SOFAStack

AntStack Plus
使用指南

产品版本：AntStack Plus 1.11.0

文档版本：20220929

蚂蚁集团
ANT GROUP

法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

未经蚂蚁集团事先书面许可，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。

商标声明

蚂蚁集团 ANT GROUP及其他蚂蚁集团相关的商标均为蚂蚁集团所有。本文档涉及的第三方的注册商标，依法由权利人所有。

免责声明

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。蚂蚁集团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，并在蚂蚁集团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蚂蚁集团授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

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

1.什么是 AntStack Plus 10
2.云游 11
2.1. 什么是云游 11
2.2. 登录云游 Local 控制台 11
2.3. 控制台概览 12
2.4. 云游接入 IAM 15
2.4.1. 云游 Local 成员管理接入 IAM 15
2.4.2. 云游接入 IAM 审计功能 19
2.5. 租户切换 21
2.6. 概览 22
2.6.1. 环境概览 22
2.6.2. 工作台 23
2.7. 交付升级 24
2.7.1. 导入解决方案 24
2.7.2. 部署前置任务 25
2.7.3. 部署解决方案 25
2.7.4. 查看解决方案 29
2.7.5. 修改应用配置项 30
2.7.6. 一键部署 34
2.7.7. 自定义分组策略 37
2.8. 产品运维 39
2.8.1. 产品基线 39
2.8.1.1. 导出基线 39
2.8.1.2. 管理产品 41
2.8.1.2.1. 查看当前环境已部署的产品 41
2.8.1.2.2. 升级产品 42

2.8.1.2.3. 升级产品最佳实践 42
2.8.1.2.4. 卸载产品 45
2.8.1.2.5. 产品回滚 47
2.8.1.3. 管理应用 48
2.8.1.4. 管理容器 49
2.8.1.4.1. 查看容器 49
2.8.1.4.2. 变更容器配置 50
2.8.1.4.3. 容器内存与 JVM 堆内存配置比 52
2.8.1.4.4. 产品扩容 54
2.8.1.4.5. 产品缩容 55
2.8.1.4.6. 容器下线 56
2.8.1.4.7. 容器上线 58
2.8.1.4.8. 重启容器 60
2.8.1.4.9. 删除容器 60
2.8.2. 自动化测试 61
2.8.3. 查看全部发布单 65
2.8.4. 查看全部运维单 67
2.8.5. 伸缩组 69
2.8.6. 错误码 71
2.8.7. 无人值守 72
2.9. 资源管理 75
2.9.1. 管理应用容器 75
2.9.2. 管理数据库实例 76
2.9.2.1. 新增数据库实例 76
2.9.2.2. 查看数据库 76
2.9.2.3. 数据库规划最佳实践 78
2.9.3. 管理负载均衡 80
2.9.3.1. 新增负载均衡实例 80

2.9.3.2. 查看负载均衡 81
2.9.3.3. 修改负载均衡 82
2.9.4. 前端发布 84
2.9.5. 查看文件存储 86
2.9.6. 容器持久化存储 86
2.9.6.1. 查看容器持久化存储 86
2.9.6.2. 容器持久化存储最佳实践 87
2.9.7. 查看域名 90
2.10. 日志查询 91
2.10.1. 操作日志 91
2.11. 权限设置 92
2.11.1. 角色定义 92
2.11.2. 角色分配 93
2.11.3. 申请和审批角色 93
2.12. 环境管理 96
2.12.1. 新增环境 96
2.12.1.1. 基于阿里云底座 96
2.12.1.2. 基于物理机底座 102
2.12.2. 查看环境信息 109
2.12.3. 修改云游环境设置注意事项 111
2.13. 导出交付数据 112
2.14. 附录：基础术语 113
3.身份访问 IAM 115
3.1. 什么是 IAM 115
3.2. 登录 IAM 控制台 115
3.3. 查询账户信息 116
3.4. 账号管理 118
3.4.1. 账号管理 118

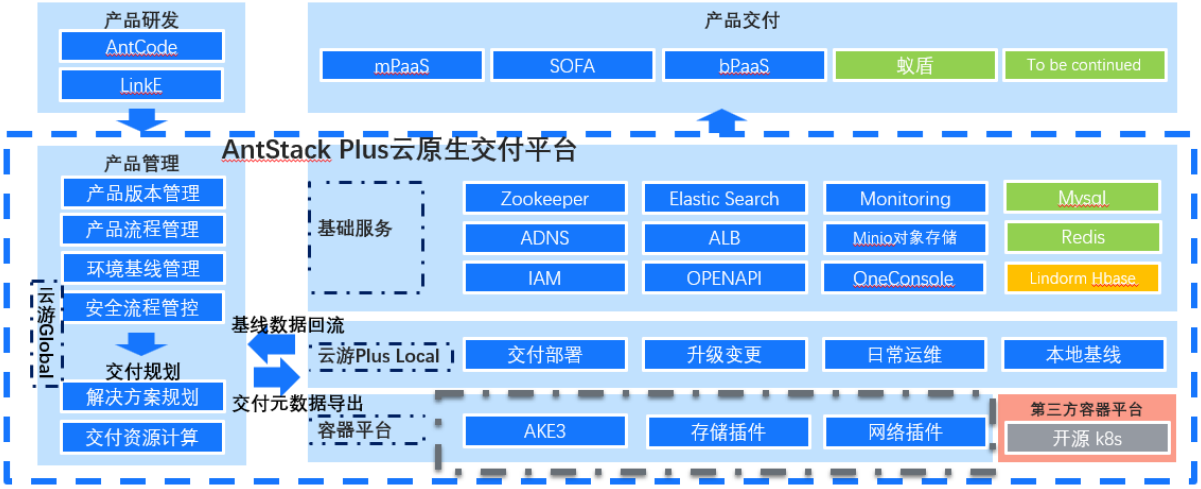
3.4.1.1. 管理租户成员 118
3.4.1.2. 管理租户成员组 121
3.4.1.3. 管理非租户内成员 122
3.4.2. 管理服务账号 123
3.4.3. 权限管理 125
3.5. 组织架构 127
3.5.1. 部门管理 127
3.6. 管理我的权限 129
3.7. 工单中心 130
3.8. 接入审批平台 131
3.9. 审计中心 137
3.9.1. 审计大盘 137
3.9.2. 操作审计 138
3.9.3. 关注订阅 138
3.9.4. 跟踪管理 139
3.9.5. 审计日志接入云盾 140
3.10. 替换产品 Logo 143
3.11. 附录：基础术语 146
4.容器底座 147
4.1. 什么是容器底座 147
4.2. 登录 Captain 控制台 148
4.3. 集群概览 149
4.4. 集群管理 150
4.4.1. 节点 150
4.4.1.1. 扩容节点 150
4.4.1.2. 查看节点 153
4.4.1.3. 设置节点调度状态 154
4.4.1.4. 管理节点标签 155

4.4.1.5. 节点的 Shell 操作 156
4.4.1.6. 删除节点 157
4.4.2. 管理命名空间 157
4.4.3. 预拉镜像 158
4.4.4. 查看操作记录 159
4.4.5. 调度回放 160
4.4.5.1. 安装调度回放组件 160
4.4.5.2. 查看调度回放 161
4.4.6. 集群容量预览 162
4.5. 工作负载 164
4.5.1. 部署（Deployments） 164
4.5.1.1. 创建部署 164
4.5.1.2. 编辑部署 167
4.5.1.3. 删除部署 167
4.5.2. 有状态副本集（Statefulsets） 167
4.5.2.1. 创建有状态副本集 167
4.5.2.2. 编辑有状态副本集 170
4.5.2.3. 删除有状态副本集 171
4.5.3. 守护进程集（Daemonsets） 171
4.5.3.1. 创建守护进程集 171
4.5.3.2. 编辑守护进程集 173
4.5.3.3. 删除守护进程集 174
4.5.4. 任务（Jobs） 174
4.5.4.1. 创建任务 174
4.5.4.2. 编辑任务 176
4.5.4.3. 删除任务 177
4.5.5. 容器组（Pods） 177
4.5.5.1. 创建容器 177

4.5.5.2. 编辑容器 179
4.5.5.3. 删除容器 180
4.6. 应用商店 180
4.6.1. 管理产品模板 180
4.6.1.1. 上传产品或产品集合模板 180
4.6.1.2. 编辑产品或产品集合模板 181
4.6.2. 产品实例 181
4.6.2.1. 发布产品 181
4.6.2.2. 查看已发布产品 183
4.7. 配置管理 183
4.7.1. 配置项 183
4.7.1.1. 创建配置项 183
4.7.1.2. 使用配置项 184
4.7.1.3. 修改配置项 185
4.7.1.4. 删除配置项 185
4.7.2. 保密字典 186
4.7.2.1. 创建保密字典 186
4.7.2.2. 管理保密字典 187
4.7.2.3. 删除保密字典 187
4.8. 网络 188
4.8.1. 创建网络 188
4.8.2. 查看网络详情 190
4.8.3. 删除网络 191
4.9. 查看运维单 191
4.10. 附录：基础术语 192

1.什么是 AntStack Plus

AntStack Plus 是蚂蚁集团产品的基础，可以提供容器部署底座、云游交付平台等服务，保障蚂蚁金融云产品更加高效，稳定、安全的输出，为客户提供更加良好的交付体验。



AntStack Plus 包含如下组件：

- 云游 Plus：金融科技的一站式专有云规划、交付、运维平台，管理专有云从诞生到落地的整个生命周期。
- 容器底座：包含容器引擎 AKE 云原生平台（AKE3） 和容器管控平台 Captain Plus。
  - AKE3：使用开源 Kubernetes+Containerd 技术，将底层物理资源按照计算、网络、存储等进行切分和抽象的容器引擎。
  - Captain Plus：原生 K8s 容器引擎管控平台，用于管控 AKE3。
- 身份访问 IAM：用于管理租户成员、成员组以及服务账号，并根据角色自定义各成员的操作权限。
- OpenAPI 平台：可以查询和回溯用户操作行为。
- ONECONSOLE：全功能前端基础组件库。
- AntStack DNS：为平台内的应用提供稳定高可用的 DNS 域名注册和解析服务。

2.云游

2.1. 什么是云游

云游是蚂蚁集团提供的一站式专有云规划、交付、运维平台，管理着蚂蚁产品从诞生到落地的整个生命周期，由云游 Global 与云游 Local 两部分共同组成。

云游旨在通过自动化、智能化的工具平台，解决专有云交付中三大痛点：

- 多环境部署带来的重复性工作。
- 手工部署引发的低效和易出错。
- 需要同时使用多个系统平台操作繁琐。

云游的工作周期可以分为如下四个阶段：

1. 云产品准备期

   准备产品部署所需的所有配置信息。每一个产品版本包含应用镜像、部署所需的资源（服务器、负载均衡、数据库、文件存储、缓存）、产品依赖信息（被依赖的产品也在云游上）、API 信息（供其他产品调用）、启动和部署参数、健康检查配置、发布日志等。每一个产品版本在部署到实际生产环境之前，都需要云游 Global 上进行模拟部署及功能验证，以确保产品版本的可用性和稳定性。

2. 解决方案规划期

   按照客户需求，综合考虑客户环境的硬件网络情况、所选云底座和过往部署情况，从云游 Global 上选择合适的云产品并确定其版本、拓扑和规格，量身定做一份解决方案。解决方案中将会自动汇总所有产品的部署信息，并由交付工程师从实施角度确认解决方案的可行性。

3. 建站部署期

   为客户项目搭建对应的环境，安装云游。通过 AKE 云原生平台（AKE3）集群管控平台初始化集群并添加节点，准备好相应的容器资源。在云游 Local 上导入制作好的解决方案后，根据实际需要，执行应用部署、扩容和缩容、自动化测试等子任务，最终将环境升级到解决方案指定的终态。交付完成后，发布成功的所有产品及其版本、拓扑、规格信息将形成当前环境的基线信息，用于后续的产品运维。基线信息通过文件回传到云游，为下一次产品交付或升级提供基础。

4. 运维期

   建站部署完成后，您可以在云游 Local 上完成日常的运维操作，如应用上线、下线、重启、扩容、缩容，以及资源查询与信息查看等操作。

2.2. 登录云游 Local 控制台

云游是蚂蚁集团的一站式专有云规划、交付、运维平台，管理着蚂蚁集团产品从诞生到落地的整个生命周期。本文介绍如何登陆云游控制台。

前提条件

- 已获得云游的 IP 地址或服务域名。
- 已拥有蚂蚁集团账号，并获得云游的相应角色。

操作步骤

1. 打开浏览器。

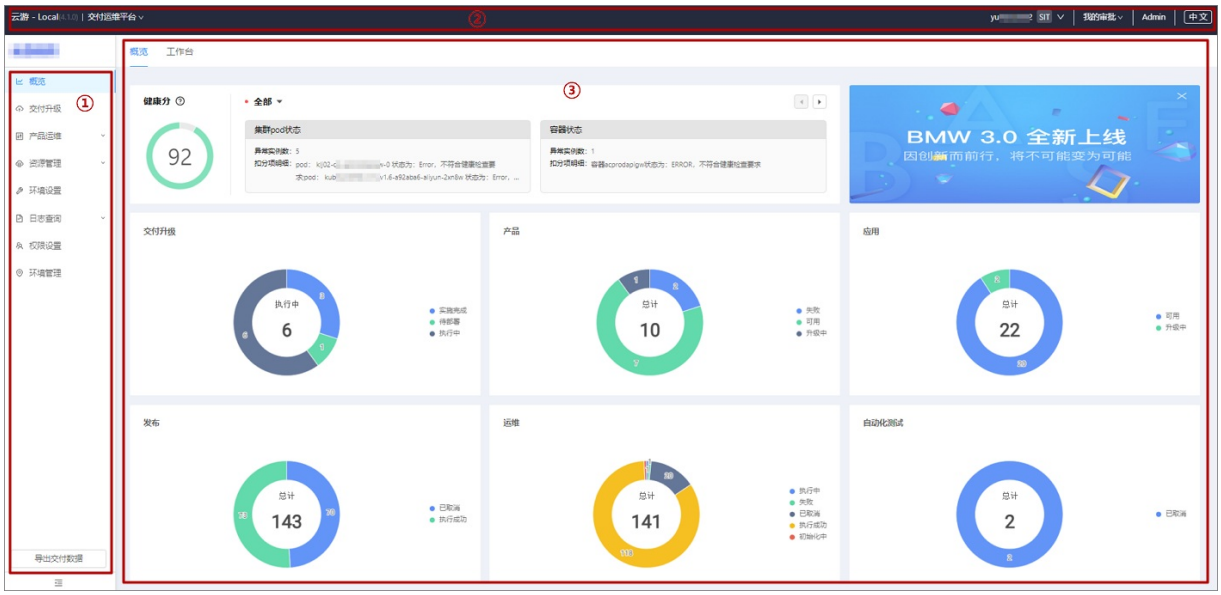
   推荐使用 Google Chrome。

2. 在地址栏输入云游 Local 的 IP 地址或服务域名。
3. 输入正确的用户名和密码后单击 **登录**。

2.3. 控制台概览

云游是蚂蚁集团的一站式专有云规划、交付、运维平台，管理着蚂蚁集团产品从诞生到落地的整个生命周期。本文介绍云游 Local 控制台的基本功能。

云游 Local 控制台主界面如下图所示：



云游 Local 主界面分为左侧导航栏（图示中①）、上方菜单栏（图示中②）、操作区（图示中③），各板块功能说明如下表所示。

区域	功能	说明
	概览	查看环境的概览信息和待完成工作。
	交付升级	导入解决方案、查看解决方案详情和部署解决方案。
	产品运维	查看和执行产品的运维操作。主要包括以下模块： • **产品基线**：查看、发布、导出产品基线，并进行自动化测试、容器上线、下线、扩容、缩容、变配，产品卸载等操作。 • **自动化测试**：用于批量测试产品。 • **全部发布单**：查看发布单的名称、类型、创建时间、创建人、状态等信息。 • **全部运维单**：查看运维单的名称、类型、创建时间、创建人、状态等信息。

左侧导航栏	**资源管理**	查看当前环境内的所有资源。主要包括以下模块：
		• **应用容器**：按产品、应用维度，查看所有容器（不包含集群中的系统容器）。
		• **数据库**：
		  ○ **物理实例视角**：以数据库物理实例为维度，查看所有数据库信息。
		  ○ **Schema 视角**：以数据库 Schema 为维度，查看所有数据库信息。
		• **负载均衡**：查看所有负载均衡信息。
		• **文件存储**：查看所有文件存储信息。
		• **前端发布**：用于快速发布前端项目。
		• **容器持久化存储**：查看容器存储的存储卷、存储类和存储声明。
		• **域名**：查看当前环境所有域名。
		• **证书**：管理 HTTPS 证书。

	环境设置	查看或编辑云游 Local 的环境配置。
	日志查询	查看云游 Local 控制台的产品日志和操作日志。 • **操作日志**：云游 Local 上每一个非查询类操作，如取消、跳过、上线、下线、删除、编辑等，均会记录操作内容、操作人、操作时间、后台请求，以便追踪使用情况、定位问题。 • **产品日志**：云游 Local 上发布的产品均会记录产品运行的相关日志。
	权限设置	用于将云游 Local 的权限管理接入 IAM，并对用户进行权限设置。
	环境管理	用于新增和管理环境信息。
	导出交付数据	导出包含产品基线或产品指标信息的 JSON 文件。
上方菜单栏	环境信息区	显示云游 Local 的基本信息，如云游 Local 版本、站点名称等。
	我的审批	显示当前用户的审批任务，按“**我发起的**”、“**待处理**”和“**已处理**”分类显示。 当有待处理任务时，会显示任务数量。

	登录用户信息区	显示当前登录的用户。 单击角色信息下拉列表中的 **+申请角色** 按钮可以提交相应的角色申请。
	语言栏	单击语言栏的按钮可以切换控制台语言，目前支持中文和英文。
操作区		当您选择左侧导航栏的任意功能后，该功能配置和操作的界面就会显示在操作区中，您可以根据需求进行操作。

2.4. 云游接入 IAM

2.4.1. 云游 Local 成员管理接入 IAM

云游 Local 1.13.0 及以上版本

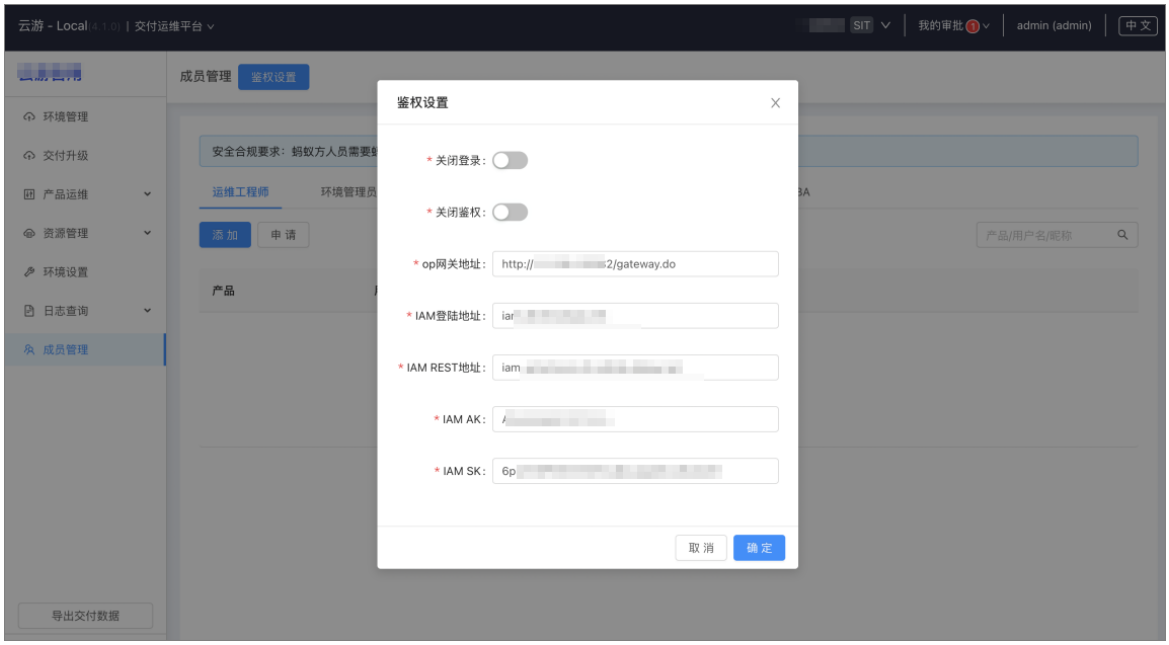
注意

- 自 1.13.0 版本开始，云游 Local 支持多租户功能。
- 自 1.13.0 版本开始，调用云游 Lcoal 的 API 可以使用内嵌的 gateway，但更推荐通过 OP 来调用。

1. 在 IAM 的 ROC 租户下，为云游创建一个服务账号并授予租户管理员角色。

   创建服务账号及获取 AK（AccessKey ID）、SK（AccessKey Secret） 的方法请参见 IAM 使用指南中《管理服务账号》的内容。

2. 登录云游 Local 控制台。
3. 在左侧导航栏单击 **权限设置**，然后单击 **鉴权设置**。
4. 配置以下参数后，单击 **确定**。



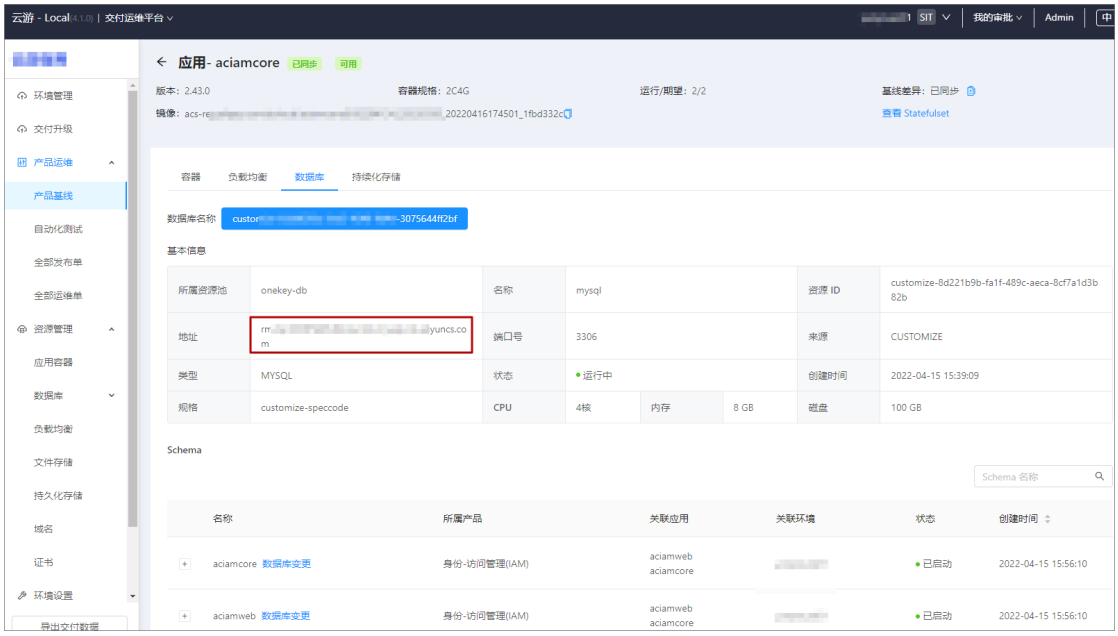
参数	说明
关闭登录	选择是否通过 IAM 登录。 选择开启。
关闭鉴权	选择是否通过 IAM 鉴权。 选择开启。
op 网关地址	配置当前环境的 OP（OpenAPI） 的 LB。格式为： `http://{当前环境的 OP的 LB（必须是域名）}/gateway.do` 。
IAM 登录 地址	当前环境 IAM 控制台的 LB 域名（必须是域名）。
IAM REST 地址	当前环境的 aciamcore 应用的内网 LB 域名（必须是域名）。
IAM AK	云游服务账号的 AK。
IAM SK	云游服务账号的 SK。

5. 单击 **确定**。

云游 Local 1.13.0 之前版本

> **注意**
>
> 云游 Local 1.13.0 版本以下版本，调用云游 Lcoal 的 API 需访问内嵌的 gateway。

1. 元数据初始化。
   i. 在云游 Local 上完成 IAM 的部署和验证。
   ii. 在云游 Local 上获取 IAM 产品的 aciamcore 数据库的相关连接信息。



iii. 通过 MySQL 命令行初始化云游相关角色权限元数据到 aciamcore 数据库中。

```
mysql -P${db_port} -h${db_url} -u${db_user} -p${db_password} --default-character-set='utf8' aciamcore < aciamcore_init.sql
```

参数说明如下：

参数	说明
${db_port}	填写 aciamcore 的数据库访问端口。
${db_url}	填写 aciamcore 的数据库地址。
${db_user}	填写 aciamcore 的数据库用户名。
${db_password}	填写 aciamcore 的数据库访问密码。
aciamcore_init.sql	是具体的初始化 SQL 文件。单击 aciamcore_init_v1 4.sql.zip 下载该文件。

示例如下：

```
mysql -P3306 -h172.**.**.28 -uaciam**** -pPaaS1**** --default-character-set='utf8' aciamcore < aciamcore_init.sql
```

2. 开启登录鉴权。

元数据初始化完成后，您可以调用以下 API 开启云游的鉴权。

```
curl -i -v -X PUT -H 'Content-Type:application/json' http://${yunyou_ip}:81/api/ops/system-params/open-auth -d '{"noLogin":false,"noAuth": false,"restUrl":"${aciamcore_vip}", "loginUrl":"${aciamweb_domain}"}'
```

参数说明如下：

参数	说明
${yunyou_ip}	填写云游 Local 的 IP 地址。
${aciamcore_vip}	填写当前环境 aciamcore 应用的内网 VIP，例如：10.0.0.1
${aciamweb_domain}	填写当前环境 IAM 控制台的访问域名。

参数	说明
isNoLogin	是否开启 IAM 登录，取值如下： ○ true：不开启 IAM 登录。 ○ false：开启 IAM 登录。 此项填写为 false。
isNoAuth	是否开启 IAM 鉴权，取值如下： ○ true：不开启 IAM 鉴权。 ○ false：开启 IAM 鉴权。 此项填写为 false。

示例如下：

```
curl -i -v -X PUT -H 'Content-Type:application/json' http://192.168.2.227:81/api/ops/system-params/open-auth -d '{"noLogin":false,"noAuth":fasle,"restUrl":"192.168.2.48","loginUrl":"admin.****.aliyuncs.com"}'
```

API 访问成功后，预计 1 分钟内生效。

> 说明
>
> ○ 您也可以在 apyunqing 数据库中开启鉴权，命令如下：
>
> ```
> update system_parameter set value='{"noLogin":false,"noAuth":fasle,"restUrl":"192.168.2.48","loginUrl":"admin.****.aliyuncs.com"}'  where type='auth_config';
> ```
>
> ○ 如果您后续不再通过 IAM 鉴权，可在 apyunqing 中执行如下命令关闭：
>
> ```
> update system_parameter set value='{"noLogin":true,"noAuth": true}' where type='auth_config';
> ```

2.4.2. 云游接入 IAM 审计功能

> 说明
>
> 云游 Local 1.10.0 及以上版本支持接入 IAM 审计功能。本文以云游 Local 1.10.2 版本为例，请根据实际情况修改版本。

准备工作

- 下载 apyunqingplus 镜像。

```
docker run --net=host -d -v /home/yunyou/staticfiles:/home/staticfiles acs-reg.alipay.com
/acloud/apyunqingplus:EI62154649_20211122_20211122161132_cdd9ca69
```

- 下载 apyunqingsetup 镜像。

```
docker run --net=host -d -v /home/yunyou/staticfiles:/home/staticfiles acs-reg.alipay.com
/acloud/apyunqingsetup:master_20211022091743_dcb7629d
```

- 备份 apyunqing 的数据库。
- 导入云游 Plus 1.10.2 的镜像到镜像仓库。

```
docker push acs-reg.alipay.com/acloud/registry:1.1
```

升级云游

1. 登录云游 Local 服务器。
2. 进入 `apyunqing-compose` 目录。

   ```
   cd /home/yunyou/staticfiles/apyunqing-compose
   ```

3. 修改 `apyunqing-compose` 目录下的 `config.json` 文件。

   在 `config.json` 中添加以下环境变量：

   ```
   "ANTCLOUD_SOFA_iam_customer_id=0000000001",
   "ANTCLOUD_SOFA_audit_address=iamcore.jr.alipay.net",
   ```

   `audit_address` 对应地址为可用的 aciamcore 地址。

4. 升级云游 Plus 镜像。

   ```
   python yunqing-setup.py y --image <apyunqingplus 镜像>
   ```

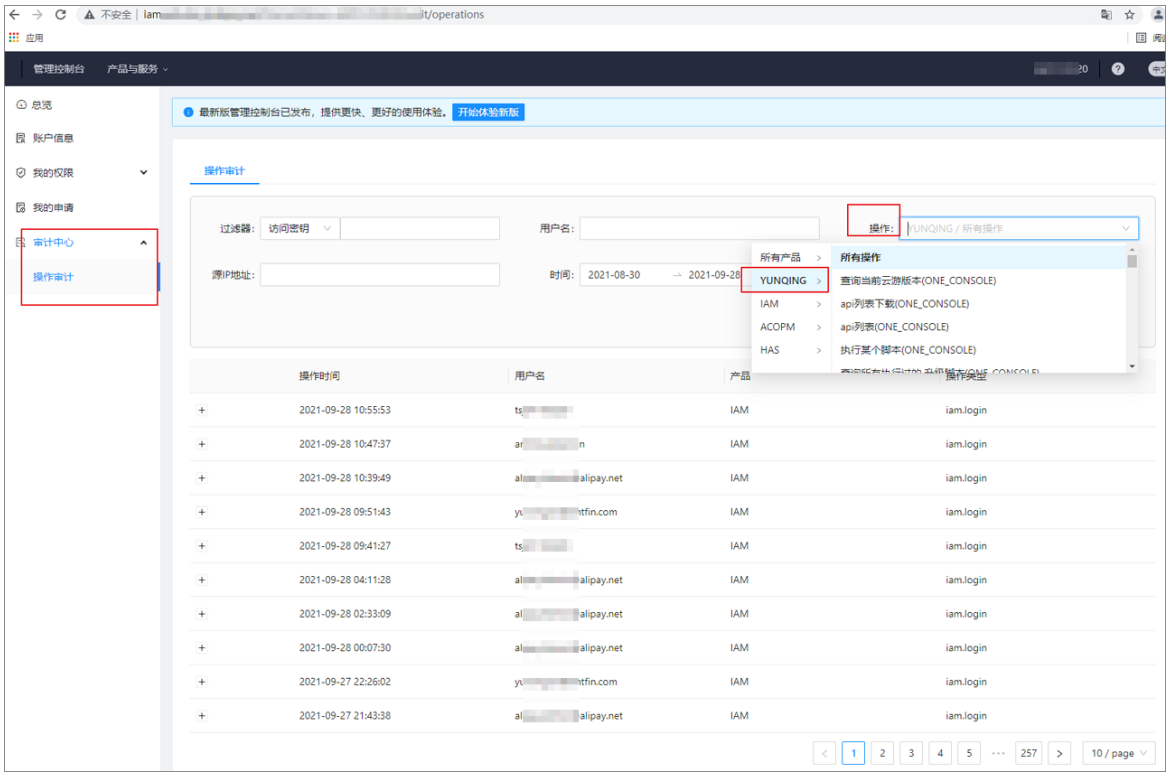
导入审计元数据

1. 下载 SQL 脚本。
   - operation_type.sql
   - operation_type_onex_extra.sql
2. 在对应环境的数据库 aciamcore 中执行步骤 1 下载的 SQL 脚本来导入已经准备好的审计元数据。

查看审计结果

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **审计中心 > 操作审计**。

3. 在 **操作** 区域选择 **YUNQING**。



附录：回滚方案

1. 登录云游 Local 服务器。
2. 使用之前镜像对云游 Local 进行回滚。

```
cd /home/yunyou/staticfiles/apyunqing-compose
## 回滚云游 Plus 镜像
python yunqing-setup.py y --image <apyunqingplus 上一版本镜像>
```

3. 还原数据库。

```
mysql -uapyunqing -pAntcloud2018 -h127.0.0.1 apyunqing < apyunqing.dump --force
```

2.5. 租户切换

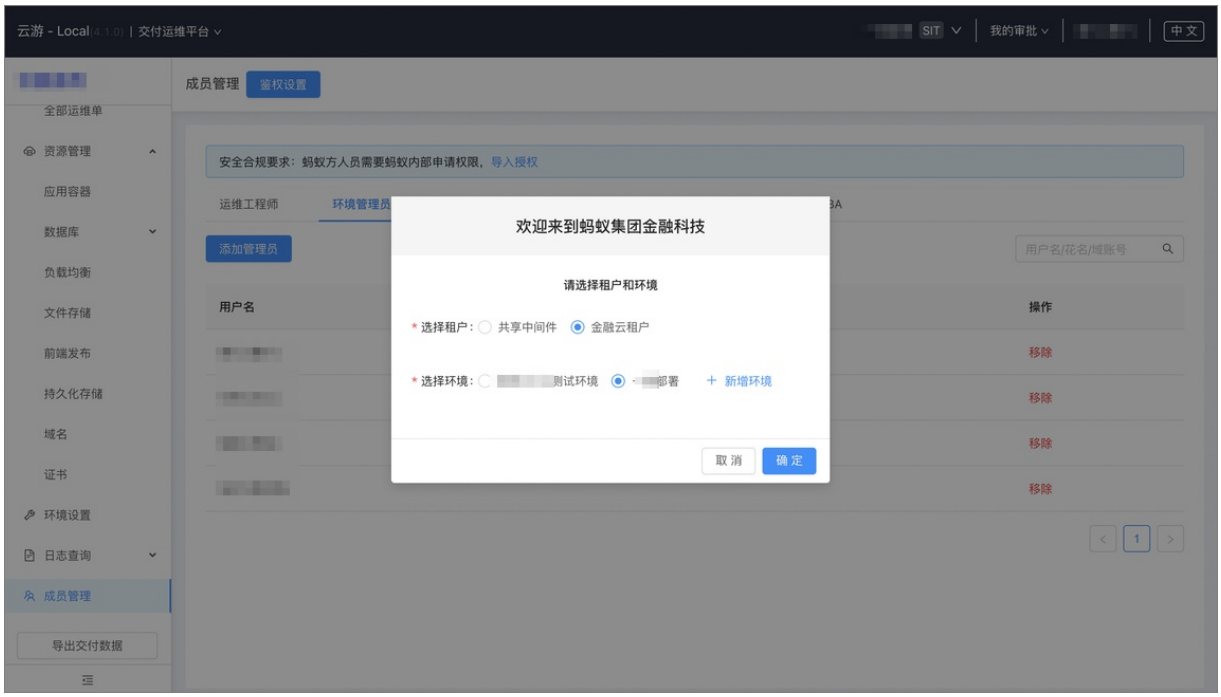
云游 Local 在 1.13.0 及以上版本增加了租户管理功能，多租户成员可以在自由切换租户。

前提条件

- 云游 Local 成员管理已接入 IAM。操作方式，请参见 云游 Local 成员管理接入 IAM。
- 用户在云游 Local 中已绑定云游角色。操作方式，请参见 角色分配 或 申请和审批角色。
- 用户在 IAM 中属于多个租户。更多信息，请参见 管理租户成员。

操作步骤

登录云游 Local 的用户在 IAM 中属于多个租户，就可以切换租户。例如下图中测试账号属于 **共享中间件** 和 **金融云租户** 这两个租户，则可以通过单击租户信息进行租户的切换。

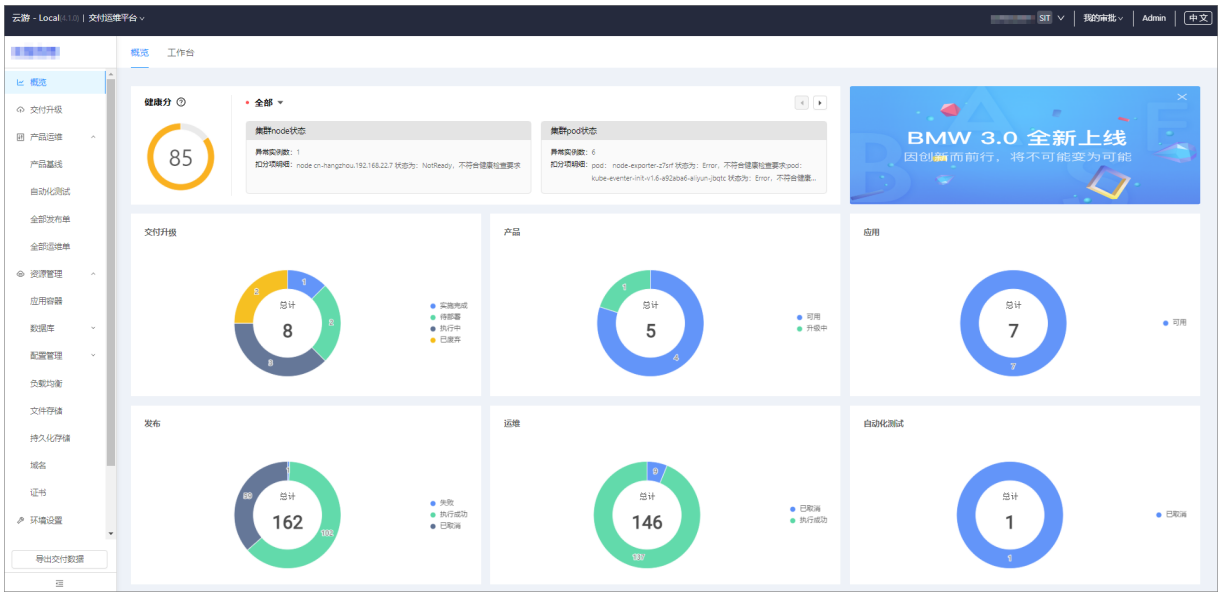


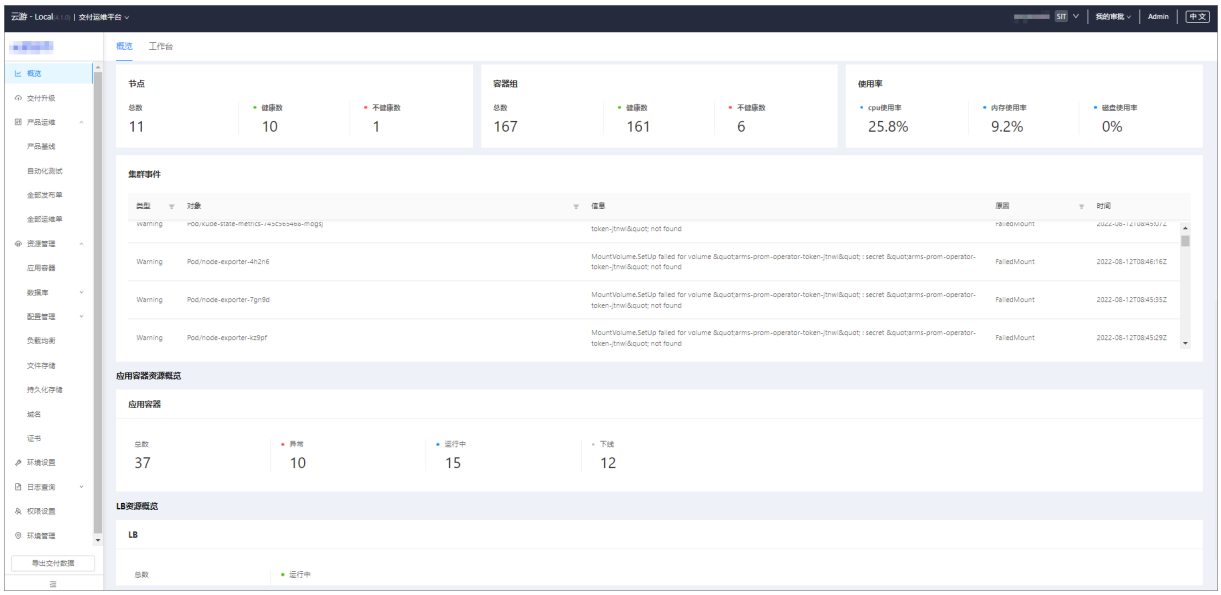
2.6. 概览

2.6.1. 环境概览

您可以通过云游 Local 概览页查看您的应用的总体情况。

您可以在概览页面查看如下信息：





健康分

云游 Local 根据当前集群状态、环境参数、产品状态、发布单状态等信息为当前环境计算的分数，您可以在右侧区域查看到所有的异常状态信息。

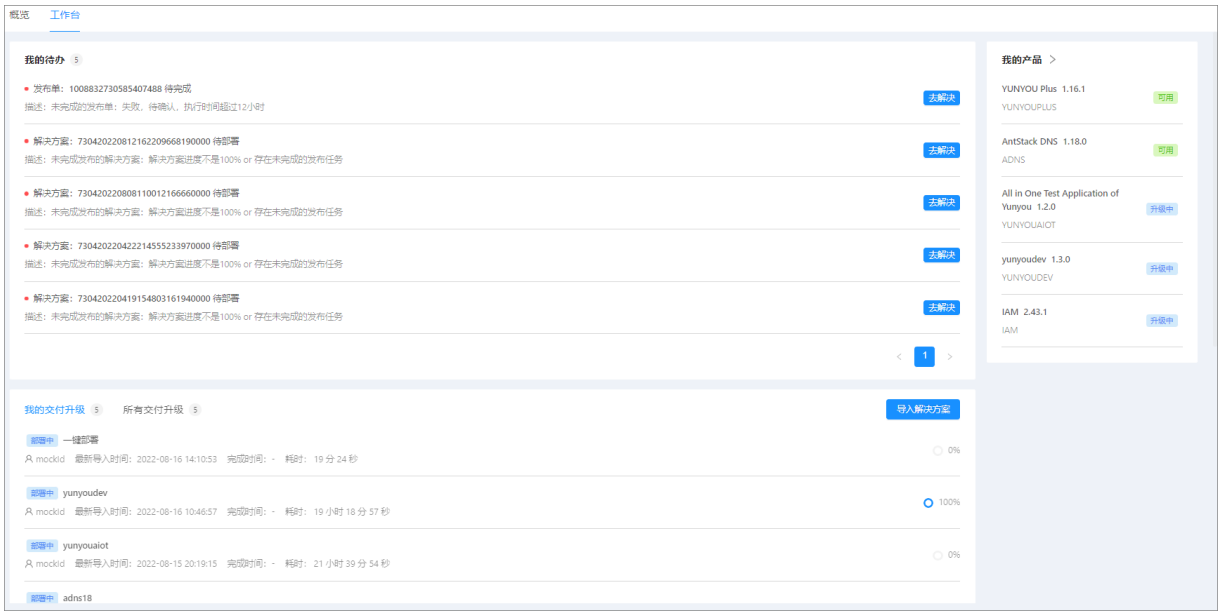
资源状态

您可以查看当前环境所有资源的统计情况，包括解决方案的状态统计、产品和应用的状态统计、集群资源概览、集群事件、应用容器资源概览、LB 资源概览。

2.6.2. 工作台

云游 Local 提供工作台功能，您可以直观的查看当前待完成的事项、解决方案和产品的状态等信息。

您可以在工作台页面查看如下信息：



我的待办

展示当前所有的待办信息，单击去解决，可直接跳转到待办事项位置。

我的产品

查看当前环境下，自己管理的所有产品。单击产品名称可跳转到产品的详情页面。

我的交付升级/所有交付升级

展示当前环境自己管理的解决方案，单击解决方案名称可直接跳转到解决方案详情页。

我的发布单/我的运维单/我的自动化测试

展示当前环境创建的发布单、运维单和自动化测试，单击任务名称可直接跳转到相关单据的详情页。

2.7. 交付升级

2.7.1. 导入解决方案

本节介绍如何导入解决方案到云游 Local 环境。

前提条件

已联系蚂蚁科技技术支持获取到解决方案文件。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，单击 **交付升级**。
3. 单击 **导入解决方案**。
4. 单击 **点击或拖拽上传** 按钮选择目标 JSON 文件或以直接拖拽的方式上传 JSON 文件。

上传完成后，云游会自动将解决方案拆箱并反馈拆箱结果。如果拆箱成功，页面会自动跳转至解决方案详情页。

2.7.2. 部署前置任务

前置任务是在部署解决方案之前必须完成的事项，否则会导致部署任务失败或卡住无法进行。

部署前置任务时，需确认以下信息：

- 确认参数配置

  确认参数配置正常，无冲突、无漏填参数。

- 确认镜像配置

  确认解决方案中所有应用镜像已正确上传到镜像中心，没有错误或遗漏。

- 确认负载均衡规划

  直接确认即可。

- 确认数据库规划
  - 确认数据库规划，完成复用数据库的设置。如果不需要复用则不用编辑任何内容，可以直接确认。
  - 确定解决方案中的每个新增的 Schema 应该部署到哪个数据库实例。
  - 确定需要共用一个数据库实例的 Schemas。
  - 已经部署成功的 Schema，不支持转移到另外的数据库实例。

- 确认解决方案是否需要使用用户自有的 MySQL 数据库

  梳理解决方案中有 Schema 需要用到客户的 MySQL 数据库的 Schema，与数据库管理员（DBA）沟通后在数据库中预先创建同名 Schema、账号和密码。

2.7.3. 部署解决方案

本文介绍如何在云游 Local 中部署解决方案。

背景信息

当解决方案导入到云游 Local 后，云游 Local 会对解决方案中是否有需要发布的应用、是否需要对应用进行扩容或缩容、是否需要降级、是否需要改拓扑等情况进行判断，识别计算出和基线的差异。针对识别出的差异，云游 Local 会生成一个或多个任务，并根据任务的不同类型采用不同的执行单完成部署。具体如下表所示：

任务名称	产生条件	完成方式（执行单类型）
扩容	解决方案中的容器数量比基线中的多。	运维单
缩容	解决方案中的容器数量比基线中的少。	运维单
应用部署	解决方案中应用镜像或应用参数与基线中不一致。	发布单
容器变配	解决方案中容器规格与基线中不一致。	运维单
自动化测试	解决方案中包含自动化测试镜像，且应用已完成部署。	测试单

通过部署任务的机制，您可以完成以下操作：

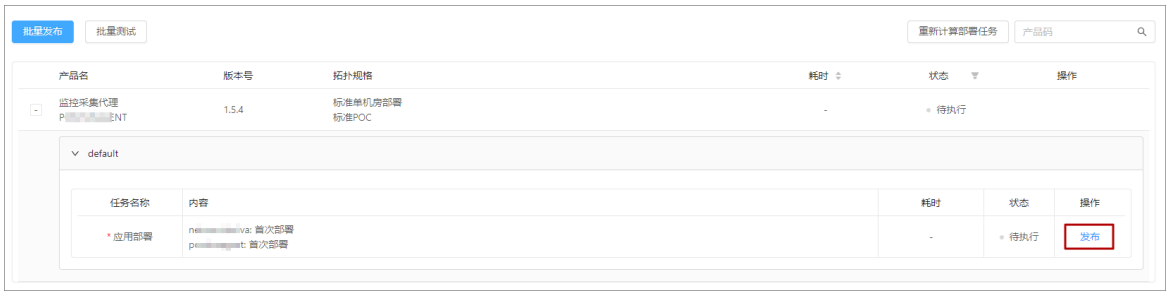
- 在实际部署前，提前预判此次交付中会产生哪些变化。
- 在进行多产品集成测试时，灵活地编排发布、调整测试顺序和控制部署节奏。

> **注意**
>
> 更新解决方案或者产品基线发生变化时，云游 Local 会自动计算部署任务。

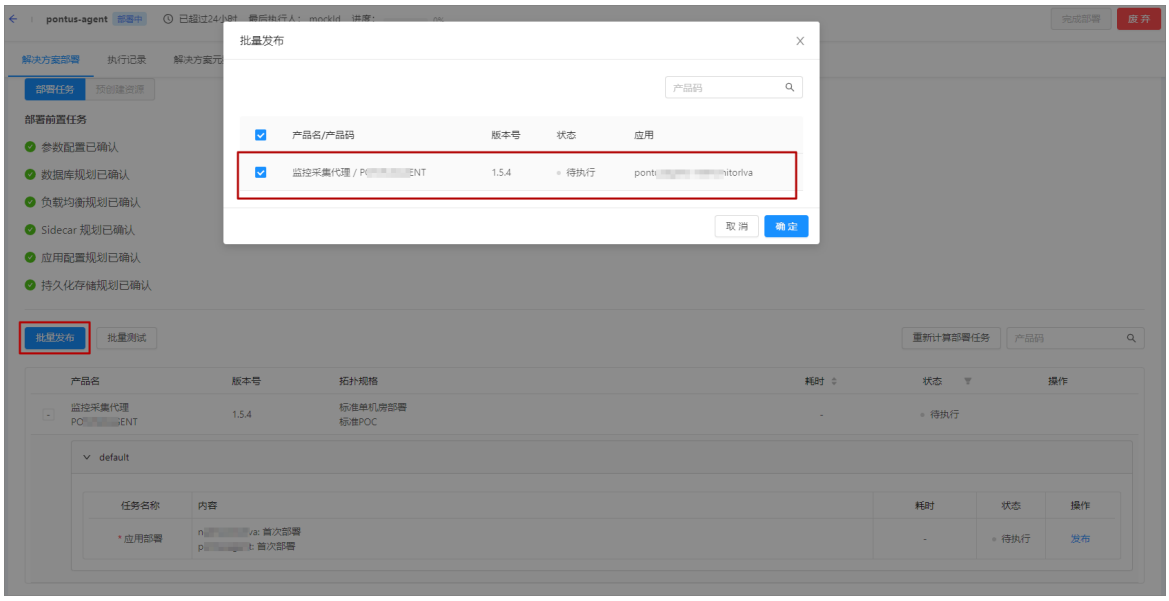
操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，单击 **交付升级**。
3. 在解决方案列表，单击目标解决方案。

4. 在发布产品列表，单击产品右侧的 **发布**。



您也可以单击 **批量发布**，然后选择多个产品，一次性发布多个产品。



5. 在 **新建发布单** 中，单击 **部署预览**。

   您还可以根据需要为容器进行分组，调整应用发布顺序等。

- 预设的发布顺序是按照产品的依赖关系自动计算，如有特殊需求可手动调整发布顺序。支持手动调整产品发布顺序和产品中不同应用的发布顺序。
- Beta 分组是指若部署策略选了分两组或每台一组，每一组发布完成后，需要人工介入验证发布的结果，确认无误后再发布下一组。
- 1.12.x 及以上版本支持手动选择本次发布单中不需要发布的应用：
  - 若您本次不需要发布某个应用，单击应用名称右侧的 × 即可。该功能适用于一个产品中存在多个应用时，只有部分应用需要升级的场景。
  - 若您需要重新加入该应用，则在本次不发布区域单击应用右侧的 √ 即可。
- 部署策略默认是 **分两组**，容器分组策略包括：
  - **系统推荐分组**：使用系统推荐的默认分组（分两组）。
  - **每台一组**：每台主机上的 Pod 为一组，发布时串行发布。适合 DaemonSet 应用。

- **共分一组**：所有 Pod 作为一组，发布时所有 Pod 一起并行发布。
- **分两组**：所有 Pod 分为两组，发布时分两组顺次发布。
- **自定义分组**：使用自定义的分组策略。更多信息，请参见 自定义分组策略。

若您觉得此次修改不符合需求，可以单击 **恢复默认发布顺序**，返回到默认值。

6. 确认产品参数无误后，单击 **开始部署**，然后单击 **确定**。
7. 在弹出的预览面板预览部署，确认无误后单击 **确定**。
8. 当所有发布任务完成后，单击 **完成部署**。

   如果本次部署的解决方案有问题，导致部署失败，您可以单击右上角的 **废弃**，以废弃解决方案，重新导入。

9. 在弹出的对话框中输入解决方案名称，然后单击 **确定**。

   页面会跳转至 **解决方案部署** 详情页。本页面上的默认设置无需求时可不做任何修改。部署策略、Beta 分组的选择会影响发布的速度，但速度越快的策略，安全性越低，可按需取舍。

   在 **解决方案部署** 详情页，您可以对整个发布单、单个产品、单个应用、单个步骤、单个节点进行重试、跳过、回滚等操作。

2.7.4. 查看解决方案

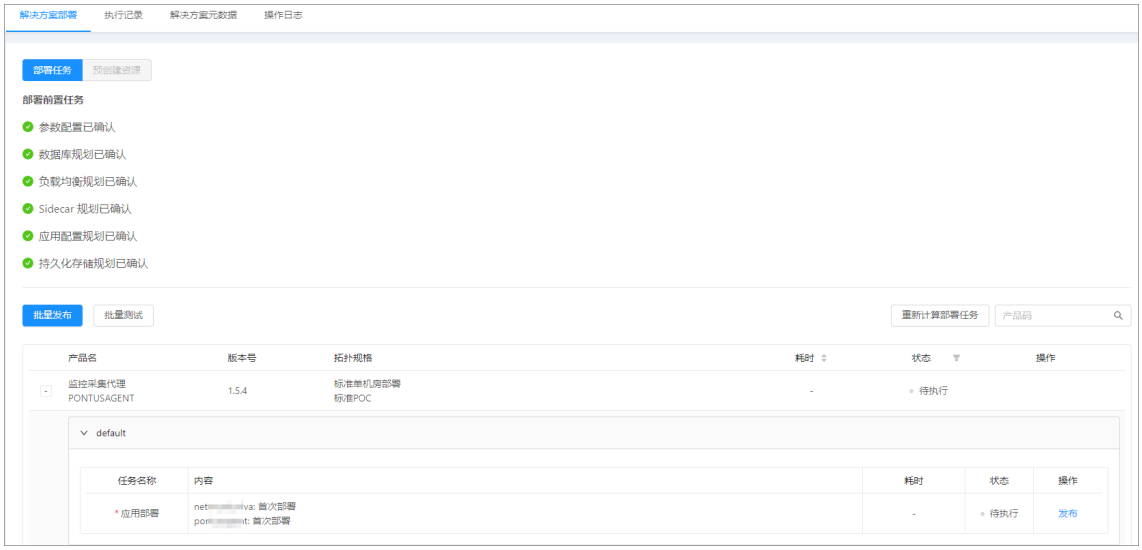
您可以通过云游 Local 控制台查看已导入的所有解决方案。

操作步骤

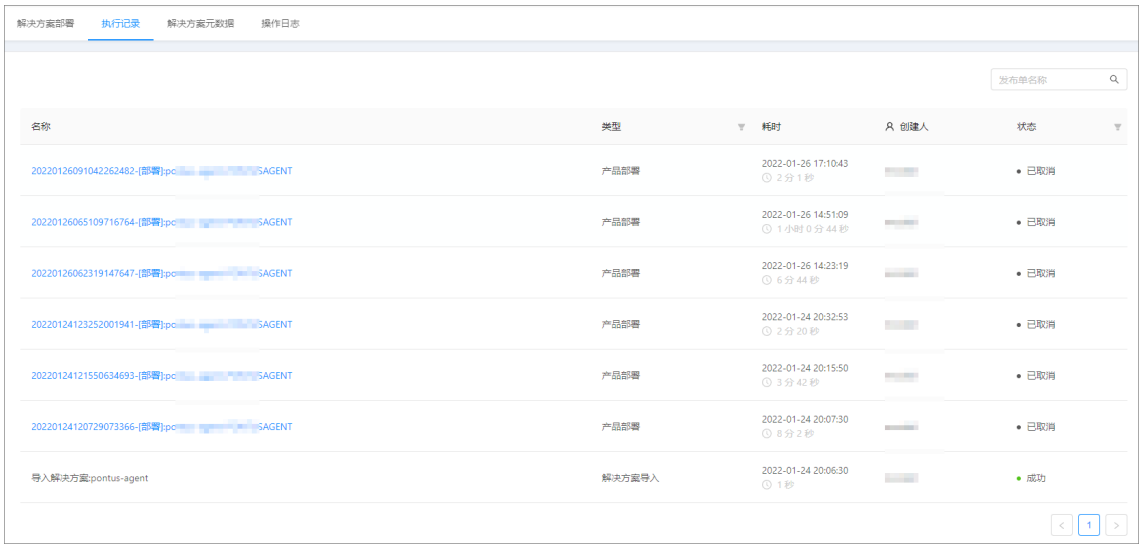
1. 登录云游 Local 控制台。
2. 在左侧导航栏，单击 **交付升级**。
3. 在解决方案列表，单击目标部署方案名称。

   您可以根据需求查看解决方案的不同信息：

   - **解决方案部署** 页签中可查看部署前置任务状态、已发布的产品名、产品版本号、产品发布状态等信息。



- **执行记录** 页签可查看解决方案中所有部署任务的执行记录和执行结果。



- **解决方案元数据** 页签可查看导入的解决方案的原始信息，即本次部署的终态。

- **操作日志** 页签可查案解决方案的所有操作日志 。

2.7.5. 修改应用配置项

您可以在云游 Local 控制台修改您解决方案中应用的配置项，以满足您的环境需求。

前提条件

解决方案已导入云游 Local。操作步骤请参见 导入解决方案。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，单击 **交付升级**。
3. 单击目标解决方案，然后单击 **解决方案元数据**。
4. 单击 **应用配置规划** 页签，然后单击目标应用右侧的 **编辑**。
5. 在 **应用配置编辑** 面板配置以下参数：

参数	说明
资源配置	
CPU 配置	查看 CPU 核数。
CPU 超卖	设置 CPU 的超卖比。
内存配置	查看内存大小，单位为 GB。
内存超卖	设置内存的超卖比。
密钥加固	选择是否开启 Keystone 加密。 开启后，您应用的敏感信息，如密钥、账号密码等都会加密传输。 **注意** 开启此功能前，您的应用必须增加 Keystone 的 SDK，否则此功能不生效。
网络配置 hostNetWork	定义 Pod 网络配置。 打开开关表示在 Pod 中使用 `hostNetwork:true` 配置网络，Pod 中运行的应用程序可以直接看到宿主主机的网络接口，宿主主机所在的局域网上所有网络接口都可以访问到该应用程序。
GPU 显存	设置 GPU 显存数量。
证书挂载	
证书挂载	开启后可挂载证书。单击 **证书挂载**，然后填写证书的 **secret 名称** 和 **挂载路径**。
工作负载配置	

应用基础信息	配置应用的发布策略、更新策略、DNS 策略、重启策略，其中发布策略、更新策略、重启策略不可配置，策略保持默认配置。 ○ **DNS策略**：配置 Pod 容器的 DNS 策略，取值如下。 ■ **Default**：使用默认 DNS 策略。 ■ **CluesteFirst**：使用集群优先策略。 ■ **ClusterFirstWithhostNet**：使用具有主机网络的集群优先策略。 ○ **首次发布部署策略**：配置应用首次发布时容器分组策略，取值如下。 ■ **并行**：所有容器并行发布。 ■ **串行**：所有容器顺次发布。 ○ **升级发布部署策略**：配置应用升级发布时容器分组策略，取值如下。 ■ **每台一组**：每台主机上的 Pod 为一组，升级时顺次升级。 ■ **共分一组**：所有 Pod 作为一组，升级时所有 Pod 一起升级。升级期间应用不可用。对于可靠性较高的应用，不建议使用这种分组策略。 ■ **分两组**：所有 Pod 分为两组，升级时分两组顺次升级。 ■ **系统推荐**：选择系统推荐时，默认使用 **分两组** 策略。
探针配置	配置应用的存活和健康检查探测类型： ○ **存活检查探测类型**：探测应用是否存活，取值如下。 ■ **None**：不进行探测。 ■ **TCP**：对指定容器使用 TCP 协议进行探测，如果被探测端口正常，则探测成功。 ■ **HTTP**：对指定容器进行 HTTP Get 请求，如果响应状态码大于 200 且小于 400，则探测成功。 ○ **健康检查探测类型**：探测应用是否健康，取值如下。 ■ **None**：不进行探测。 ■ **TCP**：对指定容器使用 TCP 协议进行探测，如果被探测端口正常，则探测成功。 ■ **HTTP**：对指定容器进行 HTTP Get 请求，如果响应状态码大于 200 且小于 400，则探测成功。 ○ **探测周期**：设置存活和健康检查的探测周期，即多长时间探测一次。单位为秒。 ○ **失败阈值**：设置探测失败阈值，当探测连续失败次数达到阈值时，才会被认定为失败。 ○ **tcpPort**：设置探测的端口，此端口必须真实存在。

节点亲和性配置	用于配置调度 Pod 时优先选择的节点。单击 **添加节点选择器** 配置如下参数： ○ Key：填写目标节点的标签键。 ○ Operator：选择亲和性规则为 **包含** 或 **不包含**。 ○ Values：填写目标节点标签键对应的值。 您可以添加多个节点亲和性配置。
污点容忍度配置	用于配置 Pod 对节点上污点的容忍度。单击 **添加污点容忍度** 配置如下参数： ○ Key：填写目标节点的标签键。 ○ Operator：选择污点容忍度规则为 Equal 或 Exists。 ○ Values：填写目标节点标签键对应的值。 ○ Effect：设置污点容忍的策略。 ■ PreferNoSchedule：不能容忍此污点的 Pod 对象尽量不要调度至当前节点，当无其他节点可供调度时也允许接受相应的 Pod 对象。节点上现存的 Pod 对象不受影响。 ■ NoSchedule：不能容忍此污点的 Pod 对象不可调度至当前节点，属于强制型约束关系。节点上现存的 Pod 对象不受影响。 ■ NoExecute：不能容忍此污点的 Pod 对象不可调度至当前节点，属于强制型约束关系。而且节点上现存的 Pod 对象因节点污点变动或 Pod 容忍度变动而不再满足匹配规则时，Pod 对象将被驱逐。 您可以添加多个污点容忍度配置
Pod 拓扑打散约束	用于控制 Pods 在集群内故障域之间的分布。单击 **添加 Pod 拓扑打散约束**，并配置如下参数： ○ Key：填写目标节点的标签键。 如果多个节点使用此键标记并且具有相同的标签值，则调度器会将这两个节点视为处于同一拓扑域中。调度器试图在每个拓扑域中放置数量均衡的 Pod。 ○ **调度策略**：指示如果 Pod 不满足分布约束时如何处理。 ■ DoNotSchedule：不进行调度。 ■ ScheduleAnyway：调度器仍然继续调度，只是根据如何将倾斜度最小化来对节点进行排序。 ○ **倾斜度**：描述 Pod 分布不均的程度。用于给定拓扑类型中任意两个拓扑域中匹配的 Pod 之间的最大允许差值。 您可以添加多个 Pod 拓扑打散约束。
高可用配置	

亲和性配置	设置多个应用部署在同一个节点。 ○ **应用**：选择多个不同应用。 ○ **策略**：设置亲和性策略。 ■ **强互斥**：所选择的应用强制部署在同一个节点。 ■ **弱互斥**：所选择的应用尽量部署在同一节点，如果不满足条件也可以部署在不同节点。
反亲和性配置	设置不同应用不允许部署在同一个节点。 ○ **应用**：选择多个不同应用。 ○ **策略**：设置反亲和性策略。 ■ **强互斥**：所选择的应用强制部署在不同节点。 ■ **弱互斥**：所选择的应用尽量部署在不同节点，如果不满足条件也可以部署在相同节点。

6. 单击 **保存**，然后单击 **确定**。

2.7.6. 一键部署

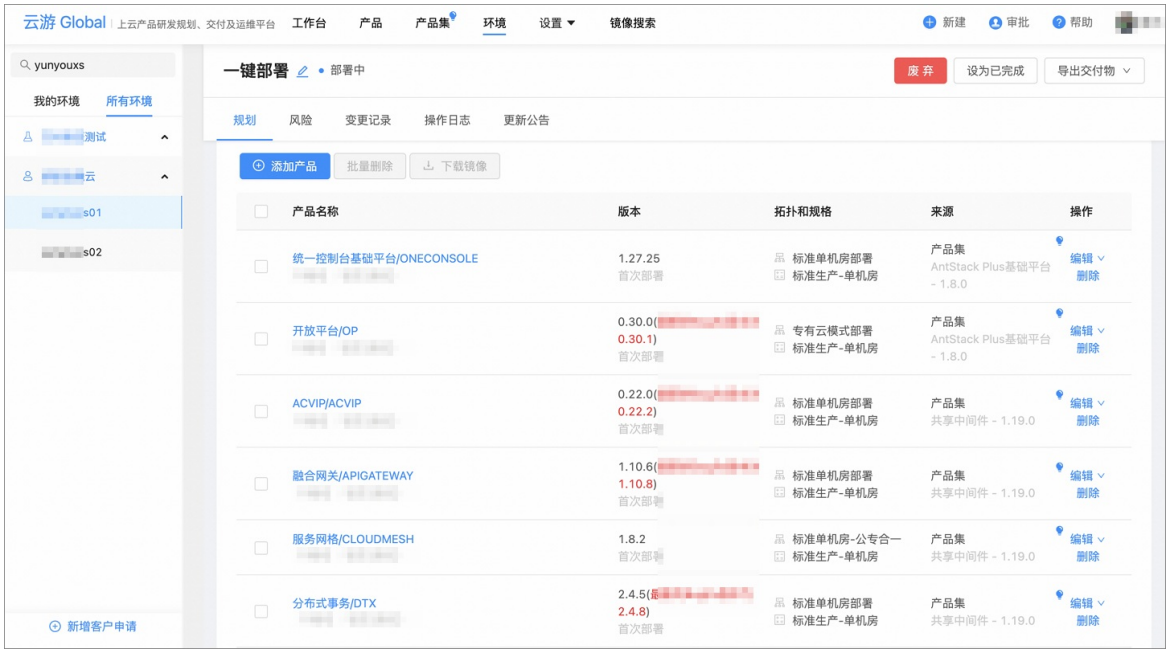
您可以在交付站点时，将本次交付的所有产品都添加在一个解决方案中，并通过一键部署功能安装所有产品。

注意事项

- 仅适用于云游 Local 1.13.x 及以上版本。
- 仅适用于交付站点时首次安装站点所有的产品。
- 仅适用于通过产品成熟度的产品，目前支持的产品线有：
  - SOFAStack
  - mPaaS（适配中）

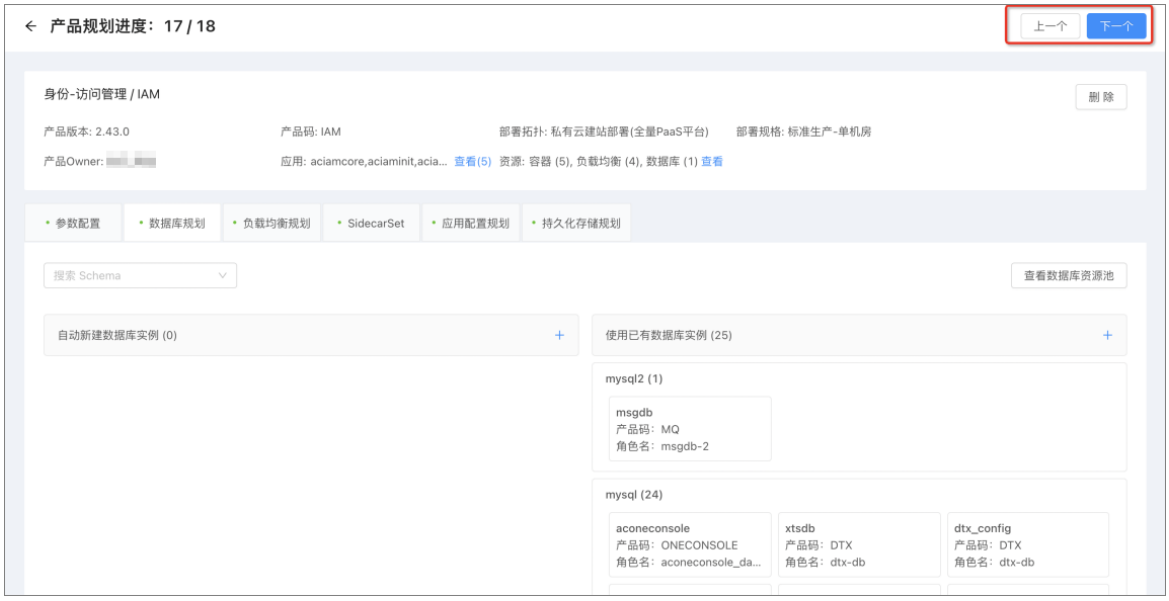
操作步骤

1. 在云游 Global 中创建环境，将首次交付的所有产品添加在一个解决方案中。



2. 导出解决方案。
3. 登录云游 Local。
4. 在左侧导航栏单击 **交付升级**，然后单击 **一键部署**。
5. 单击 **导入产品**，然后将之前导出的部署方案上传。

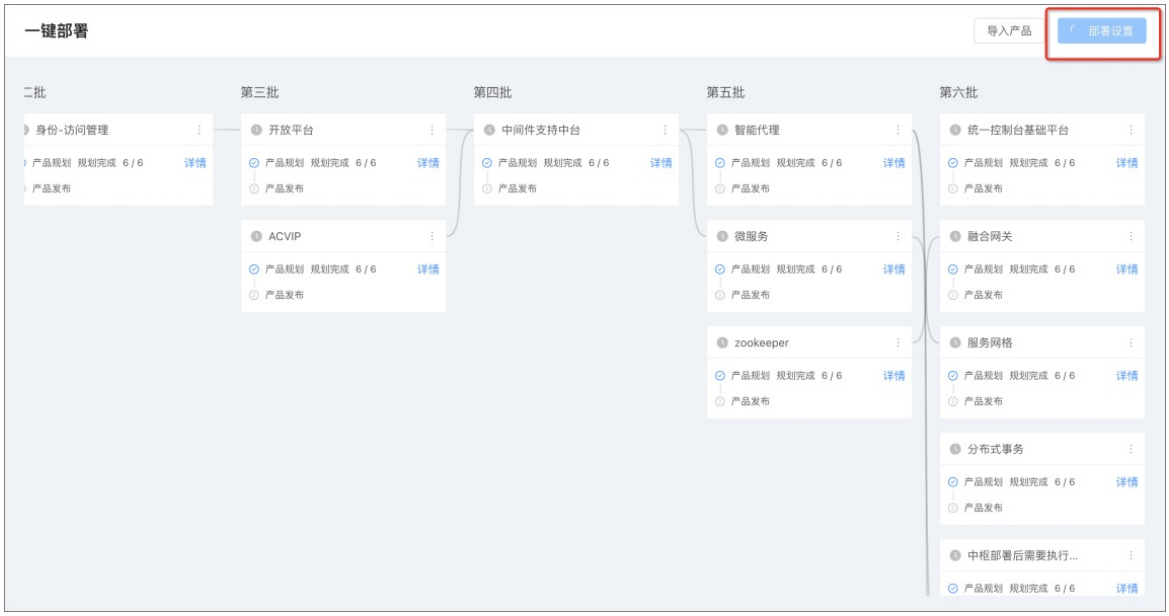
6. 单击 **开始规划**，然后依次完成所有产品部署前任务的确认。
   - 和原先的发布、批量发布逻辑一致，您需要依次完成每个产品的 **参数配置**、**数据库规划**、**负载均衡规划**、**持久化存储规划** 和 **应用配置化规划**。
   - 单击 **上一个** 或 **下一个** 可切换待规划的产品。
   - 该产品不需要在本次发布，可单击 **删除** 将其从本次发布队列中踢除。



注意

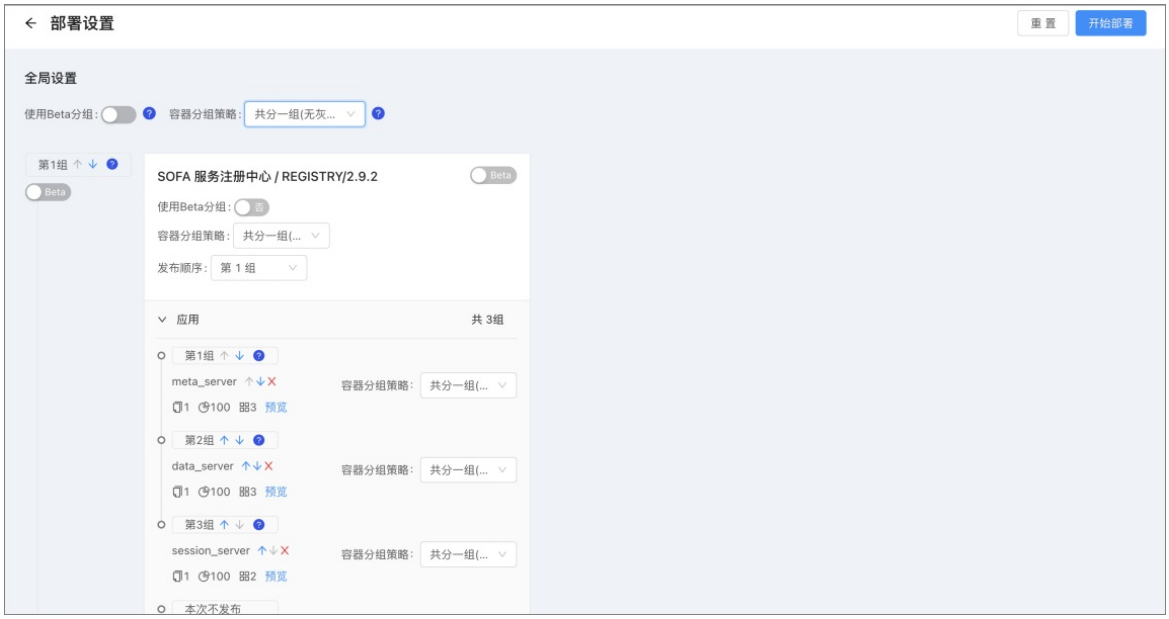
- 未通过一键部署导入的产品，且未发布过，会被加入到一键部署的任务中。如果不需要发布，需要您手动从本次一键发布中删除。
- 未通过一键部署导入的产品，且已经发布过（产品基线中会出现），无论其正在发布中或者发布失败，都不会被加入到一键部署的任务中。

7. 全部规划设置完成后，单击 **部署设置**。



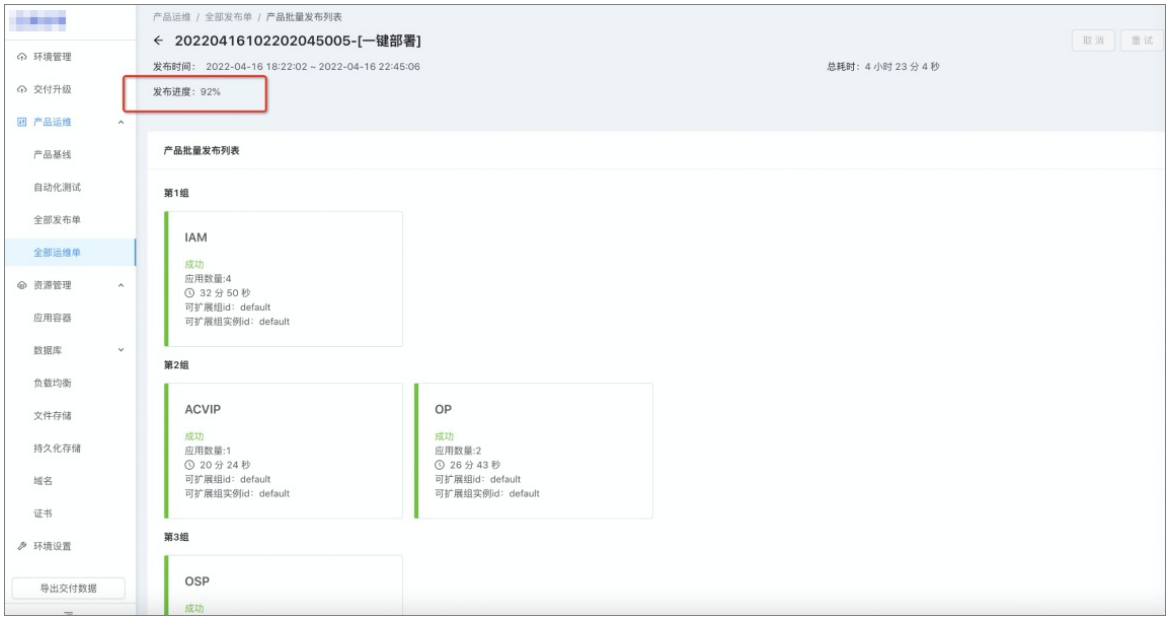
8. 在 **部署设置** 页面调整发布策略。

   首次发布时，**容器分组策略** 可以设置为 **共分一组**，让多实例并行发布；**使用 Bate 分组** 可以不开启。



9. 单击 **开始部署**。

   您可以在发布单中查看整体发布进度和每个产品部署的结果。



10. 如果产品发布中遇到问题，可以尝试使用无人值守功能。

    无人值守功能说明，请参见 无人值守。

2.7.7. 自定义分组策略

云游 Local 在进行产品发布和运维操作时，对容器的分组策略支持共分一组、分两组和每台一组，若针对的容器数量较多，您也可以选择自定义分组策略。

使用场景

您在生成发布单或运维单时，都需要设置容器分组策略，各分组策略使用建议如下：

- 产品发布和一键部署通常使用共分一组的策略。

- 强制重发建议使用分两组或自定义分组策略，同时建议使用 beta 分组。若涉及的容器较多，建议使用自定义分组策略。

> 注意
>
> 自定义分组策略适用于大规模 Pod 变更，因为产品中可能存在某个应用有上百个 Pod，但其他应用可能只有几个 Pod 的情况，所以定义自定义分组属于应用级的配置，而不能进行全局配置。

- 重启、扩容或缩容建议使用分两组策略，但通常不需要使用 beta 分组。
- 容器变配、上线或下线建议使用分两组或自定义分组策略，同时建议使用 beta 分组。若涉及的容器较多，建议使用自定义分组策略。

使用规则

分组规则

- 用户未编辑自定义分组策略，使用默认策略
  - 实例数 N≤5 时，每个实例一组，共分为 N 组。
  - 实例数 N > 5 时：
    - 默认分为 5 组。
    - 第 1 组恒定为 1 个实例。
    - 第 2 组到第 5 组默认占比为：5%、15%、20%、60%
    - 每组根据分组占比计算实例数取整，计算结果不足一个的，算一个实例（即每组最少一个实例）。
    - 第 5 组的容器数量为总容器数 N 减去前 4 组容器的数量之和。
- 用户手动编辑自定义分组策略
  - 支持自定义分组数，最少不得少于 2 个分组，最大不能大于 min{100, N}（即当实例数 N < 100 时，分组数不能超过 N；当 N≥100 时，分组数不能超过 100）。

    > 注意
    >
    > - 第一个分组组必须为 beta 分组，且必须存在，所以分组数量必须大于 2。
    > - 如果只有 2 个分组，则第一个分组实例数为 1，第二个分组的实例数为剩下的所有实例。

  - 分组时，后面分组的占比必须大于等于前面分组的占比。
  - 当分组小于等于 10 时，每组的占比都可以调整，但是得满足上面比例递增的规律；分组大于 10 时，使用默认比例分组，不支持调整。
  - 当增加或者减少分组的数量时，每组的比例都会均分重置。
  - 百分比不允许有小数，如果重置后的比例有小数，则向下取整，最后的余数给到最后一组。

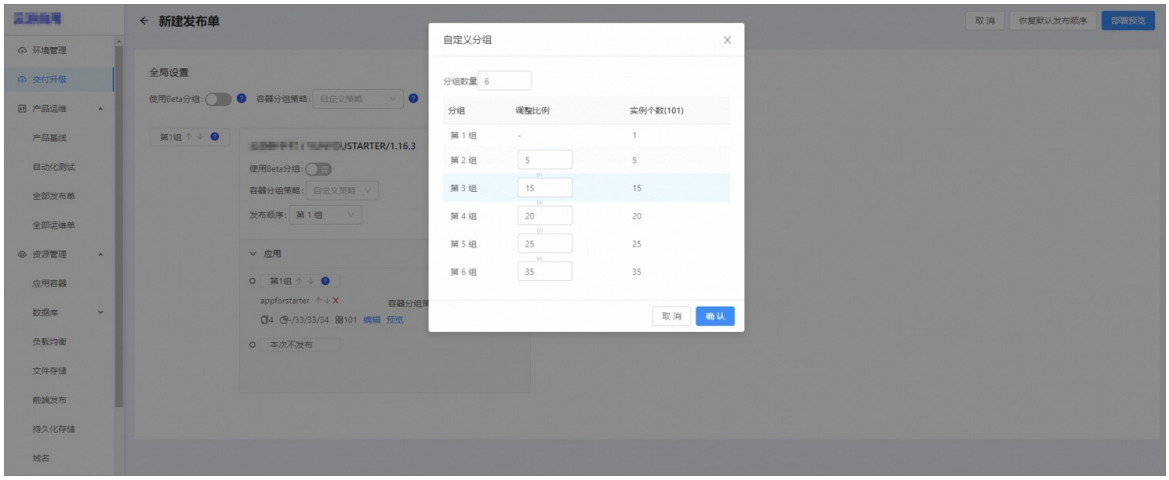
持久化规则

为了避免多次导入解决方案和多次发布的过程中重复编辑自定义发布策略的配置，所以云游 Local 提供了自定义发布策略持久化的功能，会自动将用户配置的自定义发布策略存储到数据库中。

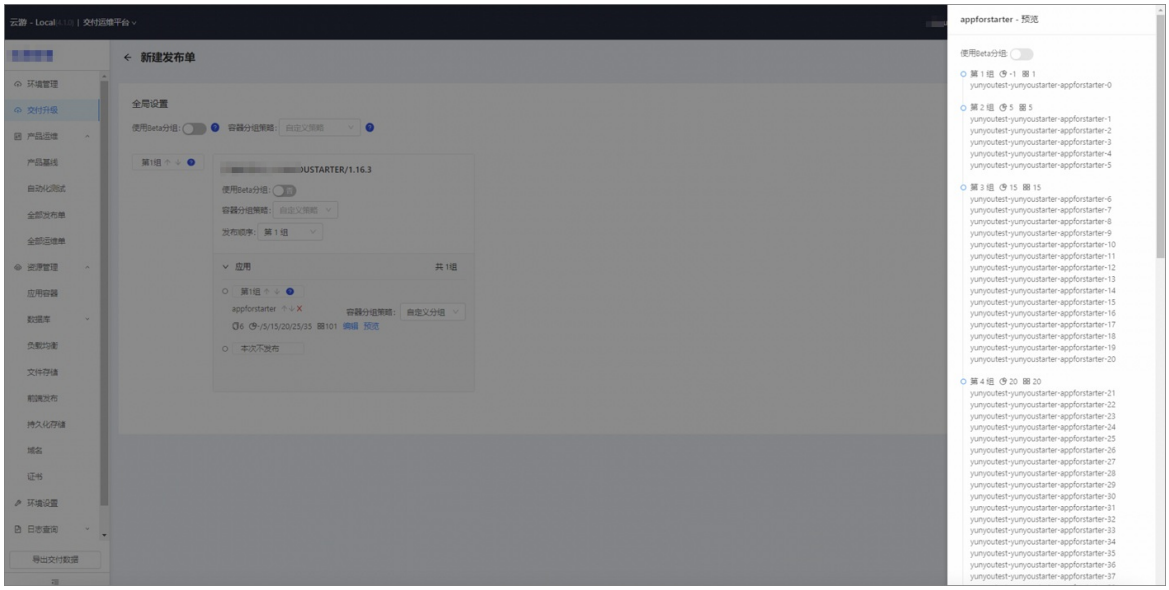
使用方法

1. 您在生成发布单或运维单时，可以在应用的容器分组策略中配置并选择自定义策略。
2. 单击 **编辑**，然后配置自定义分组。

   配置示例如下：



3. 单击 **预览** 可以看到每个分组中待发布的实例数。



2.8. 产品运维

2.8.1. 产品基线

2.8.1.1. 导出基线

本次交付或变更完成后，请一定要将基线导出并回流基线到云游 Global，作为日后制作升级方案的依据。

您可以通过以下两种方式导出基线：

方式一

1. 登录云游 Local 控制台。

2. 在左侧导航栏，选择 **产品运维 > 产品基线**。
3. 单击 **导出基线**。

   当前环境的产品基线信息会以 JSON 文件形式导出到浏览器默认的下载文件夹。

方式二

1. 将鼠标悬停在云游 Local 控制台左侧导航栏的 **导出交付数据**。
2. 单击 **导出产品基线**。

   当前环境的产品基线信息会以 JSON 文件形式导出到浏览器默认的下载文件夹。

2.8.1.2. 管理产品

2.8.1.2.1. 查看当前环境已部署的产品

您可以在云游控制台查看当前环境已部署的产品，包括产品的名称、产品码、应用、参数、执行记录等信息。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维 > 产品基线**。

您可以在右侧的产品列表中查看已部署的所有产品信息，如产品名称、版本、拓扑、规格等信息 。

3. 在产品列表中，单击目标产品名称。

   您可以根据需求查看产品的基本信息：

   - **应用** 页签可以查看产品包含的所有应用。单击应用卡片，即可查看该应用的具体信息，包括容器、负载均衡、数据库和文件存储等信息。
   - **参数** 页签可以查看应用启动的参数和产品的公共参数。
   - **执行记录** 页签可以查看对该产品的所有操作。
   - **操作日志** 页签可以查看对该产品进行扩容、销毁、下线等操作记录。
   - **成员管理** 页签可以查看产品相应的运维工程师和交付工程师。

2.8.1.2.2. 升级产品

当您需要升级产品时，您需要向蚂蚁集团的工作人员（或技术支持人员）获得产品升级的解决方案包，然后参考 部署前置任务 和 部署解决方案 说明进行产品升级操作。

2.8.1.2.3. 升级产品最佳实践

使用前提

- 云游 Local 上产品已部署完成，基线已回流。
- 已根据产品的版本信息更新云游 Global 上对应环境的解决方案。

  注意拓扑和规格的选择，需与之前的产品解决方案保持一致。
- 已根据产品的版本信息准备好应用镜像，并上传至环境中。

  镜像需从云游 Global 上导出。

操作步骤

本文以升级 IAM 产品为例，演示如何产品升级的整个过程。

1. 备份 IAM 相关数据库。

```
mysqldump -u*** -h*** -p*** aciamcore > aciamcore220413.dump
mysqldump -u*** -h*** -p*** aciamweb > aciamweb220413.dump
```

2. 导入产品镜像。

```
chmod +x docker-images-migration
./docker-images-migration --source iam.json --target iam.tar import
```

3. 更新解决方案。
   i. 从云游 Global 导出 IAM 新版本解决方案，并导入云游 Local。

      导入解决方案步骤，请参见 导入解决方案。

   ii. 在 **交付升级** 页面，单击刚导入的解决方案。

   iii. 在 解决方案部署 页签，确认所有部署前置任务。

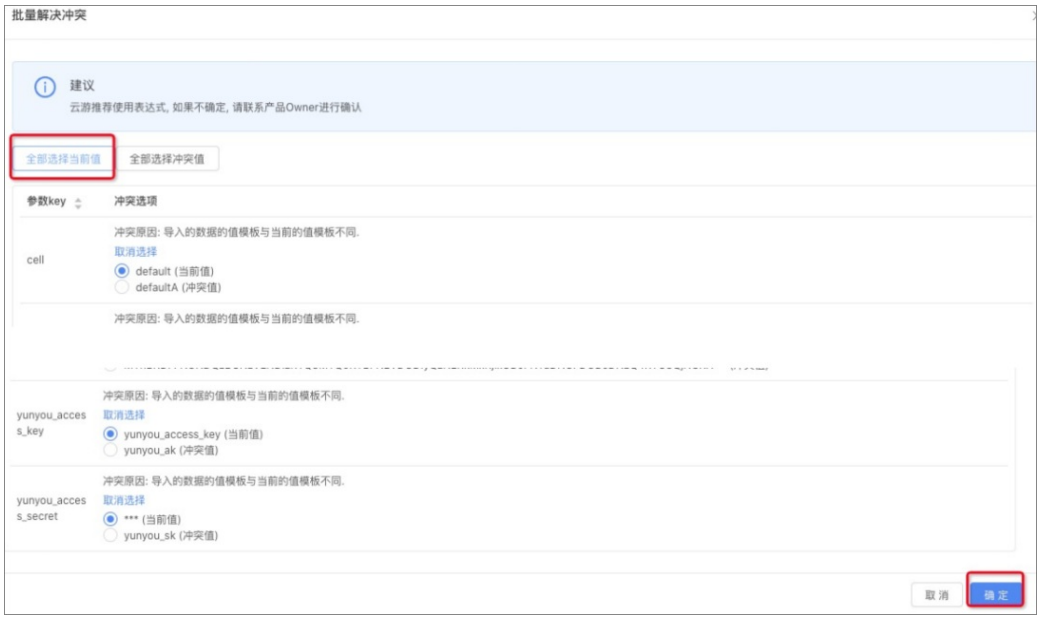
      - 确认数据库规划和负载均衡规划

        单击 **解决方案元数据**，单击 **数据库规划** 和 **负载均衡规划** 页签分别确认数据库规划和负载均衡规划。

      - 确认参数配置。

        a. 单击 **解决方案元数据**，然后单击 **参数配置**。

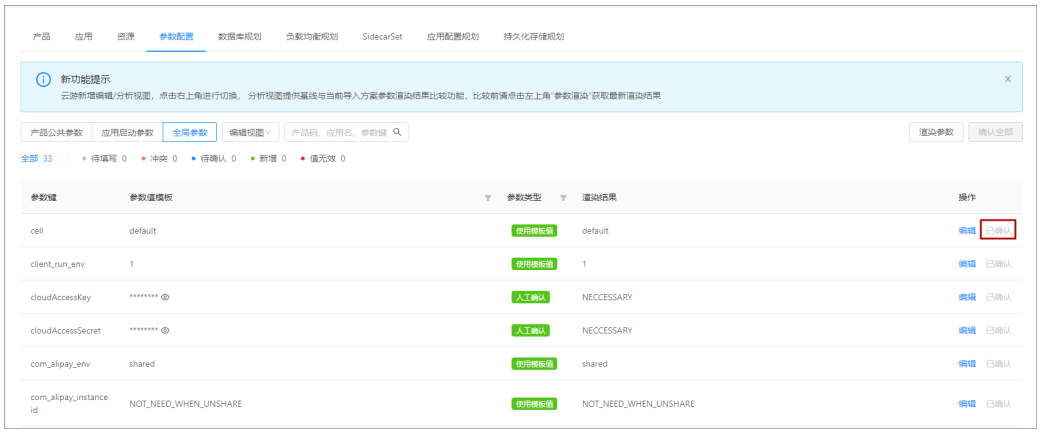
        b. 单击 **解决冲突**，然后单击 **全部选择当前值**。



        c. 单击 **确定**。

d. 回到 **全局参数** 页签，单击 **渲染参数**，然后单击 **确定**。

确认所有参数变为 **已确认** 状态。



若有未确认的参数，则单击目标参数右侧的 编辑，然后单击确认。之后再次进行渲染参数操作，直到所有参数变为 **已确认** 状态。

e. 单击 **确认全部**。

f. 按照以上步骤将 **应用启动参数** 中的所有参数变为 **已确认** 状态。

4. 发布部署。

i. 查看应用变化。

参数检查及自定义资源配置完成后，在产品发布区域，将鼠标放在产品右侧的感叹号上查看当前基线和新的解决方案直接的参数差异。

如果有预期外的参数变化（升级场景应只会有参数增加，没有参数变更），需截图发给技术支持进行确认，确认无误后再进行下一步发布。

ii. 单击应用右侧的 **发布** 按钮。

iii. 在新建发布单页面配置发布参数后，单击 **开始部署**，然后单击 **确定**。

建议打开 **使用 Beta 分组** 的开关，并将容器分组策略设置为 **系统推荐分组** 或 **分两组**。

iv. 在弹出的部署预览，确认镜像、规格、副本数均无误后，单击 **开始部署**。

> **注意**
>
> 发布完第一个 Beta 分组之后，检查发布完的这台节点功能是否正常。确认发布没有问题之后再单击 **确认** 发布下一个分组，如果有问题的需要及时进行回滚。

后置校验

- 发布部署完成后，确认容器健康检查都已通过。

  您也可以手动检查服务启动状态：

  - 登陆到 IAM 组件应用的容器，执行以下命令：

    ```
    curl localhost:9500/checkService | grep false
    ```

    返回的结果如果没有 `false` 则说明正常。

  - 使用 `telnet` 命令测试目标端口是否已开启，示例如下：

    ```
    telnet localhost 1234
    ```

- IAM 界面能正常登录。
- 打开 SOFA 或 mPaaS 页面，能正常跳转至 IAM 并完成登录操作。

回滚方案

如果升级后，IAM 无法正常登录，需和产研同学确认是否可以执行回滚方案。操作步骤，请参见 产品回滚。回滚完成后需按照后置校验检查服务是否正常。

数据库还原

若产品回滚，您还需还原 IAM 相关数据库：

```
mysqldump -u*** -h*** -p*** aciamcore < aciamcore220413.dump
mysqldump -u*** -h*** -p*** aciamweb < aciamweb220413.dump
```

2.8.1.2.4. 卸载产品

您可以在云游 Local 控制台卸载不再需要的产品。本文介绍如何卸载产品。

前提条件

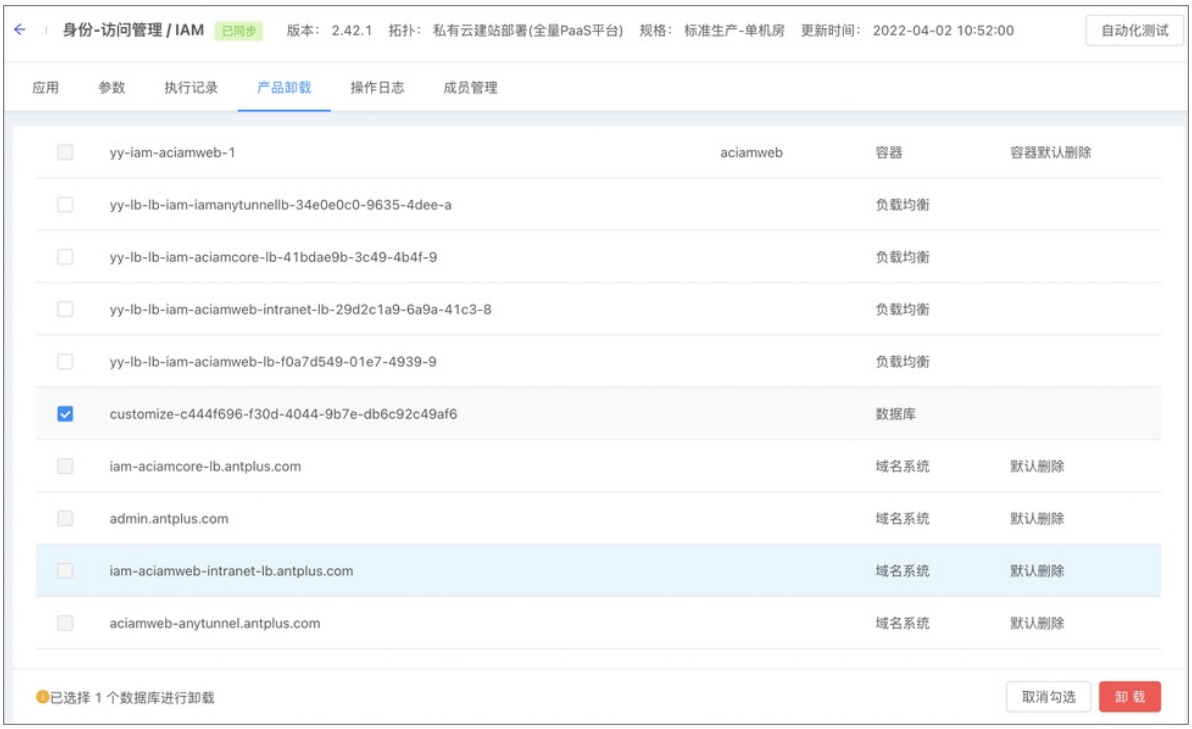
已确认无线上服务风险。卸载产品后，线上产品服务会立刻停止，版本信息和资源会全部被删除且不可恢复。请确认此次操作不会对您线上服务造成影响。

注意事项

- 卸载产品前注意下线所有容器，避免还有请求进入容器，而容器销毁导致请求丢失。
- 如果勾选了数据库实例，云游会删除该产品所用的 Schema。
  - 对于云游自动创建的 Schema，数据库变更会删除。

- 对于手动创建的 Schema，数据库变更不会删除。

- 如果不勾选数据库实例，则云游会保留该产品所用的 Schema 和 Schema 的数据库变更。



操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **产品基线**。
3. 单击目标产品名称，之后单击 **产品卸载** 页签。
4. 单击 **点此下线所有容器**，然后按步骤下线所有容器。
5. 回到 **产品卸载** 页签，选中您需要卸载的产品资源，之后单击 **卸载**。

产品卸载后您仍可以在产品资源列表中取消勾选容器，以保留负载均衡或数据库资源。保留的资源可在 **资源管理** 模块查看。

2.8.1.2.5. 产品回滚

对于已经部署，且已升级完成的产品，若升级后存在问题，您可以对其进行回滚操作。

前提条件

- 产品发布成功，且已完成解决方案部署。

  操作步骤请参见 部署解决方案。

- 对此产品导入了新版本的解决方案。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏单击 **交付升级**，然后单击目标解决方案。
3. 在 **解决方案部署** 页签选择目标产品右侧的 **快捷运维** > **回滚**。

4. 选择之前部署成功的产品版本记录。

您可以根据部署时间和参数变化选择需要回滚的应用。

5. 在 **新建产品回滚单** 页面配置部署策略后，单击 **开始回滚**。

   推荐部署策略选择 **分两组**。

2.8.1.3. 管理应用

您可以通过云游控制台管理产品中包含的所有应用。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **产品基线**。
3. 单击目标产品，然后单击 **应用** 页签。
4. 单击目标应用卡片。

   您可以在应用详情页面查看应用的基本信息、容器、负载均衡、数据库和持久化存储等信息。

   - 基本信息包含如下信息：
     - **版本：** 应用的版本号。
     - **容器规格：** 应用实例的CPU和内存限制（resources.limit）。

- **运行/期望**：环境中当前运行实例数量/发布中定义的期望运行的实例数量
- **基线差异**：
  - **已同步**：代表环境中应用状态和云游基线同步。
  - **未同步**：可能是同步延迟或遇到什么问题，您可以手动触发同步。
- **查看 Yaml**：查看环境中应用的 statefulset Yaml。

- **容器** 页签可查看和管理应用中的所有容器，例如上线、下线、重启、删除容器等操作。
- **负载均衡** 页签可查看应用暴露服务所用的 LB 信息，可查看 LB 的地址、域名和 Pod 的IP、端口。仅支持：
  - 阿里云 SLB
  - ParaLB（1.11.x）
  - AWS NLB（1.14.x）
- **数据库** 页签可查看所用的数据库实例信息和产品所用的所有 schema。
- **持久化存储** 页签可查看容器中目录挂载的持久卷 pv 的信息，包括其所属的 pvc 和 storageclass、容量、访问模式、回收策略等。

2.8.1.4. 管理容器

2.8.1.4.1. 查看容器

容器（Pod）是应用运行的实例，您可以通过云游 Local 控制台查看产品已有容器。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **产品基线**。
3. 在产品列表中，单击目标产品。
4. 单击 **应用** 页签，之后单击目标应用。
5. 单击 **容器** 页签。
   - 查看基本信息

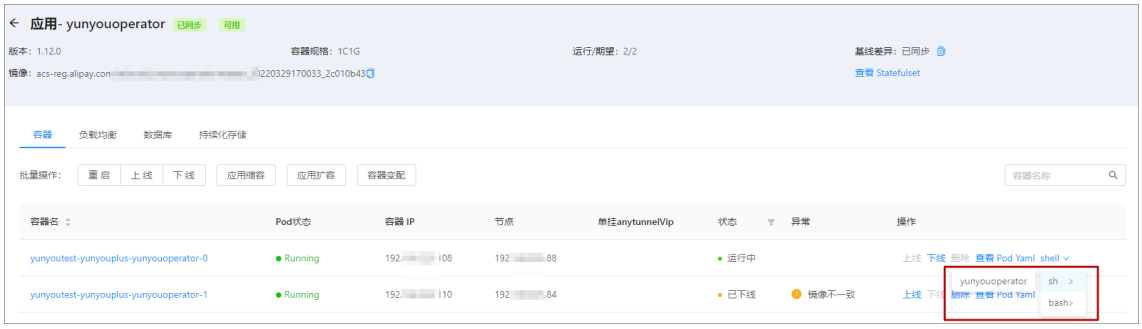
     您可以在 **容器** 页签查看当前应用的容器名称、容器 IP、宿主机 IP、状态等信息。

   - 查看容器 Yaml

单击目标容器右侧的 **查看 Pod Yaml**。

- 进入 shell

  单击目标容器右侧的 shell，然后选择 sh 或 bash，可从云游 Lcoal 进入 Pod 的 shell 终端。



2.8.1.4.2. 变更容器配置

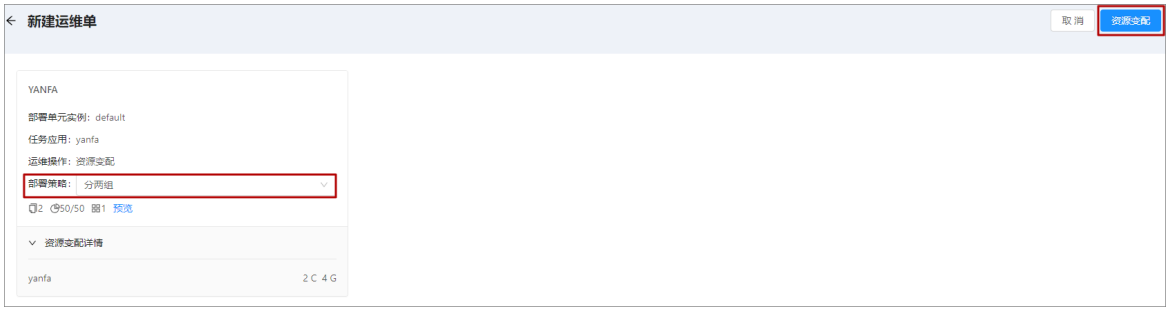
您可以通过云游 Local 控制台对应用的容器规格配置进行变更。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **产品基线**。
3. 在产品列表中，单击目标产品。
4. 单击 **应用** 页签，之后单击目标应用。
5. 单击 **容器** 页签，之后单击 **容器变配**。

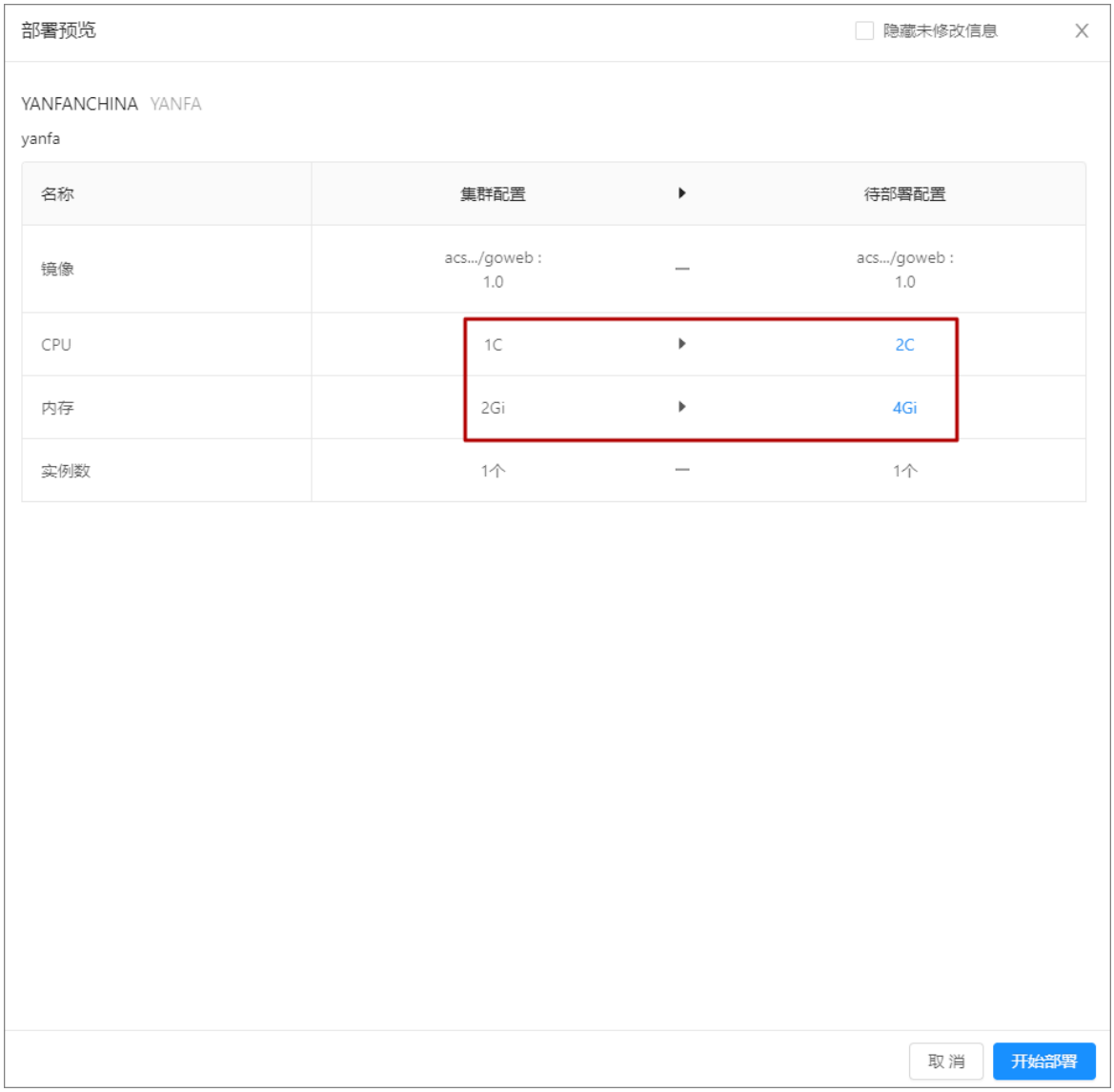
6. 在 **应用变配规格** 对话框设置 **目标 CPU** 和 **目标内存** 参数，之后单击 **确定**。

7. 在 **新建运维单** 页面，将 **部署策略** 改为 **分两组**。



8. 单击 **资源变配**，在**部署预览**面板确认部署参数无误后单击 开始部署，之后单击 **确定**。

   这里主要确认当前实例的 CPU、内存和期望变更的 CPU、内存。



注意

变配之后，AntStack Plus 底座环境，容器会自动进行滚动重启；AntStack 1X 和 2X 底座环境，您需要分批次手动重启容器。详情请参见 重启容器。

2.8.1.4.3. 容器内存与 JVM 堆内存配置比

中间件各产品容器内存与 JVM 堆内存的配置比如下：

产品名称	JVM 堆内存建议配置

产品名称	JVM 堆内存建议配置
动态配置 DRM	根据环境自动适配，适配方式如下： • 系统内存 = 2 GB；JVM = 1000 MB • 系统内存 = 4 GB；JVM = 3000 MB • 系统内存 = 8 GB；JVM = 6000 MB • 系统内存 = 10 GB；JVM = 9000 MB • 系统内存 = 14 GB；JVM = 12000 MB
注册中心 SOFARegistry	3/4 系统内存
DsrConsole	根据环境自动适配，适配方式如下： • 系统内存 = 2 GB；JVM = 1000 MB • 系统内存 = 4 GB；JVM = 3000 MB • 系统内存 = 8 GB；JVM = 6000 MB • 系统内存 = 10 GB；JVM = 9000 MB • 系统内存 = 14 GB；JVM = 12000 MB
任务调度 TS	根据环境自动适配，适配方式如下： • 系统内存 = 2 GB；JVM = 1000 MB • 系统内存 = 4 GB；JVM = 3000 MB • 系统内存 = 8 GB；JVM = 6000 MB • 系统内存 = 10 GB；JVM = 9000 MB • 系统内存 = 14 GB；JVM = 12000 MB
消息队列 MQ	系统自动调整，无需设置。
消息队列 DMS	Console：系统内存 = 4 GB；JVM = 3 GB Broker：系统内存 = 8 GB；JVM = 4 GB
分布式事务 DTX	JVM 堆内存小于系统内存。 例如系统内存为 8 GB，JVM < 8 GB。

产品名称	JVM 堆内存建议配置
数据访问代理 ODP	根据环境自动适配，适配方式如下： • 系统内存 < 2 GB；JVM 使用系统默认值（根据不同版本进行调整） • 2 GB < 系统内存 < 6 GB；JVM = 2048 MB • 6 GB < 系统内存 < 10 GB；JVM = 4800 MB • 10 GB < 系统内存 < 14 GB；JVM = 5600 MB • 系统内存 > 14 GB；JVM = 9600 MB
Mesh	不涉及
API 网关	不涉及
消息队列 SOFAKafka	系统自动调整，无需设置。

2.8.1.4.4. 产品扩容

扩容产品即增加容器的个数，本文介绍如何在云游 Local 控制台对产品进行扩容操作。

操作步骤

1. 登录云游 Local 控制台。
2. 在 **产品基线** 页面单击目标产品。
3. 单击 **应用** 页签，然后单击目标应用。
4. 单击 **应用扩容**。
5. 在 **应用扩容容器数量** 对话框设置扩容数量，然后单击 **确定**。
6. 在 **新建运维单** 页面单击 **应用扩容**。

7. 在 **部署预览** 面板确认部署参数无误后，单击 **开始部署**，然后单击 **确定**。

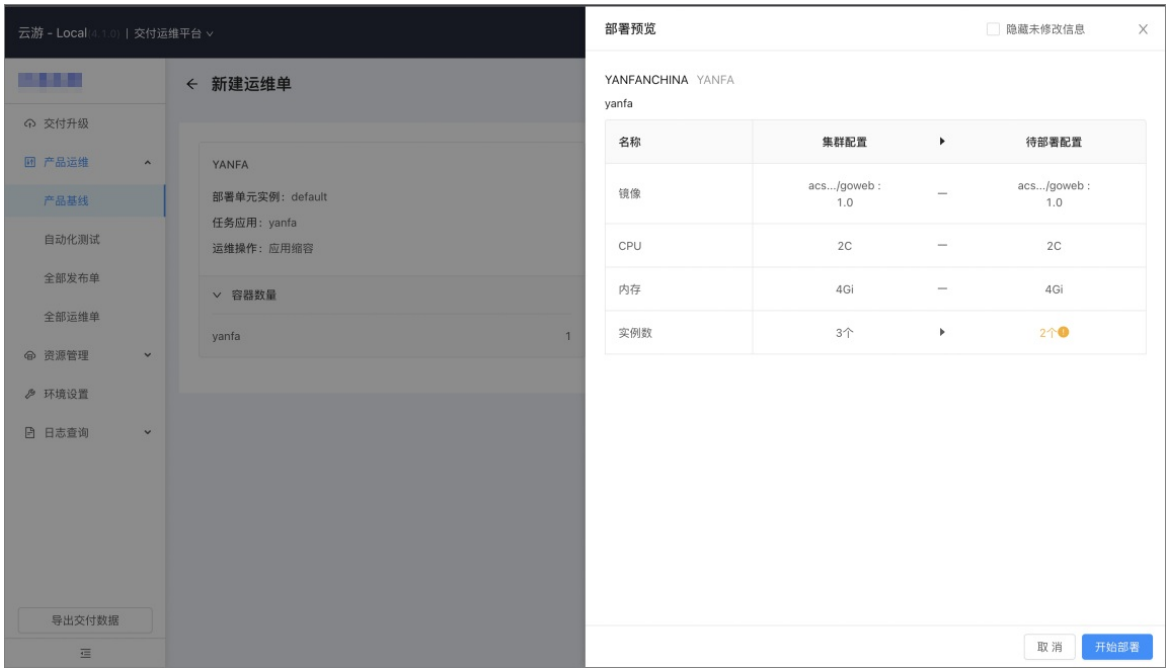
2.8.1.4.5. 产品缩容

产品缩容即减少容器的个数，本文介绍如何在云游 Local 控制台对产品进行缩容操作。

操作步骤

1. 登录云游 Local 控制台。
2. 在 **产品基线** 页面单击目标产品。
3. 单击 **应用** 页签，然后单击目标应用。
4. 单击 **应用缩容**。
5. 在 **应用缩容容器数量** 对话框设置缩容数量，然后单击 **确定**。

6. 在 **新建运维单** 页面单击 **应用缩容**。
7. 在 **部署预览** 面板确认部署参数无误后，单击 **开始部署**，然后单击 **确定**。



2.8.1.4.6. 容器下线

下线是指实例还在运行，但是不提供服务，即服务下线。云游的处理方法是运行实例数不变，但是将指定的容器镜像替换成一个不提供服务的基础镜像。

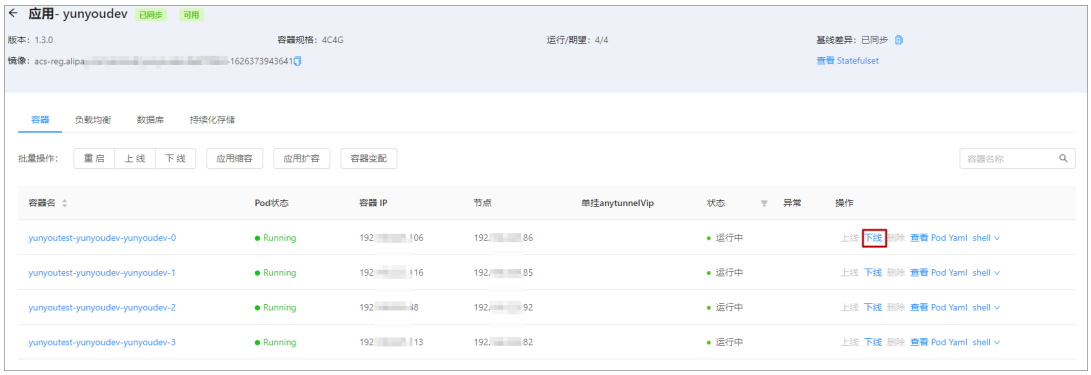
前提条件

环境的镜像仓库中已经导入镜像 `acs-reg.alipay.com/acloud/containerdefaultimage:1.3` 。

操作步骤

1. 登录云游 Local 控制台。
2. 在 **产品基线** 页面单击目标产品。
3. 单击 **应用** 页签，然后单击目标应用。
4. 下线目标容器。
   - 下线单个容器

a. 单击目标容器右侧的 **下线**。

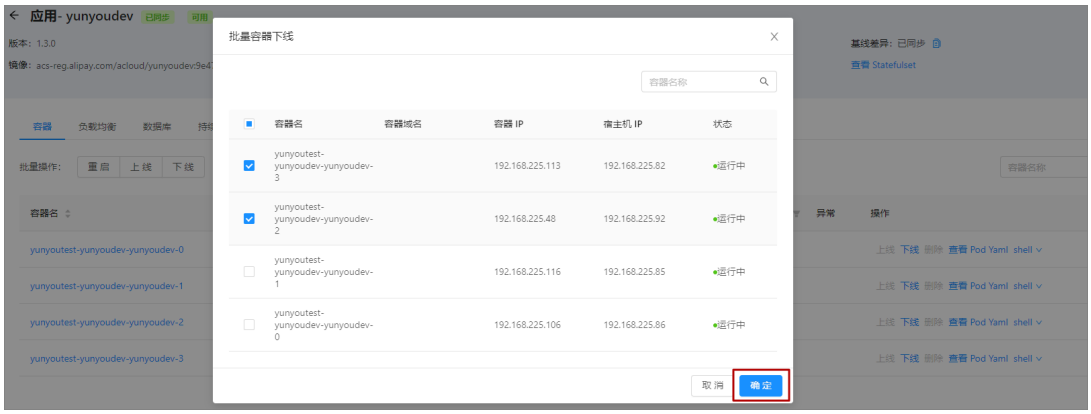


b. 在 **新建运维单** 页面单击 **容器下线**，然后单击 **确定**。

- 批量下线容器

a. 单击 **批量操作** 区域的 **下线**。

b. 选中目录容器后，单击确定。



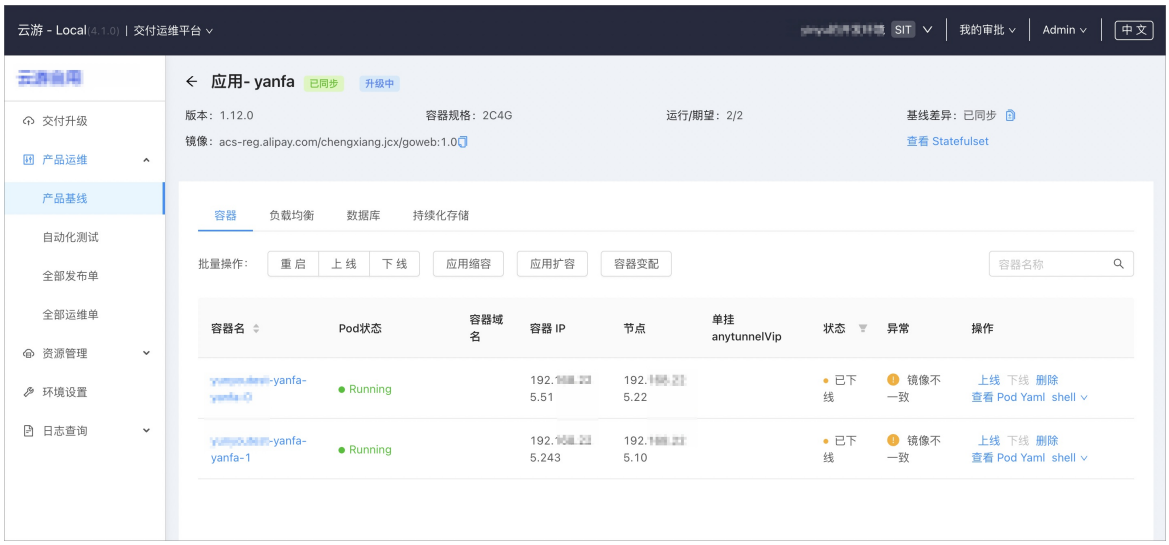
c. 在 **新建运维单** 页面选择部署策略。

推荐使用 **分两组** 策略平滑关闭服务。如果已经确认业务风险，可以选择 **共分一组** 策略，多个 Pod 会同时替换镜像。

d. 单击 **容器下线**，然后单击 **确定**。

当容器下线后，在 **发布详情** 页可以看到容器虽然还在运行，但是服务已不可用。

在应用详情页面可以看到 **基线差异** 已自动同步，容器状态为 **已下线**，镜像已被替换，与应用期望的镜像不一致。



2.8.1.4.7. 容器上线

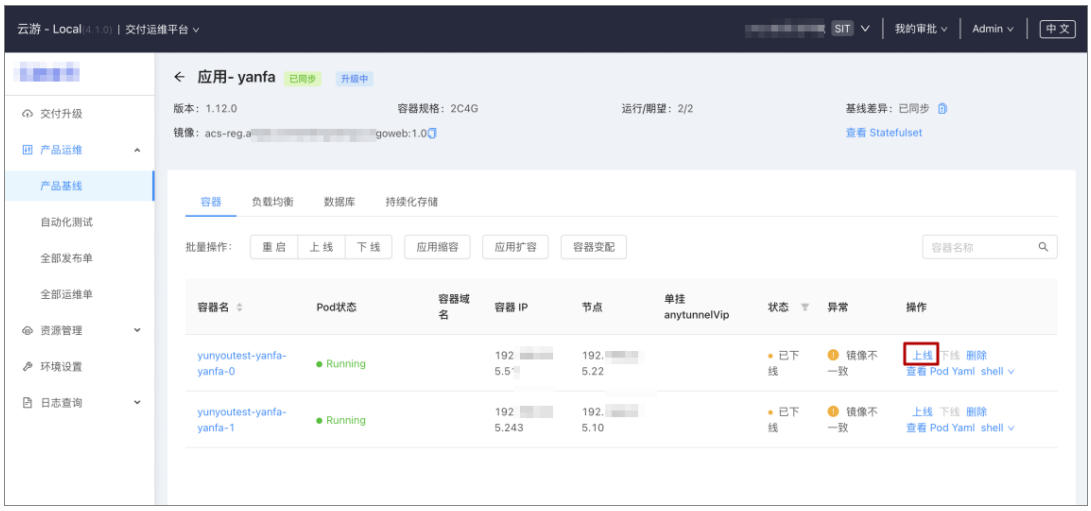
容器上线是将已下线的容器重新上线，即服务上线。云游的处理方法是将已下线的容器从不提供服务的基础镜像替换回期望的应用镜像。

操作步骤

1. 登录云游 Local 控制台。
2. 在 **产品基线** 页面单击目标产品。
3. 单击 **应用** 页签，然后单击目标应用。
4. 上线目标容器。

- 上线单个容器

  a. 单击目标容器右侧的 **上线**。

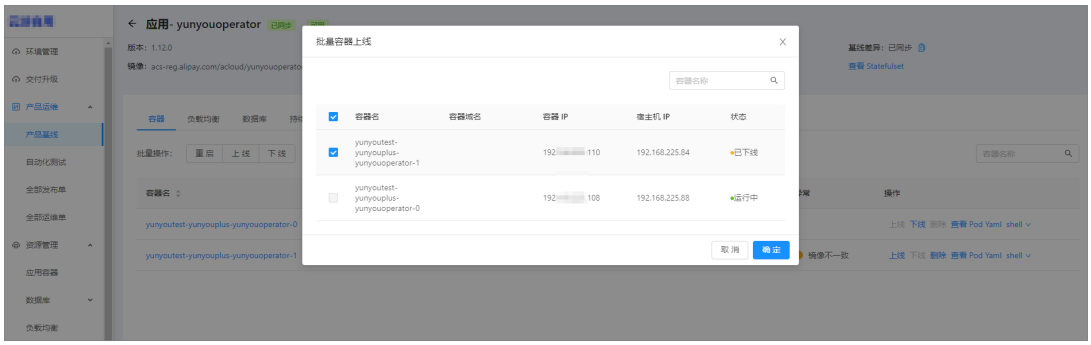


  b. 在 **新建运维单** 页面单击 **容器上线**，然后单击 **确定**。

- 批量上线容器

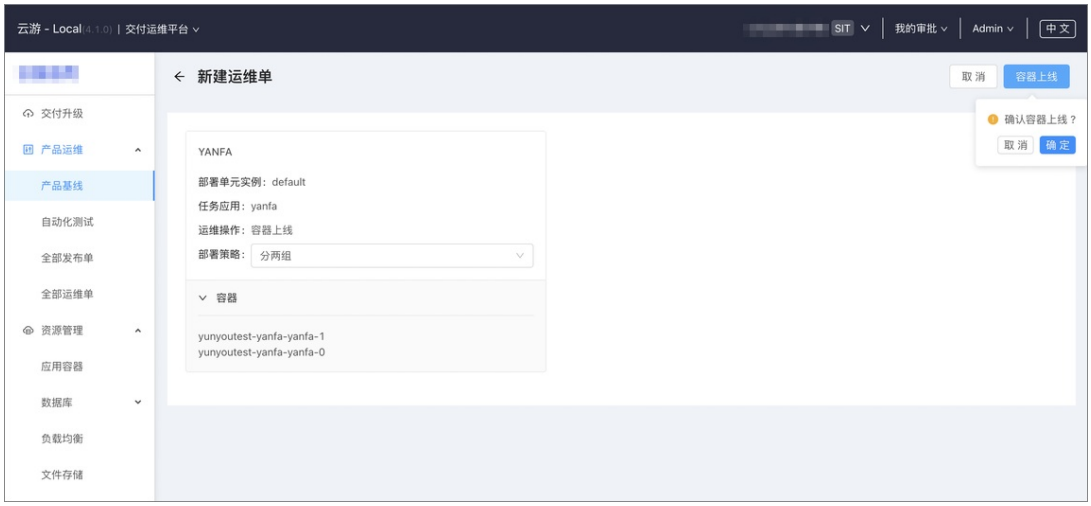
  a. 单击 **批量操作** 区域的 **上线**。

  b. 选中目录容器后，单击 **确定**。



  c. 在 **新建运维单** 页面选择部署策略。

  推荐使用 **分两组** 策略灰度上线。



d. 单击 **容器上线**，然后单击 **确定**。

2.8.1.4.8. 重启容器

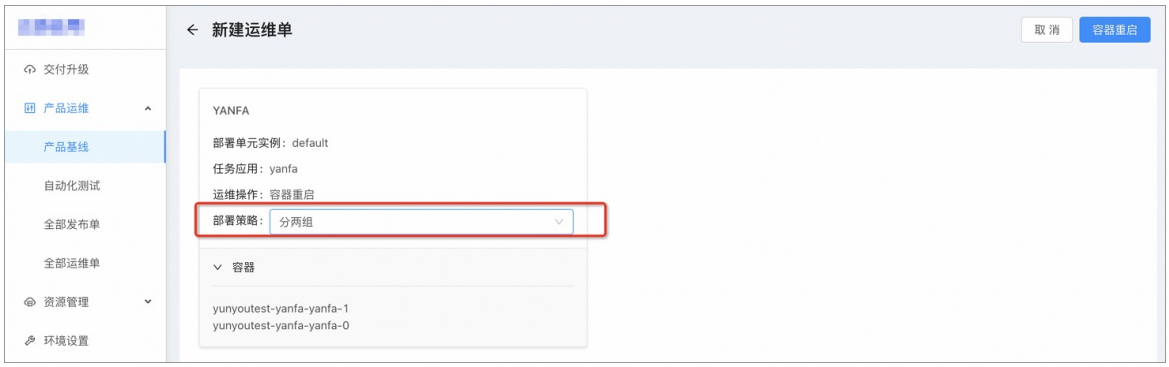
重启容器是指将指定容器（Pod）销毁后重新按期望调度出相同数量的新容器。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **产品基线**。
3. 在产品列表中，单击目标产品。
4. 单击 **应用** 页签，然后单击目标应用。
5. 单击 **容器** 页签，然后单击 **批量操作** 的 **重启** 按钮。

6. 选中一个或多个目标容器后单击 **确定**。
7. 在 **新建运维单** 页面单击 **容器重启**，然后单击 **确定**。

   如果您选择了多个容器，建议将 **部署策略** 修改为 **分两组**，以免所有运行容器同时销毁，导致业务中断。



2.8.1.4.9. 删除容器

删除容器实际是缩容操作，您需要先将容器下线后才可删除。删除容器时会从最后一个容器进行摧毁。

> **注意**
>
> 不建议使用该功能，如果您是希望让 Pod 销毁后重新运行，请使用重启操作。操作步骤请参见 重启容器。

2.8.2. 自动化测试

对于配备自动化测试镜像的产品，您可以配置自动化测试，以验证产品是否可用。

前提条件

已在云游 Global 上为产品中规划了自动化测试应用，且自动化测试的镜像可用。

操作步骤

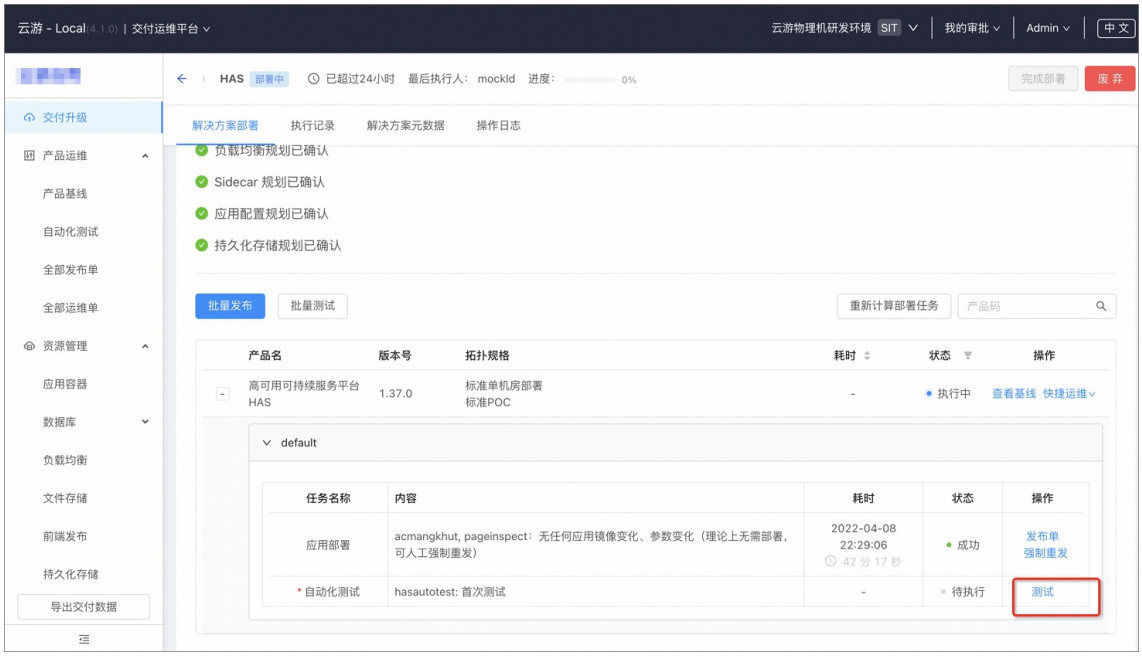
您可以通过以下两种方式配置自动化测试：

方式一

您可以在 **解决方案部署** 页面配置自动化测试，步骤如下：

1. 登录云游 Local 控制台。
2. 在左侧导航栏单击 **交付升级**，然后单击目标解决方案。
3. 在 **解决方案部署** 页面进行自动化测试。
   - 单个测试

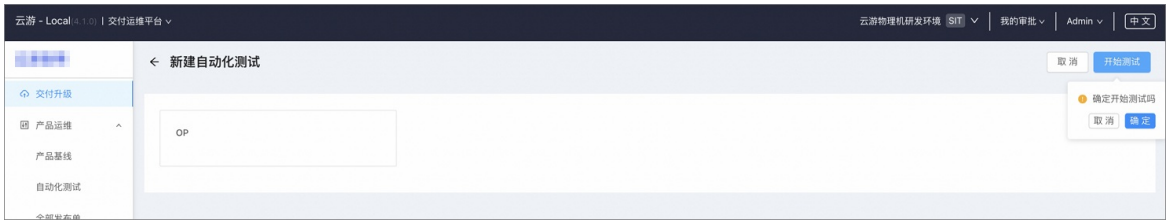
     找到规划好的自动化测试任务，然后单击 **测试**。



   - 批量测试

若您需要同时测试多个应用，可以单击 **批量测试**，然后选择目标应用后单击 **确定**。

4. 在 **新建自动化测试** 页面单击 **开始测试**，然后单击 **确定**。

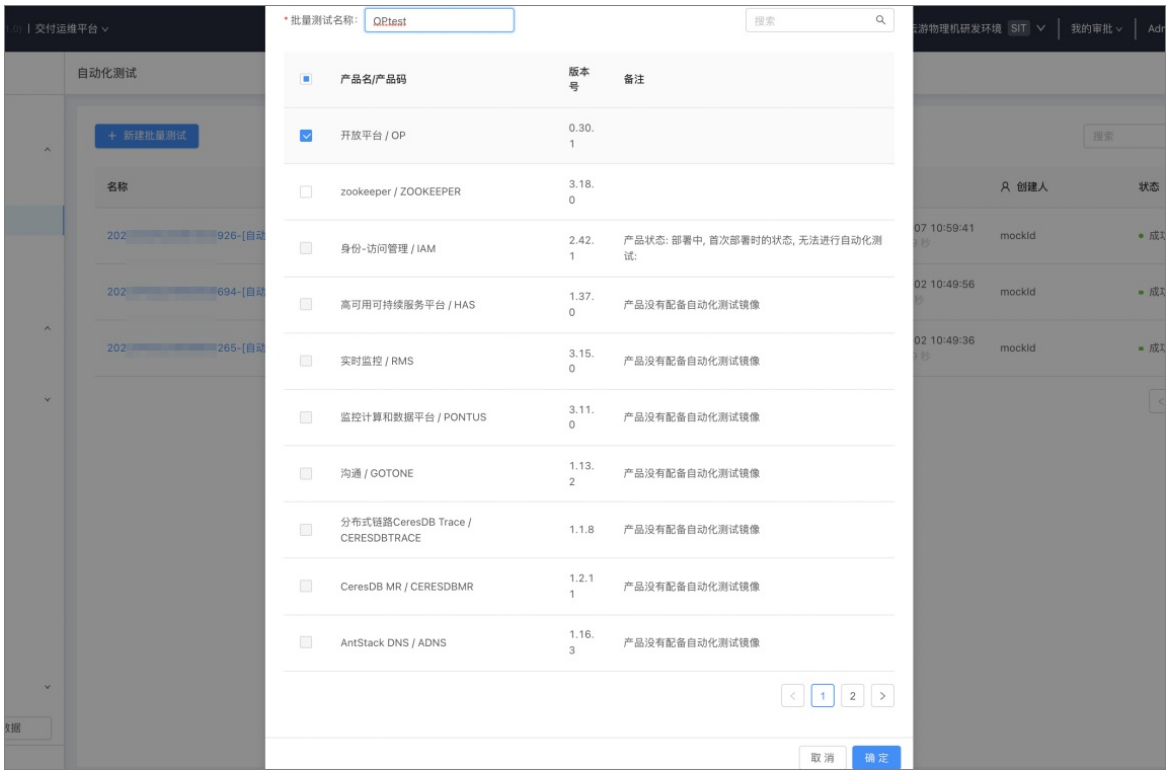


您可以在跳转的 **自动化测试** 页面查看测试进程和测试报告。

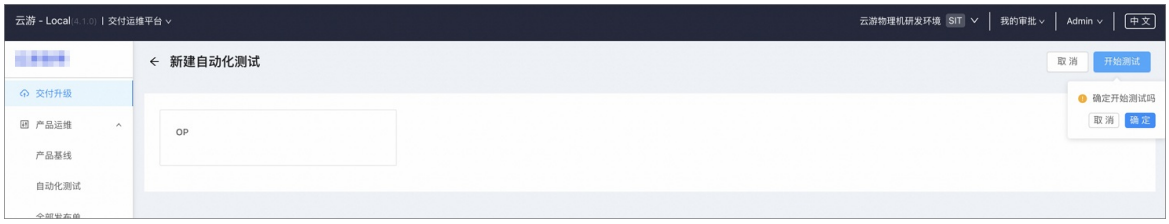
方式二

1. 在左侧导航栏，选择 **产品运维** > **自动化测试**。
2. 在 **自动化测试** 页面单击 **新建批量测试**。

3. 在 **新建批量测试** 对话框填写 **批量测试名称**，然后选择待测试的产品。



4. 单击 **确定**。
5. 在 **新建自动化测试** 页面单击 **开始测试**，然后单击 **确定**。



您可以在跳转的 **自动化测试** 页面查看测试进程和测试报告。

自动化测试出错

若自动化测试任务出现报错，可以选择以下方式处理：

- 单击 **重试**：重新发起自动化测试容器，但有可能仍然执行失败。建议您先查看自动化测试的日志，解决报错问题。
- 单击 **跳过**：忽略本次自动化测试遇到的问题，认可自动化测试结果成功。
- 单击 **取消**：取消本次自动化测试。

- 如果遇到了卡单请单击 **强制取消**。

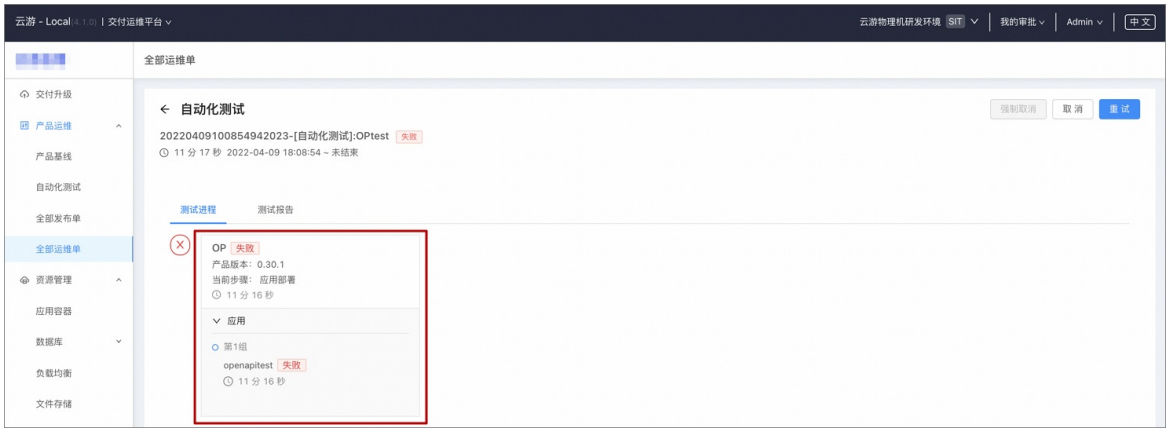
查看自动化测试日志

您可以通过如下步骤查看自动化测试日志：

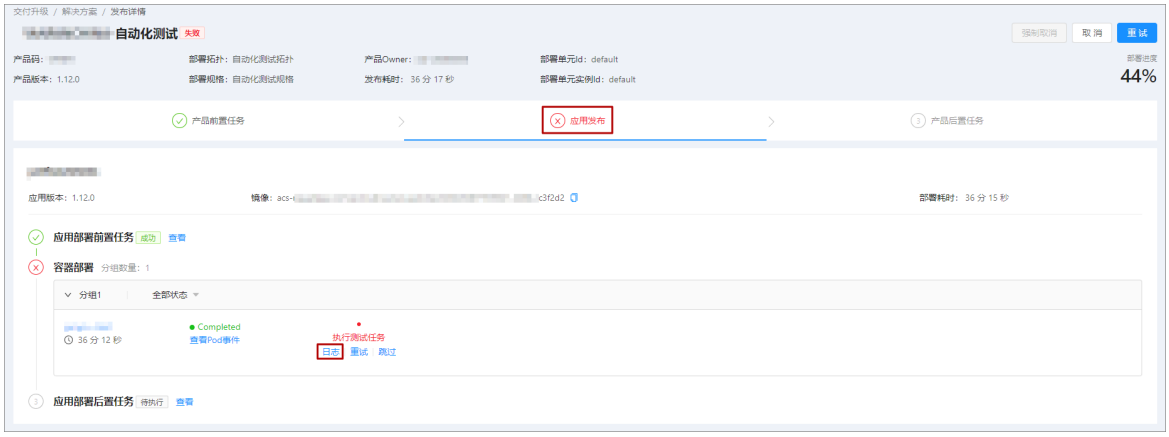
1. 在 **解决方案部署** 页面单击目标自动化测试任务右侧的 **测试单**。

   您也可以在 **自动化测试** 页面单击目标自动化测试任务名称。

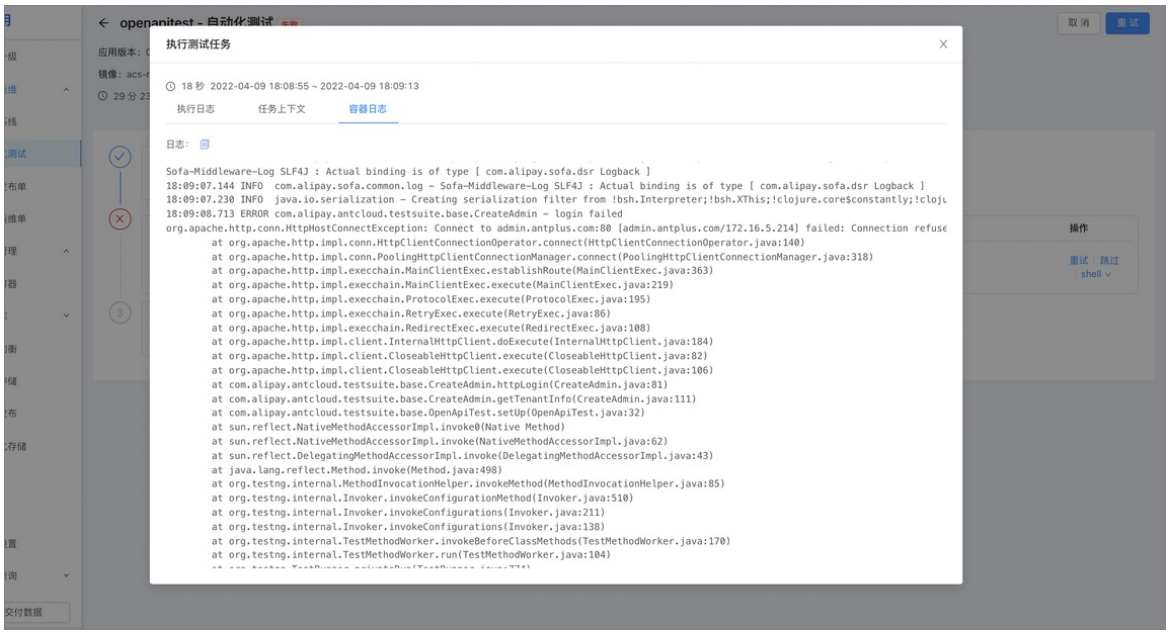
2. 单击 **测试进程** 页签，然后单击目标应用卡片。



3. 单击报错的步骤，然后单击 **日志**。



您可以查看执行日志、任务上下文和容器日志：



2.8.3. 查看全部发布单

您可以通过云游 Local 控制台查看所有已进行的产品部署和解决方案部署发布单，快速了解所有发布单的状态，发现潜在问题。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏选择 **产品运维 > 全部发布单**。

在 **全部发布单** 列表，您可以查看所有已进行的发布单，包括发布单名称、类型、创建日期、创建人、状态等信息。您还可以单击 图标对发布单进行筛选。

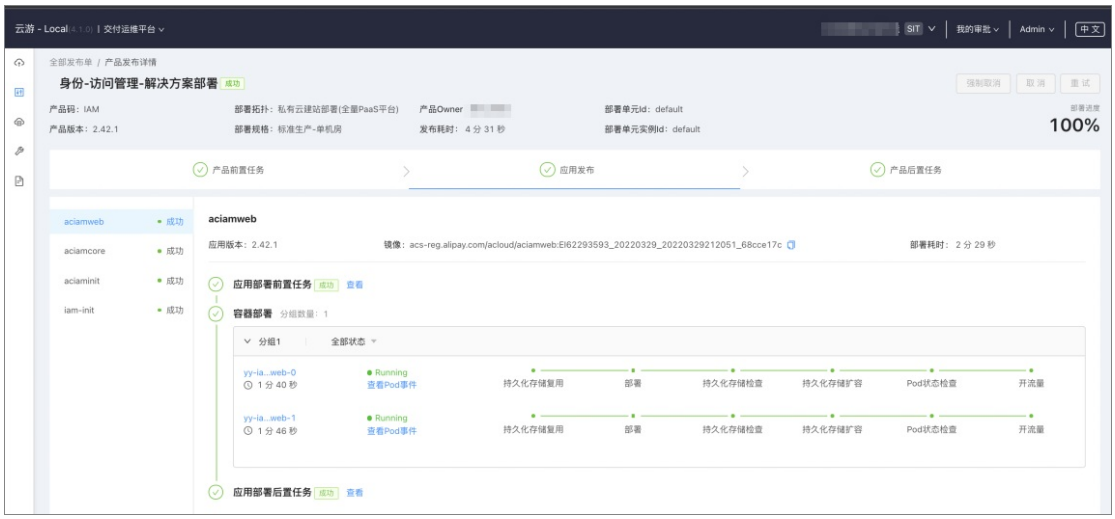
3. 单击目标发布单名称。

   在 **产品发布详情** 页面，您可以查看发布单的状态、部署进度、产品版本等信息。

   - 单击 **产品前置任务**，然后单击目标任务右侧的 **查看**，您可以查看到任务的状态、结果、参数、日志等信息。
   - 单击 **应用发布**，然后在 **容器部署** 区域可查看以下信息：
     - 单击分组可查看容器状态。
     - 单击分组中的容器名称可查看容器的环境变量、日志、Pod 事件等信息。
     - 光标放到 Pod 运行状态上可以可以查看 Pod 运行信息：

     - `PodScheduled: True` 表示 Pod 已经成功被调度到某节点。
     - `ContainersReady: True` 表示 Pod 中所有容器都已就绪。
     - `Initialized: True` 表示 Pod 中所有的 Init 容器 都已成功完成。
     - `Ready: True` 表示 Pod 可以为请求提供服务，并且应该被添加到对应服务的负载均衡池中。
     - `com.alipay.acs.engine/statefulset-pod-online: True` 是云游自定义的检测条件，true 表示 readinessgates 探测成功，SLB后端挂载上 Pod，可以引流进入 Pod。

- 单击 **查看 Pod 事件** 可以看到集群中的事件，方便排查集群问题。



  - 单击 **产品后置任务**，然后单击目标任务右侧的 **查看**，可以查看到任务的状态、结果、参数、日志等信息。

对于失败的发布单，您可以进行重试、跳过和回滚操作；对于成功和已取消的发布单，您可以进行回滚操作；如果遇到了卡单请单击 **强制取消**。

2.8.4. 查看全部运维单

您可以通过云游 Local 控制台查看所有创建的运维单，以了解产品进行的操作。

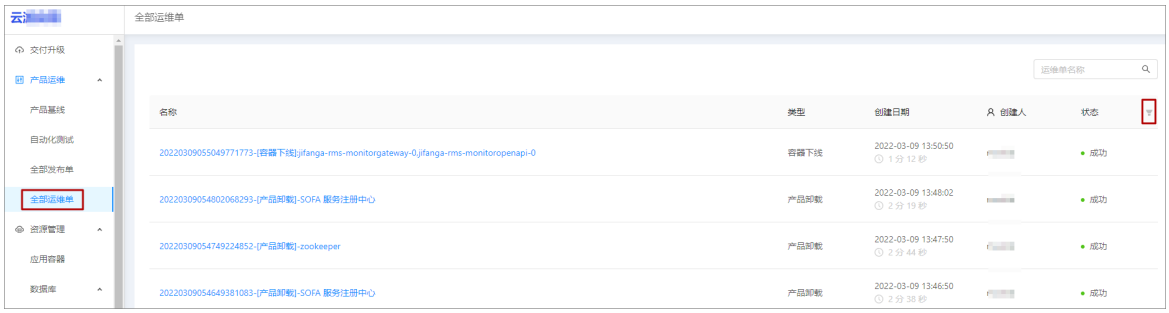
通过云游 Local 控制台查看的运维单包括：

- 重启容器
- 容器上线、下线
- 容器扩容、缩容
- 容器变配
- 产品卸载
- 单元实例卸载
- 产品回滚

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **产品运维** > **全部运维单**。

在 **全部运维单** 列表，您可以查看运维单的名称、类型、创建日期、创建人、状态等信息。您还可以单击 图标对运维单进行筛选。



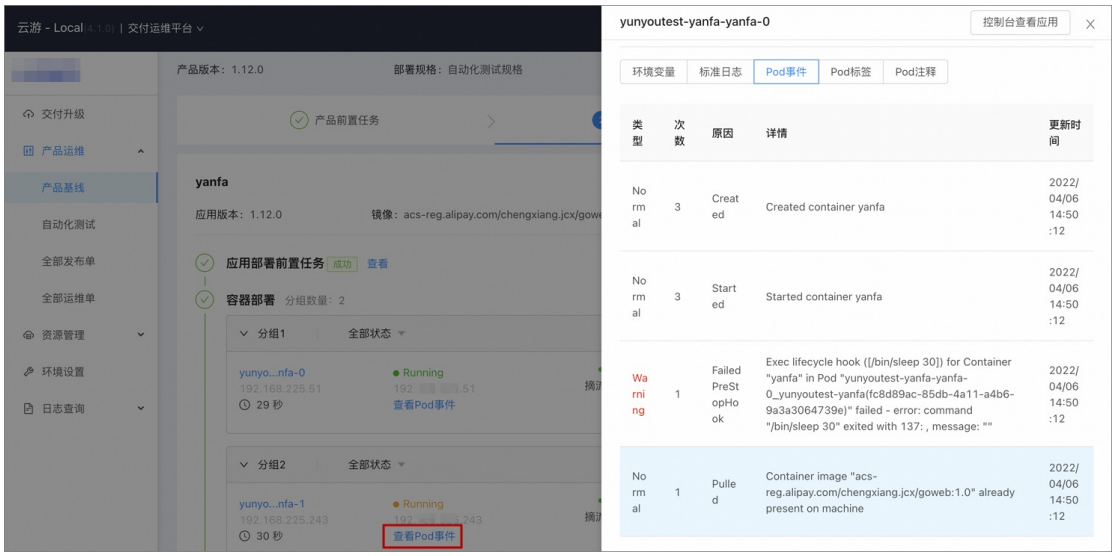
3. 单击目标运维单名称。

   在 **产品运维详情** 页面，您可以查看运维单的状态、部署进度、产品版本等信息。

   - 单击 **产品前置任务**，然后单击目标任务右侧的 **查看**，您可以查看到任务的状态、结果、参数、日志等信息。
   - 单击 **应用发布**，然后在 **容器部署** 区域可查看以下信息：
     - 单击分组可查看容器状态。
     - 单击分组中的容器名称可查看容器的环境变量、日志、Pod 事件等信息。
     - 光标放到 Pod 运行状态上可以可以查看 Pod 运行信息：

     - `PodScheduled: True` 表示 Pod 已经成功被调度到某节点。
     - `ContainersReady: True` 表示 Pod 中所有容器都已就绪。
     - `Initialized: True` 表示 Pod 中所有的 Init 容器 都已成功完成。
     - `Ready: True` 表示 Pod 可以为请求提供服务，并且应该被添加到对应服务的负载均衡池中。
     - `com.alipay.acs.engine/statefulset-pod-online: True` 是云游自定义的检测条件，true 表示 readinessgates 探测成功，SLB后端挂载上 Pod，可以引流进入 Pod。

- 单击 **查看 Pod 事件** 可以看到集群中的事件，方便排查集群问题。



- 单击 **产品后置任务**，然后单击目标任务右侧的 **查看**，您可以查看到任务的状态、结果、参数、日志等信息。

对于失败的运维单，您可以进行重试、跳过和回滚操作；对于成功和已取消的运维单，您可以进行回滚操作。如果遇到了卡单请单击 **强制取消**。

2.8.5. 伸缩组

伸缩组 scaling group 定义了产品中一个或多个应用需要在中枢集群中部署多份的一种按分组扩展的方式。使用伸缩组时，每个分组的扩容和卸载操作、每个分组的实例的启停操作都相互独立。您可以自由扩展应用中的资源，例如 LB、DNS、DB、PV 等，云游会自动创建这些资源给应用实例挂载。

背景信息

云游并没有单元化的概念，原来的部署单元也只是想表达分组的概念，分组是对业务透明的。为避免部署单元与与其他平台中单元混淆，将部署单元重命名为伸缩组，并增强了各项能力。伸缩组特性包括：

- 支持伸缩组的创建（扩容）、缩容（卸载）。
- 每个分组中的同一应用的版本一致，即同一应用的 Pod 的镜像版本一致。
- 每个分组中的同一应用的 Pod 启动参数的数量和 Key 一致。
- 支持分组中 Pod 的扩、缩容。
- 支持自定义伸缩组内的 Pod 副本数和 Pod 规格。
- 负载均衡 LB、DNS 域名可扩展，云游会自动为每个分组创建出拓扑定义的 LB，并为其分配域名。分组内的 Pod 正常启动后会自动挂载到 LB 后端。

- 支持为有状态应用的 Pod 自动创建独立的持久化存储卷并挂载。
- 对于共库的应用（即应用实例属于同一套），在 Pod 启动后会自动连入同一个数据库。
- 对于不共库的应用，扩容分组时为应用分配对应的独占数据库实例使用。
- 支持通过解决方案，更新伸缩组 Pod 的镜像版本。
- 1.9.8 及以上版本支持回滚伸缩组中 Pod 的镜像版本。
- 1.12.x 及以上版本支持批量创建伸缩组。

操作步骤

1. 在云游 Global 中制作并导出解决方案。

   本文以 ODP 产品为例，操作步骤如下：

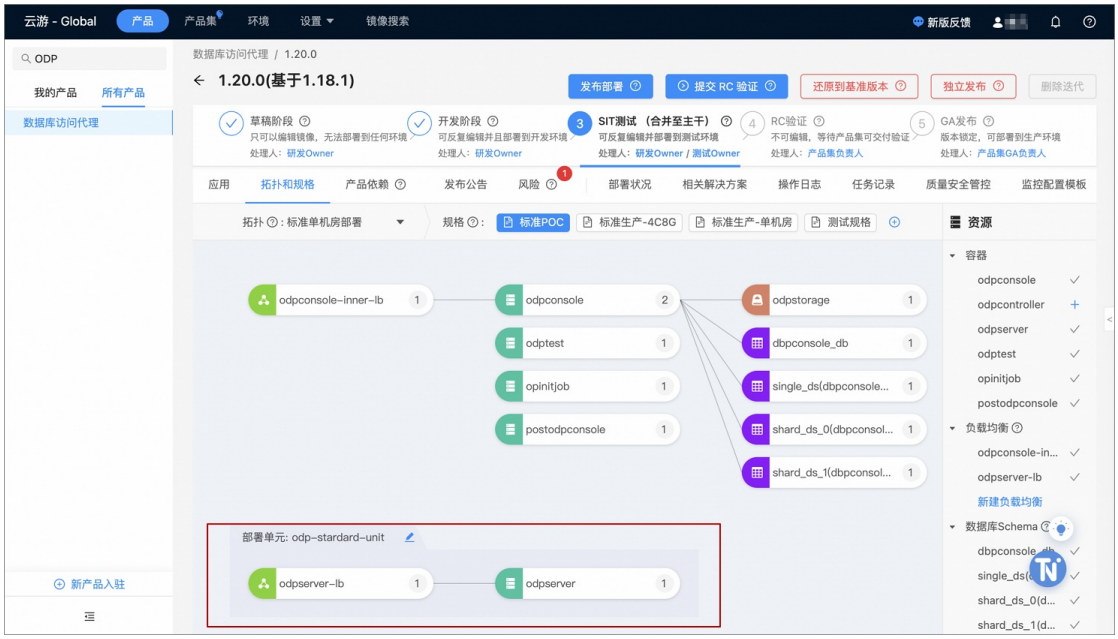
   i. 登录云游 Global。

   ii. 在顶部菜单栏单击 **产品**。

   iii. 在左侧导航栏单击 **所有产品**，然后在搜索栏中输入 **ODP**，并按回车键。

   iv. 单击 **数据库访问代理**，然后在左侧单击目标版本。

   v. 单击 **拓扑和规划** 页签，然后创建可扩展组，并将需要部署多份的应用移入并连接依赖资源。



   vi. 单击 **应用**，然后单击目标应用。

   vii. 对分组应用注入 Cell 参数，用于标识所在不同分组。

   启动参数的数量和 KV 应一致。

   viii. 将制作好的解决方案导出。

2. 在云游 Local 导入解决方案。

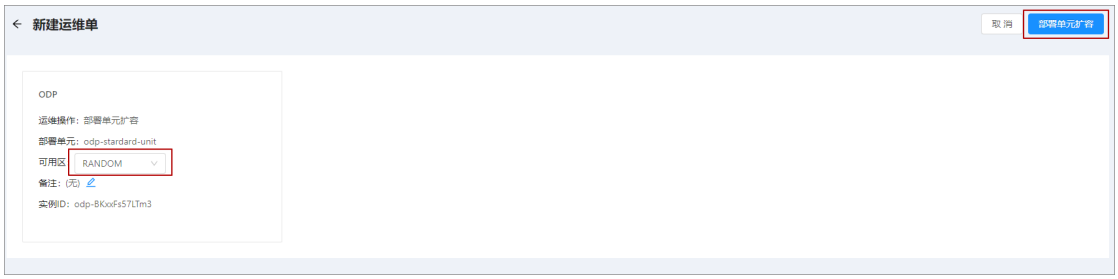
   操作步骤请参见 导入解决方案。

3. 部署完成后，在左侧导航栏单击 **产品基线**，然后在产品基线中单击 **数据库访问代理**。

4. 为分组扩容。

   i. 在 **部署单元** 区域单击 **扩容**。

ii. 选择可用区后，单击 **部署单元扩容**，然后单击 **确认**。



扩容完成后，分组显示如下：

部署完成后：

- 产品基线的参数无变化、资源无变化。
- 运维操作：
  - 分组内实例的重启，操作不变。
  - 卸载分组，操作不变，可选择只删除 Schema 或者数据库实例一并删除。
  - 如果升级解决方案更换镜像，可以按分组更新。

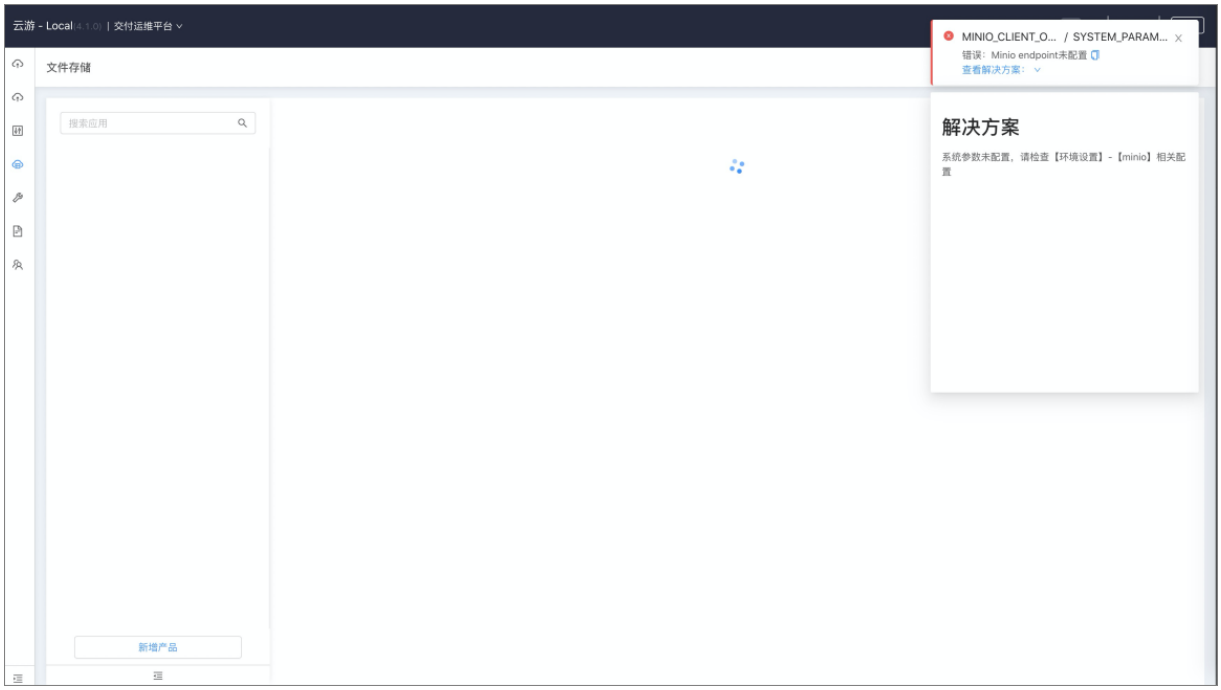
    更换镜像后，建议先通过发布预览功能预览，再执行。
  - 如果解决方案修改规格，所有分组都要重启。

    修改后，建议先通过发布预览功能预览，再执行。

2.8.6. 错误码

为方便云游 Local 的使用者能够在前端知道报错的含义、错误的原因及解决方案，云游 Local 在 1.12.0 及以上版本升级了错误码功能，让使用者可以明确出错时的问题原因及建议的解决方案，以便更好地使用云游 Local。

云游 Local 一改以往直接暴露内部错误代码给用户的方式，以一种更直观的方式为用户展示错误信息，并附加解决问题的建议，让您可以清楚的了解问题的原因，以及如何解决问题。例如如下报错信息：



- 错误码为：`MINIO_CLIENT_OPERATE/SYSTEM_PARAM_UNDEFINED`
- 报错原因：系统参数没有配置 minio Endpoint。
- 解决方案：检查 **环境设置** 中 **minio** 的相关配置是否正常。

2.8.7. 无人值守

云游 Local 的无人值守定义了错误处理机制。云游 Local 目前已预定义了部分场景的处理操作。云游 Local 在遇到指定场景时，会使用对应的操作去尝试解决问题。

预置的场景

无人值守目前预置的场景如下：

- Pod 启动超时。
- Pod 拉取镜像时间过长。
- 阿里云的接口调用失败（例如 SLB 摘流、挂载失败）。

预置的操作

- 重试：重试本次操作。
- 取消：取消本次操作。
- 跳过：跳过本次操作。

操作示例

本文以 Readiness 探针失败模拟 Pod 启动超时的场景，演示无人值守的操作流程。

1. 登录云游 Local。

2. 在左侧导航栏选择 **产品运维 > 全部发布单**。
3. 单击失败的发布单名称，进入 **产品发布详情** 页面。

4. 单击 **查看 Pod 事件**。

   报错原因为：Readiness 检查失败。

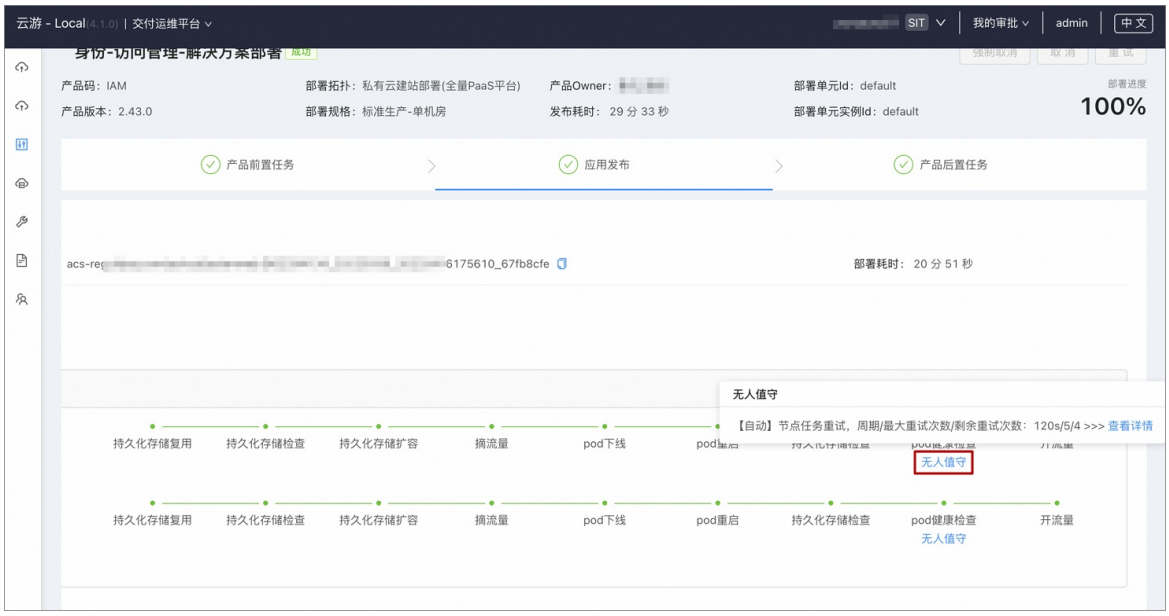
5. 返回 **产品发布详情** 页，单击出错节点下的 **日志**。

6. 展开 **执行结果失败**。

查看失败信息如下：

- 本次的错误码为：`TASK_NODE_FAILED/TASK_NODE_MAX_RETRY_TIMES` 。
- 失败原因：重试超过最大次数。
- 解决方法：按提示检查日志，尝试 **重试** 或 **跳过**。

7. 操作成功后，可单击 **无人值守** ，查看无人值守的执行记录。



单击 **查看详情**，可查看当时的场景、执行的操作、执行的时间和尝试的次数。

2.9. 资源管理

2.9.1. 管理应用容器

应用容器页面提供了集群中的容器列表信息，包括容器名称、容器 IP、所属机房、节点 IP、所属应用、所属产品及容器状态。

操作步骤

1. 登录云游 Local 控制台。

2. 在左侧导航栏，选择 **资源管理** > **应用容器**。
3. 在 **应用容器** 页面选择 **当前环境** 或 **所有环境**。
4. 单击目标容器名称跳转至集群管理平台（AKE 云原生平台），进行更多的操作管理。

> **说明**
>
> Kubernetes 是流行的开源容器编排技术。为了让您可以方便地在云游上使用 Kubernetes 管理容器应用，云游提供了 Kubernetes 集群管理支持。

2.9.2. 管理数据库实例

2.9.2.1. 新增数据库实例

您可以在当前环境或者全量环境中新增自定义数据库实例。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **数据库** > **物理实例视角**。
3. 单击 **新增自定义数据库实例**，然后根据实际情况添加数据库实例。

   目前支持 OceanBase、MySql、RDS 三种数据库实例：

   - OceanBase

     单击 **OCEANBASE**，然后根据情况选择 **已知租户 ID** 或 **不知租户 ID**：

     - **已知租户 ID**：单击 **添加**，然后填写 OceanBase 数据库实例名称和租户 ID即可。云游会自动创建 Schema、账号，无需手动录入 Schema。
     - **不知租户 ID**：单击 **添加**，然后填写 OceanBase 数据库实例的名称、服务地址、端口、CPU、内存、硬盘等信息。添加完成后，您还需要单击实例名称，然后在实例详情中添加 Schema 信息。

   - MySQL

     - 单击 **MYSQL**，然后单击 **添加**。
     - 填写 MySQL 数据库实例的名称、服务地址、端口、CPU、内存、硬盘等信息后单击 **确定**。

       添加完成后，您还需要单击实例名称，然后在实例详情中添加 Schema 信息。

   - RDS

     单击 **RDS**，然后单击 **添加**，并填写 RDS 数据库实例名称和资源 ID 即可。云游会自动创建 Schema、账号，无需手动录入 Schema。

2.9.2.2. 查看数据库

您可以通过云游 Local 控制台查看和管理您的数据库实例。

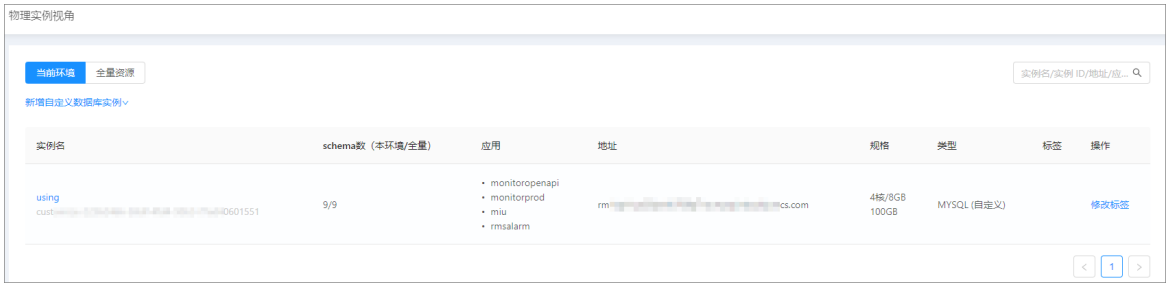
物理实例视角

以数据库物理实例为维度，查看所有数据库信息。

1. 登录云游 Local 控制台。

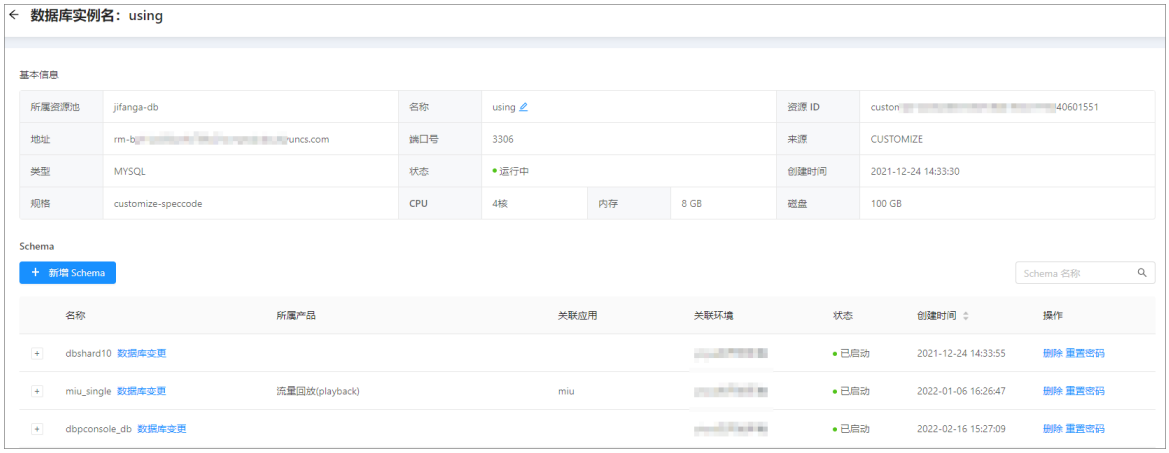
2. 在左侧导航栏，选择 **资源管理 > 数据库 > 物理实例视角**。
3. 在 **物理实例视角** 页面选择 **当前环境** 或 **所有环境**。

   您可以在数据库列表中查看所有数据库的基本信息，例如实例名、schema 数、应用、地址等信息。



4. 单击目标数据库名称。

   您可以查看目标数据库的详细信息，例如名称、资源 ID 、IP 地址、端口号等信息。您也可以单击 **新增 Schema**，为数据库实例增加 Schema。



Schema 视角

以数据库 Schema 为维度，查看所有数据库信息。

1. 在云游 Local 控制台的左侧导航栏，选择 **资源管理 > 数据库 > Schema 视角**。
2. 在 **Schema 视角** 页面选择 **当前环境** 或 **所有环境**。

   您可以在数据库列表中查看所有数据库的基本信息，例如 Schema 名称、所属物理实例、应用、数据库类型、物理实例状态等信息。

3. 单击所属的物理实例名称。

   您可以查看数据库 Schema 所属的物理实例的详细信息，例如名称、资源 ID 、IP 地址、端口号等信息。

2.9.2.3. 数据库规划最佳实践

当前云游 Local 数据库的规划流程比较复杂，经常会出现因为误操作而导致交付时间变长、反复卸载产品等问题，用户体验很差。在产品层面，数据库规划流程已经排入了优化流程中。在此之前，您可以参考本文档完成数据库规划。

数据库实例包含了数据库的连接串地址、端口等元数据信息，绑定数据库实例和产品所属 Schema 关系、Schema 关联的用户名和密码。当您进行数据库变更时，需要使用这些元数据进行数据库变更操作；部署应用时，需要将数据库元信息渲染进容器环境变量。

您可以通过云游 Local 复用您已有的 OceanBase、MySQL、RDS 数据库，步骤如下：

步骤一：创建数据库实例

1. 在 OceanBase、MySQL、RDS 数据库实例控制台创建数据库实例。
2. 创建需要绑定到该数据库实例的 Schema。
3. 获取数据库实例的元数据：连接串、用户名、密码。

步骤二：在云游 Local 上录入数据库实例元信息

以下内容以录入 MySQL 数据库实例为例，操作步骤如下：

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **数据库** > **物理实例视角**。
3. 单击 **新增自定义数据库实例**，然后根据实际情况添加数据库实例。
4. 录入 MySQL 实例元信息后，单击 **确定**。

参数	说明
实例名称	填写数据库实例标识，一般填写产品名。
服务地址	填写步骤一中创建的数据库实例的连接串。

参数	说明
端口	填写数据库实例的访问端口。
CPU 核数	填写数据库的 CPU 核数。 一般保持默认即可。
内存	填写数据库的内存大小。 一般保持默认即可。
磁盘	填写数据库的磁盘大小。 一般保持默认即可。

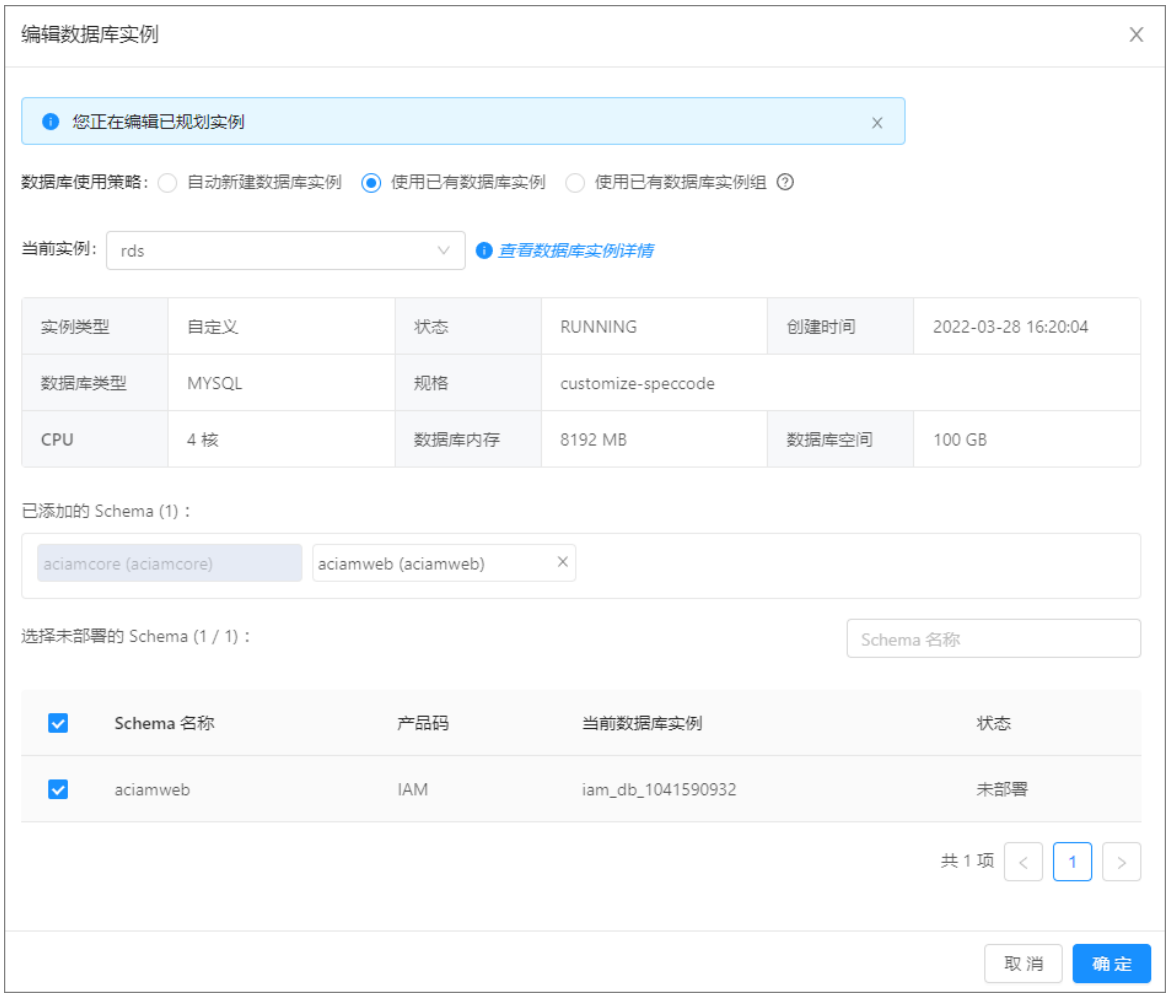
5. 单击刚刚录入的 MySQL 实例名称，然后单击 **新增 Schema**。
6. 单击 **手动输入** 页签，然后单击 **添加**。
7. 填写 **Schema 名称**、**账号**、**密码** 后，单击 **确定**。

步骤三：为解决方案规划数据库

1. 在云游 Local 控制台，单击 **交付升级**。
2. 单击目标解决方案，然后单击 **解决方案元数据**，之后单击 **数据库规划**。

3. 单击 **使用已有数据库** 右侧的加号（+）。

4. 选择需要绑定的数据库，并选择数据库实例绑定的 Schema。



5. 单击 **确定**。

2.9.3. 管理负载均衡

2.9.3.1. 新增负载均衡实例

负载均衡 SLB（Server Load Balancer）是一种对流量进行按需分发的服务，通过将流量分发到不同的后端服务来扩展应用系统的服务吞吐能力，并且可以消除系统中的单点故障，提升应用系统的可用性。您可以在云游控制台添加自定义的负载均衡实例。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **负载均衡**。
3. 在 **负载均衡** 页面选择 **当前环境** 或 **所有环境**，然后选择 **新增自定义负载均衡实例** > **SLB**。

4. 单击 **添加**，并填写负载均衡实例名称和 SLB 资源 ID。

5. 单击 **确定**。

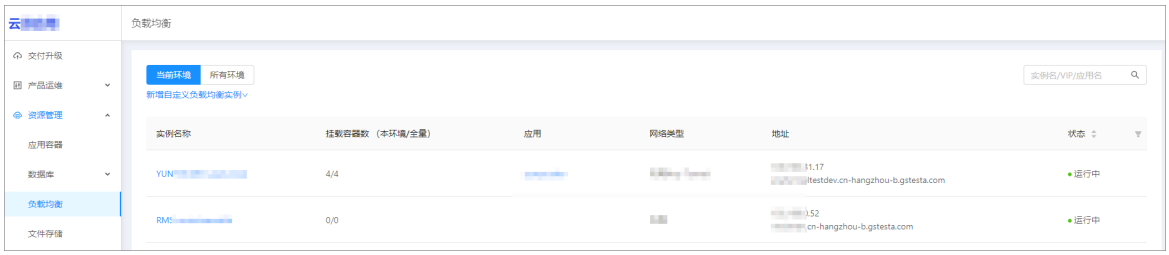
2.9.3.2. 查看负载均衡

您可以通过云游控制台查看当前环境和所有环境的负载均衡使用情况。

操作步骤

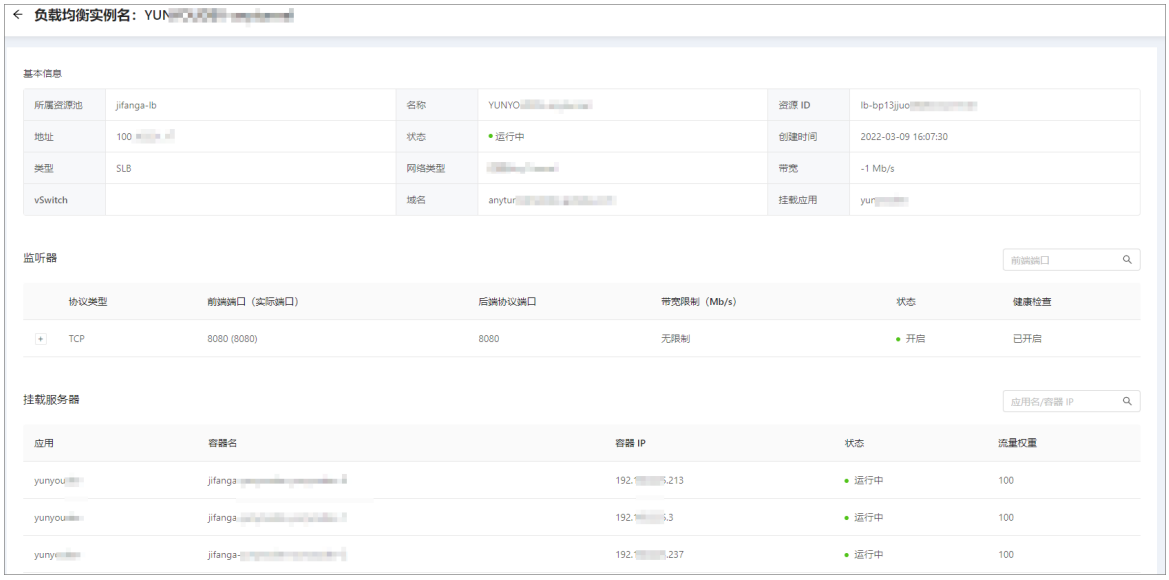
1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **负载均衡**。
3. 在 **负载均衡** 页面选择 **当前环境** 或 **所有环境**。

   您可以在负载均衡列表中查看所有负载均衡的基本信息，例如实例名称、挂载容器数、应用、IP 地址等信息。



4. 单击目标实例名称。

您可以查看目标负载均衡的详细信息，例如所属资源池、名称、资源 ID 、IP 地址、协议端口、挂载服务器等信息。

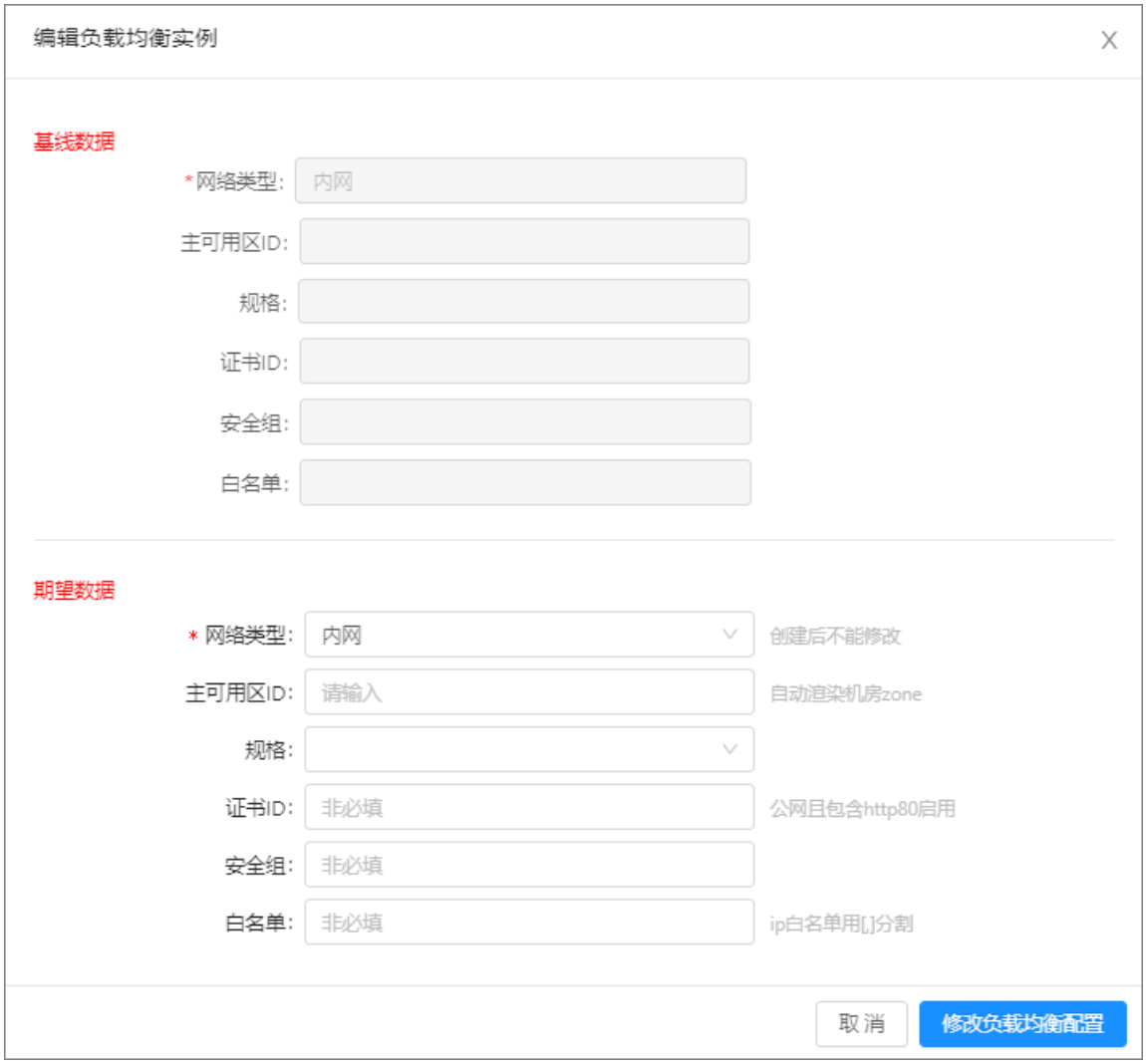


2.9.3.3. 修改负载均衡

对于已创建的负载均衡，您可以随时根据需求进行修改。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **负载均衡**。
3. 在 **负载均衡** 页面选择 **当前环境** 或 **所有环境**。
4. 单击目标负载均衡右侧的 **编辑** 按钮，然后修改 **期望数据**：



参数	说明
网络类型	选择负载均衡的网络类型，根据实际情况选择。
主可用区 ID	填写负载均衡的主可用区 ID。
规格	选择负载均衡的规格。
证书 ID（可选）	填写负载均衡的证书 ID，仅当网络类型为公网，且包含 HTTP 80 端口时填写。
安全组（可选）	填写负载均衡的安全组。
白名单（可选）	填写负载均衡的白名单，IP 白名单使用英文逗号（,）分隔。

5. 单击 **修改负载均衡配置**，然后单击 **确定**。

2.9.4. 前端发布

前端发布功能是蚂蚁科技推出的用于快速部署前端项目的功能。通过前端发布，您可以节约前端专有云交付的时间成本和人力成本，让前端交付像上传文件一般轻松方便。

背景信息

部署前端项目有两种方式，通过 ONEX 控制台发布部署，或者和后端项目一起进行发布部署。

目前，大部分前端项目都是通过 ONEX 控制台进行发布部署，ONEX 控制台在一定程度上承担了专有云的 CDN 角色。但每次前端有修改，需要前端技术人员将最新的前端代码地址同步给 ONEX 控制台的开发，然后重新拉取前端资源并重新打包部署一次，非常麻烦。使用前端发布功能后，前端项目改动无需重新发布后端项目，大大节约前端专有云交付的时间成本和人力成本（从几小时到几分钟）。

操作步骤

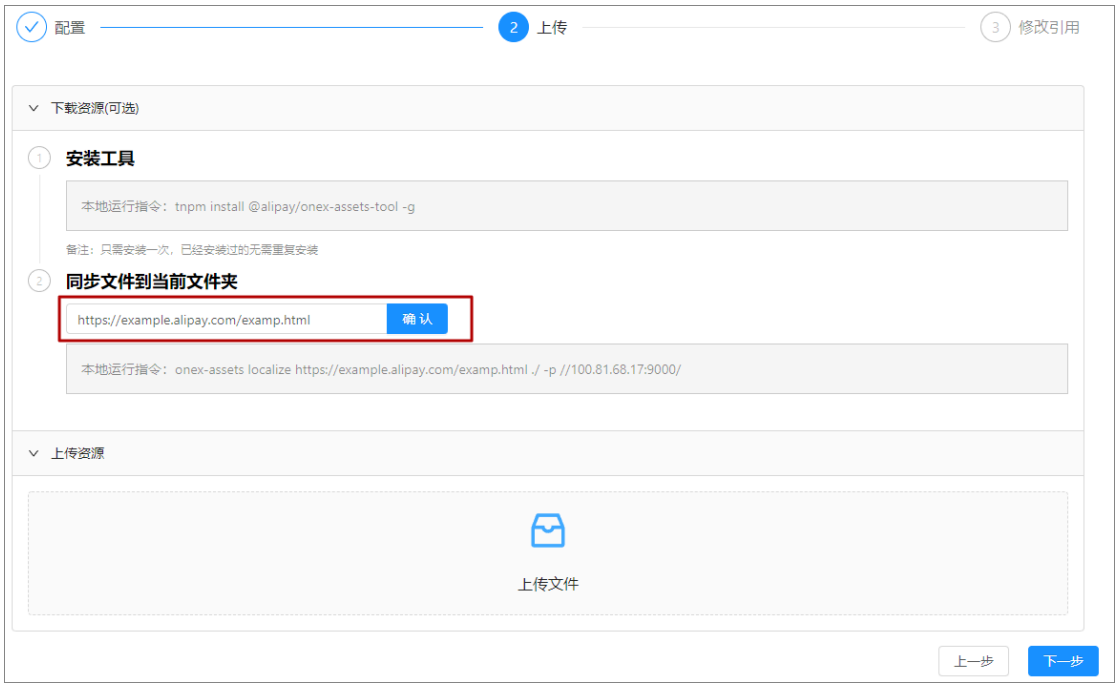
1. 新增应用。
   i. 登录云游 Local 控制台。
   ii. 选择 **资源管理** > **前端发布**，然后单击 **新增应用**。
   iii. 输入应用的名称，并选择应用类型后，单击 **确定**。

      应用类型说明如下：

      - onex：应用部署在 ONEX 控制台。
      - asset：应用部署在后端项目上。
2. 上传项目文件。
   i. 单击刚刚创建的应用名称，然后单击 **新建发布单**。
   ii. 配置发布单描述信息后，单击 **下一步**。
   iii. 本地运行 `tnpm install @alipay/onex-assets-tool -g` 命令。

      > **说明**
      > 执行操作的本地设备上必须安装 tnpm 工具。

iv. 将项目的 HTML 地址复制到 **应用 html** 文本框中，然后单击 **确认**。



v. 在命令行运行刚刚生成的本地运行指令下载项目资源。

```
onex-assets localize https://example.alipay.com/examp.html ./ -p //100.**.**.17:900
0/
```

vi. 单击 **上传文件**，然后将刚刚下载的所有文件上传。

vii. 单击 **下一步**。

viii. 在文件列表中，找到 HTML 文件，然后单击右侧的 **拷贝链接**。

3. 更新前端项目。
   - 非 ONEX 环境

     在自身环境中替换刚刚拷贝的链接。
   - ONEX 环境

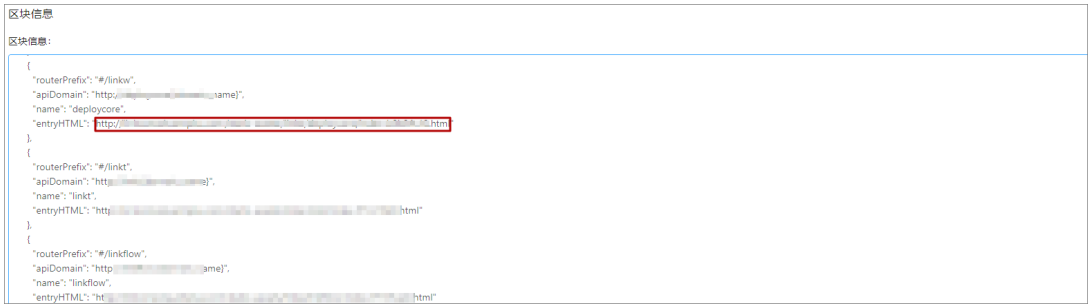
     a. 登录 ONEX 控制台。

     b. 单击 **控制台**，然后在控制台列表中，单击目标控制台名称。

     c. 在 **基本信息** 页签，单击 **更新**。

     d. 将 **区块资源模式** 改为 **本地数据库**。

     e. 在 **区块信息** 中，找到待更新的前端项目，然后替换刚刚复制的 HTML 地址链接。



4. 回到云游 Local，然后单击 **完成**。

2.9.5. 查看文件存储

文件存储功能汇总了当前环境中所有使用了文件存储功能的产品产生的文件存储资源实例。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **文件存储**。
3. 在 **文件存储** 页面，选择 **当前环境** 或 **所有环境**。

   您可以在文件存储列表中查看所有文件存储资源的基本信息，例如资源名称、Bucket 名称、关联应用等。

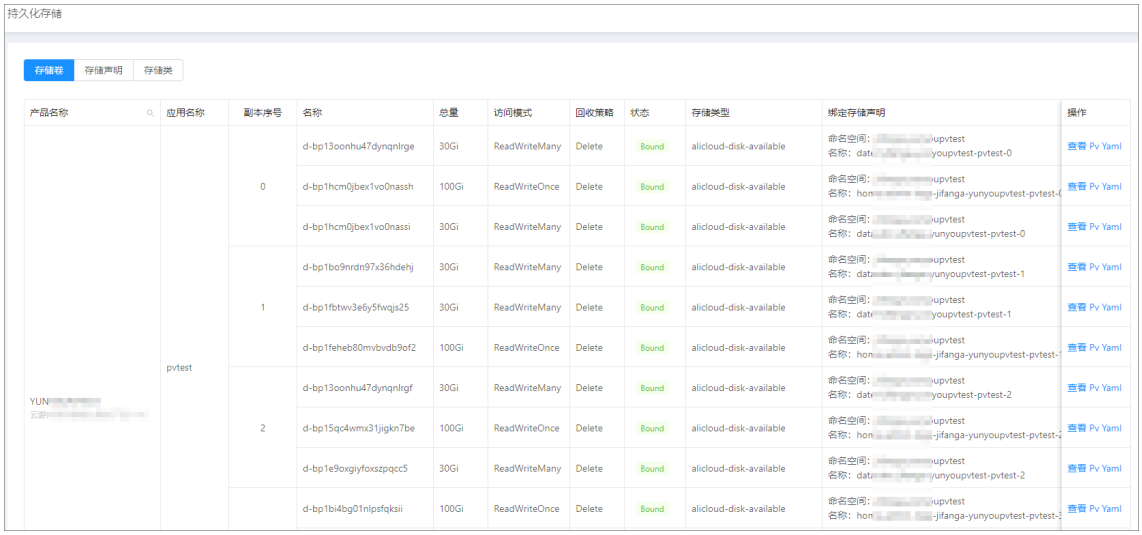
2.9.6. 容器持久化存储

2.9.6.1. 查看容器持久化存储

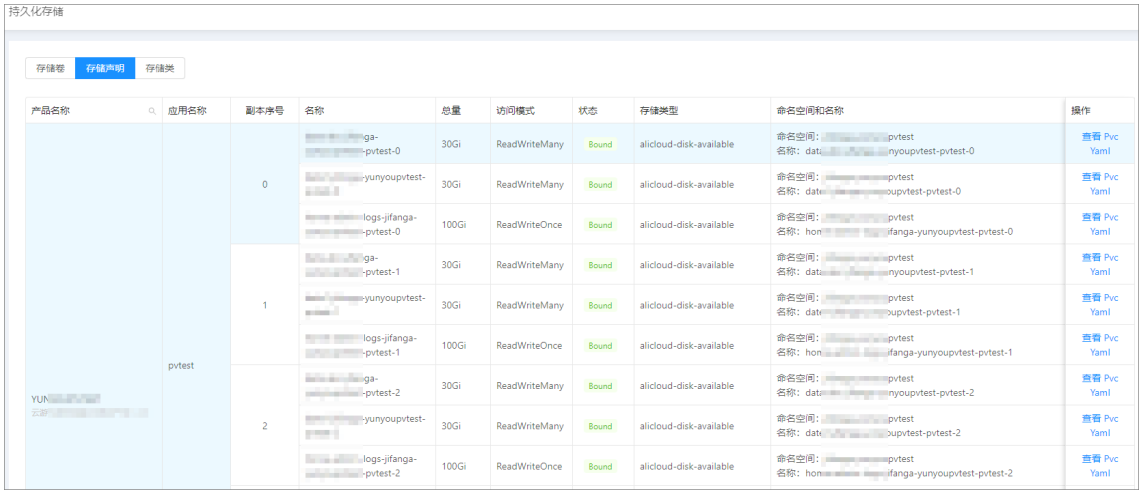
您可以通过云游 Local 控制台查看容器持久化存储的存储卷、存储声明和存储类。

操作步骤

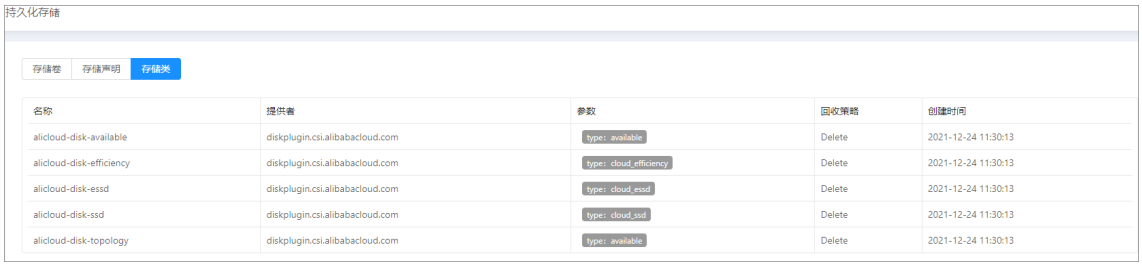
1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理** > **容器持久化存储**。
3. 在 **容器持久化存储** 页面，查看容器持久化存储信息。
   - **存储卷**：查看各产品和应用对应的存储卷信息，包括产品名称、应用名称、副本序号、总量、访问模式等信息。



- **存储声明**：查看各产品和应用对应的存储声明，包括产品名称、应用名称、副本序号、总量、访问模式等信息。



- **存储类**：查看环境涉及的存储类，包括名称、提供者、参数、回收策略、创建时间等。



2.9.6.2. 容器持久化存储最佳实践

前提条件

- 解决方案已导入云游 Local。操作步骤请参见 导入解决方案。
- 集群中已部署 CSI 且创建 storageclass，创建 pvc 后可成功创建出 pv。

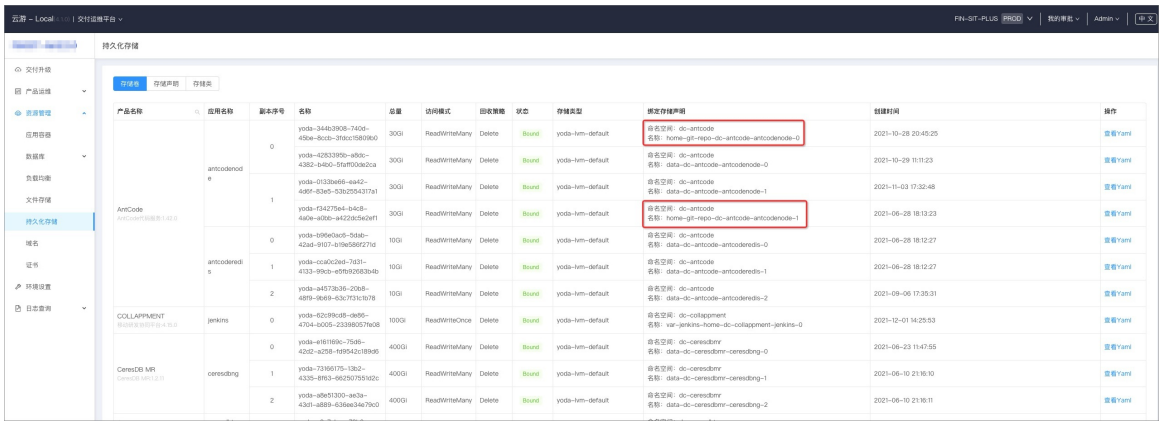
背景信息

由于云游使用了 Statefulset pvcTemplate 控制存储的使用，所以要求一个 pvc 组名称除了最后的序号不同，其余内容必须相同，否则，会导致确认规划报错。示例如下：

以下两个 pvc 属于 `home-git-repo-dc-antcode-antcodeencode` pvc 组，名称分别为：

- home-git-repo-dc-antcode-antcodeencode-0
- home-git-repo-dc-antcode-antcodeencode-1

这两个 pvc 的访问模式、大小、存储类等设置必须一致，如下图所示：



操作步骤

1. 登录云游 Local。
2. 单击 **交付升级**，然后单击目标解决方案。
3. 单击 **解决方案元数据** 页签，然后单击 **持久化存储规划**。
4. 单击目标产品码右侧的 **编辑**。

5. 配置持久化存储参数。

参数说明如下：

参数	说明

参数	说明
使用的存储	首次使用（即未发布过产品）时，会选择 **自动新建持久化存储**。如果是老的站点升级产品且已经存在绑定的 pvc，导入解决方案时会自动识别并且更新使用的存储为绑定的 pv 信息。 **说明** 以下操作可能导致规划中记录的 pv 信息和实际不符合： ○ 通过黑屏模式在后台删除了 pv，规划的 pv 已经不存在。 ○ 卸载产品时，运维单没有正常结束或被跳过。 出现该问题时，您可以重新导入一次解决方案，存储规划状态会变成未规划。您可以将 **使用的存储** 设置为 **自动新建持久化存储**。
存储	按需调整使用的存储大小。 **注意** ○ 如果 pvc 已经绑定了 pv，则不允许对 pv 进行缩容。如果填写的存储大小大于当前绑定的 pv 实际大小，后续发布会进行存储扩容。 ○ 如果同一 pvc 组下存储大小不一致时，无法确认规划。您需要手动扩容 pv 到一致的大小。扩容完成可以重新导入解决方案，刷新存储规划到最新状态。
存储类	云游会自动加载集群中存在的所有存储类，请根据实际环境选择合适的存储类。 yoda 场景推荐使用 `yoda-lvm-default` 。
访问模式	选择访问模式。建议参照 k8s 官方文档 的说明进行选择。 目前只有少数存储类由于特性限制必须使用特定的访问模式。

参数	说明
挂载目录用户	填写挂载目录的用户 ID。 由于云游多数为主站 SOFA 应用以 admin 用户启动，且基础镜像中默认 admin 用户 ID 为 500，所以此处填写为 500。如果是其他应用，您需要按需调整。例如 Neo4j 的 UserID 为100。 **注意** ○ 配置此项前，请确保环境的镜像仓库已导入 `acs-reg.alipay.com/acloud/apyunqing-chown:latest` 。 ○ 云原生下，持久化目录的挂载默认为 root 用户。当应用以非 root 用户启动时，可能遇到权限问题导致应用启动失败。您必须修改挂载目录用户。 ○ 由于每个镜像的用户 ID 都可能不同，所以您可以先本地启动镜像，查看一下使用的用户。进入容器内部后，输入如下命令： `docker run -ti {image_name} bash`
使用匿名卷	选择是否选择匿名卷。 以下情况可能需要使用匿名卷： ○ POC场景，磁盘资源有限，可以接受数据丢失不存储。 ○ 原先应用已经使用了匿名卷，不希望升级产品版本后需要使用存储（这种一般发生在低版本Local 升级到高版本 local 的情况。因为低版本上默认 `/home/admin/logs` 会使用匿名卷，而高版本不会）。 使用匿名卷后指定存储大小等将无效。如果之前已经使用了 pvc（Statefulset 的 pvcTemplate 已经存有 pvc），再勾选匿名卷是无效的。匿名卷的详细说明，请参见 k8s volume。

6. 产品所有应用的存储卷设置完成后单击 **确认全部**。

2.9.7. 查看域名

域名是指您发布的产品和应用绑定的域名，您可以通过云游 Local 控制台查看查看当前环境和所有环境的域名使用情况。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **资源管理 >域名**。
3. 在 **域名** 页面选择 **当前环境** 或 **所有环境**。

   您可以在域名列表中查看所有域名的基本信息，例如域名、IP 地址、状态、网络类型等。

   您还可以针对目标域名进行如下操作：

   - 单击域名名称，可以查看域名的基本信息和健康检查结果。

   - 单击域名所属产品名称，可以查询域名所属产品。
   - 单击域名的关联资源，可以查看域名关联的负载均衡。
   - 单击 **修改 IP 地址** 可以修改域名对应的 IP。多个 IP 地址以英文逗号（,）分隔。

2.10. 日志查询

2.10.1. 操作日志

操作日志功能记录在云游 Local 执行过的操作，主要分为解决方案类和运维类。解决方案类包含导入解决方案、发布、测试等操作；运维类包含扩容、缩容、重启等操作。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏，选择 **日志查询 > 操作日志**。

   操作日志列表会展示目前产生的所有日志概览信息，单击右侧 **高级搜索** 可按操作人、操作内容或操作时段搜索指定日志。

3. 在操作日志列表中，单击目标日志 **请求明细** 后的 ⓘ 图标。

请求明细会显示日志的明细信息，如下图所示：

2.11. 权限设置

2.11.1. 角色定义

云游定义了运维工程师、环境管理员、云游观察者、交付工程师、AKE 运维工程师和 DBA 工程师几种角色，不同角色拥有不同权限。

前提条件

- 云游 Local 已升级 1.13.x 及以上版本。
- 云游 Local 成员管理接入了 IAM。

角色及对应权限说明

云游中的角色	对应 IAM 角色	交付升级模块	产品运维模块	资源管理模块	环境设置模块	操作日志模块	成员管理模块
环境管理员	Local-环境管理员	读写	读写	读写	读写	读写	读写 可以授予其他用户环境管理员、交付工程师、运维工程师（产品）、云游观察者角色
交付工程师	Local-交付工程师	读写	读写	读写	读写	读写	读写 可以授予其他用户交付工程师、云游观察者角色
运维工程师（产品）	Local-运维工程师	只读+修改自己的产品	只读+修改自己的产品	只读	只读	读写	读写 可以授予其他用户运维工程师（产品）、云游观察者角色
云游观察者	Local-云游观察者	只读	只读	只读	只读	只读	只读

> **注意**
>
> AKE 运维工程师和 DBA 工程师角色暂无作用，请不要申请。

2.11.2. 角色分配

云游 Local 的各角色中，高权限角色可以为其他用户分配等于或低于自身权限的云游角色，以方便其他用户登录和使用云游 Local。

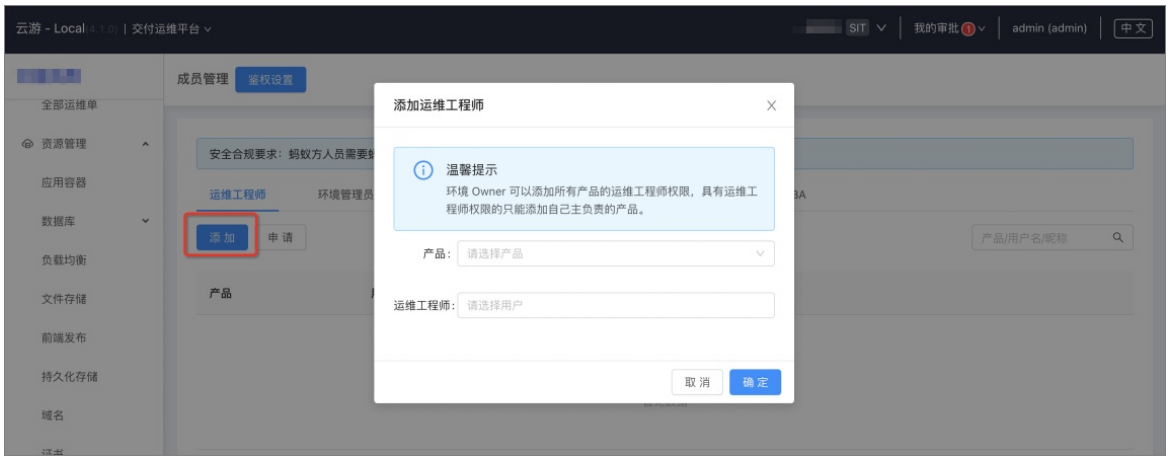
前提条件

- 云游 Local 已升级 1.13.x 及以上版本。
- 云游 Local 成员管理接入了 IAM。

操作步骤

1. 登录云游 Local 控制台。
2. 在左侧导航栏单击 **权限设置**。
3. 单击目标角色页签，然后单击 **添加**。

   以添加运维工程师角色为例，截图如下：



   - 产品：选择目标用户可以管理的产品。
   - 运维工程师：选择目标用户。

     目标用户为 IAM 当前租户下的用户。

> **说明**
>
> 云游各角色对应的权限说明，请参见 角色定义。

4. 单击 **确定**。

2.11.3. 申请和审批角色

除了通过管理员手动分配角色外，云游用户还可以通过提交角色申请，然后由环境管理员进行审批。

前提条件

- 云游 Local 已升级 1.13.x 及以上版本。
- 云游 Local 成员管理接入了 IAM。

注意事项

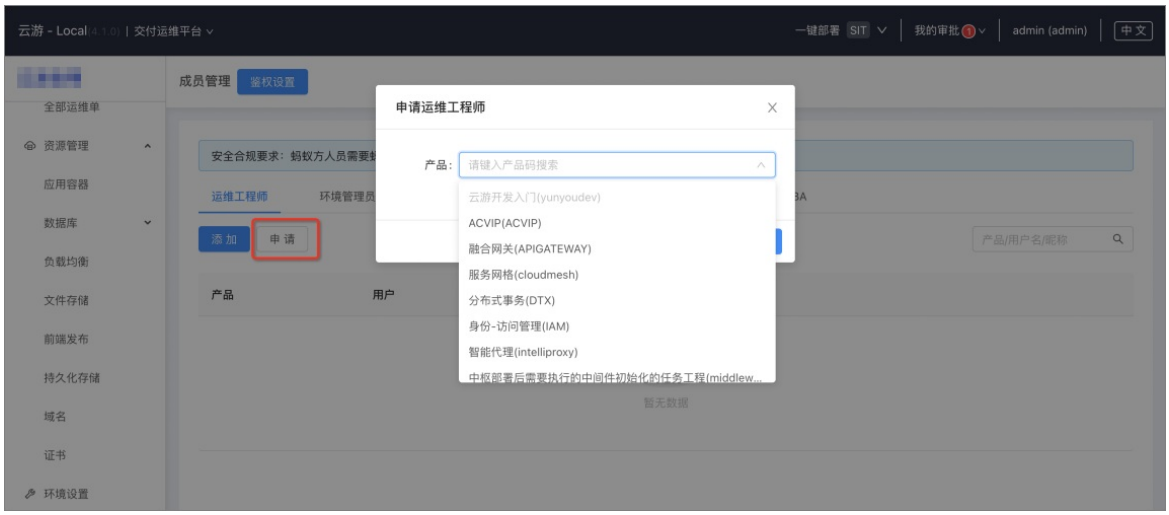
- 用户无法申请环境管理员权限，需由环境管理员在成员管理中添加。操作步骤请参见 角色分配。
- 用户可以申请环境中已经部署的某个产品的运维权限，且一次只能申请一个产品。
- 用户可以申请云游观察者和交付工程师的全局权限。

不同角色的介绍请参见 角色定义。

用户申请权限

1. 登录云游 Local 控制台。
2. 在左侧导航栏单击 **权限设置**。
3. 单击目标角色页签，然后单击 **申请**。

   以申请运维工程师权限为例，在 **申请运维工程师** 对话框选择目标产品。操作如下图所示：



4. 单击 **确定**。

   您可以选择 **我的审批** > **我发起的**，查看自己发起的申请。

管理员审批权限

环境管理员可以查看并审批当前环境所有用户发起的角色申请。

1. 选择上方菜单栏 **我的审批** > **待处理**。

2. 根据需要选择 **拒绝** 或 **通过**。

   您可以单击 **详情**，查看角色申请的详细信息。

2.12. 环境管理

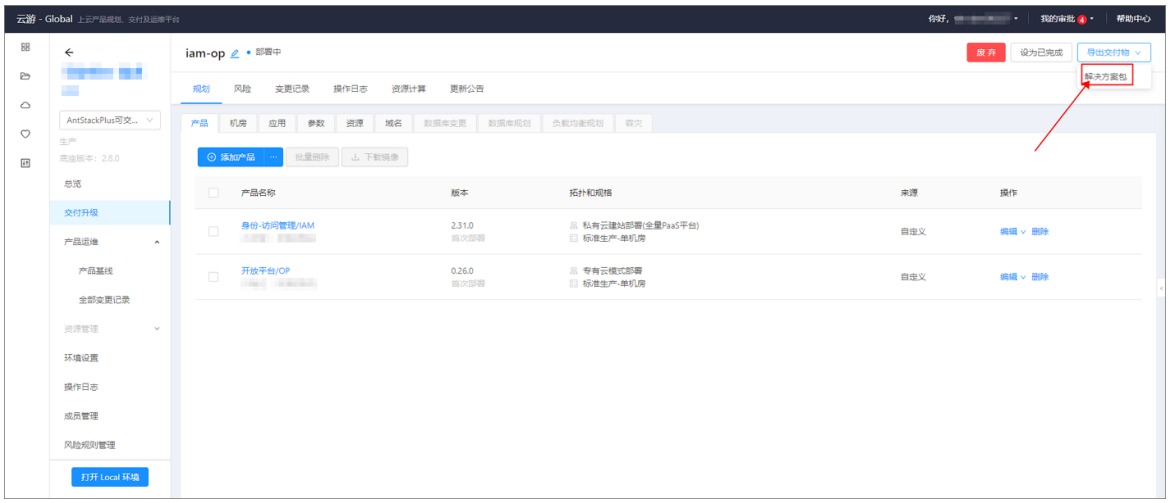
2.12.1. 新增环境

云游 Local 1.13.0 及以上版本支持环境管理，本文介绍如何在云游中添加环境。

2.12.1.1. 基于阿里云底座

操作步骤

1. 在云游 Global 新建解决方案，添加产品后，导出解决方案。

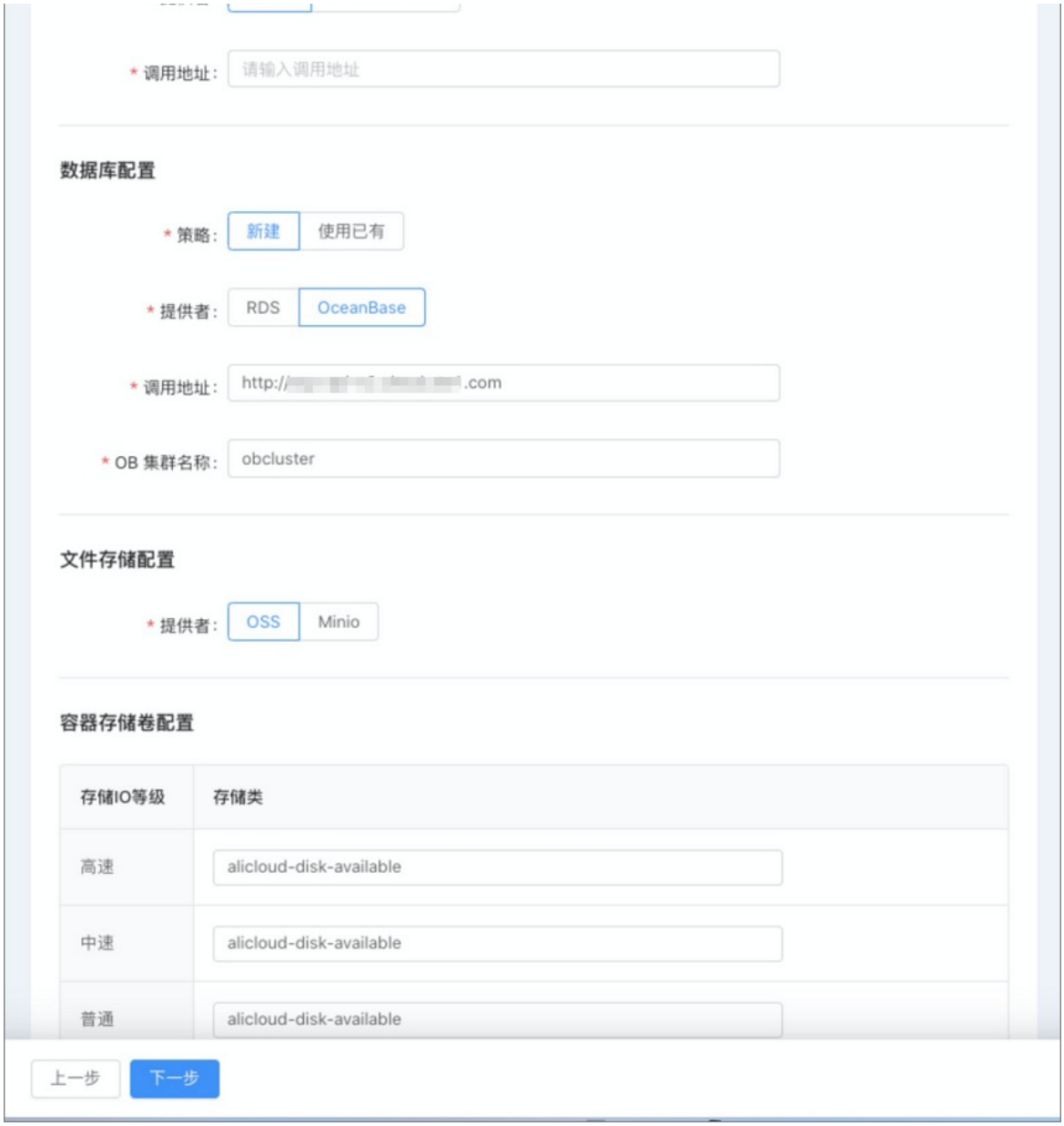


2. 登录云游 Local 控制台。

3. 在左侧导航栏单击 **环境管理**，然后单击 **新增环境**。
4. 在 **导入解决方案** 步骤上传步骤 1 导出的解决方案，然后单击 **下一步**。
5. 在 **环境基本信息** 步骤填写 **基本配置** 和 **底座配置**，然后单击 **下一步**。

参数		说明
基本配置	资源名前缀	填写环境的唯一标示，多机房下该字段不可重复。
	全局域名	当前环境产品对外提供访问的域名，双机房下使用同一套
	访问地址	云游 Local 的访问地址。
底座配置	选择底座	选择 **阿里云**。
	阿里云域名后缀	填写阿里云专有云的外网域名后缀，该域名后缀会用于拼凑出阿里云各产品的访问地址。
	AccessKey 和 AccessSecret	填写可访问阿里云产品的AccessKey 和 AccessSecret。 需使用高权限 AccessKey 和 AccessSecret。
	地域 和 可用区	需填写专有云下实际的 Region 和 Zone，会用作 SOFA 应用流量地域收敛及机房收敛的依据。
	VPC ID	专有云下 VPC ID。

6. 在 **环境资源** 配置步骤填写 Kubeconfig 及各资源配置后，单击 **下一步**。



参数		说明
基础配置	Kubernetes KubeConfig	填写 ACK 集群的 Kubeconfig。 在集群上执行 `kubectl config view --raw` 复制输出的内容。
负载均衡配置	vSwitchId	如果需要指定子网，可以填写 vSwitchId。
	支持特性	根据实际情况选择是否支持 anytunnel、公网、ENI 模式。其中专有云 3.12 版本需关闭 ENI 模式。

参数		说明
域名服务器配置	提供者	需选择 ADNS。
	调用地址	配置 ADNS 的地址。
数据库配置	策略	对于多机房场景，第一个机房一般选 **新建**，后续机房选择 **使用已有**，并复用第一个机房的连接信息。
	提供者	根据实际情况选择 RDS 或 OceanBase。
	调用地址	填写对应的调用地址。 **说明** 在专有云下，如果 OceanBase 使用 on 阿里云的方式部署，需填写 anytunnel 的地址，但该地址在飞天 3.16 版本后不再提供。地址获取方式：天基-服务注册变量中的 `${service:ocp-ocpv2:ocp_api_ram_v2_dns}` 。
	vSwitchId（可选）	提供者 RDS 时可以配置 vSwitchId。
	OB 集群名称	填写 OceanBase 的集群名称。 提供者为 OceanBase 时需填写。
文件存储配置	提供者	需选择 OSS 并填写正确的调用地址。
容器存储卷配置	-	专有云下，三种存储类型均可配置为 `alicloud-disk-available` 。

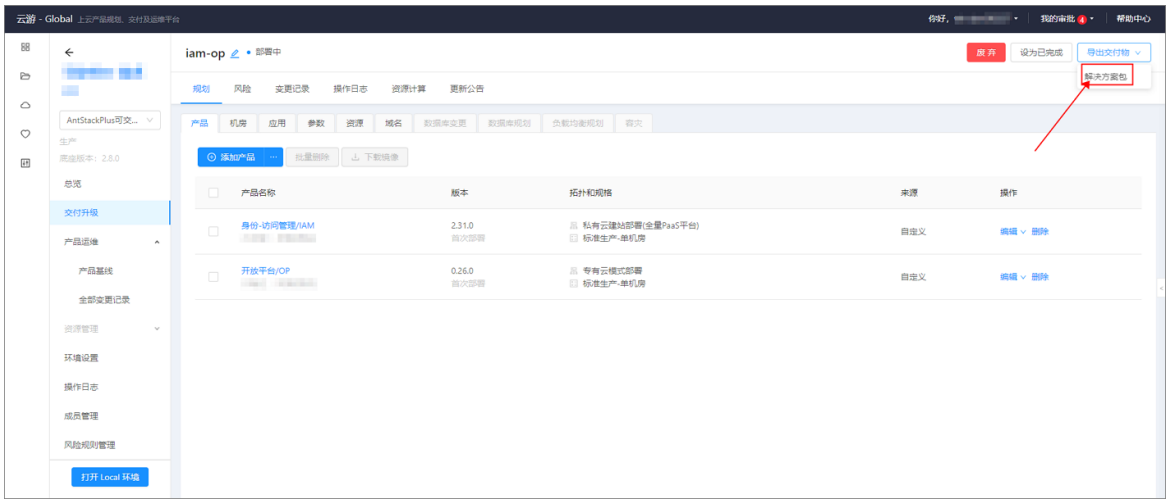
参数		说明
安全设置	**keystone 加密**	配置加密方式，取值如下： ○ **None**：表示不启用加密。 ○ **KMS**：表示启用阿里云专有云 KMS 加解密。 ○ **Local**：表示启用 keystone 本地加密。 默认使用 None。
Agent 配置	**调用地址**	填写 apyunqing Agent 的地址。如果没有安装 apyunqing Agent ，则填写为 `127.0.0.1:80` 。

7. 在 **环境初始化** 步骤确认信息无误后，单击 **完成配置**。

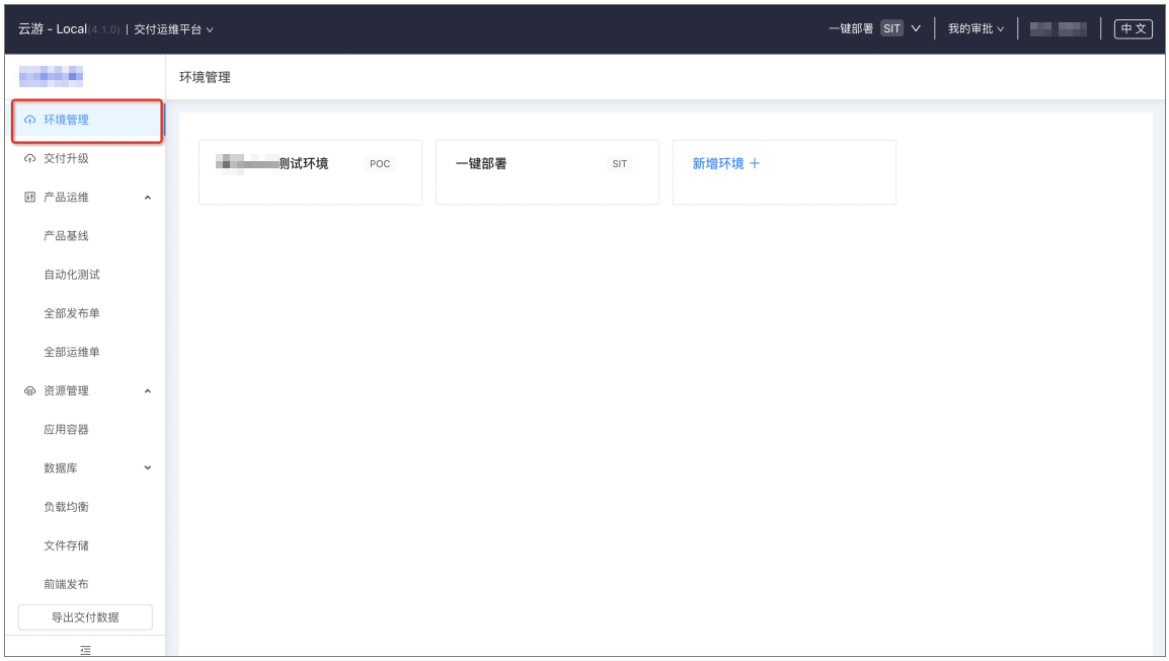
2.12.1.2. 基于物理机底座

操作步骤

1. 在云游 Global 新建解决方案，添加产品后，导出解决方案。



2. 登录云游 Local 控制台。
3. 在左侧导航栏单击 **环境管理**，然后单击 **新增环境**。



4. 在 **导入解决方案** 步骤上传步骤 1 导出的解决方案，然后单击 **下一步**。
5. 在 **环境基本信息** 步骤填写 **基本配置** 和 **底座配置**，然后单击 **下一步**。

云游 - 环境初始化设置
导入解决方案
2 环境基本信息
3 环境资源配置
4 环境初始化确认
基本信息
名称：
客户：蚂蚁金融云
站点：
是否带线：否
环境类型：POC
基本配置
* 资源名前缀：
所有创建的容器/数据库实例等的前缀
* 全局域名：
请输入全局域名，例：alipey.net
* 访问地址：
http://
t:81
底座配置
* 选择底座：
阿里云（公有云）
阿里云（专有云）
第三方
* 地域(Region)：
请输入地域，例：cn-hangzhou
* 可用区(ZONE)：
请输入可用区，例：cn-hangzhou-a
上一步
下一步

参数		说明
基本配置	资源名前缀	填写环境的唯一标示，多机房下该字段不可重复。 一般填写用户环境的简称。
	全局域名	当前环境产品对外提供访问的域名，双机房下使用同一套。 您可以通过 Antboot 查询： `antboot get config --normalize | grep dnsZone`
	访问地址	填写云游 Local 的访问地址。 建议使用默认值。
底座配置	选择底座	选择 **第三方**。
	地域 和 可用区	根据实际部署架构填写 Region 和 Zone，会用作 SOFA 应用流量地域收敛及机房收敛的依据。 同城双机房下，两个环境应地域相同，可用区不同。

6. 在 **环境资源** 配置步骤填写 Kubeconfig 及各资源配置后，单击 **下一步**。

云游 - 环境初始化设置

基础配置

* Kubernetes：KubeConfig 请输入目标集群的 KubeConfig

域名服务器配置

* 提供者：ADNS PRIVATEZONE

* 调用地址：请输入调用地址

数据库配置

* 策略：新建 使用已有

* 提供者：RDS OceanBase

* 调用地址：请输入调用地址

* OB 集群名称：请输入 OB 集群名称

文件存储配置

* 提供者：OSS Minio

* 调用地址：请输入调用地址

* AccessKey：请输入 AccessKey

* AccessSecret：请输入 AccessSecret

容器存储卷配置

存储IO等级	存储类
高速	
中速	
普通	

上一步 下一步

参数		说明
基础配置	Kubernetes KubeConfig	填写 ACK 集群的 Kubeconfig。 在集群上执行 `kubectl config view --raw` 复制输出的内容。
域名服务器配置	提供者	需选择 **ADNS**。
	调用地址	配置 ADNS 的地址。 如果配置了 VIP，填写 masterVips 的地址的其中一个 IP。您可以通过 `antboot get config --normalize | grep masterVips` 命令查询；若未配置 VIP，则填写规划了 adns 角色的一个节点的 IP。您可以通过 `antboot get config` 命令查看哪个节点有 adns 这个角色。
数据库配置	策略	对于多机房场景，第一个机房一般选 **新建**，后续机房选择 **使用已有**，并复用第一个机房的连接信息。
	提供者	选择 **OceanBase**。
	调用地址	填写为产品规划的 OceanBase 数据库的地址，没有可以不修改。
	OB 集群名称	填写 OceanBase 的集群名称。
文件存储配置	提供者	需选择 **Minio**。
	调用地址	如果没有安装 Minio，则填写 `http://127.0.0.1`，否则填写 Minio 的服务地址。
	AccessKey 和 AccessSecret	填写访问 Minio 的 AccessKey 和 AccessSecret。 您可以通过 `antboot get config --normalize | grep minioAccessKey` 和 `antboot get config --normalize | grep minioSecretKey` 命令查询。

参数		说明
容器存储卷配置	-	物理机下， 使用 open-local 存储，三种存储类型均可配置为 `open-local-lvm-default` 。
安全设置	**keystone 加密**	配置加密方式，取值如下： ○ **None**：表示不启用加密。 ○ **KMS**：表示启用阿里云专有云 KMS 加解密。 物理机环境不要选择该选项。 ○ **Local**：表示启用 keystone 本地加密。 默认使用 None。
Agent 配置	**调用地址**	填写 apyunqing Agent 的地址。如果没有安装 apyunqing Agent ，则填写为 `127.0.0.1:80` 。

7. 在 **环境初始化** 步骤确认信息无误后，单击 **完成设置**。

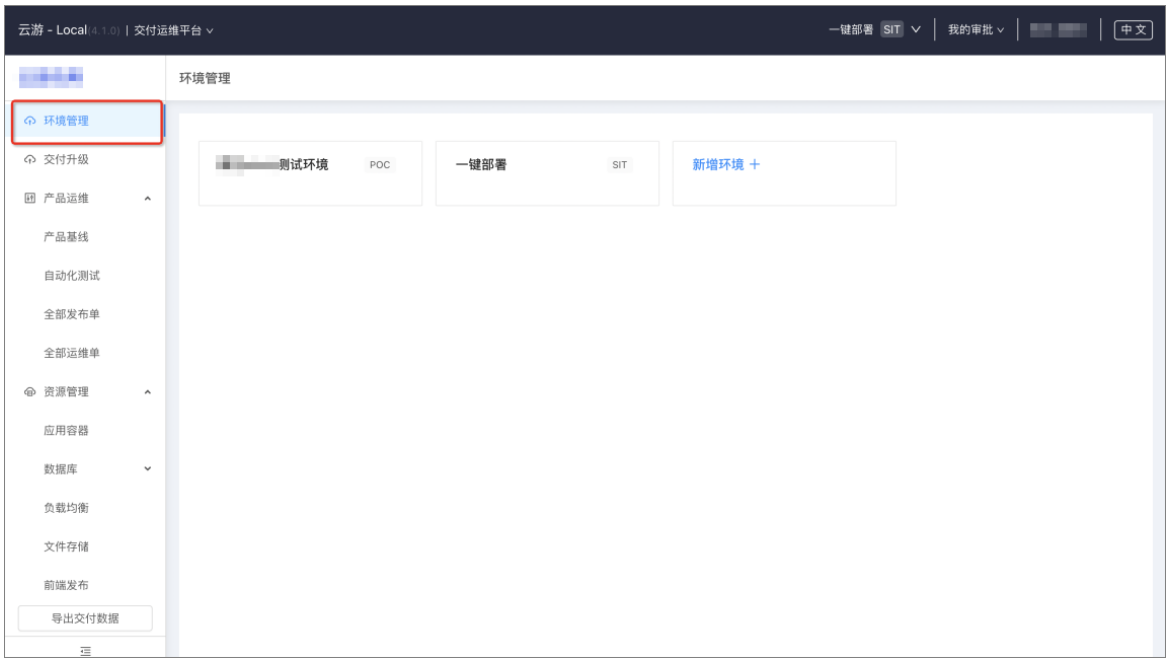
2.12.2. 查看环境信息

云游 Local 1.13.0 及以上版本支持环境管理功能，本文介绍如何查看环境信息。

查看环境信息

1. 登录云游 Local 控制台。

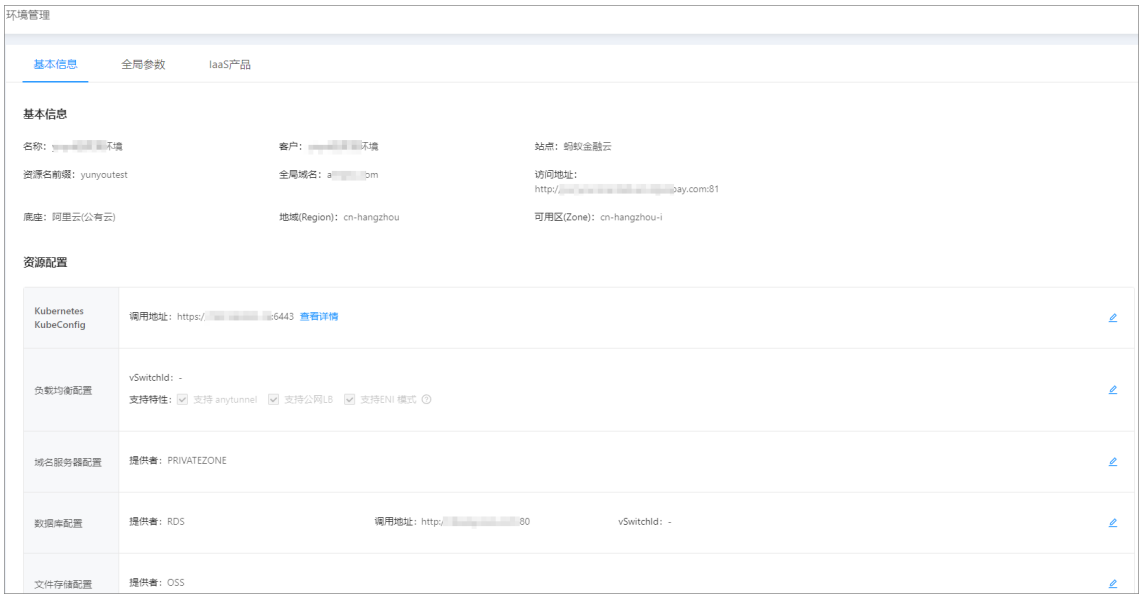
2. 在左侧导航栏单击 **环境管理**。
3. 在环境列表单击目标环境。



您可以查看环境的基本信息、全局参数、IaaS 产品信息。

- 基本信息

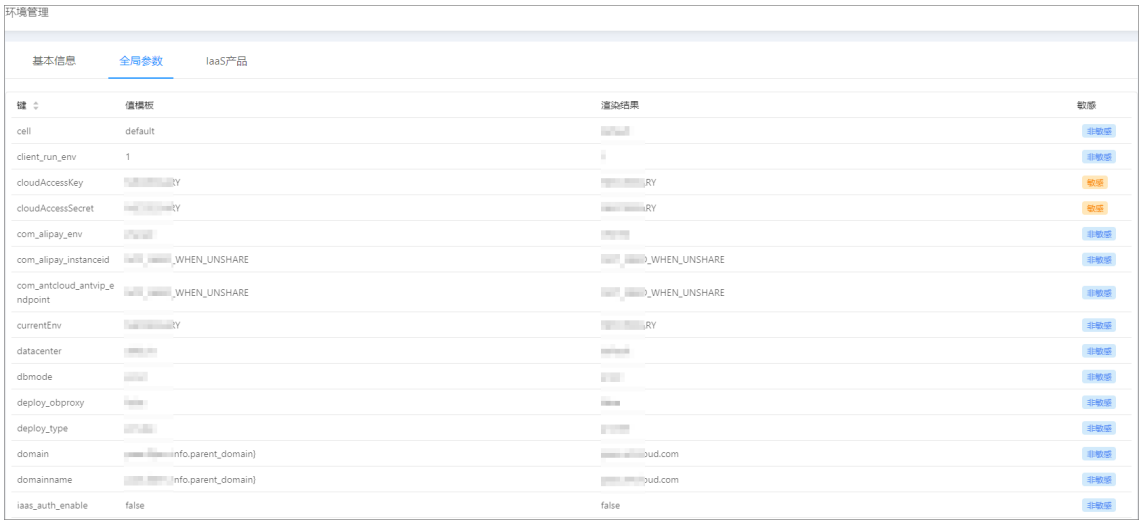
  在 **基本信息** 页签可以查看环境的基本信息、资源配置等参数。



  单击各资源右侧的铅笔图标还可以对资源配置进行编辑。

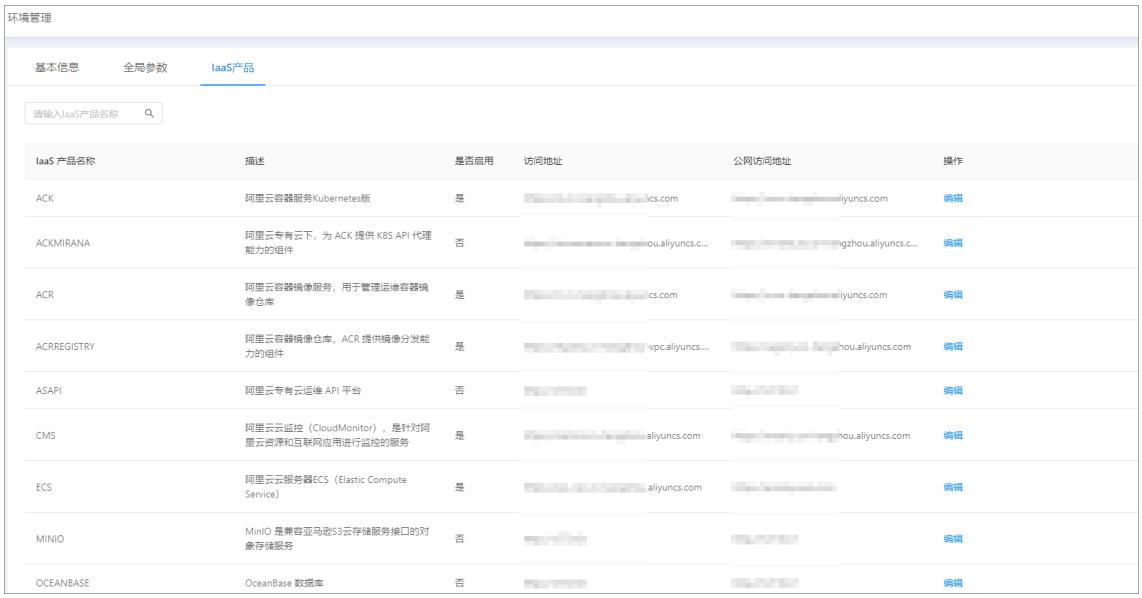
- 全局参数

在 **全局参数** 页签可以查看环境的参数信息。



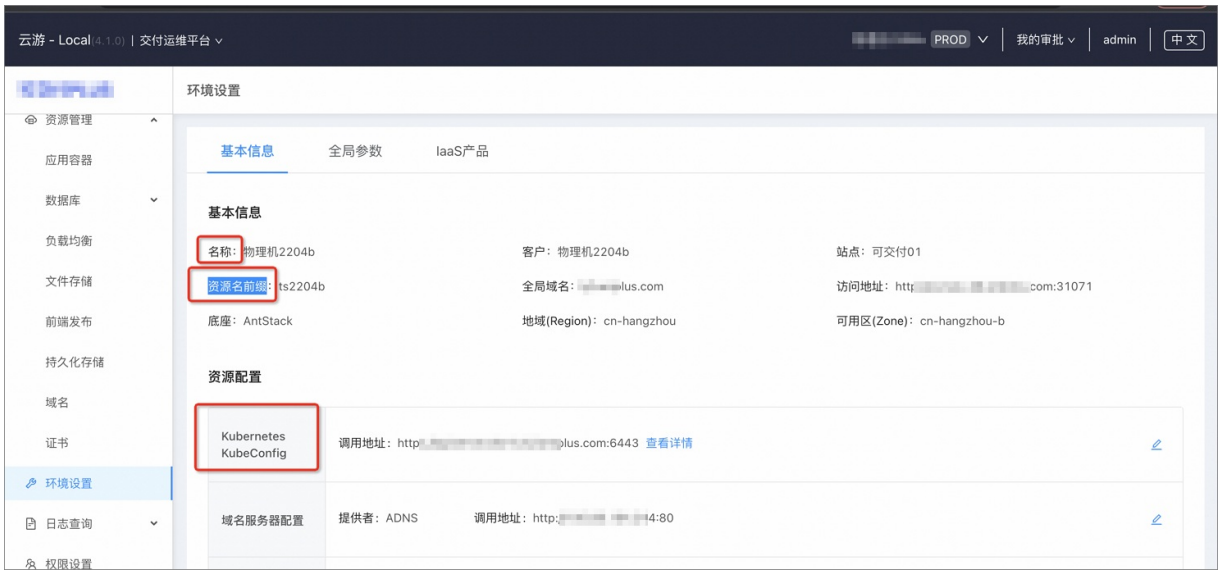
- IaaS 产品

  在 **IaaS 产品** 页签可以查看环境的 IaaS 产品信息。



2.12.3. 修改云游环境设置注意事项

凡是在 **环境设置** 中，修改过环境名称、资源名前缀、kubeconfig 等信息后，都需要重启云游的容器。



2.13. 导出交付数据

导出交付数据是把当前环境的产品基线信息和产品交付指标导出后回传云游 Global，作为日后制作升级方案的依据。

操作步骤

1. 登录云游 Local 控制台。
2. 将鼠标悬停在左侧导航栏的 **导出交付数据**。
3. 单击 **导出产品基线** 或 **导出交付指标**。
   - 单击 **导出产品基线**，云游控制台会将包含产品基线的 JSON 文件导出到浏览器默认的下载文件夹。
   - 单击 **导出交付指标**，云游控制台会将站点交付指标日志压缩文件导出到浏览器默认的下载文件夹。

2.14. 附录：基础术语

本文介绍云游涉及的基础术语。

标准应用

提供业务逻辑的应用。

部署规格

部署拓扑所需要的资源规格配置情况，您可以指定资源的数量以及每个资源实例的规格。

部署任务

云游通过计算当前基线（初始态）与解决方案（终态）之间的差异，生成一系列需要执行的子任务。完成所有子任务后，基线部署完成，达到终态。

部署拓扑

指一个产品的部署结构，包含哪些应用以及这些应用需要使用的配套基础资源，如服务器、负载均衡、数据库、文件存储。

测试应用

提供产品自动化测试镜像的应用。

产品版本

可以独立输出的版本，包含该版本的镜像以及部署配置。

基线

一个环境中，正在运行的、为上层应用服务的所有云产品及其版本、拓扑、规格、参数、资源等信息，称之为这个环境的基线。基线可以类比为一个专有云环境的水位，描述一个环境当前真实、稳定的状态。

集群

集群将多台机器的资源整合起来，统一调度和管理，是承载部署应用的载体。

节点

云游可以将物理机、虚拟机导入到集群，成为节点。节点内的资源会被统一管理和调度。

扩容

为应用增加容器。

容器

是一种轻量级的虚拟化技术，在云游中我们使用了 Docker 作为容器引擎。

容器变配

改变容器的规格，例如从 2C4G 变为 4C8G。

数据回流

指将云游的基线数据用 JSON 文件导出后回收，作为日后升级的基础参考。

缩容

为应用减少容器。

网络

定义了集群中应用容器互相访问的网络配置。

一次性任务应用

在产品部署过程中，完成一些产品提供方个性化、非标的、云游无法完成的逻辑，例如复杂的数据订正、数据库初始化等。

云产品

对外输出的最小完整单元，能给用户提供一组完整的功能。一个产品中包含多个应用以及这些应用需要用到的基础资源（服务器、数据库、负载均衡、文件存储等）。

3.身份访问 IAM

3.1. 什么是 IAM

IAM（Identity and Access Management）是基于蚂蚁集团多年发展，并结合业内其他厂商的方案，孵化出的一套通用、灵活的身份管理、认证及访问控制解决方案。

IAM 控制台主要包含以下功能：

- **总览**：快速查看成员、环境、已购产品信息。
- **账户信息**：查看及管理账户信息，包括企业信息、租户信息、租户级安全设置、个人信息、个人账户安全信息、登录信息等。
- **账号管理**：对成员、服务账号、权限等进行添加、修改、删除等操作。
- **我的权限**：用于查看、申请和撤销登录账号的权限。
- **审批管理**：空间管理员可查看所有申请，并进行审批。
- **审计中心**：空间管理员可统一查询和回溯用户操作行为。

3.2. 登录 IAM 控制台

您可以通过 IAM 控制台管理您的租户、权限以及审计信息。本文介绍如何登录 IAM 控制台。

前提条件

- 已获得 IAM 控制台的 IP 地址或服务域名。
- 已拥有蚂蚁账号，并获得 IAM 控制台的相应权限。

操作步骤

1. 打开浏览器。

   推荐使用 Google Chrome。

2. 在地址栏输入管理控制台的 IP 地址或服务域名。

3. 输入正确的用户名和密码后单击 **登录**。

4. 选择账号租户和所在空间，然后单击 **确定**。

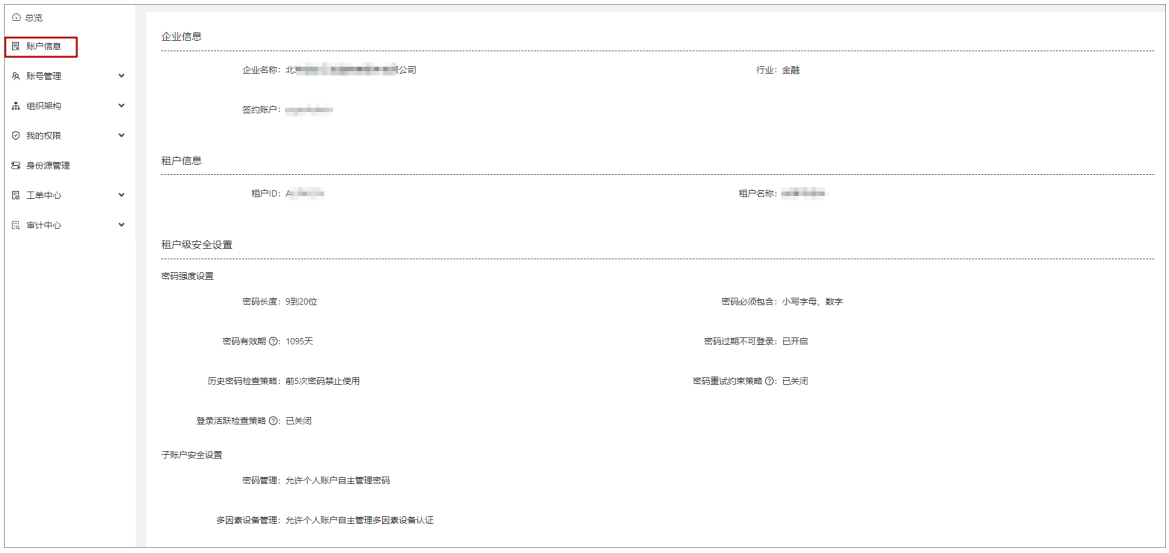
3.3. 查询账户信息

您可以在管理控制台查看并修改您的账户信息。

操作步骤

1. 登录管理控制台。
2. 在左侧导航栏单击 **账户信息**。

   您可以查看及管理如下信息：



   - **企业信息**：展示了当前所属的企业信息，在搭建金融科技平台时会默认初始化一个企业，不可修改。
   - **租户信息**：展示当前租户的相关信息，包括租户 ID 和租户名。
     - **租户 ID**：当前租户的唯一标识，企业申请开通租户时由系统自动生成，不可修改。

- **租户名称**：当前租户的名称。

同一企业下的不同租户间的成员是共享的，即一个成员可以是同一个企业下不同租户的成员。成员在进入不同的租户空间后，其账户信息中对应租户信息（租户 ID 和租户名称）也会随之改变。

当鼠标悬停在 **租户信息** 区域时，页面右侧会出现 图标，单击图标可修改租户名称。

> **注意**
>
> 普通操作员无权修改租户信息。

- **租户级安全设置**：展示租户的安全设置信息。
  - **密码强度设置**：可以设置该租户下操作员的密码安全策略，包括密码长度、密码组成内容、有效期、历史密码检查策略、密码过期是否可登录、密码重试限制、登录活跃检查策略。
  - **子账户安全设置**：可以设置子账号是否可以管理个人密码和多因素设备认证（MFA）。

    开启多因素设备认证后，每个操作员登录时都需要经过 MFA 认证。

鼠标悬停在 **租户级安全设置** 区域时，页面右侧会出现 图标，单击图标可修改租户安全设置。

> **说明**
>
> 普通操作员看不到 **租户级安全设置** 信息。

- **个人信息**：展示当前账号的相关个人信息，包括姓名、昵称、手机、座机、钉钉机器人 Token。
  - **姓名**：账号使用者的姓名。
  - **昵称**：账号使用者的昵称。
  - **手机**：当前账号关联的手机号。
  - **座机**（如果有）：当前账号关联的固定电话号码。
  - **钉钉机器人Token**（如果有）：在钉钉群中添加自定义钉钉机器人。配置中 webhook 地址的 access_token 参数值为该令牌 (Token)。

鼠标悬停在 **个人信息** 区域时，页面右侧会出现 图标，单击图标可修改个人信息。

- **个人账户安全信息**：查看账号的 AccessKey 信息，包括 ID 和 Secret。

在以程序的形式访问蚂蚁科技的服务或产品（例如调用蚂蚁金融科技 OpenAPI、使用 SDK 访问对象存储服务等）时，成员账号（管理员或其他成员）需要使用访问密钥（AccessKey）来标识自己的身份与权限。每个成员账号的 AccessKey 都不同，同一成员账号在不同租户下的 AccessKey 也不同。

  - **ID**：用于标识账号。
  - **Secret**：是用来验证账号的密钥。Secret 默认以星号（*）显示，单击图标可以查看 Secret 明文。

> **注意**
>
> Secret 一旦泄露，可能会被第三者获得此账号的全部权限，必须妥善保存。

- **登录信息**：展示当前账号的登录名、上次登录时间，以及是否启用多因素认证。
  - 单击 **修改密码** 可修改当前账号的登录密码。
  - 单击 **多因素认证** 右侧的 **开启** 链接后，您可以通过 **扫码获取** 或 **密钥获取** 的方式获取校验码，输入校验码后，单击 **确定** 可开启多因素认证。

    开启多因素认证后，您在登录金融科技控制台时需要进行二次验证以确保账户安全。

3.4. 账号管理

3.4.1. 账号管理

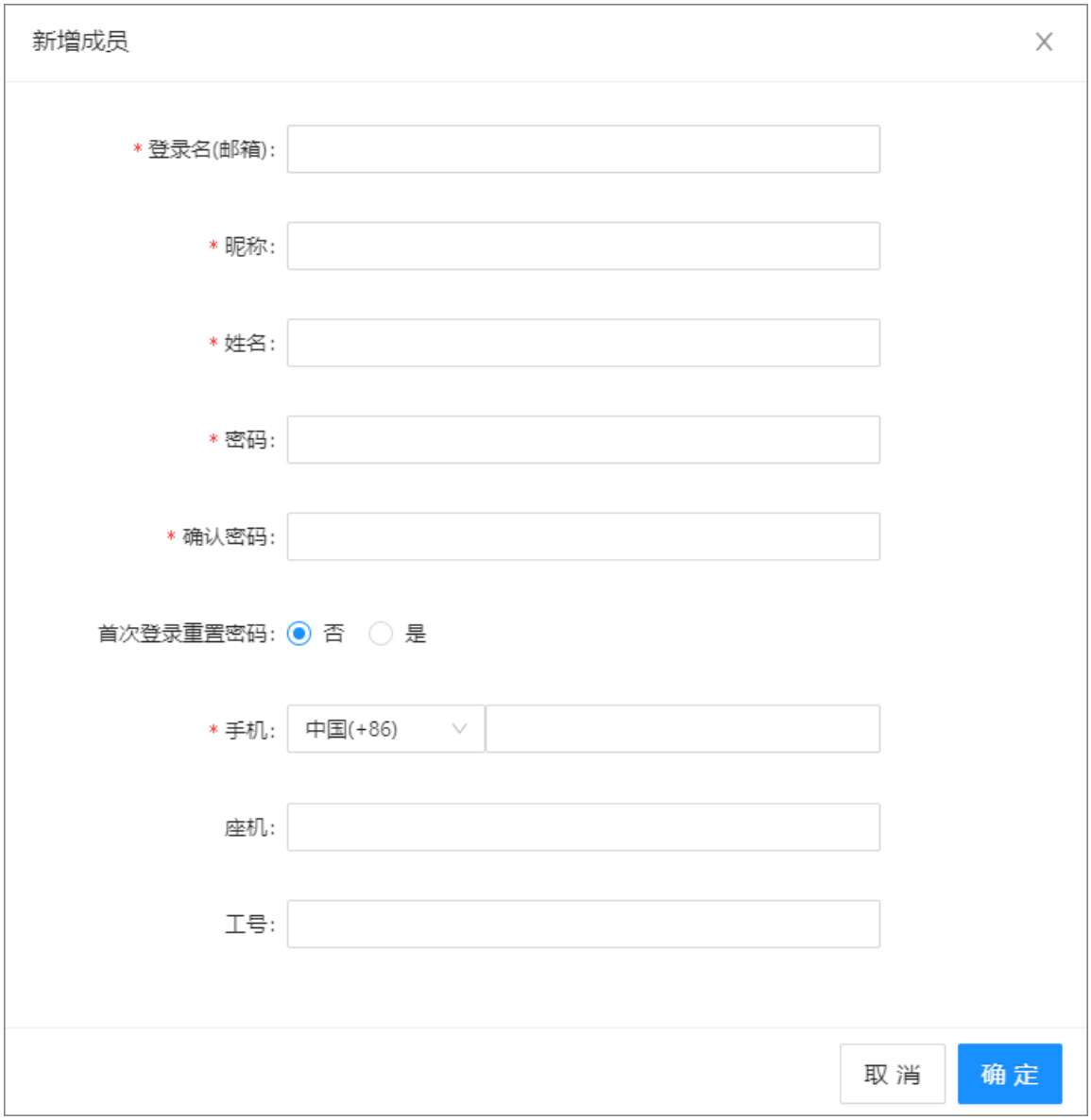
3.4.1.1. 管理租户成员

蚂蚁科技提供灵活的权限控制管理服务，拥有用户管理权限的成员（如空间管理员）可以在管理控制台中管理租户成员，并根据角色自定义各成员的操作权限。

新增成员

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **账号管理** > **账号管理**。
3. 单击 **租户成员** 页签，然后单击 **新增成员**。
4. 在 **新增成员** 对话框输入新成员的登录名（邮箱）、昵称、姓名、手机号、座机号和工号。

   其中座机号和工号为选填项。如果您选择 **首次登录重置密码** 为 **是**，则该成员首次登录时需要修改密码。



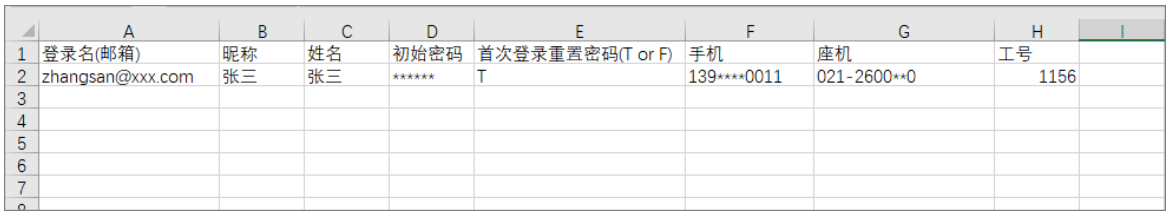
5. 单击 **确定**。

   新成员只有观察者权限，不能进行实际的操作。如果需要其他权限，可以向空间管理员申请。空间管理员可以在成员管理页面为新成员赋予相应的角色权限。

批量增加成员

1. 在 **租户成员** 页签，单击 **批量导入**。
2. 选择是否加入当前租户，并上传配置文件。

   您可以单击 **下载模板**，获取配置文件模板。文件模板示例如下：



	A	B	C	D	E	F	G	H	I
1	登录名(邮箱)	昵称	姓名	初始密码	首次登录重置密码(T or F)	手机	座机	工号	
2	zhangsan@xxx.com	张三	张三	******	T	139****0011	021-2600**0	1156	
3									
4									
5									
6									
7									

3. 校验成功后，单击 **下一步**。

4. 单击 **返回**。

> 注意
>
> 如果配置文件中包含已有登录名时，新上传的配置会覆盖已有配置。

为成员授权

新增成员仅拥有观察者权限，您需要使用空间管理员或拥有成员管理权限的用户可对租户成员进行授权，使该成员拥有角色对应的权限。操作步骤如下：

1. 在 **租户成员** 页签，单击目标成员右侧 **授权**。
2. 在 **添加授权** 页面，从角色列表中选择要赋予成员的角色，然后单击 **下一步**。

   您可以按照角色名或权限搜索角色。如果没有合适的角色可选，可先前往 **权限管理** 页面新增角色，具体操作参见 权限管理。
3. 设置权限范围。
   - **有效期**：可以指定权限生效的时间。可以指定为不限、1 天、2 天、3 天、7 天、14 天、30 天或自定义时间。
   - **条件**：通过筛选条件，进一步指定权限生效的资源或服务。
4. 单击 **确定**。

解除授权

若您不希望某个成员继续拥有指定权限时，可以解除该成员的授权。操作如下：

1. 在 **租户成员** 页签，单击目标成员名称或右侧 **详情**。
2. 在该成员详情页面的 **角色权限** 区域，单击目标角色右侧 **解除授权**。
3. 单击 **OK**。

冻结成员

若您希望让某个成员账号短时间失效，您可以选择冻结该账号。步骤如下：

在 **租户成员** 页签，选择目标成员右侧 **更多 > 冻结**。

解冻成员

若您希望恢复被冻结的账号，可以对账号进行解冻。步骤如下：

在 **租户成员** 页签，选择目标成员右侧 **更多 > 解冻**。

重置成员密码

若成员忘记密码，可以由空间管理员重置成员账号的密码。步骤如下：

1. 在 **租户成员** 页签，选择目标成员右侧 **更多 > 重置密码**。
2. 在 **修改密码** 对话框设置新的密码后单击 **提交**。

移出当前租户

若您希望某个成员登录时不允许选择当前租户与环境信息，可以将该成员移出当前租户。步骤如下：

> **说明**
>
> 您无法对空间管理员进行此操作，若您需要移出空间管理员账号，需要先解除成员授权。

1. 在 **租户成员** 页签，选择目标成员右侧 **更多** > **移出当前租户**。
2. 单击 **OK**。

删除成员

> **说明**
>
> 您无法对空间管理员进行此操作，若您需要删除空间管理员账号，需要先解除成员授权。

1. 在成员列表中，选择目标成员右侧的 **更多** > **删除**。
2. 单击 **OK**。

3.4.1.2. 管理租户成员组

您可以创建租户成员组，并为成员组内的租户添加统一的权限。本文介绍如何管理租户成员组。

新增租户成员组

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **账号管理** > **账号管理**。
3. 单击 **租户成员组** 页签，然后单击 **新增组**。
4. 在 **新增组** 会话框输入名称和描述，然后单击 **OK**。

   新增的组会出现在组列表中。

添加组成员

您可以将任意租户成员添加到成员组中，以统一管理。操作步骤如下：

1. 在 **租户成员组** 页签，单击目标成员组右侧的 **添加成员**。
2. 在 **添加成员** 对话框，选中需要添加的租户成员，然后单击 **确定**。

添加组权限

您可以使用空间管理员或拥有成员管理权限的用户为成员组添加权限，则成员组内的租户都拥有该权限。操作步骤如下：

1. 在 **租户成员组** 页签，单击目标成员组右侧的 **授权**。
2. 在 **添加授权** 页面，从角色列表中选择要赋予成员组的角色，然后单击 **下一步**。

   您可以按照角色名或权限搜索角色。如果没有合适的角色可选，可先前往 **权限管理** 页面新增角色，具体操作参见 权限管理。

3. 设置权限范围。
   - **有效期**：可以指定权限生效的时间。可以指定为不限、1 天、2 天、3 天、7 天、14 天、30 天或自定义时间。
   - **条件**：通过筛选条件，进一步指定权限生效的资源或服务。

4. 单击 **确定**。

修改租户成员组信息

您可以编辑租户成员组的信息，包括组名称和描述。操作步骤如下：

1. 在 **租户成员组** 页签，选择目标成员组右侧的 **更多 > 编辑**。
2. 在 **编辑组** 对话框输入新的组名和描述信息后，单击 **OK**。

解除租户成员组授权

若您不希望某个成员组继续拥有指定权限时，可以解除该成员组的授权。操作如下：

1. 在 **租户成员组** 页签，单击目标成员组名称或右侧的 **详情**。
2. 在该成员组详情页面的 **角色权限** 区域，单击目标角色右侧 **解除授权**。
3. 单击 **OK**。

移出组成员

您可以将任意租户成员移出某个租户成员组，以解除该租户拥有的组权限。步骤如下：

1. 在 **租户成员组** 页签，单击目标成员组名称或右侧的 **详情**。
2. 在该成员组详情页面的 **现有成员** 区域，单击目标成员右侧的 **移出组**。
3. 单击 **OK**。

   被移出的组成员依然在当前租户内，只是不再出现在当前组中。

解散组

若您不再需要某个成员组时，可以解散该组。操作步骤如下：

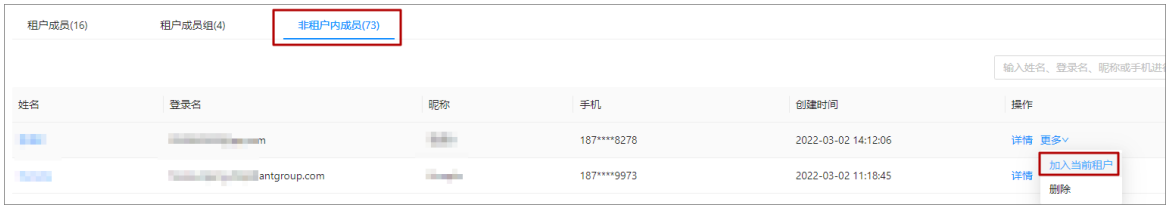
1. 在 **租户成员组** 页签，单击目标成员组名称或右侧的 **详情**。
2. 在该成员组详情页面，单击右上角的 **解散组**。
3. 单击 **OK**。

3.4.1.3. 管理非租户内成员

当租户成员进行移出租户成员操作后，都会出现在非租户内成员列表中。本文介绍如何管理非租户内成员。

加入当前租户

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **账号管理 > 账号管理**。
3. 单击 **非租户内成员** 页签，然后选择目标成员右侧 **更多 > 加入当前租户**。



加入当前租户后，该成员可在登录时选择当前租户与环境信息，并拥有观察者权限。

删除非租户内成员

1. 在 **非租户内成员** 页签，选择目标成员右侧 **更多** > **删除**。
2. 单击 **OK**。

3.4.2. 管理服务账号

服务账号是一类特殊的成员账号，它的使用者通常是一个程序或某一项服务。同成员账号一样，服务账号可以被授权、可以被分配角色、可以拥有 AccessKey，不同的是它不会被任何一个自然人持有，因此不能用于登录，也没有邮箱、手机号等信息。本文介绍如何管理服务账号。

服务账号通常用于以下场景：

- 程序或服务在调用蚂蚁科技平台或蚂蚁科技产品的 OpenAPI 时，需要在程序中配置一组有权限的访问密钥（AccessKey）。
- 蚂蚁科技平台提供功能扩展 SPI（Service Provider Interface），产品开发者研发的产品程序可通过这些 SPI 将功能接入到平台中，当平台调用产品的 SPI 时，需要使用一组与产品开发者约定好的 AccessKey。

> **注意**
>
> 以上场景中不推荐使用任何成员账号的 AccessKey，因为成员账号通常代表一个自然人，其岗位、职责可能发生变化，权限也不固定，不应将人的身份配置给程序或服务。

新增服务账号

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **账号管理** > **服务账号**。
3. 单击 **新增服务账号**，并在弹出的对话框中输入服务账号的名称和描述。
4. 单击 **OK**。

   新增的服务账号会出现在服务账号列表中，系统会自动为服务账号分配唯一 ID。

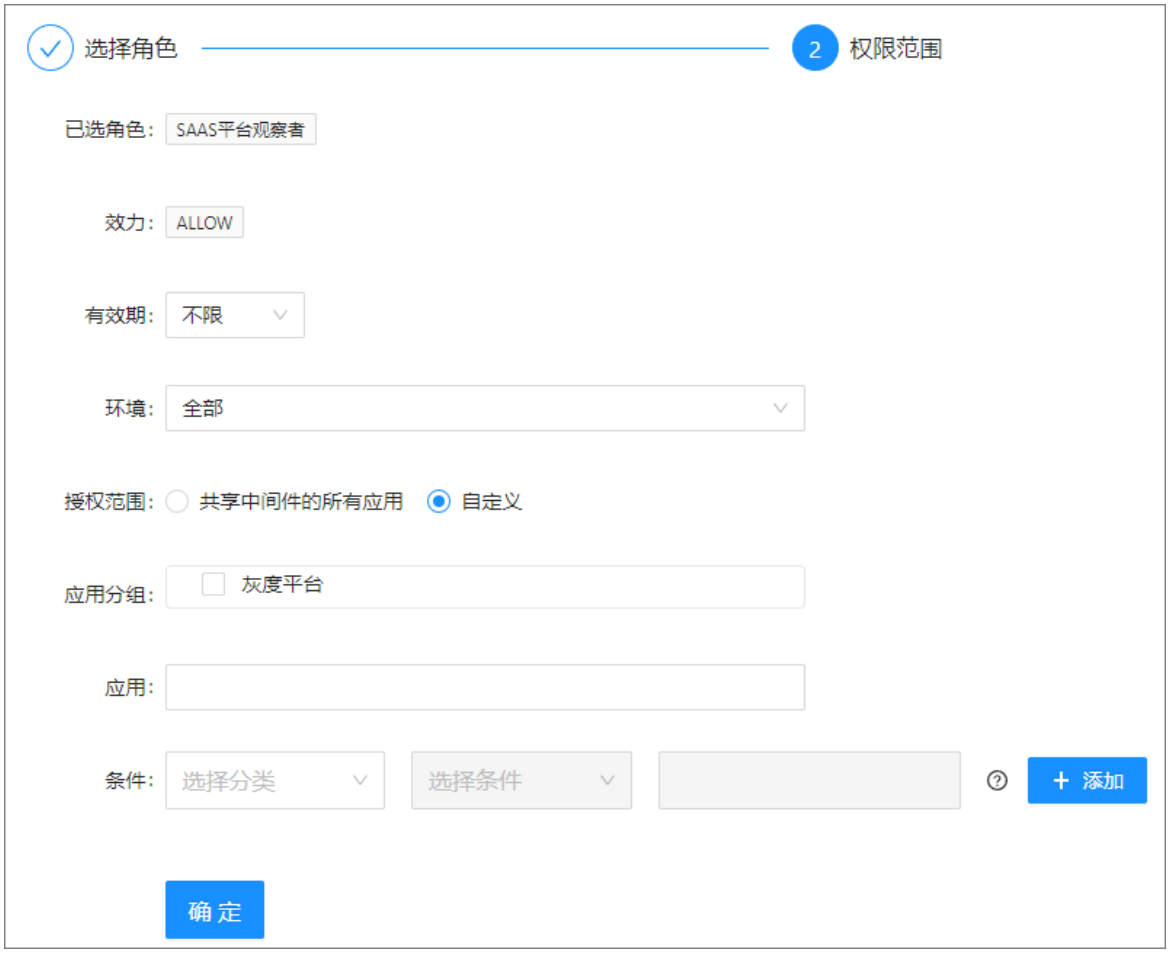
为服务账号添加权限

新增的服务账号没有任何权限，您需要使用空间管理员账号为服务账号添加指定权限。操作步骤如下：

1. 在 **服务账号** 页面，单击目标服务账号右侧 **授权**。
2. 在 **添加授权** 页面，从角色列表中选择要赋予服务账号的角色，然后单击 **下一步**。

您可以按照角色名或权限搜索角色。如果没有合适的角色可选，可先前往 **权限管理** 页面新增角色，具体操作参见 权限管理。

3. 设置权限范围。



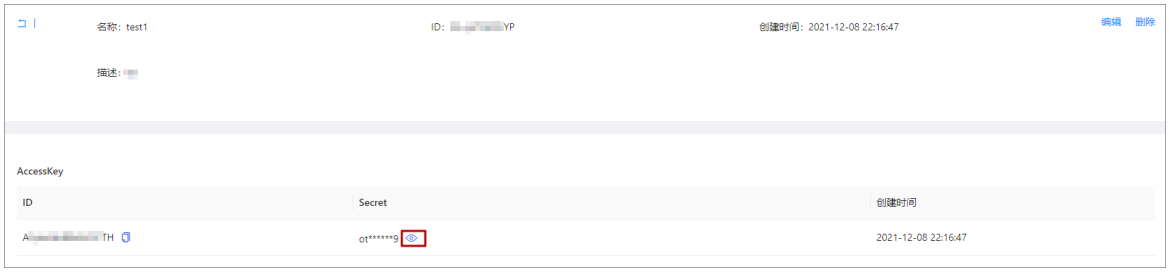
- **有效期**：可以指定权限生效的时间。可以指定为不限、1 天、2 天、3 天、7 天、14 天、30 天或自定义时间。
- **条件**：通过筛选条件，进一步指定权限生效的资源或服务。

4. 单击 **确定**。

获取服务账号的 AccessKey

使用服务账号时，您需要获取服务账号的 AccessKey。操作步骤如下：

1. 在 **服务账号** 页面，单击目标服务账号名称或右侧 **详情**。
2. 在服务账号详情页的 **AccessKey** 区域查看 AccessKey 信息。



- **ID**：该服务账号的 AccessKey ID
- **Secret**：该服务账号的 AccessKey Secret。单击 图标可查看 Secret 明文。

编辑服务账号

您可以修改服务账号的名称和描述信息，操作步骤如下：

1. 在 **服务账号** 页面，选择目标服务账号右侧的 **更多 > 编辑**。
2. 在 **编辑服务账号** 对话框修改服务账号名称和描述，然后单击 **OK**。

删除服务账号

对于不再需要的服务账号，您可以选择删除。操作步骤如下：

> **警告**
>
> 删除前请确认该账号未在任何服务或应用中使用，否则可能导致应用出现异常。

1. 在 **服务账号** 页面，选择目标服务账号右侧的 **更多 > 删除**。
2. 单击 **OK**。

3.4.3. 权限管理

权限管理主要体现在对角色的管理，角色是若干权限的集合，是权限分配的载体。本文介绍如何管理角色和查询权限。

新增角色

如果系统默认生成的角色不能满足您的需求，您可根据需要创建自定义角色。操作步骤如下：

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **账号管理 > 权限管理**。
3. 单击 **角色** 页签，然后单击 **新增角色**。
4. 在基本设置中输入角色名称和描述，然后单击 **下一步**。
5. 在选择权限步骤中选择角色需要的权限。

   您可通过以下任一方式选择角色需要的权限：

- 在权限列表中，逐个选中需要的权限。
- 在 **根据已有角色选取** 下拉列表选择一个或多个已有的角色，并以该角色为基础，通过增减权限来创建自定义角色。
- 在页面右上方的权限搜索栏中，输入要查询的权限，搜索并选择权限。

权限选择完成后，您还可以单击页面右下方的 **查看已选权限**，浏览已选的权限。

6. 确认无误后，单击 **确定**。

修改角色权限

您可以根据需要对创建的自定义角色权限进行增删操作。操作步骤如下：

1. 在 **角色** 页签单击目标角色名称或右侧 **详情**。
2. 在角色详情页面的 **拥有权限** 区域添加或删除角色权限。
   - 添加权限
     a. 单击 **添加权限**。
     b. 选择需要添加的权限，然后单击 **确定**。
   - 删除权限

     在权限列表中，单击目标权限右侧的 **删除权限**。

编辑角色

您可以根据需要修改角色名称和描述信息。操作步骤如下：

1. 在 **角色** 页签选择目标角色右侧 **更多 > 编辑**。
2. 在 **编辑角色** 对话框修改角色名称或描述，然后单击 OK。

查询角色权限

在 **角色** 页签单击目标角色名称或右侧 **详情**，可查看角色已拥有权限及权限的使用情况。

- 在角色详情页面的 **拥有权限** 区域，可查看当前角色拥有的权限。
- 在角色详情页面的 **使用情况** 区域，查看角色的权限使用情况：
  - 单击 **成员** 页签，可查看所有拥有该角色的租户成员。
  - 单击 **成员组** 页签，可查看所有拥有该角色的租户成员组。
  - 单击 **服务账号** 页签，可查看所有拥有该角色的服务账号。

解除角色授权

当您不再希望某个租户成员、成员组或服务账号拥有该角色的权限时，可以解除授权。操作步骤如下：

1. 在 **角色** 页签单击目标角色名称或右侧 **详情**。
2. 在角色详情页面的 **使用情况** 区域，根据需要单击 **成员**、**成员组** 或 **服务账号** 页签。
3. 在目标 **成员**、**成员组** 或 **服务账号** 右侧，单击 **解除授权**。
4. 单击 OK。

删除角色

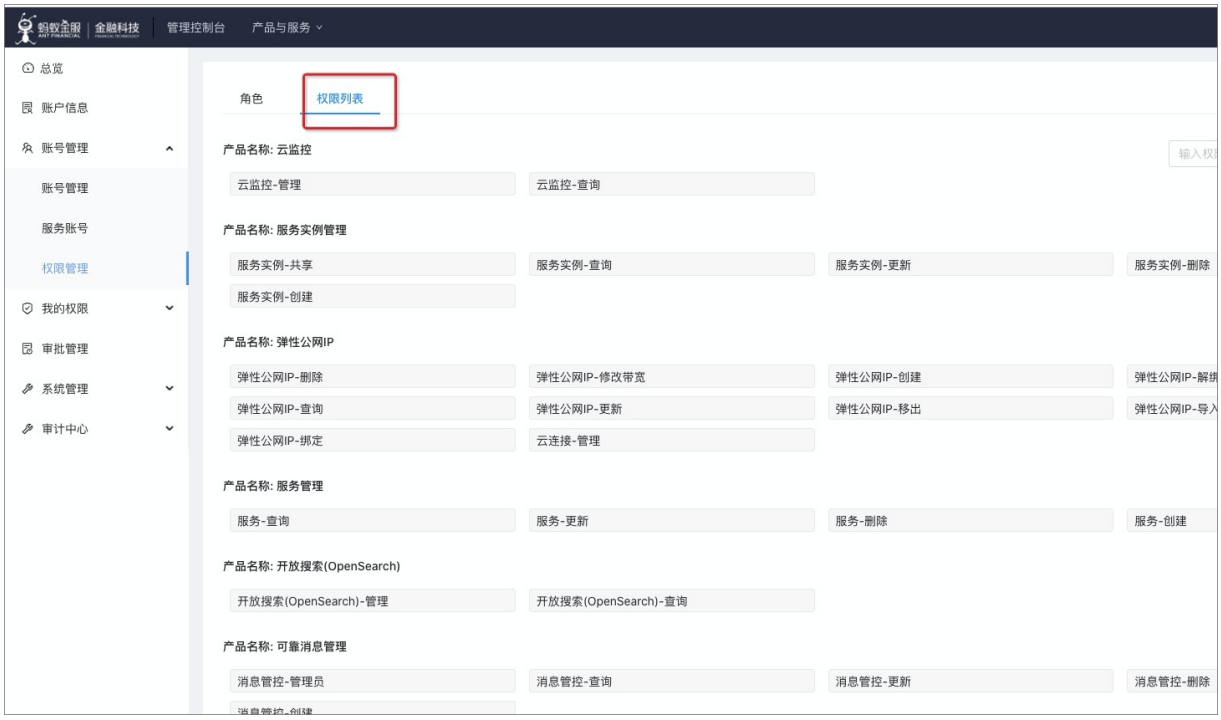
当您不再需要某个角色时，可以删除该角色。操作步骤如下：

> **注意**
>
> 删除角色前，您必须解除该角色的所有授权，否则无法删除。

1. 在 **角色** 页签选择目标角色右侧 **更多 > 删除**。
2. 单击 **OK**。

查看权限列表

您可以在 **权限列表** 页签中查询系统已有的权限列表。



3.5. 组织架构

3.5.1. 部门管理

您可以通过部门管理，管理您的组织架构。

创建部门

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **组织架构 > 部门管理**。
3. 在 **部门树** 区域，单击 **创建部门**，然后配置以下参数：

参数	说明
唯一代码	填写部门的唯一代码，只能包含字母和数字。

参数	说明
名称	填写部门的名称。
父部门	填写本部门的上级部门。
描述（可选）	为部门添加描述信息。

4. 单击 **OK**。

导入部门

您也可以通过导入部门功能，批量创建部门。

1. 在 **部门管理** 页面的 **部门树** 区域，单击 **导入部门**。
2. 上传配置文件。

   您可以单击 **下载模板**，获取配置文件模板。
3. 校验成功后，单击 **下一步**。
4. 单击 **返回**。

添加成员

1. 在 **部门管理** 页面，单击目标部门名称。
2. 单击 **添加成员**，然后选中当前账号下创建的成员。

   每个成员只能被添加到一个部门。
3. 单击 **确定**。

导入部门成员

您也可以通过导入部门成员功能，批量导入部门成员。

1. 在 **部门管理** 页面的 **部门树** 区域，单击 **导入部门成员**。
2. 上传配置文件。

   您可以单击 **下载模板**，获取配置文件模板。
3. 校验成功后，单击 **下一步**。
4. 单击 **返回**。

> **注意**
>
> 如果导入的成员在其他部门中，该成员会被移到配置文件中配置的部门。

移除成员

1. 在 **部门管理** 页面，单击目标部门名称。
2. 在 **成员列表** 区域，单击目标成员右侧的 **移除**。

3. 单击 **确定**。

编辑部门

1. 在 **部门管理** 页面，单击目标部门名称。
2. 在 **部门详情** 区域，单击 **编辑**。

   您可以部门名称、父部门、描述信息。
3. 单击 **OK**。

删除部门

1. 在 **部门管理** 页面，单击目标部门名称。
2. 在 **部门详情** 区域，单击 **删除**。
3. 单击 **确定**。

3.6. 管理我的权限

您可以在我的权限列表中查看自身账号已有的权限，若账号权限不足，您可以提交新增角色申请。本文介绍如何管理我的权限。

申请新角色

当您的账号权限无法满足工作所需时，可以申请新的角色。操作步骤如下：

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **我的权限** > **我的角色**。
3. 单击 **申请新角色**。
4. 在 **角色申请** 页面单击 **添加角色**，并配置以下参数：

参数	说明
选择角色	选择您需要申请的角色。
角色权限详情	展示您选择角色的所有权限。
添加条件	单击可添加角色的使用条件。 您可以配置多个条件。
到期时间	设置角色的到期时间，可选择指定时间或永久生效。
申请理由	填写申请该角色的理由。

多次单击 **添加角色** 可同时申请多个角色。

> **注意**
>
> 请基于工作场景按权限最小化原则申请角色，申请行为将会纳入安全审计范围。

5. 单击 **提交申请**。

   提交完成后会跳转到 **我的工单** 页面，您可以单击 **重新申请** 编辑此次申请；也可以单击 **撤销** 取消此次申请。

撤销已有权限

当您工作不再需要某个角色的权限时，建议您及时撤销该权限。操作步骤如下：

1. 在 **我的角色** 页面单击目标角色右侧 **撤销权限**。
2. 单击 **确定**。

3.7. 工单中心

工单中心用于查看与我相关的工单和我待办的工单。

查看我的工单

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **工单中心** > **我的工单**。
3. 您可以在 **我的工单** 页面查看所有与我相关的工单。
4. 单击目标工单名称。

   您可以查看工单的基本信息以及工单审批的流程。

审批工单

1. 在 IAM 控制台的左侧导航栏选择 **工单中心** > **我的待办**。
2. 选择目标单号右侧的 **同意** 或 **拒绝**，进行工单审批。

单击申请单号可以查看工单的审批流程。

3.8. 接入审批平台

流程编排 StepFlow 是一款服务编排产品，编排是指通过可视化流程图的方式将这些服务组合起来，绘制好的流程图，可以像传统的后端服务一样，通过 SOFA RPC、Http、事件等方式被上游系统调用。

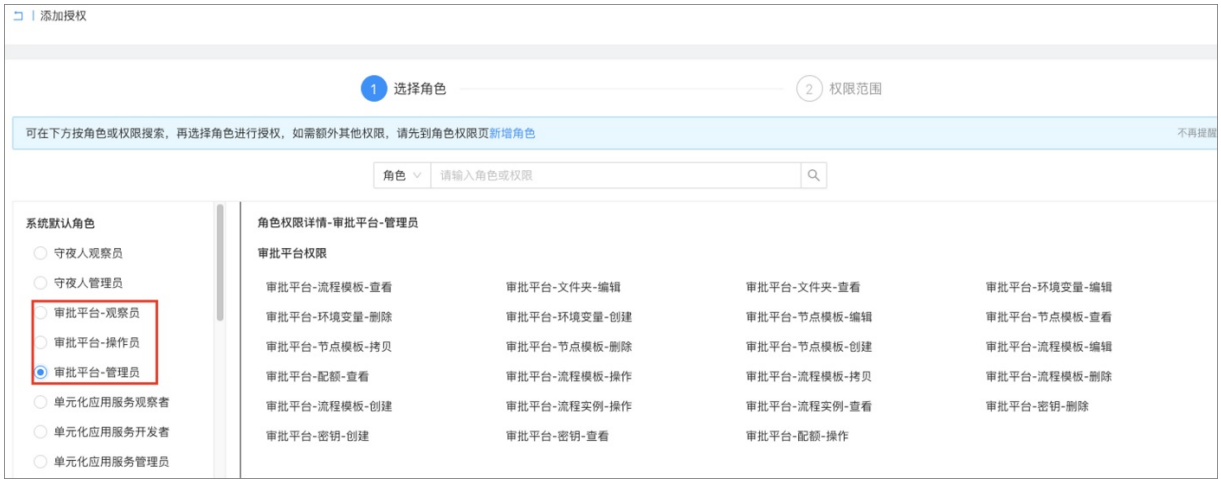
前提条件

已部署以下产品：

产品	产品版本	拓扑	规格	功能
OPS_COMPOSE	2.0.0	按需选择	按需选择	审批流管理
IAM	2.36.0	按需选择	按需选择	工单管理

步骤 1：配置流程编排权限

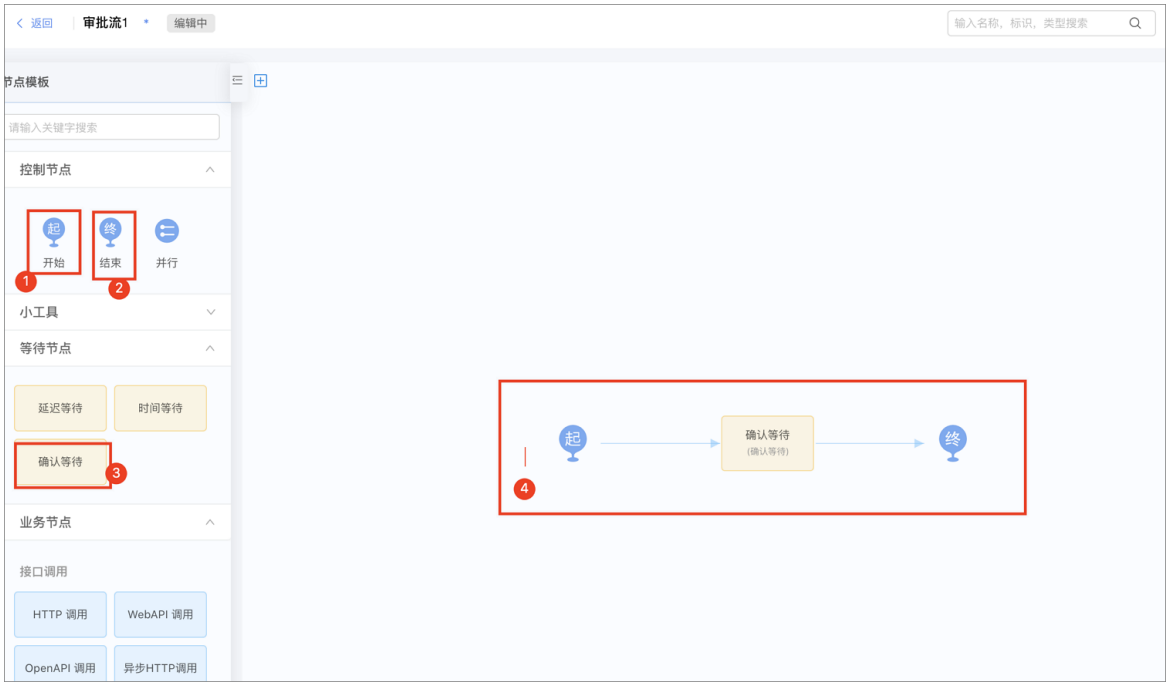
在 IAM 控制台授予目标用户 StepFlow 的相关权限，授权操作请参见 为成员授权。目前支持如下权限：



步骤 2：创建审批流模板

本文示例以最简单的审批流为例，您可以根据需要创建更复杂的审批流。

1. 登录 StepFlow 控制台。
2. 在左侧导航栏，选择 **模板管理 > 流程模板**，然后单击 **创建**。
3. 选择 **从头开始构建**，然后填写模板名称。
4. 单击 **确定** 进入该模板的 IDE 界面。
5. 在左侧将 **开始**、**确认等待**、**结束** 拖动到右侧，并进行连接。



6. 单击 **确认等待** 节点，然后单击 **编辑**。
7. 单击 **节点参数** 页签，然后配置审批人。

   目前支持三种审批用户的配置：

   - 指定用户审批（支持多选），指定用户又区分为三类：
     - 指定用户名称或者邮箱等信息进行查询确认。

- 流程执行人：代表通过模板创建流程实例的当事人。
- 流程审批人：代表审批流程实例执行的人。

- 通过汇报线关系指定审批用户，分为两类：
  - 指定某位用户、流程执行人、流程审批人 的 1、2、3 级主管全体。
  - 通过主管搜索指定某一个主管（最终效果等同于指定用户审批）。

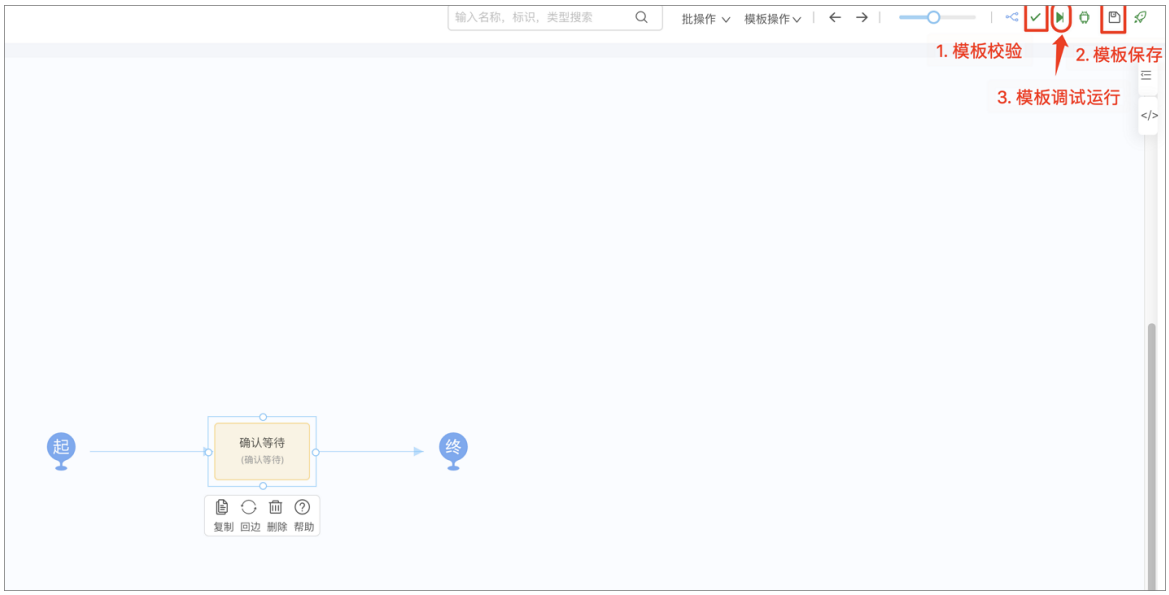
- 通过成员组指定审批用户：

8. 单击 **前置任务** 页签，然后配置通知方式和内容。

节点参数
前置任务
后置任务
添加确认等待操作
添加自定义动作
发送通知
方式
钉钉
邮件
短信
接收者
仅限指定人员
指定汇报线或成员组
汇报线
成员组
1
的所有1级主管
内容
请前往IAM审批任务，流程 ID: #{ac.processInstance.id}
使用JS的运行结果作为内容
取 消
确定

9. 单击 **确定**。

10. 在实例 IDE 页面进行模板校验、调试运行以及保存。



11. 在 **流程模板** 页面选择目标模板右侧的 **更多** > **发布**。

12. 在 **路由配置** 页面，单击 **发布**，然后单击 **确认**。

步骤 3：执行审批流实例

1. 在 **流程模板** 页面单击目标模板右侧的 **执行**。
2. 单击 **开始执行**。

步骤 4：审批工单

流程实例开始执行之后，就可以在 IAM 系统上看到工单和待办事项，详情请参见 工单中心。

3.9. 审计中心

3.9.1. 审计大盘

蚂蚁金融科技提供针对用户操作记录的查询、订阅和投递服务，可用于安全分析、资源变更跟踪及合规性审计等场景。本文介绍审计大盘。

在管理控制台的左侧导航栏选择 **审计中心** > **审计大盘**，可查看审计大盘统计的信息。

7 日内操作总数

统计 IAM 控制台 7 天内产生的所有操作的总次数。

7 日内操作统计

统计 IAM 控制台 7 天内产生的不同类型操作的总次数，例如登录控制台、添加租户成员、添加租户成员组、解散租户成员组等。

7 日内操作用户统计

分别统计不同用户 7 天内产生的操作总次数。

3.9.2. 操作审计

蚂蚁集团提供了强大的操作审计能力，拥有用户管理权限的成员（如空间管理员）可以查询和回溯用户操作行为。支持从操作时段、用户名、操作类型、源 IP 地址或数据类型等维度查询历史操作事件。

操作步骤

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **审计中心 > 操作审计**。
3. 在 **操作审计** 页面查看所有操作。

   您也可以设置查询条件，单击 **搜索** 查询操作行为数据。

条件	说明
过滤器	根据指定过滤类型过滤操作行为数据。 目前支持按 **访问密钥**、**资源类型**、**traceId** 进行过滤。
用户名	根据用户名过滤操作行为数据。
操作	根据指定产品过滤操作行为数据。 默认为 **所有产品-所有操作**。
源 IP 地址	根据执行操作的用户 IP 地址过滤操作行为数据。
时间	根据指定时间范围过滤操作行为数据，指定的时间段前后间隔不能超过一个月。例如初始时间选择 2022 年 1 月 1 日，则结束日期最多能选择到 2022 年 1 月 31 日。

   您还可以单击 **导出**，将本次的查询结果下载到浏览器默认下载文件夹。

4. 单击目标操作左侧的加号（+）查看操作的详细信息。

3.9.3. 关注订阅

蚂蚁金融科技为用户提供了订阅操作审计的能力，可将制定操作发送到接受订阅用户的邮箱、手机或钉钉。

新增订阅

空间管理员可以为指定用户、用户组或钉钉机器人添加订阅配置。操作步骤如下：

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **审计中心** > **关注订阅**。
3. 单击 **订阅管理** 页签，然后单击 **创建订阅**。
4. 填写订阅的名称和描述，然后单击 **下一步**。
5. 选择要订阅的操作，然后单击 **下一步**。
6. 单击 **添加订阅者**，并配置以下参数后，单击 **保存**。

参数	说明
类型	选择订阅的接受者，可以选择 **操作员**、**用户组**、**钉钉机器人**。
名称	根据 **类型** 输入操作员名称、组名称或钉钉 Token。
通讯方式	选择订阅的通讯方式。 ○ **类型** 为 **操作员** 和 **用户组** 时可选择 **邮件**、**短信**、**钉钉**。 ○ **类型** 为 **钉钉机器人** 时，此项不可配置。

   您可以根据需要同时添加多个订阅者。

7. 单击 **确定**。

   配置完成后，单击 **详情** 可查看订阅的详细配置。

查看我的订阅

管理员配置订阅后，涉及订阅的用户或用户组可以查看订阅的详细信息。操作步骤如下：

1. 在 IAM 控制台的左侧导航栏选择 **审计中心** > **关注订阅**。
2. 单击 **我的订阅**。

   您可以查看自己账号涉及的所有订阅配置。

3. 单击目标订阅右侧 **详情**。

   您可以查看订阅的基本信息、订阅操作和订阅者。

3.9.4. 跟踪管理

审计中心支持将操作审计日志投递到远程服务器，方便这些操作记录的后续管理、分析。目前，审计中心仅支持将操作审计日志投递至一台远程服务器。日志投递时间固定为每天的凌晨 1 点。

创建投递

1. 登录 IAM 控制台。
2. 在左侧导航栏选择 **审计中心** > **跟踪管理**。

3. 单击 **创建配置**，然后配置以下参数：

参数	说明
协议	选择投递使用的协议。 目前仅支持 SSH。
IP	填写远程服务器的 IP 地址。
端口	填写投递服务所用端口。
路径	填写审计日志文件在服务器上的保存路径。
用户名	填写远程服务器的用户名。
密码	填写远程服务器的密码。

4. 单击 **提交**。

   IAM 控制台会验证远程服务器的信息，填写错误信息会导致提交失败。

查看投递记录

1. 在 IAM 控制台左侧导航栏选择 **审计中心 > 跟踪管理**。
2. 在投递记录列表查看已执行投递的投递类型、投递的日志文件、投递状态、及投递创建时间。

   如果投递失败，您可以重新执行投递。

修改投递配置

您可以随时修改投递的目标服务器信息。操作步骤如下：

1. 在 IAM 控制台左侧导航栏选择 **审计中心 > 跟踪管理**。
2. 单击 **投递到远程服务器** 区域右上方的 **编辑** 按钮，并修改远程服务器的相关信息。
3. 单击 **提交**。

删除投递配置

如果不再需要将操作审计日志投递到服务器，可以删除投递。操作步骤如下：

1. 在 IAM 控制台左侧导航栏选择 **审计中心 > 跟踪管理**。
2. 单击 **投递到远程服务器** 区域右上方的 **删除**。
3. 单击 **确定**。

   删除后，系统不会再将操作记录投递到对应的远程服务器。

3.9.5. 审计日志接入云盾

IAM 审计日志支持接入阿里云云盾，本文介绍接入流程。

前提条件

- IAM 已升级至 2.43.0 或以上版本。
- 已获取获得专有云 SLS 的 host、AK（AccessKey ID）、SK（AccessKey Secret），以及创建好的 project 和 logstore。

操作步骤

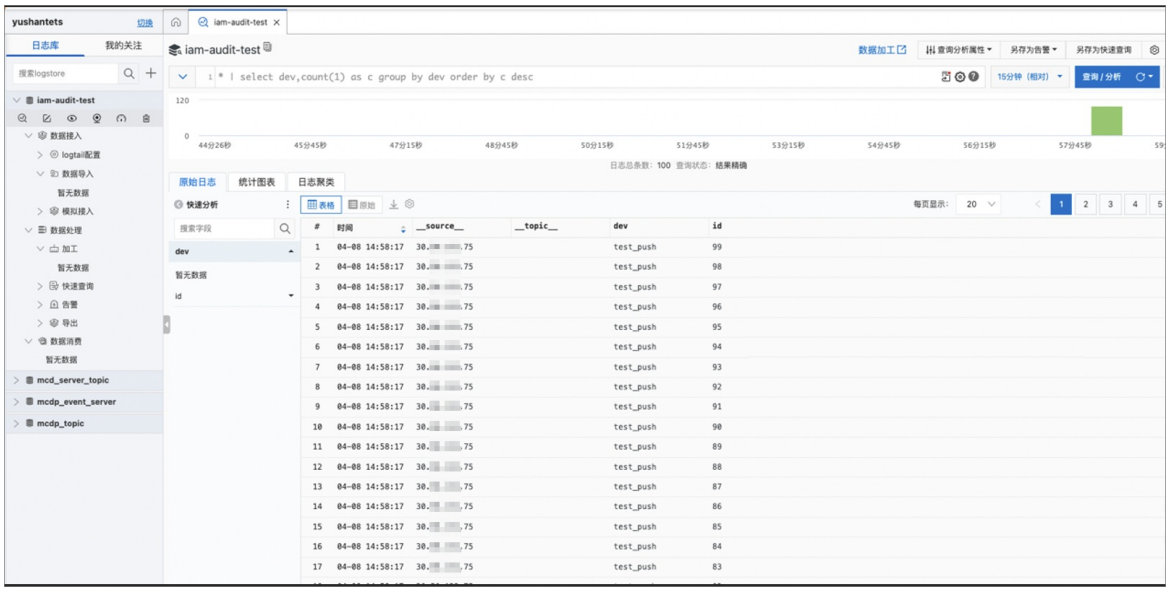
1. 登录 IAM 控制台。

   租户需要选择 ROC。

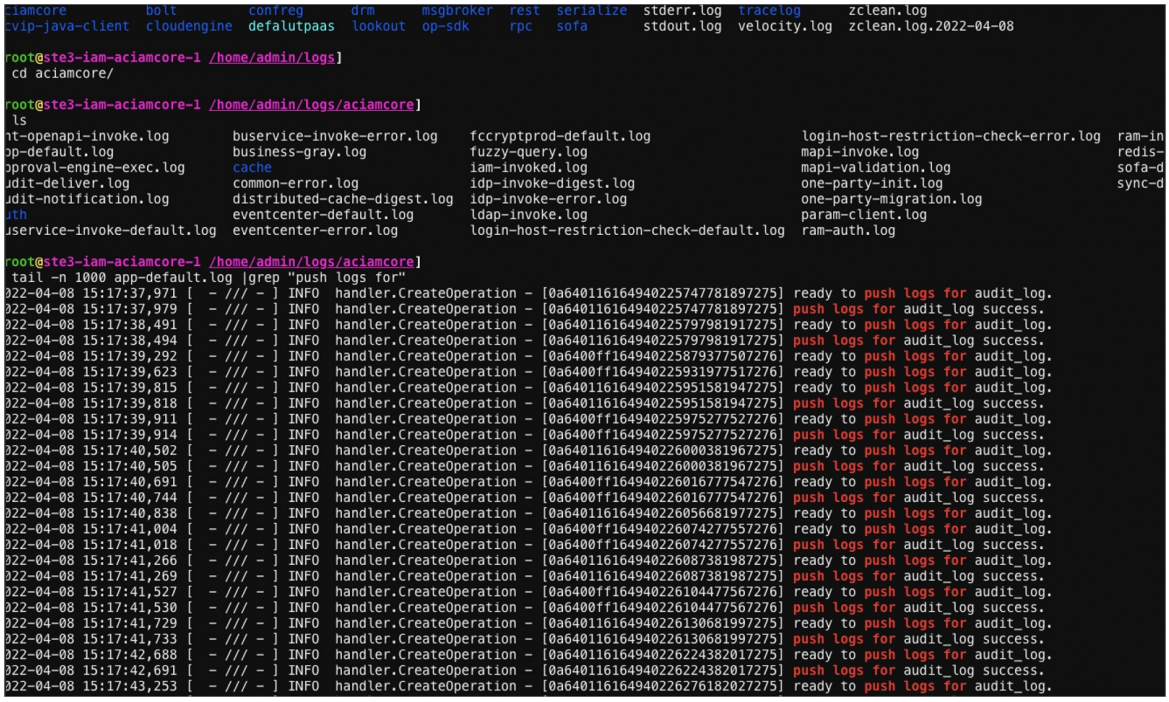
2. 在左侧导航栏选择 **系统管理** > **系统参数**。
3. 单击 **Iamcore** 页签，然后单击 **新增**。
4. 在 **创建系统参数** 对话框输入如下参数：

参数	说明
Key	输入 `SLS_CONFIG` 。
Value	填入 SLS 的 host、AK（AccessKey ID）、SK（AccessKey Secret），以及创建好的 project 和 logstore。格式如下： `{"accessId": "xoaqRuKxxxxxx", "accessKey": "cc9fgLuEuxxxxxxx", "host": "data.cn-hohhot-ste3-d01.sls.cloud.ste3.com", "projectName": "ali-audit-project", "logstoreName": "audit_log", "enable":true}`
描述（可选）	设置系统参数的描述信息。

5. 登录 SLS 控制台，查看日志是否已推送。



如果没有日志，您可以多次登录 IAM、进行查询等生成一些操作日志，然后在 aciamcore 中查询 `app-default.log` 有没有向 logstore 推送日志。



6. 将 IAM 的日志结构化字段和标准字段映射 XML 文件，并导入到云盾。

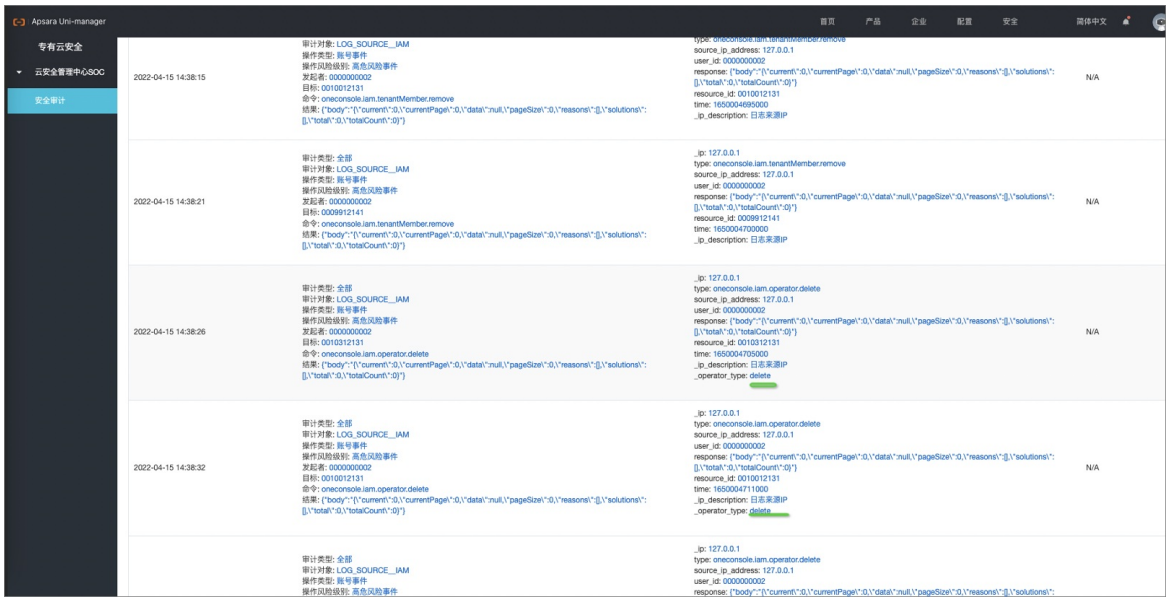
   此步骤由售后技术支持处理。

7. 登录云盾控制台。

8. 在右上方单击 **安全**，然后在 **全局平台安全** 区域单击 **云安全管理中心 SOC**。

9. 单击 **安全审计**，然后单击 **审计查询** 页签查询 IAM 日志。

若查询不到审计日志，可以多次单击 **查询** 按钮。查询到的日志示例如下：



3.10. 替换产品 Logo

您可以根据需要，替换您环境中 IAM 的产品 Logo。

操作步骤

根据 IAM 的不同版本，操作如下：

2.35.0 ~ 2.37.0 版本

1. 登录 IAM 控制台。
2. 选择租户为 **ROC**。
3. 在左侧导航栏选择 **系统管理** > **系统参数**。
4. 单击 **IamWeb** 页签，然后单击 **LOGO_CONFIG** 右侧的 **编辑**。
5. 修改以下参数后，单击 **OK**。

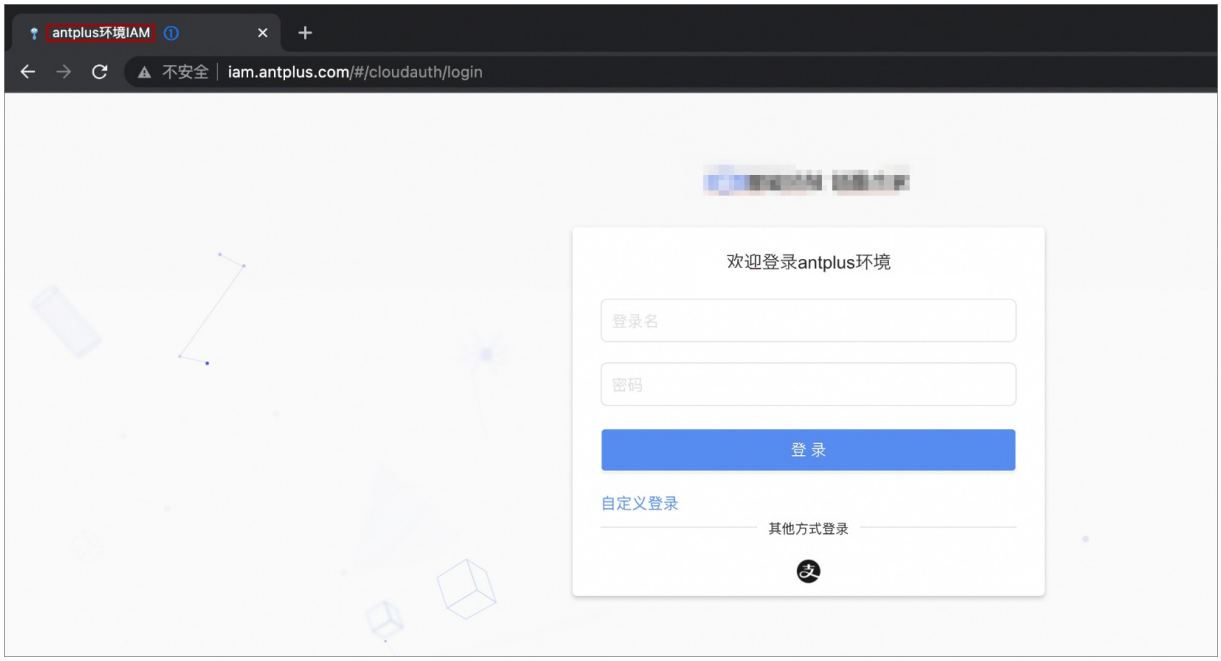
```
{
  "showCustomLogo": true,  // 是否显示自定义 Logo，需设置为 true。
  "title": "欢迎登录!",    // 设置登陆页 banner（如下图①位置），允许使用中文字符串。
  "loginLogoUrl": "http://example.com/logo1.png",  //设置登录页 Logo 图片的 URL（如下图②位置）。图片格式为 PNG，且允许 HTTP 服务器访问。
  "navLogoUrl": "http://example.com/logo2.png" //设置导航栏 Logo 图片的 URL（如下图③位置）。图片格式为 PNG，且允许 HTTP 服务器访问。
}
```

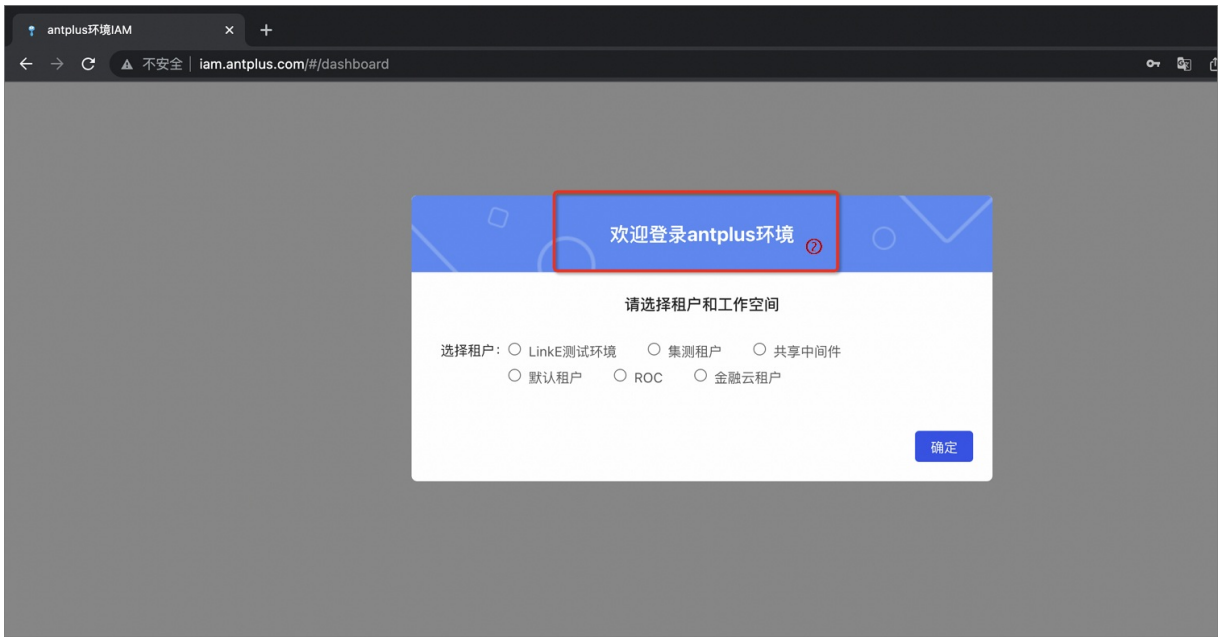
2.38.0 及以上版本

操作步骤与之前版本一致，修改参数如下：

```
{
  "productName": "antplus 环境 IAM",  // 设置浏览器的页签名称。
  "showCustomLogo": true,            // 是否显示自定义 Logo，需设置为 true。
  "title": "欢迎登录 antplus 环境",  // 设置登陆页 banner，同时也会替换切换租户时的 title。允许使用中文字符串。
  "loginLogoUrl": "http://example.com/logo1.png",  //设置登录页 Logo 图片的 URL。图片格式为 PNG，且允许 HTTP 服务器访问。
  "navLogoUrl": "http://example.com/logo2.png" //设置导航栏 Logo 图片的 URL。图片格式为 PNG，且允许 HTTP 服务器访问。
}
```

与之前版本相比，2.38.0 及以上版本增加了浏览器标签页的名称修改（如下图①位置）和切换租户时的 title 修改（如下图②位置），如图所示：





3.11. 附录：基础术语

本文介绍 IAM 控制台涉及的基础术语。

AccessKey

是访问蚂蚁科技 API 的密钥，包括 AccessKey ID 和 AccessKey Secret，用以标识用户的身份和权限。

操作员

同一企业下的不同租户间的成员是共享的，即一个操作员可以被添加到同一企业下的不同租户中。

多因素认证

多因素认证 MFA（Multi-Factor Authentication）是一种简单有效的最佳安全实践，在用户名和密码之外再增加一层安全保护。蚂蚁科技平台支持多因素认证的双重验证方式，可以有效保障账户安全。开启多因素认证后，您在登录蚂蚁科技管理控制台时，除了常规的账户密码校验外，还需要进行动态口令校验。

服务账号

服务账号是一类特殊的成员账号，它的使用者通常是一个程序或某一项服务。同其他成员账号一样，服务账号也可以被授权、被分配角色、拥有 AccessKey，不同的是它不会被任何一个自然人持有，因此不能用于登录，也没有邮箱、手机号等信息。

环境

环境又称为工作空间，是指为了完成软件开发、部署等工作所必需的硬件、软件、网络设备、数据的总称。一个租户下可以有多个环境，比如开发环境、生产环境等，各环境之间的资源是逻辑隔离的。

空间管理员

即租户的管理员，拥有租户的最高权限。

企业

可以是一个集团或者一家公司。

租户

可以是一个家子公司或者一个部门，一般来说具有财务独立性。一个企业下可以有多个租户。

4.容器底座

4.1. 什么是容器底座

云原生容器底座是一个基于 Kubernetes 和 Containerd 的应用管理平台，用于部署蚂蚁科技各产品组件。主要由容器引擎 AKE 云原生平台（AKE3）和产品控制台 Captain Plus 构成。

容器引擎 AKE 云原生平台（AKE3）

容器引擎 AKE3（Ant Financial Kubernetes Engine Plus）是将底层物理资源按照计算、网络、存储等进行切分和抽象的容器引擎。AKE3 通过使用 Kubernetes 和 Containerd 技术将整个物理资源进行池化，向上层服务提供按量使用的计算、网络和存储资源。

AKE3 包括以下组件：

- 分布式存储 etcd

  为整个 AKE3 的数据提供存储能力，其本身通过多副本提供数据一致性和高可靠性的能力。

- 中枢控制系统

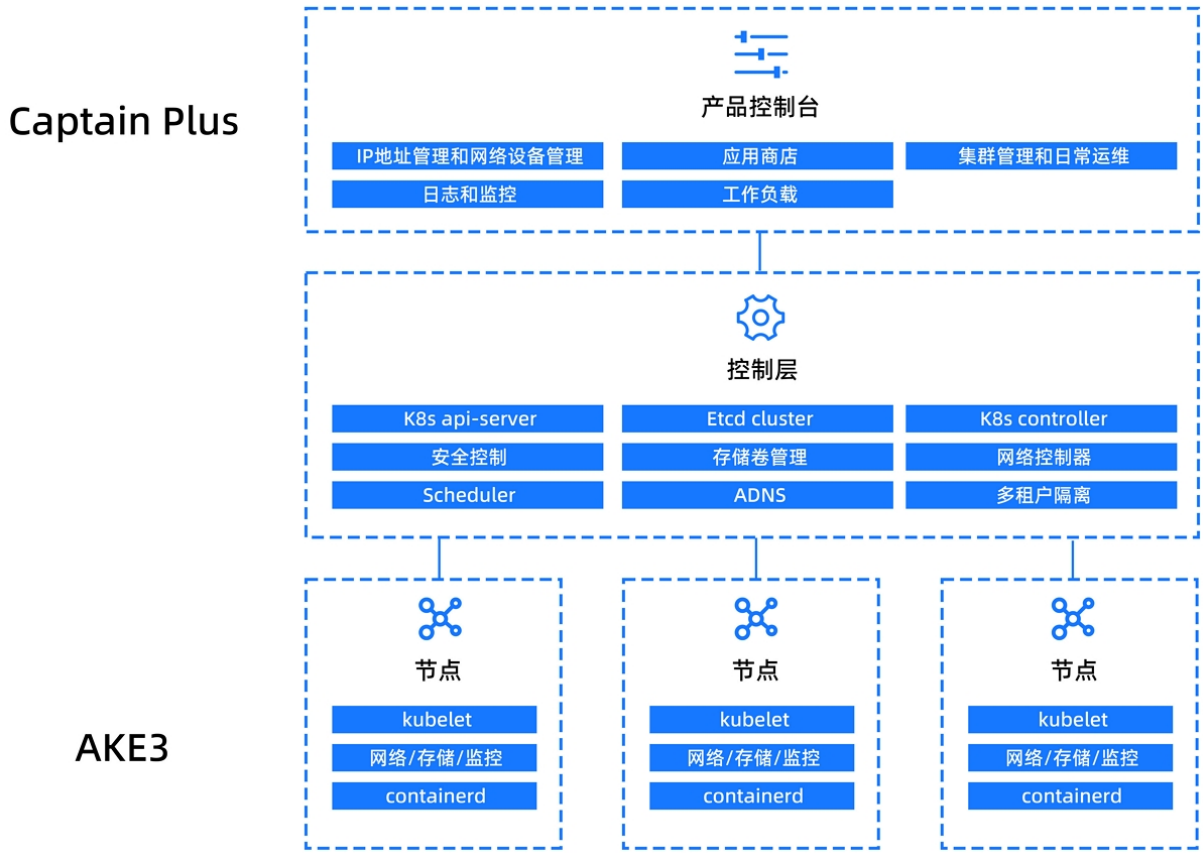
  包括 api-server、controller-manager、network-controller 以及 CNI-service 等。这些系统协同提供如网络管理、资源调度、存储调度、日志和事件等能力。

- 执行节点组件

  包括 Containerd、kubelet、CSI-plugin、CNI-plugin 等组件，运行在每台提供负载能力的物理机或者虚拟机上。

产品控制台 Captain Plus

Captain Plus 是 AKE3 的产品化入口，提供了用户鉴权、集群管理、网络管理、工作负载管理、配置管理、应用商店、镜像中心等能力。整体组件和相互关系如下图所示：



4.2. 登录 Captain 控制台

Captain 控制台是 AKE 云原生平台（AKE3）的产品化入口，提供了用户鉴权、集群管理、网络管理、工作负载管理、配置管理、应用商店、镜像中心等能力。

前提条件

- 已获得 Captain 控制台的 IP 地址或服务域名。
- 已拥有蚂蚁账号，并获得 Captain 控制台的访问权限。

操作步骤

1. 打开浏览器。

   推荐使用 Google Chrome。

2. 在地址栏输入 Captain 控制台的 IP 地址或服务域名。
3. 输入正确的用户名和密码后单击 **登录**。

4.3. 集群概览

集群是运行工作负载的逻辑分组，包含一组云服务器资源，每台云服务器即集群中的一个节点。首次使用云应用引擎基础版时，您需要创建一个初始集群，并添加至少一个节点。

集群概览页面展示集群的基础信息、节点、容器概要数据、使用情况等信息。

通过查看集群详情可了解集群的具体配置信息，包括版本配置、DNS 配置、网络配置、节点访问配置等。集群的节点和容器信息以卡片的形式展示，分别提供了查看全部资源的入口，可以快速跳转到相关页面。

查看集群信息

在概览页面，单击 **节点** 或 **容器组** 区域的 **查看全部** 可跳到对应节点或容器列表页查看相应详情。单击右上角的 **集群详情** 可查看集群相关配置信息，包括：

- **基本信息**：展示集群名称、集群状态（健康或不健康）、所属元集群、集群简介等信息。
- **基本配置**：展示 API 服务器地址、API Proxy 地址、DNS 域、服务子网等信息。
- **版本配置**：展示集群版本套件。

- **DNS 配置**：展示 DNS 控制器类型。
- **网络配置**：展示集群网络模式、节点主网卡、是否启用 ebtables 特性信息。
- **存储配置**：展示阿里云盘存储插件、阿里云 NAS 存储插件、阿里云 OSS 存储插件的启用状态。
- **节点访问配置**：展示节点访问类型。
- **云架构配置**：展示 CAFE 集群类型、地域、可用区、阿里云 VPC ID、阿里云 VSwitch ID 等信息。
- **其他配置**：展示 InsecureRegistry、节点自定义容器数据路径、节点自定义 kubelet 数据路径、 后端服务删除防护等信息。

更多操作

在集群详情界面，单击 **配置集群** 可修改集群配置；单击 **升级集群** 可对当前集群进行升级；修改初始化脚本后单击 **更新** 还可以更新初始化脚本。

4.4. 集群管理

4.4.1. 节点

4.4.1.1. 扩容节点

节点指用于部署和管理容器的服务器（可以是虚拟机实例或者物理服务器），该服务器会被注册到集群中，为集群提供相应的计算、网络、存储资源。节点内的资源会被统一管理和调度，当集群内节点资源不足时，会导致创建工作负载等操作失败。建议您及时关注节点的使用情况，并及时扩容。

云应用引擎-基础版支持以下两种扩容方式：

- 通用方式

  将环境中已有的处于运行中状态的 ECS 加入到集群中。

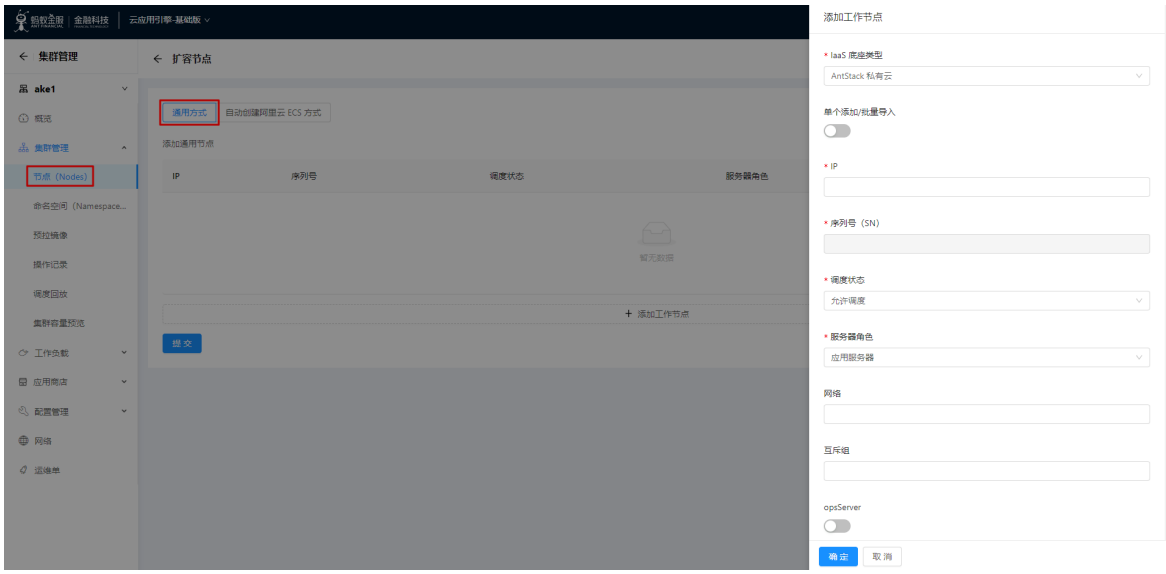
- 自动创建阿里云 ECS 方式

  添加新的阿里云 ECS 节点。

通用方式

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。
4. 在 **节点列表** 页面单击 **扩容节点**。
5. 在 **扩容节点** 页面选择 **通用方式**，然后单击 **添加工作节点**。

6. 在 **添加工作节点** 面板配置以下参数后，单击 **确定**。



参数	是否必填	说明
IaaS 底座类型	是	主要用于为节点打标签，可按需选择 **AntStack 私有云**、**阿里云** 或 **OpenStack**。
单个添加/批量导入	否	开启后可批量导入节点。
IP	是	输入要添加的节点 IP。 如果开启批量导入，则可以一次性输入多个节点 IP，多个 IP 换行填写。
调度状态	是	选择添加的节点是否允许调度。
服务器角色	是	选择节点的角色，可选值为：**应用服务器**、**数据库**、**OB**、**负载均衡**、**缓存**、**SAAS**、**Controller**。
网络	否	当集群使用 VLAN 网络模式时，可指定节点的网络名称。
互斥组	否	在 OpenStack 场景下，支持基于物理机的互斥。
opsServer	否	是否开启 opsServer。
CPU 超卖	否	设置 CPU 超卖的值。

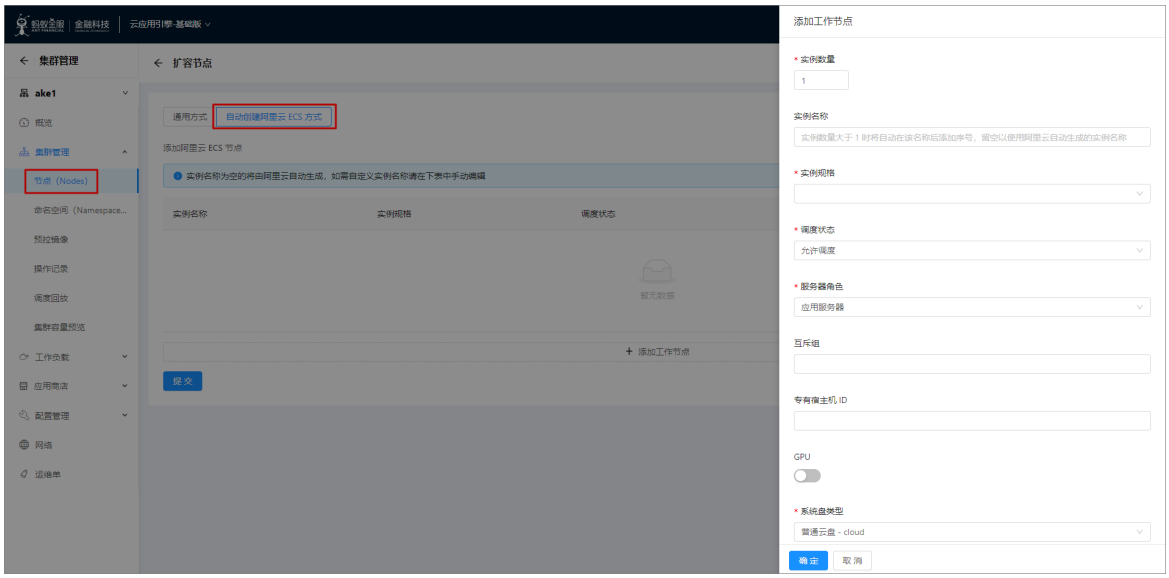
参数	是否必填	说明
内存超卖	否	设置内存超卖的值。
磁盘超卖	否	设置磁盘超卖的值。
自定义标签	否	为节点添加自定义标签。 单击 **添加标签** 并输入自定义键-值对。

7. 单击 **提交**。

   提交后，系统会自动进行节点的添加操作，请等待添加节点动作执行完成。

自动创建阿里云 ECS 方式

1. 在 **扩容节点** 页面选择 **自动创建阿里云 ECS 方式**，然后单击 **添加工作节点**。
2. 在 **添加工作节点** 面板配置以下参数后，单击 **确定**。



参数	是否必选	说明
实例数量	是	设置要添加的 ECS 实例数量。
实例名称	否	填写 ECS 实例名称，批量添加时会自动在该名称后面添加序号。 置空时使用 ECS 实例自动生成的名称。
实例规格	是	选择 ECS 实例的规格。

参数	是否必选	说明
调度状态	是	选择添加的节点是否允许调度。
服务器角色	是	选择节点的角色，可选值为：**应用服务器**、**数据库**、**OB**、**负载均衡**、**缓存**、**SAAS**、**Controller**。
互斥组	否	在 OpenStack 场景下，支持基于物理机的互斥。
专有宿主机 ID	否	填写宿主机 ID。
GPU	否	选择是否启用 GPU。开启后需选择 GPU 的 **lable** 和 **taint** 参数。
系统盘类型	是	选择系统盘类型。可选择普通云盘和高效云盘。
系统盘大小	是	设置系统盘大小。
数据盘	否	用于增加磁盘作为数据盘。 单击 **添加数据盘**，并设置数据盘类型和大小。
CPU 超卖	否	设置 CPU 超卖的值。
内存超卖	否	设置内存超卖的值。
磁盘超卖	否	设置磁盘超卖的值。
自定义标签	否	为节点添加自定义标签。 单击 **添加标签** 并输入自定义键-值对。

3. 单击 **提交**。

   提交后，系统会自动进行节点的添加操作，请等待添加节点动作执行完成。

4.4.1.2. 查看节点

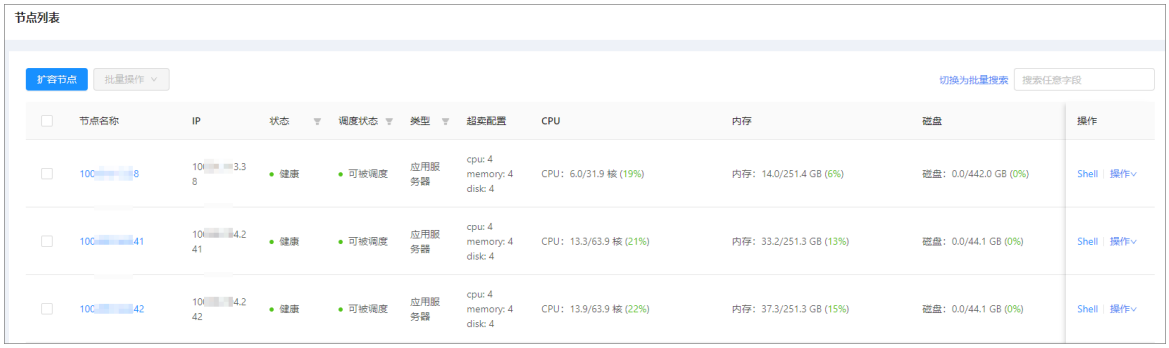
您可以通过 Captain 控制台查看节点的信息及使用情况，方便及时对节点进行调整。

操作步骤

1. 登录 Captain 控制台。

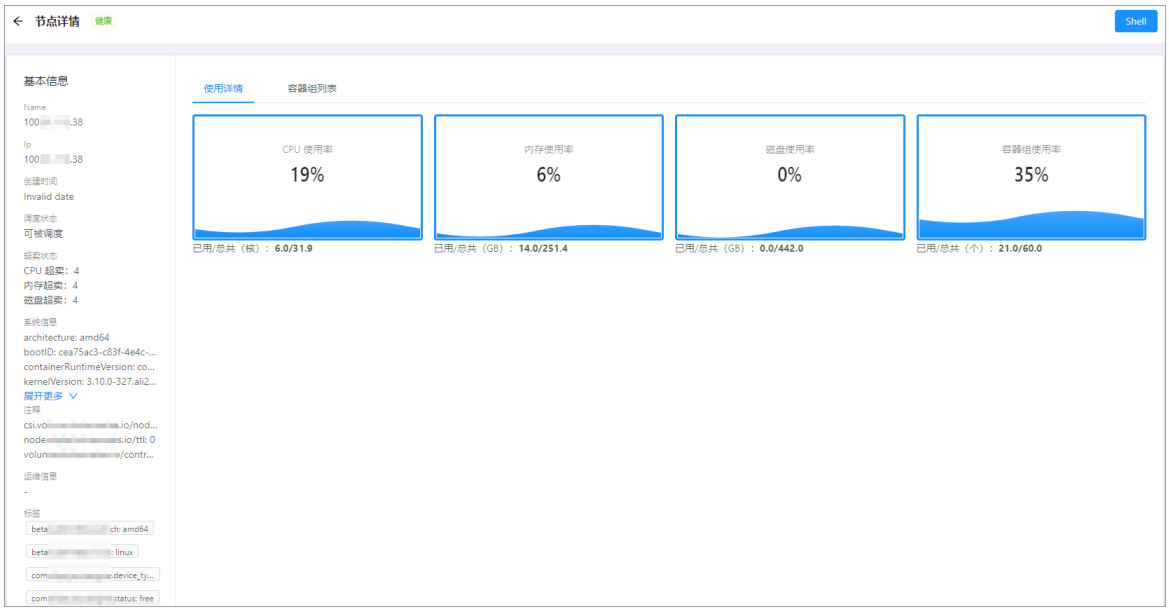
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。
4. 在 **节点列表** 查看所有节点的信息。

   您可以查看所有节点的概括信息，例如节点名称、IP、状态、CPU 使用率、内存使用率、硬盘使用率等。



5. 单击目标节点名称。

   您可以查看目标节点的详细信息，例如节点基本信息、使用详情、容器列表、容器组列表等。



4.4.1.3. 设置节点调度状态

您可以通过 Captain 控制台设置节点调度，从而合理分配各节点的负载。

前提条件

扩容节点时已设置允许调度。详细步骤，请参见 扩容节点。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。

4. 设置目标节点的调度状态。
   - 暂停调度

     节点暂停调度后，在后续进行应用部署时，Pod 不会再调度到该节点。

     a. 在 **节点列表** 选择目标节点右侧的 **操作** > **暂停调度**。

        您也可以批量选中多个节点，然后选择 **批量操作** > **暂停调度**。

     b. 单击 **提交**。

        等待任务完成，节点被设置为暂停调度状态。
   - 恢复调度

     节点恢复调度后，在后续进行应用部署时，Pod 可能会被调度到该节点。

     a. 在 **节点列表** 选择目标节点右侧的 **操作** > **恢复调度**。

        您也可以批量选中多个节点，然后选择 **批量操作** > **恢复调度**。

     b. 单击 **提交**。

        等待任务完成，节点被设置为恢复调度状态。

4.4.1.4. 管理节点标签

节点标签可以给节点定义不同的属性，通过这些标签可以快速的了解各个节点的特点，便于节点的管理和工作负载的调度。

注意事项

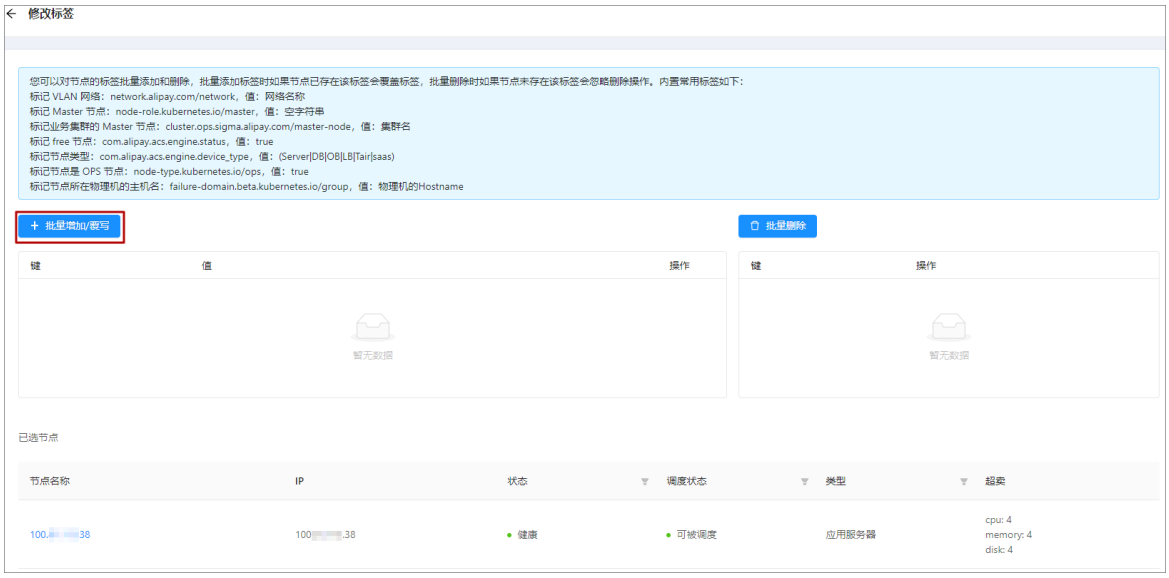
添加标签时，若节点已存在相同的标签键，则新增标签会覆写已有标签。

添加或修改标签

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。
4. 在 **节点列表** 选择目标节点右侧的 **操作** > **修改标签**。

   您也可以批量选中多个节点，然后选择 **批量操作** > **修改标签**。

5. 在 **修改标签** 页面，单击 **批量增加/覆写**。



6. 输入新增或修改的标签键和值，然后单击 **确定**。
7. 单击 **提交**。

   等待任务完成后，增加标签或修改标签操作完成。

删除标签

1. 在 **节点列表** 选择目标节点右侧的 **操作** > **修改标签**。

   您也可以批量选中多个节点，然后选择 **批量操作** > **修改标签**。
2. 在 **修改标签** 页面，单击 **批量删除**。
3. 在下拉列表选择待删除的标签。
4. 单击 **提交**。

   等待任务完成后，节点指定标签会被删除。

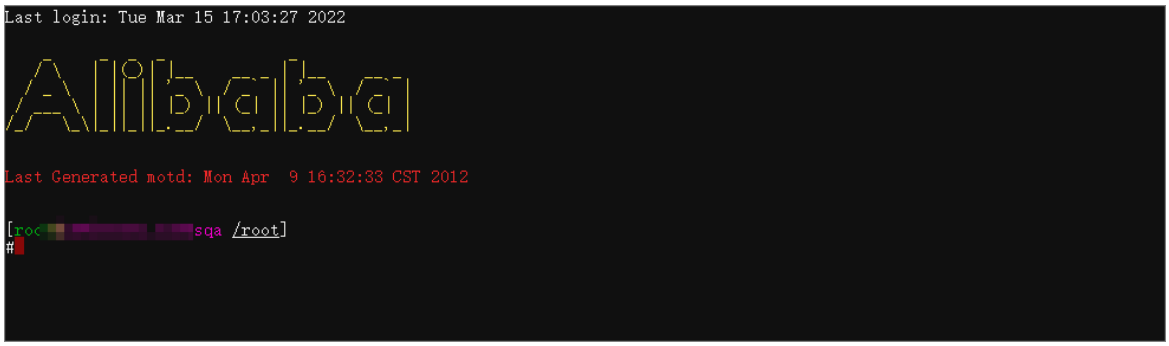
4.4.1.5. 节点的 Shell 操作

您可以通过 Captain 控制台对节点进行 Shell 操作。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。
4. 在 **节点列表** 单击目标节点右侧的 **Shell**。

您可以在弹出的 WebShell 页面像 Linux Shell 一样在节点上执行 Linux 命令。



4.4.1.6. 删除节点

当目标节点不再需要时，您可以通过 Captain 控制台删除节点，以节省资源。

注意事项

- 删除节点会引起 Pod 迁移，可能会影响业务，建议在业务低峰期操作。
- 操作过程中可能存在非预期风险，请提前做好相关的数据备份。
- 删除节点会把待删除节点从集群中移除并且清理节点上安装的软件。
- 删除节点前需确认节点上无业务容器。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **节点（Nodes）**。
4. 在 **节点列表** 选择目标节点右侧的 **操作** > **删除节点**。

   您也可以批量选择多个节点，然后选择 **批量操作** > **删除节点**。
5. 单击 **提交**。

   等待任务完成，节点即被删除。

4.4.2. 管理命名空间

命名空间（namespace）是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离，使得它们既可以共享同一个集群的服务，也能够互不干扰。例如，将开发环境、测试环境的业务分别放在不同的命名空间。

创建命名空间

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **命名空间**。
4. 单击 **创建**。
5. 在 **创建命名空间** 页面配置以下参数：
   - **名称**：输入命名空间的名称，不能与已有命名空间名称重复。

- **标签**（可选）：单击 **添加标签**，并设置标签的 **变量名** 和 **值**，可为命名空间添加标签。

6. 单击 **创建**。

   待任务完成后，命名空间创建成功。

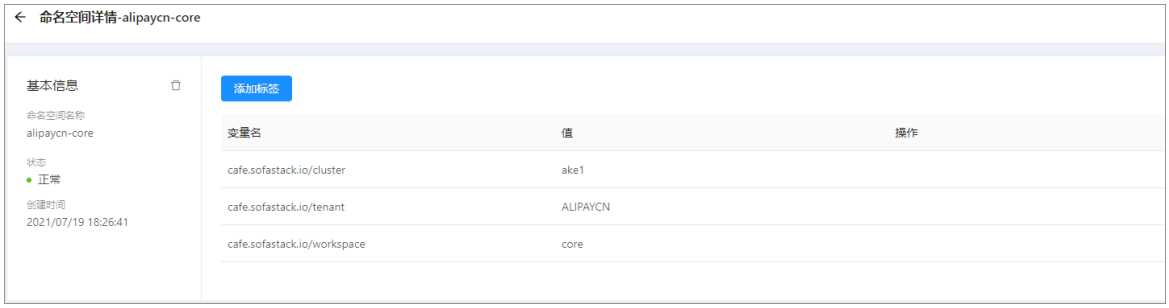
查看命名空间详情

1. 在左侧导航栏选择 **集群管理** > **命名空间**。
2. 在命名空间列表查看所有命名空间的基本信息。

   您可以查看命名空间的名称、标签、状态等信息。

3. 单击目标命名空间名称可查看命名空间的详细信息。

   您也可以在命名空间详情页添加、编辑或删除空间标签。



删除命名空间

> **注意**
>
> 删除命名空间会释放该命名空间下的所有资源，请谨慎操作。

1. 在左侧导航栏选择 **集群管理** > **命名空间**。
2. 单击目标命名空间右侧的 **删除**。
3. 单击 **确定**，然后在 **删除警告** 对话框再次单击 **确定**。

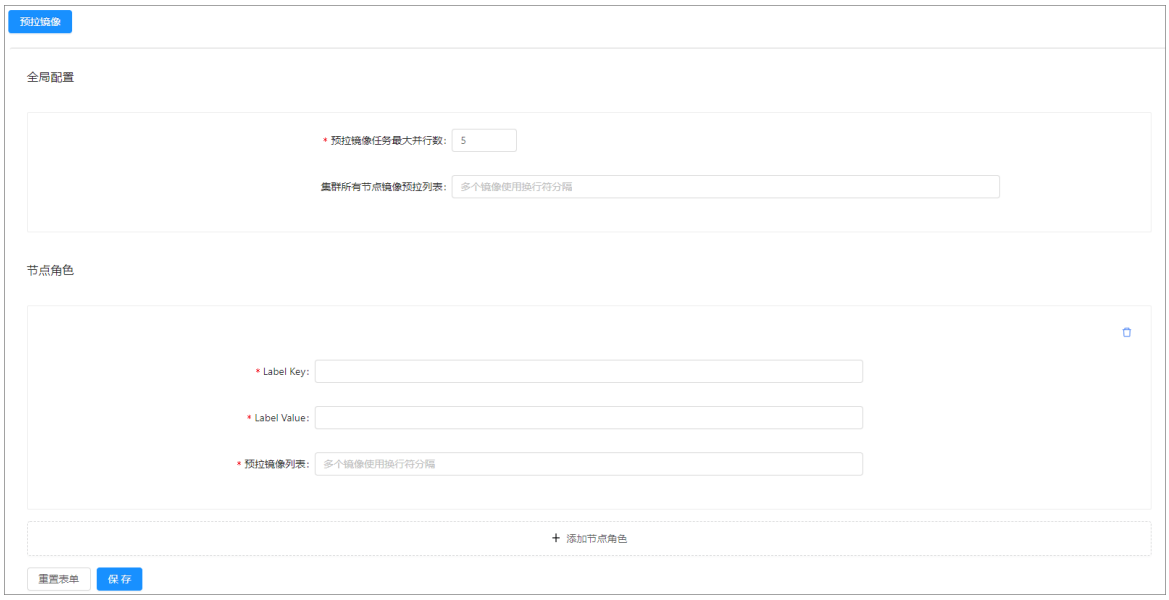
4.4.3. 预拉镜像

为加速创建容器的速度，您可以预先对一些目标节点进行镜像预拉，将预拉的镜像上传至镜像中心，方便后续查看。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **集群管理** > **预拉镜像**。

4. 在 **预拉镜像** 页面配置以下参数：



区域	参数	是否必须	说明
全局配置	预拉镜像任务最大并行数	是	设置预拉镜像任务最大并行数，默认值为 5。
	集群所有节点镜像预拉列表	否	填写集群节点的镜像地址，多个镜像需换行填写。
节点角色	Label Key	是	填写目标节点标签的键。
	Label Value	是	填写目标节点标签的值。
	预拉镜像列表	是	填写目标节点的镜像地址，多个镜像需换行填写。
	添加节点角色	否	单击可添加多个节点角色。

5. 单击 **保存**。
6. 单击 **预拉镜像**，然后单击 **确定** 开始预拉镜像。

4.4.4. 查看操作记录

您可以在 Captain 控制台查看用户在集群管理页面上的操作记录。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **操作记录**，然后根据需要查看操作记录。
   - 查看集群操作记录
     a. 单击 **集群操作记录**。
     b. 配置要查看的操作记录的时间段后，单击 **查询**。

     您可以查看集群进行的操作、操作人、操作时间等数据。

   - 查看节点操作记录
     a. 单击 **节点操作记录**。
     b. 配置要查看的操作记录的时间段后，单击 **查询**。

     您可以查看操作的节点名称和 IP、进行的操作、操作人、操作时间等数据。

4.4.5. 调度回放

4.4.5.1. 安装调度回放组件

Captain 1.2.1 及以上版本已支持调度回放功能，用于自动捕捉容器调度失败操作，并回放失败原因。本文介绍如何安装调度回放组件，以生效该功能。

前提条件

已升级 Captain 1.2.1 及以上版本。

操作步骤

1. 单击 akepluscharts 下载 akepluscharts 1.4.0 及以上版本的镜像。
2. 执行如下命令在当前文件夹下生成 chart 包。

```
docker run --rm -v $PWD/.:/helm_data acs-reg.alipay.com/acloud/akepluscharts:EI62165529
_20211201_20211201164249_082d31cc
```

生成的产品如下图所示：

```
drwxrwxrwx 1 root root    512 Dec  2 13:44 ./
drwxrwxrwx 1 root root    512 Dec  2 13:41 ../
-rwxrwxrwx 1 root root  54936 Dec  2 13:44 cert-manager-v1.1.1.tgz*
-rwxrwxrwx 1 root root 142261 Dec  2 13:44 cert-manager-v1.3.1.tgz*
-rwxrwxrwx 1 root root  26183 Dec  2 13:44 grafana-6.2.5.tgz*
-rwxrwxrwx 1 root root  23447 Dec  2 13:44 kruise-0.7.0.tgz*
-rwxrwxrwx 1 root root 318816 Dec  2 13:44 kube-prometheus-stack-12.12.6.tgz*
-rwxrwxrwx 1 root root  11238 Dec  2 13:44 kube-state-metrics-2.12.1.tgz*
-rwxrwxrwx 1 root root  26168 Dec  2 13:44 minio-8.0.9.tgz*
-rwxrwxrwx 1 root root   5770 Dec  2 13:44 node-problem-detector-1.8.6.tgz*
-rwxrwxrwx 1 root root    981 Dec  2 13:44 post-config-1.0.0.tgz*
-rwxrwxrwx 1 root root   6123 Dec  2 13:44 prometheus-node-exporter-1.14.3.tgz*
-rwxrwxrwx 1 root root   2492 Dec  2 13:44 scheduling-insight-1.0.0.tgz*
-rwxrwxrwx 1 root root   1821 Dec  2 13:44 shiva-1.0.0.tgz*
-rwxrwxrwx 1 root root  12358 Dec  2 13:44 yoda-1.1.1.tgz*
root@clive-laptop:/mnt/d/projects/云游/charts/test#
```

3. 卸载当前环境的 scheduling-insight 产品。

   卸载产品操作，请参见 删除发布。

   > **说明**
   >
   > 若未安装该产品，请忽略此步骤。

4. 将步骤 2 生成的 chart 包上传。

   操作步骤，请参见 上传产品或产品集合模板。

5. 在 kube-system 命名空间下安装 chart。

   操作步骤请参见 发布产品。

6. 验证安装是否成功。

   在左侧导航栏选择 **集群管理** > **调度回放**，若页面无报错信息，则组件安装成功。

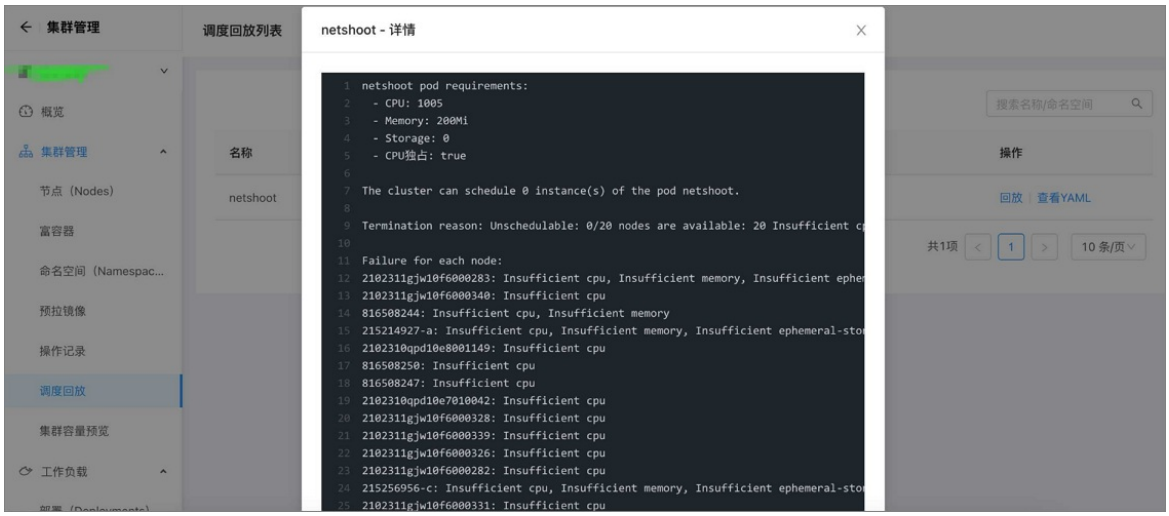
4.4.5.2. 查看调度回放

调度回放功能会自动捕捉容器调度失败操作，并回放失败原因。您可以按节点诊断失败原因，快速定位问题原因。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **调度回放**。
4. 单击目标调度任务右侧的 **回放**。

您可以从回放详情中查看 Pod 调度失败的详细信息，包括每个节点不匹配的原因。

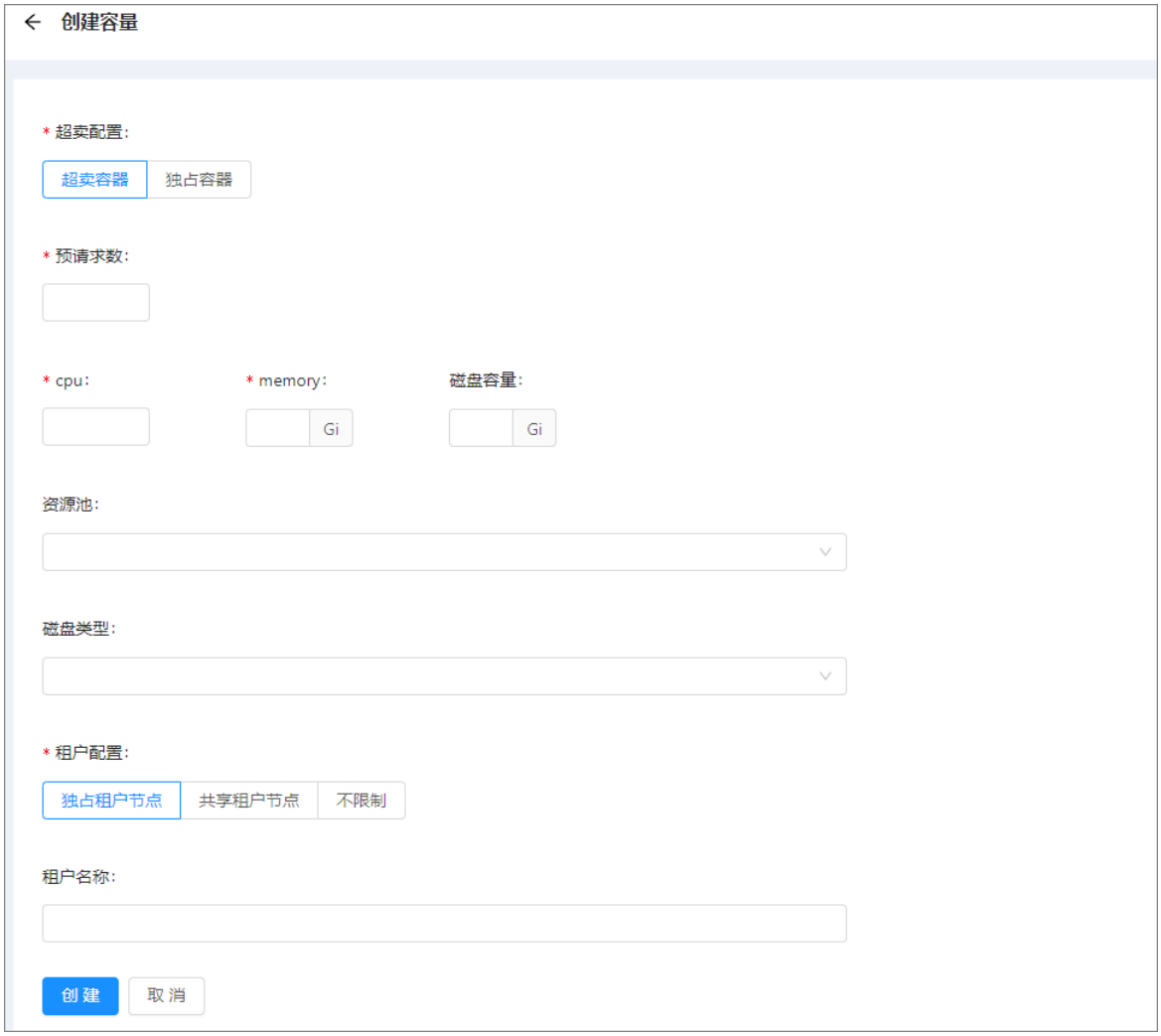


4.4.6. 集群容量预览

您可以通过集群容量预览实时评估集群当前容量和 Pods 分布情况。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **集群容量预览**，然后单击 **创建容量评估单**。
4. 在 **创建容量** 页面配置以下参数：



参数	是否必须	说明
超卖配置	是	选择容器超卖配置类型。可选择 **超卖容器** 和 **独占容器**。
预请求数	是	设置容器的预请求数量。
cpu	是	设置容器的 CPU 核数。
memory	是	设置容器的内存大小，单位 GiB。
磁盘容量	是	设置容器的磁盘容量，单位 GiB。
资源池	否	选择容器的资源池。

参数	是否必须	说明
磁盘类型	否	选择容器的磁盘类型。可选择 ssd 和 sata。
租户配置	是	选择租户节点类型。可选择 **独占租户节点**、**共享租户节点** 和 **不限制**。
租户名称	否	填写租户的名称。

5. 单击 **创建**。

   创建完成后，您可以在 **集群容量预览** 页面查看磁盘状态。

4.5. 工作负载

4.5.1. 部署（Deployments）

4.5.1.1. 创建部署

部署是一种无状态的应用集合，可用于管理 Pod 和 ReplicaSet。本节介绍如何创建部署。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **部署（Deployments）**。
4. 在 **部署（Deployments）** 页面选择创建部署的方式。

   目前支持通过导航页面和 YAML 创建：

   - 通过导航页面创建

a. 单击 **创建 Deployment**。

b. 在 **填写基本信息** 页签选择部署所属空间，并填写部署的名称，之后单击 **下一步**。

c. 在 **Pod 模板配置** 页签配置以下参数后，单击 **下一步**。

参数	是否必须	说明
名称	是	输入 Pod 名称。
镜像选择	是	目前仅支持镜像仓库。
镜像地址	是	填写镜像所在地址，格式为：`${repository_path}:${tag}`。 例如：`10.0.0.1:80`。 您还可以选中 **使用保密字典拉取镜像**，并指定保密字典，系统将使用保密字典加密镜像。
CPU 配置	是	设置容器使用的 CPU 核数： ■ **请求核数**：设置容器至少能使用的 CPU 核数。单位为：core 和 millicore。换算公式为：1 core = 1000 millicores。 ■ **最大核数**：设置容器能使用的最大 CPU 核数。
内存配置	是	设置容器使用内存的数量： ■ **请求内存**：设置容器至少能使用的内存数。单位为：GiB 和 MiB。换算公式为：1 GiB = 1024 MiB。 ■ **最大内存**：设置容器能使用的最大内存数。
启动命令	否	设置容器的启动命令，例如：`/home/admin/entrypoint.sh`。
高级配置	否	配置容器的标签元数据、环境变量和数据卷。 ■ **标签元数据配置**：配置标签的 **变量名** 和 **值**。 ■ **环境变量配置**：配置容器环境变量的 **变量名** 和 **值**。 ■ **数据卷配置**：配置容器使用的数据卷。目前仅支持挂载当前容器所在宿主机的目录。

d. 在 **伸缩配置** 页签配置以下参数后，单击 **下一步**。

参数	是否必须	说明
副本数	是	配置应用运行时保持的 Pod 副本数。

伸缩策略	是	配置部署的伸缩策略，支持 **滚动升级** 和 **删除重建**：
		■ **滚动升级**：自动创建一个新的 ReplicaSet，然后慢慢从 0 开始扩容，旧的 ReplicaSet 慢慢缩容至 0，直到完成滚动升级。升级过程中，服务会存在多个版本。
		  ■ **MAX Surge**：设置升级过程中超过预期 Pod 副本数的最大允许数量。
		  ■ **MAX Unavailable**：设置升级过程中不可用 Pod 的最大数量。
		  ■ **最小 Ready 时间**：Pod 中容器服务经过最小 Ready 时间后才会被认为可用。
		■ **删除重建**：手动删除已有的 Pod，并重建新的 Pod。此方式会导致服务短时间停用。
		最小 Ready 时间：Pod 中容器服务经过最小 Ready 时间后才会被认为可用。

e. 在 **网络配置** 页签配置以下参数：

参数	是否必须	说明
DNS 策略	是	配置部署的 DNS 策略。可选值： ■ **None**：不配置 DNS 策略。 ■ **Default**：使用默认 DNS 策略。 ■ **CluesteFirst**：使用集群优先策略。 ■ **ClusterFirstWithhostNet**：具有主机网络的集群优先策略。
是否 HostNetwork	否	选择部署是否为主机网络。

f. 单击 **立即创建**。

创建成功后，部署处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

- 通过 YAML 创建

a. 单击 **从 YAML 创建**。

b. 在输入框输入 YAML 内容后，单击 **提交**。

YAML 的内容格式请参见 Kubernetes - Pod。创建成功后，部署处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

4.5.1.2. 编辑部署

对于已创建的部署，您可以随时修改部署的配置参数。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **部署（Deployments）**。
4. 在 **命名空间** 下拉列表选择目标部署所在命名空间。
5. 编辑部署的配置。

   目前支持通过导航页面和 YAML 编辑部署的配置：

   - 通过导航页面编辑部署配置

     a. 单击目标部署右侧的 **编辑** 按钮。

     b. 按照导航流程修改部署配置。

     其中，基础配置和网络配置不允许修改，其他配置说明请参见 创建部署。

     c. 配置修改完成后，单击 **立即更新**。

     更新成功后，会自动根据新的配置信息部署。

   - 通过 YAML 编辑部署配置

     a. 单击目标部署右侧的 **编辑 YAML** 按钮。

     b. 在文本框输入新的 YAML 内容，然后单击 **更新**。

     其中，基础配置和网络配置相关参数不允许修改。更新成功后，会自动根据新的配置信息部署。

4.5.1.3. 删除部署

对于不再需要的部署，您可以通过 Captain 控制台删除。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **部署（Deployments）**。
4. 在 **命名空间** 下拉列表选择目标部署所在命名空间。
5. 单击目标部署右侧的 **删除** 按钮，然后单击 **确定**。

4.5.2. 有状态副本集（Statefulsets）

4.5.2.1. 创建有状态副本集

有状态副本集是用来管理某 Pod 集合的部署、扩容和缩容，并为这些 Pod 提供持久存储和持久标识符。本文介绍如何创建有状态副本集。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **有状态副本集（Statefulsets）**。
4. 在 **有状态副本集（Statefulsets）** 页面选择创建有状态副本集的方式。

   目前支持通过导航页面和 YAML 创建：

   - 通过导航页面创建

     a. 单击 **创建 Statefulset**。

     b. 在 **填写基本信息** 页签选择有状态副本集所属命名空间，并填写有状态副本集的名称，然后单击 **下一步**。

c. 在 **Pod 模板配置** 页签配置以下参数后，单击 **下一步**。

参数	是否必须	说明
名称	是	输入 Pod 名称。
镜像选择	是	目前仅支持镜像仓库。
镜像地址	是	填写镜像所在地址，格式为：`${repository_path}:${tag}`。 例如：`10.0.0.1:80`。
CPU 配置	是	设置容器使用的 CPU 核数： ■ **请求核数**：设置容器至少能使用的 CPU 核数。单位为：core 和 millicore。换算公式为：1 core = 1000 millicores。 ■ **最大核数**：设置容器能使用的最大 CPU 核数。
内存配置	是	设置容器使用内存的数量： ■ **请求内存**：设置容器至少能使用的内存数。单位为：GiB 和 MiB。换算公式为：1 GiB = 1024 MiB。 ■ **最大内存**：设置容器能使用的最大内存数。
启动命令	否	设置容器的启动命令，例如：`/home/admin/entrypoint.sh`。
高级配置	否	配置容器环境变量的 **变量名** 和 **值**。

d. 在 **伸缩与访问配置** 页签配置以下参数：

参数	是否必须	说明
Service Name	否	配置服务名称。
副本数	是	配置应用运行时保持的 Pod 副本数。
更新策略	是	配置有状态副本集的更新策略，支持 **滚动更新** 和 **手动删除后重建**： ■ **滚动更新**：当有状态副本集模板更新时，控制器会删除和重建有状态副本集中的每个 Pod。当您设置 **Partitions** 时，只有序号大于或等于 **Partition** 的 Pod 会在模板更新时被更新。 ■ **手动删除后重建**：您必须手动删除 Pod 以便让控制器创建新的 Pod。
Pod 管理策略	是	配置 Pod 的创建策略，可选值如下： ■ **依次创建**：Pod 按序号依次创建。 ■ **并行创建**：多个 Pod 同时创建。

e. 单击 **立即创建**。

创建成功后，有状态副本集处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

- 通过 YAML 创建

a. 单击 **从 YAML 创建**。

b. 在输入框输入 YAML 内容后，单击 **创建**。

YAML 的内容格式请参见 Kubernetes - Pod。创建成功后，有状态副本集处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

4.5.2.2. 编辑有状态副本集

对于已创建的有状态副本集，您可以随时修改有状态副本集的配置参数。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **有状态副本集（Statefulsets）**。
4. 在 **命名空间** 下拉列表选择目标有状态副本集所在命名空间。
5. 编辑有状态副本集的配置。

   目前支持通过导航页面和 YAML 编辑有状态副本集的配置：

   - 通过导航页面编辑

a. 单击目标有状态副本集右侧的 **编辑** 按钮。

b. 按照导航流程修改有状态副本集配置。

其中，基础配置和网络配置不允许修改，其他配置说明请参见 创建有状态副本集。

c. 配置修改完成后，单击 **立即更新**。

更新成功后，会自动根据新的配置信息部署。

- 通过 YAML 编辑

a. 单击目标有状态副本集右侧的 **编辑 YAML** 按钮。

b. 在输入框输入新的 YAML 内容，然后单击 **更新**。

其中，基础配置和网络配置相关参数不允许修改。更新成功后，会自动根据新的配置信息部署。

4.5.2.3. 删除有状态副本集

对于不再需要的有状态副本集，您可以通过 Captain 控制台删除。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **有状态副本集（Daemonsets）**。
4. 在 **命名空间** 下拉列表选择目标有状态副本集所在命名空间。
5. 单击目标有状态副本集右侧的 **删除** 按钮，然后单击 **确定**。

4.5.3. 守护进程集（Daemonsets）

4.5.3.1. 创建守护进程集

守护进程集是运行在所有节点上的守护应用，用于确保节点上运行一个 Pod 的副本。 当有节点加入集群时，守护进程集会为它们新增一个 Pod，当有节点从集群移除时，这些 Pod 也会被及时回收。本文介绍如何创建守护进程集。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **守护进程集（Daemonsets）**。
4. 在 **守护进程集（Daemonsets）** 页面选择创建守护进程集的方式。

目前支持通过导航页面和 YAML 创建：

- 通过导航页面创建

a. 单击 **创建 Daemonset**。

b. 在 **填写基本信息** 页签选择守护进程集所属空间，并填写守护进程集的名称，之后单击 **下一步**。

c. 在 **Pod 模板配置** 页签配置以下参数后，单击 **下一步**。

参数	是否必须	说明
名称	是	输入 Pod 名称。
镜像选择	是	目前仅支持镜像仓库。
镜像地址	是	填写镜像所在地址，格式为：`${repository_path}:${tag}`。 例如：`10.0.0.1:80`。 您还可以选中 **使用保密字典拉取镜像**，并指定保密字典，系统将使用保密字典加密镜像。
CPU 配置	是	设置容器使用的 CPU 核数： ■ **请求核数**：设置容器至少能使用的 CPU 核数。单位为：core 和 millicore。换算公式为：1 core = 1000 millicores。 ■ **最大核数**：设置容器能使用的最大 CPU 核数。
内存配置	是	设置容器使用内存的数量： ■ **请求内存**：设置容器至少能使用的内存数。单位为：GiB 和 MiB。换算公式为：1 GiB = 1024 MiB。 ■ **最大内存**：设置容器能使用的最大内存数。
启动命令	否	设置容器的启动命令，例如：`/home/admin/entrypoint.sh`。
高级配置	否	配置容器的标签元数据、环境变量和数据卷。 ■ **标签元数据配置**：配置标签的 **变量名** 和 **值**。 ■ **环境变量配置**：配置容器环境变量的 **变量名** 和 **值**。 ■ **数据卷配置**：配置容器使用的数据卷。目前仅支持挂载当前容器所在宿主机的目录。

d. 在 **更新策略配置** 页签配置 **更新策略** 后，单击 **下一步**。

更新策略可选择 **滚动更新** 和 **手动删除**。

- **滚动更新**：在更新守护进程集模板后，老的守护进程集 Pods 将被终止，并且将以受控方式自动创建新的守护进程集 pods。配置参数如下：
  - **MAX Unavailable**：设置升级过程中不可用 Pod 的最大数量。
  - **最小 Ready 时间（秒）**：Pod 中容器服务经过最小 Ready 时间后才会被认为可用。
- **手动删除**：在更新守护进程集模板后，只有当你手动删除老的守护进程集 pods，新的守护进程集 Pod 才会被自动创建。配置参数如下：

  最小 Ready 时间（秒）：Pod 中容器服务经过最小 Ready 时间后才会被认为可用。

e. 在 **网络配置** 页签配置以下参数：

参数	是否必须	说明
DNS 策略	是	配置守护进程集的 DNS 策略。可选值： ■ **None**：不配置 DNS 策略。 ■ **Default**：使用默认 DNS 策略。 ■ **CluesteFirst**：使用集群优先策略。 ■ **ClusterFirstWithhostNet**：使用具有主机网络的集群优先策略。
是否 HostNetwork	否	选择守护进程集是否为主机网络。

f. 单击 **立即创建**。

创建成功后，守护进程集处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

- 通过 YAML 创建

  a. 单击 **从 YAML 创建**。

  b. 在输入框输入 YAML 内容后，单击 **创建**。

  YAML 的内容格式请参见 Kubernetes - Pod。创建成功后，守护进程集处于 **部署中** 状态，部署成功后变为 **运行中** 状态。

4.5.3.2. 编辑守护进程集

对于已创建的守护进程集，您可以随时修改守护进程集的配置参数。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **守护进程集（Daemonsets）**。

4. 在 **命名空间** 下拉列表选择目标守护进程集所在命名空间。
5. 编辑守护进程集的配置。

   目前支持通过导航页面和 YAML 编辑守护进程集的配置：

   - 通过导航页面编辑
     a. 单击目标守护进程集右侧的 **编辑** 按钮。
     b. 按照导航流程修改守护进程集配置。

        其中，基础配置和网络配置不允许修改，其他配置说明请参见 创建守护进程集。
     c. 配置修改完成后，单击 **立即更新**。

        更新成功后，会自动根据新的配置信息部署。
   - 通过 YAML 编辑
     a. 单击目标守护进程集右侧的 **编辑 YAML** 按钮。
     b. 在输入框输入新的 YAML 内容，然后单击 **更新**。

        其中，基础配置和网络配置相关参数不允许修改。更新成功后，会自动根据新的配置信息部署。

4.5.3.3. 删除守护进程集

对于不再需要的守护进程集，您可以通过 Captain 控制台进行删除。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **守护进程集（Daemonsets）**。
4. 在 **命名空间** 下拉列表选择目标守护进程集所在命名空间。
5. 单击目标守护进程集右侧的 **删除** 按钮，然后单击 **确定**。

4.5.4. 任务（Jobs）

4.5.4.1. 创建任务

任务用于创建一个或多个 Pods，然后确保指定数量的 Pod 运行到结束，当数量达到指定的成功个数阈值时，任务结束。本文介绍如何创建任务。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **任务（Jobs）**。
4. 在 **任务（Jobs）** 页面选择创建任务的方式。

目前支持通过导航页面和 YAML 创建：

- 通过导航页面创建
  a. 单击 **创建 Deployment**。
  b. 在 **填写基本信息** 页签填写以下参数后，单击 **下一步**。

参数	是否必须	说明
命名空间	是	选择创建任务的命名空间。
名称	是	输入任务名称。
完成次数	否	设置任务结束前必须成功运行的 Pod 个数。
Pod 并行度	否	填写并行运行的 Pod 个数。
Pod 重启策略	是	设置 Pod 的重启策略： ■ **从不重启**：对于运行失败的 Pod 不进行重启。 ■ **失败时重启**：当 Pod 运行失败时自动进行重启。

c. 在 **Pod 模板配置** 页签配置以下参数：

参数	是否必须	说明
名称	是	输入 Pod 名称。
镜像选择	是	目前仅支持镜像仓库。
镜像地址	是	填写镜像所在地址，格式为：`${repository_path}:${tag}`。 例如：`10.0.0.1:80`。
CPU 配置	是	设置容器使用的 CPU 核数： ■ **请求核数**：设置容器至少能使用的 CPU 核数。单位为：core 和 millicore。换算公式为：1 core = 1000 millicores。 ■ **最大核数**：设置容器能使用的最大 CPU 核数。
内存配置	是	设置容器使用内存的数量： ■ **请求内存**：设置容器至少能使用的内存数。单位为：GiB 和 MiB。换算公式为：1 GiB = 1024 MiB。 ■ **最大内存**：设置容器能使用的最大内存数。
启动命令	否	设置容器的启动命令，例如：`/home/admin/entrypoint.sh`。
高级配置	否	配置容器的标签元数据、环境变量和数据卷。 ■ **环境变量配置**：配置容器环境变量的 **变量名** 和 **值**。 ■ **数据卷配置**：配置容器使用的数据卷。目前仅支持挂载当前容器所在宿主机的目录。

d. 单击 **立即创建**。

创建成功后，任务处于 **未完成** 状态。

- 通过 YAML 创建

a. 单击 **从 YAML 创建**。

b. 在文本框输入 YAML 内容后，单击 **创建**。

YAML 的内容格式请参见 Kubernetes - Pod。创建成功后，任务处于 **未完成** 状态。

4.5.4.2. 编辑任务

对于已创建的任务，您可以随时修改任务的配置参数。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **任务（Jobs）**。
4. 在 **命名空间** 下拉列表选择目标任务所在命名空间。
5. 编辑任务的配置。

   目前支持通过导航页面和 YAML 编辑任务的配置：

   - 通过导航页面编辑任务配置
     a. 单击目标任务右侧的 **编辑** 按钮。
     b. 按照导航流程修改任务配置。

        其中，基础配置和网络配置不允许修改，其他配置说明请参见 创建任务。
     c. 配置修改完成后，单击 **立即更新**。

        更新成功后，会自动根据新的配置信息执行任务。
   - 通过 YAML 编辑任务配置
     a. 单击目标任务右侧的 **编辑 YAML** 按钮。
     b. 在文本框输入新的 YAML 内容，然后单击 **更新**。

        其中，基础配置相关参数不允许修改。更新成功后，会自动根据新的配置信息执行任务。

4.5.4.3. 删除任务

对于不再需要的任务，您可以通过 Captain 控制台删除。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **任务（Jobs）**。
4. 在 **命名空间** 下拉列表选择目标任务所在命名空间。
5. 单击目标任务右侧的 **删除** 按钮，然后单击 **确定**。

4.5.5. 容器组（Pods）

4.5.5.1. 创建容器

容器组是一个或多个容器的组合，这些容器共享存储、网络、以及怎样运行这些容器的声明。本文介绍如何创建容器。

背景信息

一般情况下，您并不需要手动创建容器。建议您通过以下方式创建：

- 创建部署
- 创建有状态副本集
- 创建守护进程集
- 创建任务

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **容器组（Pods）**。
4. 在 **容器组（Pods）** 页面选择创建容器的方式。

   目前支持通过导航页面和 YAML 创建：

   - 通过导航页面创建

     a. 单击 **创建 Pod**。

     b. 在 **填写基本信息** 页签选择容器所属空间，并填写容器的名称，之后单击 **下一步**。

c. 在 **Pod 模板配置** 页签配置以下参数：

参数	是否必须	说明
名称	是	输入 Pod 名称。
镜像选择	是	目前仅支持镜像仓库。
镜像地址	是	填写镜像所在地址，格式为：`${repository_path}:${tag}`。 例如：`10.0.0.1:80`。
CPU 配置	是	设置容器使用的 CPU 核数： ■ **请求核数**：设置容器至少能使用的 CPU 核数。单位为：core 和 millicore。换算公式为：1 core = 1000 millicores。 ■ **最大核数**：设置容器能使用的最大 CPU 核数。
内存配置	是	设置容器使用内存的数量： ■ **请求内存**：设置容器至少能使用的内存数。单位为：GiB 和 MiB。换算公式为：1 GiB = 1024 MiB。 ■ **最大内存**：设置容器能使用的最大内存数。
启动命令	否	设置容器的启动命令，例如：`/home/admin/entrypoint.sh`。
高级配置	否	配置容器的标签元数据、环境变量和数据卷。 ■ **标签元数据配置**：配置标签的 **变量名** 和 **值**。 ■ **环境变量配置**：配置容器环境变量的 **变量名** 和 **值**。 ■ **数据卷配置**：配置容器使用的数据卷。目前仅支持挂载当前容器所在宿主机的目录。

d. 单击 **立即创建**。

- 通过 YAML 创建

  a. 单击 **从 YAML 创建**。

  b. 在文本框输入 YAML 内容后，单击 **提交**。

  YAML 的内容格式请参见 Kubernetes - Pod。

4.5.5.2. 编辑容器

对于已创建的容器，您可以随时修改容器的配置参数。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **容器组（Pods）**。
4. 在 **命名空间** 下拉列表选择目标容器所在命名空间。
5. 编辑容器的配置。

   目前支持通过导航页面和 YAML 编辑容器的配置：

   - 通过导航页面编辑容器配置
     a. 单击目标容器右侧的 **编辑** 按钮。
     b. 按照导航流程修改容器配置。

        其中，基础配置和网络配置不允许修改，其他配置说明请参见 创建容器。
     c. 配置修改完成后，单击 **立即更新**。
   - 通过 YAML 编辑容器配置
     a. 单击目标容器右侧的 **编辑 YAML** 按钮。
     b. 在文本框输入新的 YAML 内容，然后单击 **更新**。

        其中，基础配置和网络配置相关参数不允许修改。

4.5.5.3. 删除容器

对于不再需要的容器，您可以通过 Captain 控制台删除。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **工作负载** > **容器组（Pods）**。
4. 在 **命名空间** 下拉列表选择目标容器所在命名空间。
5. 单击目标部署右侧的 **删除** 按钮，然后单击 **确定**。

4.6. 应用商店

4.6.1. 管理产品模板

4.6.1.1. 上传产品或产品集合模板

您可以通过 Captain 控制台上传或查看您的产品和产品集合模板，本文介绍如何上传产品或产品集合模板。

前提条件

已从蚂蚁科技交付团队获取到产品或产品集合模板文件（Helm chart包）。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **应用商店 > 产品模板**。
4. 在 **产品模板（Charts）** 页面单击 **上传产品模板** 或 **上传产品集合模板**。
5. 选择已获取的产品或产品集合模板文件后，单击 **打开**。

   上传成功后，您可以在 **产品模板（Charts）** 页面查看到已上传的产品或产品集合模板。

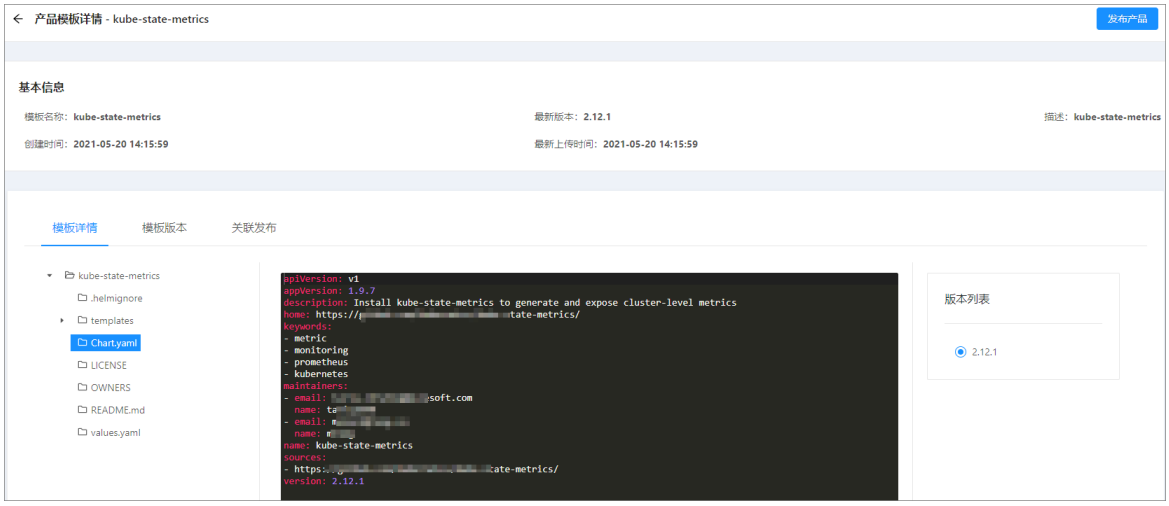
4.6.1.2. 编辑产品或产品集合模板

您可以通过 Captain 控制台查看和编辑已上传的产品或产品集合模板。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **应用商店 > 产品模板**。
4. 在 **产品模板（Charts）** 页面单击目标产品或产品集合模板的 **查看详情**。

   在 **产品模板详情** 页面，您可以查看产品模板的基本信息、详细信息、版本以及关联发布等信息。



5. 单击 **模板详情** 页签，然后根据您的需要修改模板文件。
6. 单击 **保存**。

4.6.2. 产品实例

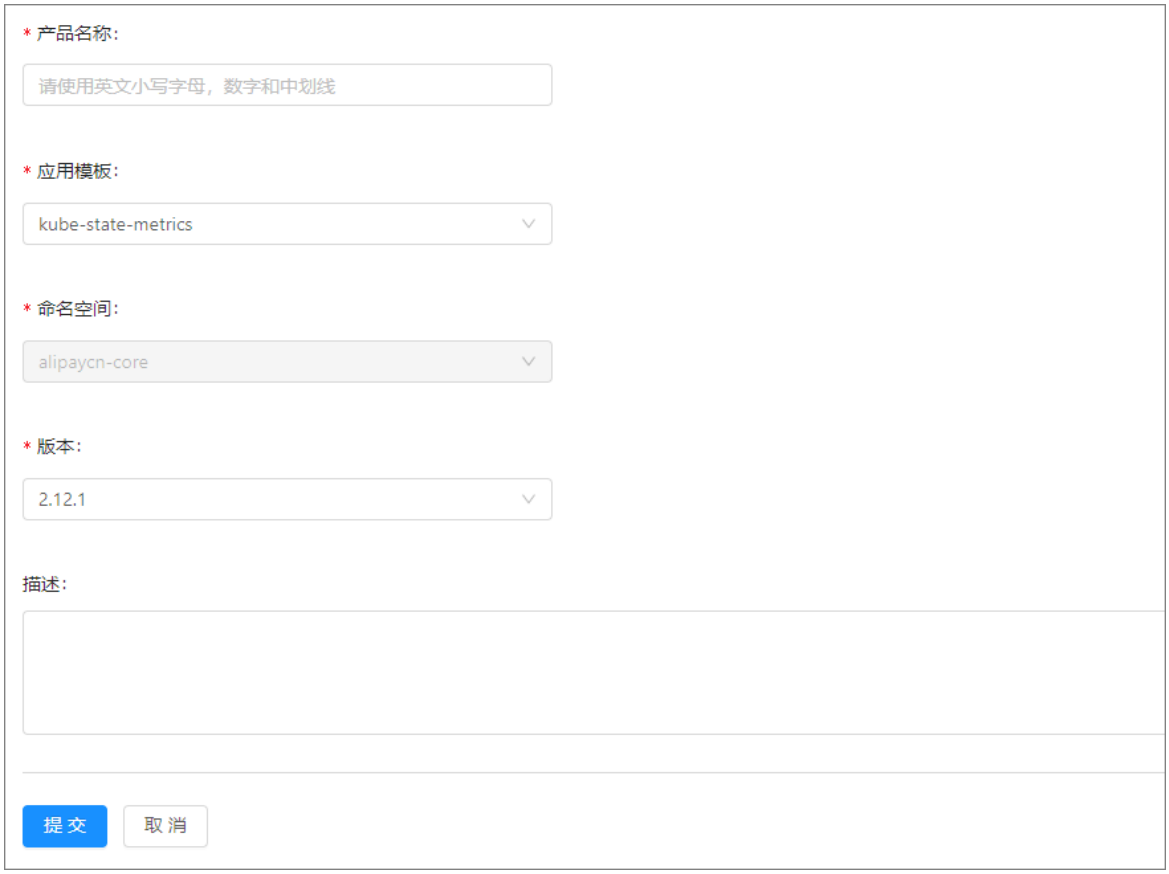
4.6.2.1. 发布产品

您可以通过 Captain 控制台创建产品发布任务，发布已编辑好的产品模板。

操作步骤

1. 登录 Captain 控制台。

2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **应用商店 > 产品实例**。
4. 在 **发布列表** 页面的 **命名空间** 下拉框，选择待发布产品的命名空间。
5. 单击 **创建发布**，并配置以下参数：



参数	是否必须	说明
产品名称	是	设置待发布产品的名称。
应用模板	是	选择发布的应用模板。
命名空间	是	使用默认选项。
版本	是	选择待发布应用的版本。
描述	否	为发布的应用添加描述信息。

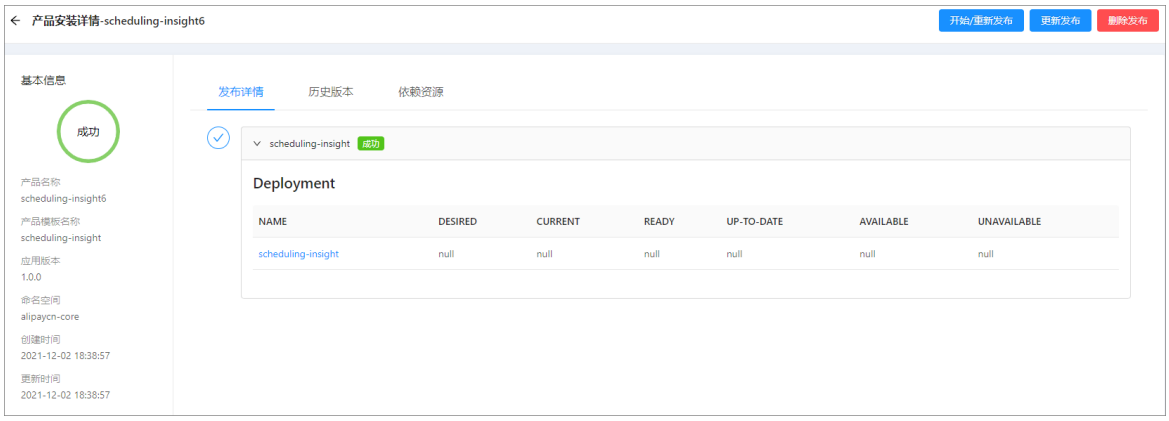
6. 单击 **提交**。

4.6.2.2. 查看已发布产品

对于已发布的产品，您可以通过 Captain 控制台查看发布状态、版本信息、依赖资源等信息。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **应用商店 > 产品实例**。
4. 在 **发布列表** 页面的 **命名空间** 下拉框，选择已发布产品的命名空间。
5. 单击目标产品查看产品信息。



- **基本信息**：查看产品的基本信息，例如产品名称、产品模板名称、应用版本等信息。
- **发布详情**：查看产品的 Deployment 和 Service 信息。
- **历史版本**：查看产品的历史版本信息，例如历史版本的模板版本、发布版本号、发布状态、发布人等信息。
- **依赖资源**：查看产品的依赖信息。

更多操作

您还可以在 **产品安装详情** 页进行如下操作：

- **开始/重新发布**：单击可开始或重新发布产品。
- **更新发布**：单击可重新发布产品的其他版本。编辑产品模板操作请参见 编辑产品或产品集合模板。
- **删除发布**：单击可删除已发布的产品。

4.7. 配置管理

4.7.1. 配置项

4.7.1.1. 创建配置项

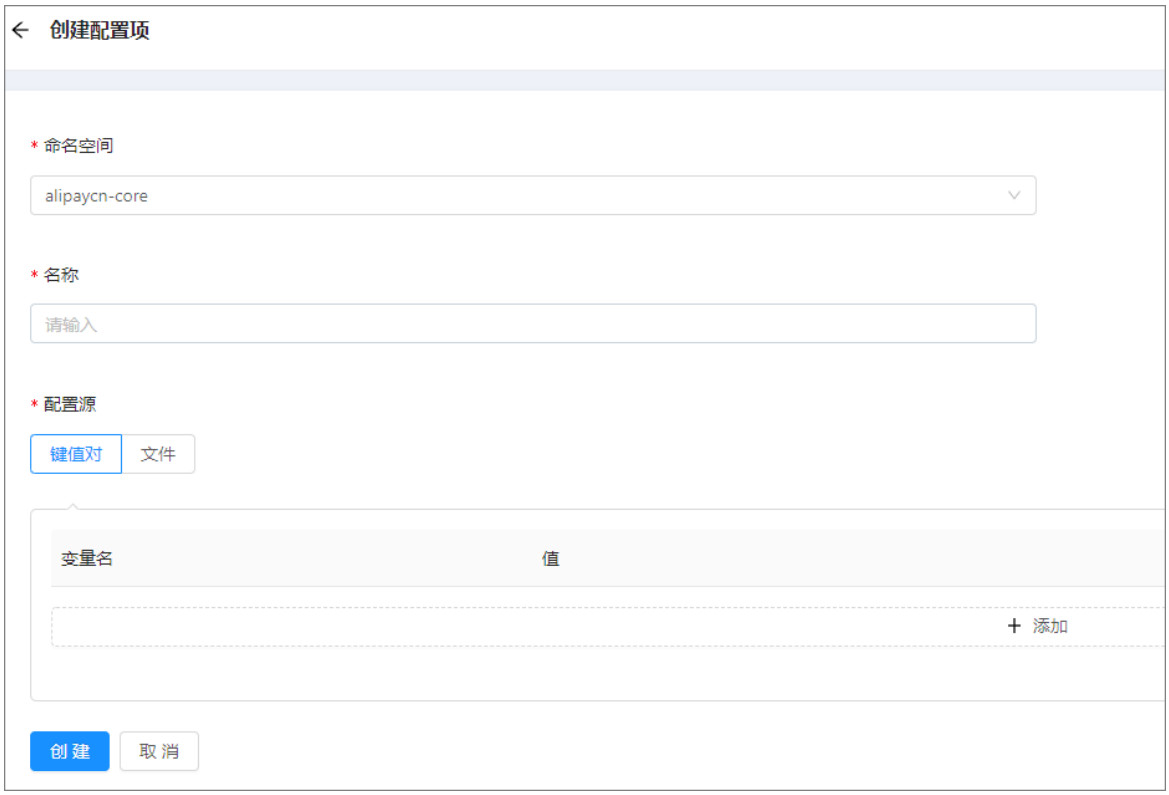
配置项（ConfigMap）是一种用于存储工作负载所需配置信息的资源类型，需要您自定义配置项的内容。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **配置项（Configmaps）**。
4. 在 **配置项（Configmaps）** 页面单击 **创建**。
5. 在 **创建配置项** 页面配置以下参数：



参数	是否必须	说明
命名空间	是	选择创建配置项的命名空间。
名称	是	输入配置项名称。
配置源	是	设置配置项的配置源信息，可选值如下： ○ **键值对**：变量名代表文件名；值代表文件中的内容。 ○ **文件**：可上传文件创建配置项。

6. 单击 **创建**。

4.7.1.2. 使用配置项

配置项创建后，您可以在 Pod 中使用，本文介绍配置项的使用场景。

配置项主要在以下使用场景中使用：

- 用配置项定义 Pod 环境变量

  使用配置项定义 Pod 中环境变量，使用 valueFrom 引用配置项数据。

  > **注意**
  >
  > 在 Pod 里使用配置项时，两者需处于同一命名空间中。

- 通过配置项设置命令行参数

  使用配置项设置容器中的命令或者参数值，使用环境变量替换语法 $(VAR_NAME)。

- 在数据卷中使用配置项

  在 volumes 下指定配置项名称，会将 key/values 的数据存储到 mountPath 路径下，最终生成以 key 为文件名，values 为文件内容的配置文件。

更多关于配置项的信息，请参见 Configure a Pod to Use a ConfigMap。

4.7.1.3. 修改配置项

对于已创建的配置项，您可以通过 Captain 控制台随时修改。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **配置项（Configmaps）**。
4. 在 **配置项（Configmaps）** 页面的 **命名空间** 下拉列表选择目标配置项所在命名空间。
5. 单击目标配置项名称，然后在 **配置项详情** 页面修改配置项：
   - 增加变量
     a. 单击 **添加配置项数据**。
     b. 在 **添加配置项数据** 面板单击 **添加配置项数据**，然后输入配置项的 **变量名** 和 **值**。
     c. 单击 **提交**。
   - 修改变量
     a. 单击目标变量右侧 **编辑**，修改 **变量名** 或变量 **值**。
     b. 单击 **提交**。
   - 删除变量

     单击目标变量右侧 **删除**，然后单击 **确定**。

4.7.1.4. 删除配置项

您可以通过 Captain 控制台删除不再需要的配置项。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **配置项（Configmaps）**。
4. 在 **配置项（Configmaps）** 页面的 **命名空间** 下拉列表选择目标配置项所在命名空间。
5. 单击目标配置项右侧的 **删除**。
6. 单击 **确认**。

4.7.2. 保密字典

4.7.2.1. 创建保密字典

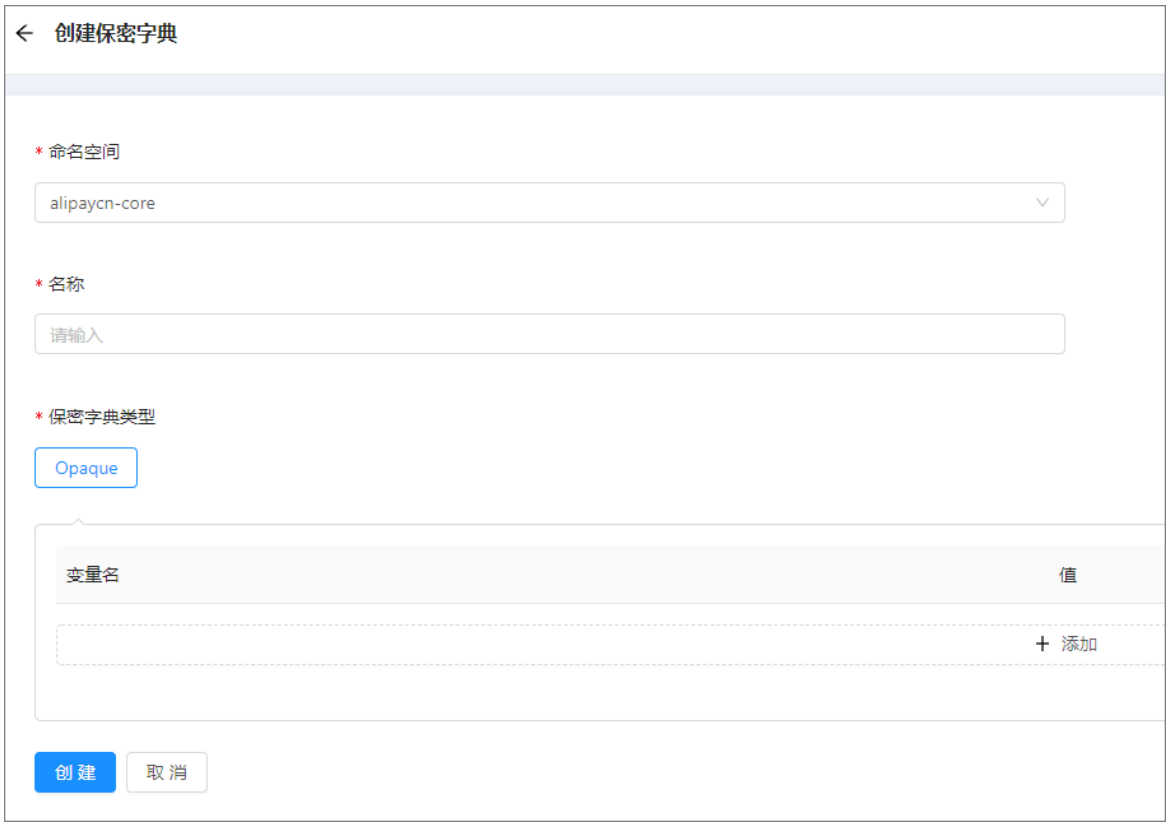
保密字典（Secret）用于存储工作负载所需要认证信息、密钥的敏感信息等。本文介绍如何创建保密字典。

前提条件

已创建命名空间。具体步骤请参见 创建命名空间。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **保密字典（Secrets）**。
4. 在 **保密字典（Secrets）** 页面单击 **创建**。
5. 在 **创建保密字典** 页面配置以下参数：



参数	是否必须	说明
命名空间	是	选择创建保密字典的命名空间。
名称	是	输入保密字典名称。
保密字典类型	是	单击 **添加**，输入 **变量名** 和 **值**。 Opaque 为一般密钥类型，值必须使用 Base64 编码。

6. 单击 **创建**。

   创建的保密字典可以在 Pod 中使用。在 Pod 里使用保密字典时，两者需处于同一命名空间中。

4.7.2.2. 管理保密字典

对于已创建的保密字典，您可以通过 Captain 控制台进行编辑。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **保密字典（Secrets）**。
4. 在 **保密字典（Secrets）** 页面的 **命名空间** 下拉列表选择目标保密字典所在命名空间。
5. 单击目标保密字典名称，然后在 **保密字典详情** 页面管理保密字典，操作如下：
   - 增加保密字典变量
     a. 单击 **添加保密字典数据**，然后输入保密字典的 **变量名** 和 **值**。
     b. 单击 **提交**。
   - 修改保密字典变量
     a. 单击目标变量右侧 **编辑**，修改 **变量名** 或变量 **值**。
     b. 单击 **提交**。
   - 删除保密字典变量

     单击目标变量右侧 **删除**，然后单击 **确定**。

4.7.2.3. 删除保密字典

您可以通过 Captain 控制台删除不再需要的保密字典。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 选择 **配置管理** > **保密字典（Secrets）**。

4. 在 **保密字典（Secrets）** 页面的 **命名空间** 下拉列表选择目标保密字典所在命名空间。
5. 单击目标保密字典右侧的 **删除**。
6. 单击 **确认**。

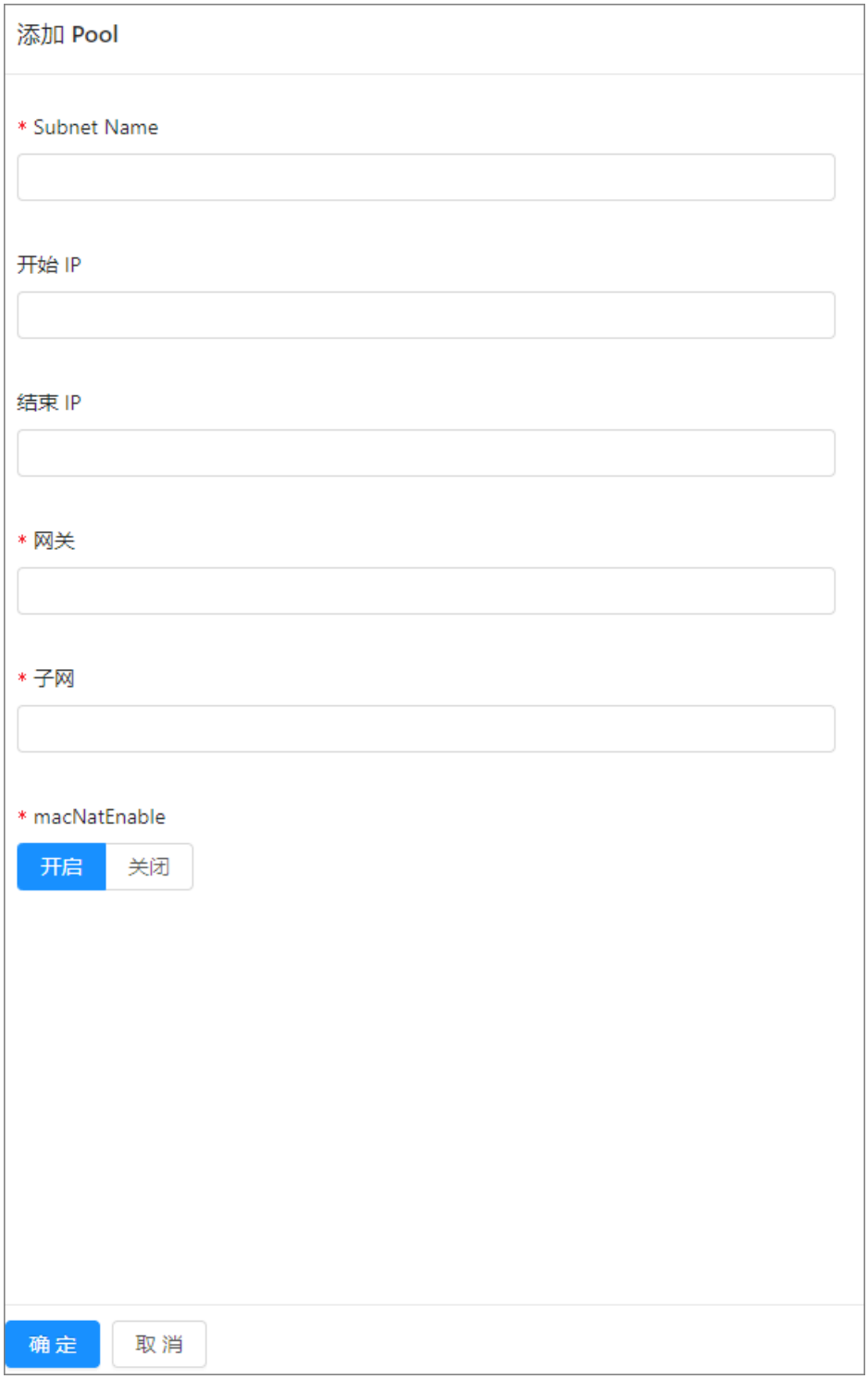
4.8. 网络

4.8.1. 创建网络

集群创建后，您需要为集群创建网络。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **网络**，然后单击 **创建网络**。
4. 输入网络名称、网络模式和 netID，然后单击 **确定**。
5. 单击 **网络池** 页签，然后单击 **添加 Pool**。
6. 在 **添加 Pool** 面板配置以下参数：



参数	是否必须	说明
Subnet Name	是	输入子网名称。
开始 IP	否	输入地址池开始 IP。

参数	是否必须	说明
结束 IP	否	输入地址池结束 IP。
网关	是	输入子网网关。
子网	是	输入子网的网络地址，使用 CIDR 格式。例如：`10.0.0.0/24`。
macNatEnable	是	选择是否开启 macNatEnable。

7. 单击 **确定**。

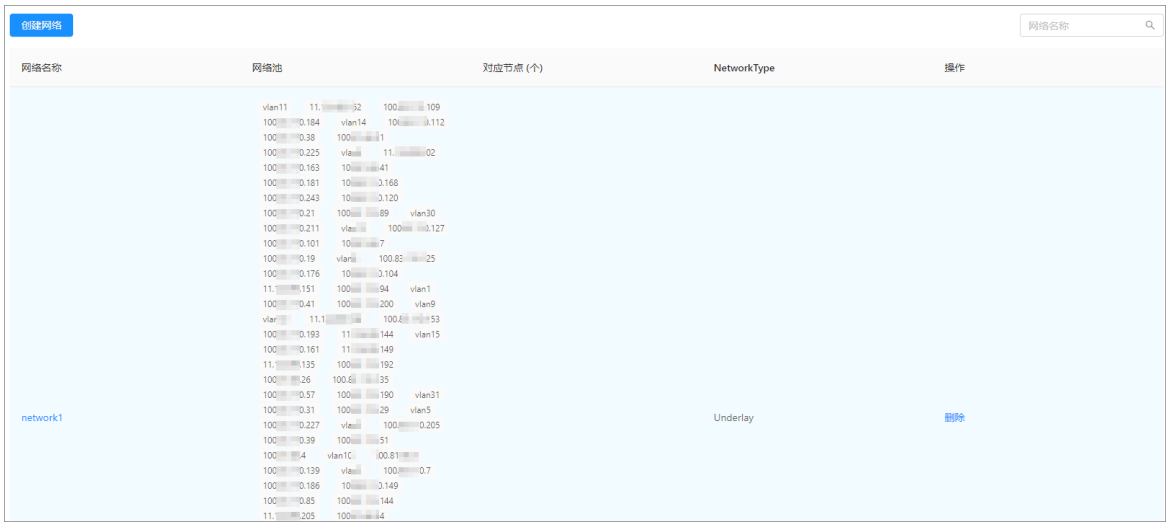
4.8.2. 查看网络详情

您可以通过 Captain 控制台查看已创建的网络详细信息。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **网络**。

   您可以在 **网络列表** 页面查看集群网络的概览信息，包括网络名称、网络池、对应节点等信息。



4. 单击目标网络名称查看目标网络的详细信息。

您可以查看网络的基本信息、网络池的详细信息和对应节点信息。

4.8.3. 删除网络

您可以通过 Captain 控制台删除不再需要的网络。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **网络**。
4. 在 **网络列表** 页面单击目标网络名称。
5. 单击 **网络池** 页签，然后删除所有子网。
6. 回到 **网络列表** 页面，然后单击目标网络名称右侧的 **删除**。
7. 单击 **确定**。

4.9. 查看运维单

运维单展示在执行解决方案的过程中产生的所有运维操作，方便您进行运维任务的快速查看和追踪。

操作步骤

1. 登录 Captain 控制台。
2. 在左侧导航栏单击 **集群管理**，然后单击目标集群。
3. 单击 **运维单**。
4. 在 **运维单列表** 页面查看运维单概览。

   您可以查看截止当前已产生的所有运维单概览信息，包括运维单 ID、名称、状态、创建时间、更新时间等信息。

5. 单击目标运维单 ID。

您可以查看到运维单的基本信息和运维单详细的执行结果。对于失败的运维操作，可以选择重试或忽略。

4.10. 附录：基础术语

本文介绍容器底座涉及的基础术语。

Ant Financial Kubernetes Engine（AKE）

AKE（Ant Financial Kubernetes Engine）是蚂蚁在开源 Kubernetes 和 Docker 基础上自研的容器云平台，通过蚂蚁自研组件进行了能力增强。对外提供统一的计算、存储、网络资源抽象、屏蔽物理机和虚拟机等各种环境的差异。

Captain Plus

云应用引擎基础版的控制台，通过可视化界面满足日常运维需求。

OVERLAY 网络

采用软件定义的一层虚拟化网络，提供了更高定制化的网络，更为灵活可配，可显著降低对二层网络地址的损耗，缺点是网络性能有一定的损失。

VLAN 网络

VLAN 网络为每个容器提供一个或多个独立 IP，用于二三层可达的网路访问，比较适合传统运维模式。VLAN 的网段配置，包含子网、网关和 VLAN ID，如果有可用 IP 限制需配置 IP 范围。对于物理 VLAN 网络场景，如果交付的多个 VLAN 网段配置在不同交换机上，还必须提供交换机、网络、物理机列表的映射关系。

部署（Deployment）

Kubernetes 的原生概念，表示无状态的应用集合。

保密字典（Secret）

Kubernetes 的原生概念，用于存储用户的加密内容。

调度器

AKE 在社区 CPU manager 之上增强的调度，可提供共享、独占，以及共享绑核的能力。

工作负载（Workload）

工作负载指应用程序运行态的载体及其上层聚合，通常包括部署（Deployments）、有状态副本集（StatefulSet）、守护进程集（DaemonSet）、任务（Jobs）、容器组（Pods）。

任务（Jobs）

Kubernetes 的原生概念，表示一次性执行的任务。

容器组（Pods）

Kubernetes 的原生概念，表示一个应用容器。

守护进程集（DaemonSet）

Kubernetes 的原生概念，表示运行在所有节点上的守护应用。

集群（Cluster）

集群将多台机器的资源整合起来，统一调度，统一管理，是承载部署应用的载体。

节点（Node）

节点指用于部署和管理容器的服务器（可以是虚拟机实例或者物理服务器），该服务器会被注册到集群中，为集群提供相应的计算，网络，存储资源。

镜像（Image）

镜像是应用包，将配置和相关软件等打在一起的二进制包，并且符合 Docker Image 规范。

命名空间（Namespace）

命名空间为 Kubernetes 集群提供虚拟的隔离作用。Kubernetes 集群初始有 3 个命名空间，分别是默认命名空间 default、系统命名空间 kube-system 和 kube-public，除此以外，管理员可以创建新的命名空间以满足需求。

网络（Network）

定义了集群中应用容器互相访问的网络配置。

网络控制器

AKE 中用来实现网络能力的控制，可以提供网络分配调度，和网络插件一起配合可以满足网络隔离需求。

网络、存储、日志、监控插件

运行于节点之上的，提供相应网络、存储、日志等功能的插件。

业务集群

基于元集群上创建出的业务集群，通过 cluster 控制器管理生命周期，业务集群的控制容器运行在元集群中，被元集群管控。

有状态副本集（StatefulSet）

Kubernetes 的原生概念，表示有状态的应用集。

元集群

在一个网络环境内的第一个集群，通过 static pod 部署控制组件。

云游（Yunyou）

云游是一个 Web 应用，主要提供的功能包括产品发布和管理、权限管理等。