容器安全卫士控制台。
- 在左侧导航栏，选择“消息中心”，进入消息中心页面。
- 支持查看“服务信息”和“删除服务”类消息。



标记已读

在消息中心页面，阅读消息后，可以勾选多条消息后，单击“标记已读”，在弹出的对话框中，可以选择“全部标记已读”或只对当前选择项标记已读，选择完成后，单击“确认”。



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。