

容器镜像服务

用户指南

文档版本

01

发布日期

2020-10-29



华为技术有限公司



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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默示的声明或保证。

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。

目录

1 欢迎使用容器镜像服务.....	1
2 权限管理.....	2
2.1 创建用户并授权使用 SWR.....	2
3 容器引擎基础知识.....	4
4 镜像管理.....	7
4.1 客户端上传镜像.....	7
4.2 获取长期有效登录指令.....	8
4.3 页面上传镜像.....	9
4.4 下载镜像.....	10
4.5 编辑镜像属性.....	11
4.6 共享私有镜像.....	13
4.7 添加触发器.....	14
4.8 添加镜像老化规则.....	17
4.9 自动同步镜像.....	19
4.10 镜像安全扫描.....	20
4.11 收藏镜像.....	21
4.12 设置镜像加速器.....	22
5 组织管理.....	23
6 授权管理.....	26
7 审计.....	31
7.1 云审计服务支持的 SWR 操作列表.....	31
7.2 查看云审计日志.....	32

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）进行精细的权限管理，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服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如[图2-1](#)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：[SWR系统权限](#)。若您需要对除SWR之外的其它服务授权，IAM支持服务的所有权限请参见[权限策略](#)。

示例流程

图 2-1 给用户授权 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 Admin”。
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：在“服务列表”中选择容器镜像服务，进入SWR主界面，左侧导航栏中选择“组织管理”，在右侧页面单击“创建组织”，如果能创建组织，说明权限设置成功。

3 容器引擎基础知识

容器引擎是一个开源的引擎，可以轻松地为任何应用创建一个轻量级的、可移植的、自给自足的容器。容器镜像服务兼容原生容器引擎，支持使用社区CLI和原生API管理容器镜像。

安装容器引擎

在安装容器引擎前，请了解容器引擎的基础知识。

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。

📖 说明

- 容器镜像的存储可以使用华为云提供的容器镜像服务，由于容器镜像服务支持容器引擎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IP后才能访问。

另外，在Linux操作系统下，可以使用如下命令快速安装容器引擎。

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

在Euler操作系统下，安装容器引擎的方法如下：

步骤1 登录弹性云服务器。

步骤2 配置yum源。如果您的机器上还没配置yum源，可以参照如下方法配置：[如何使用华为云提供的EulerOS镜像源\(x86_64和ARM\)?](#)。如果已配置过了，可跳过该步骤。

步骤3 安装并运行容器引擎。

1. 获取yum源里的docker-engine包
yum search docker-engine
2. 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
3. **systemctl enable docker**
4. **systemctl start docker**

步骤4 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 1.13.1, build 8633870/1.13.1
```

----结束

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。

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:v3 .
```

- -t nginx:v3：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v3。

```
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, -o, 表示导出到文件。(可选)

压缩包格式为: .tar或.tar.gz。

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
$ docker save -o nginx-latest.tar nginx:latest
```

----**结束**

4 镜像管理

4.1 客户端上传镜像

本章节以2048-demo:v1镜像为例，介绍如何使用客户端上传镜像。客户端上传镜像，是指使用命令将镜像上传到容器镜像服务的镜像仓库。

说明


使用客户端上传镜像，镜像的每个layer大小不能超过10G。

前提条件

- 已创建组织，请参见[创建组织](#)。
- 上传镜像的容器引擎客户端版本必须为1.11.2及以上。

操作步骤

步骤1 连接容器镜像服务。

1. 登录容器镜像服务控制台。
2. 在左侧菜单栏选择“我的镜像”，单击右侧“客户端上传”，在弹出的页面中单击“生成临时登录指令”，单击复制登录指令。登录指令末尾的域名即为当前镜像仓库地址，记录该地址。

说明

此处生成的临时登录指令有效期为24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](#)，它们之间的区别请参见[长期有效的登录指令与临时登录指令的区别是什么？](#)。

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2 在安装容器引擎的机器给2048-demo镜像打标签。

docker tag [镜像名称:版本名称] [镜像仓库地址]/[组织名称]/[镜像名称:版本名称]
样例如下：

```
docker tag 2048-demo:v1 swr.cn-north-1.myhuaweicloud.com/group/2048-demo:v1
```

其中：

- swr.cn-north-1.myhuaweicloud.com为容器镜像服务的镜像仓库地址。
- group为组织名称。
- 2048-demo:v1为镜像名称和版本号。

步骤3 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:版本名称]
```

样例如下：

```
docker push swr.cn-north-1.myhuaweicloud.com/group/2048-demo:v1
```

终端显示如下信息，表明上传镜像成功。

```
6d6b9812c8ae: Pushed
695da0025de6: Pushed
fe4c16cbf7a4: Pushed
v1: digest: sha256:eb7e3bbd8e3040efa71d9c2cacfa12a8e39c6b2ccd15eac12bdc49e0b66cee63 size: 948
```

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

4.2 获取长期有效登录指令

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。

操作步骤

步骤1 获取区域项目名称、镜像仓库地址。

1. 登录管理控制台，单击右上角您的用户名处，单击“我的凭证”。
2. 在“API凭证”的项目列表中查找当前区域对应的项目。
如下图所示，“华北-北京一”对应的项目名称为“cn-north-1”。

图 4-1 区域与项目

项目ID	项目	所属区域
0503dda89700fed2f78c00909158a4d	cn-north-1	华北-北京一
05041ffa40025702f6dc009cc6f8f33	cn-north-4	华北-北京四
0503ddabba8010df2f93c009272536d2	cn-north-5	华北-乌兰察布二零一
0503ddab5f8010df2f92c00977d3e282	cn-north-6	华北-乌兰察布二零二
0504200e748026c52f10c0092a4e9151	cn-northeast-1	东北-大连
05e1aef9040010e22fccc009adecb056	cn-east-3	华东-上海一
05041fea8a8025662f4ac00927982f3e	cn-east-2	华东-上海二

3. 镜像仓库地址为：`swr.区域项目名称.myhuaweicloud.com`，如华北-北京一对应的镜像仓库地址为：`swr.cn-north-1.myhuaweicloud.com`。

步骤2 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. 登录管理控制台，单击右上角您的用户名处，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. 输入验证码。
4. 单击“确定”，下载访问密钥，其中包含AK和SK。

📖 说明

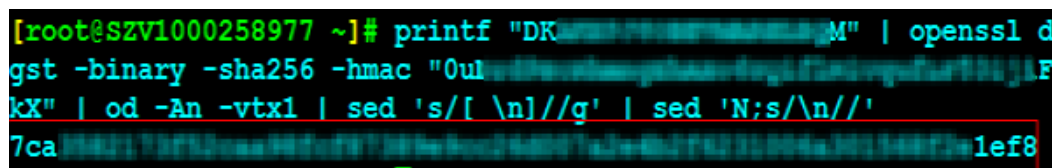
为防止访问密钥泄露，建议您将其保存到安全的位置。

步骤3 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/'
```

其中\$AK和\$SK为步骤2获取的AK/SK。

图 4-2 示例



步骤4 使用如下的格式拼接登录指令。

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

其中，区域项目名和镜像仓库地址在步骤1中获取，AK在步骤2中获取，登录密钥为步骤3的执行结果。

📖 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5 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

本章节介绍如何通过页面上传镜像。从页面上传镜像，是指直接通过页面将镜像上传到容器镜像服务。

须知

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。

前提条件

- 已创建组织，请参见[创建组织](#)。
- 镜像已存为tar或tar.gz文件，具体请参见[制作镜像压缩包](#)。
- 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。

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“页面上传”。

步骤3 在弹出的窗口中选择镜像要上传的组织，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 4-3 上传镜像



步骤4 在弹出的窗口中单击“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

4.4 下载镜像

镜像上传后，您可以获取镜像下载地址，使用docker pull命令下载镜像。

操作步骤



- 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1](#)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** 在左侧菜单栏选择“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 4-4 获取镜像下载指令

<input type="checkbox"/>	镜像版本	大小	更新时间 ↓	下载指令
<input type="checkbox"/>	1.0	43.3 MB	2020/02/17 10:44:58 GMT+08:00	docker pull swr. 

- 步骤6** 在虚拟机执行[步骤5](#)复制的镜像下载指令。
- 步骤7** 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]
```

----结束

4.5 编辑镜像属性

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”，根据需要在弹出的窗口中编辑类型（“公开”或“私有”）、分类及描述，然后单击“确定”。

图 4-5 编辑镜像属性

编辑镜像 ×

组织 paas_swf_...

名称 busybox

类型 公开 私有

分类

描述

表 4-1 编辑镜像

参数	说明
组织	镜像所属组织。
名称	镜像名称。
类型	<p>镜像类型，可选择：</p> <ul style="list-style-type: none"> ● 公开 ● 私有 <p>说明</p> <p>公开镜像所有用户都可以下载使用。</p> <ul style="list-style-type: none"> ● 如果您的节点与镜像仓库在同一区域，访问仓库是通过内网访问。 ● 如果您的节点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节点可以访问公网。
分类	<p>镜像分类，可选择：</p> <ul style="list-style-type: none"> ● 应用服务器 ● Linux ● Windows ● 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

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。

使用约束

- 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。
- 仅账号和具备该私有镜像管理权限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。

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** 在镜像详情页面选择“共享”页签。
- 步骤4** 单击“共享镜像”，根据[表4-2](#)填写相关参数，然后单击“确定”。

图 4-6 共享镜像

表 4-2 共享镜像

参数	说明
共享给	输入账号名称。
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。
描述	输入描述，0-1000个字符。
权限	当前仅支持“下载”权限。

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

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。

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，请登录云容器引擎创建工作负载页面进行创建，具体创建方法请参见[创建无状态工作负载](#)或[创建有状态工作负载](#)，或登录云容器实例创建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 在左侧菜单栏选择“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4-3填写相关参数，然后单击“确定”。

图 4-7 添加触发器

添加触发器

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

触发器名称: test-trigger
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: 全部触发

触发动作: 更新容器的镜像
需指定更新的应用,以及该应用下的指定容器镜像

触发器状态: 启用

触发器类型: 云容器引擎CCE, 云容器实例CCI

选择应用: 集群: test123, 命名空间: default, 应用: nginx, 容器: container-0

确定 取消

表 4-3 触发器

参数	说明
触发器名称	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。

参数	说明
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。 <ul style="list-style-type: none"> 全部触发：有新的镜像版本生成或镜像版本发生更新时，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。
触发动作	当前仅支持更新容器的镜像，需指定更新的应用，以及该应用下的指定容器镜像。
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-北京一”、“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。

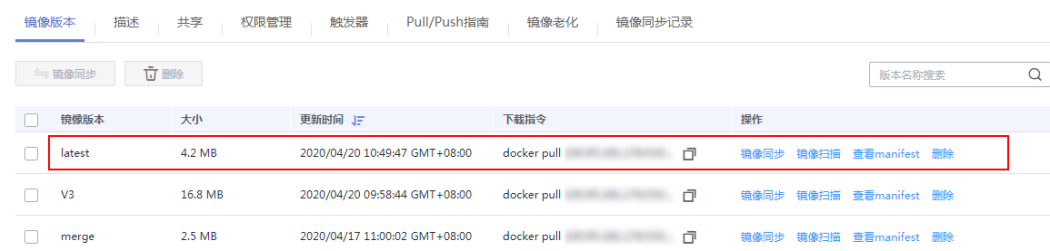
----结束

验证操作

本例中触发条件为全部触发，即有新的镜像版本生成或镜像版本发生更新时，触发应用部署。

上传新的镜像版本至容器镜像服务的镜像仓库中，可在镜像详情页查看新上传的镜像版本。

图 4-8 查看镜像版本



- 触发器类型设置为“云容器引擎CCE”时，登录云容器引擎服务控制台，在左侧菜单栏选择“工作负载”，单击要查看的工作负载名称，进入工作负载详情页面。在“实例列表”页签，可以看到应用实例正在创建。待实例创建成功，说明应用已更新完成。

图 4-9 CCE 应用已更新完成



在“访问方式”页签中获取访问地址，可以访问应用页面，看到已更新的应用信息。

- 触发器类型设置为“云容器实例CCI”时，登录云容器实例服务控制台，在左侧菜单栏选择“工作负载 > 无状态（Deployment）”，单击要查看的无状态负载名称，进入无状态负载详情页面。

在“Pod列表”中，可以看到应用实例正在创建。待实例创建成功，说明应用已更新完成。

图 4-10 CCI 应用已更新完成



The screenshot shows a table titled 'Pod列表' with a search bar on the right. The table has columns for Instance (Pod), Status, Pod IP, CPU Request (Cores), Memory Request (GB), Runtime, Price (¥/second), and Actions. One pod is listed with the name 'cci-deployment...', status '运行中' (Running), CPU request of 2.00, memory request of 4.00, runtime of 0 days 0 hours 0 minutes 6 seconds, and a price of 0.000178. There are links for '查看日志' (View Logs) and '删除' (Delete).

实例(Pod)	状态	Pod IP	CPU申请量(核)	内存申请量(GB)	运行时长	价格(¥/秒)	操作
cci-deployment...	运行中		2.00	4.00	0天 0小时 0分钟 6秒	0.000178	查看日志 删除

在“访问配置”中获取访问地址，可以访问应用页面，看到已更新的应用信息。

4.8 添加镜像老化规则

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，将在镜像存留时间超过指定时间时被删除。
- 版本数目：设置该类型的老化规则后，将在版本数超过指定值后删除旧的镜像。

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。

使用约束

当前仅支持添加1个镜像老化规则。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** 在左侧菜单栏选择“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4-4填写相关参数，然后单击“确定”。

图 4-11 创建老化规则

×

创建老化规则

* 规则类型 ?

* 保留天数 ?

过滤标签 ?

过滤正则 ?

确定
取消

表 4-4 添加镜像老化规则

参数	说明
规则类型	规则类型分为存活时间和版本数目。存活时间类型的老化规则将在镜像存留时间超过指定时间时被删除，版本数目类型的老化规则将在版本数超过指定值后删除旧的镜像。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。
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 4-12 查看规则列表和老化日志



---结束

4.9 自动同步镜像

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？](#)。

使用约束

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”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“亚太-香港”、“亚太-新加坡”区域。

操作步骤

- 步骤1** 登录容器镜像服务控制台。
- 步骤2** 在左侧菜单栏选择“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“自动同步镜像”，添加镜像同步的目标区域和目标组织，添加完成后单击“确定”。

图 4-13 添加镜像自动同步



- 目标区域：选择同步的目标区域，例如“华南-广州”。
- 目标组织：选择同步的目标组织。
- 是否覆盖：勾选则表示覆盖，同步相同名称的镜像时，同步后会替换已有的镜像。不勾选则表示不覆盖，同步相同名称的镜像时，会取消同步并提示已存在相同名称镜像。

步骤4 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、目标区域、目标组织、同步者等。

----结束

4.10 镜像安全扫描

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。

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”，单击右侧镜像名称，进入镜像详情页。
- 步骤3** 选择“镜像版本”页签，选择所需的镜像版本并单击右侧的“镜像扫描”。
- 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 4-14 镜像安全扫描结果

扫描结果 ×

扫描状态: ✔ 扫描完成 重新扫描 ↻

漏洞总个数: **35** ● 需尽快修复: **0** ● 可延后修复: **35** ● 暂可不修复: **0**

最后扫描时间: 2020/04/11 15:21:32 GMT+08:00

所有修复紧急度 请输入漏洞名称 🔍

漏洞名称	修复紧急程度	软件信息	解决方案
USN-3434-1	可延后修复	libidn111.32-3ubuntu1.1	Update the affected libi...
USN-3475-1	可延后修复	libssl1.0.0l.0.2g-1ubunt...	Update the affected libs...
USN-3489-1	可延后修复	libdb5.3.5.3.28-11	Update the affected db...
USN-3496-1	可延后修复	python2.7-minimal2.7.1...	Update the affected pyt...
USN-3512-1	可延后修复	libssl1.0.0l.0.2g-1ubunt...	Update the affected libs...

5 总条数: 35 < 1 2 3 4 5 6 7 >

确定

- 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 收藏镜像

容器镜像服务为您提供大量的公有镜像资源检索。您可以将镜像收藏到“我的收藏”中, 方便后续使用。

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“镜像资源>镜像中心”。
- 步骤3** 在右侧镜像列表中单击 。

收藏成功后，您可以在“我的收藏”中查看您收藏的镜像。

----结束

4.12 设置镜像加速器

容器镜像服务为您提供镜像加速功能，您可以通过配置/etc/sysconfig/docker中--registry-mirror参数来使用加速器。

须知

- 容器引擎客户端版本必须为1.11.2及以上。

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“镜像资源>镜像中心”。

步骤3 在右侧单击“镜像加速器”，在弹出的对话框中获取镜像加速器地址和配置镜像加速器的方法，如图4-15。

图 4-15 镜像加速器



----结束

5 组织管理

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。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 在左侧菜单栏选择“组织管理”，单击右侧“创建组织”，在弹出的页面中填写“组织名称”，然后单击“确定”。

图 5-2 创建组织



----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 在左侧菜单栏选择“组织管理”，单击右侧组织名称。

步骤3 单击“镜像”页签，查看当前组织中的镜像。

图 5-3 查看组织中的镜像

镜像名称	版本号	更新时间
swr-manage	1	2020/04/16 14:44:50 GMT+08:00
paas-aos-tosca-dsl-parser	10	2020/04/14 17:03:21 GMT+08:00
euleros_x86_64	1	2020/03/22 15:50:21 GMT+08:00
docker	2	2020/03/19 17:52:42 GMT+08:00

----结束

删除组织

删除组织前，请先删除组织下的所有镜像和软件仓库。

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。

步骤3 单击右上角“删除”按钮，在弹出的对话框中根据提示输入“DELETE”，然后单击“确定”。

图 5-4 删除组织



----结束

6 授权管理

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。

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。

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 6-1 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、编辑镜像属性以及创建触发器。
- 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。

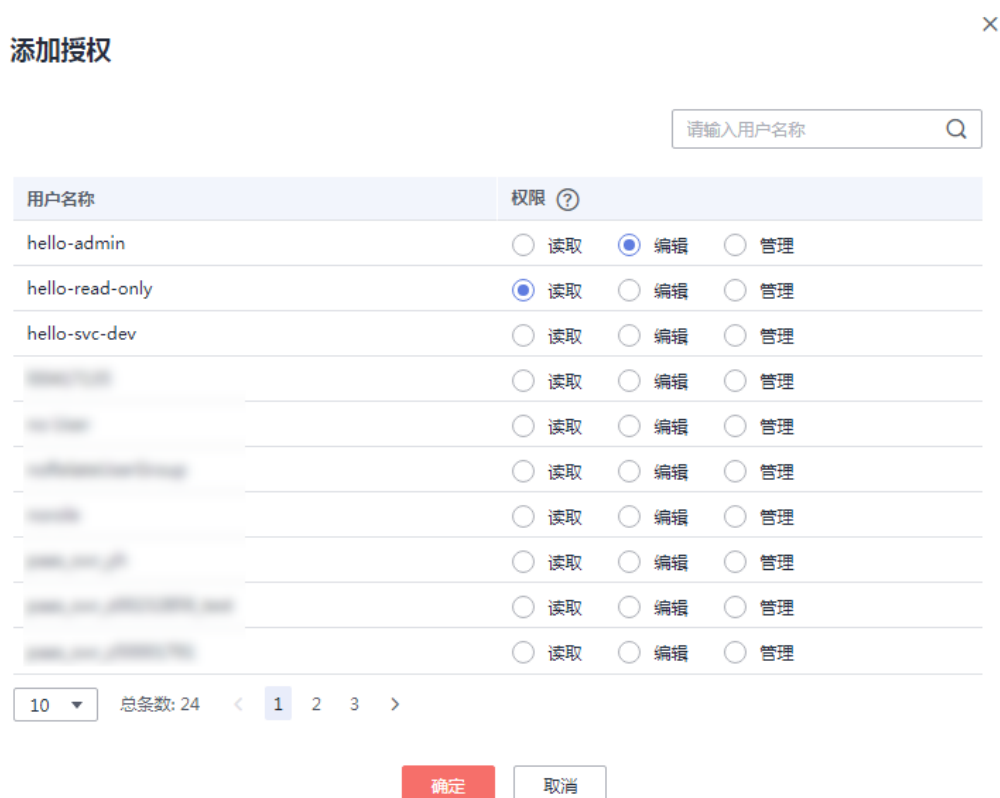
步骤3 在镜像详情页面选择“权限管理”页签。

图 6-2 权限管理



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。

图 6-3 在镜像详情中添加授权



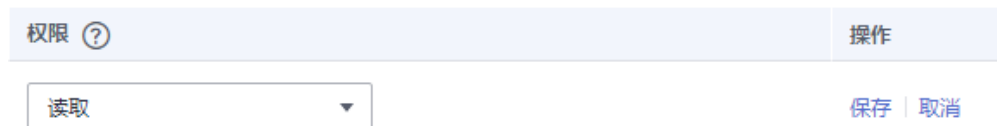
---结束

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“修改”，在“权限”所在列选择新的权限，然后单击“保存”。

图 6-4 在镜像详情中修改授权



- 删除授权：在“权限管理”页签下用户所在行单击“删除”。在弹出的对话框中根据提示输入“DELETE”，然后单击“确定”。

图 6-5 在镜像详情中删除授权



在组织中添加授权

在组织中为IAM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。

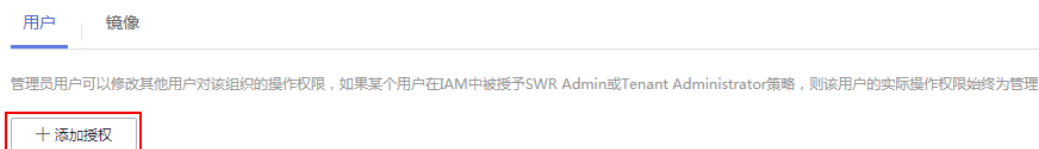
只有具备“管理”权限的账号和IAM用户才能添加授权。

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”。

图 6-6 在组织中添加授权



----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“修改”，在“权限”所在列选择新的权限，然后单击“保存”。

图 6-7 在组织中修改授权



- 在“用户”页签下用户所在行单击“删除”。在弹出的对话框中根据提示输入“DELETE”，然后单击“确定”。

图 6-8 在组织中删除授权



7 审计

7.1 云审计服务支持的 SWR 操作列表

SWR通过云审计服务（Cloud Trace Service，简称CTS）为您提供云服务资源的操作记录，记录内容包括您从云管理控制台或者开放API发起的的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

表 7-1 云审计服务支持的 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
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

操作名称	资源类型	事件名称
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	imagerepositoryaccessd omain	createImageRepositoryAccess Domain
修改共享镜像	imagerepositoryaccessd omain	updateImageRepositoryAccess Domain
删除共享镜像	imagerepositoryaccessd omain	deleteImageRepositoryAccess Domain


7.2 查看云审计日志

操作场景

开启了云审计服务后，系统开始记录SWR资源的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。


步骤2 在管理控制台左上角单击图标，选择区域。

步骤3 单击页面上方的“服务列表”，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤5 事件列表支持通过筛选来查询对应的操作事件。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：可选项为“管理事件”、“数据事件”。
- 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，事件来源选择“SWR”。
当筛选类型选择事件名称时，还需选择某个具体的事件名称。
选择资源ID时，还需选择或者手动输入某个具体的资源ID。
选择资源名称时，还需选择或手动输入某个具体的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 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。

步骤6 在需要查看的记录左侧，单击  展开该记录的详细信息。

步骤7 在需要查看的记录右侧，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。

----结束