容器安全服务

产品文档

文档目录

产品简介
产品概述
什么是容器安全服务

最近更新时间: 2023-08-17 14:29:56

容器安全服务提供容器资产管理、镜像安全及运行时入侵检测等安全服务，保障容器从镜像生成、存储到运行时的全生命周期安全，帮助企业构建容器安全防护体系。

为什么需要容器安全服务

最近更新时间: 2023-08-17 14:29:56

在容器的生命周期中，会遇到各种风险，包括：

- 运行环境安全风险，例如，操作系统组件存在漏洞、配置不当导致暴露不必要的端口、用户访问权限不当、共享操作系统内核等风险。
- 镜像安全风险，例如，镜像存在漏洞、恶意软件、明文密钥、镜像配置不当或使用非信任镜像等风险。
- 容器安全风险，例如，容器内应用存在漏洞、被植入木马病毒，容器资源配置不当等风险。

使用容器安全服务可对上述风险进行防范，保障容器的生命周期安全。

产品优势

最近更新时间: 2023-08-17 14:29:56

- 轻量级部署，高性能低占用
- 可视化的安全运营分析能力

功能介绍
安全概览

最近更新时间: 2023-08-17 14:33:59

以可视化的图形、图表等方式实时展示资产信息（容器、镜像、集群、主机节点）、漏洞风险（镜像）、集群风险、待处理安全事件数量、运行时安全事件新增趋势、本地镜像新增风险趋势及详情。

资产管理

最近更新时间: 2023-08-17 14:33:59

- **容器资产**
- **集群资产**
- **进程端口**
- **应用web资产**

漏洞管理

最近更新时间: 2023-08-17 14:55:41

- **应急漏洞**
- **系统漏洞**
- **web应用漏洞**
- **漏洞防御**

镜像风险管理

最近更新时间: 2023-08-17 14:33:59

- **本地镜像**:支持定时扫描、一键扫描本地镜像获取镜像资产基本信息及镜像安全风险详情;支持对业务环境存在风险的镜像总数、安全漏洞、木马病毒、敏感信息进行汇总。
- **仓库镜像**:支持定时扫描、一键扫描仓库镜像获取镜像资产基本信息及镜像安全风险详情。
- **镜像拦截事件**:镜像拦截策略支持对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

集群安全管理

最近更新时间: 2023-08-17 14:55:41

- **集群检查**：支持自动检查、手动检查获取集群资产基本信息及其存在的配置和漏洞风险，并对业务环境中存在风险的集群及每个集群存在的风险数据进行汇总；集群检查模式包括正常模式和主动模式。
- **风险分析**：支持按严重、高危、中危、低危对存在风险的集群节点进行统计，并按检查项对受影响的集群数、受影响的节点数进行统计。

安全基线

最近更新时间: 2023-08-17 14:55:41

- 支持CIS Benchmark基线检查标准，检测Docker及Kubernetes安全基线，并对业务环境中合规容器占比、严重检查项、高危检查项、中危检查项、低危检查项进行统计。
- 基线检测结果包括基线检测项、类型、基线标准、威胁等级、检测结果、检测项详情等，检测对象包括容器、镜像、Docker主机和Kubernetes。

运行时安全

最近更新时间: 2023-08-17 14:44:51

- **容器逃逸**：支持实时检测容器内存在的敏感路径挂载、特权容器、提权事件、逃逸漏洞利用、访问Docker API接口逃逸、篡改敏感文件逃逸、利用cgroup机制逃逸等行为，并自定义开启/关闭检测规则。
- **反弹Shell**：支持实时检测容器内存在的反弹Shell行为并产生告警，告警信息包括：进程名称、父进程名称、目标地址、进程路径、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID 等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。
- **文件查杀**：支持实时检测容器运行时存在的木马病毒并产生告警，告警信息包括文件名称、文件路径、病毒名称、首次生成时间、最近生成时间、容器名称/ID、镜像名称/ID、容器状态等；同时告警详情提供恶意文件详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息。
- **恶意外连**：支持实时检测容器内存在的进程异常启动行为并告警通知或拦截异常进程。告警信息包括：进程路径、命中规则、威胁等级、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。

高级防御

最近更新时间: 2023-08-17 14:44:51

- **异常进程**：支持实时检测容器内存在的进程异常启动行为并告警通知或拦截异常进程。告警信息包括：进程路径、命中规则、威胁等级、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。
- **文件篡改**：支持实时检测容器内存在的文件异常访问行为并告警通知或拦截异常访问。告警信息包括：文件名称、进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等。同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。
- **高危系统调用**：支持实时检测容器内存在的高危系统调用行为并产生告警，告警信息包括：进程路径、系统调用名称、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD 名称等，同时告警详情提供风险描述、解决方案、进程、父进程和祖先进程详细信息。
- **K8S API异常请求**：基于自适应学习技术，通过系统规则和用户自定义检测规则，实时监控集群API异常请求行为，并实时告警通知。

策略管理

最近更新时间: 2023-08-17 14:44:51

镜像拦截策略：镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

日志分析

最近更新时间: 2023-08-17 14:44:51

- **支持按时间**、日志类型、日志内容等自定义检索容器bash日志、容器启动审计日志、Kubernetes API审计日志，并按检索结果展示日志趋势图。支持自定义日志的展示字段和隐藏字段，查看json格式日志，并支持导出日志。
- **日志配置**：支持自定义配置容器 bash 日志、容器启动审计日志和Kubernetes API 审计日志是否开启日志审计，以及按照日志类型自定义节点是否开启审计。支持按百分比和存储天数清理日志。
- **日志投递**：支持自定义配置CKAFKA和CLS日志投递功能。CKAFKA日志投递支持按公网域名接入，客户可自定义选择投递的消息队列实例、接入的公网域名、每类日志投递的Topic ID和名称，以及是否开启投递；CLS日志投递支持自定义日志投递的日志集和日志主题，以及是否开启投递。

告警设置

最近更新时间: 2023-08-17 14:44:51

- 支持自定义对本地镜像（安全漏洞、木马病毒、敏感信息）、仓库镜像（安全漏洞、木马病毒、敏感信息）、运行时安全&高级防御（容器逃逸、反弹Shell、文件查杀、异常进程、文件篡改）等告警进行通知，可配置内容包括告警状态、告警时间和告警项，接收渠道包括站内信、邮件、短信、微信、企业微信等。

操作指南
安全概览
功能简介

最近更新时间: 2023-08-22 08:56:12

以可视化的图形、图表等方式实时展示资产信息（容器、镜像、主机）、待处理安全事件数量、运行时安全事件新增趋势、本地镜像新增风险趋势及详情。

资产信息

最近更新时间: 2023-08-22 09:03:37

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

2.在安全概览页面，单击“模块总数”，可跳转到资产管理的对应模块列表。

查看待处理安全事件

最近更新时间: 2023-08-22 09:03:37

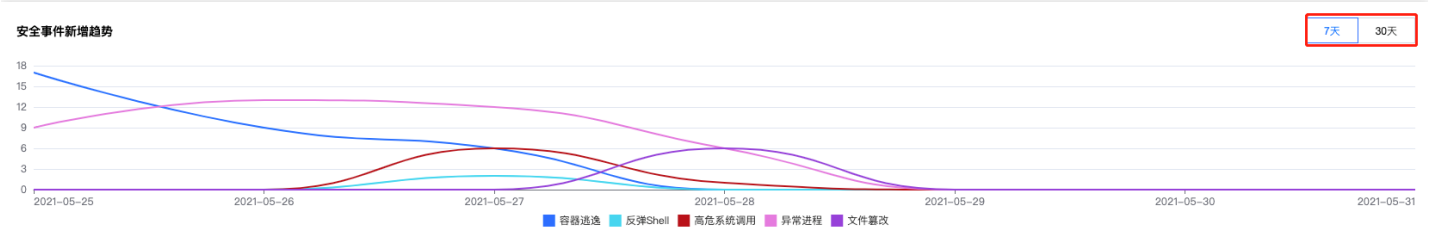
1.在安全概览页面，待处理安全事件模块展示当前待处理安全事件的数量。

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

查看安全事件新增趋势

最近更新时间: 2023-08-22 09:03:37

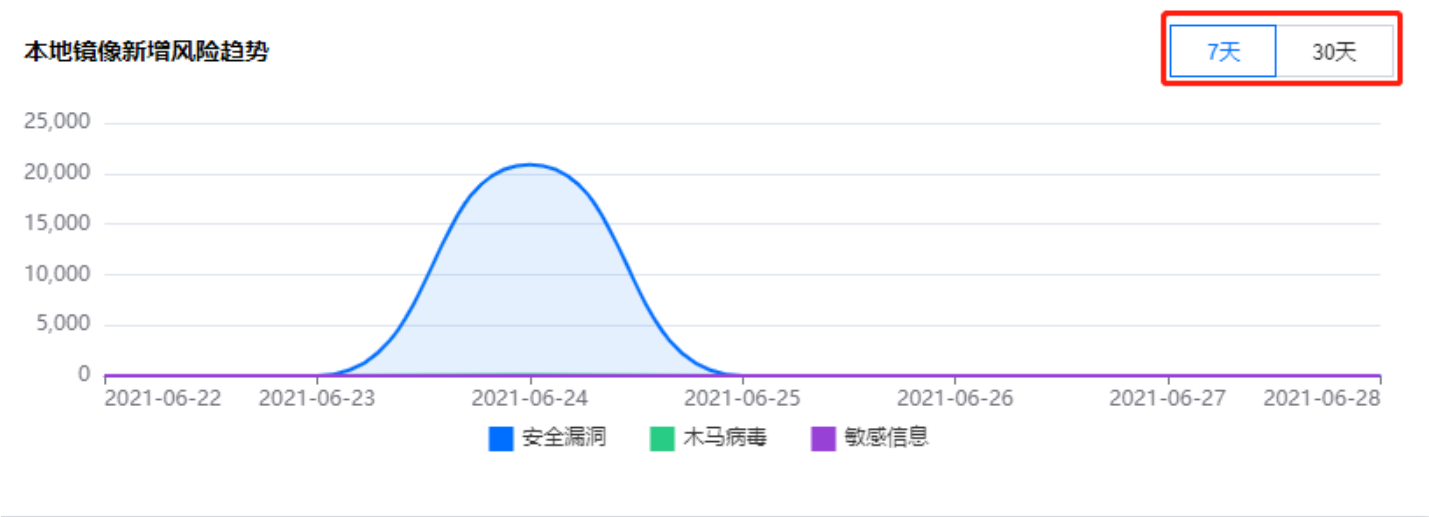
在安全概览页面，安全事件新增趋势模块展示7天或30天内运行时安全事件新增趋势。单击7天或30天可切换时间。



查看本地镜像新增风险趋势

最近更新时间: 2023-08-22 09:03:37

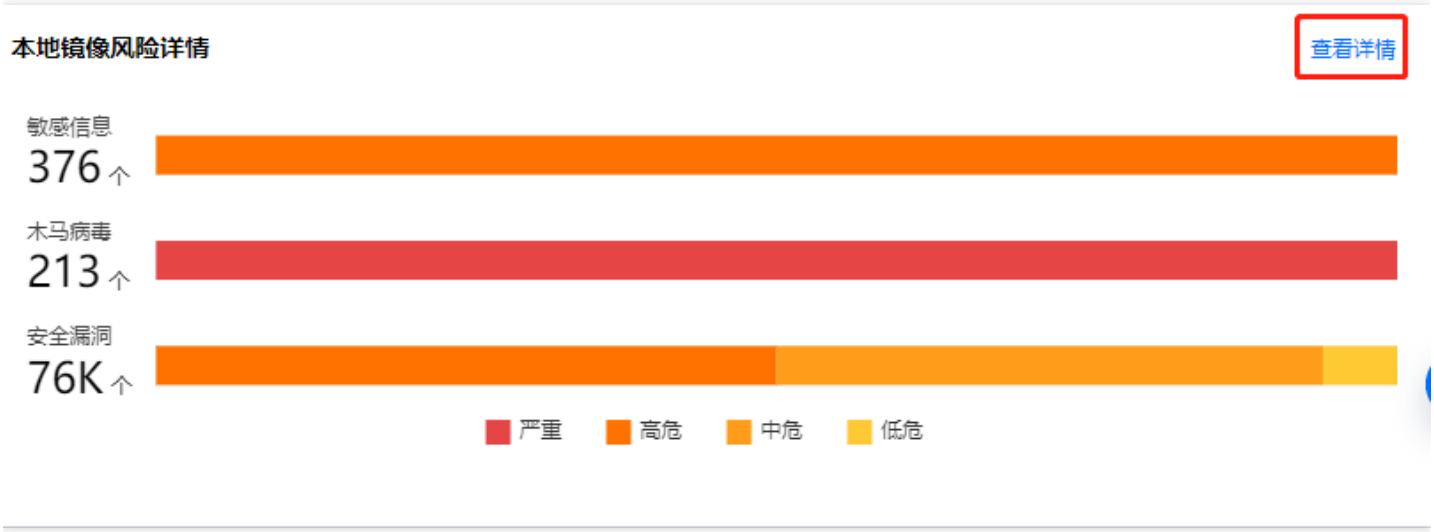
在安全概览页面，展示7天或30天内本地镜像新增的安全漏洞、木马病毒、敏感信息数量趋势。单击7天或30天可切换时间。



查看本地镜像风险详情

最近更新时间: 2023-08-22 09:04:23

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



资产管理

概述

最近更新时间: 2023-08-22 09:16:15

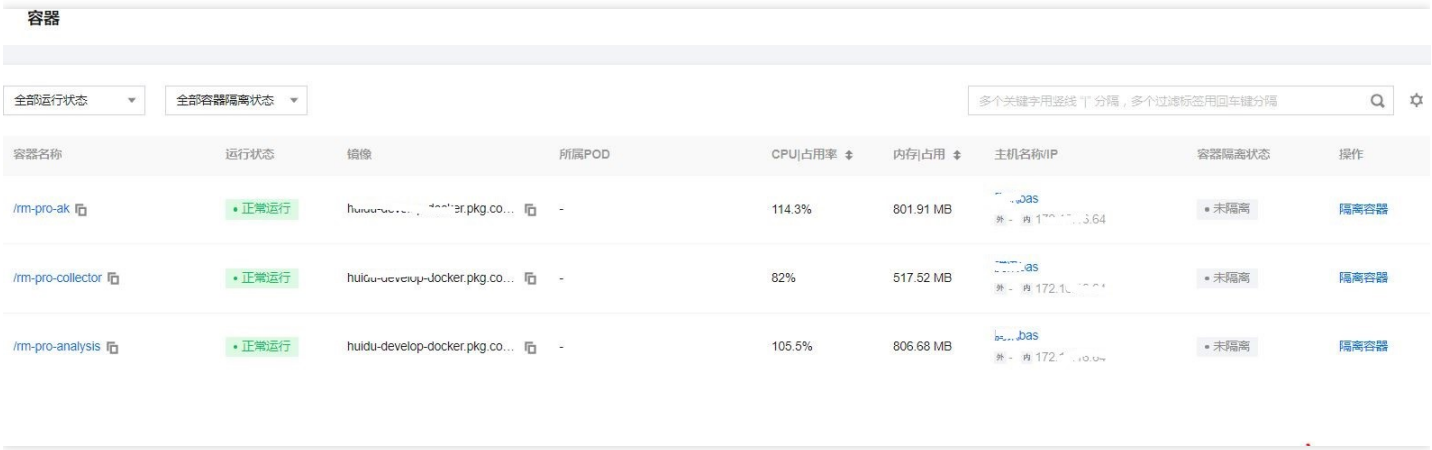
- 资产管理的数据每隔24小时自动同步一次，支持手动同步。
- 资产管理支持采集以下10种资产的信息：容器、本地镜像、仓库镜像、集群、主机节点、进程、端口、Web 服务、运行应用、数据库应用。
- 目前支持识别的资产有：

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

容器
查看容器模快

最近更新时间: 2023-08-22 09:16:15

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



2.在容器列表页面，可按运行状态对容器资产进行筛选，或搜索框通过“容器名称、容器ID、镜像名称、主机IP”等关键字对容器进行查找。

3.单击左上角的状态下拉框，按运行状态对容器资产进行筛选。

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

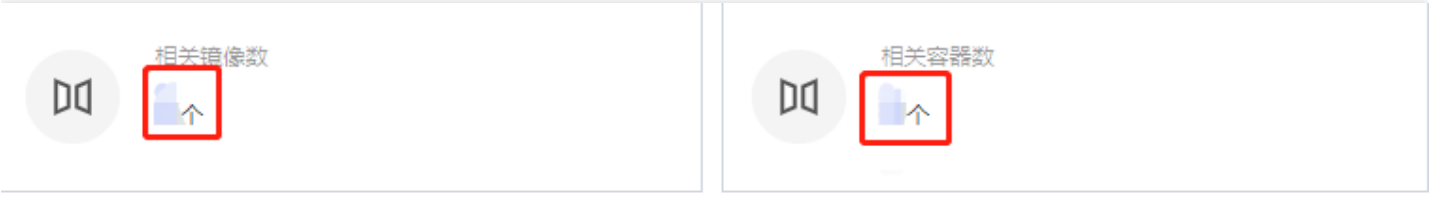
查看容器列表

最近更新时间: 2023-08-22 09:40:50

1.在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

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

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



自定义列表管理

最近更新时间: 2023-08-22 09:39:41

1.在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

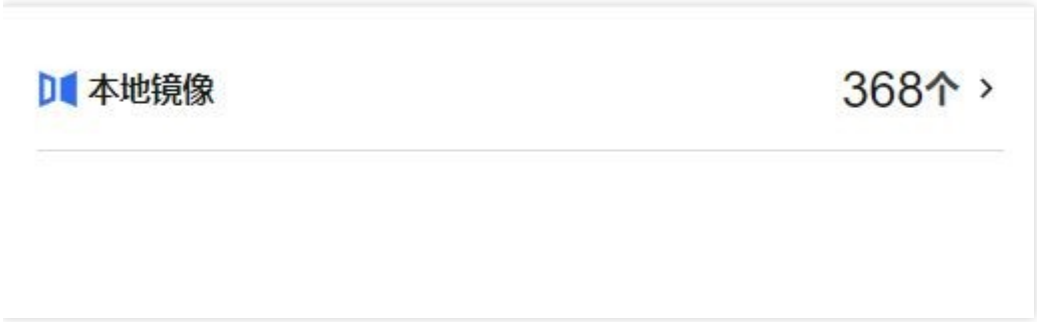
2.在容器列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

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

查看本地镜像模块

最近更新时间: 2023-08-22 09:39:41

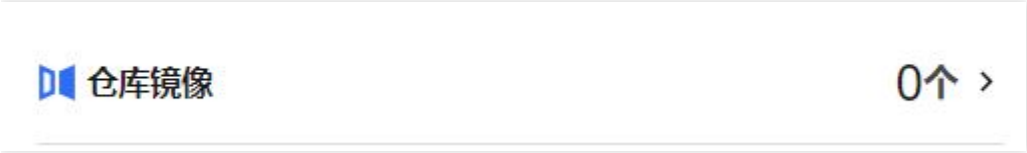
在资产管理页面，镜像模块展示了模块中本地镜像资产总数。单击“本地镜像”，可跳转镜像风险管理>本地镜像页面查看镜像详情。



查看镜像仓库模块

最近更新时间: 2023-08-22 09:39:41

在资产管理页面，镜像仓库模块展示了镜像仓库资产总数。单击“仓库镜像总数”，可跳转镜像安全>仓库镜像页面查看镜像仓库详情。



查看主机节点模块

最近更新时间: 2023-08-22 09:40:15

在资产管理页面，单击“主机节点”，可查看全部主机资产列表。

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

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

查看主机列表

最近更新时间: 2023-08-23 09:36:20

1.在资产管理页面，单击“主机节点”，可查看全部主机资产列表。

2.在主机列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、关联镜像详情和关联容器详情。

3.在主机列表页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

集群资产

最近更新时间: 2023-08-22 15:11:02

在资产管理页面，单击“集群总数”，进入集群检查页面，可查看全部集群资产。

集群资产

最近更新时间: 2023-08-24 09:44:16

在资产管理页面，单击“集群总数”，进入集群检查页面，可查看全部集群资产。

进程端口
进程

最近更新时间: 2023-08-23 09:36:20

- 在资产管理页面，单击“进程总数”，进入进程列表页面，可查看全部进程资产列表。

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

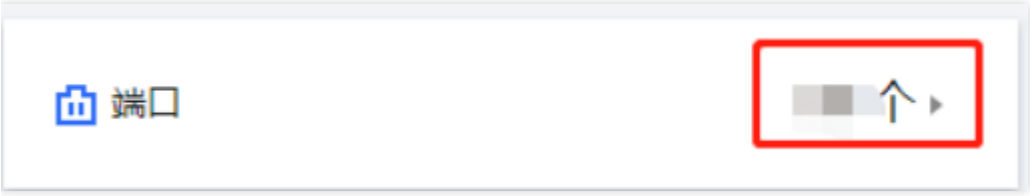
- 在进程列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。


主机详情
在线
基本信息
主机名
最近上线时间
2023-07-05 22:40:00
操作系统
CentOS Linux release 7.2.1511 (Core)
实例ID
主机来源
overlay专区服务器
所属项目
-
标签
-
AgentID
Kernel内核版本
3.10.0-514.26.2.el7.x86_64
Agent版本
4.6.1.0
Docker信息
Docker版本
18.06.1-ce
API版本
1.38
GO版本
go1.10.3
文件系统类型
overlay2
根目录
/var/lib/docker
关联资产
关联容器数
5
关联镜像数
3

查看端口模块

最近更新时间: 2023-08-24 09:44:16

在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。



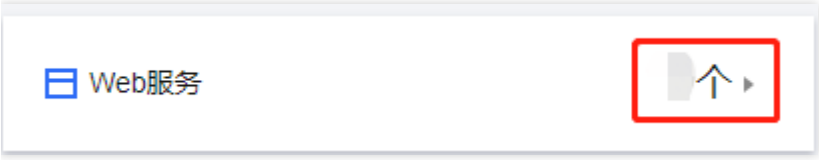
2.在端口列表页面，单击搜索框，通过“主机 IP、进程名和宿主机端口”等关键字可对端口进行查找。

3.在端口列表页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

应用web资产
Web 服务

最近更新时间: 2023-08-23 09:51:20

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



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

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

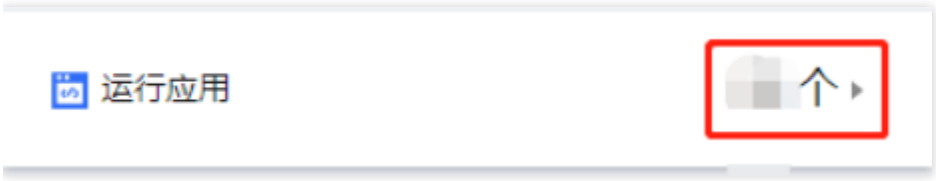
3.在 Web 服务列表页面，单击图标，弹

出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

查看运行应用

最近更新时间: 2023-08-24 09:44:08

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



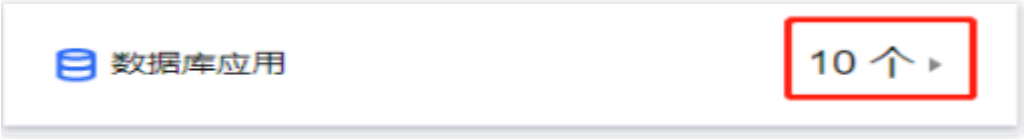
2.在运行应用列表页面，单击搜索框，可通过“容器名称、主机 IP 和应用类别”等关键字对运行应用进行查找

3.在运行应用列表页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

查看数据库应用

最近更新时间: 2023-08-24 09:44:08

1.在资产管理页面，单击“数据库应用总数”，进入运行应用列表页面，可查看全部数据库应用资产列表。



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

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

4.在数据库应用资产列表页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

漏洞管理

概述

最近更新时间: 2023-08-22 15:40:22

容器安全服务支持对本地镜像和仓库镜像上的漏洞，进行周期性和及时性的检测功能。支持对指定镜像和漏洞类别的检测，同时支持忽略漏洞等功能，可为您提供漏洞的风险、特征、严重等级及修复建议等信息，可视化界面有助于您更好的管理镜像的漏洞风险。

漏洞检测

最近更新时间: 2023-08-22 15:40:22

在漏洞管理页面，可进行漏洞检测并查看漏洞检测数据，单击一键检测。

一键检测设置：

查看漏洞

最近更新时间: 2023-08-22 15:40:22

1.在 漏洞管理界面，查看镜像检测到的系统漏洞、Web 应用漏洞、应急漏洞的漏洞信息。查看漏洞影响的本地镜像、仓库镜像、运行容器资产信息以及漏洞风险统计情况、TOP5漏洞、存在严重&高危漏洞镜像趋势。

- TOP5漏洞图：系统根据漏洞 CVSS 分数和动态风险等级等因素计算出漏洞 TOP5排名，并展示 TOP5漏洞的威胁等级、影响镜像数（只统计最新版本）和影响容器数量
- 严重&高危漏洞镜像趋势图：展示存在有严重或高危漏洞的镜像（最新版本）的数量变化趋势，当切换为运行容器时，展示存在有严重或高危漏洞且启动了容器的镜像（最新版本）的数量变化趋势。可查看7天或30天的趋势图。

2.在漏洞列表中，可以查看漏洞名称、威胁等级、CVE 编号、首次发现时间、最近检出时间等信息

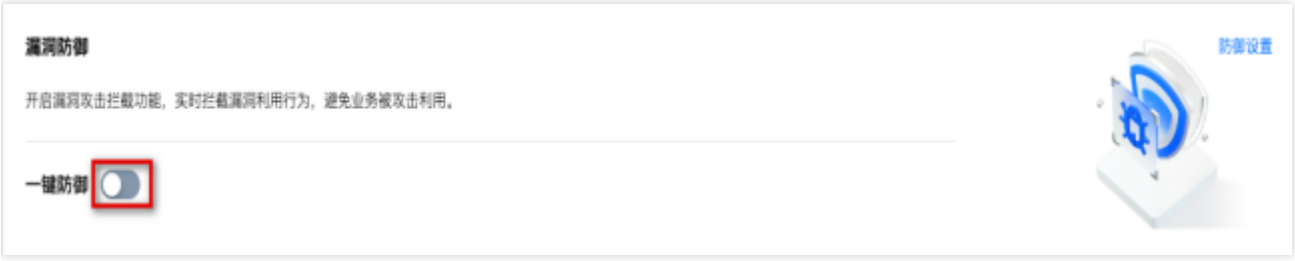
漏洞防御

最近更新时间: 2023-08-24 09:44:08

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

开启漏洞防御

1.在漏洞管理页面，开启一键防御开关，右侧抽屉展示漏洞防御配置页面。



2.在漏洞管理页面，单击右上角的漏洞设置。

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

查看防御漏洞

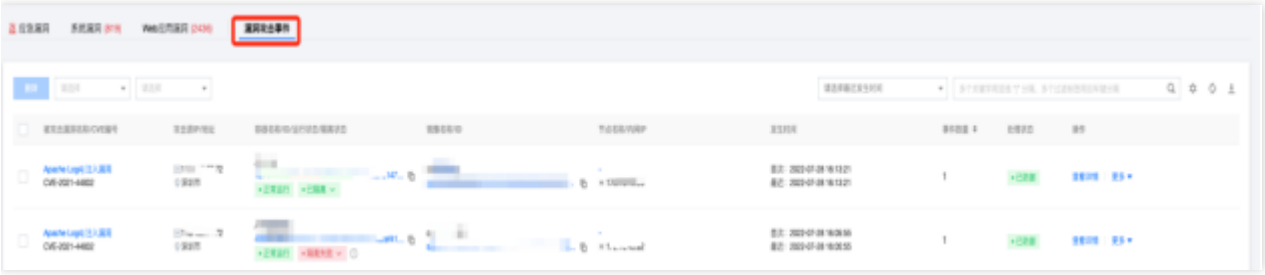
最近更新时间: 2023-08-22 15:40:22

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

漏洞攻击事件

最近更新时间: 2023-08-24 09:44:08

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



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

镜像风险管理

最近更新时间: 2023-08-23 16:28:08

本地镜像

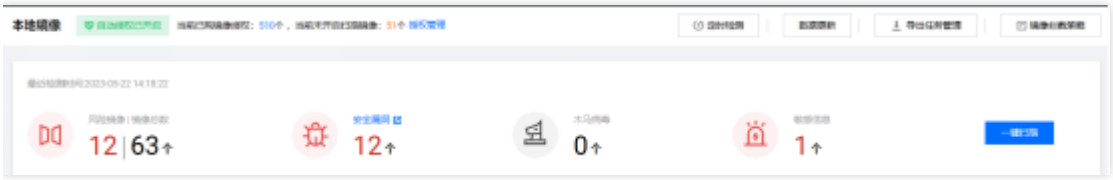
开启扫描数据

在本地镜像页面，单击右侧一键扫描，可重新扫描获取最新镜像数据或镜像风险信息。

在扫描设置页面，可根据需求选择检测风险类别和镜像范围

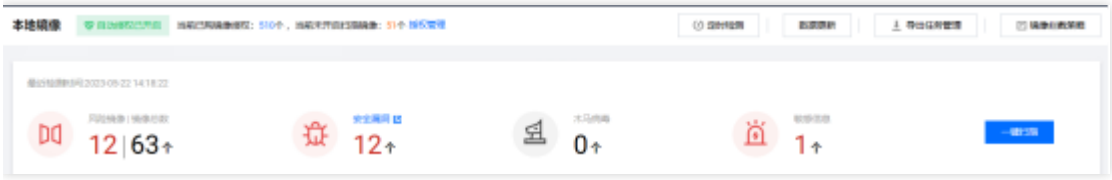
开启定时扫描

在本地镜像页面，单击右侧定时扫描设置，可自定义设置是否开启定时扫描功能。



1.在定时扫描设置页面，单击开启扫描开关，并根据需求设置定时扫描时间、检测风险类别和镜像范围。

开启数据更新



导出镜像资产

仓库镜像

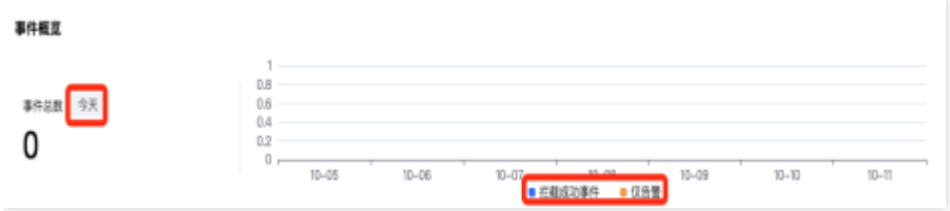
镜像拦截事件

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

事件概览

用户配置镜像启动拦截策略后，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录。

事件概览中，将对每日镜像启动拦截事件和仅告警的事件进行统计，展示近7日两类事件的趋势图和当前的事件总数



策略概览

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

事件列表

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

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

基线管理

概述

最近更新时间: 2023-08-22 15:46:42

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

容器

最近更新时间: 2023-08-24 09:44:08

在容器页面，基线概览窗口展示合规容器占比百分比和严重、高危、中危、低危四个威胁等级的检测项数量。

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

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

在容器抽屉中，单击基线检测项，可查看指定容器的基线检测情况。

查看检测信息

1.在容器页面，检测信息窗口展示容器资产最近一次的基线检测时间、检测耗时和自动检测周期配置。

在容器页面，单击重新检测，可立即对容器资产进行一次基线检测。

在容器页面，单击基线设置，可设置基线策略和基线忽略列表

设置基线策略

在基线策略设置页面，可通过单击图标开关开启或关闭当前基线标准的周期性检测。

2.在基线策略设置页面，单击检测周期设置，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。

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

4.点击确定，即可完成检测周期设置

镜像

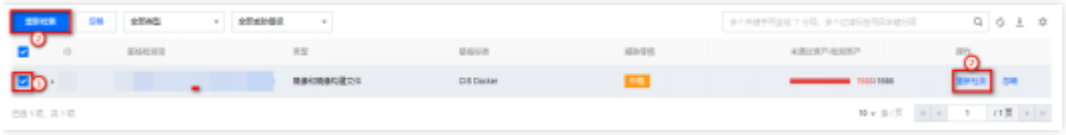
最近更新时间: 2023-08-24 09:44:08

在镜像页面，基线概览窗口展示合规镜像占比百分比严重、高危、中危、低危四个威胁等级的检测项数量。

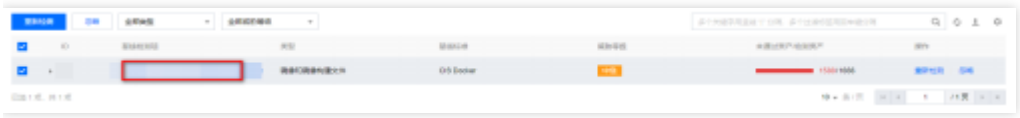
在镜像页面，单击百分比中的查看，可在弹出的镜像抽屉中查看镜像资产的检测结果列表。

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

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



在镜像抽屉中，单击基线检测项，可查看指定镜像的基线检测情况。



查看检测信息

1.在镜像页面，检测信息窗口展示镜像资产最近一次的基线检测时间、检测耗时和自动检测周期配置。

在镜像页面，单击重新检测，可立即对镜像资产进行一次基线检测。

3.在镜像页面，单击基线设置，可设置基线策略和基线忽略列表。

Docker主机

最近更新时间: 2023-08-23 16:31:17

1.在 Docker 主机页面，基线概览窗口展示合规主机占比百分比中严重、高危、中危、低危四个威胁等级的检测项数量。

2.在 Docker 主机页面，单击百分比中的查看，可在弹出的主机抽屉中查看主机资产的检测结果列表。

3.在 Docker 主机抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对主机资产的检测结果进行查询。

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

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

查看检测信息

1.在 Docker 主机页面，检测信息窗口展示主机资产最近一次的基线检测时间、检测耗时和自动检测周期配置。

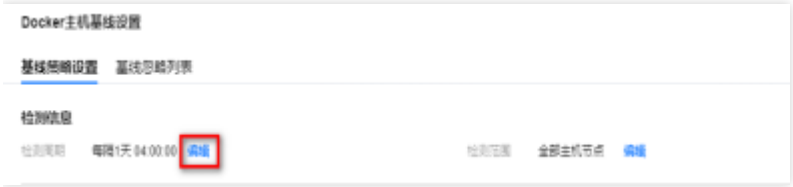
在 Docker 主机页面，单击重新检测，可立即对主机资产进行一次基线检测。

在 Docker 主机页面，单击基线设置，可设置基线策略和基线忽略列表。

设置基线策略

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

2.在基线策略设置页面，单击检测周期的编辑，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。



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

4.点击确定，即可完成检测周期设置

Kubernetes

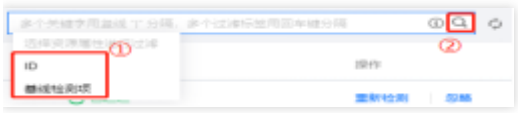
最近更新时间: 2023-08-24 09:44:08

查看 Kubernetes 概览

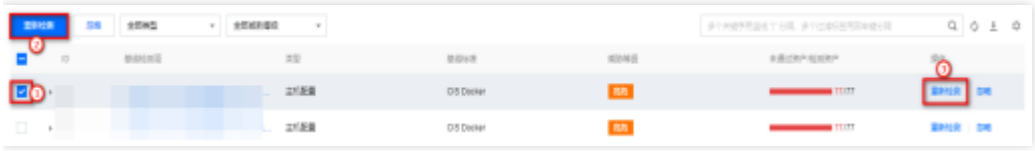
在 Kubernetes 页面，基线概览窗口展示合规 K8S 检测项通过率占比以及严重、高危、中危、低危四个威胁等级的检测项数量

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

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



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



查看检测信息

在 Kubernetes 页面，检测信息窗口展示 Kubernetes 基线检测项最近一次的基线检测时间、检测耗时和自动检测周期配置。

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

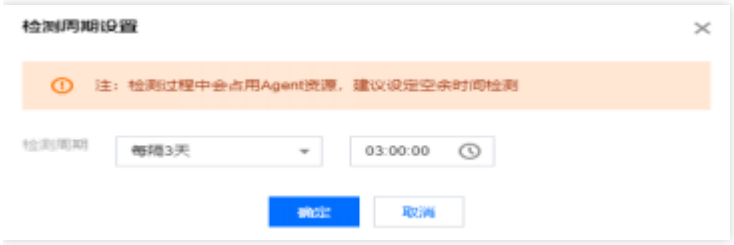
2.在 Kubernetes 页面，单击基线设置，可设置基线策略和基线忽略列表。

设置基线策略

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

2.在基线策略设置页面，单击检测周期的编辑，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。

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



4.点击确定，即可完成检测周期设置

运行时安全

概述

最近更新时间: 2023-08-22 16:24:58

- 运行时安全支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供容器逃逸、反弹 Shell 和文件查杀安全功能。
- 容器逃逸：指的是容器利用系统漏洞，“逃逸”出了其自身所拥有的权限，实现了对宿主机和宿主机上其他容器的访问。由于容器与宿主机共享操作系统内核，为了避免容器获取宿主机的 root 权限，通常不允许采用特权模式运行容器。按照入侵者执行容器逃逸的顺序，容器安全服务将风险事件类型划分为三类，分别是：风险容器、程序提权、容器逃逸。
- 风险容器：指当前容器存在部分潜在风险行为，可能会存在被提权或被逃逸的风险，包含敏感路径挂载、特权容器。
- 程序提权：指当前容器出现了提权的风险行为，可能会进一步导致其逃逸，需要您进行关注。
- 容器逃逸：指当前容器已经出现了逃逸行为，此时您应该立即对出现的风险事件进行关注，并立即通过推荐解决方案进行对应的处置响应。
- 反弹shell：基于建行云安全技术及多维度多手段，对 Shell 反向连接行为进行识别记录，为您运行时容器提供反弹 Shell 行为的实时监控能力。
- 文件查杀：通过实时监测运行容器调用的文件是否存在风险；或手动触发一键扫描，检查容器内是否存在恶意的木马病毒、webshell 等。

容器逃逸
查看设置状态

最近更新时间: 2023-08-24 09:44:07

1.在容器逃逸页面，安全状态模块展示是否存在容器逃逸事件。如检测发现容器逃逸事件，建议立即处理。

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

查看容器逃逸列表

最近更新时间: 2023-08-24 09:44:07

筛选刷新容器逃逸

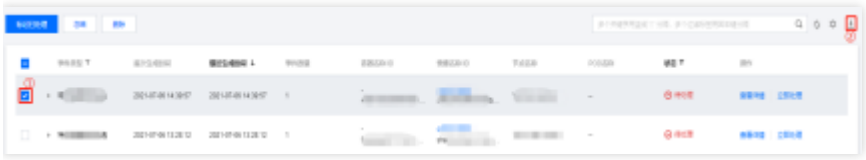
在容器逃逸页面，单击搜索框，可通过“容器名称、镜像名称和节点名称”等关键词对容器逃逸事件进行查询。

1.在容器逃逸页面，单击操作栏右侧图标，即可刷新容器逃逸事件。

导出容器逃逸

最近更新时间: 2023-08-24 09:01:36

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



自定义列表管理

最近更新时间: 2023-08-24 09:01:36

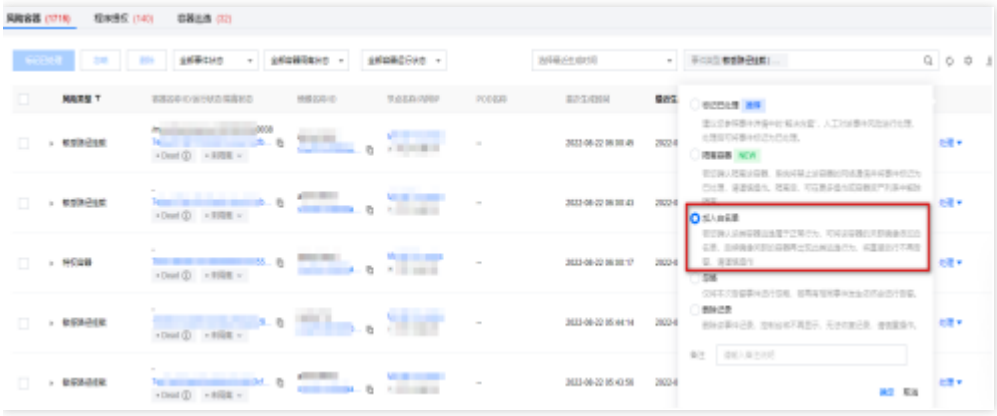
1.在容器逃逸页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。
2.在自定义列表管理弹窗，选择所需的类型后，单击确定，即可完成设置自定义列表管理。

逃逸白名单

最近更新时间: 2023-08-24 09:01:36

加白告警事件

在容器逃逸界面，如需对告警事件进行加白，单击处理，选择加入白名单，单击确定。



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

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

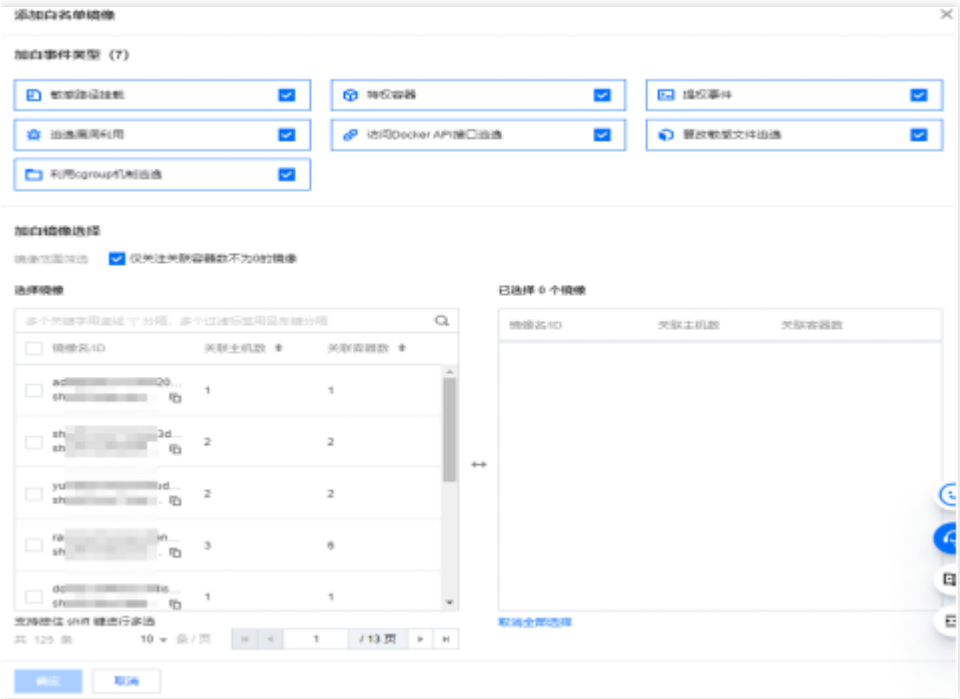
白名单管理

用户也可在白名单管理页面，批量新增白名单，避免后续产生告警。

添加白名单

1.在 容器逃逸> 白名单管理页面，单击添加白名单策略。

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



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

编辑白名单

在 容器逃逸> 白名单管理页面，单击目标镜像操作列的编辑加白类型。

在编辑加白事件类型对话框中，修改加白事件类型，单击保存。

删除白名单

1.在容器逃逸 > 白名单管理页面，可删除单个白名单或批量删除白名单。

2.在确认删除对话框中，单击确认，即可删除目标白名单。

反弹Shell
事件列表

最近更新时间: 2023-08-24 09:46:32

删选刷新事件列表

1.在事件列表页面，单击搜索框，可通过“进程名称、父进程名称”等关键词对反弹 Shell 事件进行查询。

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

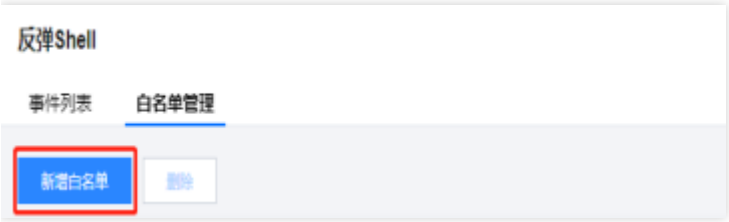
导出事件列表

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

配置白名单

新增白名单

在白名单管理页面，单击新增白名单，右侧弹出新增白名单设置页面

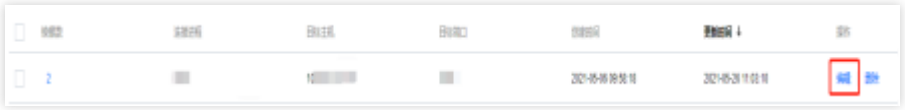


2.在新增白名单设置页面，需配置白名单生效的目标地址、连接进程和选择白名单生效范围。

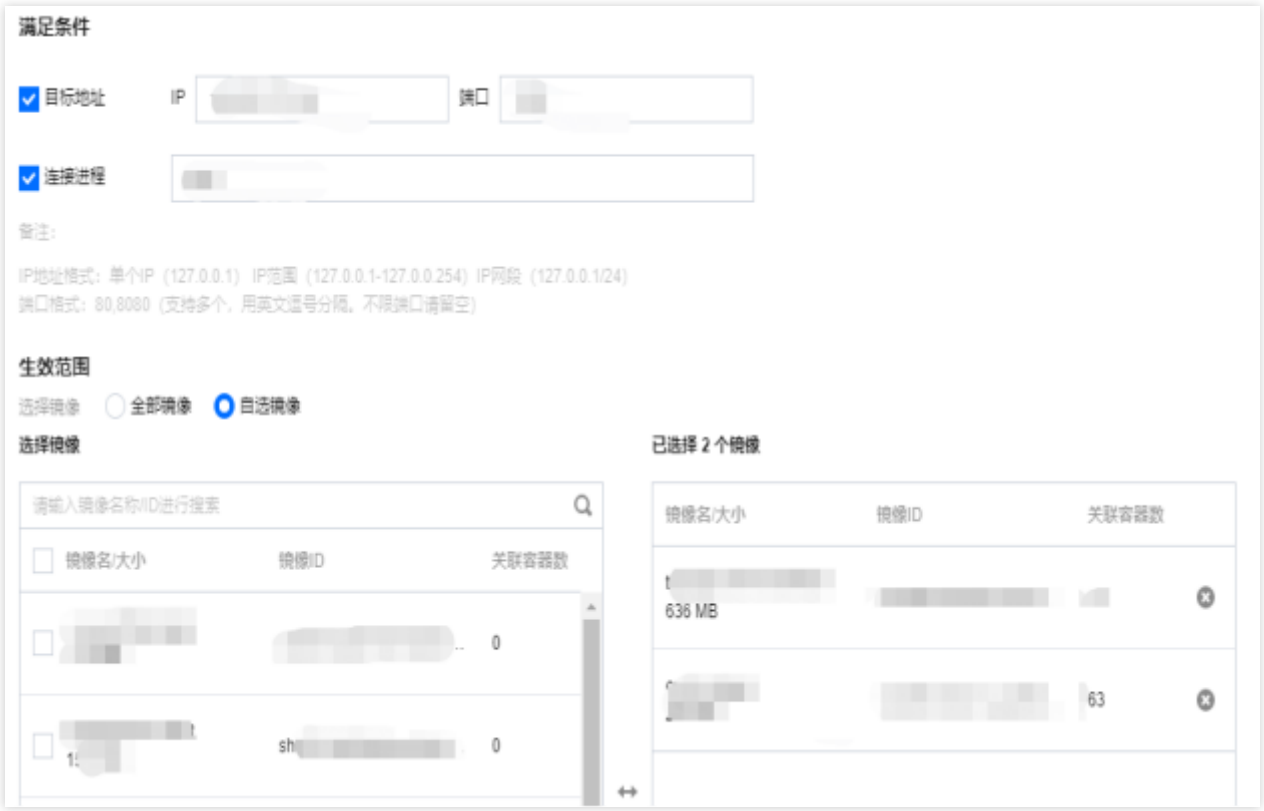
- 单击目标地址左侧图标，输入目标地址的 IP 和端口。
- 单击连接进程左侧图标，输入支持命令行通配符。
- 白名单生效范围为全部镜像或自选镜像。其中单击所需的自选镜像或图标，即可选中或删除自选镜像
- 选择所需内容后，单击确定或取消，即可完成或取消新增白名单。
- 配置完成后，满足条件的目标地址和连接进程将直接放行不再告警。

  编辑白名单

  1.在白名单管理页面，单击右侧编辑，右侧弹出编辑白名单设置页面。



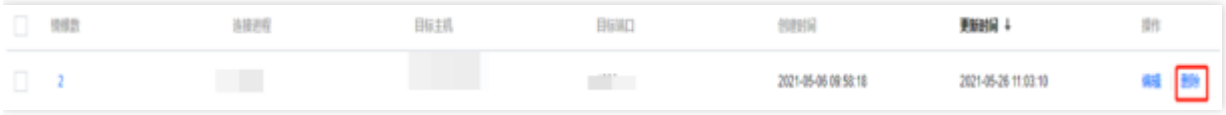
2.在编辑白名单设置页面，可修改白名单生效的目标地址、连接进程和白名单生效范围。



3.选择所需内容后，单击确定或者取消，即可完成或者取消修改白名单

删除白名单

1.在白名单管理页面，单击右侧删除，弹出“确认删除”弹窗。



2.在“确认删除”弹窗中，单击删除或取消，即可删除或取消删除白名单。

文件查杀

最近更新时间: 2023-08-24 09:10:32

查看风险趋势

在文件查杀页面，可以查看待处理风险、影响容器的数量和趋势。

- □待处理风险：展示近7天待处理风险趋势图和较昨日新增风险数据。将鼠标悬停在趋势图上，展示某一天的待处理风险数据
- □待处理风险：展示近7天待处理风险趋势图和较昨日新增风险数据。将鼠标悬停在趋势图上，展示某一天的待处理风险数据

设置风险检测

在 文件查杀页面 的风险检测模块，支持对定时检测和实时监控功能进行设置。

设置定时检测

1.在风险测模块，单击定时检测右侧的，进入定时检测设置页面。

2.在定时检测设置页面，单击，开启定时检测，并依次设置检测时间、检测路径、检测范围。

参数说明：

- 实时检测开关：支持通过单击“开关”，可开启或关闭实时检测功能。
  检测时间
- 检测周期：包括每天、每隔三天、每隔七天。
- 开始检测时间：配置定时任务何时开始扫描。
- 超时时长：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。
  检测路径
- 全部路径：检测容器内全部文件路径。
- 自选路径：按自选的配置路径检测容器内文件。
- 主机节点：选择主机节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。
- 容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器

设置实时监控 1.在风险检测模块，单击实时监控右侧的，进入实时监控设置页面。

2.在实时监控设置页面，单击，开启实时监控，配置相关参数

参数说明：

□实时监控开关：支持通过单击或开启或关闭实时监控功能。

□检测路径

□全部路径：检测容器内全部文件路径。

□自选路径：按自选的配置路径检测容器内文件。

□选择路径：根据实际需求选择检测以下文件路径或检测除以下文件路径外的其他路径。单击可添加多个路径，最多为30个。

3.单击保存设置，即可完成实时监控设置

设置一键检测

1.在风险检测模块，单击一键检测，进入一键检测页面。

2.在一键检测页面，选择检测路径、检测范围，并设置超时时间。

参数说明：

o检测路径：

□全部路径：检测容器内全部文件路径。

□自选路径：按自选的配置路径检测容器内文件。

o检测范围：

□主机节点：选择主机节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。

□容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器。

□超时设置：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。

3.单击开始检测，即按配置条件开始扫描容器内文件

查看最后一次检测结果

在风险检测模块，单击最近一次检测结果，可查看近一次扫描任务详情。

检测详情展示内容：

□检测详情概览

o近一次扫描任务是否发现风险文件，如有发现，将展示风险文件数量、风险容器数量和扫描容器数量。

o近一次扫描任务开始检测和结束检测时间。

□检测详情列表：展示近一次扫描任务扫描出的风险文件概况，按容器资产进行聚合。

o列表字段包括：容器名称/ID、镜像名称/ID、主机节点名称/IP、检测状态、检测用时、风险数和操作项。

□支持对扫描任务进行重新检测，或停止正在检测中的任务。

□支持按主机名称、主机 IP、容器名称、容器 ID、镜像名称、镜像 ID 进行检索。

□单击可查看风险文件的文件名称、文件路径、病毒名称和查看详情按钮；单击查看详情，可查看恶意文件详情。

查看事件列表

在文件查杀页面 的事件列表模块中，展示模块中提供容器木马病毒检测结果。

筛选事件

在事件列表模块中，支持通过如下两种方法对事件进行筛选。

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

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

查看详情

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

处理事件

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

参数说明：

□添加白名单：若您确认该文件无恶意并添加白名单，系统将不再对该文件进行检测，请谨慎操作。

□隔离（推荐）：隔离此病毒文件，让黑客无法再次启动它，便于您定位病毒文件位置，对其进行查杀。

□忽略：仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。

□删除：删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

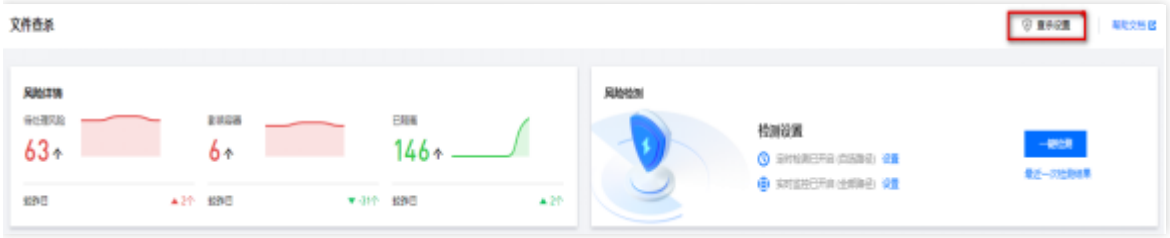
自动隔离文件

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

系统自动隔离文件

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

1.在文件查杀页面，单击右上角的查杀设置。



2.在查杀设置窗口中，单击自动隔离文件。

3.在系统自动隔离文件模块，可单击开启或关闭自动隔离，同时，支持隔离并结束恶意文件相关进程

用户自定义隔离文件

1.在文件查杀页面，单击右上角的查杀设置。

2.在文件查杀设置窗口中，单击自动隔离文件。

3.在用户自定义隔离文件模块，支持控制自动隔离开关、查看详情和下载文件。

操作说明：

o单击自动隔离开关，可开启或关闭自动隔离。

o单击详情查看恶意文件的基本信息、危害描述和修复建议。

o单击下载，可下载该恶意文件。

隔离文件列表

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

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

恶意外连

最近更新时间: 2023-08-24 09:31:06

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

1.检查容器内的恶意进程及非法端口，删除可疑的启动项和定时任务。

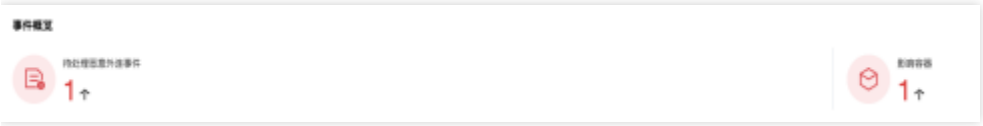
2.对容器存在的风险进行排查，如进行漏洞扫描、木马扫描等

3.对容器所使用的镜像进行加固，并替换运行中的容器。

事件列表

事件概览

在事件列表页面的事件概览中，将根据系统上报的安全事件，实时统计待处理的恶意外连事件及其影响的容器数量。



事件列表

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

查看详情

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

处理事件

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

2.在二次确认窗口中，进行如下操作：

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

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

□隔离容器：若您确认隔离该容器，系统将禁止该容器的网络通信并将事件标记为已处理，请谨慎操作。单击确定隔离后，可在更多操作或容器资产列表中解除隔离。

□忽略：单击确定，仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。 □删除：单击删除，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。 **黑白名单管理**

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

□黑名单：当容器向名单中的域名发起外连请求时，系统将判定为恶意外联行为，为您产生实时告警，可前往 事件列表 查看。

□白名单：当容器向白名单中的域名发起外连请求时，系统将直接放行，不再进行告警。 **黑名单管理**

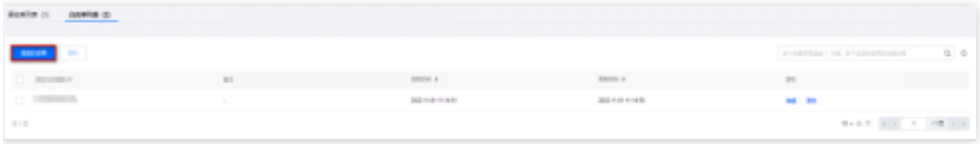
1.在黑名单列表页签，单击添加黑名单。

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

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

白名单管理

在白名单列表页签，单击添加白名单。



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

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

高级防御

最近更新时间: 2023-08-24 10:23:13

概述

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

异常进程：通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并告警通知或拦截。系统监控策略包括代理软件、横向渗透、恶意命令、反弹 Shell、无文件程序执行、高危命令、敏感服务异常子进程启动等。

文件篡改：通过系统规则和用户自定义检测规则，实时监控核心文件被修改的文件异常访问行为，并告警通知或拦截。系统监控策略包括篡改计划任务、篡改系统程序、篡改用户配置等。

高危系统调用：基于建行云云安全自适应学习技术，实时审计容器内发起的可能引起安全风险的 Linux 系统调用行为。

异常进程

事件列表

筛选刷新事件列表

1.在事件列表页面，单击搜索框，可通过“连接进程”关键词对白名单事件进行查询。

2.在事件列表页面，击操作栏右侧刷新图标，即可刷新事件列表。

导出事件列表

1.在事件列表页面，单击刷新勾选选所需的异常进程事件后，单击刷新图标即可导出异常进程事件

自定义列表管理

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

列表重点字段说明

列表重点字段说明

1.首次生成时间：该异常进程事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2.最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3.事件数量：聚合时间范围内该异常进程事件触发告警的总数量。

4.动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。

5.状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

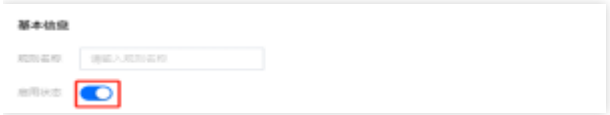
筛选刷新规则

新增规则

1.在规则配置页面，单击创建规则，右侧抽屉弹出新增规则页面

2.在新增规则页面，需配置基本信息、配置规则和镜像生效范围

(1)基本信息：输入事件的规则名称，单击图标开启或关闭规则检测



(2)配置规则：需输入进程路径和执行动作，单击添加或者删除，可以进行添加或者删除规则

(3)镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像，即可选中或者删除自选镜像

复制规则

1.在规则配置页面，单击右侧复制，右侧弹出复制规则页面

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

编辑规则

1.在规则配置页面，单击右侧编辑，右侧弹出编辑规则设置页面。

2.在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。

3.选择所需内容后，单击确定或者取消，即可完成或取消修改规则

删除规则

1.在规则配置页面，可选择如下两种方式删除规则：

(1)选择所需的规则单击图标，单击操作栏左侧删除，弹出确认删除弹窗

(2)选择所需规则的所作行，单击右侧删除，弹出“确认删除”弹窗。

2.在确认删除弹窗中，单击删除或者取消，即可删除或者取消删除规则

导出规则

1.在规则配置页面，单击图标勾选所需的异常进程规则后，单击下载图标即可导出异常进程规则

自定义列表管理

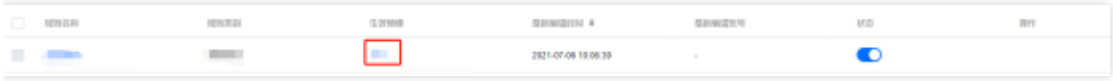
1.在规则配置页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

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

列表重点字段说明

1.规则类别：系统规则或自定义规则。

2.生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。



3.状态：启用/禁用

4操作：系统策略操作栏仅复制规则，用户自定义规则支持复制、编辑和删除。

文件篡改

事件列表

筛选刷新事件列表

1.在事件列表页面，单击搜索框，可通过“文件名称、进程路径和命中规则”等关键词对文件篡改检测结果进行查询。

导出检测结果

1.在事件列表，勾选所需的文件篡改检测事件后，单击下载图标可导出文件篡改检测事件

更改事件状态

1.在事件列表页面，可对文件篡改检测事件进行标记已处理、忽略和删除处理。

2.单击确定或取消，即可完成或取消事件状态更改。

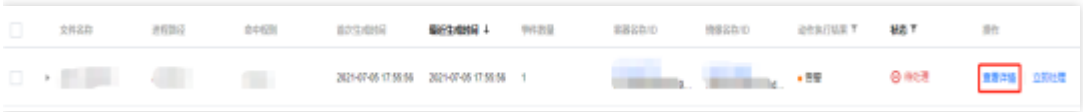
3.在事件列表页面，事件状态为已忽略时，可单击取消忽略或删除，可将事件取消忽略或删除。

4.在事件列表页面，事件状态为已处理时，可单击删除，删除该事件。

查看事件详情

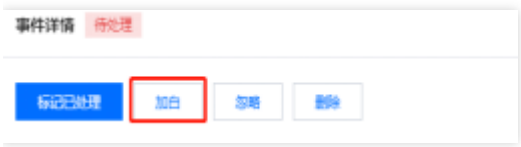
1.在事件列表页面，单击进程路径左侧 图标，可查看事件描述。

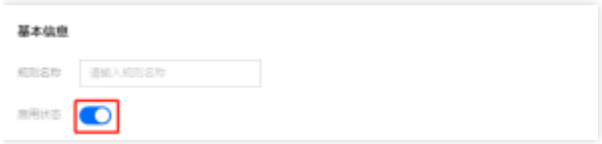
2.在事件列表页面，单击查看详情，右侧弹出事件详情页面。



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

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





自定义列表管理

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

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

列表重点字段说明：

1.首次生成时间：该文件篡改事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2.最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3.事件数量：聚合时间范围内该文件篡改事件触发告警的总数量。

4.动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。

5.状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

筛选刷新规则

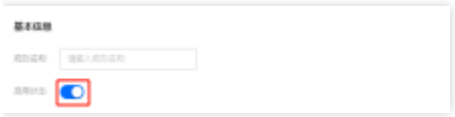
1.在规则配置页面，单击搜索框，可通过规则名称关键字对配置规则进行查询

2.在规则配置页面，单击操作栏右侧刷新图标

新增规则

1.在规则配置页面，单击创建规则，右侧抽屉弹出新增规则页面。

2.在新增规则页面，需配置基本信息、配置规则和镜像生效范围



复制规则

1.在规则配置页面，单击右侧复制，右侧弹出编复制规则页面。

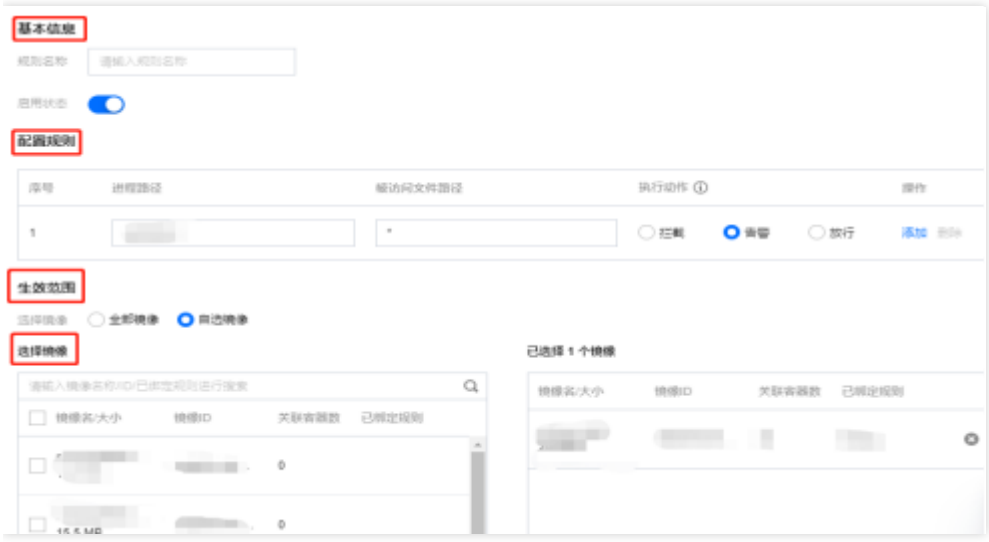
2.在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围

。

编辑规则

1. 在规则配置页面，单击右侧编辑，右侧弹出编辑规则设置页面。

2. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。



删除规则

单击操作栏左侧删除，弹出“确认删除”弹窗。

导出规则

在规则配置页面，单击图标勾选所需要的文件篡改规则后，单击下载图标可导出文件篡改规则

自定义列表管理

1. 在规则配置页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗以自定义设定列表管理。
2. 在自定义列表管理弹窗，选择所需的类型后，单击确定，即可完成设置自定义列表管理。

列表重点字段说明

1.规则类别：系统规则或自定义规则

2.生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。

3.状态：启用/禁用

4.操作：系统策略操作栏仅复制规则；用户自定义规则支持复制、编辑和删除。

高危系统调用

事件列表

筛选刷新事件列表

1. 在事件列表页面，单击搜索框，可通过“进程路径、系统调用名称和容器名称”等关键词对高危系统调用检测事件进行查询。

2. 在事件列表页面，单击操作刷新图标，即可刷新事件列表

导出事件列表

在事件列表页面，单击勾选所需的文件篡改检测事件后，单击下载图标即可导出高危系统调用事件

更改事件状态

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

2.单击确定或取消，即可完成或取消事件状态更改。

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

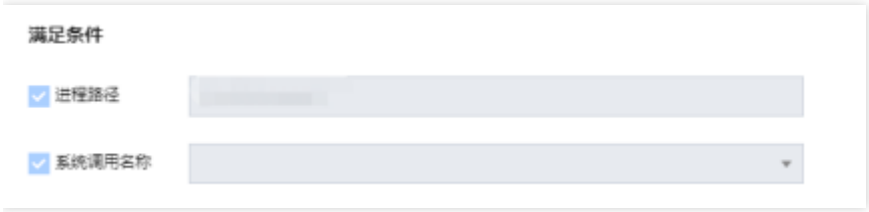
4. 在事件列表页面，事件状态为已处理时，可单击删除，删除该事件。

查看事件详情

1. 在事件列表页面，单击进程路径左侧图标，可查看事件描述

2. 在事件列表页面，单击查看详情，右侧弹出事件详情页面。

3. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。
4. 在事件详情页面，单击加白进入新增白名单页面，需确认满足条件（进程路径、系统调用名称）和镜像生效范围。



自定义列表管理

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

列表重点字段说明

1. 首次生成时间：该系统调用事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。

4. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。

5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

白名单管理

筛选刷新白名单

1. 在白名单管理页面，单击搜索框，可通过“进程路径、系统调用名称”关键词对配置的白名单进行查询。

2. 在白名单管理页面，单击操作栏右侧图标，即可刷新白名单管理列表

新增白名单

1. 在白名单管理页面，单击新增白名单，右侧弹出新增白名单设置页面

2.在新增白名单设置页面，需配置白名单生效的进程路径、系统调用名称和生效范围

编辑白名单

1.在白名单管理页面，单击右侧编辑，右侧弹出编辑白名单设置页面。

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

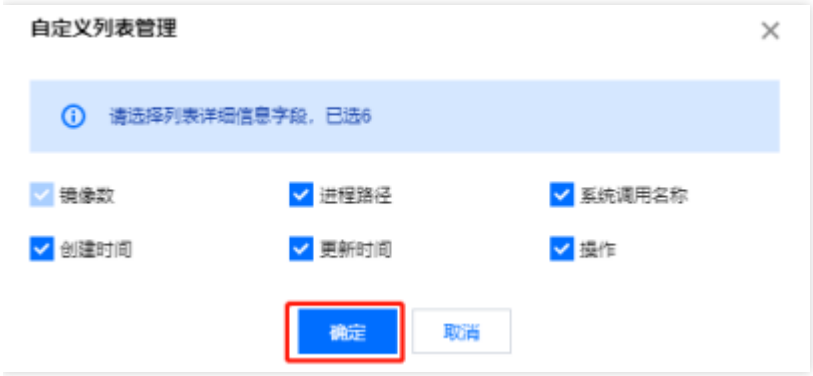
删除白名单

3. 在白名单管理页面，单击右侧删除，弹出“确认删除”弹窗。

2.在“确认删除”弹窗中，单击删除或取消，即可删除或取消删除白名单。

自定义列表管理

1. 在白名单管理页面，单击图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。



列表重点字段说明

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

K8S API异常请求

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

(1) 系统策略：基于建行云安全技术及多维度多种手段，通过匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 pod 创建、可疑容器创建等共9个规则类型，对集群 API 异常请求行为进行监测。

(2) 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求。

事件列表

安全状态和事件趋势

1. 安全状态将根据系统上报的安全事件，实时统计待处理的 K8s API 异常请求事件，以及按高危、中危、低危、提

示来统计安全事件数量。

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

事件列表

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

查看详情

处理事件

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

2. 在二次确认窗口中，进行如下操作

(1) 标记已处理：建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，单击确定，处理后可将事件标记为已处理。

(2) 添加白名单：配置相关参数，单击确定。

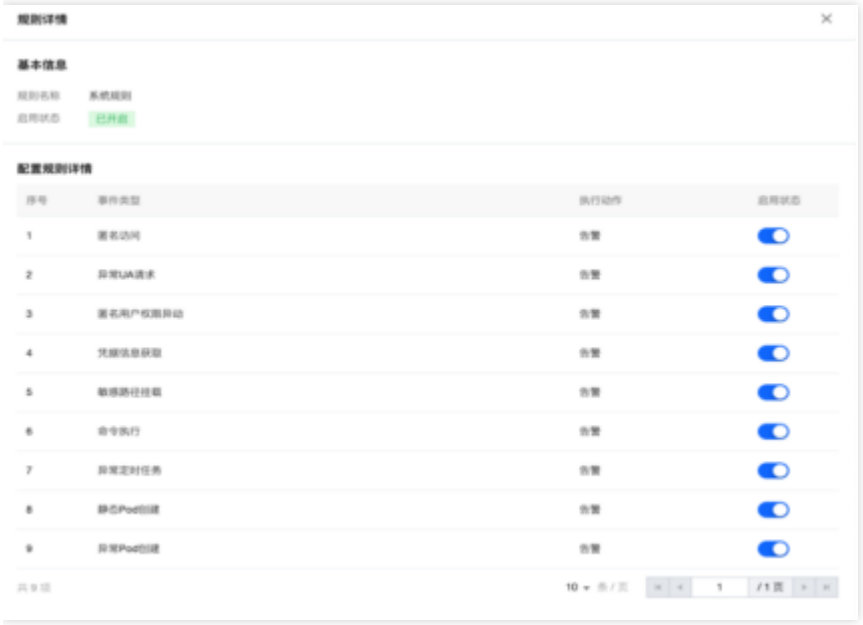
(3) 忽略：单击确定，仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

(4) 删除记录：单击确定，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

规则配置

系统规则

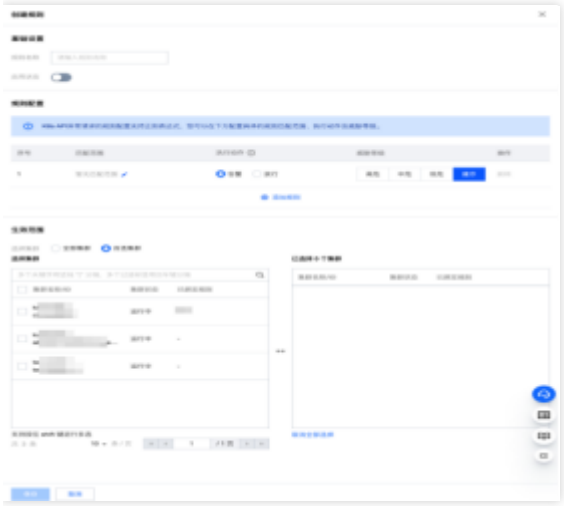
在规则配置页面，开启或关闭系统规则和自定义规则。单击系统规则名称，可查看全部系统规则类型，如下图所示。用户也可以通过此页面，关闭部分系统规则类型。



自定义规则

除容器安全服务产品提供的系统规则，用户也可以自定义创建规则。

在规则配置页面，单击创建规则，配置相关参数，单击保存。



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

策略管理
镜像拦截策略

最近更新时间: 2023-08-24 10:23:13

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

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

查看策略概览

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

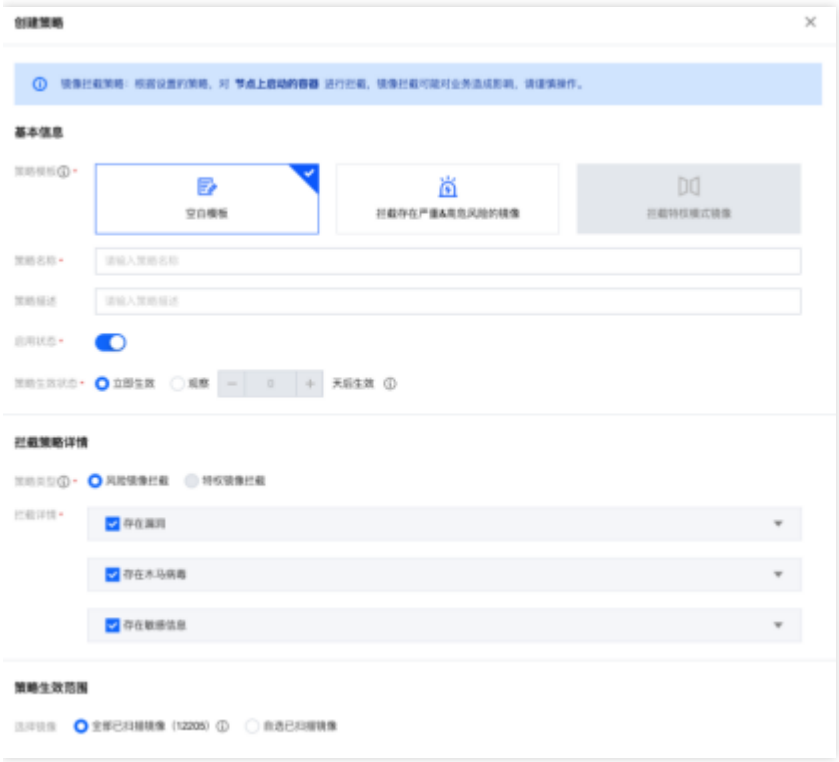
查看事件概览

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

创建策略

1. 在镜像拦截策略页面，单击创建策略，配置相关参数，单击确定。

(1) 新建风险镜像拦截策略



(2) 新建特权模式镜像拦截策略

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

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

管理策略

• 查看：在镜像拦截策略页面，单击镜像拦截策略名称，查看拦截策略详情，

• 开启或关闭：通过开启或关闭启动状态列的按钮调整策略是否生效。

o 开启后，开始执行镜像拦截动作，或观察期开始倒计时。

o 关闭时，策略不生效。

• 编辑：单击编辑，对策略的名称、描述、启动状态、策略生效状态、拦截策略详情、策略生效范围进行调整；策略模板不可调整。

日志分析

概述

最近更新时间: 2023-08-24 10:28:30

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

背景信息

最近更新时间: 2023-08-24 10:28:30

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

- 容器 bash 日志：提供 bash 日志审计，帮助用户溯源异常进程。
- 容器启动审计日志：提供容器启动日志审计，帮助用户记录容器启动行为。
- Kubernetes API 审计日志：帮助用户记录 k8s API 调用的日志。

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》规定，日志存储时长不少于6个月，建议用户对核心资产开启日志审计功能，根据实际所需购买存储，以便采集和留存日志数据。

容器安全服务专业版提供日志采集功能，建议用户购买专业版后再购买日志存储。若已购买日志存储，但出现容量不够的情况，此时日志分析服务将会对历史日志数据进行清理，建议用户及时升级扩容。

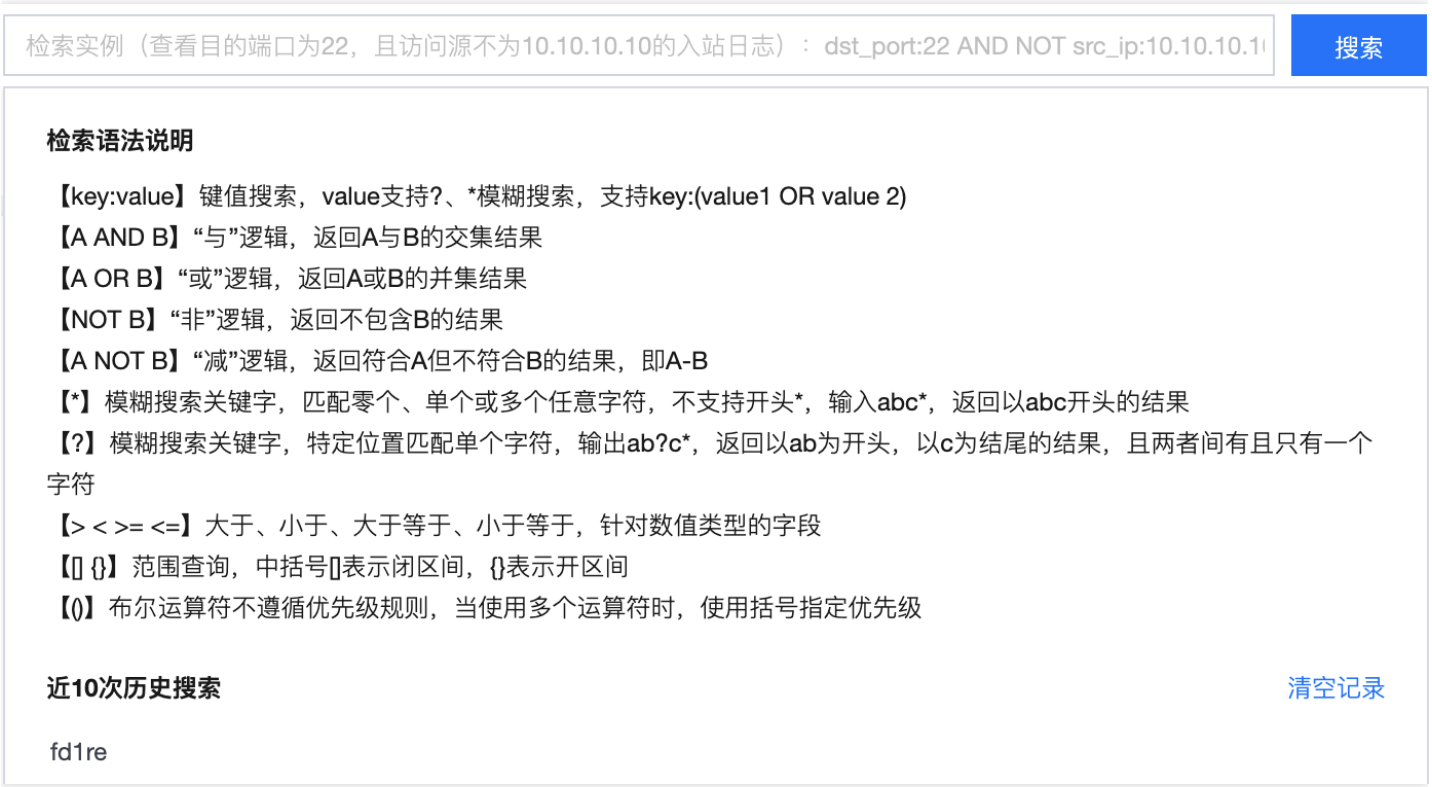
查询日志

最近更新时间: 2023-08-24 10:31:09

1. 在日志分析页面，检索日志分析结果并进行相关操作。
   (1) 按时间类型筛选日志：在日志分析页面上方，支持按时间（近15分钟、近60分钟、近12小时、近24小时、今天、近7天、近14天、近30天、近90天及自定义日期）、日志类型筛选日志分析结果，选择需要查看的时间和日志类型，单击确定即可。

(2) 按纪录字段筛选日志：在日志分析页面上方，支持按日志记录字段筛选，提供手动输入字段、自动输入字段两种方式

① 手动输入字段：在输入框内以字段名和字段值成对的形式输入需要筛选的字段，单击搜索即可。可参考下图检索语法说明。



② 自动输入字段：单击搜索模板，选中需要复用的查询模板名称即可。或单击筛选输入框中的历史纪录，如上图所示。复用查询模板，需用户在手动输入查询语句时，单击保存搜索以达到保存当前配置（日志类型、检索语句）的目的。

③ 快速检索查看日志趋势图：

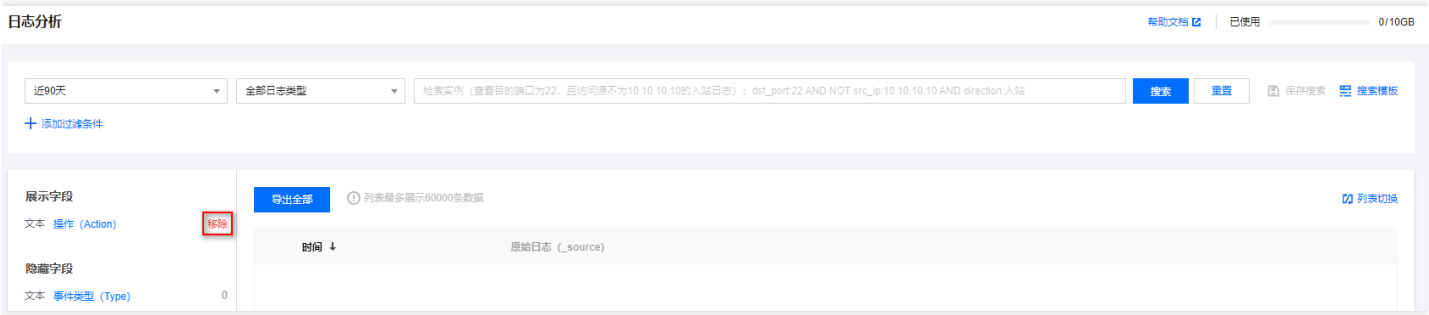
1) 方法一：为了方便对指定时间范围内的日志量进行查看，您可以滑动鼠标快速查看日志趋势图上的“蓝色柱形图”，查看日志统计时间和日志量

2) 方法二：单击日志趋势图“蓝色柱形图”，可进一步对日志进行放大检索。

(3) 在日志分析页面的日志列表中，根据“展示字段”模块内容，在列表中展示并查看相关字段详情。展示字段中为“原始日志（_source）”时，列表中展示所有日志字段。列表最多展示60000条数据。

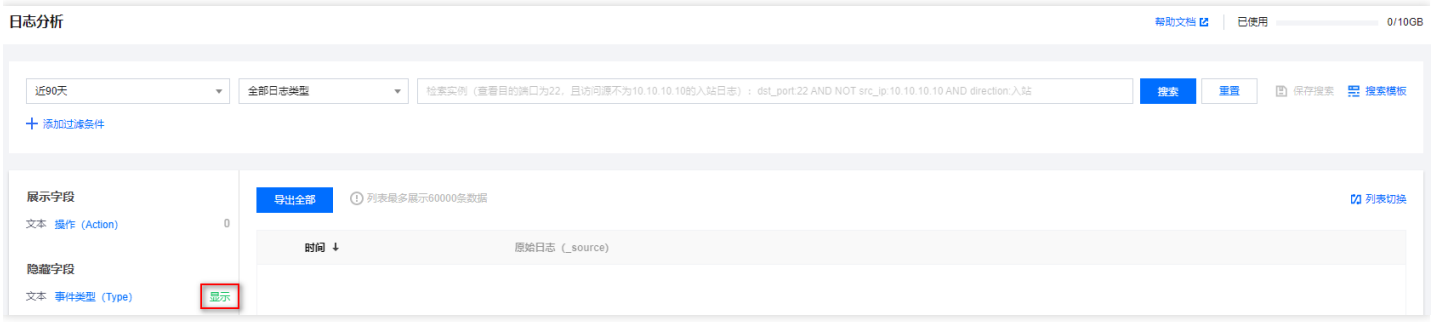
① 自定义需要展示或隐藏的字段：

② 显示：将鼠标移动至隐藏字段上方，在隐藏字段右侧，单击显示，该隐藏字段将出现在展示字段中，列表中仅展示选定显示的字段，其他隐藏字段不展示



1) 隐藏：将鼠标移动至展示字段上方，在展示字段右侧，单击移出，该隐藏字段将在展示字段中删除，对应右侧日

志列表将不再展示该字段内容



③ 导出：在字段详情左上角，单击导出全部，日志分析会将满足检索条件的60000条日志导出为文件，并通过浏览器下载到本地。

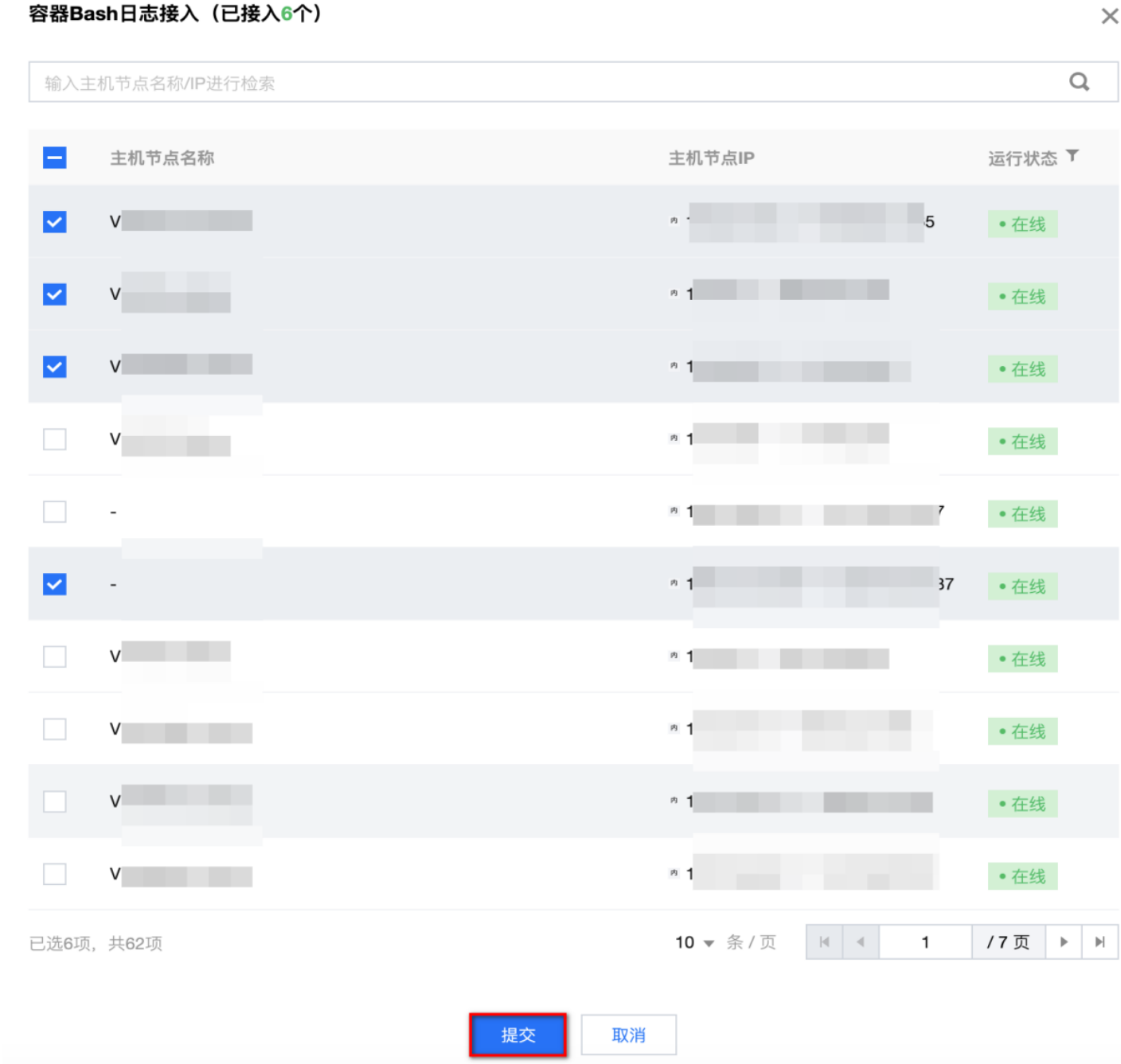
④ 切换表格列展示：在字段详情右上角，单击列表切换，可将展示字段切换为表格列展示。

配置日志
日志接入

最近更新时间: 2023-08-24 10:34:15

1. 在日志接入页面，支持对容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志是否开启采集进行配置。在“是否接入日志”列开启开关，即可对该类日志进行采集。关闭按钮，即不对该类日志进行采集。

2. 在日志接入页面，单击已接入资产列的编辑，即可配置采集日志的节点范围。勾选需要采集日志的主机节点，单击提交后，配置生效。


容器Bash日志接入（已接入6个）
输入主机节点名称/IP进行检索
主机节点名称
主机节点IP
运行状态
在线
已选6项，共62项
10 条 / 页
1
/ 7 页
提交
取消

日志清理

最近更新时间: 2023-08-24 10:34:15

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

告警设置

前提条件

最近更新时间: 2023-08-24 09:53:21

请确认消息订阅中“安全消息-安全事件通知”已打开，单击 设置。

事件类型

告警设置中事件类型、默认告警时间和告警如列表所示：

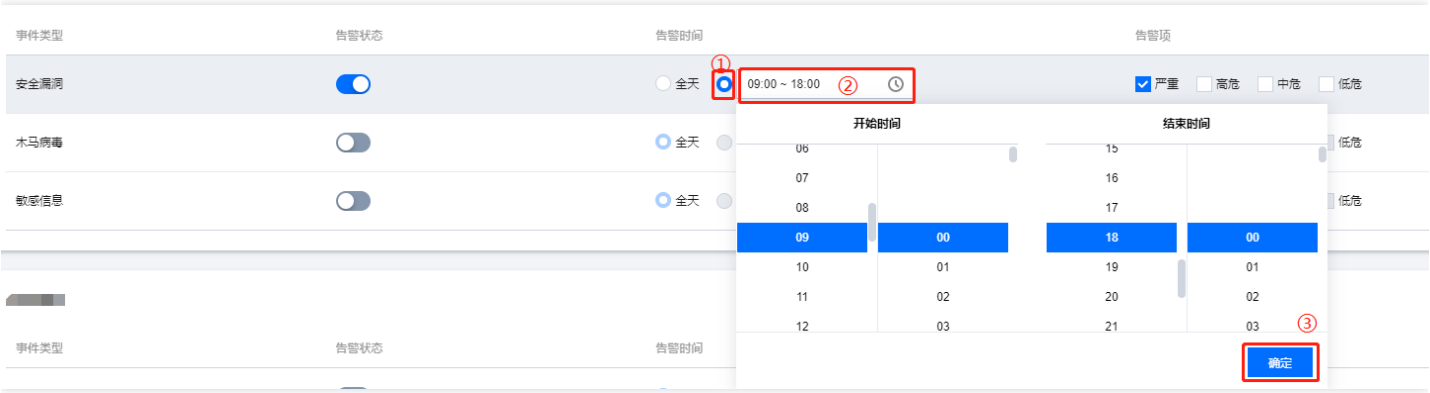
事件类型	默认告警时间	默认告警项
安全漏洞	全天	严重
木马病毒	全天	严重、高危、中危、低危
敏感信息	全天	严重、高危、中危、低危
容器逃逸	全天	-
异常进程	全天	拦截失败、告警
文件篡改	全天	拦截失败、告警
反弹 Shell	全天	-
文件查杀	全天	-

操作步骤

最近更新时间: 2023-08-24 09:53:21

1. 在告警设置页面，单击开启“告警状态”，开启告警设置模式。
2. 开启告警设置模式后，告警时间可以单击图标选择全体或自定义时间。
   (1) 单击全体左侧图标即可完成全天告警通知设置。

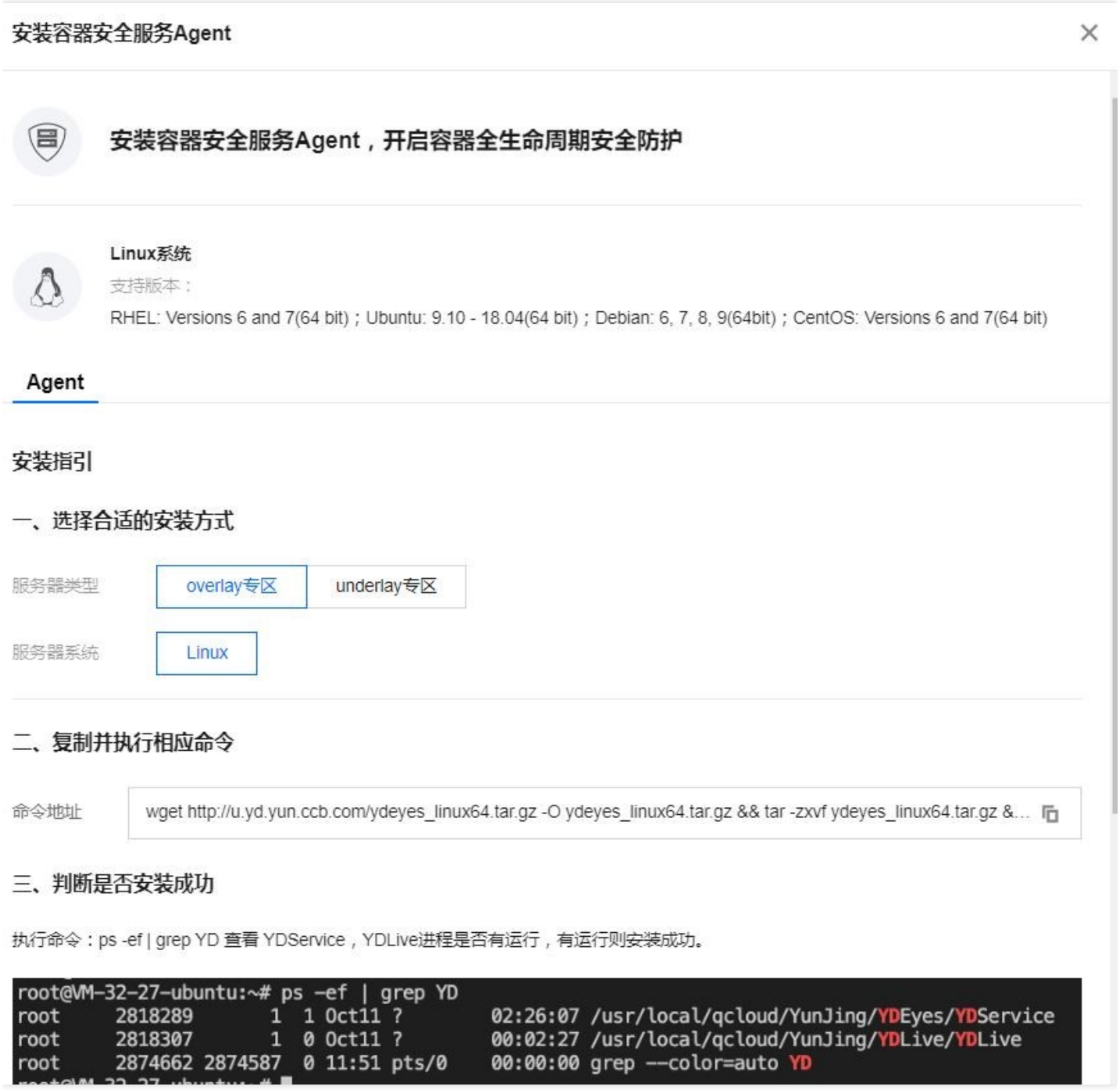
(2) 单击自定义时间框左侧图标，按需选择开始时间和结束时间后，单击确定，即可完成自定义时间通知设置。



快速入门
Agent安装指引

最近更新时间: 2023-08-17 14:54:19

下载安装 Agent



- 基础网络下载地址

示例

wget http://u.yd.yun.ccb.com/ydeyes_linux64.tar.gz –O ydeyes_linux64.tar.gz && tar –zxvf ydeyes_linux64.tar.gz && ./self_cloud_install_linux64.sh

查看是否安装成功

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

```
ps -ef|grep YD
```

- 如果进程没有起来，可以使用 root 用户手动执行命令，启动程序。命令

```
/usr/local/qcloud/YunJing/YDEyes/YDService
```

卸载Agent服务

```
/var/lib/qcloud/YunJing/uninst.sh
```

故障处理

linux客户端离线排查

最近更新时间: 2023-08-17 16:06:26

客户端进程未启动排查

1. 请查询容器安全服务进程是否存在。输入：ps -ef|grep YD。

- 正常状态下，容器安全服务存在两个进程，如下图所示：

```
[root@VM_145_42_centos ~]# ps -ef|grep YD
root      2890  2857  0 11:05 pts/0    00:00:00 grep YD
root      9059     1  0 Oct30 ?        00:00:41 /usr/local/qcloud/YunJing/YDEyes/YDService
root     14340     1  0 Oct23 ?        00:00:58 /usr/local/qcloud/YunJing/YDLive/YDLive
```

- 如果进程不存在，可能存在以下情况：
  ■ 服务器未安装容器安全服务或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
  ■ 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 若服务器已安装容器安全服务或者客户端，可采用以下方法排查客户端进程未启动原因：

- 可查看客户端日志，存放路径：/usr/local/qcloud/YunJing/log。
- 可执行命令：sh /usr/local/qcloud/YunJing/startYD.sh 启动容器安全服务服务

网络故障排查

如果进程存在，但容器安全服务不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 如果无法访问容器安全服务域名，可以尝试修改 DNS。可以通过执行如下命令行，排查容器安全服务域名是否可以访问：
   (1) VPC 网络和黑石服务器环境：telnet s.yd.yun.ccb.com 5574。
   正常情况下：返回如下图所示结果。

```
[root@VM_0_10_centos ~]# telnet s.yd.tencentyun.com 5574
Trying 169.254.0.55...
Connected to s.yd.tencentyun.com.
Escape character is '^]'.
```

如果无法访问:
■ 可以尝试修改dns nameserver字段：vim /etc/resolv.conf
nameserver 183.60.83.19
nameserver 183.60.82.98

■ 修改完成后，重新执行telnet s.yd. yun.ccb.com 5574检测能否连通。

```
[root@VM_0_7_centos ~]# cat /etc/resolv.conf
options timeout:1 rotate
; generated by /usr/sbin/dhclient-script
nameserver 183.60.83.19
nameserver 183.60.82.98
```

■ 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

(2) 基础网络环境（非 VPC 上的服务器）：telnet s.yd.qcloud.com 5574。

正常情况下：返回如下图所示结果。

```
[root@VM-28-45-centos ~]# telnet s.yd.qcloud.com 5574
Trying 10.53.78.111...
Connected to s.yd.qcloud.com.
Escape character is '^]'.
```

如果无法访问：

■ 可以尝试修改dns nameserver字段：vim /etc/resolv.conf，先把原有的nameserver字段注释，再新增nameserver字段，具体的 nameserver ip 相关内容，请参见 内网服务。

■ 修改完成后，重新执行telnet s.yd.qcloud.com 5574检测能否连通。

■ 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

2. 防火墙策略限制，需要在 Linux 客户端开放 TCP 端口：5574、8080、80、9080。
3. 如果容器安全服务进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径：/usr/local/qcloud/YunJing/log）并 提交工单 进行反馈。

常见问题

如何防护容器安全?

最近更新时间: 2023-08-22 08:54:17

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

如何监控容器的健康状况?

最近更新时间: 2023-08-22 08:54:17

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

容器安全服务和其他安全产品是否冲突?

最近更新时间: 2023-08-22 08:54:17

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

容器安全服务的漏洞库多久更新一次?

最近更新时间: 2023-08-22 08:54:17

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

镜像与容器之间有什么关系?

最近更新时间: 2023-08-22 08:54:12

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