ALIBABA CLOUD

阿里云

云安全中心（态势感知）
控制台总览

文档版本：20210202

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

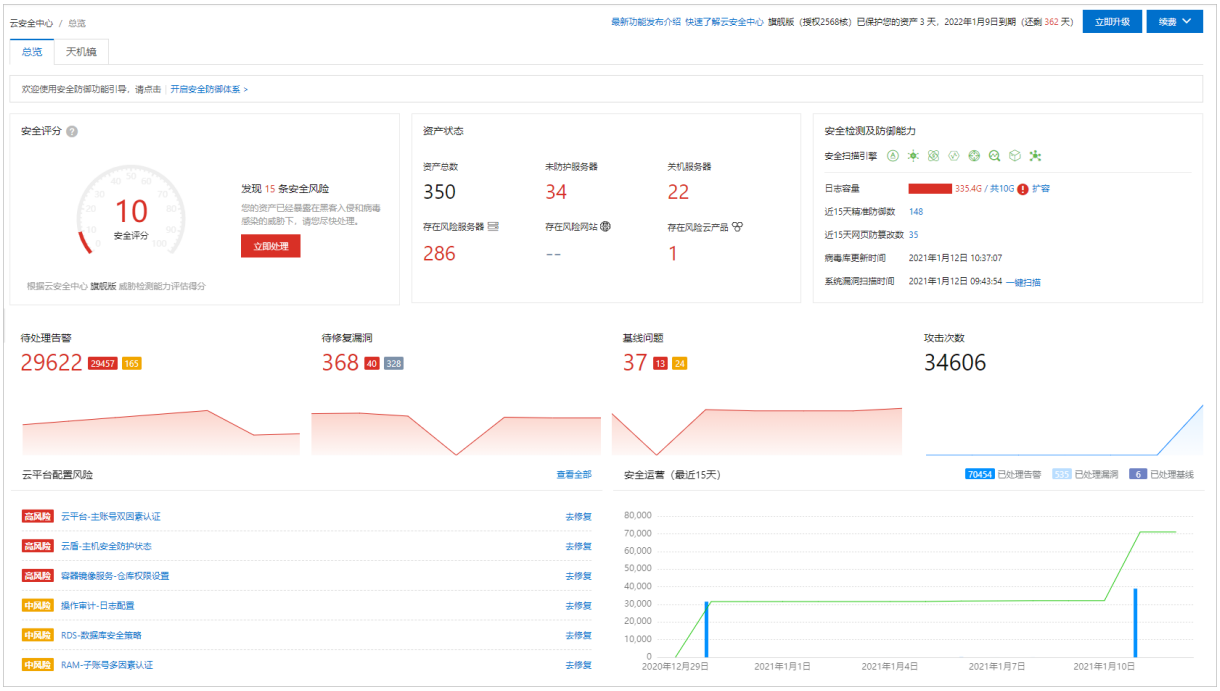
目录

1.总览 ---------- 05
2.安全评分 ---------- 09
3.容器网络拓扑 ---------- 12
4.常见问题 ---------- 15

1.总览

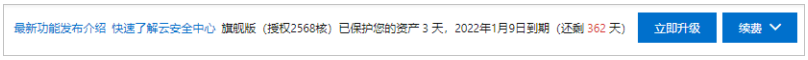
云安全中心总览页面作为阿里云云平台的安全运营中心，实时展示了您所有资产的威胁概览信息和安全评分信息、以及您开通的所有云安全服务，并提供升级、续费、扩充资产规模、调整接收通知规则等设置功能，帮助您对资产进行统一的安全管控。

您可在云安全中心控制台**总览**页面查看您资产的安全概览信息，进行相关操作。



总览页面展示以下模块：

- **立即升级**、**续费**：云安全中心的版本信息，提供升级防病毒版、高级版、企业版或旗舰版、扩充资产规模、续费操作。详细内容，请参见升级、、或、扩充资产规模、续费。



- **试用报告**：基础版用户免费试用旗舰版7天后，试用结束。系统将自动生成试用报告。您可以单击**点击查看**，查看试用报告。试用报告展示了试用期间已检测、自动修复和需要处理的系统安全问题。您可以基于报告针对性地进行安全加固，防止黑客入侵破坏业务运行。

  试用报告如下图所示，您可以单击**安全分析**、**漏洞**、**云平台配置检查**等页签，查看相应功能的安全防护报告。

- **安全评分**：展示您资产的安全分值以及发现资产安全风险数量。安全分值的详细介绍，请参见安全分值表。 如何提高资产的安全分值，请参见提高安全评分最佳实践。

单击**立即处理**展开**安全风险处理**面板，您可根据该面板的提示，参考对应的帮助文档或直接对风险进行处理。

安全风险处理包含所有需要您尽快处理的安全风险和威胁，包含以下类别：

  - 关键功能配置
  - 待处理告警
  - 待修复漏洞
  - 基线问题
  - AK泄露问题
  - 云平台配置风险（云产品安全风险项）
  - 攻击事件等其他风险或威胁

- **资产状态**：查看您已安装和未安装Agent插件的资产数量（即已在云安全中心防护范围内的资产和还未受云安全中心防护的资产数量），以及资产的风险状态统计数据。

单击**未防护服务器**下的**安装Agent**，跳转到**安装/卸载插件**页面，您可以将未受保护的资产接入云安全中心的安全防护内。有关Agent安装的详细操作，请参见安装Agent。

- **安全检测及防御能力**：提供安全扫描引擎、日志容量、病毒库更新时间、系统漏洞扫描时间、精准防御数量和网页防篡改数量等相关信息，帮助您实时掌握安全防御情况，了解资产安全状态。

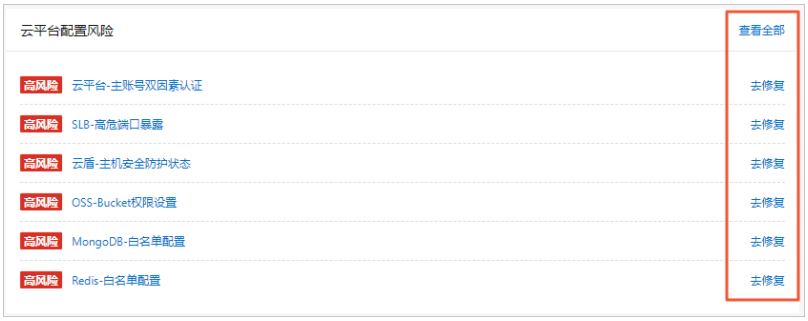
单击**一键扫描**，可实时检测资产是否存在漏洞风险、基线问题或云平台配置问题。

不同版本支持的安全检测及防御能力有较大差异。各版本支持的安全检测及防御能力详情，请参见功能特性。

- **威胁统计**：查看威胁统计数据。

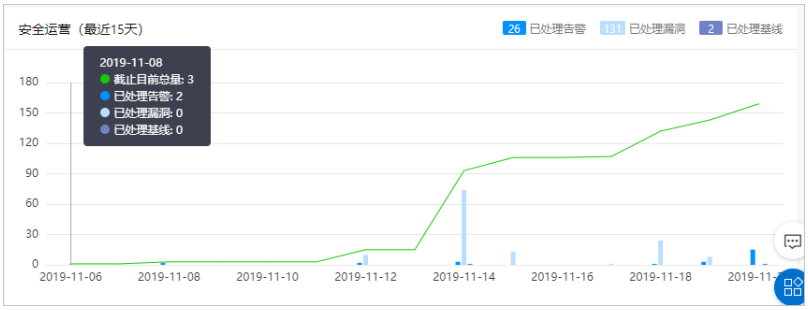
威胁类型	说明
待处理告警	展示您资产中的告警总数量和不同风险等级的告警的数量。 云安全中心对安全告警风险等级的分类如下： ○ **紧急**：即高危风险，表示您的服务器中检测到了入侵事件（例如反弹Shell等），建议您立即查看告警事件的详情并及时进行处理。 ○ **可疑**：即中危风险，表示服务器中检测到了可疑的异常事件（例如可疑CMD命令序列等），建议您查看该告警事件、判断是否存在风险并进行相应处理。 ○ **提醒**：即低危风险，表示服务器中检测到了低危的异常事件（例如可疑端口监听等），建议您及时查看该告警事件的详情。 单击待处理告警总数值跳转到**安全告警处理**页面，查看并处理告警事件。更多信息，请参见安全告警处理。
待修复漏洞	展示您资产中还未修复的漏洞总数和不同漏洞风险等级对应的数量。 单击待修复漏洞的总数量跳转到**漏洞修复**页面，查看并处理漏洞。更多信息，请参见漏洞修复。
基线问题	展示您资产中存在的基线风险总数量和不同危险等级的基线风险对应的数量。 单击基线问题总数值跳转到**基线检查**页面，查看并处理基线检查出的风险问题。更多信息，请参见基线检查。
攻击次数	展示您资产受到攻击的总次数。 单击攻击总次数跳转到**攻击分析**页面，查看攻击分析详情。更多信息，请参见攻击分析。

- **云平台配置风险**：检测到的云产品基线配置存在的风险。



单击**查看全部**跳转到**云平台配置检查**页面，查看并处理云平台配置检查结果。具体操作，请参见查看和处理云平台配置检查结果。

- **安全运营**：展示15天内已处理的告警、漏洞、基线配置数量柱状图和趋势图。



升级防病毒版、高级版、企业版或旗舰版、扩充资产规模、续费

云安全中心支持基础版、防病毒版、高级版、企业版和旗舰版，您可在**总览**页面右上角查看云安全中心的版本信息。有关各版本支持的功能的详细内容，请参见功能特性。

- **基础版**：页面右上角显示云安全中心的版本信息和**升级**按钮。升级到基础杀毒版、高级版或企业版后可使用基线检查、资产指纹、恶意进程（云查杀）、日志分析等高级功能。
- **防病毒版、高级版、企业版、旗舰版**：页面右上角显示云安全中心的到期日期和资产规模（服务器台数或计算核数），并提供**立即升级**、**手动续费**和**按月自动续费**操作按钮。

> **说明**
>
> - 升级和续费的具体操作，请参见升级与降配和到期续费。
> - 如果当前服务器数量超过购买服务时配置的服务器数量，或当前服务器的总核数超过计算核数时，页面右上角会出现**扩充资产规模**操作按钮，提示您尽快扩充资产规模。

更多信息

如果您需要安全专家帮助提升系统安全性，可使用安全加固服务。在您授权后，专业安全工程师会为您修复安全基线和漏洞、排查系统潜在安全威胁、提升资产安全性。

更多信息，请参见安全加固。

2.安全评分

云安全中心为您实时检测您资产的安全状态，并提供的安全分值以及发现资产安全风险数量。本文为您介绍安全评分中，不同分值范围和扣分项的解释。

安全分值表

安全分值	分值说明	字体颜色
95~100	恭喜，您的资产安全状态良好。	绿色
85~94	您的资产存在安全隐患，建议您尽快加固安全防护体系。	黄色
70~84	您的资产存在较多安全隐患，建议您及时加固安全防护体系。	黄色
69分以下	您的资产防御黑客入侵的能力很弱，建议您尽快加固安全防护体系。	红色

安全评分扣分项目表

说明

- 云安全中心判定的安全评分总分最高分不超过100分，最低分不低于10分。
- 当减去扣分后剩余分数高于60分、但存在未处理的告警事件时，总分只能为60分。
- 当减去扣分后剩余分数高于80分、但待修复漏洞或者待处理告警事件存在扣分项时，总分只能为80分。
- 当减去扣分后剩余分数高于90分、但存在未处理的基线检查风险时，总分只能为90分。
- 以下表格中所有付费版本是指云安全中心防病毒版、高级版、企业版和旗舰版。

扣分分类	版本要求	扣分项	单项扣分值	处理建议
关键功能配置	所有付费版本	未开启网页防篡改功能	5	开通网页防篡改服务
	基础版	未配置防暴力破解策略	2	设置IP拦截策略
	基础版	未授权一键安装Agent客户端	2	首次使用该功能时需要先完成授权操作
	高级版、企业版、旗舰版	未授权云平台配置检查	2	首次使用该功能时需要先完成授权操作
	所有付费版本	未开通日志分析功能	2	开通日志分析
	所有付费版本	未开通防病毒功能	2	主动防御
	所有付费版本	未创建防勒索策略	2	创建防护策略
	所有付费版本	未开启周期病毒扫描策略	5	周期性扫描病毒

扣分分类	版本要求	扣分项	单项扣分值	处理建议
	旗舰版	未开启容器K8s威胁检测	5	容器K8s威胁检测
待处理告警	所有付费版本	存在未处理的高危告警事件	20	处理告警事件
	所有付费版本	存在未处理的中危告警事件	20	处理告警事件
	所有付费版本	存在未处理的低危告警事件	20	处理告警事件
待修复漏洞	高级版、企业版、旗舰版	存在未修复的CMS漏洞	2	Web-CMS漏洞
	高级版、企业版、旗舰版	存在未修复的Windows系统漏洞	2	Windows系统漏洞
	高级版、企业版、旗舰版	存在未修复的Linux软件漏洞	2	Linux软件漏洞
	高级版、企业版、旗舰版	存在未修复的应急漏洞	5	应急漏洞
	高级版、企业版、旗舰版	存在未检测的应急漏洞（无ECS用户该项不扣分）	3	应急漏洞
基线问题	企业版、旗舰版	存在基线检查风险	1	处理风险检查项
云平台配置风险	高级版、企业版、旗舰版	云盾-高防回源配置检查未通过	• 高危风险：2分 • 中低危风险：1分	处理云平台配置检查结果
	高级版、企业版、旗舰版	主账号未开启双因素认证	• 高危风险：2分 • 中低危风险：1分	
	高级版、企业版、旗舰版	RDS-数据库安全策略检查未通过	• 高危风险：2分 • 中低危风险：1分	
	高级版、企业版、旗舰版	云产品配置存在高危风险	2	
	高级版、企业版、旗舰版	云产品配置存在中低危风险	1	
AK泄露问题	所有版本	存在AK泄漏风险	30	查看和处理AK泄露事件

扣分分类	版本要求	扣分项	单项扣分值	处理建议
其他	企业版、旗舰版	存在攻击事件	5	提高安全评分最佳实践

相关文档

安全评分中处理事件优先级是怎样的？

、和、、的安全评分扣分项有什么不同？

修改漏洞关注等级与提高安全评分有什么关系？

修改基线关注等级与提高安全评分有什么关系？

提高安全评分最佳实践

3.容器网络拓扑

容器网络拓扑功能从集群、容器、镜像、应用等资产维度为您提供安全可视化的管控能力和云上容器资产的网络拓扑。使用该功能您可以轻松掌控容器资产的安全状态，并了解容器资产间的网络连接情况，帮助您提升管理容器资产安全的效率。本文介绍如何查看您资产中的容器网络拓扑。

版本限制说明

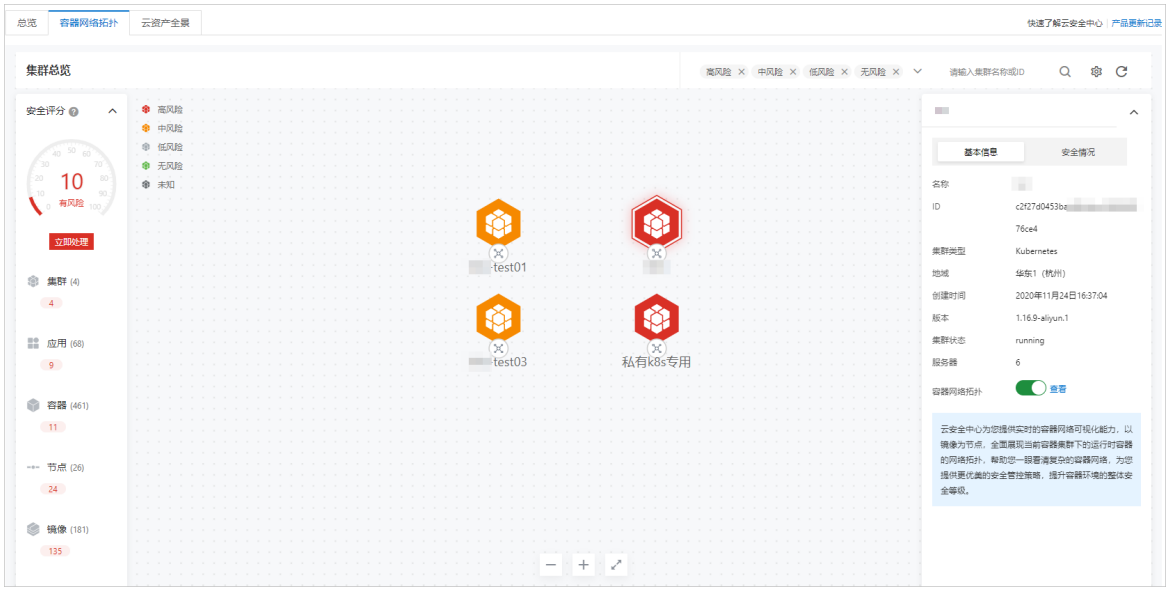
仅旗舰版支持该功能，其他版本用户需要升级到旗舰版才可使用该功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。各版本的功能详情，请参见功能特性。

应用场景

- 满足等保合规要求，为您提供云上资产的网络拓扑图。
- 为运维人员提供自动化公网暴露端口的可视化能力。
- 为运维人员从集群、容器、镜像、应用等资产维度提供可视化安全管控能力。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**总览**。
3. 在**总览**页面，单击**容器网络拓扑**页签。
4. 查看您资产中的容器网络拓扑图。



在**容器网络拓扑**页签，您可以执行以下操作：

- **查看您资产整体状态的安全评分**

  在**容器网络拓扑**页签左侧，查看云安全中心根据您资产整体的安全状态计算出的安全评分。安全评分越高说明您资产的安全隐患越少。安全评分更多信息，请参见安全评分。

- **集群、应用、容器、节点、镜像数量和存在风险的资产数量**

  在**容器网络拓扑**页签左侧，查看您资产中的集群、应用、容器、节点、镜像数量和存在安全风险的各类型资产数量（红色数字表示存在风险的资产数量），单击对应资产类型名称，可跳转至**资产中心**页面查看该类型资产的详细信息。

- **查看集群的基本信息和安全情况**

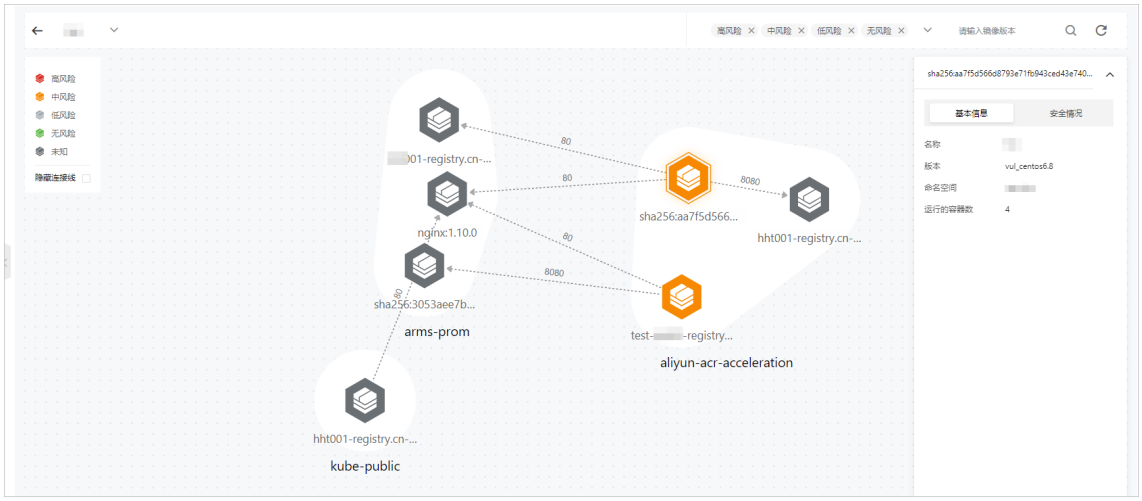
  在**容器网络拓扑**页签，单击需要查看基本信息和安全情况的集群图标，右侧面板会为您展示该集群的基本信息和安全情况。展示的集群基本信息包括：**名称**、**ID**、**集群类型**、**地域**、**创建时间**、**版本**、**集群状态**和**服务器**数量。展示的安全情况包括以下内容：

  - 集群中的服务器存在的安全风险：
    - **安全告警**：集群中服务器存在的安全告警数量。
    - **漏洞风险**：集群中服务器存在的漏洞数量。
    - **基线风险**：集群中服务器存在的基线风险项数量。
  - 集群中存在的容器安全风险：
    - **镜像漏洞（CVE）**：集群中存在的镜像系统漏洞数量。
    - **镜像应用漏洞**：集群中存在的镜像应用漏洞数量。
    - **镜像恶意文件**：集群中存在的镜像恶意样本数量。

- **查看集群内的容器网络拓扑**

  单击需要查看网络拓扑的集群**容器网络拓扑**右侧的**查看**，查看该集群内的网络拓扑图。

网络拓扑图以镜像为节点，展示了该集群下所有容器之间的通信链路。单击容器网络拓扑图中的镜像图标，可以查看该镜像的基本信息和安全状态（包括检测出的告警、漏洞、恶意文件的数量）。



> **说明** 灰色图标表示该镜像还未启用云安全中心镜像扫描功能，您可以在**镜像安全扫描**页面接入该镜像后启用镜像安全扫描功能，以便及时获取该镜像的安全风险信息。目前仅支持接入仓库类型为Harbor和Quay的私有镜像。具体操作，请参见接入私有镜像仓库。

- **开启或关闭所有集群的网络拓扑**

  集群的网络拓扑开关默认开启，如果您无需查看集群的网络拓扑，您可以单击**容器网络拓扑**页签右上角 图标，单击 图标，关闭所有集群的网络拓扑。关闭网络拓扑后，如果您需要再次查看集群的网络拓扑，可以重新打开该开关。

  > **说明** 建议您开启所有集群的网络拓扑图，及时获取容器集群网络拓扑中各节点的风险状态。

4.常见问题

本文汇总了云安全中心总览页面的常见问题。

安全评分

- 安全评分中处理事件优先级是怎样的？
- 、和、、的安全评分扣分项有什么不同？
- 如何开通防暴力破解功能？
- 常见告警处理方法有哪些？
- 修改漏洞关注等级与提高安全评分有什么关系？
- 修改基线关注等级与提高安全评分有什么关系？

安全评分中处理事件优先级是怎样的？

以下是安全评分中处理事件的优先级排序。数字越小优先级越高，1为最高优先级。

优先级	事件
1	已配置或开启关键功能，包括： • 开启网页防篡改功能。 • 配置防暴力破解规则。 • 授权一键安装Agent客户端。 • 授权云平台配置检查。 • 开通日志分析功能。 • 开通防病毒功能。 • 创建防勒索策略。 • 开启病毒防御周期扫描。 • 开启容器K8s威胁检测。
2	处理AK泄漏检测事件。
3	处理云平台配置风险。
4	修复基线检查问题。
5	处理安全告警。
6	修复漏洞。

企业版、旗舰版和基础版、防病毒版、高级版的安全评分扣分项有什么不同？

云安全中心基础版、防病毒版和高级版不支持攻击分析功能，因此该项没有纳入安全评分的评分范围。安全评分扣分项的更多信息，请参见安全评分扣分项目表。

如何开通防暴力破解功能？

开通防暴力破解功能可以拦截恶意登录服务器的IP，提高您资产的安全评分。建议您开通防暴力破解功能。更多信息，请参见如何开通防暴力破解功能。

常见告警处理方法有哪些？

处理云安全中心检测出的告警可以降低资产的安全风险，提高安全评分。常见告警的处理方法的更多信息，请参见常见告警处理方法有哪些。

修改漏洞关注等级与提高安全评分有什么关系？

如果您只关注高、中危漏洞的修复，不关注低危漏洞，那么安全评分中将不再将低危漏洞纳入评分范围。您可以在云安全中心**漏洞修复 > 漏洞管理设置**漏洞扫描等级中选择**高**、**中**两个等级，设置云安全中心只对高、中危漏洞进行检测。

修改基线关注等级与提高安全评分有什么关系？

如果您只关注高、中等级基线的修复，不关注低等级的基线风险，那么安全评分中将不再将低等级基线风险纳入评分范围。您可以在云安全中心**基线检查 > 策略管理**基线检查等级中选择**高**、**中**两个等级，设置云安全中心只对高、中等级基线风险进行检测。