容器镜像服务

用户指南

文档版本 01

发布日期 2023-05-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

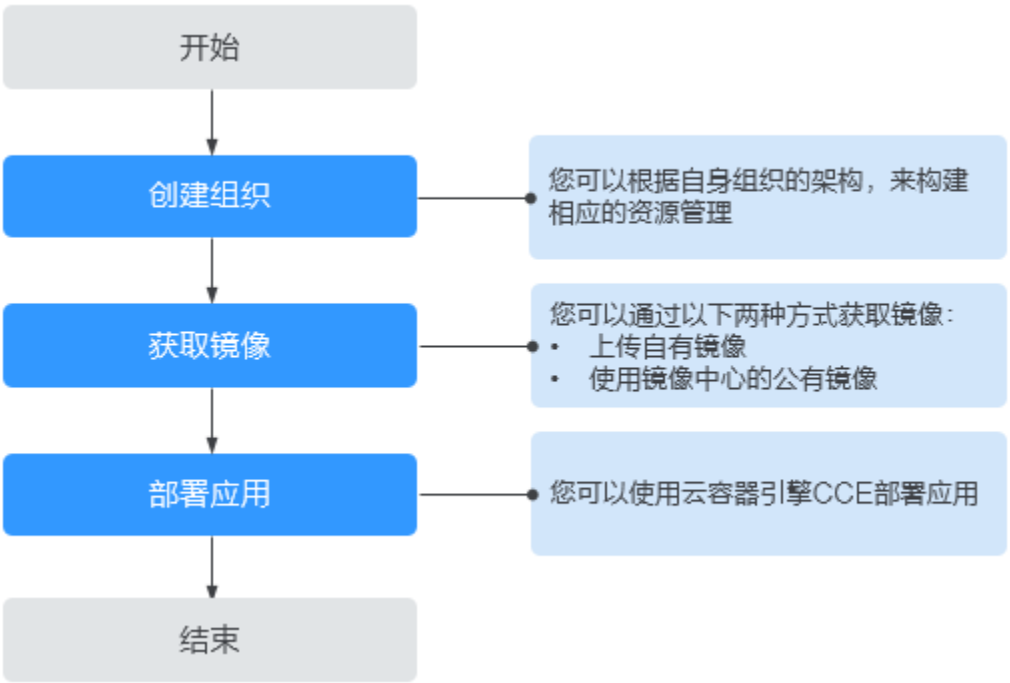
1 欢迎使用容器镜像服务

容器镜像服务（SoftWare Repository for Container，简称SWR）是一种支持镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，包括镜像的上传、下载、删除等。

SWR提供私有镜像库，并支持细粒度的权限管理，可以为不同用户分配相应的访问权限（读取、编辑、管理）。SWR还支持容器镜像版本更新自动触发部署。您只需要为镜像设置一个触发器，通过触发器，可以在每次镜像版本更新时，自动更新云容器引擎（CCE）中使用该镜像部署的应用。

您可以通过**控制台**、**API**使用容器镜像服务。

图 1-1 SWR 使用流程



2 权限管理

2.1 创建用户并授权使用 SWR

如果您需要对您所拥有的容器镜像服务（SWR）进行角色与策略的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用SWR资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将SWR资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用SWR服务的其他功能。

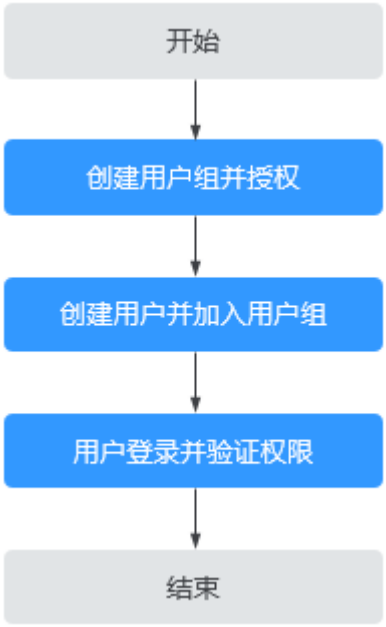
本章节为您介绍对用户授权的方法，操作流程如下图给用户授予SWR权限流程所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的SWR权限，并结合实际需求进行选择，SWR支持的系统权限，请参见：**角色与策略权限管理**。若您需要对除SWR之外的其他服务授权，IAM支持服务的所有权限请参见**授权参考**。

示例流程

图 2-1 给用户授予 SWR 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予容器镜像服务的管理员权限“SWR Administrator”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限（如果能顺利完成如下操作，说明权限设置成功）：

   a. 在“服务列表”中选择容器镜像服务，进入SWR主界面。

   b. 在左侧导航栏选择“组织管理”，单击右上角“创建组织”，输入组织名称，能够成功创建组织。

   c. 在左侧导航栏选择“我的镜像”，单击右上角“页面上传”，选择上一步创建的组织，以及一个本地的镜像文件，能够成功上传镜像。

3 容器引擎基础知识

容器引擎（Docker）是一个开源的引擎，可以轻松的为任何应用创建一个轻量级的、可移植的、自给自足的容器。

安装前的准备工作

在安装容器引擎前，请了解容器引擎的基础知识，具体请参见**Docker Documentation**。

选择容器引擎的版本

容器引擎几乎支持在所有操作系统上安装，用户可以根据需要选择要安装的容器引擎版本，具体请参见**https://docs.docker.com/engine/install/**。

说明

- 由于SWR支持容器引擎1.11.2及以上版本上传镜像，建议下载对应版本。
- 安装容器引擎需要连接互联网，内网服务器需要绑定弹性公网IP后才能访问。

安装容器引擎

你可以根据自己的操作系统选择对应的安装步骤：

Linux操作系统下安装

EulerOS操作系统下安装

- **Linux操作系统下安装**

  在Linux操作系统下，可以使用如下命令快速安装Docker的最新稳定版本。如果您想安装其他特定版本的Docker，可参考**安装Docker**。

  ```
  curl -fsSL get.docker.com -o get-docker.sh
  sh get-docker.sh
  sudo systemctl daemon-reload
  sudo systemctl restart docker
  ```

- **EulerOS操作系统下安装**

  在EulerOS操作系统下，安装容器引擎的方法如下：

  a. 登录弹性云服务器。

  b. 配置yum源。

如果您的机器上还没有配置yum源，可以参照如下方法配置：**如何使用自动化工具配置华为云镜像源(x86_64和ARM)?** 如果已配置，可跳过该步骤。

c. 安装并运行容器引擎。

i. 获取yum源里的docker-engine包。

yum search docker-engine

ii. 使用**yum install -y**命令安装上一步获取的docker-engine包，x86架构示例：

yum install docker-engine.x86_64 -y

iii. 设置开机启动Docker服务。

systemctl enable docker

iv. 启动Docker。

systemctl start docker

d. 检查安装结果。

docker --version

回显如下类似信息，表示容器引擎安装成功。

```
Docker version 18.09.0, build 384e3e9
```

制作容器镜像

本节指导您通过Dockerfile定制一个简单的Web应用程序的容器镜像。Dockerfile是一个文本文件，其内包含了一条条的指令（Instruction），每一条指令构建一层，因此每一条指令的内容，就是描述该层应当如何构建。

使用Nginx镜像创建容器应用，在浏览器访问时则会看到默认的Nginx欢迎页面，本节以Nginx镜像为例，修改Nginx镜像的欢迎页面，定制一个新的镜像，将欢迎页面改为“Hello, SWR!”。

步骤1 以root用户登录容器引擎所在机器。

步骤2 创建一个名为Dockerfile的文件。

mkdir mynginx

cd mynginx

touch Dockerfile

步骤3 编辑Dockerfile。

vim Dockerfile

增加文件内容如下：

```
FROM nginx
RUN echo '<h1>Hello, SWR!</h1>' > /usr/share/nginx/html/index.html
```

Dockerfile指令介绍如下。

- FROM语句：表示使用nginx镜像作为基础镜像，一个Dockerfile中FROM是必备的指令，并且必须是第一条指令。
- RUN语句：格式为RUN <命令>，表示执行echo命令，在显示器中显示一段“Hello, SWR!”的文字。

按“Esc”，输入**:wq**，保存并退出。

步骤4 使用**docker build** [*选项*] <*上下文路径*> 构建镜像。

docker build -t nginx:v1 .

- -t nginx:v1：指定镜像的名称和版本。
- **.**：指定Dockerfile所在目录，镜像构建命令将该路径下所有的内容打包给容器引擎帮助构建镜像。

步骤5 执行以下命令，可查看到已成功部署的nginx镜像，版本为v1。

docker images

----结束

制作镜像压缩包

本节指导您将容器镜像制作成tar或tar.gz文件压缩包。

步骤1 以root用户登录容器引擎所在机器。

步骤2 执行如下命令查看镜像。

docker images

查看需要导出的镜像及tag。

步骤3 执行如下命令制作镜像压缩包。

docker save [OPTIONS] IMAGE [IMAGE...]

说明

OPTIONS：--output或-o，表示导出到文件。

压缩包格式为：.tar或.tar.gz。

使用docker save制作镜像压缩包时，请用{image}:{tag}，不要用image id，否则无法在swr页面上传。

示例：

```
$ docker save nginx:latest > nginx.tar
$ ls -sh nginx.tar
108M nginx.tar

$ docker save php:5-apache > php.tar.gz
$ ls -sh php.tar.gz
372M php.tar.gz

$ docker save --output nginx.tar nginx
$ ls -sh nginx.tar
108M nginx.tar

$ docker save -o nginx-all.tar nginx    # 将nginx所有版本打包
$ docker save -o nginx-latest.tar nginx:latest
```

----结束

导入镜像文件

本章节将指导你通过docker load命令将镜像压缩包导入为一个镜像。

执行方式有2种：

docker load < 路径/文件名.tar

docker load --input或者-i 路径/文件名.tar

示例：

```
$ docker load --input fedora.tar
```


4 镜像管理

4.1 客户端上传镜像（推荐）

操作场景

客户端上传镜像，是指在安装了容器引擎客户端的机器上使用docker命令将镜像上传到容器镜像服务的镜像仓库。

如果容器引擎客户端机器为云上的ECS或CCE节点，根据机器所在区域有两种网络链路可以选择：

- 若机器与容器镜像仓库在同一区域，则上传镜像走内网链路。
- 若机器与容器镜像仓库不在同一区域，则上传镜像走公网链路，机器需要绑定弹性公网IP。

约束与限制

- 使用客户端上传镜像，镜像的每个layer大小不能超过10G。
- 上传镜像的容器引擎客户端版本必须为1.11.2及以上。

前提条件

已创建组织，请参见**创建组织**。

操作步骤

步骤1 **制作容器镜像**或**导入镜像文件**。

步骤2 连接容器镜像服务。

1. 登录**容器镜像服务控制台**。
2. 选择左侧导航栏的“总览”，单击页面右上角的“登录指令”，在弹出的页面中单击 复制登录指令。

图 4-1 登录指令

说明

- 此处生成的登录指令有效期为6小时，若需要长期有效的登录指令，请参见**获取长期有效登录指令**。获取了长期有效的登录指令后，在有效期内的临时登录指令仍然可以使用。
- 登录指令末尾的域名为镜像仓库地址，请记录该地址，后面会使用到。

3. 在安装容器引擎的机器中执行上一步复制的登录指令。
   登录成功会显示“Login Succeeded”。

步骤3 在安装容器引擎的机器上执行如下命令，为**nginx**镜像打标签。

docker tag [镜像名称1:版本名称1] [镜像仓库地址]/[组织名称]/[镜像名称2:版本名称2]

其中，

- [镜像名称1:版本名称1]：请替换为您所要上传的实际镜像的名称和版本名称。
- [镜像仓库地址]：可在SWR控制台上查询，即**步骤2.2**中登录指令末尾的域名。
- [组织名称]：请替换为您创建的组织。
- [镜像名称2:版本名称2]：请替换为您期待的镜像名称和镜像版本。

示例：

docker tag nginx:v1 swr.cn-east-3.myhuaweicloud.com/cloud-develop/nginx:v1

步骤4 上传镜像至镜像仓库。

docker push [镜像仓库地址]/[组织名称]/[镜像名称2:版本名称2]

示例：

docker push swr.cn-east-3.myhuaweicloud.com/cloud-develop/nginx:v1

终端显示如下信息，表明上传镜像成功。

```
The push refers to repository [swr.cn-east-3.myhuaweicloud.com/cloud-develop/nginx:v1]
fbce26647e70: Pushed
fb04ab8effa8: Pushed
8f736d52032f: Pushed
009f1d338b57: Pushed
678bbd796838: Pushed
d1279c519351: Pushed
```



```
f68ef921efae: Pushed
v1: digest: sha256:0cdfc7910db531bfa7726de4c19ec556bc9190aad9bd3de93787e8bce3385f8d size: 1780
```

返回容器镜像服务控制台，在“我的镜像”页面，执行刷新操作后可查看到对应的镜像信息。

----结束

常见问题

为什么使用客户端上传镜像失败?

4.2 获取长期有效登录指令

操作场景

本章节介绍如何获取长期有效的登录指令，长期有效登录指令的有效期为永久。

说明

- 为保证安全，获取登录指令过程建议在开发环境执行。
- 用户登录IAM控制台前，请确保已具有IAM服务访问权限，授权方式请参考**创建用户组并授权**。

操作流程

您可以按照以下流程获取长期有效登录指令。

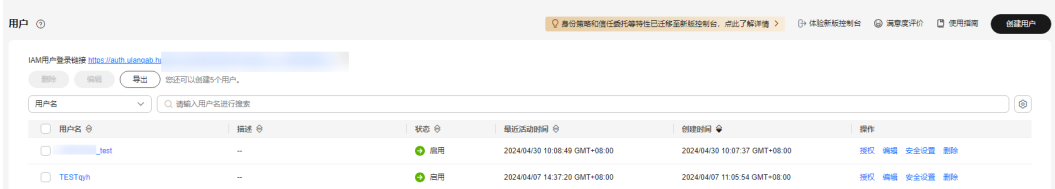
图 4-2 流程示意图

操作步骤

步骤1 获取编程访问权限。(如果当前用户已有编程访问权限，请忽略此步骤)

1. 以管理员身份，登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 单击左侧导航栏，选择“管理与监管”>“统一身份认证服务IAM”。
4. 在“用户”页搜索框输入并搜索要授予编程访问权限的用户名称。

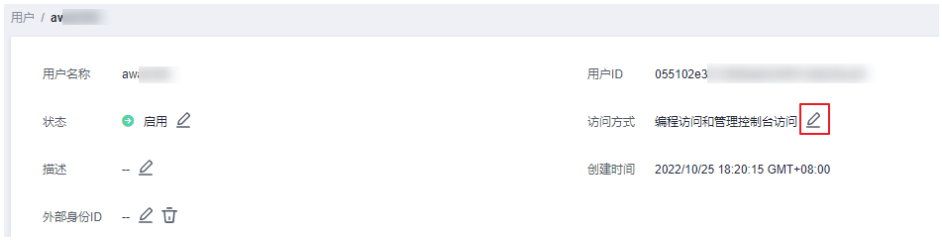
图 4-3 用户列表



5. 单击用户名称，进入用户详情页。

6. 单击“访问方式”后面的按钮。

图 4-4 修改访问方式



7. 勾选“编程访问”选项。（可单独勾选编程访问，也可以2种访问方式同时勾选。）

图 4-5 修改访问方式

步骤2 获取区域项目名称、镜像仓库地址。

1. 登录IAM管理控制台。
2. 将鼠标移至页面右上角用户名称上。

图 4-6 IAM 首页

3. 在下拉菜单中，单击“我的凭证”。
4. 在项目列表中找到您的虚拟机的所属区域及项目：

图 4-7 区域与项目

5. 您可以按照获取到的项目信息拼接镜像仓库地址，拼接方式为：swr.区域项目名称.myhuaweicloud.com
   *如用户a*****虚拟机所在区域为华北-北京四，那么对应的镜像仓库地址为：swr.cn-north-4.myhuaweicloud.com。*

步骤3 获取AK/SK访问密钥。

说明

访问密钥即AK/SK（Access Key ID/Secret Access Key），表示一组密钥对，用于验证调用API发起请求的访问者身份，与密码的功能相似。如果您已有AK/SK，可以直接使用，无需再次获取。

1. 登录IAM管理控制台，将鼠标移到用户名处，单击“我的凭证”。
2. 在左侧导航栏中选择“访问密钥”，单击“新增访问密钥”。
3. 输入描述信息，单击“确定”。
4. 在弹出的提示页面单击“立即下载”。
   下载成功后，在“credentials”文件中即可获取AK和SK信息。

表 4-1 *credentials 文件示例*

User Name	*Access Key Id*	*Secret Access Key*
*a****	*RVHVMX*******	*H3nPwzgZ*******

说明

为防止访问密钥泄露，建议您将其保存到安全的位置。

步骤4 登录一台Linux系统的计算机，执行如下命令获取登录密钥。

printf "AK" | openssl dgst -binary -sha256 -hmac "SK" | od -An -vtx1 | sed 's/[\n]//g' | sed 'N;s/\n//'

请将**AK**替换为**步骤3***credentials文件*的*Access Key Id*，**SK**替换为**步骤3***credentials文件*的*Secret Access Key*。

示例：

```
printf "RVHVMX******" | openssl dgst -binary -sha256 -hmac "H3nPwzgZ******" | od -An -vtx1 | sed 's/[ \n]//g' | sed 'N;s/\n//'
```

执行上面的命令后，我们得到的登录密钥如下：

```
cab4ceab4a1545***************
```

说明

以上密钥仅为示例，请以实际获得的密钥为准。

步骤5 使用如下的格式拼接登录指令。

docker login -u [区域项目名称]@[AK] **-p** [登录密钥] [镜像仓库地址]

其中，区域项目名称和镜像仓库地址在**步骤2**中获取，AK在**步骤3**中获取，登录密钥为**步骤4**的执行结果。

示例：


```
docker login -u cn-north-4@RVHVMX****** -p cab4ceab4a1545********** swr.cn-north-4.myhuaweicloud.com
```

当显示“Login Succeeded”，即为登录成功。

说明

- 登录密钥字符串是经过加密的，无法逆向解密，从-p无法获取到SK。
- 获取的登录指令可在其他机器上使用并登录。

步骤6 （可选）当您退出仓库时，请使用以下命令删除您的认证信息。

```
cd /root/.docker/
rm -f config.json
```

步骤7 （可选）使用history -c命令清理相关使用痕迹，避免隐私信息泄露。

----结束

4.3 页面上传镜像

操作场景

本章节介绍如何通过页面上传镜像。从页面上传镜像，是指直接通过控制台页面将镜像上传到容器镜像服务的镜像仓库。

约束与限制

- 每次最多上传10个文件，单个文件大小（含解压后）不得超过2G。
- 仅支持上传1.11.2及以上容器引擎客户端版本制作的镜像压缩包。

前提条件

- 已创建组织，请参见**创建组织**。
- 镜像已保存为tar或tar.gz文件，具体请参见**制作镜像压缩包**。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右上角“页面上传”。

步骤3 在弹出的窗口中选择组织，单击“选择镜像文件”，选择要上传的镜像文件。

说明

多个镜像同时上传时，镜像文件会按照顺序逐个上传，不支持并发上传。

图 4-8 上传镜像

步骤4 单击“开始上传”。

待任务进度显示“上传完成”，表示镜像上传成功。

----结束

常见问题

[为什么通过页面上传镜像失败?]

4.4 下载镜像

操作场景

您可以使用docker pull命令下载容器镜像服务中的镜像。

前提条件

- 在下载镜像前，请确保您的网络畅通。详细网络配置步骤请参考**配置访问网络**。
- 在下载镜像前，请联系管理员在IAM控制台授权容器镜像服务下载权限，详情请参考**权限管理**。
- “我的镜像”展示当前用户所有的自有镜像（该用户所在组织所拥有的镜像）和共享镜像（该组织下其他用户共享的私有镜像）。
- IAM用户创建后，需要管理员在组织中为您添加授权，您才具有该组织内镜像的读取、编辑等权限。详情请参考**授权管理**。

下载“我的镜像”

步骤1 以root用户登录容器引擎所在的虚拟机。

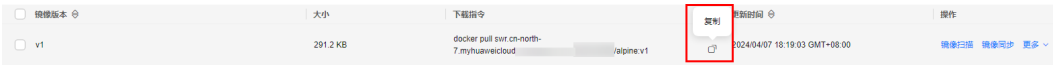
步骤2 参考**步骤2**获取登录访问权限，连接容器镜像服务。

步骤3 登录**容器镜像服务控制台**。

步骤4 在左侧导航栏选择“我的镜像”，单击右侧镜像名称。

步骤5 在镜像详情页面中，单击对应镜像版本“下载指令”列的复制图标，复制镜像下载指令。

图 4-9 获取镜像下载指令



步骤6 在虚拟机中执行**步骤5**复制的镜像下载指令。

示例：**docker pull swr.cn-east-3.myhuaweicloud.com/group/nginx:v2.0.0**

使用**docker images**命令查看是否下载成功。

```
# docker images
REPOSITORY                                                TAG       IMAGE ID       CREATED         SIZE
swr.cn-east-3.myhuaweicloud.com/group/nginx               v2.0.0    22f2bf2e2b4f   5 hours ago     22.8MB
```

步骤7 （可选）执行如下命令将镜像保存为归档文件。

docker save [镜像名称:版本名称] > [归档文件名称]

示例：**docker save swr.cn-east-3.myhuaweicloud.com/group/nginx:v2.0.0 > nginx.tar**

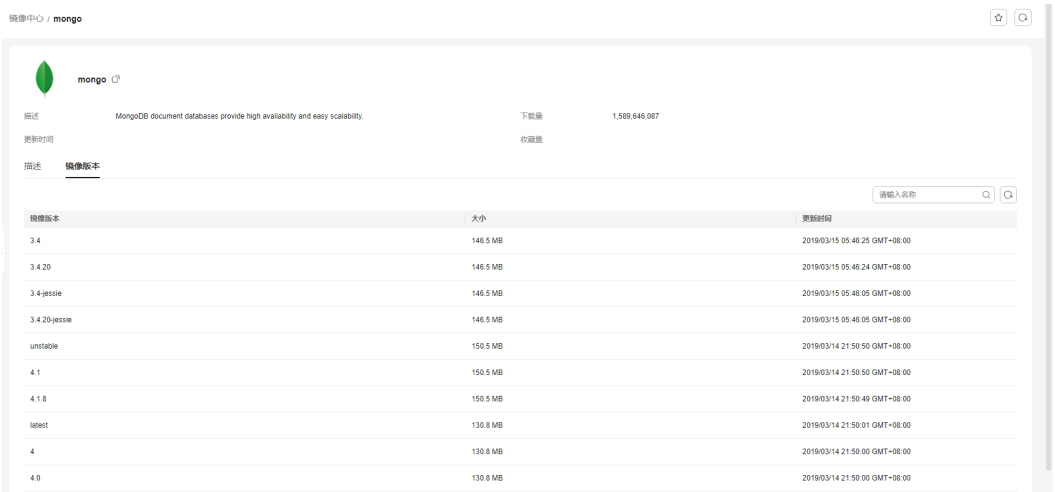
----结束

下载镜像中心的镜像

镜像中心的镜像可直接下载，无需添加仓库地址。如**图4-10**所示的mongo镜像，只需**容器引擎所在虚拟机连接SWR**，且执行如下命令即可将其下载。

docker pull mongo:*4.1*

图 4-10 mongo 镜像详情示例



4.5 编辑镜像属性

操作场景

镜像上传后默认为私有镜像，您可以设置镜像的属性，包括镜像的类型（“公开”或“私有”）、分类及描述。

公开镜像所有用户都能下载，私有镜像则受具体权限管理控制。您可以为用户添加授权，授权完成后，用户享有读取、编辑或管理私有镜像的权限，具体请参见**在镜像详情中添加授权**。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧菜单栏选择“我的镜像”，单击右侧要编辑镜像的名称。

步骤3 在镜像详情页面，单击右上角“编辑”，在弹出的窗口中根据需要编辑类型（“公开”或“私有”）、分类及描述，然后单击“确定”。

图 4-11 编辑镜像属性

表 4-2 编辑镜像

参数	说明
所属组织	镜像所属组织。

参数	说明
镜像名称	镜像名称。
类型	镜像类型，可选择： ● 公开 ● 私有 **说明** 公开镜像所有用户都可以下载使用。 ● 如果您的机器与镜像仓库在同一区域，访问仓库是通过内网访问。 ● 如果您的机器与镜像仓库在不同区域，通过公网才能访问仓库，下载跨区域仓库的镜像需要机器可以访问公网。
类别	镜像分类，可选择： ● 应用服务器 ● Linux ● Arm ● 框架与应用 ● 数据库 ● 语言 ● 其他
描述	输入镜像仓库描述，0-30000个字符。

----结束

4.6 共享私有镜像

操作场景

镜像上传后，您可以共享**私有镜像**给其他账号，并授予下载该镜像的权限。

被共享的用户需要登录**容器镜像服务控制台**，在“我的镜像 > 他人共享”页面查看共享的镜像。被共享的用户单击镜像名称，可进入镜像详情页面查看镜像版本、下载指令等。

约束与限制

- 镜像共享功能只支持私有镜像进行共享，不支持公有镜像共享。
- 仅具备该私有镜像管理权限的IAM用户才能共享镜像，被共享者只有只读权限，只能下载镜像。
- 镜像共享功能只能在同一区域内使用，不支持在不同区域间镜像共享。
- 一个私有镜像最多可以共享给500个租户。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧镜像的名称。

步骤3 在镜像详情页面选择“共享”页签。

步骤4 单击“共享镜像”，根据**表4-3**填写相关参数，然后单击“确定”。

图 4-12 共享镜像

表 4-3 共享镜像

参数	说明
使用者类型	账号名、账号ID或者组织。
使用者ID	输入账号ID。
截止日期	选择共享截止日期。如勾选“永久有效”，则共享永久有效。
权限	当前仅支持“下载”权限。
描述	输入描述，0-1000个字符。

步骤5 共享完成后，您可以在“我的镜像 > 自有镜像”中，勾选“我共享的镜像”，查看所有共享的镜像。

----结束

4.7 添加触发器

操作场景

容器镜像服务可搭配云容器引擎CCE、云容器实例CCI一起使用，实现镜像版本更新时自动更新使用该镜像的应用。您只需要为镜像添加一个触发器，通过触发器，可以在每次生成新的镜像版本时，自动执行更新动作，如：自动更新使用该镜像的应用。

说明

目前仅“华北-北京四”区域同时支持添加CCE和CCI类型的触发器，其他区域仅支持添加CCE类型的触发器。

前提条件

更新应用镜像版本之前，请确保已创建容器应用，将镜像部署到云容器引擎CCE或云容器实例CCI。

如未创建，请登录云容器引擎工作负载页面进行创建，具体创建方法请参见**创建无状态负载（Deployment）**或**创建有状态负载（StatefulSet）**，或登录云容器实例无状态负载页面进行创建，具体创建方法请参见**创建无状态负载**。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧镜像名称，进入镜像详情页。

步骤3 选择“触发器”页签，单击“添加触发器”，根据**表4-4**填写相关参数，然后单击“确定”。

图 4-13 *添加触发器*

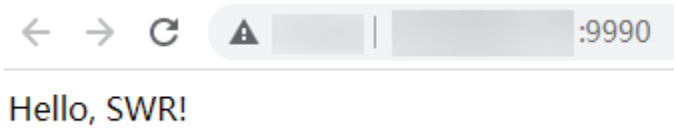
表 4-4 触发器

参数	说明
触发器名称	自定义触发器的名称。 字母开头，由字母、数字、下划线_、中划线-组成，下划线、中划线不能连续且不能作为结尾，1-64个字符。
触发条件	支持如下三种触发条件，当镜像有新版本时，触发部署应用。 • 全部触发：有新的镜像版本生成或镜像版本号不变，镜像内容发生变化重新推送时，触发部署。 • 指定版本号触发：有指定镜像版本生成或更新时，触发部署。 • 正则触发：有符合正则表达式的镜像版本生成或更新时，触发部署。正则表达式规则如下： – *****：匹配不包含路径分隔符“/”的任何字段。 – ******：匹配包含路径分隔符“/”的任何字段。 – **?**：匹配任何单个非“/”的字符。 – **{选项1, 选项2, ...}**：同时匹配多个选项。
触发动作	当前仅支持更新容器的镜像，需指定更新的应用，以及该应用下的容器。
触发器状态	选择“启用”。
触发器类型	选择“云容器引擎CCE”或“云容器实例CCI”。 **说明** 当前仅“华北-北京四”区域支持“云容器实例CCI”的触发器类型。
选择应用	选择要更新镜像的容器。

----结束

示例 1：触发条件为“全部触发”

假设有一个欢迎页面为“Hello, SWR!”的Nginx镜像（版本号为v1），使用该镜像创建了名称为“nginx”的无状态负载，该负载提供对外访问。



1. 为Nginx镜像添加触发器。
   触发器名称填写“All_tags”，触发条件选择“全部触发”，选择使用了Nginx镜像的无状态负载及容器。
2. Nginx镜像新增一个v2版本，该版本的欢迎页面为“Hello, SoftWare Repository for Container!”。

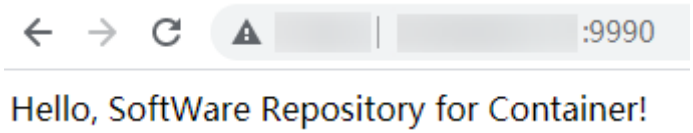
图 4-14 镜像版本 v2

3. 确认是否触发成功。

   在“触发器”页签，单击触发器对应的行的“触发历史”，查看触发结果为“成功”。

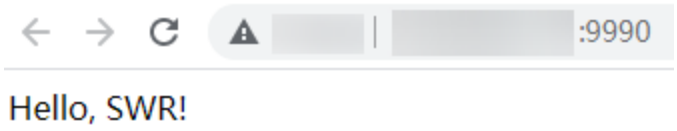
图 4-15 触发结果

工作负载的访问页面已变更为“Hello, SoftWare Repository for Container!”。



示例 2：触发条件为“正则触发”

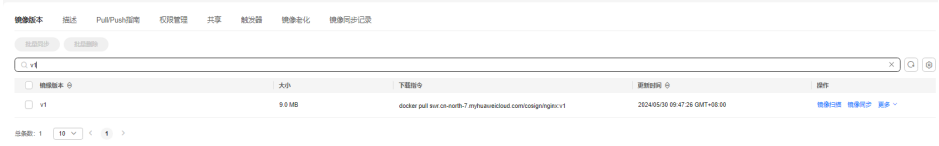
假设有一个欢迎页面为“Hello, SWR!”的Nginx镜像（版本号为v0），使用该镜像创建了名称为“nginx”的无状态负载，该负载提供对外访问。



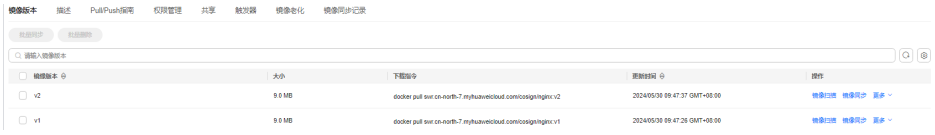
1. 为Nginx镜像添加触发器。

   触发器名称填写“Tags_regular_expression”，触发条件选择“正则触发”，输入正则表达式：^v2.*（匹配以v2开头的版本号），选择使用了Nginx镜像的无状态负载及容器。

2. Nginx镜像新增一个v1版本，该版本的欢迎页面为“Hello, SWR! (v1)”。



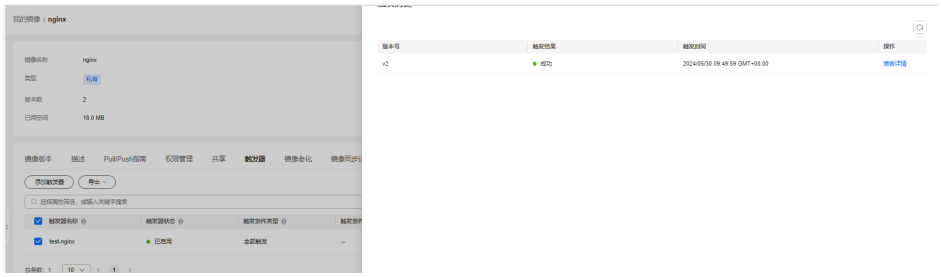
3. Nginx镜像新增一个v2版本，该版本的欢迎页面为“Hello, SWR! (v2)”。



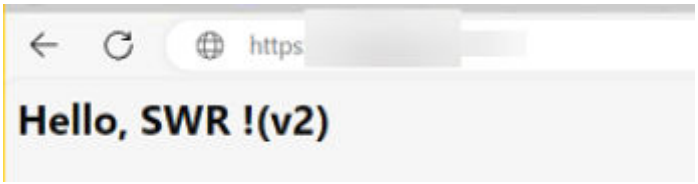
4. 确认是否触发成功。

   在“触发器”页签，单击 图标，查看触发结果。从图4-16中可以看出，只有v2版本被触发了，符合设置的正则表达式规则。

   图 4-16 触发结果示例



   工作负载的访问页面已变更为“Hello, SWR! (v2)”。



4.8 添加镜像老化规则

操作场景

镜像上传后，您可以添加镜像老化规则。容器镜像服务提供了如下两种类型的镜像老化处理规则，规则设置完成后，系统会根据已定义的规则自动执行镜像老化操作。

- 存活时间：设置该类型的老化规则后，留存时间超过指定时间的老旧镜像将被删除。
- 版本数目：设置该类型的老化规则后，留存镜像超过指定值时，老旧镜像将被删除。

此外，对于特定版本的镜像可通过添加过滤策略来保留，免受老化规则的影响。

约束与限制

一个镜像仅支持添加一个老化规则。如需添加新的老化规则，需要删除已有老化规则。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧镜像名称，进入镜像详情页。

步骤3 选择“镜像老化”页签，单击“添加规则”，根据**表4-5**填写相关参数，然后单击“确定”。

图 4-17 创建老化规则

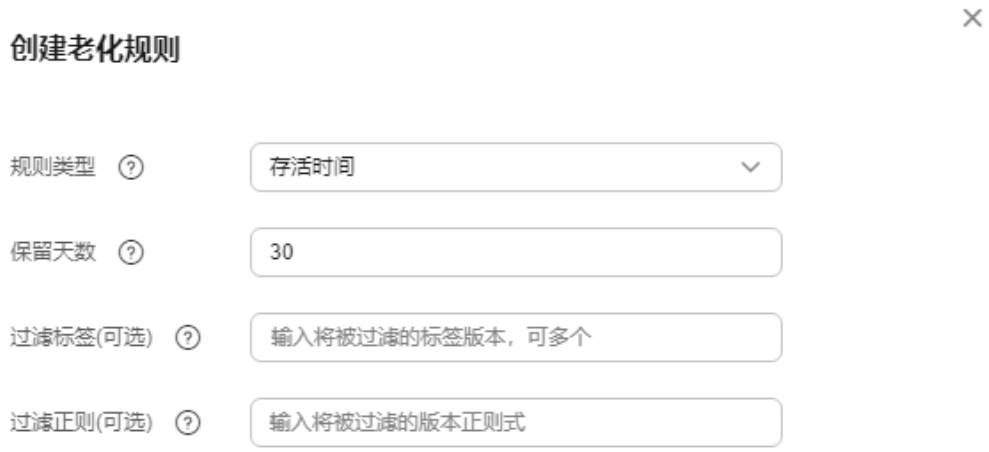


表 4-5 添加镜像老化规则

参数	说明
规则类型	分为存活时间和版本数目。 • 存活时间：设置该类型的老化规则后，留存时间超过指定时间的老旧镜像将被删除。 • 版本数目：设置该类型的老化规则后，留存镜像超过指定值时，老旧镜像将被删除。
保留天数	镜像留存的最大天数，可设置为1~365的整数。规则类型设置为“存活时间”时，需要配置此参数。
保留数目	镜像留存的最大数目，可设置为1~1000的整数。规则类型设置为“版本数目”时，需要配置此参数。
过滤标签	输入将被过滤的镜像版本，在应用老化规则前指定版本的镜像将被过滤掉。
过滤正则	输入将被过滤的版本正则式，在应用老化规则前所有版本号满足正则表达式的镜像将被过滤掉。

镜像老化规则添加成功后，系统会立即进行一次查询，清理掉符合老化规则的镜像，且在“老化日志”中显示清理结果。

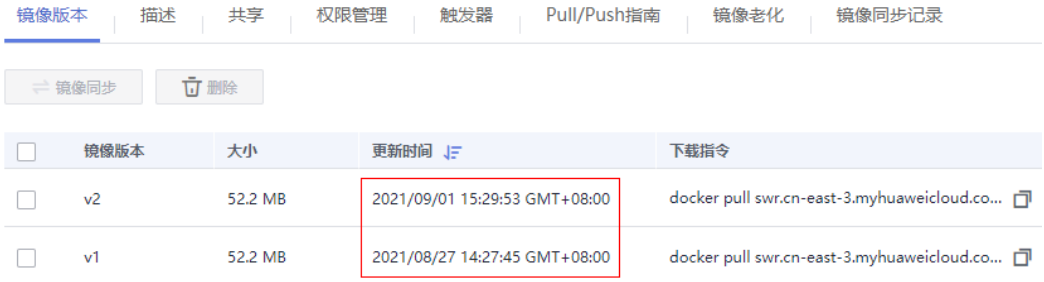
图 4-18 查看规则列表和老化日志

----结束

示例 1：规则类型为“存活时间”

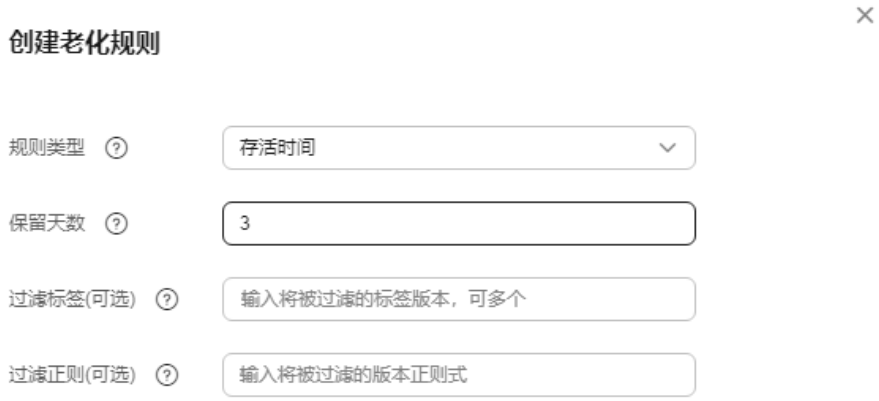
假设“nginx”镜像包含两个版本：v1和v2，更新时间如下图：

图 4-19 镜像版本



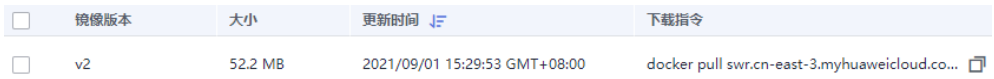
1. 添加老化规则。
   规则类型为“存活时间”，保留天数为“3”。

   图 4-20 创建老化规则示例

2. 确认规则是否生效。
   查看“老化日志”，v1版本的镜像留存时间超过3天（当前时间为2021/09/01 16:00:00），因此被自动清除。
   查看“镜像版本”，v1版本已被清除，只剩v2版本。

图 4-21 镜像版本 V2



以上现象说明老化规则已生效。

示例 2：规则类型为“版本数目”，且设置“过滤正则”

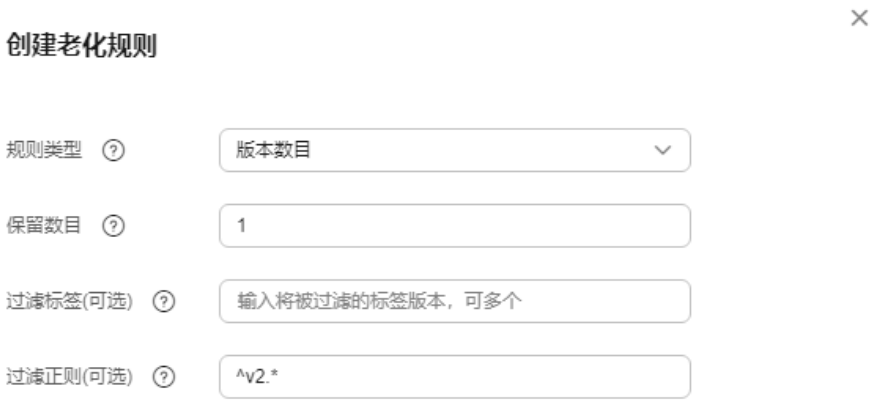
假设“nginx”镜像包含四个版本：v1、v2、v1.0.0、v2.0.0，如下图：

图 4-22 nginx 镜像版本

1. 添加老化规则。

   规则类型为“版本数目”，保留数目为“1”，过滤正则为：^v2.*（匹配以v2开头的版本号）。

   图 4-23 创建老化规则-版本数目

2. 确认规则是否生效。

   因为v2和v2.0.0版本匹配设置的正则表达式，在应用老化规则前会被过滤掉，v1和v1.0.0版本只会保留一个，v1更老旧，因此会被清除掉。

   查看“老化日志”和“镜像版本”，v1版本被清除，说明老化规则已生效。

图 4-24 镜像版本示例

这里给出几个过滤正则表达式以供参考：

- 匹配版本号为数字的版本：^[0-9]*$
- 匹配版本号长度为2-5的所有版本：^.{2,5}$
- 匹配由26个小写英文字母组成的版本号：^[a-z]+$
- 匹配版本号为英文和数字的版本：^[A-Za-z0-9]+$

注意

在写正则表达式"或"(“|”)的时候请加上括号，如果不加括号会导致老化删除掉该镜像下所有版本。

例如：镜像版本只需要保留包含a或者包含s的版本，此时正则表达式可写成：(.*a.*|.*s.*)。

4.9 自动同步镜像

操作场景

镜像上传后，您可以添加镜像自动同步功能，帮助您把最新推送的镜像自动同步到其他区域镜像仓库内。

说明

镜像自动同步帮助您把最新推送的镜像自动同步到其他区域镜像仓库内，后期镜像有更新时，目标仓库的镜像也会自动更新，但已有的镜像不会自动同步。

已有镜像的同步方法请参见**为什么已有镜像自动同步不成功？**。

约束与限制

- 仅账号及具有管理员权限的用户才能使用镜像自动同步功能。
- 目前仅支持“华北-北京一”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”、“华北-乌兰察布一”、“中国-香港”、“亚太-新加坡”、“亚太-曼谷”、“非洲-约翰内斯堡”区域。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧镜像名称。

步骤3 在镜像详情页面单击右上角“镜像自动同步”。

步骤4 单击 + 图标，选择目标区域和目标组织，然后单击“确定”完成添加。

图 4-25 添加镜像自动同步

- 目标区域：选择同步的目标区域，例如“华北-北京一”。
- 目标组织：选择同步的目标组织。
- 覆盖：

  勾选则表示覆盖，同步相同名称相同版本的镜像时，同步后会替换已有的镜像版本。

  不勾选则表示不覆盖，同步相同名称相同版本的镜像时，会取消同步并提示已存在相同版本镜像。

步骤5 在镜像详情页面的“镜像同步记录”页签下，可查看镜像同步启动时间、镜像版本、状态、同步类型、同步耗时等。

----结束

4.10 镜像安全扫描

操作场景

容器镜像服务为您提供了镜像安全扫描的功能，您只需要一键就可以对您的镜像进行安全扫描。容器镜像服务可扫描镜像仓库中的私有镜像，发现镜像中的漏洞并给出修复建议，帮助您得到一个安全的镜像。

约束与限制

目前仅支持“华北-北京一”区域。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧镜像名称，进入镜像详情页。

说明

在执行镜像安全扫描任务前，请确保“我的镜像”中已经有1个以上的私有镜像。如果您当前账户下没有私有镜像，请参考**客户端上传镜像**，上传一个镜像到您的镜像仓库中。

步骤3 在“镜像版本”页签，选择待操作的镜像版本并单击右侧的“镜像扫描”。

图 4-26 我的镜像

步骤4 单击“重新扫描”，触发镜像的安全扫描，稍等片刻将展示镜像的漏洞扫描结果。

图 4-27 镜像安全扫描结果

- 漏洞名称：显示该镜像上扫描出的漏洞名称。
- 修复紧急程度：提示您是否需要立刻处理该漏洞。

- 软件信息：显示该镜像上受此漏洞影响的软件及版本信息。
- 解决方案：针对该漏洞给出的解决方案。单击“解决方案”列的链接，查看修复意见。

----结束

4.11 镜像中心

操作场景

容器镜像服务为您提供大量的公有镜像资源检索，您可以收藏这些镜像并推送到自己的仓库中，方便使用。

约束与限制

“华北-乌兰察布一”、“亚太-雅加达”、“拉美-墨西哥城一”、“拉美-墨西哥城二”和“拉美-圣保罗一”区域暂不支持“镜像中心”功能，如需使用，请切换到其他区域。

收藏镜像

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧菜单栏选择“镜像资源 > 镜像中心”。

步骤3 在镜像列表中，选择待收藏镜像，单击右侧 ☆ 图标。

镜像收藏成功后，您可以在“我的收藏”页面查看。

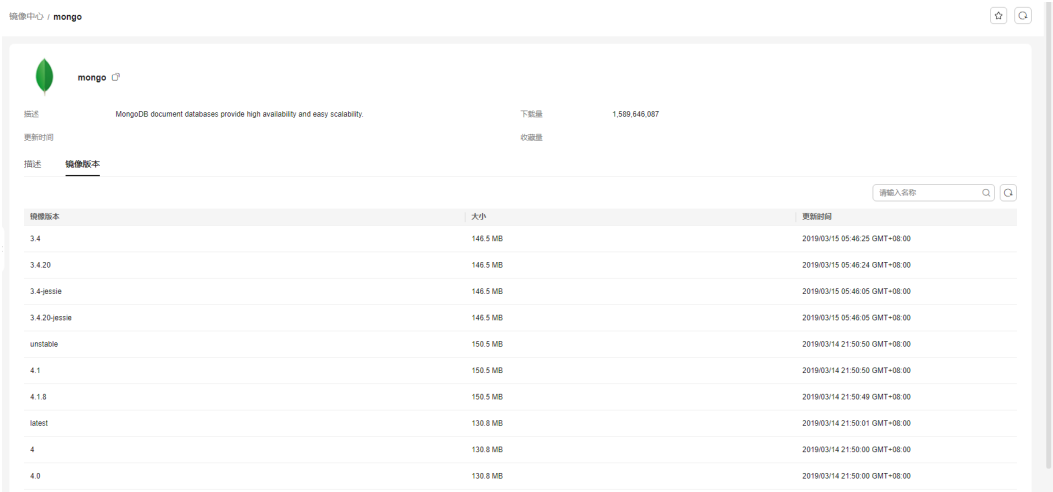
----结束

下载镜像中心的镜像

镜像中心的镜像可直接下载，无需添加仓库地址。如**图4-28**所示的mongo镜像，只需**容器引擎所在虚拟机连接SWR**，且执行如下命令即可将其下载。

docker pull mongo:*4.1*

图 4-28 mongo 镜像详情示例



详细镜像下载步骤，请参考**下载镜像**。

4.12 设置镜像加速器

操作场景

通过docker pull命令下载镜像中心的公有镜像时，往往会因为网络原因而需要很长时间，甚至可能因超时而下载失败。为此，容器镜像服务提供了镜像下载加速功能，帮助您获得更快的下载体验。

约束与限制

- 构建镜像的客户端所安装的容器引擎（Docker）版本必须为1.11.2及以上。
- “华北-乌兰察布一”、“亚太-雅加达”、“拉美-墨西哥城一”、“拉美-墨西哥城二”和“拉美-圣保罗一”区域不支持该功能，如需使用，请切换到其他区域。

操作步骤

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“镜像资源 > 镜像中心”。

说明

在使用镜像中心功能前，请确保您的当前区域支持镜像中心功能，详情请见**镜像中心约束与限制**。

步骤3 单击“镜像加速器”，在弹框中找到“加速器地址”，单击，将加速器地址复制到剪切板。

图 4-29 镜像加速器地址

步骤4 以root用户登录容器引擎所在的虚拟机。

步骤5 修改“/etc/docker/daemon.json”文件（如果没有，可以手动创建），在该文件内添加如下内容：

vi /etc/docker/daemon.json

```
{
  "registry-mirrors": ["加速器地址"]
}
```

其中，加速器地址请替换为**步骤3**中获取的镜像加速器地址。

按“Esc”，输入**:wq**保存并退出。

步骤6 配置完成后，执行**systemctl restart docker**重启容器引擎。

如果重启失败，则检查操作系统其他位置（如：/etc/sysconfig/docker、/etc/default/docker）是否配置了registry-mirrors参数，删除此参数并重启容器引擎即可。

步骤7 执行**docker info**，当Registry Mirrors字段的地址为加速器的地址时，说明加速器已经配置成功。

图 4-30 Registry Mirrors 信息

```
Registry Mirrors:
 https://                                .mirror.swr.myhuaweicloud.com/
```

----结束

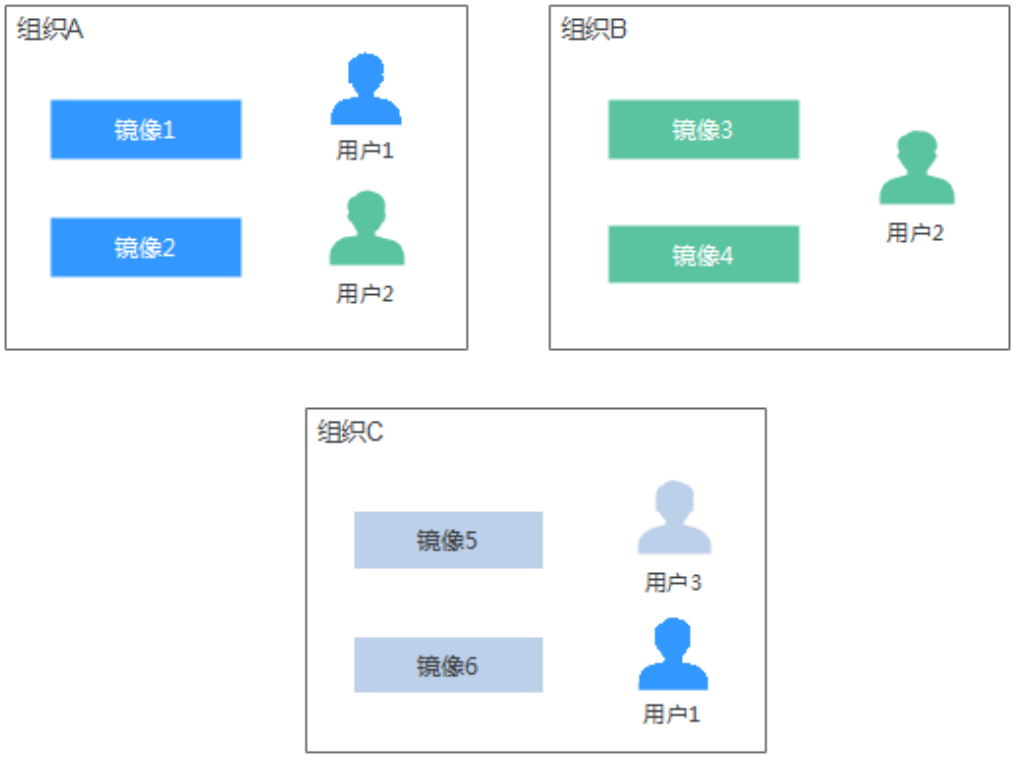
5 组织管理

操作场景

组织用于隔离镜像仓库，每个组织可对应一个公司或部门，将其拥有的镜像集中在该组织下。在不同的组织下，可以有同名的镜像。同一IAM用户可属于不同的组织，如**图5-1**所示。

SWR支持为账户下IAM用户分配相应的访问权限（读取、编辑、管理），具体请参见**授权管理**。

图 5-1 组织



创建组织

容器镜像服务为您提供组织管理功能，方便您根据自身组织架构来构建镜像的资源管理。上传镜像前，请先创建组织。

步骤1 登录**容器镜像服务控制台**。

步骤2 单击控制台左上角的，选择区域和项目。

步骤3 在左侧导航栏单击“组织管理”，进入组织管理页面。

步骤4 单击页面右上角的“创建组织”按钮，在弹框中填写“组织名称”，然后单击“确定”。

说明

- 组织名称全局唯一，即当前区域下，组织名称唯一。创建组织时如果提示组织已存在，可能该组织名称已被其他用户使用，请重新设置一个组织名称。
- 用户在IAM中被授予SWR Admin或Tenant Administrator策略才有创建组织的权限。

----结束

查看组织中的镜像

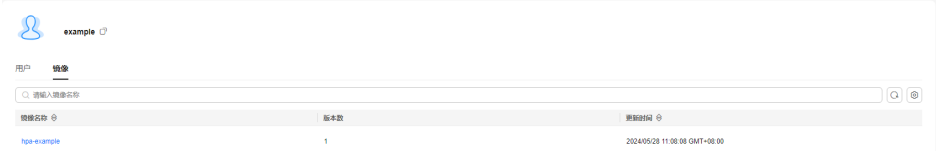
创建组织后，您可以查看当前组织中的镜像。

步骤1 登录**容器镜像服务控制台**。

步骤2 单击控制台左上角的，选择区域和项目。

步骤3 在左侧导航栏选择“组织管理”，单击右侧组织名称。

步骤4 单击“镜像”页签，查看当前组织中的镜像。



----结束

删除组织

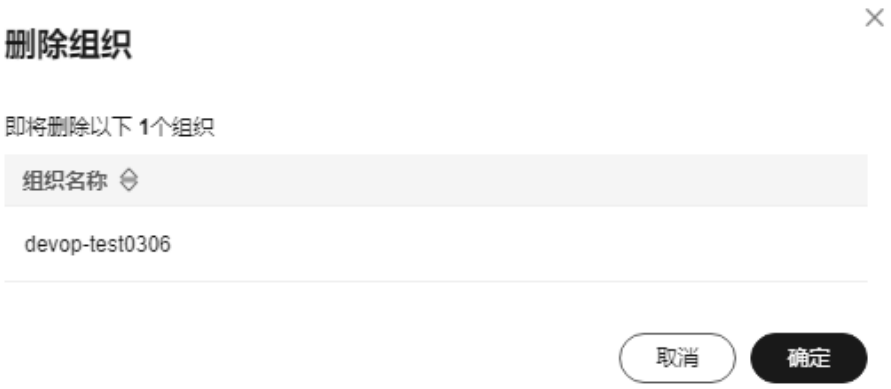
删除组织前，请先删除组织下的所有镜像。

步骤1 登录**容器镜像服务控制台**。

步骤2 单击控制台左上角的，选择区域和项目。

步骤3 在左侧导航栏选择“组织管理”。

步骤4 单击待删除组织右上角“删除”按钮，单击“确定”。



----结束

6 授权管理

操作场景

如果您需要对容器镜像服务进行权限管理，您可以使用统一身份认证服务IAM，设置权限的方法请参见**创建用户并授权使用SWR**。当您具有SWR Admin或者Tenant Administrator系统权限时，您就拥有了SWR的管理员权限，可以在SWR中为其他IAM用户进行授权。

说明

拥有SWR管理员权限的用户，默认拥有所有组织下的镜像管理权限，即使该用户不在组织的授权用户列表中。

如果您没有SWR的管理员权限，就需要已拥有SWR管理员权限的用户在SWR中进行授权管理，为您添加对某个镜像的权限或对某个组织中所有镜像的权限。

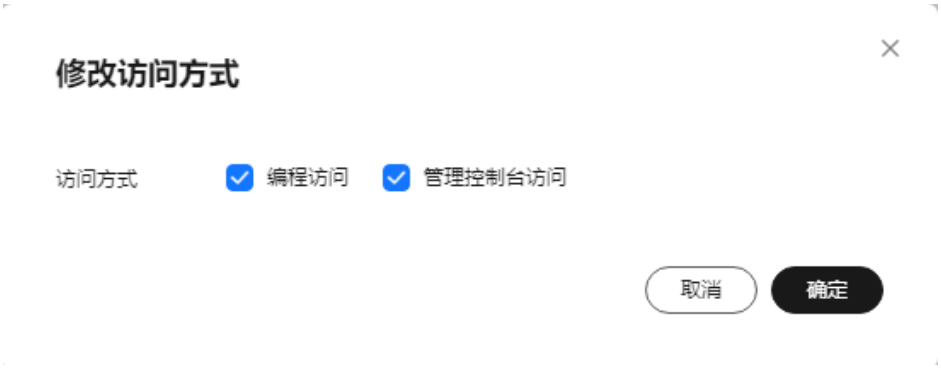
场景示例：

- 示例一：我是拥有ServiceStage Developer权限（SWR只读权限）的IAM用户，想要下载SWR管理员所创建的“group”组织下的“nginx”镜像。

  策略：SWR管理员在“nginx”镜像详情中为您授予“读取”权限，授权完成后，您将享有下载该镜像的权限。
- 示例二：我是SWR管理员，需要给公司外部员工授权一个组织的镜像上传权限，但是不允许他登录控制台，只能通过Docker客户端push镜像。

  策略：您在组织详情“用户”页签下为该员工授予“编辑”权限，并且在IAM中设置访问方式为“编程访问”。

图 6-1 修改访问方式示例



授权方法

容器镜像服务中给IAM用户添加权限有如下两种方法：

- **在镜像详情中添加授权**，授权完成后，IAM用户享有读取/编辑/管理该镜像的权限。
- **在组织中添加授权**，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限。

图 6-2 用户权限

容器镜像服务中为用户添加的权限有如下三种类型：

- 读取：只能下载镜像，不能上传。
- 编辑：下载镜像、上传镜像、编辑镜像属性以及添加触发器。
- 管理：下载镜像、上传镜像、删除镜像或版本、编辑镜像属性、添加授权、添加触发器以及共享镜像。

说明

页面上传镜像功能要求具备组织的编辑或管理权限，在镜像详情中添加的编辑或管理权限不支持页面上传镜像。

在镜像详情中添加授权

在镜像详情中为IAM用户添加授权，授权完成后，该账号下IAM用户享有读取/编辑/管理该镜像的权限。

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧待编辑镜像的名称。

步骤3 在镜像详情页面选择“权限管理”页签。

步骤4 单击“添加授权”，选择IAM用户名称，添加“读取/编辑/管理”的权限，添加后，该IAM用户享有对应权限。

----结束

在镜像详情中修改/删除授权

您还可以在镜像详情中修改用户权限及删除用户权限。

- 修改授权：在“权限管理”页签下用户所在行单击“编辑”，在“权限”所在列选择新的权限，然后单击“保存”。

- 删除授权：在“权限管理”页签下用户所在行单击“删除”，然后单击“确定”。

在组织中添加授权

IAM用户创建后，需要管理员在组织中为用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限。

只有具备“管理”权限的账号和IAM用户才能添加授权。

步骤1 登录**容器镜像服务控制台**。

步骤2 在左侧菜单栏选择“组织管理”，单击右侧组织名称后的“详情”。

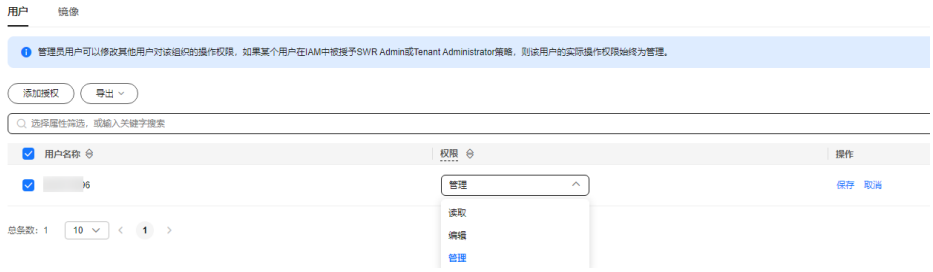
步骤3 在“用户”页签下单击“添加授权”，在弹出的窗口中为IAM用户选择权限，然后单击“确定”。

----结束

在组织中修改/删除授权

您还可以在组织中修改用户权限及删除用户权限。

- 修改授权：在“用户”页签下用户所在行单击“编辑”，在“权限”所在列选择新的权限，然后单击“保存”。



- 在“用户”页签下用户所在行单击“删除”，然后单击“确定”。

7 审计

7.1 支持云审计的关键操作

操作场景

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

通过云审计服务，您可以记录与SWR相关的操作事件，便于日后的查询、审计和回溯。

支持审计的关键操作列表

表 7-1 云审计服务支持的共享版 SWR 操作列表

操作名称	资源类型	事件名称
创建命名空间权限	usernamespaceauth	createUserNamespaceAuth
修改命名空间权限	usernamespaceauth	updateUserNamespaceAuth
删除命名空间权限	usernamespaceauth	deleteUserNamespaceAuth
创建软件包	package	createPackage
修改软件包	package	updatePackage
删除软件包	package	deletePackage
创建仓库	repository	createRepository
修改仓库	repository	updateRepository
删除仓库	repository	deleteRepository
创建版本	version	createVersion
修改版本	version	updateVersion

操作名称	资源类型	事件名称
删除版本	version	deleteVersion
上传镜像包	image	uploadImagePackage
上传文件	file	uploadFile
下载文件	file	downloadFile
删除文件	file	deleteFile
创建组织	usernamespace	createUserNamespace
删除组织	usernamespace	deleteUserNamesapce
收藏镜像	usercollections	createUserCollections
取消收藏镜像	usercollections	deleteUserCollections
创建触发器	trigger	createTrigger
修改触发器	trigger	updateTrigger
删除触发器	trigger	deleteTrigger
创建仓库权限	userrepositoryauth	createUserRepositoryAuth
修改仓库权限	userrepositoryauth	updateUserRepositoryAuth
删除仓库权限	userrepositoryauth	deleteUserRepositoryAuth
创建镜像仓库	imagerepository	createImageRepository
修改镜像仓库	imagerepository	updateImageRepository
删除镜像仓库	imagerepository	deleteImageRepository
删除镜像版本	imagetag	deleteImageTag
生成登录指令	dockerlogincmd	createDockerConfig
创建共享镜像	imagerepositoryaccessdomain	createImageRepositoryAccessDomain
修改共享镜像	imagerepositoryaccessdomain	updateImageRepositoryAccessDomain
删除共享镜像	imagerepositoryaccessdomain	deleteImageRepositoryAccessDomain
下载镜像层	downloadimagelayer	downloadimagelayer

7.2 查看云审计日志

操作场景

开启了云审计服务（CTS）后，系统开始记录SWR相关的操作。CTS会保存最近1周的操作记录。

本小节介绍如何在CTS管理控制台查看最近1周的操作记录。

操作步骤

步骤1 登录CTS管理控制台，单击页面右上角“返回旧版”。

步骤2 选择左侧导航栏的“事件列表”，进入事件列表页面。

步骤3 事件记录了云资源的操作详情，设置筛选条件，单击“查询”。

当前事件列表支持四个维度的组合查询，详细信息如下：

- 事件类型、事件来源、资源类型和筛选类型。

  在下拉框中选择查询条件。其中，“事件类型”选择“管理事件”，“事件来源”选择“SWR”。

  图 7-1 设置筛选条件

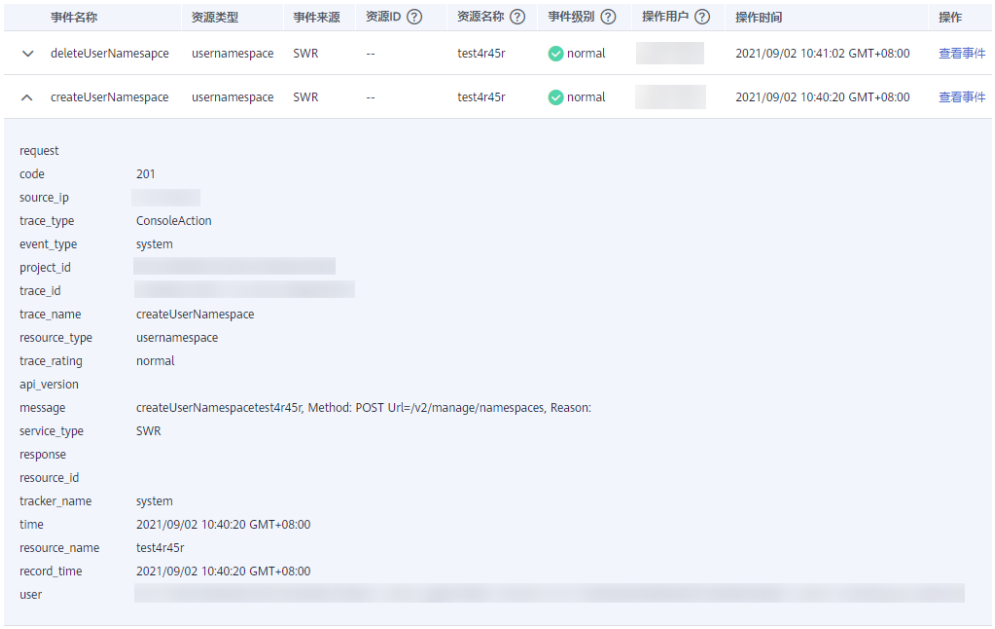
  其中，筛选类型选择“按资源ID”时，还需手动输入某个具体的资源ID，目前仅支持全字匹配模式的查询。

  筛选类型选择“按资源名称”时，选框下拉列表会自动显示符合筛选条件的资源名称。

- 操作用户：在下拉框中选择某一具体的操作用户。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选项为“最近1小时”、“最近1天”、“最近1周”和“自定义时间段”，本示例选择“最近1周”。

步骤4 在需要查看的事件左侧，单击 ﹀ 图标展开该事件的详细信息。

图 7-2 展开事件



步骤5 在需要查看的事件右侧，单击“查看事件”，弹出一个窗口，显示了该操作事件结构的详细信息。

关于云审计事件结构的关键字段详解，请参见**事件结构**。

----结束

