ALIBABA CLOUD

阿里云

应用实时监控服务 ARMS

ARMS公共云合集

文档版本：20220712

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.动态与公告

1.1. 功能发布记录

1.1.1. 2022年

本文为ARMS 2022年的版本发布记录，介绍历次发布的特性变更情况。

2022年05月

模块	功能名称	功能概述	支持地域	版本号
Prometheus监控	Prometheus for ACK上线新版集成中心	集成中心作为Prometheus实例的入口，将容器服务、自定义服务发现、组件监控的关联数据和高频操作进行集中化展示，提供ACK集群内一站式监控配置与管理。更多信息，请参见集成中心。	请参见Prometheus监控目前支持的地域。	v2.8.4.1
	同步ServiceMonitor和PodMonitor	阿里云Prometheus支持同步集群内的ServiceMonitor和PodMonitor。更多信息，请参见如何实现集群内ServiceMonitor和PodMonitor的同步。		2.8.4.1
Grafana服务	商业化计费正式发布	Grafana服务于2022年05月18日0点起正式商用，提供免费共享版、专家版和高级版三种规格。更多信息，请参见计费规则。	请参见Grafana服务目前支持的地域。	v2.8.4.2
	新增支持数据迁移	您可以通过API Key授权或者提供Admin账号密码，将自建的Grafana大盘、数据源一键同步到托管版上。		v2.8.4.2
	高级版支持数据报表功能	Grafana服务支持将整个大盘以图片形式导出，并且可以设置定时任务，将大盘发送到指定邮箱。更多信息，请参见数据报表。		v2.8.4.2

2022年04月

模块	功能名称	功能概述	支持地域	版本号
Prometheus监控	新增开服地域	新开服华北6（乌兰察布）地域。	请参见Prometheus监控目前支持的地域。	v2.8.3.4
	更新全局聚合实例功能	提供多个阿里云Prometheus实例或自建Prometheus集群的虚拟聚合实例，针对这个虚拟聚合实例可以实现Prometheus指标的统一查询，统一Grafana数据源和统一告警。更多信息，请参见GlobalView聚合实例（旧版）。	请参见Prometheus监控目前支持的地域。	v2.8.3.4

模块	功能名称	功能概述	支持地域	版本号
应用监控	自定义RAM授权	ARMS应用监控支持通过自定义策略为RAM用户授权。更多信息，请参见应用监控自定义RAM授权策略。 说明 仅新开通ARMS的用户支持此功能，已开通ARMS的用户如果需要体验此功能，可以通过提交工单添加白名单。	请参见应用监控目前支持的地域。	v2.8.3.4
	新增ARMS OpenTelemetry Collector功能	ARMS OpenTelemetry Collector是一套基于开源OpenTelemetry Collector开发的可观测数据（Traces、Metrics、Logs）边缘侧统一采集与处理平台，具备安全、可靠、易用等特性，适合生产环境接入。更多信息，请参见ARMS OpenTelemetry Collector。	应用监控支持的中国地域，请参见应用监控目前支持的地域。	v2.8.4
告警管理	IM机器人新增飞书机器人	IM机器人功能新增支持飞书自定义机器人，告警内容将以消息卡片形式推送，全面提升告警接收体验。更多信息，请参见飞书机器人。	告警管理支持的中国地域。	v2.8.4

2022年03月

模块	功能名称	功能概述	支持地域	版本号
应用监控	应用标签	ARMS应用监控支持为应用添加标签键值对。更多信息，请参见标签管理。	请参见应用监控目前支持的地域。	v2.8.3.3
	启动分析	ARMS应用监控支持对部署在ACK集群下的Dubbo应用进行启动分析，统计应用下各Dubbo实例启动耗时，单位为毫秒（ms），并支持从容器启动、应用初始化、服务注册和正常流量进入四个维度进行数据展示分析。更多信息，请参见启动分析。	应用监控支持的中国地域，请参见应用监控目前支持的地域。	v2.8.3.3
	应用环境	ARMS应用监控支持查看ACK集群下Dubbo应用的环境信息，包括环境依赖信息和配置信息。更多信息，请参见应用环境。	应用监控支持的中国地域，请参见应用监控目前支持的地域。	v2.8.3.3
	JVM配置优化	ARMS应用监控支持查看应用下所有的JVM实例，以及实例配置信息。同时，ARMS应用监控还支持对JVM参数调优，为您提供JVM参数优化建议。更多信息，请参见JVM配置优化。	应用监控支持的中国地域，请参见应用监控目前支持的地域。	v2.8.3.3

模块	功能名称	功能概述	支持地域	版本号
Grafana服务	告警管理集成基于Loki的ARMS告警大盘	告警概览通过集成Grafana服务提供告警信息的数据大盘，支持历史告警总览、告警处理效率总览，提供SLA、告警处理统计、每日告警趋势等数据图表，方便用户统计告警数据，实时分析处理情况，改进告警处理效率。	请参见Grafana服务支持的开服地域。	v2.8.3.3
告警管理	商业化计费正式发布	ARMS告警管理于2022年03月18日0点开始商用，目前提供免费试用版、免费基础版和后付费专家版三种模式。更多信息，请参见告警管理计费规则。	告警管理支持的中国地域。	v2.8.3.3
	支持在移动端屏蔽告警规则	在钉钉群或企业微信群中收到告警通知后，可以直接在钉钉群或企业微信群中执行屏蔽操作。更多信息，请参见在告警通知群中处理告警。	不涉及	v2.8.3.3
	支持根据通知策略的分派条件预览告警事件	在新建或编辑通知策略时，支持根据设置的分派条件预览最近24小时符合条件的事件。	不涉及	v2.8.3.3

2022年02月

模块	功能名称	功能概述	支持地域	版本号
应用监控	新增支持Spring定时任务@Scheduled	支持在固定间隔时间执行指定的程序或者指令，帮助您了解Spring定时任务的详细情况。	请参见应用监控目前支持的地域。	v2.8.3.2
Prometheus监控	针对部分地域进行商业化计费	针对政务云、金融云、青岛、呼和浩特、河源、广州、成都、中国香港、美国、英国、德国等地域正式收费。更多信息，请参见按量付费。	请参见Prometheus监控目前支持的地域。	v2.8.3.2

模块	功能名称	功能概述	支持地域	版本号
	新增报警模板功能，支持针对多个Kubernetes集群统一做报警配置	为了实现同步管理多个跨地域Prometheus实例的告警，阿里云Prometheus监控提供了告警规则模板功能，帮助您快速为多个Prometheus实例创建告警规则，统一管理，降低管理多个Prometheus实例告警规则的成本。更多信息，请参见Prometheus告警规则模板。	请参见Prometheus监控目前支持的地域。	v2.8.3.2
Kubernetes监控	优化集群拓扑	支持快捷搜索节点，查看上下游，定位问题更加快捷。	请参见Kubernetes监控目前支持的地域。	v2.8.3.2
	新增保存过滤条件	提升用户体验，减少重复查找和筛选。	请参见Kubernetes监控目前支持的地域。	v2.8.3.2

2022年01月

模块	功能名称	功能概述	支持地域	版本号
Prometheus监控	RocketMQ组件监控新增大盘	阿里云Prometheus监控提供一键安装配置RocketMQ类型组件，并提供开箱即用的专属监控大盘。更多信息，请参见使用阿里云Prometheus监控RocketMQ。	请参见Prometheus监控目前支持的地域。	v2.8.3

模块	功能名称	功能概述	支持地域	版本号

应用监控	Java Agent 2.7.1.3版本优化	• 新增Dubbo在网络调用和解析时的埋点，增强在出现Dubbo调用问题时的分析能力。
		• 支持JVM参数调优，帮助用户在线优化JVM参数配置。
		• Arthas诊断支持ECS环境，利用字节码增强技术，可以在不重启JVM进程的情况下，查看程序的运行情况。更多信息，请参见Arthas诊断（新版）
		• BUG修复：
		  ○ 修复了对于Lettuce的操作获取不正确问题。
		  ○ 修复了kafka等组件的维度发散问题。
		  ○ 修复了Async注解异步的支持。
		  ○ 修复了Hikaricp线程池的功能。
			请参见应用监控目前支持的地域。	v2.8.3

Grafana服务	集成阿里云Elasticsearch	Grafana服务已集成阿里云检索分析服务Elasticsearch版，通过Elasticsearch插件，可以实现Elasticsearch数据同步并实时呈现在Grafana大盘中。更多信息，请参见通过公网地址添加并使用阿里云Elasticsearch数据源。	请参见Grafana服务支持的开服地域。	v2.8.3
云拨测	API性能任务	全面监控API接口性能，支持单个API及多个业务流API监控，验证API数据完整性，确保API返回正确数据。	不涉及	v2.8.3
	新增开服	金融云开服。	不涉及	v2.8.3
应用监控	Insights新增巡检配置和订阅	• Insight内置了多种巡检模块，您可以根据巡检需求定制模块参数。更多信息，请参见巡检配置。 • Insights会基于系统默认设置或自定义设置对您名下的所有应用自动进行异常识别，发现任何异常都会根据您配置的订阅规则第一时间发送通知信息。更多信息，请参见订阅规则。	• 华东1（杭州） • 华东2（上海） • 华北2（北京） • 华北3（张家口） • 华南1（深圳）	v2.8.3
告警管理	新版告警管理新增API	进一步优化告警配置流程。支持通过API创建或修改告警联系人、查询告警规则、查询告警发送历史。更多信息，请参见告警管理（新版）。	不涉及	v2.8.2.4
	新增开服	政务云开服	不涉及	v2.8.2.4

1.1.2. 2021年

本文为ARMS 2021年的版本发布记录，介绍历次发布的特性变更情况。

2021年12月

模块	功能名称	功能概述	发布时间	支持地域	版本号
Grafana服务	新增8.2.x版本Grafana支持	全面支持8.2.x版本Grafana，进一步强化数据源管理、告警管理以及安全能力。	2021-12-30	请参见Grafana服务支持的地域。	v2.8.2.4
	云服务管理能力优化	• 简化数据源接入流程，全面优化云服务管理体验。 • 新增集成Lindorm，通过Alibaba Cloud Lindorm数据源插件，可实现Lindorm数据同步并实时呈现在Grafana大盘中。更多信息，请参见添加并使用Lindorm数据源。	2021-12-30	请参见Grafana服务支持的地域。	v2.8.2.4
	免登大盘分享	免登录查看Grafana大盘共享链接，使用户无需登录即可直接查看大盘。更多信息，请参见为Grafana大盘生成免登录查看的共享链接。	2021-12-30	请参见Grafana服务支持的地域。	v2.8.2.4
应用安全	全面防护Apache Log4j2漏洞	将应用接入应用安全后，当应用受到Log4j2远程代码执行漏洞攻击时，应用安全会识别上报攻击行为事件。更多信息，请参见Apache Log4j2远程代码执行漏洞（CVE-2021-44228）。	2021-12-17	请参见应用安全目前支持的地域。	v2.8.2.3
云拨测	即时拨测	即时拨测能够无侵入的快速进行单次拨测，并将结果数据实时回传，方便对于已发现的问题进行迅速验证。更多信息，请参见云拨测概述。	2021-12-17	不涉及	v2.8.2.3
	云拨测控制台页面换新	创建定时拨测控制台页面换新，提示用户体验。	2021-12-17	不涉及	v2.8.2.3
应用监控	Arthas诊断新增性能分析功能	Arthas诊断的性能分析功能支持对CPU耗时、内存分配等对象进行一定时间的采样并生成相应的火焰图。更多信息，请参见Arthas诊断（新版）。	2021-12-17	• 华北2（北京） • 华南1（深圳） • 华东1（杭州） • 华东2（上海） • 华北3（张家口）	v2.8.2.3

模块	功能名称	功能概述	发布时间	支持地域	版本号
Kubernetes监控	接入方式更新	• 新增接入方式。更多信息，请参见接入。 • 支持监控接入本地数据中心的注册集群。更多信息，请参见注册集群安装组件。 • 更新Kubernetes监控运行环境要求和限制。	2021-12-03	请参见Kubernetes监控目前支持的地域。	v2.8.2.2
Prometheus监控	多实例聚合查询GlobalView	阿里云Prometheus监控提供地域级别的GlobalView聚合实例的功能。GlobalView聚合实例功能可以为您提供在当前地域下所有Prometheus实例的一个虚拟聚合实例。针对这个虚拟聚合实例可以实现统一的指标查询和告警。更多信息，请参见GlobalView聚合实例（旧版）。	2021-12-03	请参见Prometheus监控目前支持的地域。	v2.8.2.2
	提供指标存储市场自定义功能	指标存储时长最高支持180天。	2021-12-03	请参见Prometheus监控目前支持的地域。	v2.8.2.2
应用监控	arms-pilot新增1.51.0版本	1.51.0版本的arms-pilot组件支持监控容器集群下JDK11版本的应用。更多信息，请参见为容器服务Kubernetes版Java应用安装探针。	2021-12-03	请参见应用监控目前支持的地域。	v2.8.2.2

2021年11月

模块	功能名称	功能概述	发布时间	支持地域	版本号
Prometheus监控	预聚合	预聚合（Recording Rule）可以对落地的指标数据做二次开发。可以配置预聚合规则将计算过程提前到写入端，减少查询端资源占用，尤其在大规模集群和复杂业务场景下可以有效的降低PromQL的复杂度，从而提高查询性能，解决用户配置以及查询慢的问题。	2021-11-19	请参见Prometheus监控目前支持的地域。	v2.8.2.1
应用监控	Trace Explorer	ARMS应用监控的链路分析Trace Explorer功能是基于已存储的全量链路明细数据，自由组合筛选条件与聚合维度进行实时分析，可以满足不同场景的自定义诊断需求。更多信息，请参见Trace Explorer。	2021-11-19	• 华北2（北京） • 华南1（深圳） • 华东1（杭州） • 华东2（上海） • 华北3（张家口）	v2.8.2.1

模块	功能名称	功能概述	发布时间	支持地域	版本号
应用安全	新增访问授权	在接入应用安全之前，您需要先授权访问阿里云安全服务。经过您的授权后，ARMS仅限于访问应用安全依赖的相关资源，用于完成后续的产品功能。更多信息，请参见接入应用安全。	2021-11-19	请参见应用安全目前支持的地域。	v2.8.2.1

2021年10月

模块	功能名称	功能概述	发布时间	支持地域	版本号
告警管理	告警管理新增开服地域	ARMS告警管理功能新增以下开服地域： • 亚太东南（新加坡） • 澳大利亚（悉尼） • 马来西亚（吉隆坡） • 印度尼西亚（雅加达）	2021-10-25	不涉及	v2.8.1.5
应用安全	新增全新的功能模块：应用安全	ARMS应用安全是一款基于RASP（Runtime Application Self-Protection）技术的安全产品，可为应用在运行时提供自我保护。您无需修改应用代码，只需在实例中安装应用安全探针，即可为应用提供强大的安全防护能力，并抵御绝大部分未知漏洞所利用的攻击手法。更多信息，请参见什么是应用安全。	2021-10-14	请参见应用安全目前支持的地域。	v2.8.1.5
Prometheus监控	新增Recording Rule	阿里云Prometheus监控的RecordingRule.yaml只需配置Rule Group。 暂不支持Recording Rule的Remote Write。更多信息，请参见Prometheus监控设置。	2021-10-14	请参见Prometheus监控目前支持的地域。	v2.8.1.5

2021年09月

模块	功能名称	功能概述	发布时间	支持地域	版本号
Prometheus监控	鉴权Token	阿里云Prometheus接入自建Grafana，使用Prometheus Metrics实现HPA等场景需要远程读取ARMS Prometheus存储数据；自建Prometheus、纳管集群（注册集群）等场景需要远程写入ARMS Prometheus存储。在远程读写Prometheus数据时，使用鉴权Token可以提高数据读写的安全性。更多信息，请参见探针设置。	2021-09-29	请参见Prometheus监控目前支持的地域。	v2.8.1.4

模块	功能名称	功能概述	发布时间	支持地域	版本号
Grafana托管服务	插件管理	Grafana托管服务支持一键安装Grafana插件，安装好的Grafana插件将会同步显示到Grafana的**Plugins**页面。更多信息，请参见插件管理。	2021-09-29	请参见Grafana服务目前支持的地域。	v2.8.1.4
	告警管理	Grafana托管服务默认集成到ARMS告警管理中，通过在Grafana中配置告警的通知对象可以将Grafana的告警事件上报至ARMS告警管理中。更多信息，请参见告警管理。	2021-09-29	请参见Grafana服务目前支持的地域。	v2.8.1.4
Grafana托管服务	新增全新的功能模块：Grafana托管服务	• 支持创建Grafana工作区，通过工作区实现免运维和快速启动Grafana运行环境的能力。更多信息，请参见工作区管理。 • 支持一键同步ARMS Prometheus数据源和大盘。更多信息，请参见云服务管理。 • 支持手动添加阿里云日志服务SLS和云监控数据源。更多信息，请参见添加并使用日志服务SLS数据源和添加并使用云监控数据源。 • 支持使用OAuth 2.0协议进行用户认证和应用授权。	2021-09-09	请参见Grafana服务目前支持的地域。	v2.8.1.3
告警管理	新增Skywalking集成	ARMS告警管理支持接入Skywalking，使SKywalking创建的告警可以上报至ARMS告警管理中。更多信息，请参见集成Skywalking。	2021-09-02	不涉及	v2.8.1.3
	新增事件处理流	ARMS告警管理集成多个告警源后，您可以通过设置事件处理流将告警源产生的事件进行过滤和分类。更多信息，请参见事件处理流。	2021-09-02	不涉及	v2.8.1.3
Kubernetes监控	优化集群拓扑	• 优化集群拓扑页面。 • 优化实例异常状态条件：仅产生告警的实例为异常实例。	2021-09-02	请参见Kubernetes监控目前支持的地域。	v2.8.1.3

2021年08月

模块	功能名称	功能概述	发布时间	支持地域	版本号

模块	功能名称	功能概述	发布时间	支持地域	版本号

告警管理	应用监控和前端监控告警指标部分单位优化	• 告警规则中所有指标的单位由Byte（SAE告警除外）变更为MB，原有告警规则会自动转化，告警阈值也会随单位自动变更。
		• 所有百分比的指标统一为0～100，原有0～1的指标的小数阈值会自动转化为0～100的百分比。
			2021-08-19	• 应用监控：
				  ○ 华东1（杭州）
				  ○ 华东2（上海）
				  ○ 华南1（深圳）
				  ○ 华北1（青岛）
				  ○ 华北2（北京）
				  ○ 华北3（张家口）
				• 前端监控：华东1（杭州）
					v2.8.1.2

	应用监控和前端监控告警内容优化	• 指标名称规范化，优化不必要符号。
		• 告警内容增加单位后缀，以便于理解。
		• 对告警值保留两位小数。
			2021-08-19	• 应用监控：
				  ○ 华东1（杭州）
				  ○ 华东2（上海）
				  ○ 华南1（深圳）
				  ○ 华北1（青岛）
				  ○ 华北2（北京）
				  ○ 华北3（张家口）
				• 前端监控：华东1（杭州）
					v2.8.1.2

	应用监控告警规则增加部分指标筛选类型	应用调用统计指标在原有的遍历、=、无基础上增加!=、包含、不包含、正则匹配筛选类型。	2021-08-19	• 华东1（杭州） • 华东2（上海） • 华南1（深圳） • 华北1（青岛） • 华北2（北京） • 华北3（张家口）	v2.8.1.2
	集成Grafana	ARMS告警管理支持接入Grafana，使Grafana创建的告警可以上报至ARMS告警管理中。更多信息，请参见集成Grafana告警。	2021-08-19	不涉及	v2.8.1.2
	集成Zabbix	ARMS告警管理支持接入Zabbix，使Zabbix创建的告警可以上报至ARMS告警管理中。更多信息，请参见集成Zabbix。	2021-08-19	不涉及	v2.8.1.2
	集成Jira	ARMS告警管理支持接入Jira工单系统，使告警创建时可以同步在Jira中创建问题工单，告警状态与工单状态可以实现双向同步。更多信息，请参见通过Jira账号信息集成Jira工单系统。	2021-08-19	不涉及	v2.8.1.2

模块	功能名称	功能概述	发布时间	支持地域	版本号
Kubernetes监控	告警配置	阿里云Kubernetes监控提供开箱即用的告警模板，您可以根据预置的告警模板创建告警规则，也可以自定义针对特定Kubernetes集群的告警规则。更多信息，请参见创建Kubernetes监控告警规则。	2021-08-19	请参见Kubernetes监控目前支持的地域。	v2.8.1.2
	重启探针	Kubernetes监控支持手动重启探针。更多信息，请参见探针管理。	2021-08-19	请参见Kubernetes监控目前支持的地域。	v2.8.1.2
Kubernetes监控	容器监控更名	容器监控正式更名为Kubernetes监控。	2021-08-05	请参见Kubernetes监控目前支持的地域。	v2.8.1.1
	优化集群拓扑	• 优化集群拓扑和容器层3D的功能入口。 • 支持查看拓扑节点连线的详细信息。 • 集群拓扑增加**Workload**页签，支持查看Deployment、StatefulSet和DaemonSet的网络拓扑。 更多信息，请参见查看集群网络拓扑。	2021-08-05	请参见Kubernetes监控目前支持的地域。	v2.8.1.1
Prometheus监控	产品优化	• 支持ACK纳管集群采集存储指标。 • 预置大盘Ingress更新。	2021-08-05	请参见Prometheus监控目前支持的地域。	v2.8.1.1
	Bug修复	修复CMS采集的指标Region Label值错误问题。	2021-08-05	请参见Prometheus监控目前支持的地域。	v2.8.1.1

2021年07月

模块	功能名称	功能概述	发布时间	支持地域	版本号
容器监控	新增国际地域	阿里云容器监控新增以下6个地域： • 亚太东南（新加坡） • 印度尼西亚（雅加达） • 日本（东京） • 美国（硅谷） • 美国（弗吉尼亚） • 德国（法兰克福） 容器监控支持的所有地域，请参见Kubernetes监控目前支持的地域。	2021-07-15	请参见Kubernetes监控目前支持的地域。	v2.8.0.3

模块	功能名称	功能概述	发布时间	支持地域	版本号
	新增按协议类型查看指标	容器监控支持分别查看HTTP、MySQL、TCP、Redis和Kafka协议的指标详情。更多内容，请参见多协议指标详情。	2021-07-15	请参见Kubernetes监控目前支持的地域。	v2.8.0.3
云拨测	新增预付费计费模式	云拨测新增预付费版（包年包月），您可以按需预先购买可用拨测次数。当您的使用量在预付费额度以内，则不产生额外费用；若使用量超过预付费额度时，超出部分会按照后付费版的计费模型进行补充计费。更多内容，请参见云拨测计费规则。	2021-07-15	不涉及	v2.8.0.3
Prometheus监控	支持接入VPC网络下的ECS集群	Prometheus监控支持接入VPC网络的ECS集群，创建大盘后可以监控ECS集群的众多性能指标。更多内容，请参见Prometheus实例 for VPC。	2021-07-15	• 华东2（上海） • 华南1（深圳） • 华北2（北京） • 华北3（张家口）	v2.8.0.3

2021年06月

模块	功能名称	功能概述	发布时间	支持地域	版本号
容器监控	新增全新的功能模块：容器监控	阿里云容器监控是一套针对Kubernetes集群开发的一站式可观测性产品。基于Kubernetes集群下的指标、应用链路、日志和事件，阿里云容器监控旨在为IT开发运维人员提供整体的可观测性方案。更多内容，请参见什么是阿里云Kubernetes监控。	2021-06-18	请参见Kubernetes监控目前支持的地域。	v2.8.0.2
应用监控	支持OpenTelemetry Java SDK	通过OpenTelemetry Java SDK手动埋点后，无需任何改动，ARMS会将相关的Span记录作为独立入口或者内部方法栈，从而监控您的应用。更多内容，请参见通过OpenTelemetry Java SDK进行手工埋点。	2021-06-18	请参见应用监控目前支持的地域。	v2.8.0.2

模块	功能名称	功能概述	发布时间	支持地域	版本号
	异步任务监控	应用监控新增三种方式监控异步任务：Spring @Async标签、自定义异步任务和复杂场景手动透传。更多内容，请参见使用ARMS监控异步任务。	2021-06-18	请参见应用监控目前支持的地域。	v2.8.0.2

2021年05月

模块	功能名称	功能概述	发布时间	支持地域	版本号
Prometheus监控	功能优化	标签值更新之后，Prometheus监控不再采集旧的指标。	2021-05-13	请参见Prometheus监控目前支持的地域。	v2.8.0
地域开服	印度尼西亚雅加达地域开服	雅加达地域支持应用监控、Prometheus监控、APP监控、业务监控、云拨测和链路追踪。更多内容，请参见开服地域。	2021-05-13	不涉及	v2.8.0

2021年04月

模块	功能名称	功能概述	发布时间	支持地域	版本号
应用监控	线程池监控	您可以通过线程池监控功能监控指定应用的线程池的各项指标，包括核心线程数量、当前线程数量、最大线程数量等。更多内容，请参见池化监控。	2021-04-22	请参见应用监控目前支持的地域。	v2.7.9.3
云拨测	海外监测点	云拨测新增海外监测点。更多内容，请参见监测点说明。	2021-04-22	全部	v2.7.9.3

模块	功能名称	功能概述	发布时间	支持地域	版本号
Prometheus监控	HTTP监测	Prometheus的健康巡检支持对ACK Service的HTTP类型的外部端点进行监测。更多内容，请参见创建ACK Service巡检。	2021-04-22	请参见Prometheus监控目前支持的地域。	v2.7.9.3
Prometheus监控	重置大盘	• 支持将所有基础大盘重置到最新版本。 • 支持升级单个基础大盘。 • 支持查看大盘的核心指标。 更多内容，请参见大盘列表。	2021-04-08	请参见Prometheus监控目前支持的地域。	v2.7.9.2

2021年03月

模块	功能名称	功能概述	发布时间	支持地域	版本号
应用监控	Arthas诊断	应用诊断功能下，新增Arthas诊断。更多内容，请参见Arthas诊断（新版）。	2021-03-18	请参见应用监控目前支持的地域。	v2.7.9
	接口调用	接口调用功能中，接口快照页签新增总快照次数和快照响应时间两个图表。更多内容，请参见接口调用。	2021-03-18	请参见应用监控目前支持的地域。	v2.7.9

2021年02月

模块	功能名称	功能概述	发布时间	支持地域	版本号

模块	功能名称	功能概述	发布时间	支持地域	版本号
应用监控	异常过滤和错误数过滤配置	SaveTraceAppConfig接口新增异常过滤和错误数过滤配置字段。更多内容，请参见SaveTraceAppConfig。	2021-02-25	请参见应用监控目前支持的地域。	V2.7.8.3
API	OpenXtraceDefaultSLR	支持调用OpenXtraceDefaultSLR接口开通链路追踪服务关联角色AliyunServiceRoleForXtrace。更多内容，请参见OpenXtraceDefaultSLR。	2021-02-25	全部	V2.7.8.3
	OpenArmsDefaultSLR	调用OpenArmsDefaultSLR接口开通ARMS服务关联角色AliyunServiceRoleForARMS。更多内容，请参见OpenArmsDefaultSLR。	2021-02-25	全部	V2.7.8.3
Prometheus监控	默认服务发现	支持开启和关闭Prometheus的默认服务发现。	2021-02-25	请参见Prometheus监控目前支持的地域。	V2.7.8.3

2021年01月

模块	功能名称	功能概述	发布时间	支持地域	版本号
应用监控	分析调用链	调用链统计页面支持对多条调用链进行聚合分析。更多内容，请参见调用链路查询。	2021-01-29	请参见应用监控目前支持的地域。	v2.7.8.2
Prometheus监控	更新报警配置	Prometheus报警新增设置通知策略。更多内容，请参见创建报警。	2021-01-29	请参见Prometheus监控目前支持的地域。	v2.7.8.2

模块	功能名称	功能概述	发布时间	支持地域	版本号
云拨测	报警功能	云拨测创建任务过程中支持配置报警功能。更多内容，请参见创建浏览任务。	2021-01-14	全部	v2.7.8.1

更多往期版本更新内容，请参考2020年。

1.1.3. 2020年

本文为ARMS在2020年的版本发布记录，介绍发布的特性变更情况。

V2.7.8

发布时间：2020-12-24

新特性：

- 报警
  - 支持配置静默期。
- Prometheus监控
  - 支持远程存储。

V2.7.7.3

发布时间：2020-12-17

新特性：

- 报警
  - 支持对飞书发送Webhook报警。

优化和提升：

- 应用监控
  - 修复线程剖析问题。
  - 修复PHP Agent问题。
- 报警
  - 修复选择报警发送历史为全部时没有数据的问题。

V2.7.7.2

发布时间：2020-11-26

新特性：

- 云拨测
  - 接入告警中心。

V2.7.7.1

发布时间：2020-11-03

新特性：

- 云拨测
  - 新增拨测录制器v0.1。
  - 支持Chrome浏览器的拨测脚本录制。

优化和提升：

- 应用监控
  - 提升拓扑查询性能。

V2.7.7

发布时间：2020-10-15

新特性：

- 云拨测
  - 新增云拨测v0.1。
  - 支持针对HTTP/HTTPS和网络的多城市多运营商的定时拨测。

V2.7.6.2

发布时间：2020-09-15

新特性：

- 大盘和报警
  - 报警指标阈值支持动态基线。

V2.7.5.3

发布时间：2020-08-20

新特性：

- 应用监控
  - 支持Node js应用接入 。

V2.7.4.1

发布时间：2020-08-03

新特性：

- 应用监控
  - AIOps自动诊断支持业务影响评估。

V2.7.3

发布时间：2020-07-09

新特性：

- Prometheus监控
  - 支持函数计算服务的默认监控接入。

V2.7.2

发布时间：2020-06-05

新特性：

- Prometheus监控
  - 支持自建Kubernetes集群接入。

V2.7.1

发布时间：2020-05-15

新特性：

- Prometheus监控
  - 支持基于blackbox的内网监控巡检。

V2.7.0

发布时间：2020-04-02

新特性：

- 应用监控
  - 支持针对调用链的性能问题自动分析。

V2.6.5

发布时间：2020-03-05

新特性：

- 前端监控
  - 支持多维查询性能指标功能。

V2.6.2

发布时间：2020-02-14

新特性：

- 应用监控
  - 支持业务监控。
  - 支持Webflux、Gateway等SpringCloud组件。

V2.6.1

发布时间：2020-02-11

新特性：

- 应用监控
  - 支持获取微服务元数据等相关功能。

V2.6.0.2

发布时间：2020-01-02

新特性：

- 应用监控

- 支持新版异常分析。

优化和提升：

- 应用监控
  - 修复Thrift插件问题。

1.1.4. 2019年

本文为ARMS在2019年的版本发布记录，介绍发布的特性变更情况。

V2.6.0

发布时间：2019-12-17

新特性：

- 应用监控
  - 支持异步调用链。
  - 支持记录Dubbo或HSFProvider调用参数。

V2.5.9.5

发布时间：2019-11-28

新特性：

- 应用监控
  - 支持jfinal-undertow插件。

优化和提升：

- 应用监控
  - 修复若干错误，包括获取不到Dubbo线程剖析数据等问题。

V2.5.9.3

发布时间：2019-11-25

新特性：

- 应用监控
  - 支持ARMS和链路追踪产品打通。

V2.5.9

发布时间：2019-09-06

优化和提升：

- 应用监控
  - 修复FastJson拒绝服务漏洞。
  - 修改获取网卡IP逻辑。

V2.5.8

发布时间：2019-08-02

新特性：

- 应用监控
  - 支持二元状态报警功能，即针对仅具有是和否、有和无这两种状态的指标设置报警规则。
  - 支持国产达梦数据库插件。

V2.5.7.2

发布时间：2019-07-30

新特性：

- 应用监控
  - 支持JVM Metaspace指标。
  - 支持自定义要忽略的HTTP状态码。默认情况下，大于400的状态码会计入错误数，您可以自定义大于400但不计入的HTTP状态码。[相关文档：配置高级设置]

V2.5.7

发布时间：2019-07-11

优化和提升：

- 应用监控
  - 升级依赖的有安全漏洞的FastJson版本。

V2.5.6.1

发布时间：2019-06-28

新特性：

- 应用监控
  - 支持Dubbo和MariaDB插件。
  - 自定义配置支持获取SQL绑定值：捕获PrepareStatement参数绑定的变量值，无需重启应用即可生效。[相关文档：配置高级设置]

优化和提升：

- 应用监控
  - 去除Log4j日志依赖，避免冲突。

V2.5.6

发布时间：2019-06-07

新特性：

- 应用监控
  - 支持分位数统计功能。

V2.5.5

发布时间：2019-06-03

新特性：

- 应用监控

- 支持HSF-HTTP调用。

V2.5.3

发布时间：2019-03-15

新特性：

- 应用监控
  - 支持应用运行过程中的线程指标上报。
  - 支持Spring-Data-Redis插件。
  - 支持Druid数据库连接池插件。

V2.5.1

发布时间：2019-02-01

新特性：

- 应用监控
  - 支持容器服务Kubernetes版应用：可在控制台或开源环境中对部署在容器服务Kubernetes版中的应用开启应用监控。[相关文档：为容器服务Kubernetes版Java应用安装探针 | 为开源Kubernetes环境中的应用安装探针]
- 前端监控
  - 支持小程序监控：可对钉钉E应用、支付宝小程序、微信小程序和其他类别的小程序开启前端监控。[相关文档：开始监控钉钉小程序 | 开始监控支付宝小程序 | 开始监控微信小程序 | 开始监控其他类别小程序]

V2.5.0

发布时间：2019-01-21

新特性：

- 应用监控
  - 新增标签功能：可在应用监控列表中按标签分类应用站点。

优化和提升：

- 前端监控
  - 优化报警。

V2.4.8

发布时间：2019-01-06

新特性：

- 应用监控
  - 新增类冲突检测功能。
  - 支持动态开启和关闭URL收敛规则。

1.1.5. 2018年

本文为ARMS在2018年的版本发布记录，介绍发布的特性变更情况。

V2.4.7

发布时间：2018-12-13

新特性：

- 应用监控
  - 支持对Java应用一键开启应用监控。[相关文档：使用脚本为Java应用快速安装探针]
  - 支持对PHP应用开启应用监控。

优化和提升：

- 应用监控
  - 优化了对Java应用开启应用监控的传统方法。[相关文档：为Java应用手动安装Agent]
- 前端监控
  - 优化了JS错误定位功能：线上的JS代码往往会压缩为一行，因此无法根据浏览器报告的错误行号找到真正的出错位置。ARMS前端监控可利用Source Map还原真正的出错位置。[相关文档：用ARMS前端监控诊断JS错误]

V2.4.6

发布时间：2018-10-26

新特性：

- 应用监控
  - 支持对NoSQL数据库开启监控。
  - 全新概览页：优化了页面布局，新增了应用监控详情、前端监控详情、产品快报模块。

V2.4.5

发布时间：2018-09-17

新特性：

- 应用监控
  - 支持MongoDB：支持的组件和框架中现包括MongoDB。

V2.4.4

发布时间：2018-08-17

新特性：

- 应用监控：
  - 支持线程剖析：对于请求超时的线程，您可以快速定位其内部所有堆栈的耗时情况。[相关文档：使用线程剖析诊断代码层面的问题]
- 前端监控：
  - 支持资源加载明细：您可以快速定位页面的所有慢加载资源，例如图片、JS、CSS、API等。[相关文档：慢会话追踪]
- 自定义监控：
  - 自定义监控正式商用。

V2.4.3.4

发布时间：2018-07-16

新特性：

- 应用监控：
  - 支持全息排查：您可以通过业务ID关联查询到应用监控分布式调用链，从而显著提高问题诊断效率。

V2.4.3.3

发布时间：2018-06-16

优化和提升：

- 通用：
  - 支持以RAM子账号调用OpenAPI，并进一步加强了API调用安全认证。[相关文档：相关文档]
- 应用监控：
  - 应用监控首页全新改版，展示了更多核心摘要信息。
  - 优化了不同网络环境下的内存快照抓取分析功能，抓取效率提高50% 以上。

V2.4.3

发布时间：2018-05-19

新特性：

- 应用监控：
  - 新增内存快照分析功能，让内存对象分布情况一览无余，帮助您迅速定位内存泄露问题。[相关文档：内存快照]
  - 新增监控方法自定义配置功能，让您可以自行动态配置要监控和捕获异常的具体方法，使监控细粒度范围进一步扩大，并且配置立即生效，无需重启机器。
  - 新增应用监控概览页，问题排查和定位更加方便准确。
  - 新增MQ链路监控，可快速定位消息延时、错误、堆积等情况。

V2.4.2

发布时间：2018-04-19

新特性：

- 应用监控：
  - 新增JVM监控功能，可监控一系列JVM重要指标，包括堆内存、非堆内存、线程数等相关指标。[相关文档：JVM监控]
  - 新增主机监控功能，可监控一系列主机性能指标，包括CPU、内存、磁盘、网络流量等相关指标。[相关文档：主机监控]
  - 新增自定义配置功能，可直接在用户界面上修改配置，包括调用链采样、Agent开关、阈值设置等。
- 前端监控：
  - 新增抽样上报配置，可通过随机抽样上报来减小用户上报量并降低负载。[相关文档：SDK参考]
- 自定义监控
  - 新增模式检测配置功能，日志模式概览和日志模式对比模块可帮助您及时发现日志中的异常。

V2.4.1

发布时间：2018-03-22

新特性：

- 通用：
  - 报警规则：支持批量导入导出，报警管理更方便。
  - 针对EDAS部分应用监控正式商用，长期五折优惠。
- 应用监控：
  - 支持查看Agent在线列表，用户已安装Agent版本和状态一目了然。
- 前端监控：
  - 支持将以平均数改为以分位数查看响应时间，慢请求的耗时和分布情况更加清晰。
- 应用监控：
  - 支持分位数算子，指标统计除了平均值、最大值、最小值以外，还能通过分位数查看更详细的统计。

V2.4.0

发布时间：2018-02-26

新特性：

- ARMS前端监控和应用监控功能正式商用。

V2.3.3.1

发布时间：2018-01-31

新特性：

- ARMS应用监控全面支持EDAS应用：EDAS用户可将EDAS应用一键接入ARMS应用。

V2.3.3

发布时间：2018-01-14

新特性：

- 全新首页和配套文档，产品页重大改版，产品正式定位为面向**应用监控**、**前端监控**，和**自定义监控**的应用性能管理（APM）组合型产品。
- 面向APM底座功能基本改造完毕，为用户提供面向应用监控、前端监控，和自定义监控三大子产品的统一报警平台和统一交互大盘。
- 全面支持五大地域：杭州、北京、上海（新增）、青岛（新增）、深圳（新增）。

优化和提升：

- 控制台中心化优化，中国地域统一使用一个控制台。
- 报警查询界面优化，提供多维报警查询。

1.1.6. 2017年

本文为ARMS在2017年的版本发布记录，介绍发布的特性变更情况。

V2.3.1

发布时间：2017-12-14

新特性：

- 应用监控功能，支持大部分常见的Java应用监控APM功能，例如调用拓扑、链路跟踪、慢事务报表、慢SQL查询等。支持十余种云上普通用户需要的Java栈框架，例如Spring、Redis、MySQL（RDS）、Dubbo等。应用可以通过挂载javaagent的方式接入，无需修改应用代码。

优化和提升：

- 优化了大盘控件数据集设置的方法，将基本指标和复合指标融合在一起展示。
- 优化了新人提示逻辑，新人提示默认仅在第一次登录时打开。

V2.2.6.2

发布时间：2017-09-23

新特性：

- 交互式大盘支持热力图。
- 新增异常切分器，支持Java Exception的数据清洗。
- 数据清洗流程中新增IP到物理地址映射功能模块。
- 支持数据集过滤条件为NULL类型。

优化和提升：

- 优化告警内容，邮件中告警内容带有日志采样内容。
- 优化了Nginx模板，更加清晰好用的Nginx监控功能全新上线。

V2.2.6

发布时间：2017-08-31

新特性：

- 全新发布针对质量和性能监控的前端监控功能。
- 支持使用MQ数据源进行业务监控。

V2.2.5

发布时间：2017-07-26

新特性：

- ARMS数据源支持MQ数据接入。
- 数据集支持百万级数据查询。
- 同类报警支持聚合展示，展示效果更加高效。
- 交互式大盘的共享链接创建和对接，浏览大盘无需用户登录。
- 交互式大盘新增黑白主题，更加美观。
- 交互式的表格属性增强，浏览时表头可固定，且可按时间顺序倒排。

V2.2.4

发布时间：2017-06-21

新特性：

- 支持通用数据集。

- 前端可视化组件全新改版切换至G2，且单控件支持多数据集。
- 支持ARMS交互式大盘外链。
- 数据集报警热编辑。
- API支持百万级别数据查询。
- 数据清洗支持XML/换行日志切分。

V2.2.3

发布时间：2017-03-30

新特性：

- 数据集Pop接口支持Python。
- 交互式大盘控件增强，如面积图支持堆叠模式等。
- 开通北京地域。

优化和提升：

- 报警功能整体优化，支持单个报警生效时间、报警级别，以及报警方式的灵活设定。
- API查询结果支持维表关联输出。

V2.2.2

发布时间：2017-03-08

新特性：

- 支持维表功能，允许用户自定义属性的映射关系，如城市zipcode映射到具体城市省市区。
- 标准任务模板发布，支持用户基于标准任务模板快速定制监控任务。
- 增加报警恢复功能，当报警恢复时，通过邮件发送通知。

优化和提升：

- 交互式大盘持续优化，增加TopN过滤、数据补0，和更多的时间粒度支持等。

V2.2.1

发布时间：2017-02-17

新特性：

- 增加rate算子支持，适用场景包括速率变化统计等。
- RAM授权规则支持。

优化和提升：

- 大幅优化ARMS实时计算响应时间，某些场景从之前10秒以上响应时间缩短到5秒内。
- 交互式大盘持续优化，各类窗口缩放模式更加细粒度。

V2.2.0

发布时间：2017-01-23

新特性：

- 交互式大盘上线。
- 支持任务的复制和导入导出，方便用户快速复制已有监控方案。
- 用户任务自检，包括任务错误统计、错误抽样。

- 复合算子支持。

1.1.7. 2016年

本文为ARMS在2016年的版本发布记录，介绍发布的特性变更情况。

V2.1.0

发布时间：2016-10-08

新特性：

- 新增SLS Loghub，SDK API数据源。
- 报警功能支持各类常用高级算子（指定过去N分钟/天/小时，指标MAX/AVG/MIN阈值设定）。
- 高级算子Count Distinct、Sample支持。
- 数据集交互式查询界面支持。

V2.0.0

发布时间：2016-08-04

新特性：

- 支持ECS日志收集形式的数据接入。
- 支持各类清洗计算：单/多/顺序分隔符、KV清洗、JSON清洗，以及其他各类定制化（如异常堆栈）清洗逻辑。
- 支持多种聚合计算：基于各类时间粒度的所有常规聚合计算，例如SUM、COUNT、MAX等。
- 业务报警设置支持各类内容指标定义、等级区分定义，和各类联系人通知方式定义。
- 展示图表定制提供时间序列或其他类似各种维度的全套解决方案，集成柱状、折线、饼图、翻牌器、表格等常见展现形式及大盘配置，提供数据下钻、上钻能力。
- 支持通过拖拽已定义的报警和图表来定制大盘。

1.2. 产品公告

1.2.1. 【产品变更】ARMS应用安全商用通知

ARMS应用安全于2022年06月18日0点起正式商用。

计费说明

ARMS应用安全转为商用后，关于定价计费的更多信息，请参见计费规则。

应用安全功能概述

ARMS应用安全是一款基于RASP（Runtime Application Self-Protection）技术的安全产品，可为应用在运行时提供自我保护。您无需修改应用代码，只需在实例中安装应用安全探针，即可为应用提供强大的安全防护能力，并抵御绝大部分未知漏洞所利用的攻击手法。更多信息，请参见什么是应用安全。

1.2.2. 【产品变更】应用监控部分地域商用通知

ARMS应用监控于2022年06月08日00:00起对部分地域正式商用。

ARMS应用监控目前有基础版、专家版（按量付费）和专家版（预付费资源包）3个计费版本。

ARMS应用监控于2022年06月08日00:00起针对以下地域进行商业化计费：

基础版：

- 华北5（呼和浩特）
- 华北6（乌兰察布）
- 华南2（河源）
- 华南3（广州）
- 西南1（成都）
- 印度（孟买）
- 马来西亚（吉隆坡）
- 印度尼西亚（雅加达）
- 日本（东京）
- 澳大利亚（悉尼）
- 德国（法兰克福）
- 英国（伦敦）
- 美国（弗吉尼亚）

专家版（按量付费）：

- 华北5（呼和浩特）
- 华北6（乌兰察布）
- 华南2（河源）
- 华南3（广州）
- 西南1（成都）
- 马来西亚（吉隆坡）
- 印度尼西亚（雅加达）
- 日本（东京）
- 澳大利亚（悉尼）
- 德国（法兰克福）
- 英国（伦敦）
- 美国（弗吉尼亚）

专家版（预付费资源包）：

- 华北5（呼和浩特）
- 华北6（乌兰察布）
- 华南2（河源）
- 华南3（广州）
- 西南1（成都）
- 印度（孟买）
- 马来西亚（吉隆坡）
- 印度尼西亚（雅加达）
- 日本（东京）

- 澳大利亚（悉尼）
- 德国（法兰克福）
- 英国（伦敦）
- 美国（硅谷）
- 美国（弗吉尼亚）

计费说明

阿里云ARMS应用监控定价详情，请参见应用实时监控服务ARMS价格说明。

1.2.3. 【产品变更】ARMS Grafana服务商用通知

ARMS Grafana服务于2022年05月18日0点起正式商用。

计费说明

ARMS Grafana服务转为商用后，关于定价计费的更多信息，请参见计费规则。

Grafana服务功能概述

阿里云Grafana服务提供免运维和快速启动Grafana运行环境的能力，并与阿里云账号打通，支持直接登录或授权其他阿里云账号使用Grafana服务。更多信息，请参见什么是Grafana服务。

1.2.4. 【产品变更】ARMS关于自定义监控下线公告

ARMS将计划分阶段下线自定义监控，从2022年01月01日起，自定义监控不再支持创建新的监控任务，同时停止自定义监控收费。对于已有的监控任务，自定义监控将免费维护至2022年03月31日，到期后将不再维护。建议您在2022年03月31日之前完成监控任务的迁移。

迁移建议：

- 对于数据源是日志服务（SLS）的监控任务，建议迁移到ARMS业务监控下的日志监控，日志监控提供日志转换成Prometheus时序数据的能力。更多信息，请参见开始使用日志监控。
- 对于其他数据源的监控任务，建议将数据接入日志服务（SLS）。更多信息，请参见日志服务官方文档。

1.2.5. 【产品变更】ARMS告警管理商用通知

ARMS告警管理于2022年03月18日0点起正式商用。

计费说明

ARMS告警管理转为商用后，关于定价计费的更多信息，请参见告警管理计费规则。

告警管理功能概述

告警管理提供了可靠的告警收敛、通知、自动升级以及其他功能，帮助您快速检测和修复业务告警。更多信息，请参见告警管理概述。

1.2.6. 【产品公告】Prometheus监控商用通知

阿里云Prometheus监控在金融云、政务云、华北1（青岛）、华北5（呼和浩特）、华南2（河源）、华南3（广州）、西南1（成都）、中国香港（香港）、美国东部1（弗吉尼亚）、美国西部1（硅谷）、英国伦敦（伦敦）以及欧洲中部1（法兰克福）这些地域于2022年02月17日00:00起正式商用。

收费说明

商用后阿里云Prometheus监控定价详情，请参见按量付费。

阿里云Prometheus监控目前支持的地域信息，请参见开服地域。

1.2.7. 前端监控计费改动通知

从2020年2月1日开始，前端监控计费模型进行试调整，之后是否取消调整另行通知。

收费规则

本次调整前，前端监控的收费项包括PV上传次数、API上传次数、自定义上传次数。

从2020年2月1日开始，API上传次数将不再做为主要收费项，具体改动如下：

- 提供API上传免费额度，每日免费赠送50万次。
- 超过50万上传次数的部分，按照原先十分之一的价格进行计费。

如何预估前端监控成本

1. 预估每日上报流量

   计算公式：每日上报流量 = PV +（API - 每天50万）* 0.1 + 自定义上报

2. 换算成金额

   金额计算器：ARMS价格计算器

   金额计算公式：（上报流量 / 资源包容量）* 资源包单价

   以杭州区域为例。假设平均每天PV上报是200万，API上报是2000万，自定义上报是20万，则每月产生的金额计算方法如下：

   计费流量（万）=（200+（2000 - 50）* 0.1 + 20）* 30 = 12,450

   金额（元）=（12,450 / 12800）* 15120 = 14,706

> **注意** 做API采样上报能够进一步降低费用。建议您购买资源包。其中高级资源包单价约为按量计费的40%。详情参见下表。

前端监控专家版资源包

名称	规格	价格	折合计费单价	有效期
初级资源包	200万页面上报次数	420元	0.21元 / 1000前端数据上报次数	6个月
中级资源包	1600万页面上报次数	2,520元	0.158元 / 1000前端数据上报次数	1年
高级资源包	12800万页面上报次数	15,120元	0.118元 / 1000前端数据上报次数	1年

相关文档

- 什么是ARMS前端监控？

2.Grafana服务

2.1. 产品简介

2.1.1. 什么是

阿里云Grafana服务提供免运维和快速启动Grafana运行环境的能力，并与阿里云账号打通，支持直接登录或授权其他阿里云账号使用Grafana服务。

Grafana服务可以帮助您在高效分析与查看指标、日志和跟踪的同时，无需关注服务器配置、软件更新等繁杂工作，有效降低运维复杂性与工作量，并借助阿里云强大的云原生能力，全面提升Grafana的安全性与可用性。

Grafana服务提供各类阿里云数据源（如应用实时监控服务ARMS、阿里云Prometheus监控、日志服务SLS等），并提供预置数据源大盘，也可使用VPC内自建的数据源（如Elasticsearch、InfluxDB等）。

阿里云Grafana服务全面对接开源Grafana。关于开源Grafana的详细信息，请参见Grafana官方文档。

核心优势

- 弹性、免运维：通过Grafana服务，无需管理运维服务器即可使用高可用服务。
- 统一可视化：支持阿里云各数据源（如ARMS、阿里云Prometheus监控、SLS等）以及自建数据源和第三方云厂商数据源。
- 数据安全与授权：支持阿里云账号SSO和自建账号体系，实现数据源与大盘的精细化管理。

功能特性

- 默认集成各种云服务

  默认集成ARMS、阿里云Prometheus监控、云监控、SLS、阿里云Elasticsearch等云服务，并提供各种云服务的数据源配置、预置大盘与一键告警。

- 多种插件任意选

  可以使用Grafana插件连接您的工具和您的团队。数据源插件通过API连接到现有数据源并实时呈现数据，而无需您手动获取或迁移数据。

- 自定义告警体系

  使用Grafana告警，您可以在一个简单的UI中创建、管理和静音所有告警，允许您轻松整合和集中所有告警。

- 多维度数据查询

  支持跨数据源查询、数据源重命名、汇总、组合和执行计算。

- 自建数据源

  支持打通同地域多个VPC或添加多个VPC中的数据源到同一个工作区，支持统一查询展示与告警。

- 面板编辑器

  通过一致的UI轻松配置、自定义和浏览所有面板，以便跨所有可视化面板设置数据选项。

2.1.2. 开服地域

本文介绍Grafana服务提供支持的地域。

Grafana服务当前部署地区如下，跨地域内网链接可在Grafana控制台内通过创建VPC打通。具体操作，请参见VPC数据源通道管理。

地区	地域名称	所在城市	Region ID
中国	华东1	杭州	cn-hangzhou
东南亚	新加坡	新加坡	ap-southeast-1
欧洲	德国	法兰克福	eu-central-1
日本	日本	东京	ap-northeast-1
美国	美国	硅谷	us-west-1

2.2. 使用教程

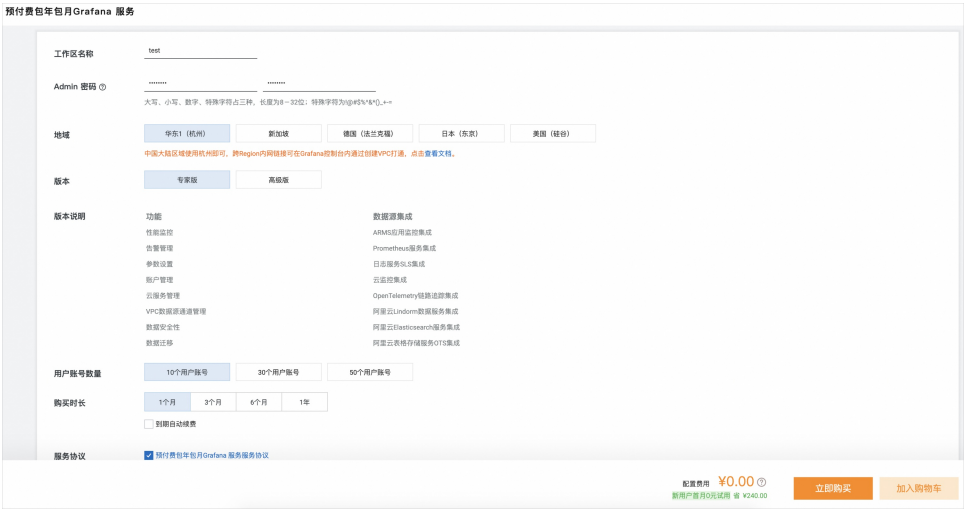
2.2.1. 工作区管理

本文介绍如何创建并管理Grafana工作区。

创建工作区

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击**创建工作区**。
4. 在工作区购买页面输入工作区名称和Admin密码，选择工作区所在地域、购买版本和时长，选中服务协议，然后单击**立即购买**。

> **说明** 各版本计费详情，请参见计费规则。



5. 在**支付完成**页面单击**管理控制台**。

   在**工作区管理**页面可以查看已创建的工作区，以及工作区到期时间。

管理工作区

在**工作区管理**页面，您可以执行以下操作管理Grafana工作区。

- 单击目标工作区ID或右侧**操作**列的**管理**，可以查看或修改工作区的基本信息，并管理工作区下的参数和数据源。
- 单击目标工作区的**访问地址url**，可以进入工作区对应的Grafana页面。

> **说明** 在Grafana登录页面，您可以使用Admin账号和创建工作区时设置的Admin密码登录Grafana，也可以单击Sign in with Alibaba Cloud直接使用当前阿里云账号登录Grafana。

- 单击目标工作区右侧**操作**列的**续费**，可以延长工作区到期时间。
- 单击目标工作区右侧**操作**列的**升配**或**降配**，可以更新工作区版本。

相关文档

- Grafana HTTP API Reference

2.2.2. 工作区信息

在**工作区信息**页面，您可以查看或修改工作区的基本信息和连接信息。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**，进入**工作区信息**页面。

功能说明

在**基本信息**区域，您可以执行以下操作：

- 修改工作区名称和描述。
- 释放当前工作区。

> **说明** 释放后工作区的IP地址将不会保留，但对应的Grafana数据将会保留。

在**连接信息**区域，您可以执行以下操作：

- 单击**网络协议**列的**修改**，切换HTTP或HTTPS协议。
- 单击**端口号Port**列的**修改**，修改端口号。
- 单击**操作**列的**登录**进入Grafana页面。

> **说明** 在Grafana登录页面，您可以使用admin账号和创建工作区时设置的密码登录Grafana，也可以单击**Sign in with Alibaba Cloud**直接使用当前阿里云账号登录Grafana。

2.2.3. 云服务管理

在**云服务管理**页面，您可以查看当前工作区集成的数据源，并手动同步数据源及大盘。

查看集成的数据源

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**云服务管理**。

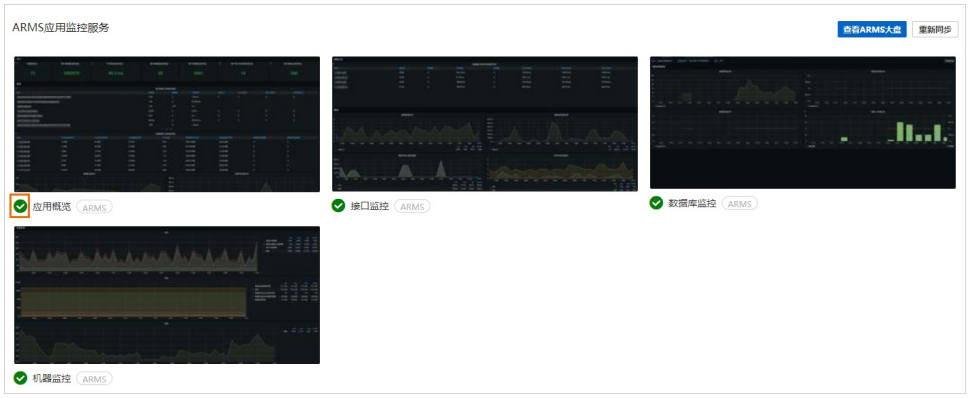
同步数据源和大盘

Grafana服务目前仅支持一键同步ARMS应用监控、Prometheus监控、告警管理下的数据源和大盘。

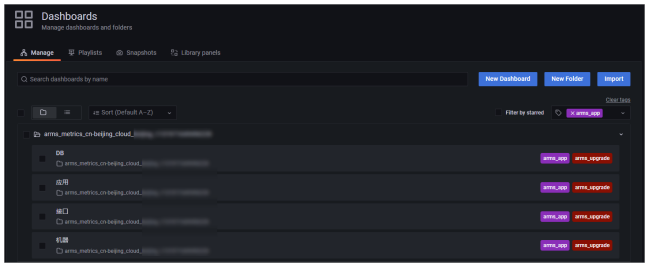
其他数据源的接入配置请参见以下文档：

- SLS数据源的接入配置，请参见添加并使用日志服务SLS数据源。
- 云监控数据源的接入配置，请参见添加并使用云监控数据源。
- Lindorm数据源的接入配置，请参见添加并使用Lindorm数据源。
- Elasticsearch数据源的接入配置，请参见通过公网地址添加并使用阿里云Elasticsearch数据源。
- Tablestore数据源的接入配置，请参见添加并使用Tablestore数据源。

1. 在**云服务管理**页面左侧选择需要同步的数据源类型。
2. 单击**立即集成**。
   等待几分钟后，当大盘名称前出现图标时，表示数据源和大盘已完成同步。

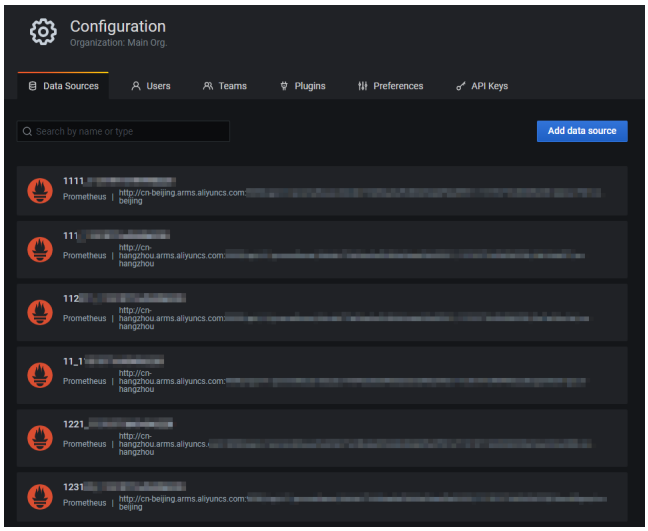


3. 单击右上角的查看大盘进入Grafana的**Dashboards**页面。
   在**Dashboards**页面您可以查看已同步的大盘。



4. 在Grafana左侧导航栏选择 > **Data sources**。

   在**Data sources**页签可以查看已同步的数据源。

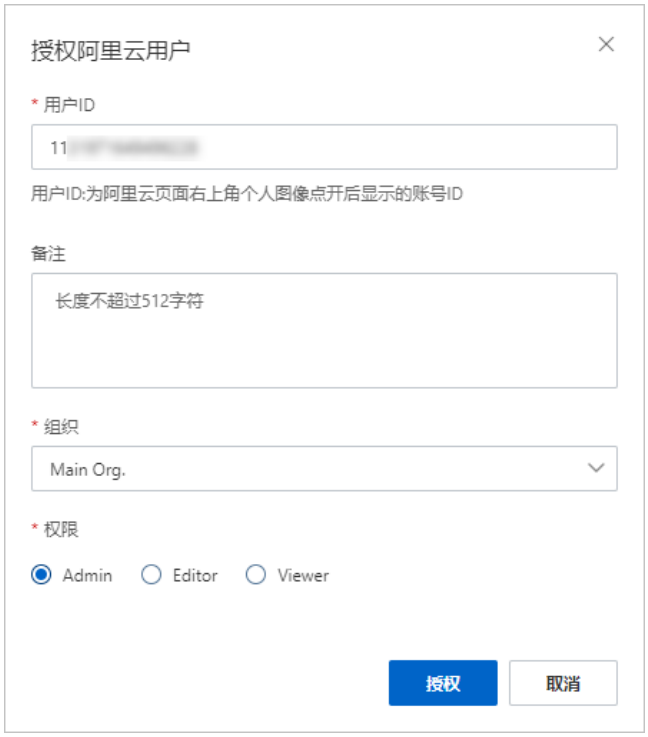


2.2.4. 账号管理

在Grafana服务的账号管理页面，您可以授权其他阿里云账号使用Grafana工作区。本文介绍如何为阿里云账号授权，并使用被授权账号登录Grafana。

授权用户

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**账号管理**，然后在右侧页面单击**授权阿里云用户**。
5. 在**授权阿里云用户**对话框输入阿里云用户的账号ID，并选择组织和授予权限，然后单击**授权**。



参数	说明
用户ID	需要授权的阿里云账号ID。
备注	当前授权用户的备注信息，仅在阿里云控制台上做展示。
组织	选择账号归属的Grafana组织。您可以在Grafana的**Server Admin > Org**页面管理组织，具体操作，请参见Grafana官方文档。
权限	设置用户对Grafana工作组中所有大盘的使用权限。 ○ Admin：管理员权限。 ○ Editor：编辑权限。 ○ Viewer：只读权限。 更详细的权限信息，请参见Grafana官方文档。

设置完成后，在账号管理页面可以查看已授权的用户。

6. 授权完成后，返回**工作区管理**页面，将目标工作区的**访问地址url**复制并分享给被授权的用户。

被授权用户登录Grafana

1. 使用被授权用户的账号登录阿里云。
2. 通过Grafana访问地址URL进入Grafana页面。
3. 在Grafana登录页面，单击**Sign in with Alibaba Cloud**即可使用授权过的阿里云账号登录Grafana。

管理账号

在账号管理页面，您可以修改当前工作区的Admin账号密码，或管理授权用户的账号权限。

- 单击页面右上角的**重置Admin密码**，在**重置Admin密码**对话框设置Admin账号的新密码。
- 单击目标授权用户**操作**列的**新增权限**，可以为用户增加归属的Grafana组织，并设置用户在组织中的权限。
- 单击目标授权用户**操作**列的**修改权限**，可以修改用户在Grafana组织中的权限。
- 单击目标授权用户**操作**列的**删除权限**，可以删除用户归属的Grafana组织。
- 单击目标授权用户**操作**列的**删除账号**，可以删除当前授权用户。

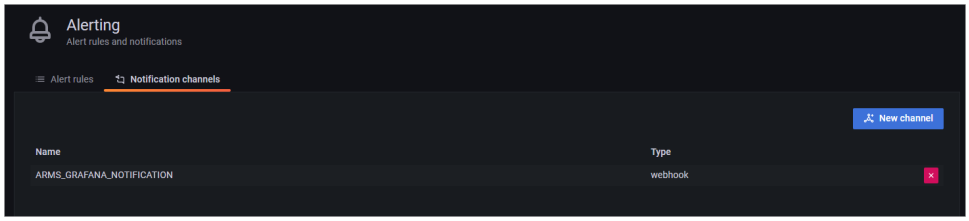
2.2.5. 告警管理

Grafana服务默认集成到ARMS告警管理中，通过在Grafana中配置告警的通知对象可以将Grafana的告警事件上报至ARMS告警管理中。在ARMS告警管理中配置Grafana对应的通知策略后，系统将会通过电话、短信、邮件或钉钉的方式发送告警通知。本文介绍如何通过配置Grafana告警将Grafana告警上报至ARMS告警管理。

步骤一：查看Grafana告警通道

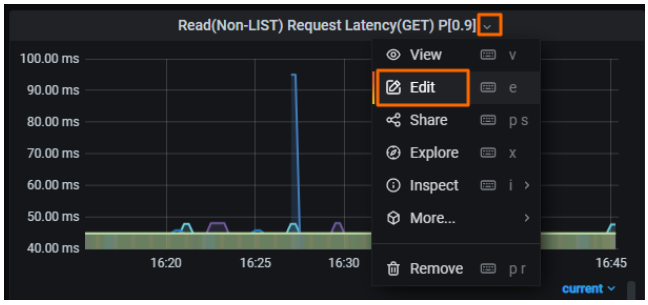
1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**告警管理**。

   告警管理页面显示了Grafana服务自动创建的Grafana告警通道。
5. 单击告警通道右侧**操作**列的**配置管理**。
6. 在Grafana的**Notification channels**页签查看Grafana服务创建的告警通道。

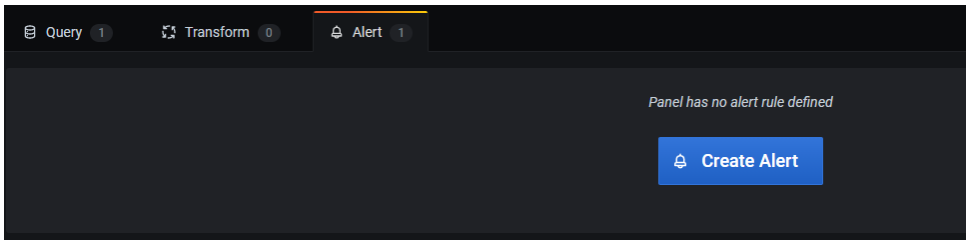


步骤二：创建Grafana告警

1. 在左侧导航栏，选择 > **Manage**。
2. 在**Manage**页签，单击需要创建告警的监控大盘。
3. 在大盘页面选择需要创建告警的面板，单击面板名称右侧的箭头，然后单击**Edit**。



4. 在Edit Panel页面单击Alert页签，然后单击Create Alert。



5. 在Notifications区域，单击Send to右侧的+图标，然后选择名称为ARMS_GRAFANA_NOTIFICATION的告警通道。
6. 根据需求设置其他告警参数。具体操作，请参见Grafana官方文档。
7. 告警创建完成后，单击右上角的Save。
   当Grafana告警被触发时，告警事件将会上报至ARMS告警管理的**告警事件历史**页面，更多信息，请参见查看告警事件历史。

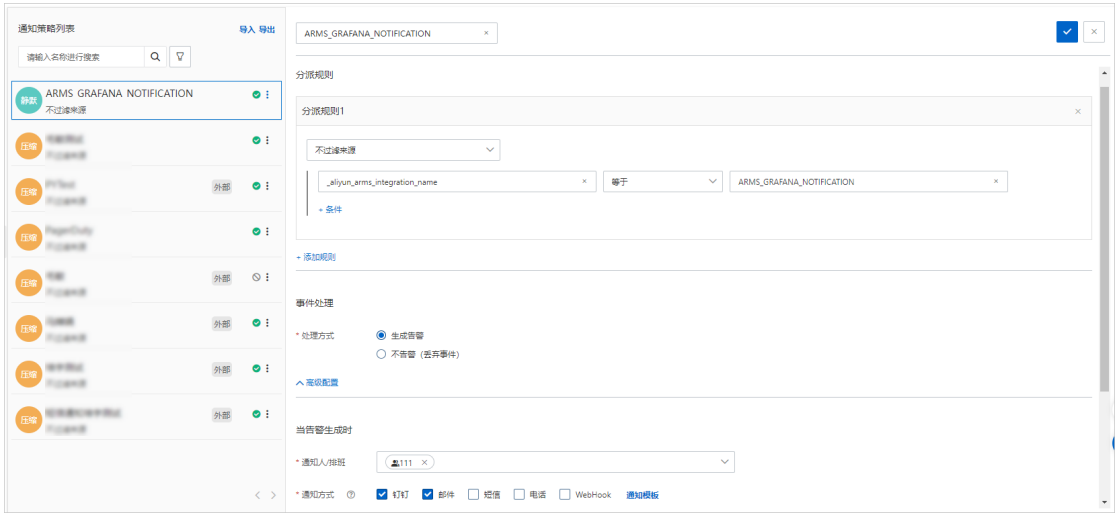
步骤三：创建通知策略

Grafana服务默认创建了对应的通知策略，您需要在通知策略中配置通知人信息才能接收Grafana告警通知。

1. 登录ARMS控制台。
2. 在左侧导航栏中选择**告警管理 > 通知策略**。
3. 在**通知策略列表**区域选择名称为ARMS_GRAFANA_NOTIFICATION的通知策略，然后单击右上角的 图标。
4. 在右侧区域进行以下操作。
   i. 在**事件处理**区域，选择处理方式为生成告警。
   ii. 在**当告警生成时**区域选择告警通知人和通知方式。

参数	说明
通知人/排班	通知人支持设置联系人、联系人组、IM机器人或排班表。联系人创建方法，请参见联系人概述。
通知方式	通知方式支持钉钉、邮件、WebHook、短信和电话，可以同时选择多种方式。 **说明** ■ 未验证手机号的联系人无法使用电话通知方式。验证手机号的操作，请参见验证手机号。 ■ 单击**通知模板**，可以在**通知模板**对话框中设置邮件、短信和电话的通知信息格式。

iii. 根据需求设置其他参数，具体操作，请参见通知策略。

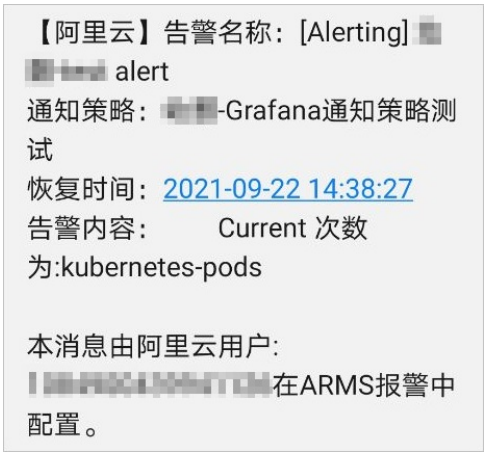


5. 设置完成后，单击右上角的 图标。

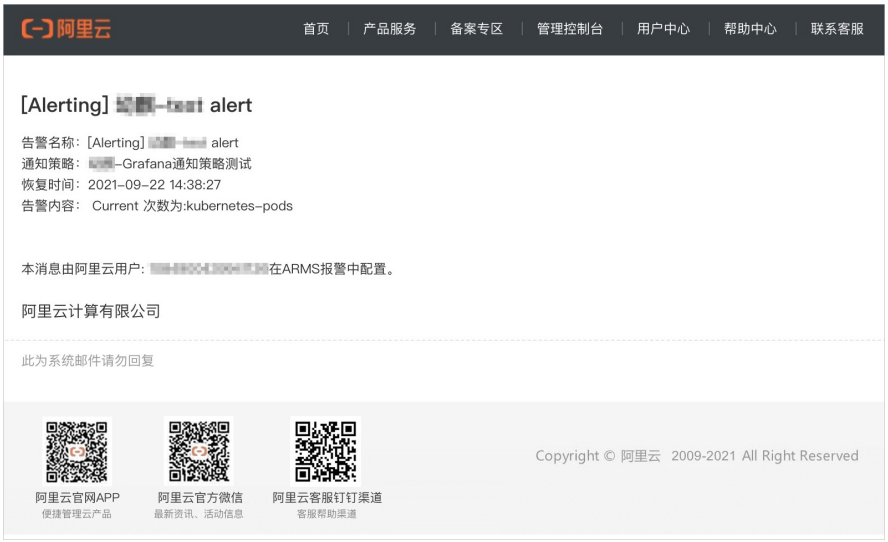
查看告警通知

当通知策略被触发时，收到的告警通知如下所示：

- 短信：



- 邮件：

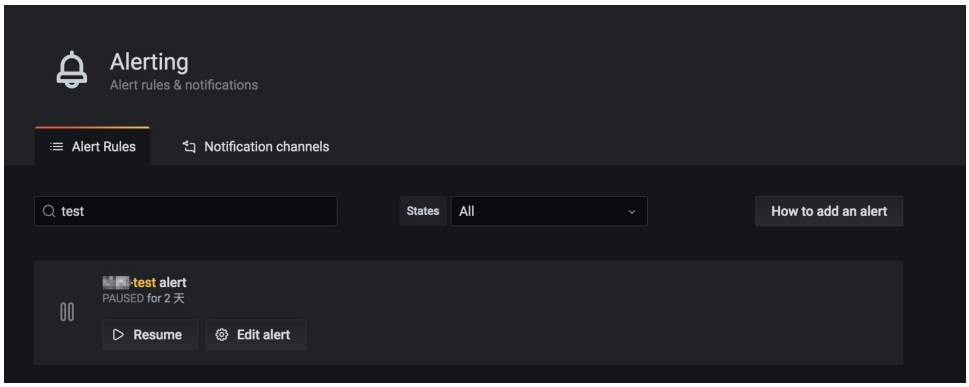


- 钉钉群：

  在钉钉群中收到告警通知后，您可以直接在钉钉群中处理告警。具体操作，请参见在告警通知群中处理告警。

管理Grafana告警规则

您可以在Grafana的**Alert Rules**页签启用或禁用Grafana告警。更多信息，请参见Grafana官方文档。



2.2.6. 参数设置

本文介绍如何在Grafana服务控制台修改Grafana的*.ini*配置文件。

背景信息

Grafana存在多种配置项，您可以在*.ini*配置文件下修改Grafana环境变量等参数。

- 7.5.x版本的Grafana参数配置，请参见Grafana官方文档。
- 8.2.x版本的Grafana参数配置，请参见Grafana官方文档。

操作步骤

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**参数设置**。

在**参数设置**页面，您可以根据需求设置以下类型的Grafana参数。

- auth.generic_oauth
- auth.azuread
- server
- auth.anonymous
- auth
- smtp
- security
- unified_alerting
- alerting
- auth.ldap
- rendering

> 说明
>
> - 7.5.x版本的Grafana参数配置，请参见Grafana官方文档。
> - 8.2.x版本的Grafana参数配置，请参见Grafana官方文档。

相关文档

- OAuth统一登录
- 为Grafana大盘生成免登录查看的共享链接
- 使用SMTP邮箱邀请用户
-
-
-

2.2.7. 数据安全性管理

当您需要通过公网或私网来访问Grafana服务工作区时，可将待访问设备的IP地址加入到工作区的公网或私网对应的访问白名单组中。本文介绍如何配置Grafana服务工作区的公网或私网访问白名单。

操作步骤

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**数据安全性**。
5. 在**白名单设置**页签单击**通用白名单**右侧的**修改**。
6. 在**修改通用白名单**对话框中，设置白名单IP信息。

   组内白名单：公网和私网访问白名单都支持配置为单个IP地址或IP网段的形式，例如192.168.0.1或192.168.0.0/24，多个IP地址之间用半角逗号（,）隔开。127.0.0.1代表禁止所有IPv4地址访问，0.0.0.0/0代表允许所有IPv4地址访问。
7. 单击**确认**。

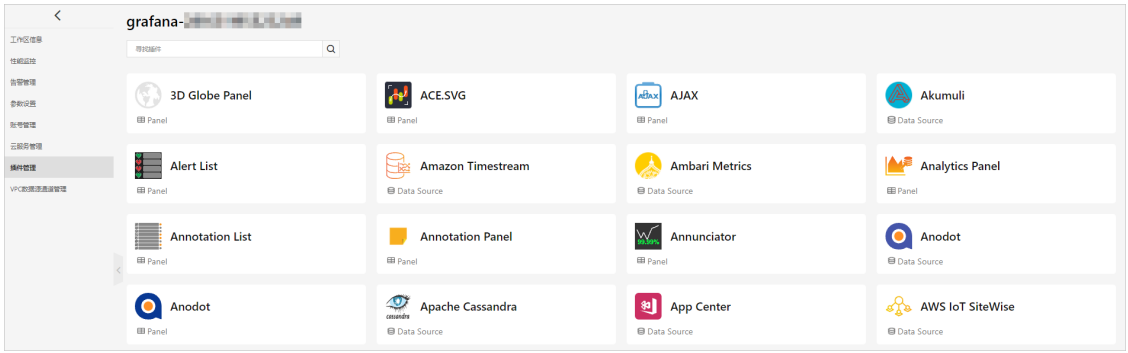
2.2.8. 插件管理

Grafana服务支持一键安装Grafana插件，安装好的Grafana插件将会同步显示到Grafana的**Plugins**页面。本文介绍如何在Grafana服务中安装Grafana插件。

> **说明** 8.2.x版本的Grafana已支持直接在Configuration > Plugins页面安装插件，具体操作，请参见Grafana官方文档。因此，Grafana服务仅为7.5.x版本的Grafana提供一键安装插件的功能，具体操作，请参见本文档。

安装插件

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**插件管理**。
5. （可选）在搜索框中输入需要安装的插件的关键词，然后单击图标。



6. 单击目标插件所在区域，在右侧**插件详情**面板中单击**安装**。
7. 在弹出的**安装插件**对话框中选择需要安装的插件版本，然后单击**安装**。

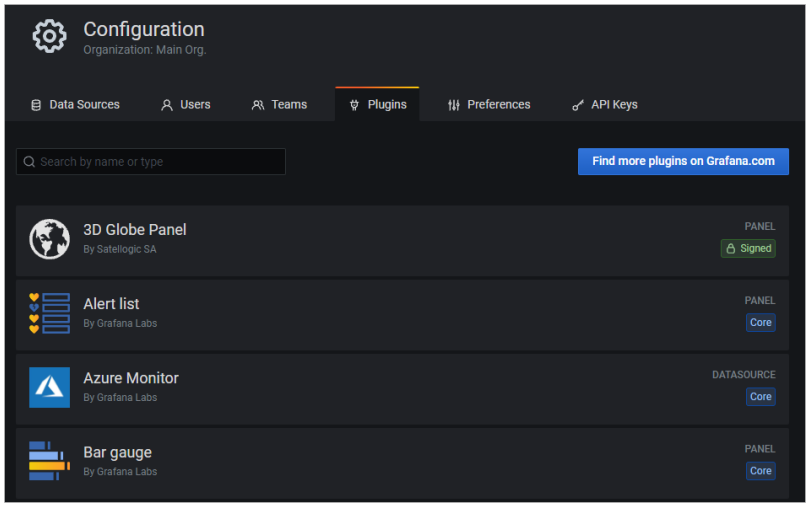
> **说明** 根据插件大小不同，插件安装预计需要1~5分钟。

安装完成后，**插件详情**面板中显示的插件状态为已安装。

在Grafana中查看已安装的插件

1. 在Grafana服务左侧导航栏单击**工作区信息**。
2. 在**工作区信息**页面，单击**连接信息**区域的**登录**进入Grafana。
3. 在Grafana左侧导航栏选择 > Plugins。

在**Plugins**页签可以查看所有已安装的Grafana插件。



卸载插件

1. 在Grafana服务左侧导航栏单击**插件管理**。
2. （可选）在搜索框中输入需要卸载的插件的关键词，然后单击图标。
3. 单击目标插件所在区域，在右侧**插件详情**面板中单击**卸载**。
4. 在弹出的**卸载提示**对话框中单击**卸载**。

> **说明** 由于插件信息异步加载机制，插件卸载后**插件详情**面板中的插件状态存在10秒左右的延迟。

更新插件版本

Grafana服务暂不支持直接更新已安装插件的版本，您可以通过先卸载插件，再安装新版本插件实现更新。

2.2.9. 数据报表

Grafana服务的数据报表功能，支持将指定的整张大盘导出，也可以定时将指定大盘发送到预设的邮箱。

前提条件

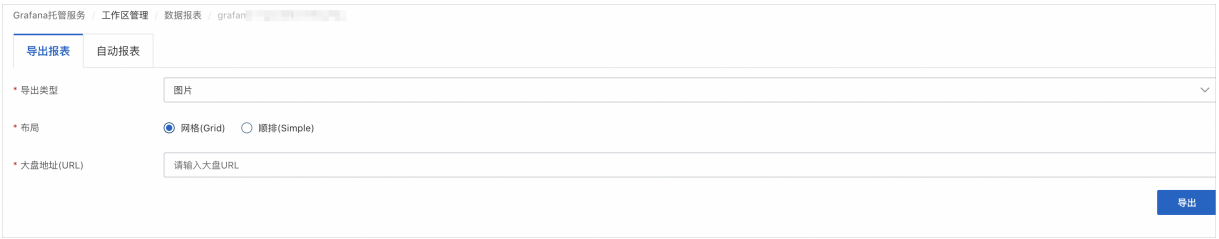
数据报表为高级版工作区功能，请确认您的工作区已开通高级版。您可以在Grafana服务控制台开通或升级工作区版本，更多信息，请参见专家版和高级版。

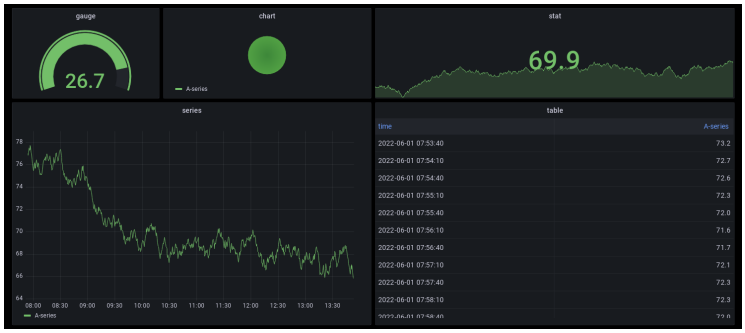
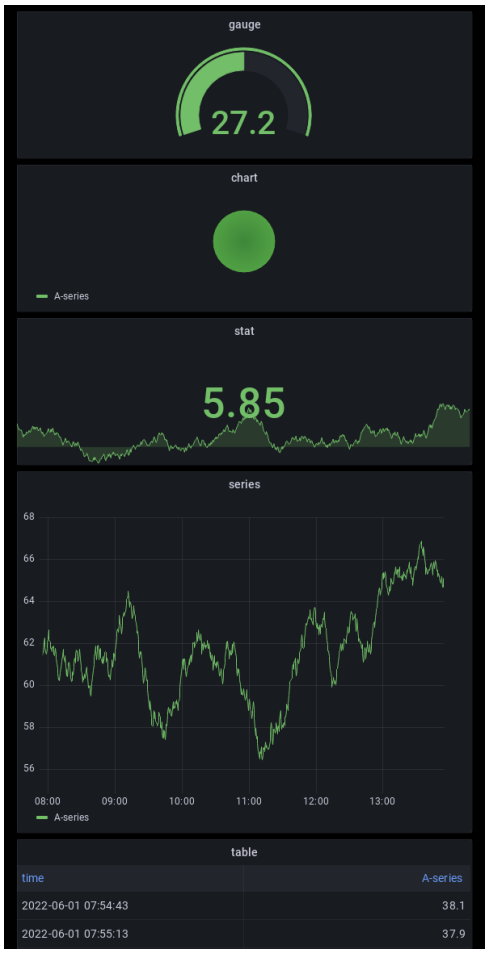
功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID。
4. 在左侧导航栏选择**高级功能 > 数据报表**。

导出报表

在**导出报表**页签下，设置以下参数导出大盘报表。



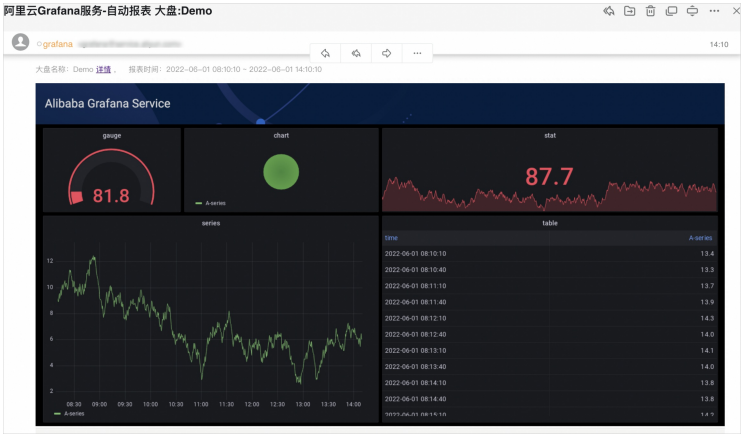
参数	说明
导出类型	目前仅支持导出图片类型。
布局	• 网格(Grid)：用于在PC端展示。  • 顺排(Simple)：用于在移动端展示。 

参数	说明
大盘地址（URL）	需要导出的大盘URL，您可以在浏览器地址栏里直接获取。 **说明** 大盘打开时间过长时，可能会导致系统放弃对该大盘进行导出。请合理配置查询参数，更多信息，请参见大盘设置。 

定时发送报表

在**自动报表**页签单击**创建自动报表**，设置大盘定时发送信息。

参数	说明
名称	定时发送任务名称。
通知渠道	目前仅支持发送至邮箱。
通知目标	邮箱地址，多个地址之间使用半角逗号（,）分隔。
导出类型	目前仅支持导出图片类型。

参数	说明
布局	• 网格(Grid)：用于在PC端展示。  • 顺排(Simple)：用于在移动端展示。 

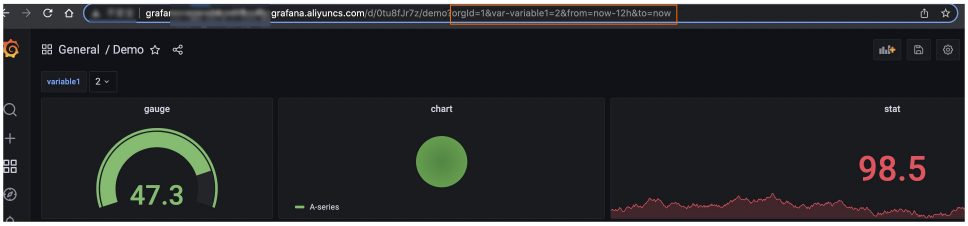
参数	说明
大盘地址（URL）	需要发送的大盘URL，您可以在浏览器地址栏里直接获取。 说明 大盘打开时间过长时，可能会导致系统放弃对该大盘进行导出。请合理配置查询参数，更多信息，请参见大盘设置。
状态	当前定时任务的状态。
发送时间	按周设置，发送时间精确到分钟。

创建完定时任务后，在**自动报表**页签可以看到任务以及运行的情况。您可以通过编辑功能关闭指定任务。

说明 一个工作区最多创建5个定时任务，对不需要的废弃任务可以进行删除释放出额度。

大盘设置

在大盘中设置的查询参数、时间，会自动体现在地址栏上，设置导出大盘URL时需要保留配置参数。



目前的大盘渲染时间为5分钟。如果当前大盘的加载时间超过5分钟，则导出大盘时系统会放弃对该大盘进行导出。请设置合理查询参数避免整个大盘打开时间超过5分钟，建议大盘打开渲染完成控制在30秒以内。

2.2.10. VPC数据源通道管理

通过在Grafana服务中安装VPC数据源通道，可以使Grafana工作区访问到VPC内未开通公网访问的数据源。本文以Grafana访问VPC内自建的Prometheus数据源为例，介绍如何通过VPC数据源通道使Grafana服务可以访问VPC内的数据源。

背景信息

VPC未开通公网访问一般存在以下几种原因：

- 安全问题：公网增加暴露被攻击的风险。
- 成本问题：开通弹性公网IP需要一定的成本。

Grafana服务的VPC数据源通道管理功能适用于不便于暴露公网的数据源或多个VPC数据源需要在同一个Grafana中展示的场景。

（可选）步骤一：在VPC内安装Prometheus数据源

如果您的VPC下已有数据源，可以跳过此步骤。

此处以安装Prometheus数据源为例，您可以根据需求在ECS内安装其他数据源。

1. 登录VPC下的ECS实例。
2. 执行以下命令在ECS实例中安装Prometheus。

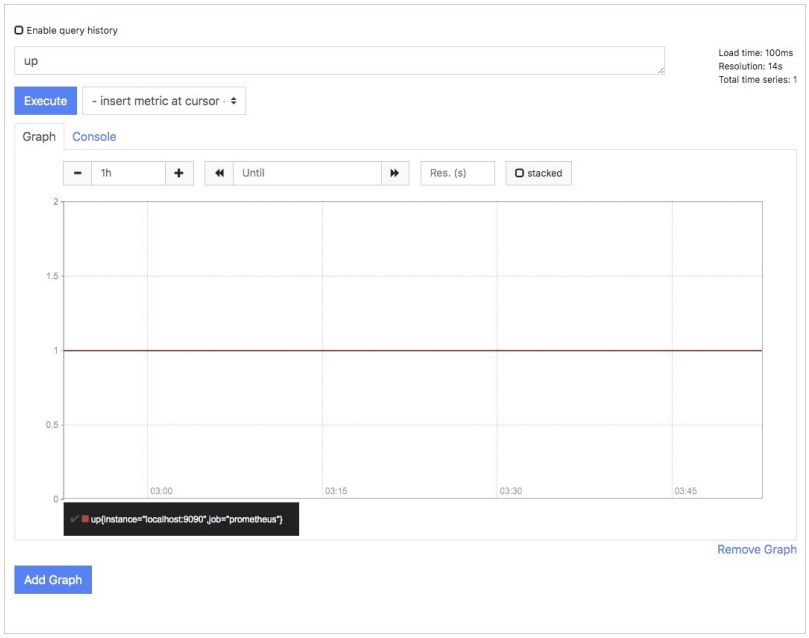
```
#下载Prometheus安装包。
wget https://github.com/prometheus/prometheus/releases/download/v2.8.1/prometheus-2.8.1
.linux-amd64.tar.gz
#解压Prometheus安装包。
tar -zxvf prometheus-2.8.1.linux-amd64.tar.gz -C /usr/local/
#重命名安装包文件夹。
cd /usr/local
mv prometheus-2.8.1.linux-amd64/ prometheus
cd prometheus/
#检查Prometheus版本。
 ./prometheus --version
#请根据实际需求修改配置prometheus.yml（如果仅测试Grafana的VPC管理功能可以跳过该配置）。
#启动Prometheus。
./prometheus &
```

3. 通过访问以下地址进入Prometheus。

```
http://[ECS公网IP]:9090/graph
```

在Prometheus中查询 `up` 指标，如果显示如下页面，表示Prometheus安装成功。

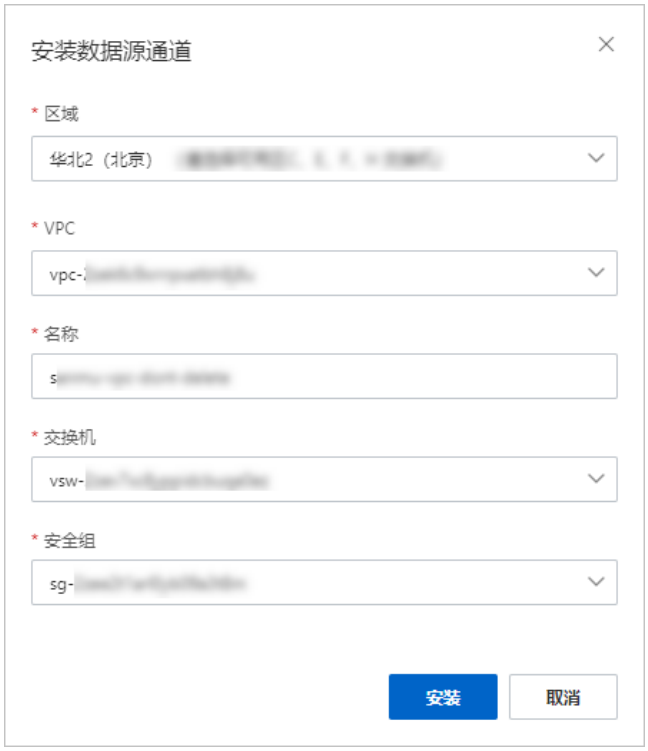
> **说明** `job="prometheus"` 的 `up` 指标是Prometheus默认对自身的监控指标。



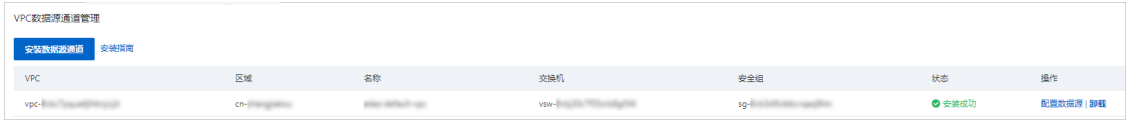
步骤二：管理VPC数据源通道

1. 登录ARMS控制台，在左侧导航栏选择**Grafana服务 > 工作区管理**。
2. 在**工作区管理**页面，单击目标工作区ID，然后在左侧导航栏单击**VPC数据源通道管理**。

3. 在**VPC数据源通道管理**页面单击**安装数据源通道**，然后在弹出的对话框输入数据源的所在地域、VPC ID、VPC名称、交换机和安全组，然后单击**安装**。



安装完成后，在**VPC数据源通道管理**页面可以查看已安装的数据源。



步骤三：在Grafana中添加ECS数据源

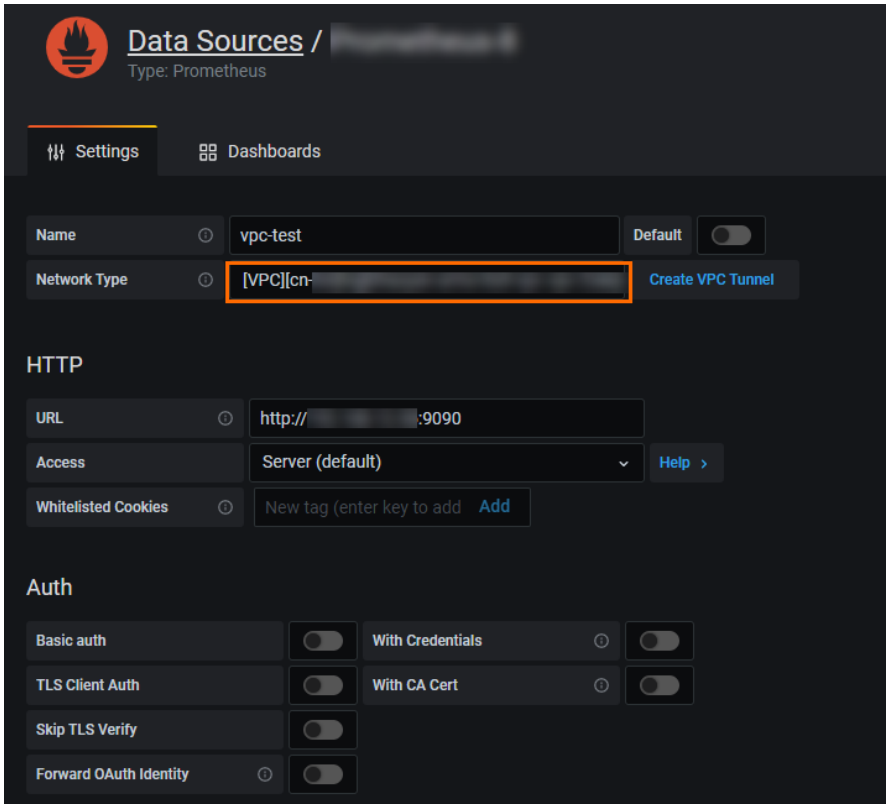
1. 在Grafana服务的**VPC数据源通道管理**页面，单击目标数据源右侧的**配置数据源**进入Grafana配置页面。
2. 在**Data Sources**页签单击**Add data source**，然后单击**Prometheus**。

> **说明** 您可以根据实际情况选择数据源类型。

3. 在Prometheus的**Settings**页面根据需求设置Prometheus参数。

   选择**Network Type**为步骤二已经创建好的VPC数据通道，URL参数格式为 `http://[ECS主私网IP]:9090` ，其他参数的含义请参见Grafana官方文档。

> **说明** 您可以在ECS的**实例详情**页面查看实例的主私网IP，更多信息请参见云服务器ECS文档。

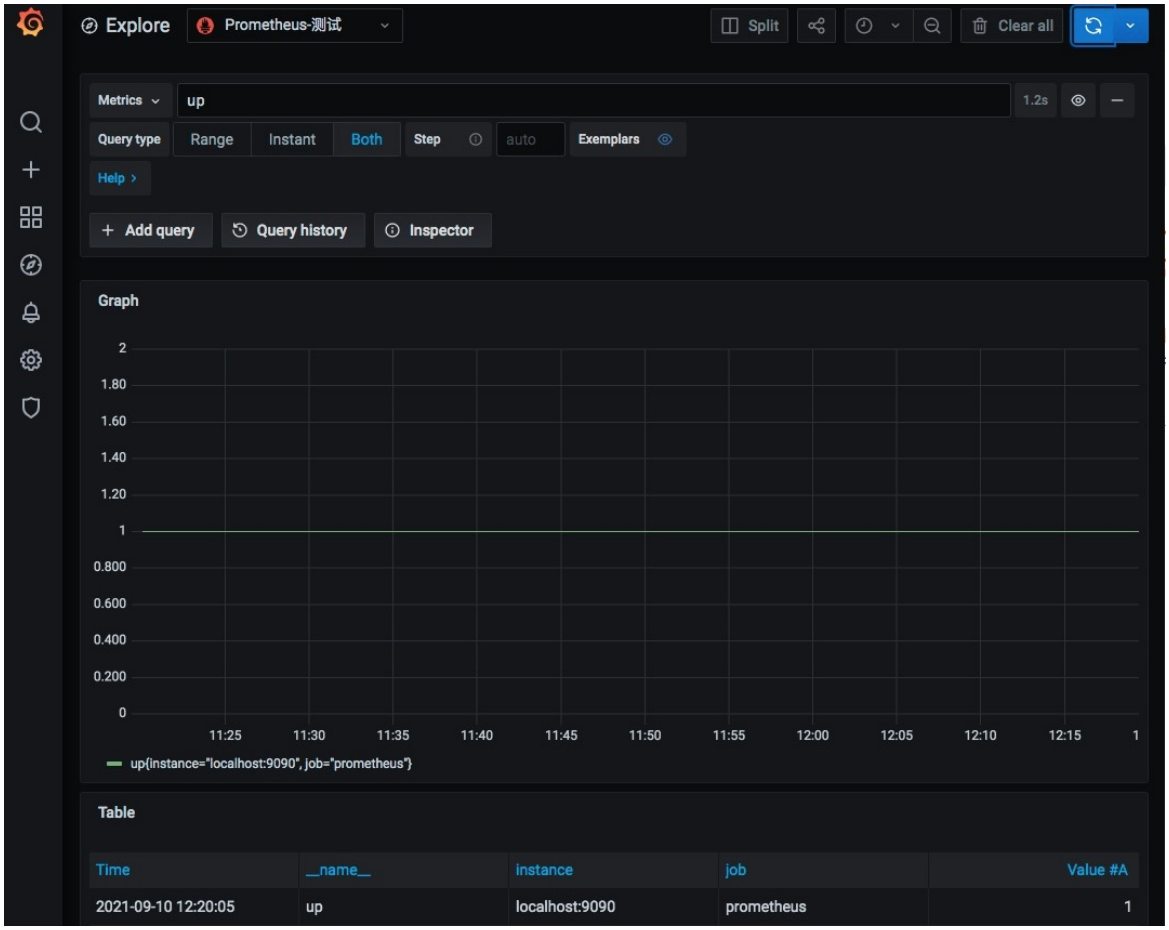


4. 单击Save & Test。
   当页面显示 `Data source is working` 时，表示Prometheus数据源已成功添加至Grafana。

结果验证

添加VPC数据源后，您可以在Grafana的Explore页面验证是否可以使用该数据源设置监控指标。

1. 在Grafana控制台左侧导航栏单击图标。
2. 在Explore页面顶部的下拉框中选择步骤三中添加的数据源。
3. 在Metrics区域输入 `up` ，然后单击Run query。
   如果Grafana中显示的Prometheus监控面板与步骤一中Prometheus页面的监控面板相同，则表示Prometheus数据源已成功接入。



2.3. 最佳实践

2.3.1. 如何组织Grafana

本文将从工作区的选型、账号登录认证和权限管理3个方面提供组织Grafana的建议。

背景信息

Grafana中存在多种结构用于组织资源和权限，当公司存在多个团队、部门或客户需要服务时，常常出现以下问题：

- 如何根据实际情况选择不同版本的Grafana。
- 部门A不应该看到部门B的信息，该如何分配账号并管理权限。
- 部门的成本归属计费。
- 不同部门对身份验证、插件等有很大不同，如何配置隔离。
- 当需要对客户展示公共内容时如何使用户免鉴权查看。

本文将从工作区的选型、账号登录认证和权限管理3个方面提供组织Grafana的建议。

工作区的选型

目前Grafana服务提供了4个版本：专家版（10账号）、专家版（30账号）、专家版（50账号）和高级版（100账号）。

功能选择

高级版比专家版多了报表、审计等功能，如果有明确的功能需求，选择对应的版本即可。具体功能对比，请参见专家版和高级版。

账号规模选择

1. 定义出一个最小粒度的人群范围。

   如果没有严格的约束，大部分场景下，一个工作区能够满足绝大部分用户的需求。但例如在以下场景下，为了实现权限或数据完全隔离，您可以以部门或者团队的维度购买工作区：

   - 部门A和部门B需要区分计算成本，为了便于区分建议各自使用一个工作区。
   - 当需要将公司的账号体系与Grafana打通时，例如使用OAuth 2.0协议，公司给不同团队都分配了一个独立的AppID，由于Grafana的自定义OAuth配置只能映射一个AppID，那么这种场景就需要一个团队使用一个工作区。
   - 当需要用于生产和日常测试时，环境要求对数据的安全、用户权限有严格区分，使用多个工作区即可根据环境做隔离。

2. 匹配对应版本。
   - 100人的部门，建议直接购买高级版（100账号）。
   - 20人的团队，可以选择专家版（30账号）。
   - 日常环境有30人要用，而生产只开放给10个人，那么只需一个专家版（30账号）加上一个专家版（10账号）。

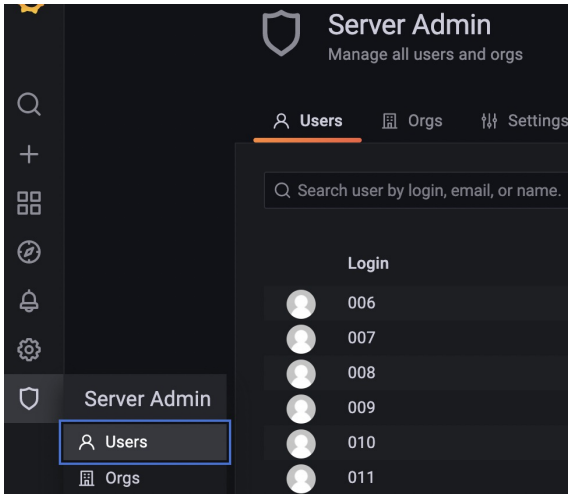
如果您还不确定使用场景，建议先购买专家版（10账号），在后续使用过程中明确需求后，可以根据实际情况进行升配或降配。

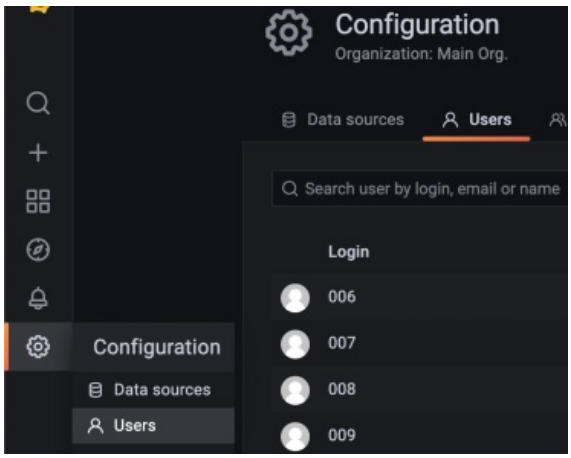
账号登录认证

官方Grafana除了自己的账号管理体系外，还支持通过其它多种认证方式实现账号的同步、登录。更多信息，请参见Grafana官方文档。

阿里云托管的Grafana服务在原生的基础上，额外集成了阿里云的登录方式。下述表格罗列了目前Grafana服务上常用的几种登录方式，一个工作区可以同时使用多种登录方式，请根据实际需求选择。

类型	场景	说明

类型	场景	说明
Admin账号的用户管理	常规的账号、密码创建	在Admin账号（最高权限）的Grafana页面可以看到管理员菜单，通过Admin账号可以直接创建账号、设置密码、赋予权限。同时也能管理通过邮件、阿里云SSO、OAuth、LDAP集成进来的账号。 

类型	场景	说明
Admin权限的用户管理	邮件邀请创建	Admin账号和Admin权限的级别不同。下图为Admin权限的Grafana页面，可以看到左侧菜单栏没有图标，因此无法直接添加账号，只能通过发送邮件让收件人通过指定链接自行创建，收件人的权限在发送邮件时设定。Admin权限和Admin账号最大区别是Admin权限管理员不知道创建的账号密码。阿里云Grafana服务有默认的SMTP配置，如果有需要可以自行配置SMTP邀请用户，更多信息，请参见使用SMTP邮箱邀请用户。 
阿里云SSO	使用阿里云账号登录	通过在Grafana控制台填写阿里云账号ID（如果是子账号则填写子账号ID），即可使用阿里云账号登录Grafana，若您已经登录阿里云则可以免登录直接进入Grafana。更多信息，请参见账号管理。
OAuth授权	企业登录系统打通	Grafana服务支持标准的OAuth协议，Grafana官方除了默认支持通过谷歌、微软登录外，还支持自定义登录，适用于需要使用公司登录系统做集成登录的场景。对于自建系统的集成，对接操作请参见OAuth统一登录，该文档以阿里云为例模拟企业的登录系统，详细介绍了对接过程。
LDAP	企业登录系统打通	目前控制台暂未提供上传LDAP文件的入口，如有需要请加入Grafana服务钉钉群（群号：34785590）进行反馈。
匿名模式	访客无需登录即可查看	部分大盘配置后需要对外展示，此时无需用户登录即可直接查看大盘，例如官方示例网站就是通过匿名模式生成的Demo展示。配置匿名模式的操作，请参见为Grafana大盘生成免登录查看的共享链接。

权限的管理

开源Grafana提供了多样的权限管理方式，这些权限管理方式已经能够满足绝大部分场景。除了Grafana官方推荐使用的文件夹（Folders）+团队（Team）的方式之外，组织（Orgs）和更严格层面的工作区都可以作为权限管理控制的方式。

三种方式对比

方式	优势	劣势
文件夹+团队（推荐）	• 灵活轻量，允许团队之间灵活共享。 • 更少的配置。 • Grafana官方后续也会针对当前方式开发更多特性。更多信息，请参见Grafana官方文档。	缺乏工作区的实际隔离。
组织	账号登录认证只需配置一次即可。	• 隔离了数据源、仪表板、文件夹和其他资源，需要自行编码实现数据同步。 • 组织之间的用户管理更加复杂，不同组织下的用户需要单独配置。 • 缺乏文件夹的灵活性以及工作区的实际隔离。
工作区	不同工作区DB、配置文件都是独立的，实现真正的隔离。	配置无法共享，不同工作区之间的数据源、仪表板、文件夹和其他资源同步，需要自行编码实现。

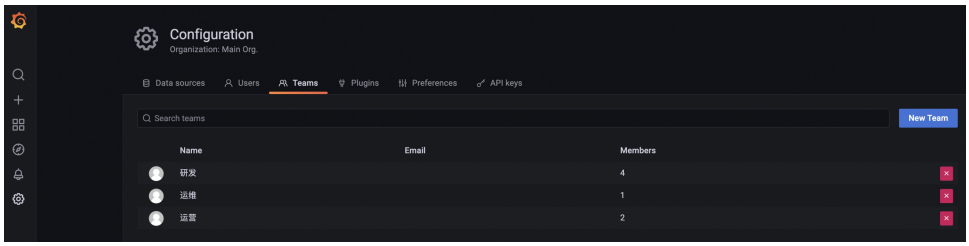
文件夹+团队方式的最佳实践

以某公司一个线上团队为例：

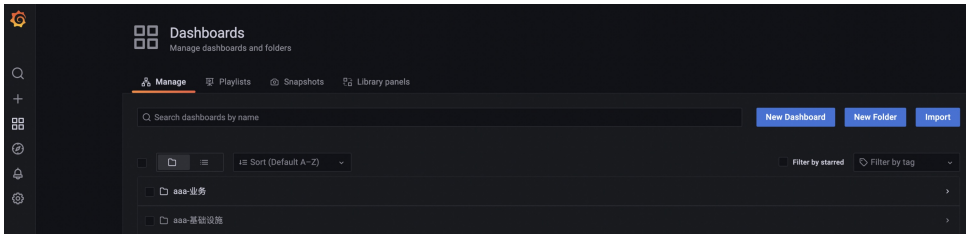
- 团队维度划分了研发、运维和运营，文件夹划分了业务和基础设施。
- 业务文件夹下，存放了基于应用运行过程中采集配置的业务大盘，由研发配置，运营查看。
- 基础设施下，存放了阿里云上的ECS、RDS等基础设施的监控大盘，由运维配置，研发查看。

建议配置如下：

1. 在Grafana的Configuration > Teams页签下创建研发、运维和运营团队并添加对应用户。具体操作，请参见Grafana官方文档。

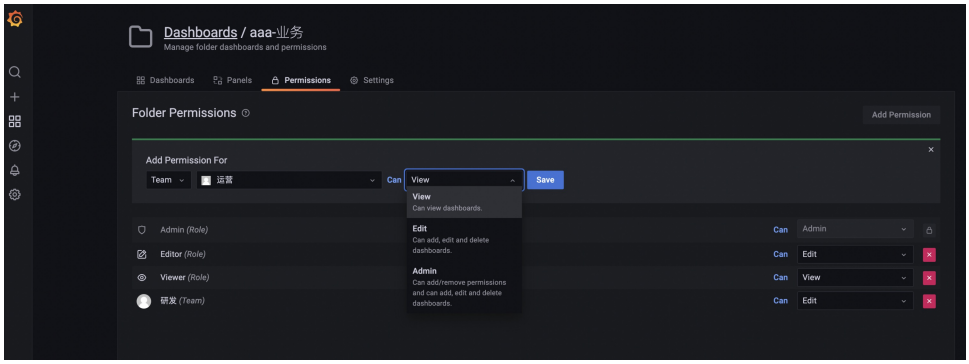


2. 在Create > Folder页签下创建业务和基础设施文件夹。具体操作，请参见Grafana官方文档。



3. 配置文件夹权限。

   进入文件夹，在Permissions页签下增加权限，配置对应团队在当前文件夹下的权限。



配置完成后，只有View权限的团队成员登录Grafana时，只有查看权限。

> **说明** 若用户本身是Admin权限，所在团队只有View权限，在多权限叠加的情况下高等级权限优先，即用户仍是Admin权限。

2.3.2. OAuth统一登录

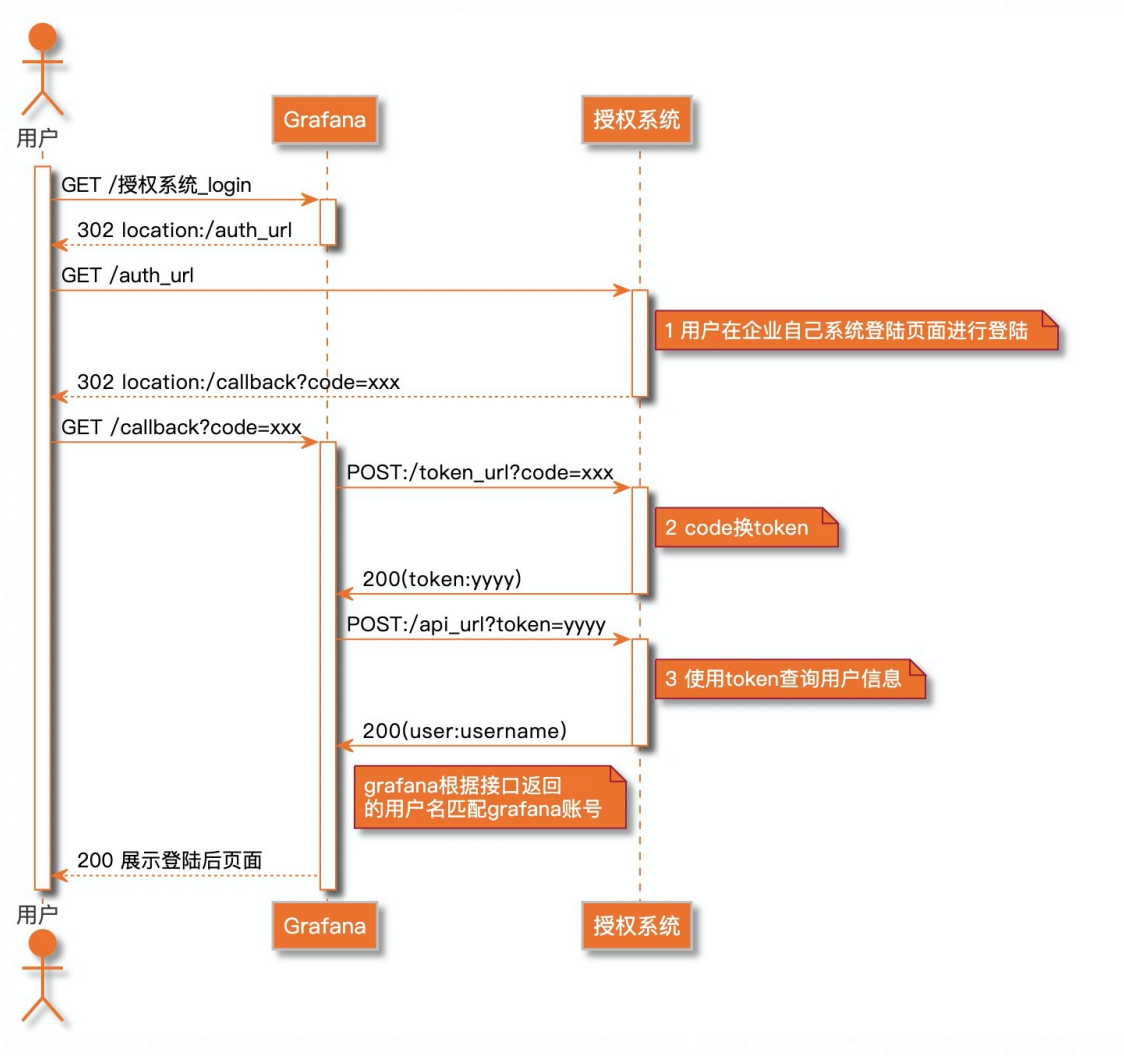
Grafana服务支持使用OAuth 2.0协议进行用户认证和应用授权。本文以阿里云系统模拟第三方应用为例介绍对接Grafana实现第三方应用登录的操作。

背景信息

OAuth（Open Authorization，开放授权）是一种开放协议，支持以简单和标准的方法为Web、移动或桌面应用程序进行安全授权，被授权的应用不需要使用用户名和密码即可访问受保护的信息。更多信息，请参见OAuth官方文档。

用户自建系统在授权的前提下可以访问托管Grafana存储的各种信息。此处以阿里云系统授权登录托管Grafana为例，为您演示OAuth接入，其他产品账号授权的操作，请参见Grafana官方文档。

基本流程



接下来将为您演示如何使用阿里云系统模拟上图的授权系统。下述步骤涉及的配置仅供参考，具体的系统配置属性在符合OAuth2.0标准下，以您的实际设置为准。

步骤一：创建应用

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**OAuth应用管理**。
3. 在**企业应用**页签，单击**创建应用**。
4. 在**创建应用**面板，设置应用参数。
   i. 输入**应用名称**和**显示名称**。
   ii. 选择**应用类型**。
   - **WebApp**：指基于浏览器交互的网络应用。
   - **NativeApp**：指操作系统中运行的本地应用，主要为运行在桌面操作系统或移动操作系统中的应用。
   - **ServerApp**：指直接访问阿里云服务，而无需依赖用户登录的应用，目前仅支持基于SCIM协议的用户同步应用。示例请参见通过SCIM协议将企业内部账号同步到阿里云RAM。

   iii. 设置**访问令牌有效期**时长。

   访问令牌有效期范围：900秒（15分钟）~10,800秒（3小时）。默认值为3,600秒。

iv. 对于WebApp和NativeApp，设置**刷新令牌有效期**和**回调地址**。

- 刷新令牌有效期范围：7,200秒（2小时）~31,536,000秒（1年）。默认值为2,592,000秒。
- 回调地址为Grafana工作区的连接地址加 `/login/generic_oauth` 后缀，例如 `http://[Grafana连接地址:端口号]/login/generic_oauth` 。您可以在**工作区信息**页面查看Grafana工作区的连接地址和端口号，更多信息，请参见工作区管理。

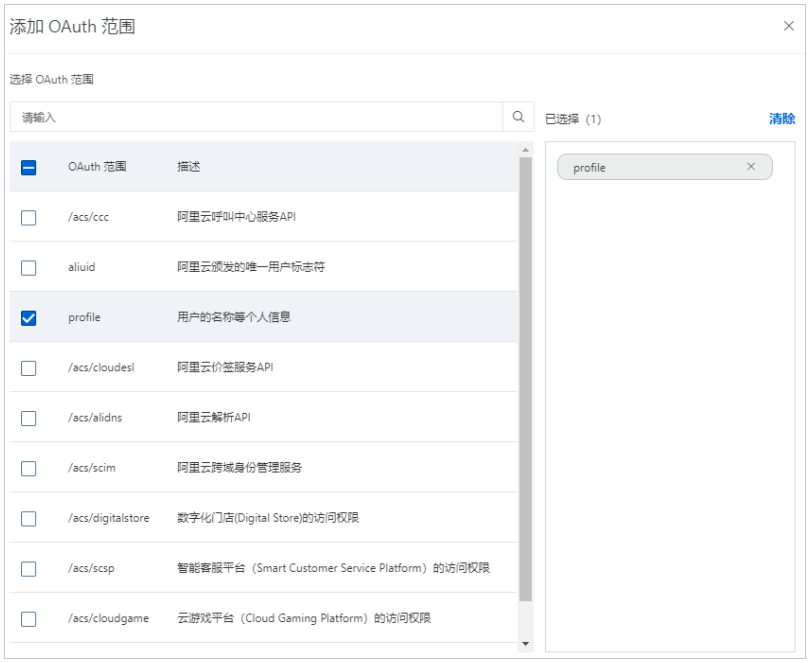
5. 单击**保存**。

步骤二：添加范围

1. 在**企业应用**页签，单击目标应用名称。

> **说明** 在应用详情页面的**基本信息**区域可以查看应用ID，应用ID在步骤四设置参数时需要使用。

2. 在**应用OAuth范围**页签，单击**添加OAuth范围**。
3. 在**添加OAuth范围**面板，选择添加profile范围。



4. 单击**确定**。

步骤三：创建密钥

1. 在目标应用详情页面，单击**应用密钥**页签，然后单击**创建密钥**。
2. 在**创建应用密钥**对话框，查看并复制创建成功的应用密钥，然后单击**关闭**。

> **注意**
> - 应用密钥内容仅在创建时可见，不支持查询，请及时保存。
> - 每个应用最多允许创建2个应用密钥。

步骤四：修改工作区参数

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**参数设置**。
5. 在左侧参数列表选择auth.generic_oauth，然后单击**修改参数**。
6. 参考以下配置，修改参数的运行参数，然后单击**保存并生效**。

```
name = Alibaba
enabled = true
allow_sign_up = true
client_id = {应用ID}       //您可以在RAM控制台的应用基本信息页面查看应用ID。
client_secret = {步骤三中创建的应用密钥}
scopes = openid profile
auth_url = https://signin.aliyun.com/oauth2/v1/auth
token_url = https://oauth.aliyun.com/v1/token
api_url = https://oauth.aliyun.com/v1/userinfo
email_attribute_path=login_name
```

7. 在左侧参数列表选择server，然后单击**修改参数**。
8. 参考以下配置，修改参数的运行参数，然后单击**保存并生效**。

```
root_url = http://[Grafana连接地址:端口号]
```

> **说明** 您可以在**工作区信息**页面查看Grafana工作区的连接地址和端口号。

2.3.3. 添加并使用云监控数据源

ARMS的Grafana服务默认安装云监控数据源插件。通过此插件，可实现云监控数据同步并实时呈现在Grafana大盘中。您无需手动获取或迁移数据。本文介绍如何通过云监控数据源插件同步云监控数据，并使用云监控数据源创建大盘面板。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。

配置数据源

1. 在Grafana左侧导航栏选择  > **Data sources**。
2. 在**Data Sources**页签单击**Add data source**。
3. 在页面最下方单击**CMS Grafana Service**。

4. 在CMS Grafana Service的Settings页面设置以下参数。

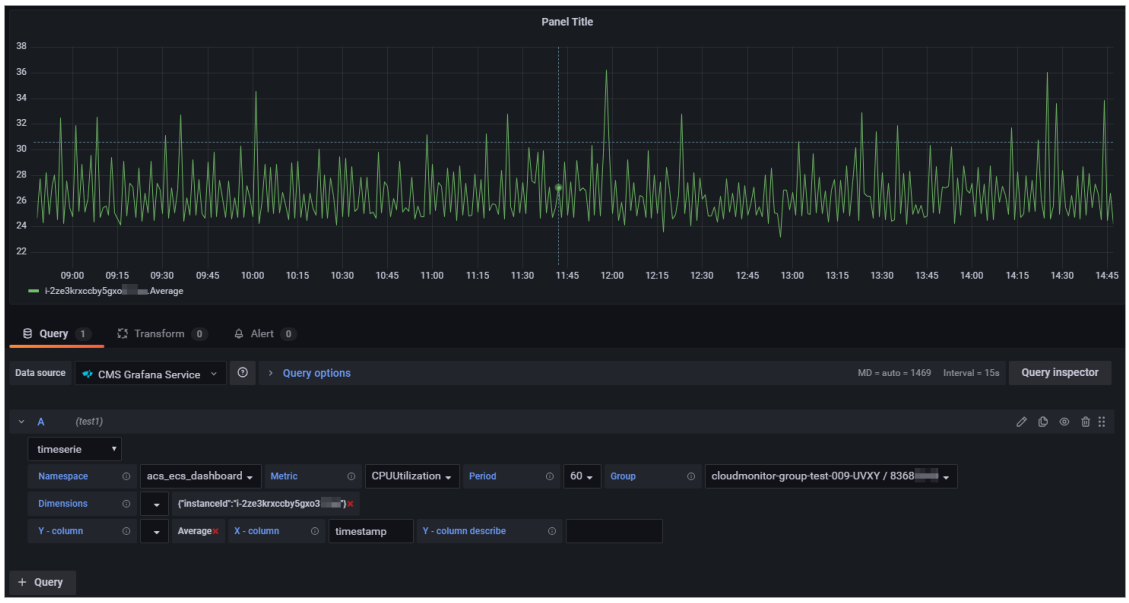
参数	说明
Name	数据源名称。您可以使用默认名称CMS Grafana Service。
Aliyun UserId	阿里云账号ID。您可以将鼠标悬浮于阿里云控制台右上角的头像上查看当前账号的账号ID。
AccessKeyId	阿里云账号或RAM用户的AccessKey ID。关于如何获取AccessKey ID，请参见获取AccessKey。 说明 RAM用户必须由当前阿里云账号创建，且具备读取云监控数据的权限。
AccessKey	阿里云账号或RAM用户的AccessKey Secret。关于如何获取AccessKey Secret，请参见获取AccessKey。 说明 RAM用户必须由当前阿里云账号创建，且具备读取云监控数据的权限。

5. 单击Save & Test。
   当页面显示 `Data source is working` 时，表示云监控数据已成功添加至Grafana。

创建大盘面板

添加云监控数据源后，您可以在创建面板时使用已添加的云监控数据源。

1. 在Grafana控制台左侧导航栏选择+ > Dashboard。
2. 在New dashboard页面单击Add an empty panel。
3. 在Edit Panel页面的Query区域的下拉列表中选择云监控数据源，并设置目标云服务的监控指标。



目标云服务的主要参数说明如下表所示。

参数	说明
Namespace	上报监控数据的数据命名空间。命名方式：`acs_云服务名称`。 关于云服务的命名空间，请参见云服务监控项。
Metric	上报监控数据的监控项名称。 关于云服务的监控项名称，请参见云服务监控项。
Period	上报监控数据的时间间隔。单位：秒。 关于云服务的时间间隔，请参见云服务监控项。
Group	上报监控数据的**Metric**对应的应用分组名称和应用分组ID。
Dimensions	上报监控数据的维度Map，用于查询指定资源的监控数据。 格式为key-value键值对形式的集合，例如：`instanceId:i-2ze2d6j5uhg20x47****`，可以选择多个。 关于云服务的维度，请参见云服务监控项。
Y-column	上报监控数据的统计方法，例如：Average、Maximum、Minimum、Sum等。 关于云服务的统计方法，请参见云服务监控项。

4. 在右侧设置监控图表的名称、类型、展示样式等。
5. 单击右上角的**Apply**。
   大盘面板创建成功。
6. 单击右上角的  图标，设置监控大盘的名称和归属目录。
7. 单击**Save**。
   大盘创建成功。

查看监控数据

1. 在左侧导航栏，选择  > **Manage**。
2. 在**Manage**页签，单击目标目录下的监控大盘。
   查看目标大盘上的所有监控图表。

2.3.4. 添加并使用日志服务SLS数据源

ARMS的Grafana服务默认安装日志服务SLS数据源插件。通过此插件，可实现SLS数据同步并实时呈现在Grafana大盘中。您无需手动获取或迁移数据。本文介绍如何通过SLS数据源插件同步SLS数据，并使用SLS数据源创建大盘面板。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**，进入**工作区信息**页面。
4. 在左侧导航栏单击**云服务管理**。
5. 在**云服务管理**页面的**SLS日志服务**区域，单击**配置管理**进入Grafana数据源配置页面。

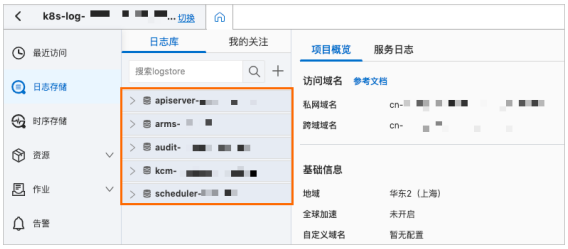
> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。

配置数据源

1. 在Grafana数据源配置页面，单击**Add data source**。
2. 在**Add data source**页面的**Others**区域，单击**log-service-datasource**。

> **说明** 您也可以通过在页面上方的搜索框中输入*log-service-datasource*来快速找到该插件，支持模糊搜索。

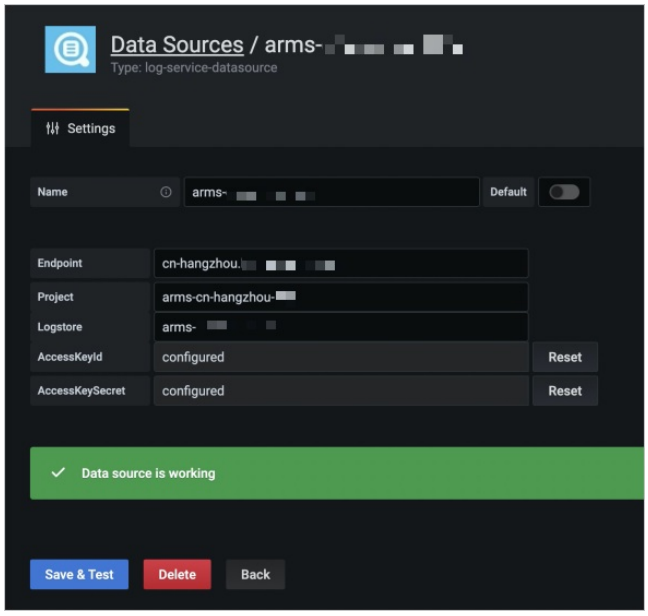
3. 在log-service-datasource的配置页面，完成以下参数的配置。

参数	说明
Name	数据源名称，可自行定义。
Endpoint	根据使用的数据源地域填写。详细地域信息，请参见SLS服务入口。
Project	需进行数据同步的Project名称，在SLS控制台的**Project列表**区域获取。 
Logstore	目标Project中需进行数据同步的日志库名称，从SLS控制台进入目标Project空间后获取。 

参数	说明
AccessKeyId	获取方式： i. 在SLS控制台首页，将鼠标悬浮在页面右上角的账号头像上，然后在出现的对话框中单击**AccessKey管理**。  ii. 关闭页面弹出的提示框后，在**AccessKey**页面单击**创建AccessKey**。 iii. 在**手机验证**对话框中填入校验码，然后单击**确定**。 iv. 在**创建AccessKey**对话框中，复制并记录下生成的AccessKey ID和AccessKey Secret。 **注意** 请及时保存创建的AccessKey ID和AccessKey Secret的信息，对话框关闭后将无法再次获取相关信息。
AccessKeySecret	

4. 单击**Save & Test**。

   返回如下页面，表明配置成功。

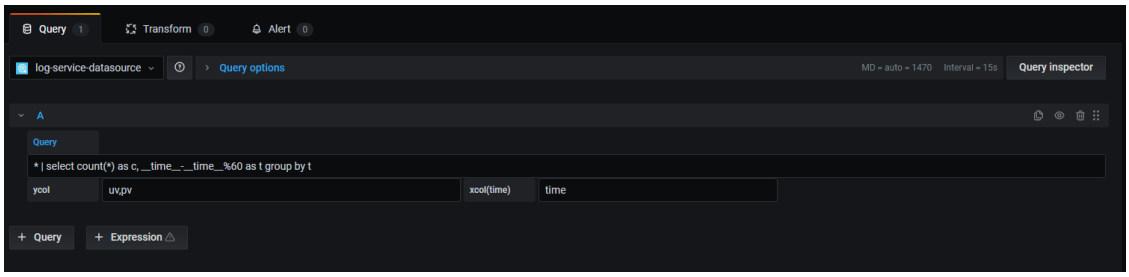


创建大盘面板

说明 此处以展示PV&UV的图表（Graph）为例，其他图标的添加步骤，请参见添加仪表盘。

1. 在Grafana控制台左侧导航栏选择**+ > Dashboard**。

2. 在New dashboard页面单击Add an empty panel。
3. 在Edit Panel页面的Query区域的下拉列表中选择log-service-datasource数据源，并完成如下配置。



参数	说明
Query	查询和分析语句示例如下： `*|select count(*) as c, __time__-__time__%60 as t group by t` **说明** 更多查询语句，请参见对接Grafana。
ycol	配置为uv,pv。
xcol(time)	配置为time。

4. 在右侧设置监控图表的名称、类型、展示样式等。
5. 单击右上角的Apply。

   大盘面板创建成功。
6. 单击右上角的  图标，设置监控大盘的名称和归属目录。
7. 单击Save。

   大盘创建成功。

查看监控数据

1. 在左侧导航栏，选择  > Manage。
2. 在Manage页签，单击目标目录下的监控大盘。

   查看目标大盘上的所有监控图表。

2.3.5. 添加并使用Lindorm数据源

ARMS的Grafana服务默认安装Alibaba Cloud Lindorm数据源插件。通过此插件，可实现Lindorm数据同步并实时呈现在Grafana大盘中。您无需手动获取或迁移数据。本文介绍如何通过Lindorm数据源插件同步Lindorm数据，并使用Lindorm数据源创建大盘面板。

背景信息

Lindorm时序引擎是一款高性能、低成本、稳定可靠的在线时序数据库引擎服务，提供高效读写、高压缩比

存储、时序数据聚合计算等能力。更多信息，请参见引擎简介。

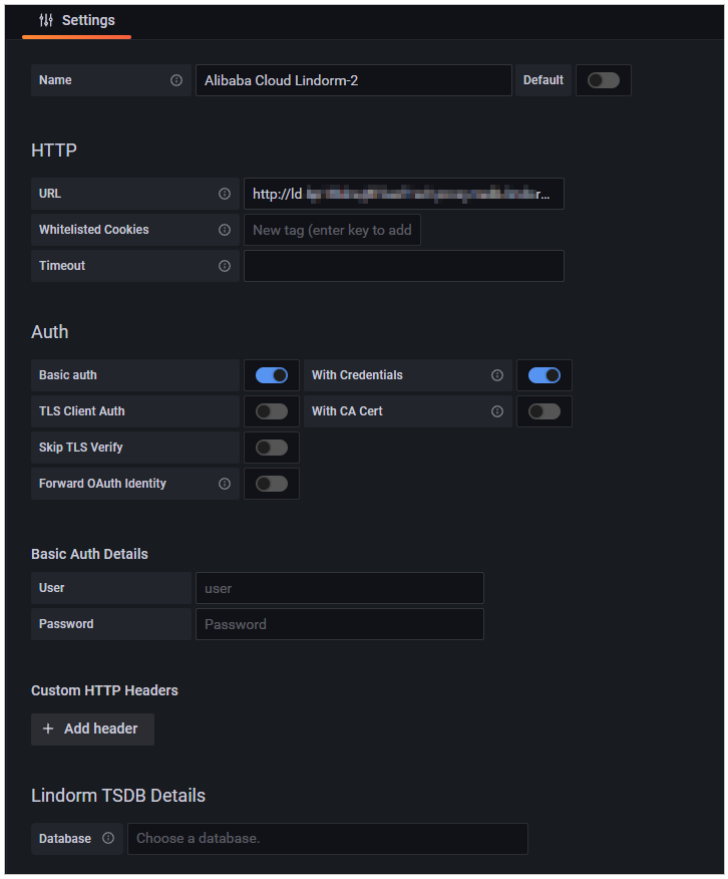
功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**云服务管理**。
5. 在**云服务管理**页面的Lindorm云原生多模数据库区域，单击**配置管理**进入Grafana配置页面。

> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。

配置数据源

1. 在Grafana配置页面的**Data Sources**页签单击**Add data source**。
2. 在页面最下方单击**Alibaba Cloud Lindorm**。
3. 在**Settings**页面设置以下参数。



配置项	参数	描述
Name		数据源名称，可自定义。

配置项	参数	描述
HTTP	URL	Lindorm时序引擎的连接地址，获取方法请参见操作步骤。
Auth	Basic auth	如果需要使用鉴权认证请打开Basic auth。
	With Credentials	如果需要使用鉴权认证请打开With Credentials。
Basic Auth Details	User	如果打开Basic auth需要填写Lindorm实例的用户名。
	Password	如果打开Basic auth需要填写Lindorm实例的密码。
Lindorm TSDB Details	Database	填写需要访问的Lindorm实例中的数据库。

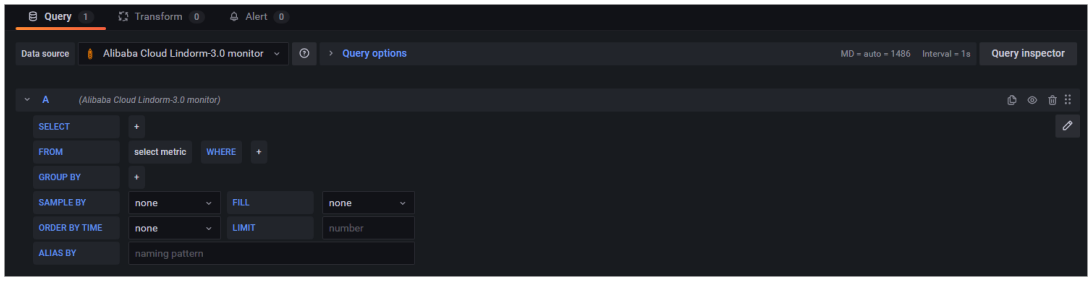
4. 单击Save & Test。
   当页面显示 `Data source is working` 时，表示Lindorm数据已成功添加至Grafana。

创建大盘面板

添加Lindorm数据源后，您可以在创建面板时使用已添加的Lindorm数据源。

1. 在Grafana控制台左侧导航栏选择+ > Dashboard。
2. 在New dashboard页面单击Add an empty panel。
3. 在Edit Panel页面的Query区域的下拉列表中选择Lindorm数据源，并设置监控指标。
   i. 在Data source列表中选择目标数据源名称。
   ii. TSQL查询操作有两种方式，包括使用编辑框查询和使用TSQL语句查询。

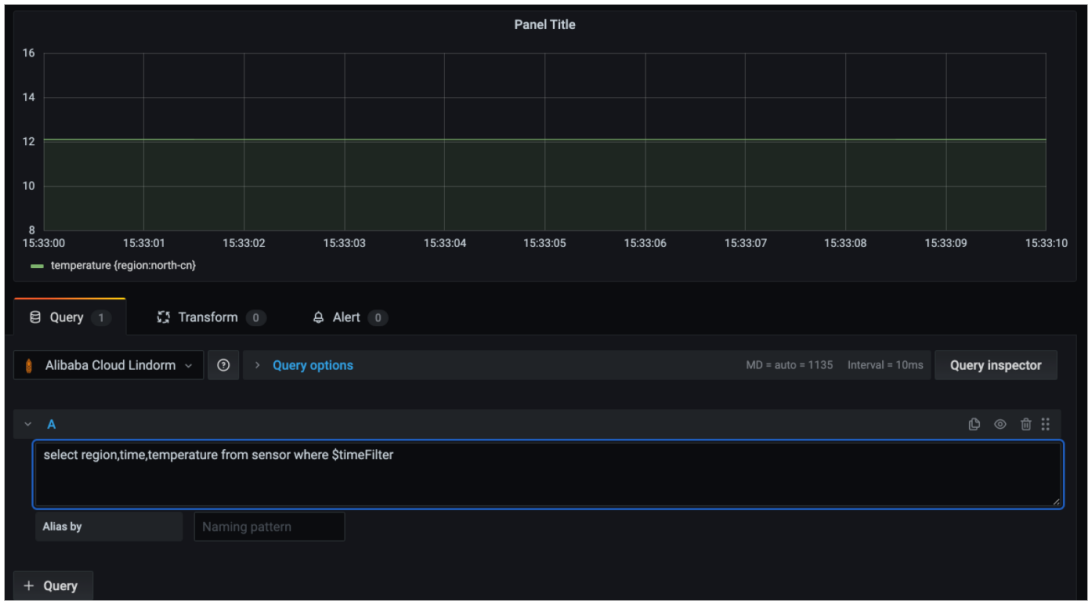
- 使用编辑框查询：在A区域下的选择框选择需要查询的数据，可以完成简单的查询操作，关键字说明如下表。



关键字	说明
SELECT	选择需要查询的字段名。
FROM	选择需要查询的表名。
WHERE	添加查询条件。
GROUP BY	添加聚合条件。
SAMPLE BY	选择降采样时间间隔，具体请参见降采样查询。
FILL	选择填充策略。
ORDER BY TIME	选择排列顺序。
LIMIT	输入查询返回最多的数据数量。
ALIAS BY	重命名时间线标签。

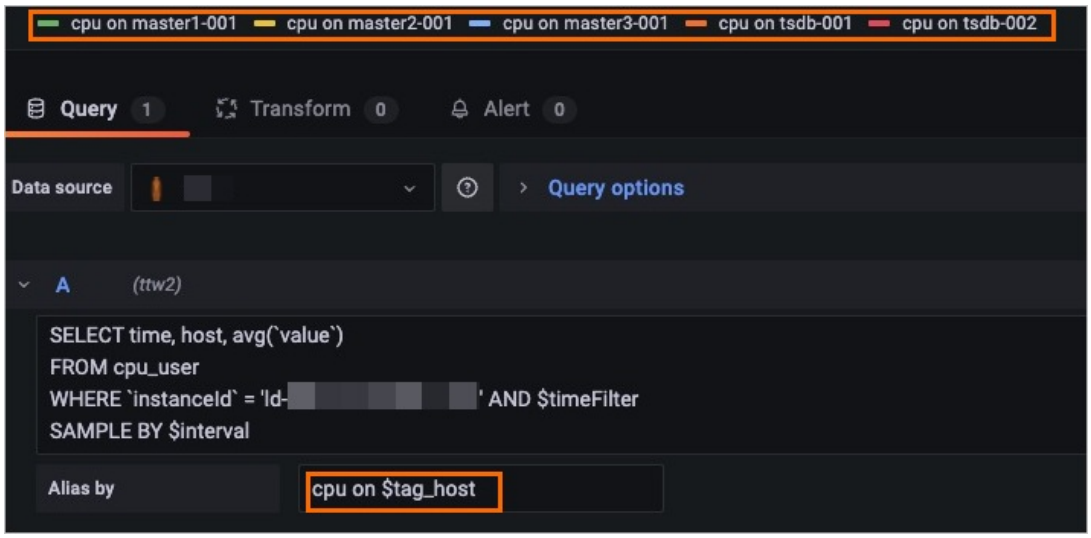
- 使用TSQL语句查询：单击A区域右上角的，可以通过输入TSQL语句完成复杂的查询操作（例如嵌套查询），数据查询结果如下图。TSQL语句字段说明如下表。

```
SELECT region,time,temperature FROM sensor WHERE $timeFilter
```



> **说明** TSQL语句使用请参见SELECT语法。
>
> - `$timeFilter` 表示时间条件，会自动替换为页面中选择的时间范围，定义为 `time >=xxx and time<=xxx` 。
> - `time` 为必选项，否则不会出现分析结果图。
> - SELECT语句中通过tag方式对不同时间线进行分组聚合。

通过Alias by重命名时间线标签，例如使用 `$tag_host` 进行区分时间线，如下图所示：



iii. TSQL语句中的 `$interval` 表示降采样时间间隔，语句示例如下：

```
SELECT region,time,avg(temperature) FROM sensor WHERE $timeFilter SAMPLE BY $interv
al
```

> **说明** 单击Query options，通过Min interval和Max data points参数来设置Interval参数大小。

4. 在右侧设置监控图表的名称、类型、展示样式等。
5. 单击右上角的**Apply**。

   大盘面板创建成功。
6. 单击右上角的  图标，设置监控大盘的名称和归属目录。
7. 单击**Save**。

   大盘创建成功。

查看监控数据

1. 在左侧导航栏，选择  > **Manage**。
2. 在**Manage**页签，单击目标目录下的监控大盘。

   查看目标大盘上的所有监控图表。

2.3.6. 添加并使用Tablestore数据源

Grafana服务默认已集成阿里云表格存储（Tablestore）。通过Tablestore插件，可以实现Tablestore数据同步并实时呈现在Grafana大盘中。本文介绍如何在Grafana中同步Tablestore数据，并使用Tablestore数据源创建大盘面板。

背景信息

表格存储（Tablestore）是阿里云自研的多模型结构化数据存储，提供大量结构化数据存储以及快速的查询和分析服务。表格存储的分布式存储和强大的索引引擎能够支持PB级存储、千万TPS以及毫秒级延迟的服务能力。更多信息，请参见什么是表格存储。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

   > **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。
4. 在Grafana左侧导航栏选择  > **Data sources**。
5. 在**Data Sources**页签单击**Add data source**。
6. 通过页面顶部文本框搜索*aliyun-tablestore-grafana-datasource*，然后单击**aliyun-tablestore-grafana-datasource**。
7. 在**Settings**页面设置以下参数。

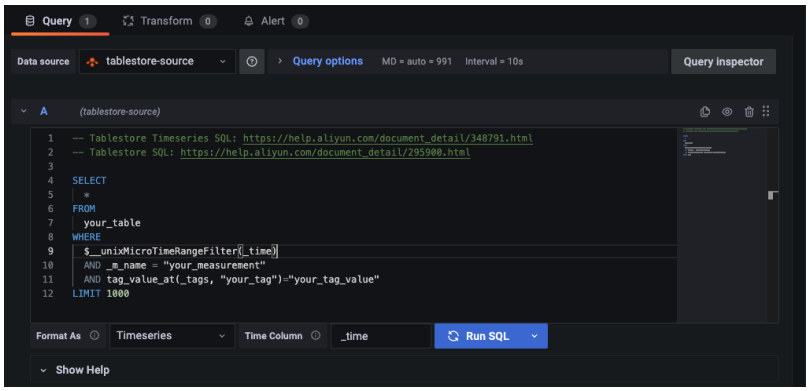
参数	说明
Name	数据源名称，可自定义。

参数	说明
Endpoint	Tablestore实例的服务地址。获取方式，请参见获取服务地址。
Instance	Tablestore实例名。
AccessId	用于访问Tablestore的阿里云账号的AccessKey ID。获取方式，请参见获取AccessKey。
AccessKey	用于访问Tablestore的阿里云账号的AccessKey Secret。获取方式，请参见获取AccessKey。

8. 单击**Save & Test**。
   当页面显示 `Data source is working` 时，表示Tablestore数据已成功添加至Grafana。

创建大盘面板

1. 在Grafana控制台左侧导航栏选择**+ > Dashboard**。
2. 在**New dashboard**页面单击**Add an empty panel**。
3. 在**Edit Panel**页面的**Query**区域的下拉列表中选择Tablestore数据源，并完成如下配置。



参数	示例

参数	示例

Query	SQL查询语句，更多信息，请参见Tablestore文档。
	SQL查询示例：
	`SELECT`
	`  *`
	`FROM`
	`  your_table`
	`WHERE`
	`  $__unixMicroTimeRangeFilter(_time)`
	`  AND _m_name = "your_measurement"`
	`  AND tag_value_at(_tags, "your_tag")="your_tag_value"`
	`LIMIT 1000`
	说明
	○ 在WHERE子句中通过预定义宏过滤时间范围，即例子中的 `$__unixMicroTimeRangeFilter` 。更多的时间宏函数，请参见使用SQL查询时序数据。
	○ 如以时序图形式展示，需要返回以数字时间戳形式表示的时间列，并配置时间列的列名。

Format As	结果处理形式，包括三种类型： ○ Timeseries：普通时序图。 ○ FlowGraph：多维图表展示。 ○ Table：普通表格形式。
Time Column	返回数据中的时间列的列名，时间列会作为时序图的横坐标。
Aggregation Column	当Fortmat As为FlowGraph时需设置此参数，用于将同一时间点的多行单列数据转换为同一时间点的单行多列数据，特别适用于将Tablestore时序SQL产生的单值模型数据转换为多值模型数据。格式为 `<数据点名称列>#:#<数值列>` ，例如： `"_field_name#:#_double_value"` 。

4. 单击**Run SQL**，执行SQL查看数据和调试。
5. 在右侧设置监控图表的名称、类型、展示样式等。
6. 单击右上角的**Apply**。

   大盘面板创建成功。
7. 单击右上角的  图标，设置监控大盘的名称和归属目录。
8. 单击**Save**。

大盘创建成功。

查看监控数据

1. 在左侧导航栏，选择 > Manage。
2. 在Manage页签，单击目标目录下的监控大盘。

   查看目标大盘上的所有监控图表。

2.3.7. 通过公网地址添加并使用阿里云Elasticsearch数据源

Grafana服务已集成阿里云检索分析服务Elasticsearch版，通过Elasticsearch插件，可以实现Elasticsearch数据同步并实时呈现在Grafana大盘中。本文介绍如何通过公网地址将Elasticsearch数据添加至Grafana，并使用Elasticsearch数据源创建大盘面板。

背景信息

检索分析服务Elasticsearch版是基于开源Elasticsearch构建的全托管云服务，在100%兼容开源功能的同时，支持开箱即用、按需付费。不仅提供云上开箱即用的Elasticsearch、Logstash、Kibana、Beats在内的Elastic Stack生态组件，还与Elastic官方合作提供免费X-Pack（白金版高级特性）商业插件，集成了安全、SQL、机器学习、告警、监控等高级特性，被广泛应用于实时日志分析处理、信息检索、以及数据的多维查询和统计分析等场景。更多信息，请参见什么是阿里云Elasticsearch。

步骤一：配置公网白名单

在阿里云Elasticsearch控制台上将Grafana连接IP添加为白名单。

1. 登录阿里云Elasticsearch控制台。
2. 在左侧导航栏，单击**Elasticsearch实例**。
3. 进入目标实例。
   i. 在顶部菜单栏处，选择资源组和地域。
   ii. 在左侧导航栏，单击**Elasticsearch实例**，然后在**Elasticsearch实例**中单击目标实例ID。
4. 在左侧导航栏，选择**配置与管理 > 安全配置**。
5. 在**集群网络设置**区域，单击公网地址访问白名单右侧的**修改**，配置IP白名单相关信息。

   > **说明** 配置**公网地址访问白名单**时，请确认已打开**公网地址**开关（默认关闭），再进行如下操作。

   i. 在**修改公网访问白名单**面板，单击default白名单右侧的**配置**。
   ii. 在**新增IP白名单分组**对话框的**白名单内IP地址**区域输入Grafana的连接IP。

   > **说明** 您可以在Grafana服务控制台的工作区信息页面获取Grafana的连接IP，具体操作，请参见工作区信息。

   iii. 单击**确认**。

步骤二：添加数据源

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。

4. 在Grafana左侧导航栏选择  > **Data sources**。
5. 在**Data Sources**页签单击**Add data source**。
6. 通过页面顶部文本框搜索Elasticsearch，然后单击**Elasticsearch**。
7. 在**Settings**页面设置以下参数。

配置项	参数	描述	示例
Name		数据源名称，可自定义。	Elasticsearch数据源
HTTP	URL	Elasticsearch的连接地址，格式为`http://{Elasticsearch地址}:9200`。 **说明** • 您可以在阿里云Elasticsearch控制台的实例基本信息页面获取Elasticsearch的公网地址。 • 如果需要使用HTTPS协议，请先在阿里云Elasticsearch控制台上开启HTTPS协议。 具体操作，请参见查看实例的基本信息。	`http://es-cn-xxxxxxxxx.public.elasticsearch.aliyuncs.com:9200`
Auth	Basic auth	打开Basic auth开关，然后填写**Basic Auth Details**。	无
Basic Auth Details	User	填写Elasticsearch实例的用户名。	elastic
	Password	填写Elasticsearch实例的访问密码。 **说明** 如果您忘记了Elasticsearch实例的访问密码，您可以在阿里云Elasticsearch控制台实例的**配置与管理 > 安全配置**页面重置Elasticsearch实例访问密码。	无

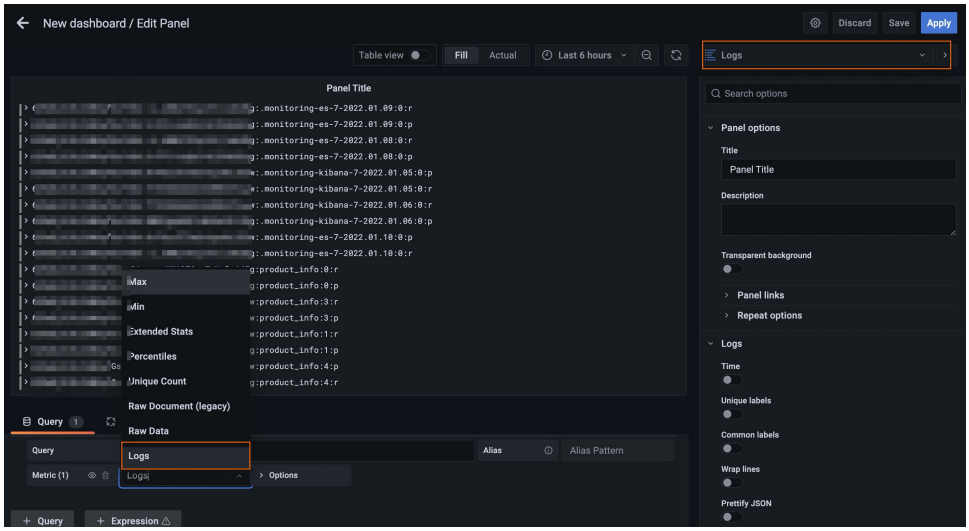
配置项	参数	描述	示例
Elasticsearch Detail	Index name	填写Elasticsearch实例中创建的Index名称。 **说明** ○ 如果您的ES实例中暂未创建Index，您可以暂时填写ES自监控的Index，用于检测Grafana是否可以成功访问您的ES实例。ES自监控的Index名称为.monitoring-es-7-2022.01.11，其中名称后的日期请填写近两天的，否则可能没有数据。同时确保该日期是ES实例创建以后的日期。 ○ 更多信息，请参见Grafana官方文档。	.monitoring-es-7-2022.01.11
	Time field name	填写Index中对应的时间戳field。 **说明** 如果您使用的是Index name参数说明中提到的ES自监控的Index，对应的Time field为timestamp。	timestamp
	Version	填写Elasticsearch版本。 **说明** Elasticsearch版本需要和阿里云Elasticsearch控制台实例基本信息页面展示的版本一致。	7.10+

8. 单击**Save & Test**。
   当页面显示 `Index OK. Time field name OK.` 时，表示Elasticsearch数据已成功添加至Grafana。更多配置信息，请参见Grafana官方文档。

步骤三：创建大盘面板

添加Elasticsearch数据源后，您可以在创建面板时使用已添加的Elasticsearch数据源。

1. 在Grafana控制台左侧导航栏选择**+ > Dashboard**。
2. 在**New dashboard**页面单击**Add an empty panel**。
3. 在**Edit Panel**页面的**Query**区域的下拉列表中选择Elasticsearch数据源，并设置监控指标。
   例如，如果您想配置一个浏览日志列表和明细的面板，您可以选择Metric为*Logs*，并在右上角的Visualization中选择*Logs*。



4. 在右侧设置监控图表的名称、类型、展示样式等。
5. 单击右上角的**Apply**。

   大盘面板创建成功。
6. 单击右上角的 图标，设置监控大盘的名称和归属目录。
7. 单击**Save**。

   大盘创建成功。

查看监控数据

1. 在左侧导航栏，选择 **> Manage**。
2. 在**Manage**页签，单击目标目录下的监控大盘。

   查看目标大盘上的所有监控图表。

2.3.8. 为Grafana大盘生成免登录查看的共享链接

本文介绍如何生成免登录查看的Grafana大盘共享链接，使用户无需登录即可直接查看大盘。

（可选）

（可选）步骤一：创建Grafana组织

分享免登录即可查看的大盘需要开放大盘所在的Grafana组织，但这会让该组织下的所有大盘均处于开放状态。为了您的数据安全，建议您新建一个组织，专门用于分享大盘。

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击Sign in with Alibaba Cloud直接使用当前购买工作区的阿里云账号登录Grafana。

4. 在Grafana左侧导航栏单击图标，然后单击Orgs页签。
5. 在Orgs页签单击+New org。
6. 在New Organization页面输入组织名称，然后单击Create。

步骤二：将组织设定为匿名访问

1. 登录ARMS控制台。
2. 在左侧导航栏选择Grafana服务 > 工作区管理。
3. 在工作区管理页面，单击目标工作区ID或右侧操作列的管理。
4. 在左侧导航栏单击参数设置。
5. 在参数设置页面，单击修改参数，然后选择auth.anonymous。
6. 修改以下auth.anonymous类型的参数，然后单击保存并生效。
   - enabled：设置为*true*，表示开启匿名。
   - org_name：填写需分享大盘所在的组织。
   - org_role：无需填写，默认为*viewer*，表示只有只读权限。

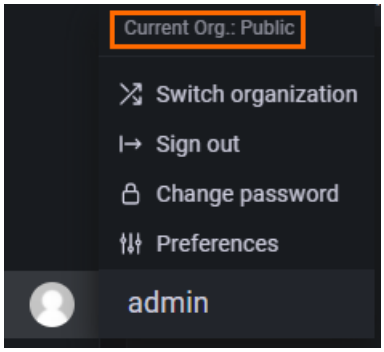
> **说明** org_role参数还可以设置为*editor*和*admin*，但不建议为查看大盘人员授予编辑和管理权限。

（可选）

（可选）步骤三：创建大盘

在组织中创建需要分享的大盘。

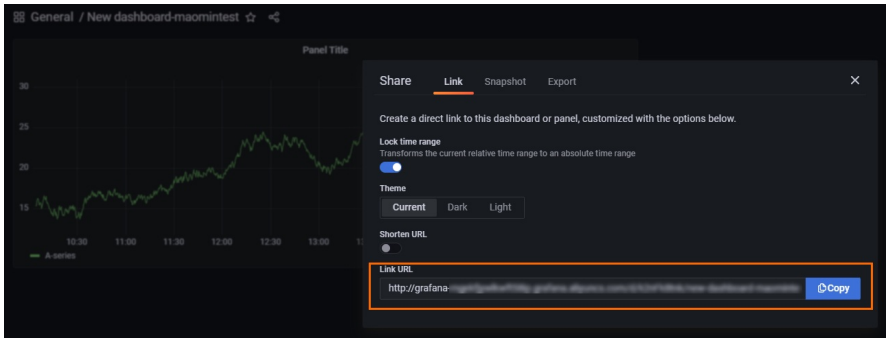
1. 将鼠标悬浮于Grafana页面左下角的头像上查看当前组织是否是用于分享大盘的组织。
   如果不是，则单击Switch organization，在Switch Organization对话框中切换组织。



2. （可选）添加数据源。
   - 添加阿里云数据源的操作，请参见云服务管理。
   - 添加其他数据源的操作，请参见Grafana官方文档。
3. 创建大盘。具体操作，请参见Grafana官方文档。

步骤四：获取分享链接

1. 在Grafana页面，进入需要分享的大盘页面。
2. 单击图标，在Link页签获取大盘分享链接。



3. 退出Grafana当前账号，访问上一步获取的链接，验证链接是否可以打开。

2.3.9. 使用SMTP邮箱邀请用户

如果您需要为多个客户或运维人员创建Grafana用户，直接创建新用户再告知账号密码的操作较为繁琐。若通过SMTP邮箱邀请的方式，则只需要获取被邀请人员的邮箱地址，被邀请人员即可通过Grafana发送的邀请邮件自行创建Grafana用户。本文以网易邮箱为例，介绍如何通过SMTP邮箱邀请用户加入指定的Grafana组织。

步骤一：为邮箱开通SMTP服务

> **说明** 此处的邮箱用于发送Grafana邀请邮件。

1. 在网易邮箱顶部菜单栏，选择**设置 > POP3/SMTP/IMAP**。
2. 在**POP3/SMTP/IMAP**区域开启**POP3/SMTP服务**。

> **注意** 开启过程中需根据页面提示完成账号安全验证，并保存返回的授权密码。

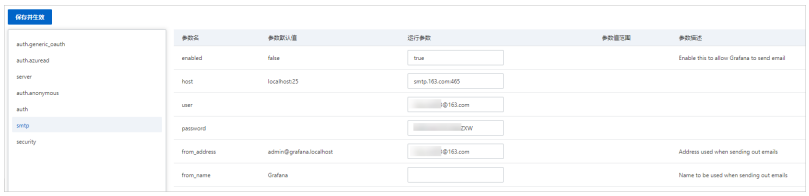
3. 开启SMTP服务后，在**提示**区域获取SMTP服务器地址。

> **说明** 您也可以通过网易邮箱官方文档获取网易邮箱的SMTP服务器地址和端口号。

步骤二：配置Grafana组织参数

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**参数设置**。
5. 在**参数设置**页面，单击**修改参数**，然后选择smtp。
6. 修改以下smtp类型的参数，然后单击**保存并生效**。
   - enabled：设置为*true*。
   - host：SMTP服务器地址 `smtp.163.com:465` 。

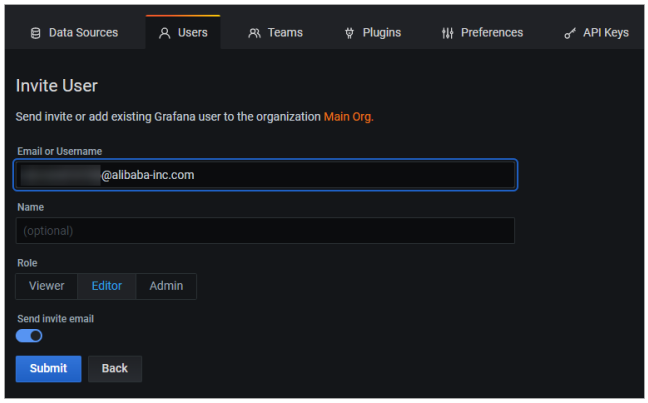
     > **说明** 此处的SMTP服务器地址和端口号以网易邮箱为例，请替换为您实际使用邮箱的SMTP服务器地址和端口号。
   - user：邮箱的地址。
   - password：步骤一中获取的授权密码。
   - from_address：邮箱的地址。
   - from_name：无需设置。



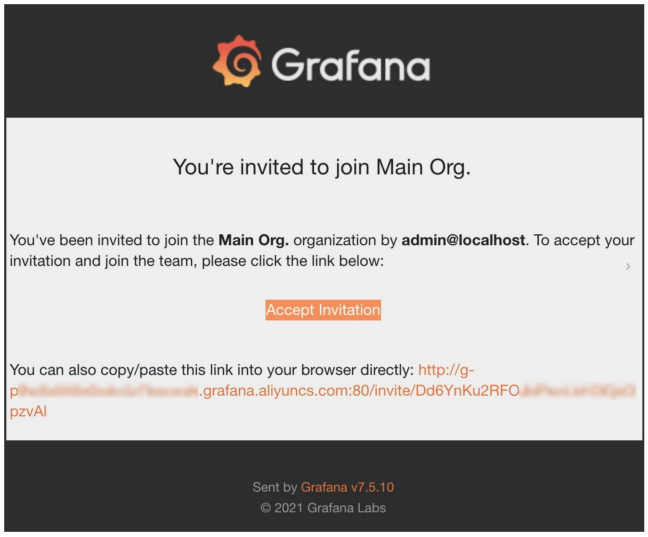
步骤三：在Grafana配置页面邀请新用户

1. 在控制台左侧导航栏单击**工作区信息**，然后在右侧**连接信息**区域单击**操作**列的**登录**进入Grafana。

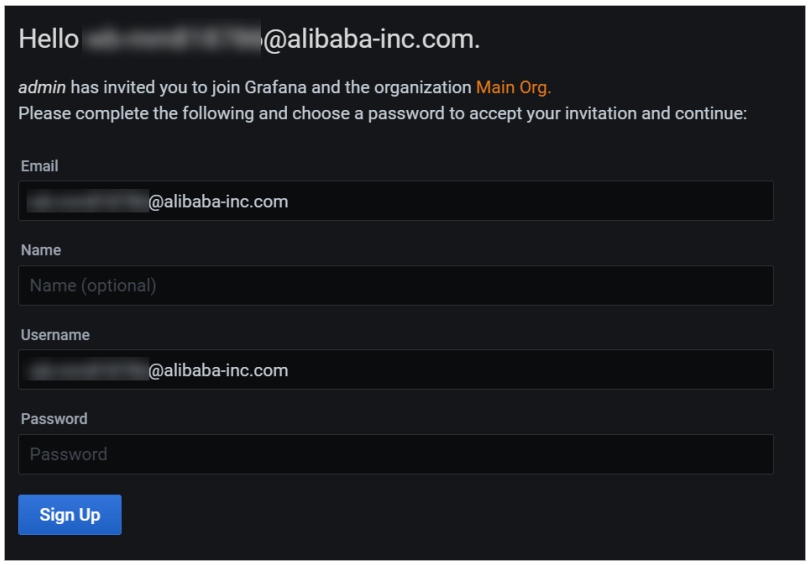
   > **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击Sign in with Alibaba Cloud直接使用当前购买工作区的阿里云账号登录Grafana。
2. （可选）单击Grafana页面左下角的人像，然后单击**Switch**，在**Switch Organization**页面切换目标组织。
3. 在Grafana左侧导航栏，选择 > **Users**。
4. 在**Users**页签单击**Invite**。
5. 在**Invite User**页面的**Email or Username**栏输入被邀请用户的邮箱地址，并设置邀请用户的角色，然后单击**Submit**。
   被邀请用户的邮箱将会收到通过步骤一中的邮箱发送的Grafana邀请邮件。



6. 被邀请用户在收到的邮件中单击Accept Invitation，然后根据跳转链接进入Grafana页面。



7. 在Grafana页面设置用户密码，然后单击Sign Up。



2.3.10. 多阿里云账号云服务大盘配置

Grafana作为可观测的大门，支持将各数据整合并提供一站式的可视化界面，您可以通过一个Grafana账号管理需要监控的全部数据。本文以ECS数据为例，介绍如何将多个阿里云账号下的云服务数据添加到一个Grafana服务中。

背景信息

目前有不少用户拥有多个阿里云账号，并且每个阿里云账号都购买了ECS或者其它各类云产品，如果需要同时监控这些云产品，通过Grafana即可实现将各账号下的云服务数据集成到同一个Grafana工作区中。

示例场景

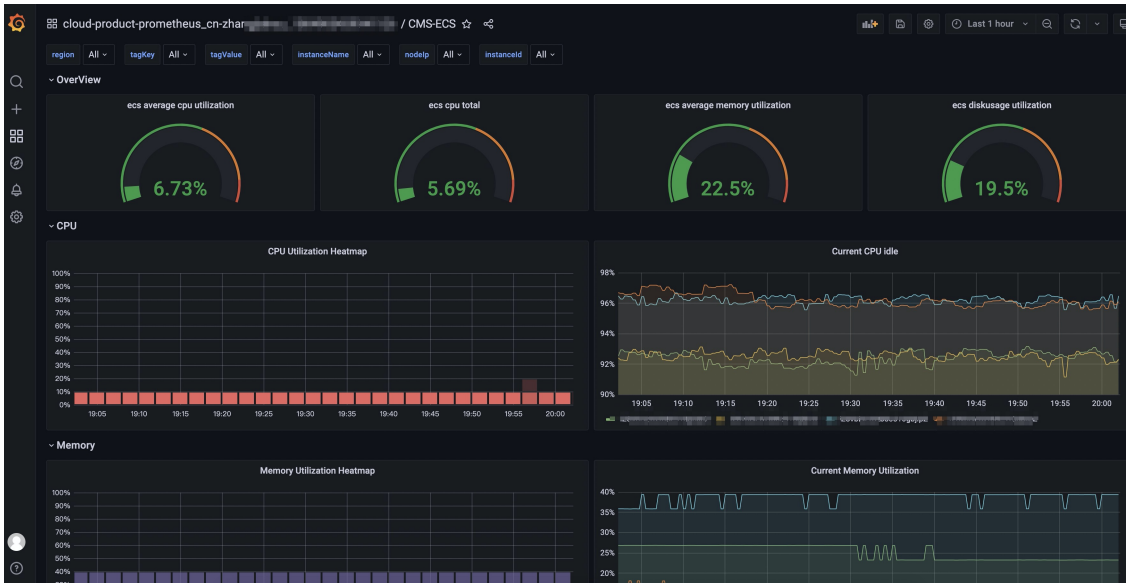
本文演示如何将阿里云账号A和B下的ECS数据全部集成到账号A下的Grafana工作区中。

步骤一：集成账号A的ECS数据并生成大盘

登录阿里云账号A，并在Grafana服务中集成ECS数据。

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区ID或右侧**操作**列的**管理**。
4. 在左侧导航栏单击**云服务管理**。
5. 在**云服务管理**页面左侧单击**CloudMonitor云监控**。
6. 在**CloudMonitor云监控**页面选择需要集成的数据源所在的地域，然后单击ECS大盘左侧的 + 图标，在弹出的集成对话框中单击**确认**。
   Grafana服务会同步当前阿里云账号下ECS的数据源和大盘。等待几分钟后，当大盘名称前出现 ✓ 图标时，表示数据源和大盘已完成同步。

7. 在**CloudMonitor云监控**页面单击**查看云监控大盘**。
8. 在Grafana的**Manage**页面单击名称为CMS-ECS的大盘。
   查看Grafana服务基于模板自动创建的ECS大盘。



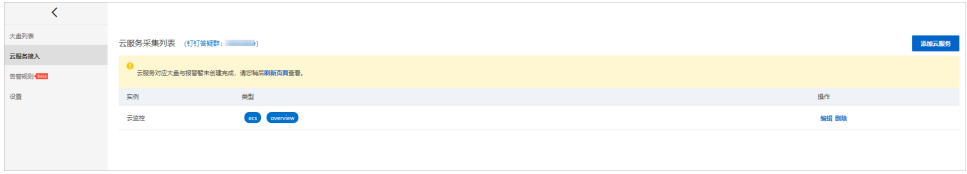
步骤二：集成账号B的ECS数据

将阿里云账号B的ECS数据接入阿里云Prometheus云服务，并通过阿里云Prometheus云服务将ECS数据源添加至阿里云账号A创建的Grafana工作区中。

1. 切换阿里云账号B，登录ARMS控制台。
2. 在**概览**页面的**接入中心**区域单击**查看全部**，或者在左侧导航栏单击**接入中心**。
3. 在**接入中心**页面的**云服务**区域单击**Alibaba Cloud ECS**。
4. 在**接入云服务**面板单击**确定**。

   页面将会跳转至阿里云Prometheus监控的**云服务接入**页面。

   > **说明** 如果当前账号下的ECS已接入阿里云Prometheus云服务，您可以在ARMS控制台的**Prometheus监控 > Prometheus实例列表**页面，单击实例类型为**Prometheus for 云服务**的实例名称，查看已接入云服务的ECS。



5. 在左侧导航栏单击**设置**。
6. 在**设置**页签的**云服务：cms**折叠面板下，复制并保存**HTTP API地址（Grafana 读取地址）**的公网地址。

   > **说明** 由于跨账号VPC不支持，因此无法使用内网地址。

7. 切换阿里云账号A，登录ARMS控制台。
8. 在**Grafana服务 > 工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

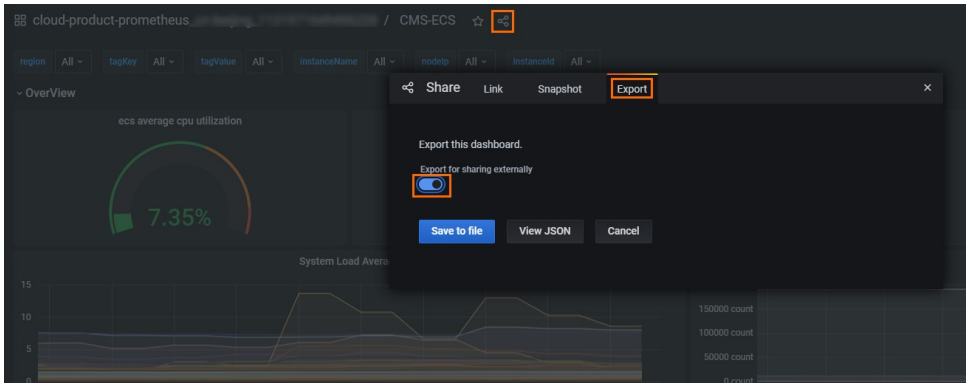
> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击Sign in with Alibaba Cloud直接使用当前购买工作区的阿里云账号登录Grafana。

9. 在Grafana左侧导航栏选择 > Data sources。
10. 在Data Sources页签单击Add data source。
11. 在Add data source页面，单击Prometheus。
12. 在Settings页面，输入Name为数据源名称，在HTTP区域输入URL为步骤6获取的HTTP API地址。
13. 单击Save & Test。
    当页面显示 `Data source is working` 时，表示ECS数据已成功添加至Grafana。更多配置信息，请参见Grafana官方文档。

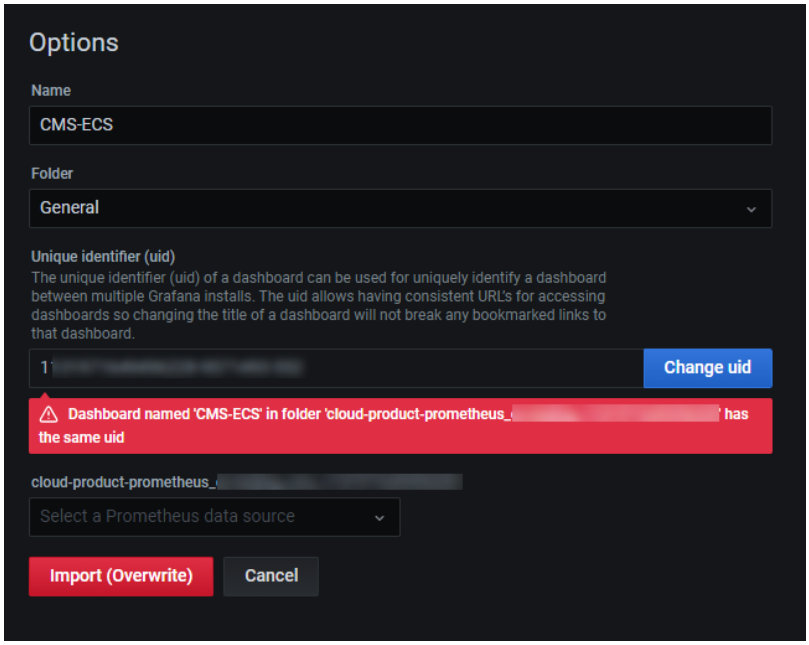
步骤三：为账号B的ECS数据创建Grafana大盘

使用账号A的ECS大盘模板，为账号B的ECS数据源创建Grafana大盘。

1. 在步骤一创建的大盘页面，单击图标，然后在Export页签打开Export for sharing externally开关，然后单击Save to file。



   当前大盘将会导出一个JSON文件。
2. 在Grafana的左侧导航栏选择+ > Import。
3. 在Import页面单击Upload JSON file，然后选择并打开步骤1导出的JSON文件。
4. 在Options区域修改大盘信息。



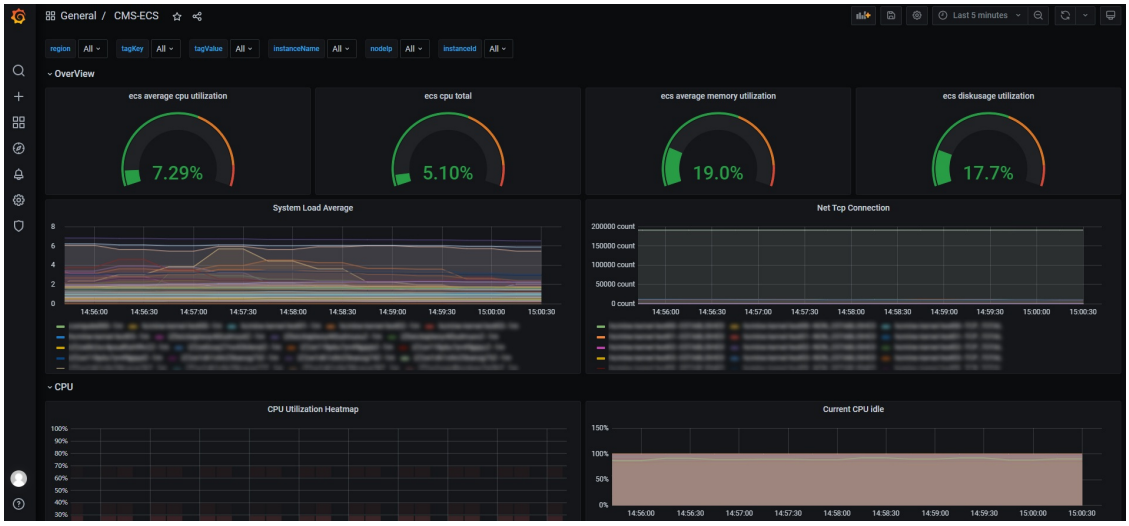
i. 输入Name为自定义大盘名称。

ii. 在Folder区域选择大盘存放的文件夹。

iii. 在Unique identifier (uid)区域单击**Change uid**，修改大盘的UID确保该串字符唯一即可。

iv. 在**Select a Prometheus data source**下拉框选择步骤二集成的数据源。

5. 单击**Import**。
等待几秒钟后，即可查看大盘。

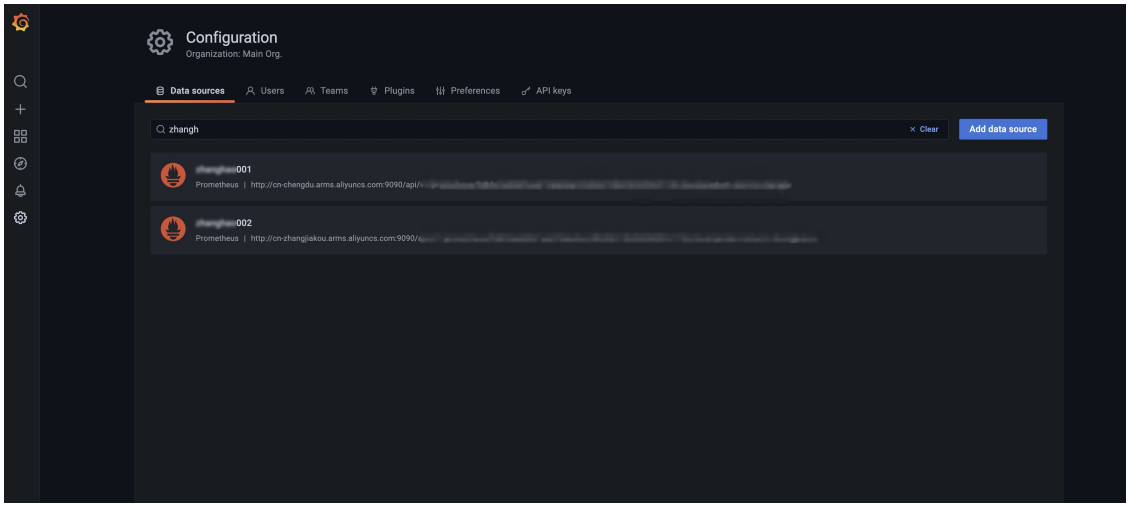


进阶操作

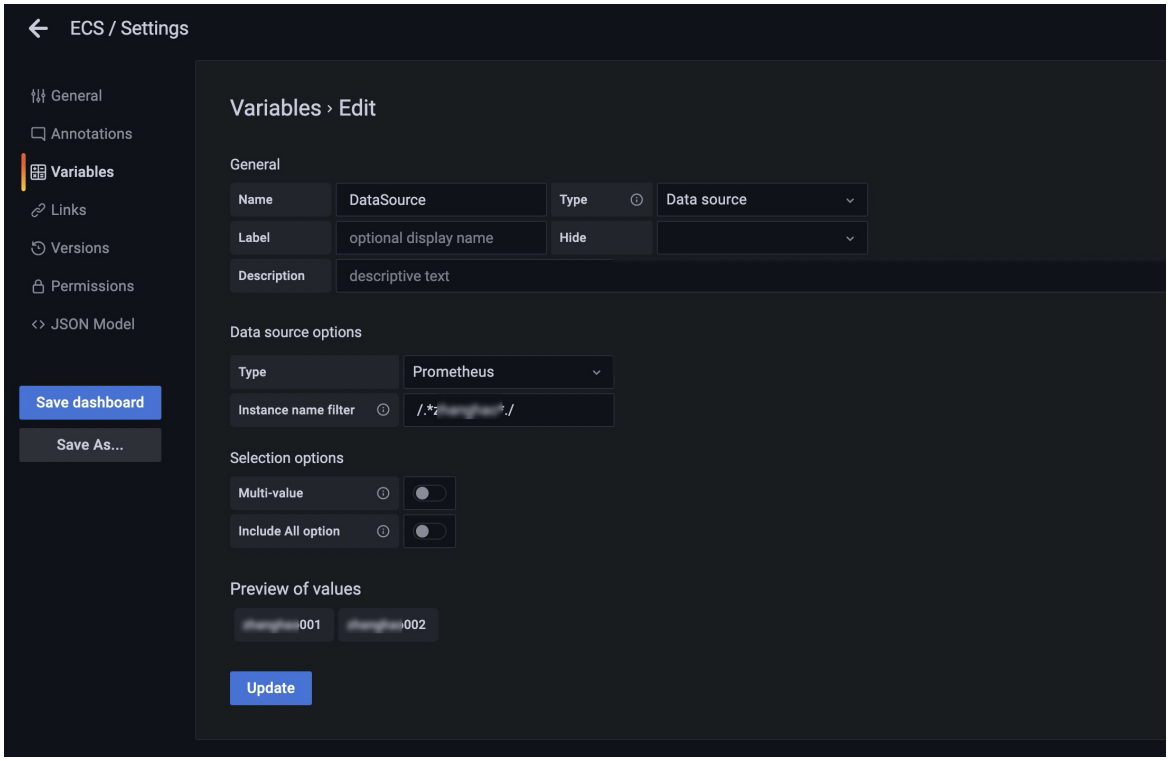
以上步骤仅将不同账号的数据集成到同一个Grafana工作区下，但仍需分开查看大盘。以下步骤将演示如何在一张大盘里展示所有数据。

1. 参考步骤二，将所有账号下的云服务数据添加至Grafana。

> 注意 请按一定规律命名数据源名称，方便后续使用正则匹配选择对应的数据源。

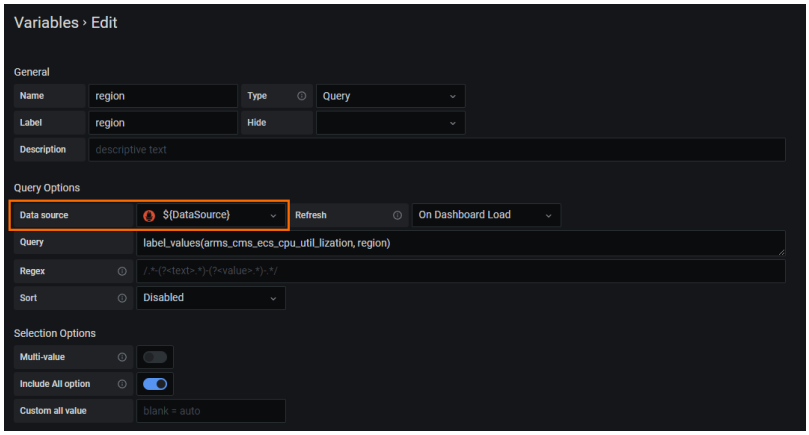


2. 参考步骤二为其中任意一个数据源创建大盘。
3. 在大盘页面右上角单击图标，然后在Settings页面左侧导航栏单击Variables。
4. 在Variables页签单击New。
5. 在Edit 页面进行以下设置。



   i. 在General区域自定义变量名称Name，例如*DataSource*；选择Type为Datasource。
   ii. 在Data source options区域选择Type为Prometheus，然后通过正则匹配筛选Instance name filter为需要添加的数据源。
   iii. 单击Update。
6. 修改其他涉及数据源的变量和面板为上一步添加是数据源。
   - 修改变量：
     a. 在Variables页签单击涉及数据源的变量。

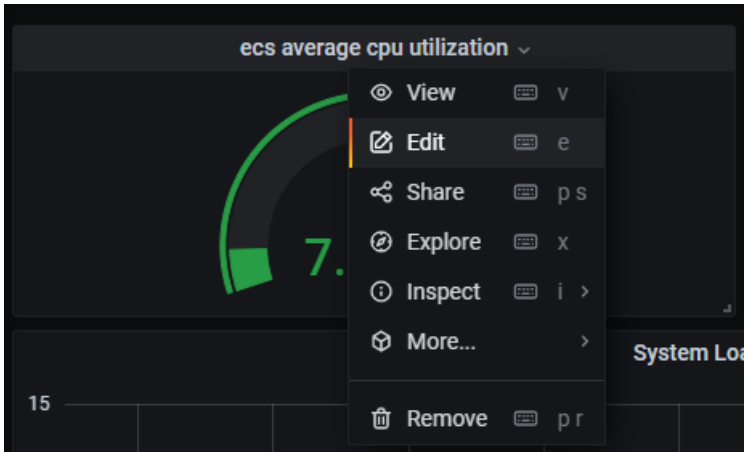
b. 在Edit页面的Query Options区域修改Data source为上一步创建的变量名称，例如*${DataSource}*。



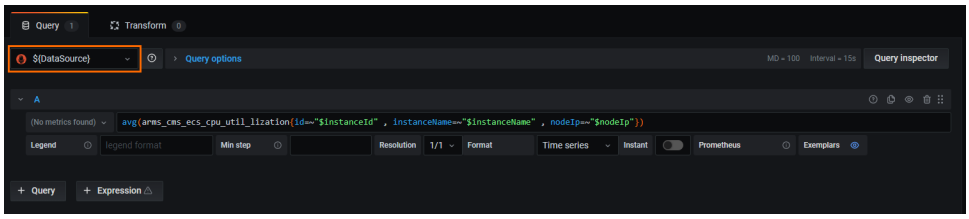
c. 单击Update。

- 修改面板：

a. 返回大盘页面，单击需要修改数据源的面板名称，然后在下拉框单击Edit。



b. 在Edit Panel页面的Query页签，在数据源选择框中选择上一步创建的变量名称，例如*${DataSource}*。



c. 单击右上角的Apply。

i. 在大盘页面右上角单击⚙图标，然后在Settings页面左侧导航栏单击JSON Model。

ii. 在JSON Model页面批量修改 `datasource` 为上一步创建的变量名称，例如*${DataSource}*。

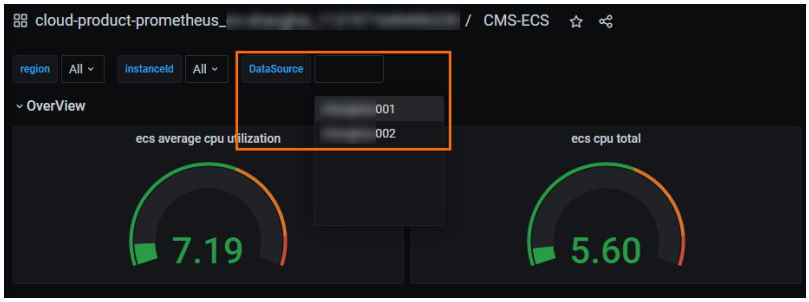
```
"datasource": "${DataSource}"
```

iii. 单击Save Changes。

逐个修改变量和面板的数据源

批量修改变量和面板的数据源

7. 修改完成后，在大盘页面即可通过切换数据源查看不同数据源对应的大盘。



2.3.11. 添加并使用Prometheus数据源

本文介绍如何在Grafana中添加并使用Prometheus数据源。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Grafana服务 > 工作区管理**。
3. 在**工作区管理**页面，单击目标工作区右侧的**访问地址url**链接进入Grafana。

> **说明** 如果需要登录Grafana，可以使用Grafana的Admin账号和创建工作区时设置的密码登录Grafana，或单击**Sign in with Alibaba Cloud**直接使用当前购买工作区的阿里云账号登录Grafana。

4. 在Grafana左侧导航栏选择 > **Data sources**。
5. 在**Data Sources**页签单击**Add data source**，然后单击**Prometheus**。
6. 在**Settings**页面设置以下参数。

参数	说明
Name	数据源名称，可自定义。
Url	Prometheus服务地址。

根据需求设置其他参数，更多信息，请参见Grafana官方文档。

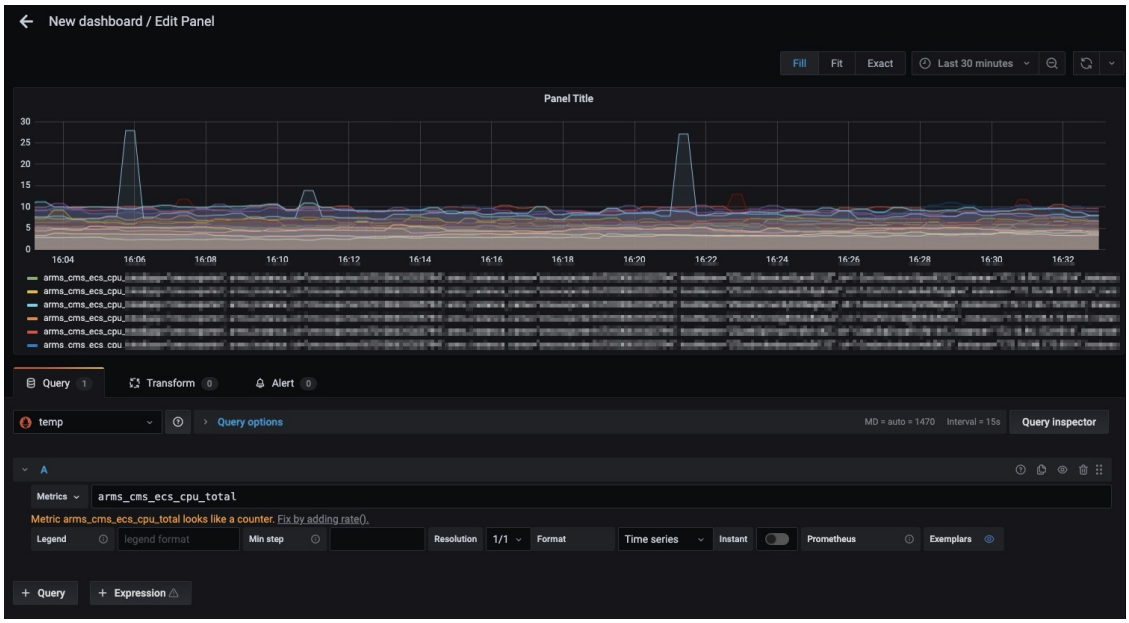
7. 单击**Save & Test**。

验证结果

请按照以下步骤验证操作是否成功：

1. 在Grafana左侧导航栏中选择**+ > Create**。
2. 在**New dashboard**页面单击**Add an empty panel**。
3. 在**Edit Panel**页面的**Query**页签的下拉框中选择添加的数据源，在A区域的**Metrics**字段输入指标名称并按回车。
   如果能显示出相应指标的图表，则说明操作成功。否则请检查填写的接口地址或Token是否正确，以及

数据源是否有Prometheus监控数据。



相关文档

- Grafana官方文档

3.应用安全

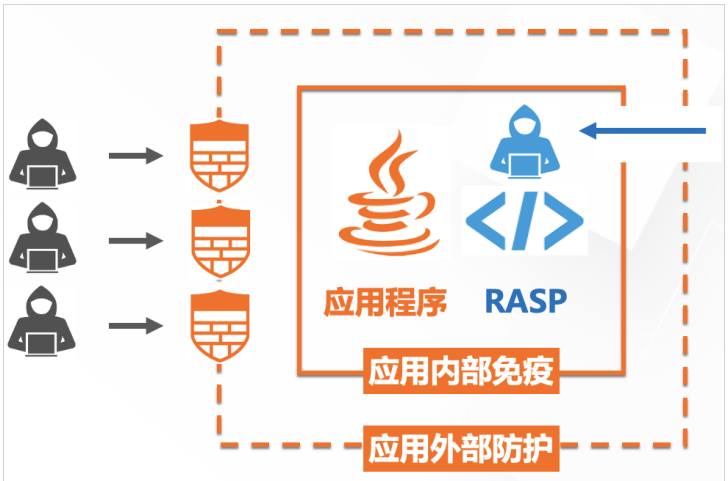
3.1. 什么是应用安全

ARMS应用安全是一款基于RASP（Runtime Application Self-Protection）技术的安全产品，可为应用在运行时提供自我保护。您无需修改应用代码，只需在实例中安装应用安全探针，即可为应用提供强大的安全防护能力，并抵御绝大部分未知漏洞所利用的攻击手法。

背景信息

ARMS应用安全是基于阿里云安全的RASP技术所开发的功能。RASP安全技术可在应用运行时检测攻击并进行自我保护。它运行在应用程序内部，通过钩住（Hook）关键函数，实时监测应用在运行时与其他系统的交互过程。当应用出现可疑行为时，RASP会根据当前上下文环境识别并阻断攻击。

以疫情防护类比，传统的防火墙和Web应用防火墙（WAF）等边界防护方案类似于防护服和口罩，是通过阻断或过滤病毒传播通路降低人体感染风险。而RASP更像是疫苗，通过在人体内部产生抗体，在病毒入侵的时候消灭它们。



RASP与WAF并不是相互取代的关系，二者在不同业务和安全防护场景下各有所长。对于应用防护来说，您可根据自己的业务环境和要求接入ARMS应用安全以及阿里云Web应用防火墙，协同构建边界与应用内生双重防护能力，最大程度降低应用被入侵、数据泄露、服务不可用等风险。

使用限制

应用安全目前仅支持Java应用接入。

功能特性

ARMS应用安全功能可以帮助应用对威胁其安全的攻击手法进行防护，包括但不限于SQL注入、恶意文件读写、恶意文件上传、命令执行、任意文件读取、恶意外连、线程注入、恶意DNS查询、内存马注入等。此外，基于RASP技术的应用安全不依赖于静态的规则库，对未知漏洞（0day漏洞）也可进行防御。

针对存在安全漏洞的第三方应用组件，应用安全功能可以进行自动化梳理，关联组件对应的CVE漏洞、组件的详细路径、漏洞风险等级和评分以及相关实例信息等，帮助研发和安全团队盘点危险第三方组件风险，快速定位风险详情并按照优先级进行修复。

您可以选择将应用安全保持在监控模式，作为保证应用安全的纯监测组件，帮助您在发现攻击行为时及时修复对应的漏洞。

> **说明**
> - 在使用应用安全功能前，相关应用需已接入ARMS应用监控。
> - 应用监控的Java探针版本需为2.7.1.3或以上。您可以登录ARMS控制台，在**应用监控 > Agent列表**页面查看已接入应用的探针版本。

监控模式监测应用安全状况

应用安全案例实践

常见问题

1. 应用安全对应用运行是否存在影响？

   应用安全自身对性能、兼容性和稳定性有良好的控制，对应用运行的影响几乎可以忽略不计。实际测试中，CPU的额外开销小于1%，内存开销小于30 MB，应用延迟（RT）小于1 ms。此外，应用安全还提供观察模式、软熔断逃生机制等功能，最大限度降低对应用运行的干扰。

2. 如何接入应用安全？

   您可通过ARMS控制台一键接入应用安全，接入后重启目标应用对应的实例即可，无需修改任何应用代码。应用安全目前仅支持Java应用接入。具体操作，请参见接入应用安全。

3. 接入应用安全后应如何进行应用防护？

   理论上来说，应用安全检测到的攻击是能够实际产生安全威胁的行为，相比基于流量特征的传统检测技术而言，误报率较低，所以对应用安全功能所检测到的攻击，必须引起重视。在接入应用安全后，应用安全对攻击的默认防护模式为“监控”。在应用稳定运行后，您可切换为“监控并阻断”模式。

更多应用安全相关常见问题，请参见应用安全常见问题。

联系我们

ARMS应用安全功能目前正在免费公测中，欢迎加入应用安全答疑钉钉群（群号：34833427）进行咨询。若您对应用安全有任何相关问题，除了参考帮助文档外，也欢迎您加入钉钉群与产品经理和安全专家一起交流。

3.2. 接入应用安全

您可以通过ARMS控制台将目标应用一键接入应用安全。接入后，重启该应用对应的实例即可使用应用安全功能，无需修改任何应用代码。

前提条件

- 应用安全功能目前仅支持Java应用接入。使用前，目标Java应用需已接入ARMS应用监控。具体操作，请参见应用监控接入概述。
- 应用监控的Java探针版本要求：
  - 容器服务应用、EDAS应用等自动升级场景要求版本需为v2.7.1.2或以上。

    > **说明** 自动升级场景是指可以通过重启应用或Pod等操作自动升级探针版本的场景。更多信息，请参见升级探针。

  - 其他手动升级场景要求版本需为v2.7.1.3或以上。

您可以登录ARMS控制台，在**应用监控 > Agent列表**页面查看已接入应用的探针版本。若需升级探针版本，请参见升级探针。

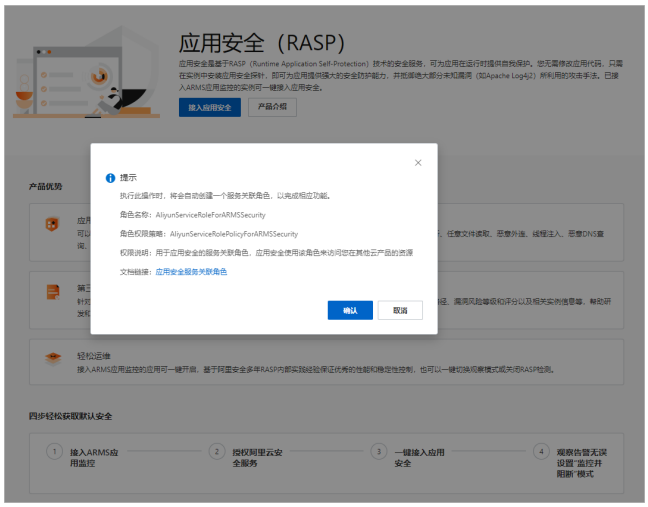
服务授权

在接入应用安全之前，您需要先授权访问阿里云安全服务。经过您的授权后，ARMS仅限于访问应用安全依赖的相关资源，用于完成后续的产品功能。

1. 登录ARMS控制台。
2. 在左侧导航栏，选择**应用安全 > 应用列表**。
3. 在**应用安全**区域单击**接入应用安全**。
4. 在弹出的**提示**对话框中单击**确认**。

   授权后，ARMS将会自动创建应用安全服务关联角色AliyunServiceRoleForARMSSecurity，授权成功后，您可以查看应用列表并接入目标应用。关于应用安全服务关联角色AliyunServiceRoleForARMSSecurity的权限说明，请参见应用安全服务关联角色。

   > **说明** 如果页面提示用户没有创建服务关联角色的权限，请联系阿里云账号为当前RAM用户添加指定权限策略。具体操作，请参见常见问题。



接入目标应用

1. 登录ARMS控制台。
2. 在左侧导航栏，选择**应用安全 > 应用列表**，然后在页面顶部菜单栏，选择地域。
   应用列表页面列出当前可以接入应用安全的全部Java应用。

   > **说明** 接入应用前，请先确认您当前使用的探针版本符合版本要求（v2.7.1.3或以上）。

3. 接入目标应用。
   - 接入单个应用：在目标应用**操作**列，单击**接入**，然后在弹出的对话框中单击**确认**。
   - 批量接入应用：
     a. 在**应用列表**页面，单击左上角的**接入应用**。
     b. 在**接入应用**对话框的**未接入应用安全应用**列表中，选择需接入应用安全的目标应用，单击>图标将其移动至**已接入应用安全应用**列表后，单击**确定**。
4. 在本地重启目标应用对应的实例，使接入生效。

您可以在**应用列表**页面的**接入状态**列查看当前应用的接入状态。待全部实例重启完毕后，应用安全功能将对目标应用的全部实例生效。若只有部分实例重启完成，则应用安全功能只在重启成功的实例上生效。

接入状态列的**已接入实例**区域显示目标应用中已接入实例和全部实例的数量。您可以单击数字查看实例接入状态详情。

设置防护模式

在完成目标应用接入应用安全功能后，您可以设置目标应用的防护模式。目前防护模式包括以下三种：**监控**、**监控并阻断**和**禁用**。应用接入后，默认的防护模式为**监控**。您可在观察一段时间确定应用运行无误后，将防护模式切换为**监控并阻断**，以确保攻击发生时能及时防护您的应用。

1. 在**应用安全 > 应用列表**页面，单击目标应用**操作**列的**防护设置**。
2. 在弹出的**防护设置**对话框中，完成以下设置后，单击**确定**。

设置项	说明
防护模式	○ **监控**：只监控攻击行为，若有配置告警规则，则会产生告警，不影响应用运行。 ○ **监控并阻断**：监控并阻断攻击行为，阻断时应用会抛出异常。 ○ **禁用**：关闭当前应用的应用安全功能，不检测也不阻断任何攻击行为。
检测超时时间	攻击检测的最大时间，输入范围为5～200000毫秒，默认设置为300毫秒。若攻击检测超过设置的时间，即使未完成检测逻辑也会继续执行原始业务逻辑。如无特殊原因，建议使用默认值。
检测类型	检测攻击的分类，建议使用默认配置（即全选）。具体检测类型说明，请参见检测攻击类型说明和防护建议。

> **说明** 若需修改应用的防护设置，需注意，防护设置变更非立即生效，最大延迟在30秒左右。

取消接入目标应用

若需为目标应用取消接入应用安全，您可在**应用安全 > 应用列表**页面，单击目标应用**操作**列的**取消接入**，然后在弹出的对话框中单击**确认**。完成后，需在本地重启目标应用所关联的相关实例，即可取消接入应用安全。

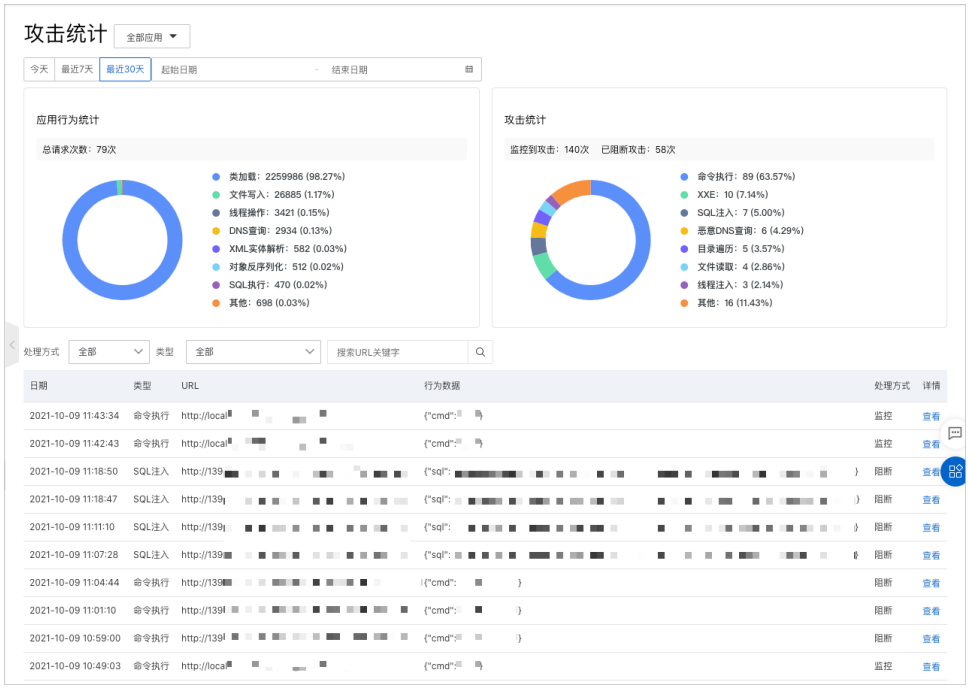
但若没有特殊情况，只是出于对应用运行性能方面的考虑，则不建议您取消接入应用安全。接入应用安全后，默认防护模式为“监控”。在这种模式下，系统仅上报攻击告警，不会产生实际阻断，对应用运行不会产生任何影响，您还可以选择切换至“禁用”模式来关闭所有安全检测能力。这种模式下，若存在安全攻击，系统也不会上报攻击告警。

3.3. 查看攻击统计

ARMS应用安全的攻击统计页面展示应用攻击防护情况。您可以查看攻击的详细数据，包括产生时间、类型和攻击URL等，以及应用安全针对该攻击所采取的处理方式。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏，选择**应用安全 > 攻击统计**，然后在页面顶部菜单栏，选择地域。
   攻击统计页面默认展示全部应用受到攻击的统计情况。

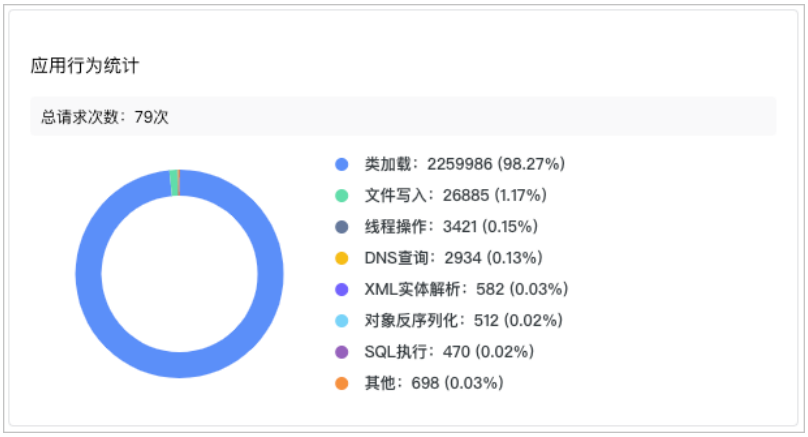


3. （可选）若需查看单个应用的统计情况，您可以选择以下任意一种方式：
   - 单击**攻击统计**页面上方的**全部应用**下拉菜单，切换至具体应用。
   - 在**应用安全 > 应用列表**页面，单击具体的应用名称，则会跳转至**攻击统计**页面，展示该应用受到攻击的统计情况。

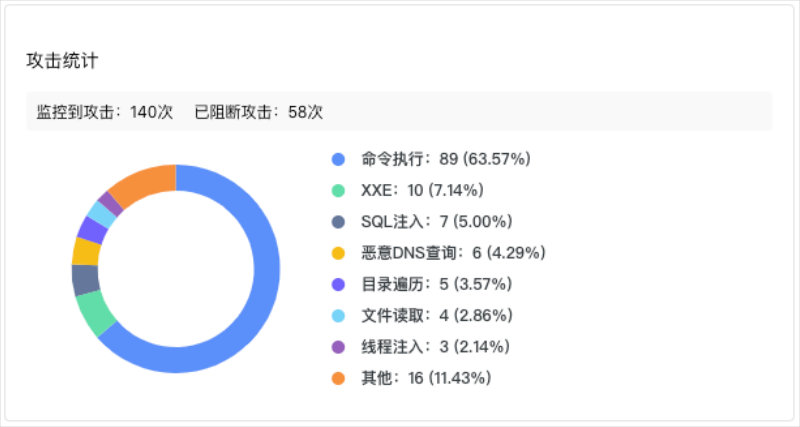
查看攻击统计详情

攻击统计页面以环图的形式展示接入应用安全后应用产生的行为以及应用受到攻击的统计情况。页面下方列表则展示了每一攻击行为的详细数据，包括攻击行为的类型、URL、行为数据以及该行为的处理方式等。

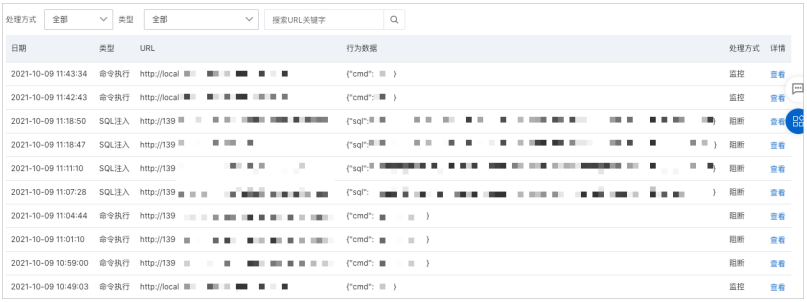
应用行为统计区域展示经过应用安全检测的应用行为以及其对应的分类，包括正常行为和攻击行为。



攻击统计区域展示应用安全检测到的具有实际威胁的攻击行为以及其对应的攻击类型。



攻击统计页面下方列表展示每一个攻击行为的具体情况。您可以在列表中查看攻击行为产生的时间、具体类型、URL、具体数据和该行为的处理方式。您也可以单击列表最右侧**详情**列的**查看**，在弹出的面板中查看目标攻击行为的详情，包括攻击所利用的安全漏洞、攻击请求以及对应服务器的详细信息。



> **说明** 若**攻击统计**页面中没有攻击数据，可能存在以下三种原因：
>
> 1. 目标应用没有完成接入。在控制台单击**接入**后没有重启目标应用对应的实例（或只重启了部分实例）。
> 2. 目标应用的Java探针版本较低。应用安全对探针版本要求如下。更多信息，请参见接入应用安全
>   - 容器服务应用、EDAS应用等自动升级场景要求版本需为v2.7.1.2或以上。
>
>   **说明** 自动升级场景是指可以通过重启应用或Pod等操作自动升级探针版本的场景。更多信息，请参见升级探针。
>
>   - 其他手动升级场景要求版本需为v2.7.1.3或以上。
> 3. 没有产生真实有效的攻击行为。与传统防火墙不同，应用安全仅记录真实有效的攻击。传统防火墙会在检测到报文中存在恶意攻击特征时进行上报，但存在恶意特征不代表攻击有效，例如利用PHP漏洞的攻击请求在Java环境中则没有意义。若产生真实有效的攻击，往往表明攻击者已成功突破外层防御，可以打入应用内部环境并执行危险动作。您的应用可能不会存在大量真实有效的攻击，但发生时请务必引起重视，及时拦截或者修复相关安全漏洞。

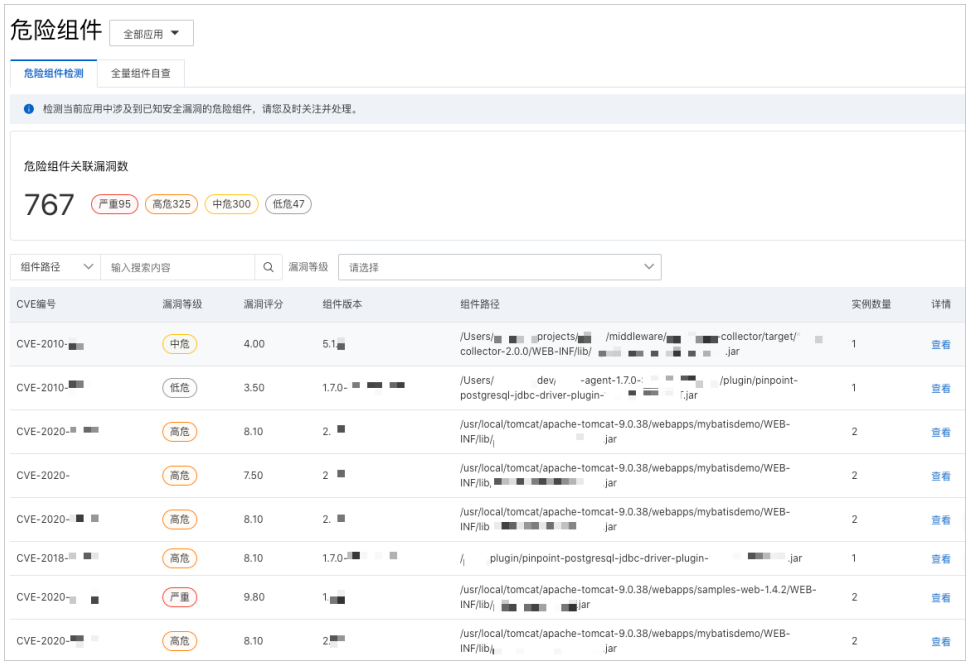
3.4. 查看危险组件

ARMS应用安全的危险组件检测功能盘点应用中所使用的危险第三方组件（指非应用本身开发人员开发，直接从外部获取的第三方人员开发的依赖包，例如Maven中引用的第三方依赖库），包括组件对应的CVE漏洞编号、组件版本、路径等。

若使用存在安全漏洞的组件，会对应用的安全性产生影响，因此对于存在漏洞风险的组件，建议您尽快通过升级等方式修复。若短时间内无法修复，请将对应应用的防护模式设置为**监控并阻断**，以确保攻击者利用这些漏洞时，能被应用安全及时拦截。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏，选择**应用安全 > 危险组件检测**，然后在页面顶部菜单栏，选择地域。
   危险组件页面默认展示全部应用的危险组件存在的漏洞数。



3. （可选）若需查看单个应用危险组件的检测情况，您可以选择以下任意一种方式：
   - 单击**危险组件**页面上方的**全部应用**下拉菜单，切换至具体应用。
   - 在**应用安全 > 应用列表**页面，单击具体应用**危险组件**列的数字，则会跳转至**危险组件**页面，展示该应用危险组件的检测情况。

查看危险组件详情

危险组件检测页签下展示应用安全检测到的危险组件关联漏洞数的总体情况以及每一个漏洞的CVE编号、漏洞等级、漏洞评分、该漏洞所对应组件的版本和路径等信息。您可以通过筛选框按照组件路径、CVE编号或漏洞等级进行筛选，快速搜索目标漏洞。

您还可以单击列表中目标漏洞**详情**列的**查看**，在弹出的面板中查看该漏洞的详细信息以及其关联的组件和实例的详情。

全量组件自查

危险组件检测页签下列出的组件均包含有明确漏洞编号的安全漏洞。除了检查此类组件之外，您还可以在**全量组件自查**页签下查看接入应用安全的应用所包含的全部第三方组件，以便在最新漏洞出现时可以快速排查您的应用中是否包含与此漏洞相关联的组件。

3.5. 使用应用安全告警规则

在创建应用安全告警规则后，当告警被触发时，系统会以您指定的通知方式向告警联系人或钉群发送告警信息，以便您及时采取必要的解决措施，防护您的应用。

创建告警规则

1. 登录ARMS控制台。
2. 在左侧导航栏中选择**应用安全 > 应用安全告警规则**，然后在顶部菜单栏选择地域。
3. 在**应用安全告警列表**页面右上角，单击**创建应用安全告警**。
4. 在**创建应用安全告警**页面，完成填写所有必填信息，然后单击**保存**。

设置项	说明
告警名称	自定义的应用安全告警名称。
告警分组	应用安全默认告警分组为**安全告警指标分组**，且无法修改。
告警指标	产生告警的指标。目前，应用安全告警仅支持**攻击次数**告警指标。
告警条件	设置当攻击次数满足何种条件时，会触发告警并发送通知。例如，当攻击次数大于或等于1时，发送告警。
筛选条件	设置当前配置的告警规则所适用的应用范围，即所有符合筛选条件的应用满足此条告警规则时，均会产生告警。 可选筛选条件包括： ○ **遍历**：告警规则适用于当前接入应用安全的全部应用。筛选条件默认为遍历。 ○ **等于**：选择该条件后，需继续输入具体应用名。所创建的告警规则将仅适用于该应用。不支持同时填写多个应用。 ○ **不等于**：选择该条件后，需继续输入具体应用名。所创建的告警规则将适用于除该应用之外的其他应用。不支持同时填写多个应用。 ○ **正则匹配**：选择该条件后，按需输入正则表达式匹配相应的应用名称。所创建的告警规则将适用于符合该正则表达式的所有应用。 ○ **正则不匹配**：选择该条件后，按需输入正则表达式匹配相应的应用名称。所创建的告警规则将过滤符合该正则表达式的所有应用。 **说明** 完成筛选条件设置后，会弹出**数据预览**区域，以时序曲线的形式展示相应的告警设置和所选应用的实际指标。筛选条件为**遍历**时，默认在**数据预览**区域展示相关应用的指标，您可以在该区域的筛选框中选择目标应用以及时间区间进行数据展示。
数据预览	以时序曲线的形式展示当前告警规则配置的监控指标的值。
持续时间	需持续满足告警条件的时长，才会触发告警。例如，若持续时间设置为1分钟，则表示连续1分钟均满足告警条件时，才会触发告警。
告警等级	自定义告警等级。默认告警等级为**默认告警**，告警严重程度从P4、P3、P2、P1逐级上升。
告警内容	用户收到的告警信息，可自定义。默认告警内容为*应用名称：{{$labels.appName}}发生应用安全攻击，当前值{{$value}}次*。
高级设置	

设置项	说明
快速指定通知策略	○ 不指定通知规则：若选择此选项，当完成创建告警规则后，您可以在**通知策略**页面新建通知策略并指定分派规则和分派条件（如告警规则名称等）来匹配该告警规则。当该告警规则被触发产生告警事件后，告警信息会被发送给通知策略中指定的联系人或联系人组。更多信息，请参见通知策略。 ○ 指定通知规则发送告警：告警被触发时，ARMS通过指定通知策略的通知方式发送告警信息。您可以选择已有的通知策略，也可以新建一个通知策略。更多信息，请参见通知策略。
标签	设置告警标签，设置的标签可用作通知策略匹配规则的选项。
注释	设置告警的注释。

管理告警

已创建的应用安全告警规则会显示在**应用安全 > 应用安全告警规则**页面上，您可以在此页面对已创建的告警规则执行启动、停止、编辑、删除、查看告警历史等操作。

1. 登录ARMS控制台。
2. 在左侧导航栏中选择**应用安全 > 应用安全告警规则**，然后在顶部菜单栏选择地域。
3. （可选）在**应用安全告警列表**页面的搜索框中输入告警名称，并单击搜索图标。

   > **说明** 您可以输入告警名称的一部分内容进行模糊搜索。

4. 在搜索结果列表的**操作**列中，按需对目标告警规则采取以下操作：
   - 如需编辑告警规则，请单击**编辑**，在**编辑应用安全告警**页面中编辑告警规则，并单击**保存**。
   - 如需删除告警规则，请单击**删除**，并在**提示**对话框中单击**确定**。
   - 如需启动已停止的告警规则，请单击**启动**，并在**提示**对话框中单击**确定**。
   - 如需停止已启动的告警规则，请单击**停止**，并在**提示**对话框中单击**确定**。
   - 如需查看告警事件历史，请单击**告警历史**，在**告警事件历史**页面上查看相关记录。

相关文档

- 查看告警发送历史
- 查看告警事件历史

3.6. 应用安全常见问题

本文介绍使用应用安全过程中可能会遇见的常见问题。

应用安全对应用运行是否存在影响？

应用安全自身对性能、兼容性和稳定性有良好的控制，对应用运行的影响几乎可以忽略不计。实际测试中，CPU的额外开销小于1%，内存开销小于30 MB，应用延迟（RT）小于1 ms。此外，应用安全还提供观察模式、软熔断逃生机制等功能，最大限度降低对应用运行的干扰。

如何接入应用安全？

您可通过ARMS控制台一键接入应用安全，接入后重启目标应用对应的实例即可，无需修改任何应用代码。应用安全目前仅支持Java应用接入。具体操作，请参见接入应用安全。

接入应用安全后应如何进行应用防护？

理论上来说，应用安全检测到的攻击是能够实际产生安全威胁的行为，相比基于流量特征的传统检测技术而言，误报率较低，所以对应用安全功能所检测到的攻击，必须引起重视。在接入应用安全后，应用安全对攻击的默认防护模式为“监控”。在应用稳定运行后，您可切换为“监控并阻断”模式。

为什么攻击统计中没有攻击数据？

没有攻击数据可能存在以下三种原因：

1. 目标应用没有完成接入。在控制台单击**接入**后没有重启目标应用对应的实例（或只重启了部分实例）。
2. 目标应用的Java探针版本较低。应用安全对探针版本要求如下。更多信息，请参见接入应用安全
   - 容器服务应用、EDAS应用等自动升级场景要求版本需为v2.7.1.2或以上。

     > **说明** 自动升级场景是指可以通过重启应用或Pod等操作自动升级探针版本的场景。更多信息，请参见升级探针。

   - 其他手动升级场景要求版本需为v2.7.1.3或以上。
3. 没有产生真实有效的攻击行为。与传统防火墙不同，应用安全仅记录真实有效的攻击。传统防火墙会在检测到报文中存在恶意攻击特征时进行上报，但存在恶意特征不代表攻击有效，例如利用PHP漏洞的攻击请求在Java环境中则没有意义。若产生真实有效的攻击，往往表明攻击者已成功突破外层防御，可以打入应用内部环境并执行危险动作。您的应用可能不会存在大量真实有效的攻击，但发生时请务必引起重视，及时拦截或者修复相关安全漏洞。

危险组件检测中的漏洞应该如何处理？

危险组件检测中关联到的漏洞均为已被公开的漏洞，这些漏洞可能会被攻击者利用进行入侵（即使当前无法被利用，未来应用代码改动后也存在被利用的风险）。通常情况下，这些漏洞可以被应用安全防御，前提是相关应用的防护模式已经切换到**监控并阻断**而不是默认的**监控**模式。

同时，建议您及时修复这些漏洞。您可以登录ARMS控制台，在**应用安全 > 危险组件检测**页面单击列表中目标漏洞**详情**列的**查看**，在**漏洞详情**页签的**修复参考**区域查看相关修复建议。这些建议多数为相关组件官方提供的升级或修复方案。您也可以通过在搜索引擎中搜索漏洞的CVE编号检索相关修复方案。

3.7. 检测攻击类型说明和防护建议

本文介绍攻击统计中涉及的攻击类型以及相关防护建议。

攻击类型	说明	防护建议
JNDI注入	当应用进行JNDI查询的时候，若查询的URL可以由攻击者控制，则攻击者往往可以使服务器去查询恶意的链接使得服务器加载一些恶意Class，实现任意代码执行。	• 若该漏洞源于第三方组件，请及时进行组件版本升级。 • 若为自写JNDI查询代码，请对查询的URL进行限制，禁止一些危险协议的查询。

攻击类型	说明	防护建议
JNI注入	JNI注入是一种通用的RASP（Runtime Application Self-Protection）绕过手段。当攻击者拿到代码执行权限后，可以通过Java Native函数去调用外部的恶意动态链接库，从而绕过Java层的安全防护，并隐匿具体的恶意行为。	您的服务器可能存在代码执行漏洞，请检查漏洞的位置并限制执行代码的功能。
SQL注入	SQL注入手段通过把SQL命令插入到页面请求或Web表单的查询字符串中，以达到欺骗服务器执行指定SQL语句的目的。它可以通过在Web表单中输入SQL语句，得到存在安全漏洞的网站上的数据。	SQL注入是由拼接SQL语句引起的。请尽可能使用预编译来处理传入的参数，或通过白名单和黑名单来限制拼接参数。
XXE	指XML外部实体注入漏洞（XML External Entity Injection）。当XML文件在引用外部实体时，通过构造恶意内容，可以导致任意文件读取，命令执行和内网攻击等不良后果。	请检查应用程序在解析XML时是否需要加载外部实体。如果不需要，请在XML解析配置中禁用外部实体。
XSS	跨站脚本攻击是指恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的。	XSS漏洞本质上是一种HTML注入，也就是将HTML代码注入到网页中。那么其防御的根本就是在将用户提交的代码显示到页面上时做好一系列的过滤与转义。 1. 过滤输入的数据，对例如：“ ‘ ”，“ “ ”，“ < ”，“ > ”，“ on* ”，script、iframe等危险字符进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括HTTP请求中的Cookie中的变量，HTTP请求头部中的变量等。 2. 不仅验证数据的类型，还要验证其格式、长度、范围和内容。 3. 不仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。 4. 对输出到页面的数据进行相应的编码转换，如HTML实体编码、JS编码等。对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行检查。
恶意Attach	Attach API是Java提供的动态修改字节码技术，该功能可以实现动态修改运行时应用的字节码。很多攻击者通过该手法进行Agent型内存马的注入，具有较高的欺骗性。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。

攻击类型	说明	防护建议
恶意DNS查询	恶意DNS查询存在多种利用方式。攻击者极有可能通过DNS协议来突破内网网络限制，从而将敏感信息带出内网，也可能通过DNS协议去探测内网系统是否存在SSRF、JNDI注入等漏洞。	恶意DNS查询是由服务器向用户控制的参数发送请求所引起的。请检查参数并通过白名单进行限制。
恶意反射调用	RASP自保护模块，禁止攻击者通过反射的方式去修改运行时RASP的相关数据。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
恶意外连	SSRF（Server-side request forgery）服务器端请求伪造漏洞指的是攻击者通过构造由服务端发起的请求，对网站内部系统进行攻击。	SSRF是由服务器向用户传入的参数发送请求所引起的。请检查参数并通过白名单进行限制。
恶意文件读写	Java提供RandomAccessFile，用于文件读写操作。当使用该Class进行文件读写的时候，如果未对文件路径、文件内容进行限制，攻击者可能读取到系统敏感文件，也可能上传木马文件。	请检查文件读取和上传是否正常。如果出现异常，请检查函数代码，并通过黑名单进行限制。
恶意文件上传	对于网站提供的文件上传功能，如果未对上传文件的类型进行限制，攻击者可能通过上传木马文件来获取服务器的更大权限，从而造成严重危害。	请限制上传文件的类型，禁止上传具有执行权限的文件，如JSP。
反序列化攻击	Java反序列是指把字符序列恢复为Java对象的过程，在对象生成过程中，若该对象包含一些危险度较高的代码，则攻击者可能通过控制生成对象的成员变量在对象进行反序列化的时候实现一些恶意攻击。	1. 及时升级存在漏洞的组件版本。 2. 若官方还未提供漏洞修复的组件版本，请暂时关闭该功能。
命令执行	命令执行漏洞是指服务器没有对执行的命令进行过滤，用户可以随意执行系统命令。	通常远程命令执行是由Web Shell或服务器的危险代码引起的。请检查命令执行的位置。如果是Web Shell，请及时删除。如果是服务器的正常功能，则可以通过白名单限制执行的命令。
目录遍历	网站自身的配置缺陷可能会使得网站目录被任意浏览，导致隐私信息泄露。攻击者可以利用该信息对网站进行攻击。	请检查目录遍历操作是否正常。如果异常，请检查函数的代码，并通过黑名单对相关命令（如“./”和“../”）进行限制。
内存马注入	内存马是一种新兴的木马技术，攻击者通过一些特殊的技术手段将木马注入到内存中，可以有效绕过WAF和主机防御的检测。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
任意文件删除	对于网站提供的文件删除功能，如果是直接通过绝对路径或目录穿越符对文件进行读取和下载，没有相关文件路径的限制，那么，攻击者就可以利用这种方式获取敏感信息，对服务器进行攻击。	请检查文件删除操作是否正常。如果异常，请检查函数的代码，并使用黑名单对传入参数（如“./”和“../”）进行限制。

攻击类型	说明	防护建议
任意文件读取	对于网站提供的文件下载和读取功能，如果是直接通过绝对路径或目录穿越符对文件进行读取和下载，没有相关文件路径的限制，那么，攻击者就可以利用这种方式获取敏感信息，对服务器进行攻击。	请检查文件读取操作是否正常。如果异常，请检查函数的代码，并使用黑名单对传入参数（如“./”和“../”）进行限制。
数据库弱口令	当数据库使用强度较低的密码时，攻击者可能通过暴力破解获取正确的数据库密码，从而达到窃取数据库数据、获取系统权限等目的。	请使用更复杂的密码。
线程注入	线程注入是一种通用的RASP绕过手段。当攻击者拿到代码执行权限后，可以通过新建线程的方式使RASP丢失掉运行环境的上下文，从而影响RASP的防御能力。	您的服务器可能存在代码执行漏洞。请检查漏洞的位置并限制执行代码的功能。
危险协议使用	若服务端进行访问的URL用户端可控，而应用本身又未对该URL的协议进行限制，那么攻击者可能通过File、NetDoc等危险协议对服务器上的敏感文件进行读取。	请对URL可以访问的协议进行限制。

3.8. 安全通告

3.8.1. Apache Log4j2远程代码执行漏洞（CVE-2021-44228）

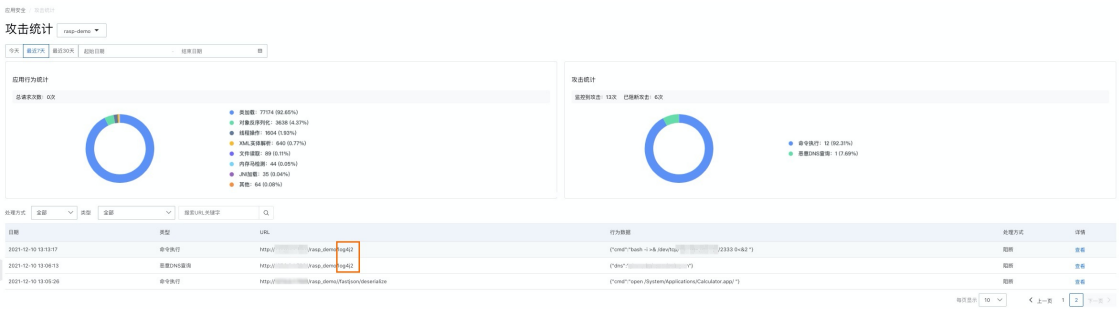
近日，阿里云计算有限公司发现阿帕奇Log4j2组件存在远程代码执行漏洞，并将漏洞情况告知阿帕奇软件基金会。

更多有关漏洞的详细信息，请参见【漏洞通告】Apache Log4j2 远程代码执行漏洞（CVE-2021-44228/CVE-2021-45046）。

您可以接入ARMS应用安全，开启一键防护，在运行时监控并阻断远程命令执行等攻击行为并上报。具体操作，请参见接入应用安全。将应用接入应用安全后，当应用受到Log4j2远程代码执行漏洞攻击时，应用安全会识别上报攻击行为事件。在应用安全的以下页面可以查看Apache Log4j2漏洞信息。

- 在ARMS控制台左侧导航栏，选择**应用安全 > 攻击统计**。

  如果存在攻击行为，在**攻击统计**页面可以查看Apache Log4j2漏洞的行为数据。



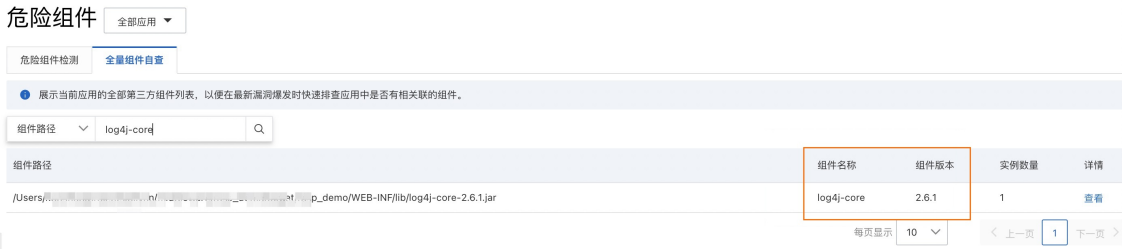
- 在ARMS控制台左侧导航栏，选择**应用安全 > 危险组件检测**。

在**危险组件检测**页签查看应用安全自动监测到的Apache Log4j2漏洞和提供的修复建议。

> **说明** 应用安全的危险组件检测针对第三方组件依赖自动分析关联CVE漏洞库并提供修复建议。

- 在ARMS控制台左侧导航栏，选择**应用安全 > 危险组件检测**，然后单击**全量组件自查**页签。

  在**全量组件自查**页签通过搜索查看所有接入应用是否包含Log4j组件，并确定Log4j组件的版本。



您还可以通过配置告警规则，通过短信、钉钉、邮件等渠道接收攻击告警通知。创建告警规则的操作，请参见使用应用安全告警规则。

应用安全默认的防护模式为监控模式，建议观察一段时间后调整防护模式为监控并阻断，一旦发生攻击行为可以直接阻断，保障应用安全运行。修改防护模式的操作，请参见设置防护模式。

相关文档

- 什么是应用安全

3.9. 访问控制

3.9.1. 应用安全服务关联角色

本文介绍应用安全服务关联角色AliyunServiceRoleForARMSSecurity以及如何删除该角色。

背景信息

应用安全服务关联角色AliyunServiceRoleForARMSSecurity是ARMS因为需要获取其他云服务的访问权限而提供的RAM角色。更多关于服务关联角色的信息，请参见服务关联角色。

AliyunServiceRoleForARMSSecurity应用场景

应用安全功能需要访问阿里云安全服务的资源时，可通过自动创建的应用安全服务关联角色AliyunServiceRoleForARMSSecurity获取访问权限。

AliyunServiceRoleForARMSSecurity权限说明

AliyunServiceRoleForARMSSecurity具备以下云服务的访问权限：

- 安全服务的访问权限

```
{
      "Action": [
        "yundun-waf:ModifyProtectionConfig",
        "yundun-waf:ModifyApplicationsRaspState",
        "yundun-waf:DescribeRiskDependencyStatisticsInfo",
        "yundun-waf:DescribeRiskDependencies",
        "yundun-waf:DescribeRiskCount",
        "yundun-waf:DescribeProtectionStatisticsInfo",
        "yundun-waf:DescribeProtectionConfig",
        "yundun-waf:DescribeMiddlewareInstances",
        "yundun-waf:DescribeDependencyInstances",
        "yundun-waf:DescribeDependencies",
        "yundun-waf:DescribeAttackStatisticsInfo",
        "yundun-waf:DescribeAttacks",
        "yundun-waf:DescribeAttackCount",
        "yundun-waf:DescribeAttackApplicationCount",
        "yundun-waf:DescribeApplications"
        "yundun-waf:GetRaspCommercialStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

删除AliyunServiceRoleForARMSSecurity

如果您使用了应用安全功能，然后需要删除应用安全服务关联角色AliyunServiceRoleForARMSSecurity（例如您出于安全考虑，需要删除该角色），则需要先明确删除后的影响：删除AliyunServiceRoleForARMSSecurity后，将无法正常查看应用安全相关页面。如需继续使用应用安全服务，则需要重新授权。

删除AliyunServiceRoleForARMSSecurity的操作步骤如下：

> **说明** 如果当前账号下存在应用已接入应用安全，请先取消接入并重启，然后再删除角色，否则会导致删除失败。应用取消接入的操作，请参见取消接入目标应用。

1. 登录RAM控制台，在左侧导航栏选择**身份管理 > 角色**。
2. 在**角色**页面的搜索框通过关键词搜索名称为AliyunServiceRoleForARMSSecurity的RAM角色。
3. 在右侧**操作**列，单击**删除**。
4. 在弹出的对话框单击**确定**。

常见问题

Q：为什么我的RAM用户无法自动创建ARMS服务关联角色AliyunServiceRoleForARMSSecurity?

A：RAM用户需要拥有指定的权限，才能自动创建或删除AliyunServiceRoleForARMSSecurity。因此，在RAM用户无法自动创建AliyunServiceRoleForARMSSecurity时，您需要为RAM用户添加指定自定义权限策略或名称为AliyunARMSFullAccess系统策略。

自定义权限策略和系统策略的使用场景如下：

- 指定自定义策略可以用于为只读RAM用户仅添加使用应用安全的权限。
- 名称为AliyunARMSFullAccess系统策略可以为RAM用户添加管理ARMS的所有权限（包括应用安全的使用

权限）。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**创建权限策略**页面，单击**脚本编辑**页签。
5. 在策略文档中输入以下自定义权限策略内容，然后单击**下一步**。

```
{
  "Statement": [{
    "Action": [
      "ram:CreateServiceLinkedRole"
    ],
    "Resource": "acs:ram:*:主账号ID:role/*",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "ram:ServiceName": [
          "security.arms.aliyuncs.com"
        ]
      }
    }
  }, {
    "Action": "arms:CreateSecurityAuth",
    "Effect": "Allow",
    "Resource": "*"
  }],
  "Version": "1"
}
```

> **说明** 请将 `主账号ID` 替换为您实际的阿里云账号（主账号）ID。

6. 填写策略*名称*，然后单击**确定**。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，为RAM用户添加权限。
   i. 选择授权范围为**整个云账号**。
   ii. 输入被授权主体。

   被授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。
   iii. 选择添加上一步创建的自定义权限策略或名称为AliyunARMSFullAccess的系统策略。
5. 单击**确定**。
6. 单击**完成**。

（可选）步骤一：创建自定义权限策略

步骤二：为RAM用户添加权限策略。

相关文档

- 服务关联角色

4.Insights

4.1. 什么是Insights?

Insights是一个对应用进行定时巡检的智能运维工具。针对巡检后发现的问题，Insights可以给出具体的根因分析和建议，同时支持订阅告警。

功能说明

Insights巡检问题主要针对应用性能指标RT（平均响应时间）、Error（应用错误数）、QPS（平均请求量）进行阈值检测校验。您无需做任何设置，Insights将会基于应用历史数据并结合智能算法完成巡检，同时您可以订阅不同的异常事件类型。

目前Insights支持巡检以下类型的事件。

事件类型	事件描述
应用服务整体平均响应时间突增	基于服务历史3小时数据，判断最近5分钟平均响应时间是否有异常突增点。目前服务支持按照HTTP、Dubbo、HSF和MQ进行分类查询，并给出具体根因结果。
应用服务整体错误率突增	基于服务历史3小时数据，判断最近5分钟应用错误率是否有异常突增点。目前服务支持按照HTTP、Dubbo、HSF和MQ进行分类查询，并给出具体根因结果。
Top N接口平均响应时间突增	默认对流量Top 5的服务进行检测，基于服务历史3小时数据，判断最近5分钟平均响应时间是否有异常突增点，并给出具体根因结果，具体巡检接口可以在巡检配置模块修改定制。更多信息，请参见巡检配置。
Top N接口错误率突增	默认对流量Top 5的服务进行检测，基于服务历史3小时数据，判断最近5分钟错误率是否有异常突增点，并给出具体根因结果，具体巡检接口可以在巡检配置模块修改定制。更多信息，请参见巡检配置。
流量不均	基于应用最近30分钟某个类型服务（HTTP、Dubbo、HSF）的流量数据，判断应用是否存在流量不均异常。默认单机5分钟流量不小于1000，默认最大流量和最小流量差30%。
Pod pending突增	基于集群10分钟内Pod pending事件量判断，默认情况集群10分钟内Pod pending事件量超过3个，就会对该集群的资源以及关联事件进行根因分析。

4.2. 查看Insights事件列表

Insights支持对不同地域的不同应用进行定时巡检，并且可以针对巡检到的事件给出具体的根因分析和建议。本文介绍如何查看Insights巡检结果。

前提条件

已创建应用监控，具体操作，请参见应用监控接入概述。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Insights > 事件列表**。
3. 在顶部菜单栏，选择地域。
4. 在页面右上角的时间选择框，选择需要查看的时间段。
5. 在事件列表页面顶部的下拉框选择需要查看的应用。

> **说明** 默认查看全部应用。

1. 登录ARMS控制台。
2. 在左侧导航栏，选择**应用监控 > 应用列表**。
3. 在顶部菜单栏，选择地域。
4. 在**应用列表**页面，单击应用名称。
5. 在左侧导航栏，单击**Insights**。
6. 在页面右上角的时间选择框，选择需要查看的时间段。
7. 在事件列表页面顶部的下拉框选择需要查看的应用。

应用服务整体平均响应时间突增

入口二

事件类型

事件类型区域显示了当前巡检到的事件对应的各事件类型的数量。

在**事件类型**区域，您可以执行以下操作：

- 选中或取消选中不同类型的事件，在**事件数**图表区域和事件列表区域将显示或隐藏对应类型的事件。事件类型的详细说明，请参见什么是Insights？。
- 单击**添加订阅**，可以订阅您关注的事件类型。当Insights巡检到目标事件类型的事件时，将会为您发送订阅通知。更多信息，请参见订阅规则。

事件数

事件数区域显示了所有事件类型在各时间点的分布情况。

在**事件数**区域，您可以执行以下操作：

- 将鼠标悬浮于柱状图上，查看对应时间点上各事件类型的具体事件数。
- 在柱状图上单击某个时间点，可以过滤目标时间点前后一段时间的事件。
- 单击柱状图下方的图例，可以隐藏或显示对应事件类型的数据。

事件列表

事件列表区域显示了所有事件对应的事件类型、描述、严重程度和异常开始时间。

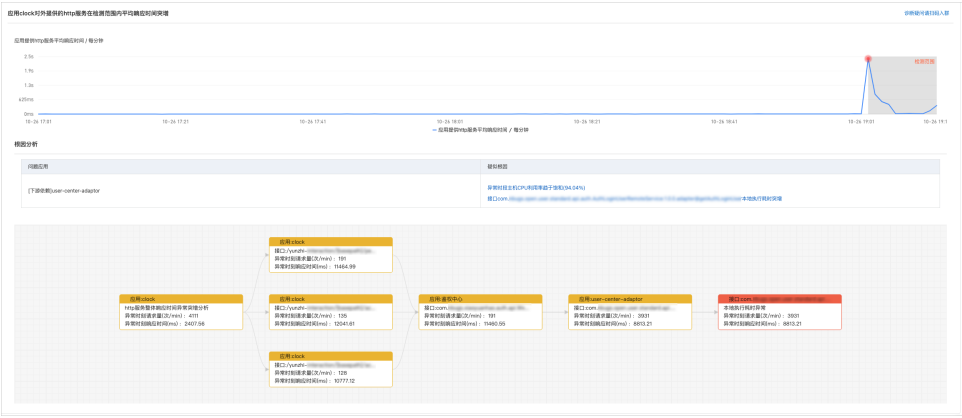
事件类型	描述	严重程度	异常开始时间	详情
应用服务整体平均响应时间突增	应用【[redacted]】【DUBBO】服务整体的响应时间在【2022-01-07 15:15:00】出现突增	P0	2022-01-07 15:15	查看详情
应用服务整体平均响应时间突增	应用【[redacted]】【MQ】服务整体的响应时间在【2022-01-07 15:12:00】出现突增	P0	2022-01-07 15:15	查看详情
TopN接口平均响应时间突增	应用【[redacted]】TOP服务【[redacted]Page】的响应时间在【2022-01-07 15:15:00】出现突增	P0	2022-01-07 15:15	查看详情
TopN接口平均响应时间突增	应用【[redacted]】TOP服务【[redacted]Status】的响应时间在【2022-01-07 15:14:00】出现突增	P0	2022-01-07 15:15	查看详情
TopN接口平均响应时间突增	应用【[redacted]】TOP服务【[redacted]NoLock】的响应时间在【2022-01-07 15:15:00】出现突增	P0	2022-01-07 15:15	查看详情
TopN接口平均响应时间突增	应用【[redacted]】TOP服务【[redacted]Code】的响应时间在【2022-01-07 15:15:00】出现突增	P0	2022-01-07 15:15	查看详情
应用服务整体平均响应时间突增	应用【[redacted]】【HTTP】服务整体的响应时间在【2022-01-07 15:10:00】出现突增	P0	2022-01-07 15:14	查看详情
应用服务整体平均响应时间突增	应用【[redacted]】【DUBBO】服务整体的响应时间在【2022-01-07 15:11:00】出现突增	P0	2022-01-07 15:14	查看详情
应用服务整体平均响应时间突增	应用【[redacted]】【HTTP】服务整体的响应时间在【2022-01-07 15:14:00】出现突增	P0	2022-01-07 15:14	查看详情
应用服务整体平均响应时间突增	应用【[redacted]】【MQ】服务整体的响应时间在【2022-01-07 15:12:00】出现突增	P0	2022-01-07 15:13	查看详情

在事件列表区域，您可以执行以下操作：

单击事件右侧**操作**列的**详情**，查看目标事件的详细信息。更多信息，请参见Insights详情。

Insights详情

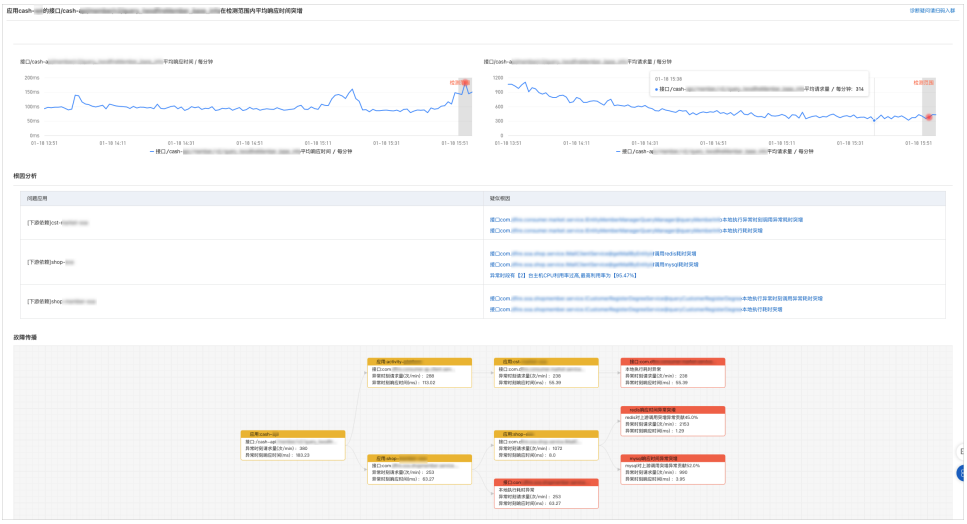
应用服务整体平均响应时间突增类型的事件详情页面显示了事件发生时间点、根因分析和故障传播链。



在Insights详情页面，您可以执行以下操作：

单击**根因分析**区域的疑似根因链接，在疑似根因面板可以查看事件产生的具体原因。

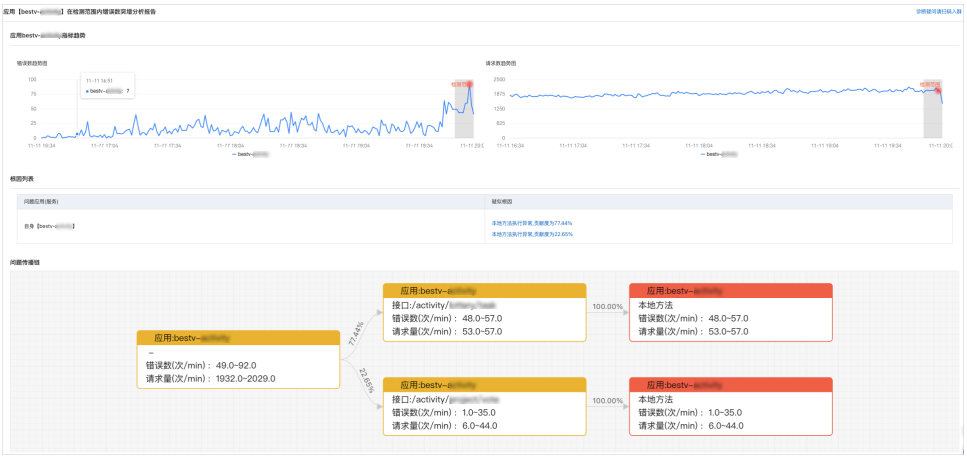
Top N接口平均响应时间突增类型的事件详情页面显示了事件发生时间点、根因分析和故障传播链。



在Insights详情页面，您可以执行以下操作：

单击**根因分析**区域的疑似根因链接，在疑似根因面板可以查看事件产生的具体原因。

应用服务整体错误率突增类型的事件详情页面显示了事件发生时间点、根因列表和问题传播链。



在Insights详情页面，您可以执行以下操作：

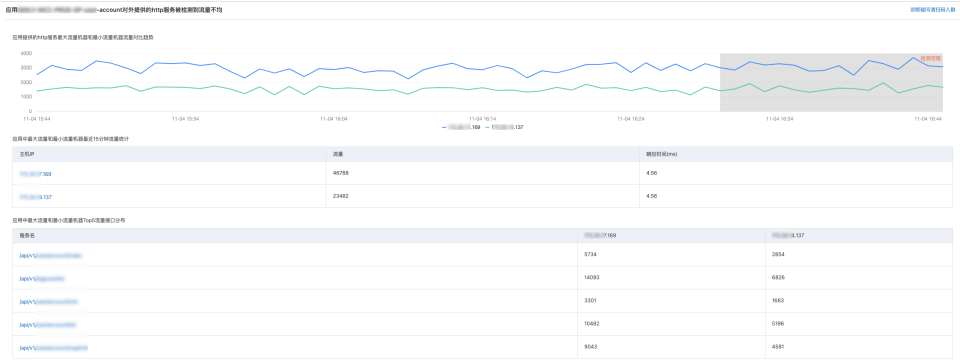
单击**根因列表**区域的疑似根因链接，在疑似根因面板可以查看事件产生的具体原因。

Top N接口错误率突增类型的事件详情页面显示了事件发生时间点、根因列表和问题传播链。

在Insights详情页面，您可以执行以下操作：

- 单击应用名称和接口名称链接，可以在应用监控的**应用详情**和**接口调用**页面查看对应应用和接口详情。更多信息，请参见应用概览和接口调用。
- 单击**根因列表**区域的疑似根因链接，在疑似根因面板可以查看事件产生的具体原因。

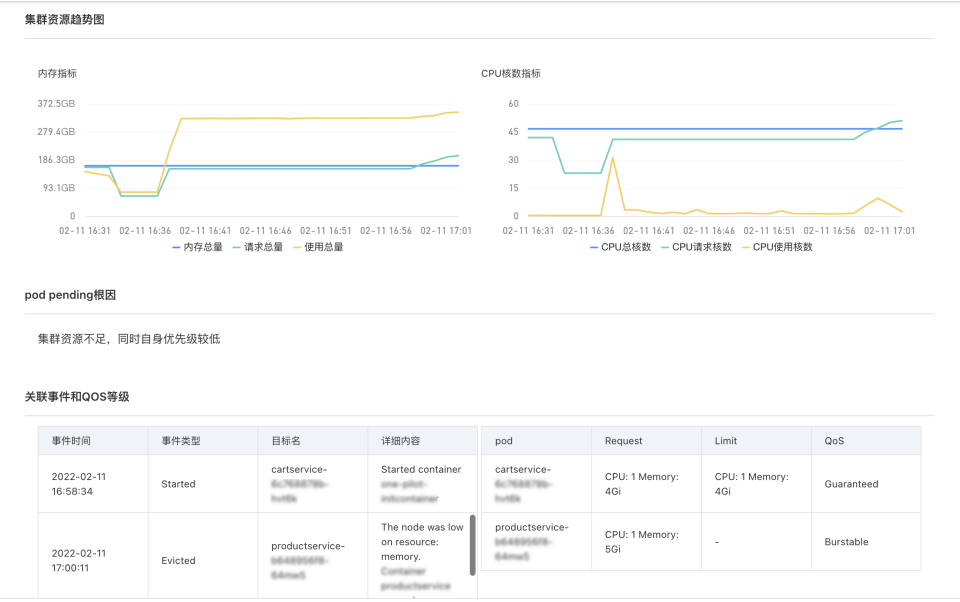
流量不均类型的事件详情页面显示了事件发生时间段、最大流量和最小流量近15分钟流量统计、最大流量和最小流量机器Top5流量接口分布。



在Insights详情页面，您可以执行以下操作：

- 单击最大流量和最小流量机器IP，可以在应用监控的**应用详情**页面查看对应机器的详情。更多信息，请参见应用概览。
- 单击接口分布区域的服务名，可以在应用监控的**接口调用**页面查看对应服务的详情。更多信息，请参见接口调用。

Pod pending突增类型的事件详情页面显示了最近30分钟内问题集群的内存和CPU总量、请求总量以及使用总量的趋势图，同时可以查看相应时间段内关联事件以及相应Deployment的配置信息。



Top N接口平均响应时间突增

应用服务整体错误率突增

Top N接口错误率突增

流量不均

Pod pending突增

4.3. 订阅配置

4.3.1. 订阅规则

Insights会基于系统默认设置或自定义设置对您名下的所有应用自动进行异常识别，发现任何异常都会根据您配置的订阅规则第一时间发送通知信息。

添加订阅

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Insights > 订阅配置**。
3. 在顶部菜单栏，选择地域。
4. 在**订阅配置**页面单击**订阅规则**。
5. 在**订阅规则**页签右上角单击**添加订阅**。
6. 在**添加订阅配置**面板设置以下参数，然后单击**确认**。

参数	说明
订阅配置名称	自定义订阅的名称。
事件类型过滤	选择需要发送通知的事件类型。 ○ 全部 ○ 应用服务整体平均响应时间突增 ○ Top N接口平均响应时间突增 ○ 应用服务整体错误率突增 ○ Top N接口错误率突增 ○ 流量不均
严重程度过滤	选择需要发送通知的事件严重程度。事件严重程度从P3、P2、P1、P0逐级上升。
应用过滤	选择需要发送通知的应用。
通知模式	○ 极简模式：通过设置联系人、通知方式和通知时段参数，指定通知方式。 ○ 高级模式：通过设置通知策略指定通知方式。
联系人	选择通知联系人，可以选择多个联系人或者联系人组。若没有联系人，则需先新建联系人。联系人支持手机号码、邮箱、钉钉机器人和Webhook等。具体操作，请参见联系人。
通知方式	订阅通知方式，支持多选。 **注意** 所选联系人需有对应的通知方式才能够生效。

参数	说明
通知时段	只在指定的时间段内产生的事件才会被发送，其它时间产生的事件会被忽略。
通知策略	○ 不指定通知策略：事件被巡检到时不会发送通知。 ○ 指定某个通知策略：事件被巡检到时，ARMS将会通过指定通知策略的通知方式发送通知信息。您可以选择已有的通知策略，也可以新建一个通知策略。更多信息，请参见通知策略。

启停订阅

如果您需要关闭或开启对应的订阅，在**订阅规则**页签单击目标订阅右侧对应的开关即可。

4.3.2. 查看订阅通知发送历史

Insights巡检到被订阅的事件后，将会通过订阅规则指定的通知方式发送告警通知。在**发送历史**页面，您可以筛选并查看所有通过订阅规则发送过的告警通知。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Insights > 订阅配置**。
3. 在**订阅配置**页面单击**发送历史**页签。

告警通知列表

发送历史页面显示了订阅规则发送过的告警通知列表。告警列表中主要参数如下，更多信息，请参见查看告警发送历史。

字段	说明
等级	Insights事件等级。
告警名称	Insights事件概述。
处理人	如果告警通知被认领将会显示认领告警的处理人。
通知策略	在订阅规则中，如果通知模式设置为极简模式，此处显示为具体联系人的分派规则；如果通知模式设置为通知策略，此处显示为具体的通知策略名称。
发生时间	事件产生的时间。
告警状态	告警通知目前的处理状态，共有以下3种状态： • 待认领 • 处理中 • 已解决

在**发送历史**页面，您可以执行以下操作：

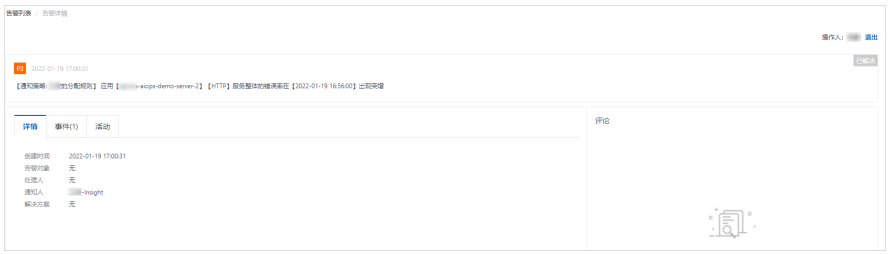
- 设置筛选字段，然后单击**搜索**，查看对应的告警发送历史。

> **说明** 打开更多开关，可以设置更多的过滤筛选字段。

- 单击告警名称，可以查看目标告警的详细信息。更多信息，请参见告警通知详情。
- 对于未解决的告警，可以认领、解决、指定告警处理人或修改告警等级。具体操作，请参见处理告警。

告警通知详情

告警详情页面显示了事件等级、发送信息、告警状态，以及告警基本信息、关联事件和活动记录。



在**告警详情**页面，您可以执行以下操作：

对于未解决的告警，可以认领、解决、指定告警处理人或修改告警等级。具体操作，请参见处理告警。

在**详情**、**事件**和**活动**页签可以分别查看以下信息：

- **详情**页签显示了告警创建时间、告警对象、处理人和通知人。
- **事件**页签显示了告警关联事件、事件创建时间和事件状态。单击事件名称，可以查看目标事件的详细信息。更多信息，请参见事件详情。

- **活动**页签显示了告警的活动记录。

事件详情

事件详情面板显示了事件的基本信息、监控数据和扩展字段。

单击事件地址链接，可以查看事件的分析报告。各类型事件的分析报告详情，请参见查看Insights事件列表。


事件详情

事件名称 应用【-aiops-demo-server-2】错误率突增
创建时间 2022-01-19 16:56:00
事件等级 P3
事件描述 应用【-aiops-demo-server-2】【HTTP】服务整体的错误率在【2022-01-19 16:56:00】出现突增
对象类型 无
事件对象 无
事件数量 1
事件状态 已恢复
开始时间 2022-01-19 16:56:00
结束时间 2022-01-19 17:06:00
事件地址 https://arms.
集成名称 ARMS-DEFAULT
集成类型 ARMS-Insights
告警类型 ARMS-Insights

监控数据

无数据

扩展字段

aiops.subscribeId: 2
severity: P3
_aliyun_arms_alert_type: 1919
_aliyun_arms_integration_name: ARMS-DEFAULT
alertname: 应用【-aiops-demo-server-2】错误率突增
_aliyun_arms_product_type: ARMS_INSIGHTS
_aliyun_arms_userid: 145
_aliyun_arms_integration_id: 2
_aliyun_arms_is_denoise_filtered: false

4.4. 巡检配置

Insights是一个对应用进行定时巡检的智能运维工具。针对巡检后发现的事件，Insights可以给出具体的根因分析和建议。Insight内置了多种巡检模块，您可以根据巡检需求定制模块参数。本文介绍如何修改巡检模块参数并管理巡检模块。

功能入口

1. 登录ARMS控制台。
2. 在左侧导航栏选择**Insights > 巡检配置**。
3. 在顶部菜单栏，选择地域。

在**巡检配置**页面可以查看Insights预置的巡检模块。目前，Insights支持以下3种巡检模块：

- 错误率突增巡检模块：使用系统内置的异常检测算法基于历史数据来自动判断应用错误率是否存在异常，

如果发现异常则会产生相应的异常事件并进行根因分析。

- 平均响应时间突增巡检模块：使用系统内置的异常检测算法基于历史数据来自动判断应用平均响应时间是否存在异常，如果发现异常则会产生相应的异常事件并进行根因分析。
- 流量分布巡检模块：基于应用最近15分钟某个类型服务（如HTTP、Dubbo、HSF）的流量数据，判断应用是否存在流量不均异常。默认单机5分钟流量不小于1000，默认最大流量和最小流量差30%。如果发现异常则会产生相应的异常事件并进行根因分析。

启停模块

Insights预置的巡检模块默认都是开启状态，如果您需要关闭指定模块，或开启已关闭的模块，在**模块管理**页签单击目标模块右侧对应的开关即可。

巡检模块关闭后，Insights将不会巡检对应类型的事件。各巡检模块对应的事件类型如下：

巡检模块	事件类型
错误率突增巡检模块	• Top N接口错误率突增 • 应用服务整体错误率突增
平均响应时间突增巡检模块	• Top N接口平均响应时间突增 • 应用服务整体平均响应时间突增
流量分布巡检模块	流量不均

修改模块参数

> **说明** 流量分布巡检模块暂不支持修改模块参数。

在**巡检配置**页面单击目标模块右侧**操作**列的**编辑**，在模块修改面板中修改参数后单击**确定**。

各巡检模块的参数说明如下：

错误率突增巡检模块

参数	说明
应用整体检测	• 开启：系统将检测应用整体的错误率是否异常。 • 关闭：不再触发相关功能。
Top N接口检测	• 开启：系统将根据设置的Top N参数，筛选出对应的接口，然后逐一检测每个接口的错误率是否存在异常。 • 关闭：不再触发相关功能。
额外接口	如果Top N接口无法满足您的巡检诉求，您可以在此处添加自己关心的接口。额外接口的优先级最高。
应用黑名单	如果某些应用完全不需要巡检，可以在此处添加。
接口黑名单	如果某些接口不需要巡检，可以在此处添加。优先级仅次于额外接口。

参数	说明
高级设置	
最小检测RT（ms）	当待检测的应用或接口的RT低于设置的阈值时，系统将不进行检查。
最小检测流量（qps）	当待检测的应用或接口的流量低于设置的阈值时，系统将不进行检查。
最小检测错误率（百分比）	当待检测的应用或接口的错误率低于设置的阈值时，系统将不进行检查。
异常阈值设定	系统检测到错误率升高，且当升高的情况满足下述任一条件时，系统都会生成异常事件并进行根因诊断。 • 异常持续时长（分钟）：当异常情况持续设置时间，才会被认定为有效异常，避免毛刺影响。 • 错误率增幅：当错误率增幅超过设置的阈值时，才会被认定为有效异常。 • 错误率大于（百分比）：当错误率大于设置的阈值时，才会被认定为有效异常。 • 错误数大于：当错误数大于设置的阈值时，才会被认定为有效异常。

平均响应时间突增巡检模块

参数	说明
应用整体检测	• 开启：系统将检测应用整体的平均响应时间是否异常。 • 关闭：不再触发相关功能。
Top N接口检测	• 开启：系统将根据设置的topN参数，筛选出对应的接口，然后逐一检测每个接口的平均响应时间是否存在异常。 • 关闭：不再触发相关功能。
额外接口	如果Top N接口无法满足您的巡检诉求，您可以在此处添加自己关心的接口。额外接口的优先级最高。
应用黑名单	如果某些应用完全不需要巡检，可以在此处添加。
接口黑名单	如果某些接口不需要巡检，可以在此处添加。优先级仅次于额外接口。
高级设置	
最小检测RT（ms）	当待检测的应用或接口的RT低于设置的阈值时，系统将不进行检查。
最小检测流量（qps）	当待检测的应用或接口的流量低于设置的阈值时，系统将不进行检查。
异常阈值设定	系统检测到RT升高，且当升高的情况满足下述任一条件时，系统都会生成异常事件并进行根因诊断。 • 异常持续时长（分钟）：当异常情况持续设置时间，才会被认定为有效异常，避免毛刺影响。 • RT增幅：当RT增幅超过设置的阈值时，才会被认定为有效异常。 • RT大于：当RT大于设置的阈值时，才会被认定为有效异常。

5.常见问题

本文汇总了使用ARMS时的常见问题。

ARMS子产品常见问题

- 应用监控常见问题
- 前端监控常见问题
- 常见问题概述
- App监控常见问题

一般使用常见问题

- ARMS报表数据可以在服务器保存多长时间？
- 如何查看消费账单？
- 如何查看资源包使用情况？
- 如何关闭应用监控Agent？
- 如何停止前端监控？

ARMS报表数据可以在服务器保存多长时间？

数据默认保存时间为半年。

如何查看消费账单？

1. 登录ARMS控制台。
2. 在顶部菜单栏选择**费用 > 费用账单**。
3. 在**费用账单**页面单击**账单明细**页签。
4. 在**账单明细**页签查看您的消费账单。

如何查看资源包使用情况？

1. 登录ARMS控制台。
2. 在顶部菜单栏选择**费用 > 费用账单**。
3. 在左侧导航栏选择**资源管理 > 资源包**，在**资源包总览**页签查看资源包概览。
4. 在**资源包管理**页面单击**使用明细**页签查看资源包使用明细。

如何关闭应用监控Agent？

在应用监控中，若您暂时不需要监控某个应用，则可以通过关闭该应用的Agent总开关来实现，具体操作步骤如下：

若您想恢复ARMS对该应用的监控，则打开该应用的Agent总开关即可。

1. 登录ARMS控制台。
2. 在左侧导航栏中选择**应用监控 > 应用列表**，并在**应用列表**页面顶部选择所在地域。
3. 在**应用列表**页面单击您想要停止计费的应用的名称。
4. 在左侧导航栏中单击**应用设置**。
5. 在**应用设置**页面单击**自定义配置**页签，在**Agent开关配置**区域关闭**Agent总开关**。

如何停止前端监控？

在前端监控中，若需停止对某个应用的前端监控，您可以将该应用从监控列表中删除。具体步骤如下：

> **警告** 此操作不可恢复，请谨慎操作。

1. 登录ARMS控制台。
2. 在左侧导航栏单击**前端监控**。
3. 在**前端监控**页面单击目标应用右侧**操作**列的**设置**。
4. 在**设置**页面单击**其他设置**页签。
5. 在**其他设置**页签单击**删除站点**，并在**操作确认**对话框中单击**确认**。

6.技术支持

如果您在使用ARMS的过程中有任何问题和建议，欢迎提交工单或通过钉钉联系我们。

- 如果在使用ARMS的过程中遇到问题，请首先查看什么是应用实时监控服务ARMS？并自助排查。
- 如果问题依旧存在，请提交工单。
- 如果需要获取进一步帮助，请联系我们的钉钉账号 `arms160804` 。