ALIBABA CLOUD

阿里云

# 应用实时监控服务 ARMS

## 容器监控

文档版本：20210111

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<br>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<br>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<br>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<br>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`<br>*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.容器监控概述

随着容器技术的发展与使用，大量的业务运行于容器中，使得容器技术越来越离不开对容器本身的监控。ARMS容器监控能够对阿里云容器服务Kubernetes版的节点机器上的资源及容器进行实时监控和性能数据采集，并进行可视化展示，为您提供容器化环境端到端的监控排查路径。

## 产品功能

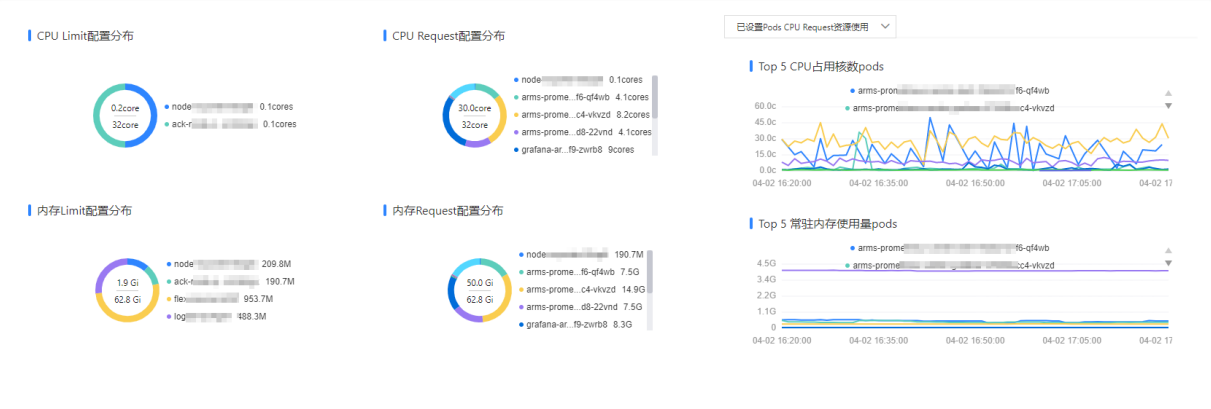
容器监控自动获取当前账号下的阿里云容器服务Kubernetes版集群信息，能够基于Prometheus监控数据、集群事件持久化数据以及集群的基本配置信息提供以下功能。

## 异常Pod检测

异常Pod是指：

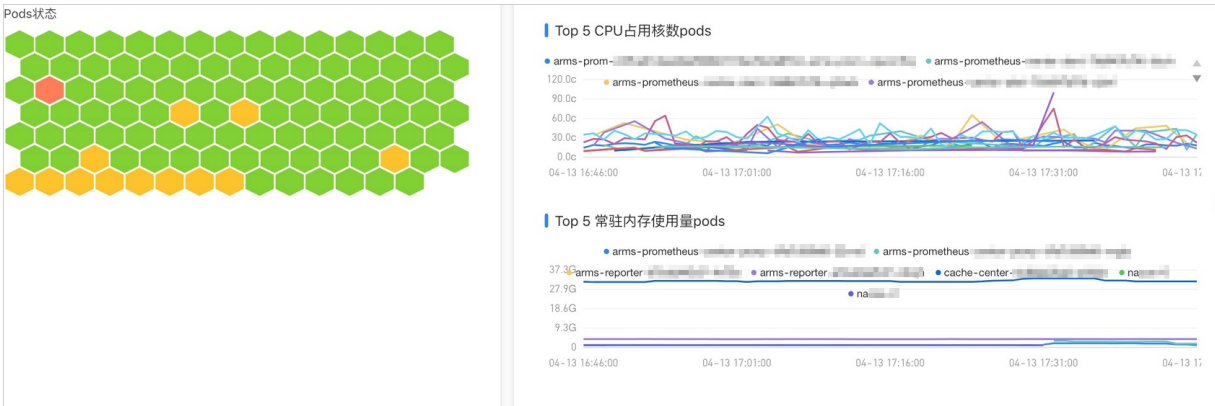
- 频繁重启的Pod
- 网络流量不均的Pod
- 未设置Limit资源但实际占用资源较多的Pod
- 实际占用资源较少但设置Request较大的Pod
- 有驱逐风险的Pod以及其他异常Pod

容器监控提供异常Pod检测功能，通过Pod资源配置、资源使用分布情况和历史异常事件预估和展示当前集群中可能有风险的Pod，并帮助您降低其风险。




## 资源使用情况可视化

容器监控提供集群资源监控功能，帮助您快速查看集群内Pod的健康状态、Pod的CPU和内存资源的使用情况。



## Deployment监控

ARMS容器监控提供Deployment监控，主要监控应用运行时对环境的依赖情况，包括CPU以及内存的监控。

## Pod监控

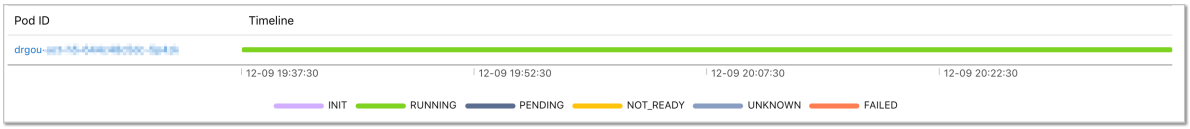
ARMS容器监控还提供集群中运行的所有Pod状态以及Pod本身的监控，Pod本身的监控包括事件监控、生命周期监控、资源监控以及日志监控：

- 事件监控是监控集群的事件信息，例如告警和错误事件等。

  Kubernetes的架构设计是基于状态机的，不同的状态之间进行转换则会生成相应的事件，正常的状态之间转换会生成Normal等级的事件，正常状态与异常状态之间的转换会生成Warning等级的事件。您可以通过获取事件，实时诊断集群的异常与问题。

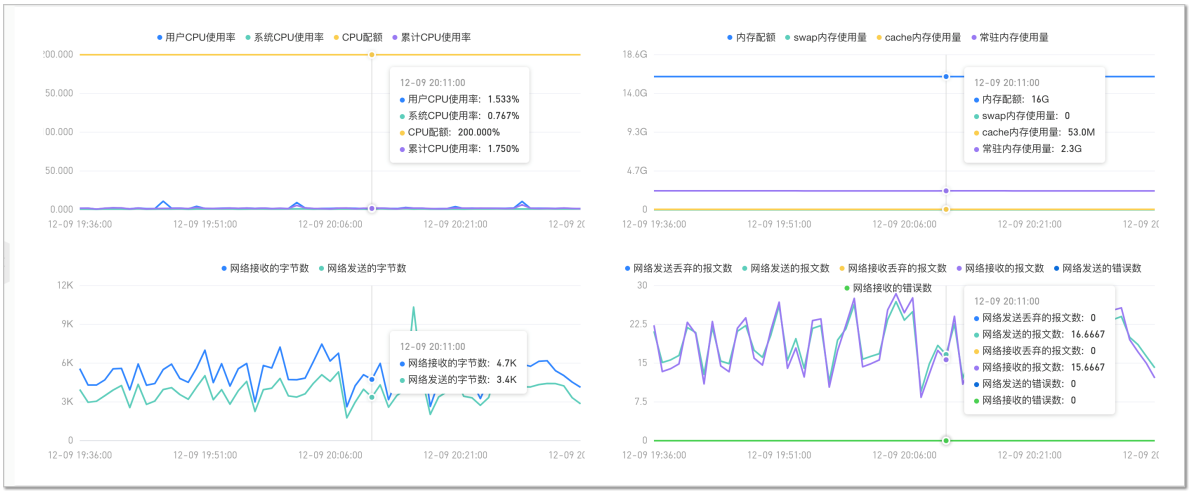
- 生命周期监控

  生命周期监控可以帮助您随时掌握Pod在整个生命周期的各个状态，以便您更好地调度和管理Pod。



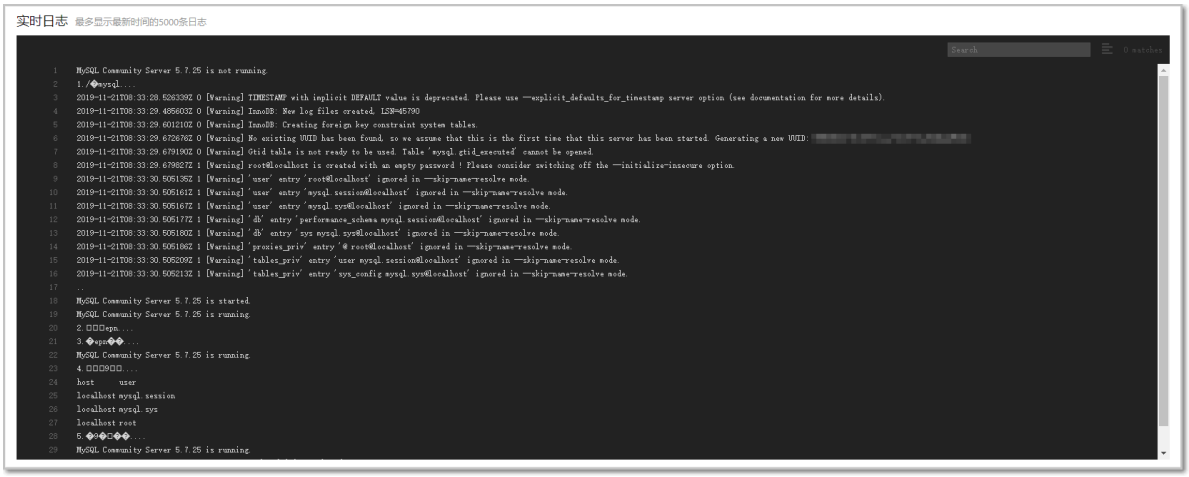

- 资源监控

  通过资源监控可以快速查看负载的CPU、内存、网络等指标的使用率。




- 日志监控

  日志监控展示Pod实时监控日志，方便您进行问题诊断。




## 应用性能监控

对于部署在容器服务Kubernetes版集群中的应用，您可以使用ARMS应用监控对其监控，详情请参见准备工作概述。安装应用监控探针后，可将容器与应用关联，即将容器的CPU、内存和网络资源使用情况，以及集群异常事件和日志等信息与应用关联，帮助您排查当前容器环境是否会对您的业务产生影响。

# 2.控制台功能

## 2.1. 节点监控

ARMS容器监控可监控Kubernetes集群所在的节点，并通过Pod资源配置、资源使用分布情况和历史异常事件来预估和展示当前集群中可能有风险的Pod。

### 背景信息

作为生产环境的容器编排系统，Kubernetes最重要的功能之一是根据您的配置，自主进行容器的调度和编排。因此通常情况下，当启动一个容器组时，Kubernetes会自动将容器均匀地分布到各个节点中，充分利用每个节点的资源。

然而事实上，由于您的配置原因，可能会导致Kubernetes集群所在的节点存在风险。例如Pod驱逐行为：kubelet能够主动监测和防止计算资源的全面短缺，在节点配置资源不足时，kubelet会主动结束一个或多个Pod以回收短缺的资源。

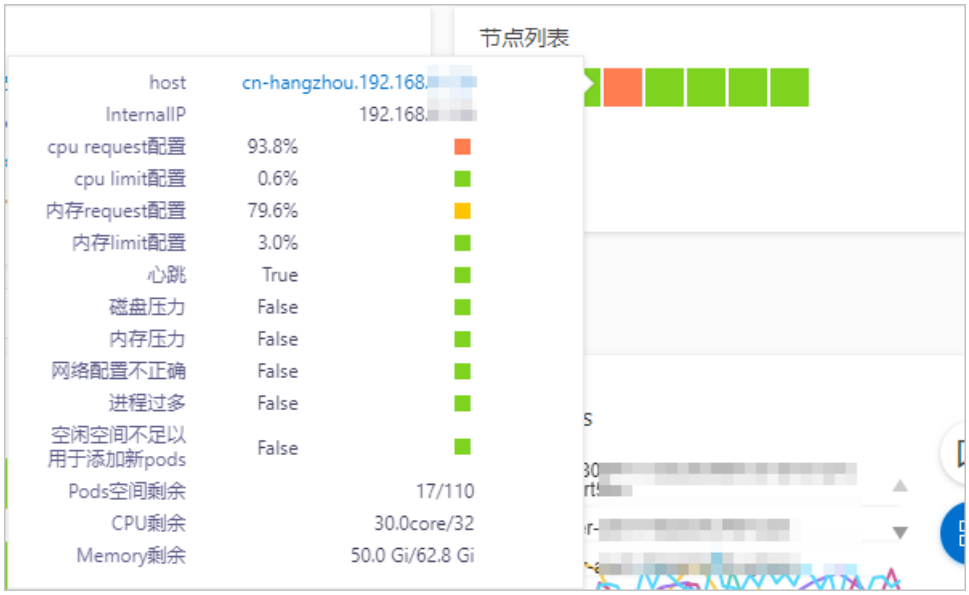
### 使用容器监控来监控K8s集群所在节点

合理的Request和Limit资源配置对于部署在K8s集群上的应用的稳定性至关重要，容器监控提供的节点监控主要监控Request和Limit资源配置，以及受配置影响的节点健康状态。您可以按照以下步骤使用容器监控来监控K8s集群所在节点：

1. 登录ARMS控制台。
2. 在左侧导航栏单击**容器监控**。
3. 在**容器监控**页面的K8s集群列表中单击目标集群名称。
4. 在**概览页**页面的**节点列表**区域查看节点的健康状态，将鼠标移动至异常节点，并在浮层中单击host对应的链接。

   其中，不同的颜色表示不同的状态：

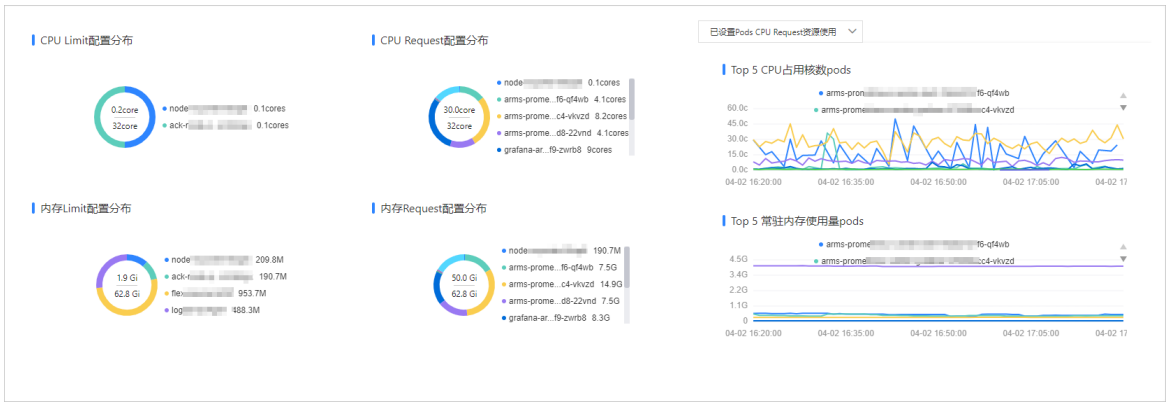
   - 绿色表示节点处于Normal状态。
   - 橙色表示节点处于Warning状态。
   - 红色表示节点处于Error状态。



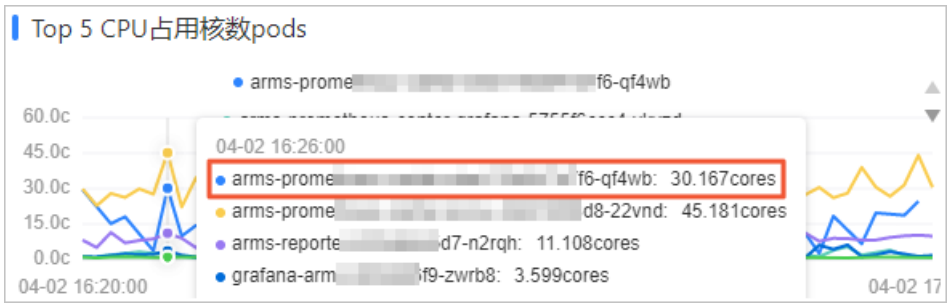
5. 在**节点**页面查看资源使用分布情况。

   资源使用分布情况包括以下内容：

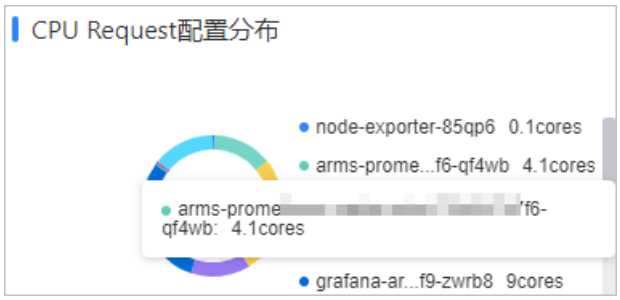
   - 基于K8s元数据展示Pod的Request和Limit资源配置的分布情况。
   - 基于K8s提供的数据展示的Pod实际使用资源的分布情况。




例如，在**Top5 CPU占用核数pods**折线图中发现某个Pod的实际CPU占用核数较高，为30.167 Cores。




然后在**CPU Request配置分布**环形图中查看此Pod的Request配置为4.1 Cores。




最后在**CPU Limit配置分布**环形图中查看，发现此Pod没有Limit配置，判断此Pod可能存在Pod驱逐风险，您需要采取相应措施避免产生此风险，详情请参见后续操作。

## 后续操作

为避免出现Pod驱逐风险从而保障应用稳定性，请遵循以下建议：

- 合理设置Kubernetes资源调度的关键参数Request和Limit。
- Pod驱逐会按照BestEffort > Burstable > Guaranteed的顺序进行驱逐，因此请将重要业务Pod的驱逐等级设置为Guaranteed。
- 将BestEffort驱逐等级的Pod用于处理离线批处理类业务。