容器镜像服务

用户指南

文档版本 08

发布日期 2025-09-19

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。

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。

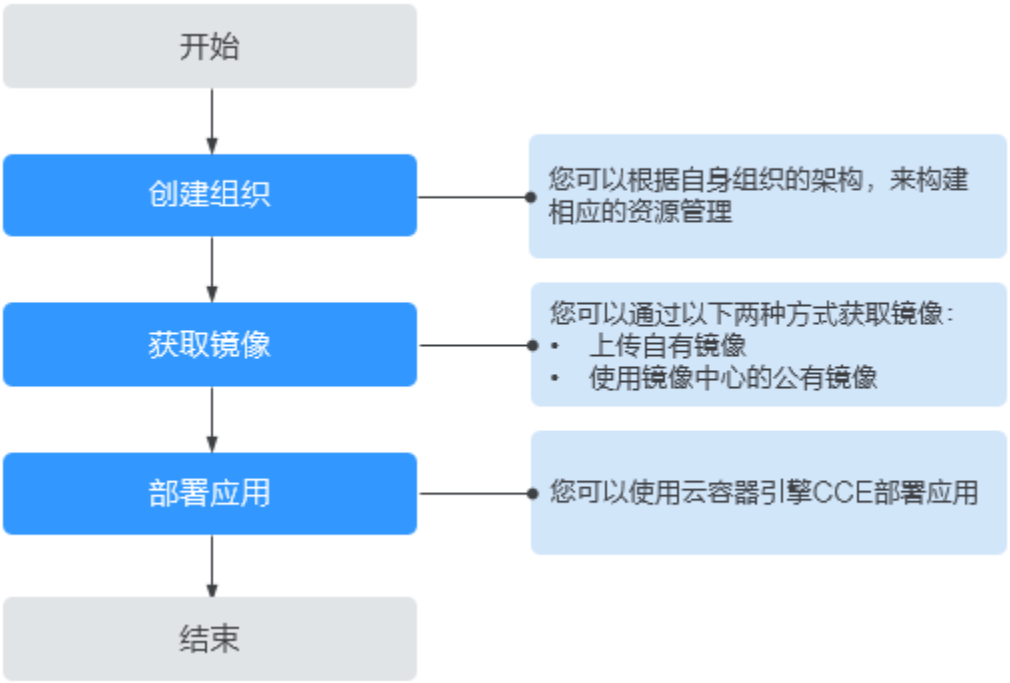
SWR提供私有镜像库，并支持细粒度的权限管理，可以为不同用户分配相应的访问权限（读取、编辑、管理）。SWR还支持容器镜像版本更新自动触发部署。您只需要为镜像设置一个触发器，通过触发器，可以在每次镜像版本更新时，自动更新云容器引擎（CCE）中使用该镜像部署的应用。

您可以通过控制台、API使用容器镜像服务。

说明

容器镜像服务免费提供给您。

图 1-1 SWR 使用流程



2 通过 IAM 授予使用 SWR 的权限

2.1 通过 IAM 角色或策略授予使用 SWR 的权限

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。

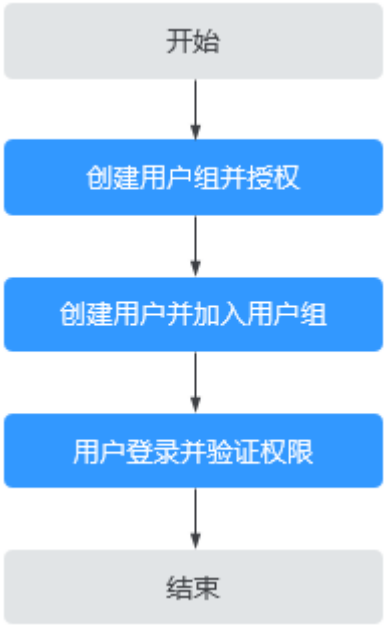
本章节为您介绍对用户授权的方法，操作流程如**图2-1**所示。

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：**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 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（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。

SWR 资源

资源是服务中存在的对象。在SWR中，资源包括：组织、镜像，您可以在创建策略时，通过指定资源路径来选择特定资源。

表 2-1 SWR 的指定资源与对应路径

指定资源	资源路径
namespace	【格式】 swr:*:*:namespace:组织名称 【说明】 对于组织资源，IAM自动生成资源路径前缀SWR:*:*:namespace: 通过组织名称指定具体的资源路径，支持通配符*。例如： swr:*:*:namespace:*表示任意组织。
repo	【格式】 swr:*:*:repo:镜像仓库名称 【说明】 对于镜像仓库资源，IAM自动生成资源路径前缀SWR:*:*:repo: 通过镜像仓库名称指定具体的资源路径，支持通配符*。例如： SWR:*:*:repo:*表示任意镜像仓库。

例1：只允许用户查询镜像仓库概要信息，则可以通过如下方式配置。

```
{
"Version": "5.0"
"Statement": [
{
"Effect": "Allow",
"Action": [
"swr:repo:getRepo"
],
"Resource": [
"swr:*:*:repo:*"
]
}
]
}
```

例2：比如说要把cn-north-4下组织source下的镜像test，同步到cn-north-7的组织target下，那么用户需要有cn-north-4创建自动镜像同步任务的权限、要同步的镜像的下载权限，cn-north-4和cn-north-7的获取临时登录指令的权限，以及cn-north-7目前组织的镜像推送权限：

```
{
"Version": "5.0",
```



```
"Statement": [
{
"Effect": "Allow",
"Action": [
"swr:repo:createAutoSyncRepoJob",
"swr:repo:download"
],
"Resource": [
"swr:cn-north-4:*:repo:source/test"
]
},
{
"Effect": "Allow",
"Action": [
"swr:repo:upload"
],
"Resource": [
"swr:cn-north-7:*:repo:target"
]
},
{
"Effect": "Allow",
"Action": [
"swr::createLoginSecret"
]
}
]
}
```

2.2 通过 IAM 身份策略授予使用 SWR 的权限

如果您需要对您所拥有的（SWR）进行身份策略的权限管理，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用户或用户组，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、高效的其他华为云帐号或者云服务，这些帐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，您可以跳过本章节，不影响您使用SWR服务的其它功能。

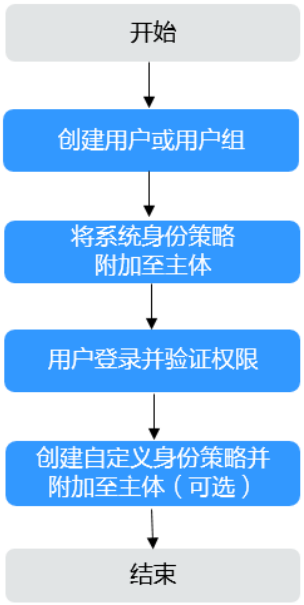
本章节为您介绍使用身份策略的授权方法，操作流程如**下图**所示。

前提条件

在授权操作前，请您了解可以添加的SWR权限，并结合实际需求进行选择。SWR支持的系统策略，请参见**身份策略权限管理**。

示例流程

图 2-2 给用户授予 SWR 权限流程



1. **创建用户**或**创建用户组**

   在IAM控制台创建用户或用户组。

2. **将系统身份策略附加至用户或用户组**

   为用户或用户组授予容镜像服务*只读权限*的系统身份策略“*SWRReadOnlyPolicy*”，或将身份策略附加至用户或用户组。

3. **用户登录**并验证权限

   使用已授权的用户登录控制台，验证权限：

   - *在“服务列表”中选择容器镜像服务，进入SWR主界面，单击右上角“创建组织”，尝试创建组织，如果无法创建（假设当前权限仅包含SWRReadOnlyPolicy），表示“SWRReadOnlyPolicy”已生效。*
   - *在“服务列表”中选择除容器镜像服务外（假设当前策略仅包含SWRReadOnlyPolicy）的任一服务，若提示权限不足，表示“SWRReadOnlyPolicy”已生效。*

SWR 自定义身份策略样例

如果系统预置的权限不满足您的授权要求，可以创建策略。策略中可以添加的授权项（Action）请参考**表2-2**。

目前华为云支持以下两种方式创建策略：

- 可视化视图创建策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义身份策略并附加至主体**。

- 示例：用户可以创建、查看、删除组织。

```
{
"Version": "5.0",
"Statement": [
{
"Effect": "Allow",
"Action": [
"swr:namespace:createNamespace",
"swr:namespace:deleteNamespace",
"swr:namespace:listNamespaces",
"swr:namespace:deleteNamespaceAccess",
"swr:namespace:getNamespaceAccess"
]
}
]
}
```

授权操作与系统身份策略关系

表 2-2 授权操作与系统身份策略关系

操作	Action名称	SWR Admin
创建组织	swr:namespace:createNamespace	√
删除组织	swr:namespace:deleteNamespace	√
查询组织列表	swr:namespace:listNamespaces	√
获取组织详情	swr:namespace:getNamespace	√
在组织下创建镜像仓库	swr:repo:createRepo	√
删除组织下的镜像仓库	swr:repo:deleteRepo	√
查询镜像仓库列表	swr:repo:listRepos	√

操作	Action名称	SWR Admin
查询共享镜像列表	swr:repo:listSharedRepos	√
查询镜像仓库概要信息	swr:repo:getRepo	√
更新镜像仓库的概要信息	swr:repo:updateRepo	√
删除镜像仓库中指定tag的镜像	swr:repo:deleteRepoTag	√
查询镜像tag列表	swr:repo:listRepoTags	√
创建共享账号	swr:repo:createRepoDomain	√
删除共享账号	swr:repo:deleteRepoDomain	√
获取共享账号列表	swr:repo:listRepoDomains	√
判断共享账号是否存在	swr:repo:getRepoDomain	√
更新共享账号	swr:repo:updateRepoDomain	√
创建镜像自动同步任务	swr:repo:createAutoSyncRepoJob	√
手动同步镜像	swr:repo:createManualSyncRepoJob	√
删除镜像自动同步任务	swr:repo:deleteAutoSyncRepoJob	√
获取镜像自动同步任务列表	swr:repo:listAutoSyncRepoJobs	√
获取镜像自动同步任务信息	swr:repo:getSyncRepoJobInfo	√
创建触发器	swr:repo:createTrigger	√
删除触发器	swr:repo:deleteTrigger	√
获取镜像仓库下的触发器列表	swr:repo:listTriggers	√
获取触发器详情	swr:repo:getTrigger	√
更新触发器配置	swr:repo:updateTrigger	√
创建镜像老化规则	swr:repo:createRetention	√
删除镜像老化规则	swr:repo:deleteRetention	√
获取镜像老化记录	swr:repo:listRetentionHistories	√
获取镜像老化规则列表	swr:repo:listRetentions	√
获取镜像老化规则记录	swr:repo:getRetention	√
修改镜像老化规则	swr:repo:updateRetention	√
生成临时登录指令	swr::createLoginSecret	√
获取配额信息	swr::listQuotas	√

操作	Action名称	SWR Admin
获取租户总览信息	swr::getDomainOverview	√
获取租户资源统计信息	swr::getDomainResourceReports	√
分段上传镜像（页面上传）	swr:namespace:multipartUpload	√
docker上传镜像	swr:repo:upload	√
docker下载镜像	swr:repo:download	√

说明

手动镜像同步和自动镜像同步都需要同时要有同步镜像的下载权限(swr:repo:download)、生成临时登录指令(swr::createLoginSecret)和对端Region目标组织的镜像上传权限(swr:repo:upload)。

3 容器引擎基础知识

容器引擎是Kubernetes最重要的组件之一，负责管理镜像和容器的生命周期。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。

SWR当前支持Docker和Containerd两种容器引擎。下文以Docker容器引擎为例简单介绍容器引擎的安装和镜像文件的制作。

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

- 容器镜像的存储可以使用容器镜像服务（SWR），建议下载18.06及以上版本的Docker容器引擎。
- 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

您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。
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

本章节将指导您通过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
```

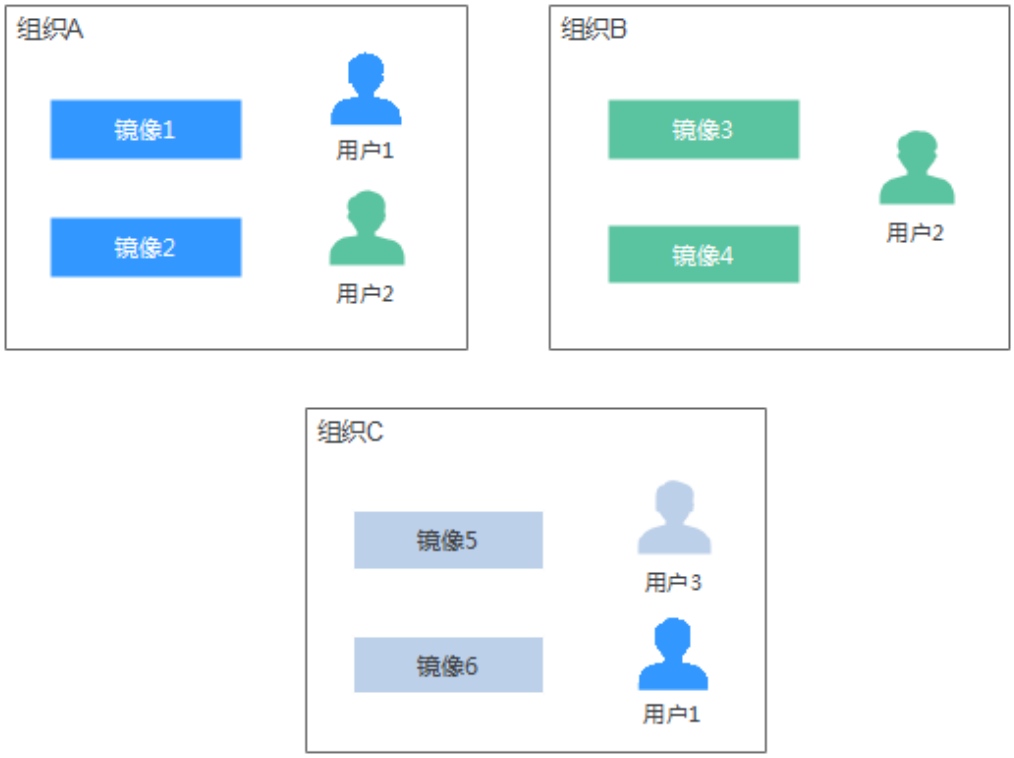

4 组织管理

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4-1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**镜像授权管理**。

图 4-1 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。
- 不允许创建名称为library的组织，该组织为系统预留，请更换一个其他的名称。

----结束

查看组织中的镜像

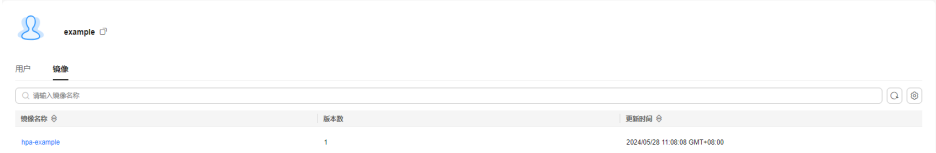
创建组织后，您可以查看当前组织中的镜像。

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

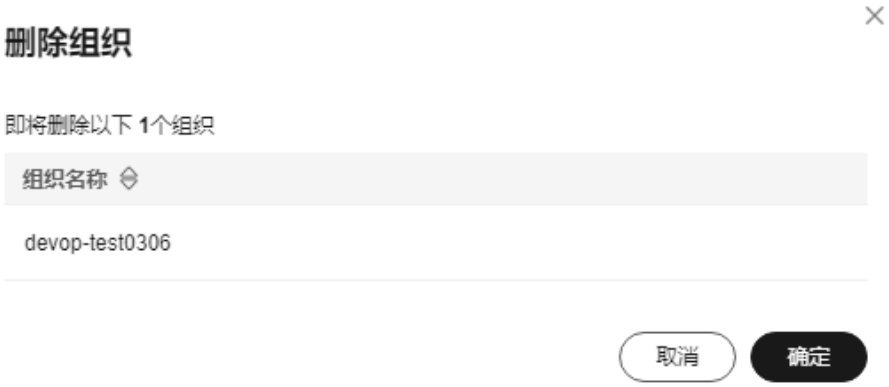
删除组织前，请先删除组织下的所有镜像。

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

5 权限管理

5.1 SWR 权限概述

容器镜像服务SWR的权限管理可以分为三部分。

- **配置IAM权限**：该部分主要介绍如何创建IAM用户并授权使用SWR服务。
- **配置镜像权限**：当您已经有了SWR的管理员用户之后，您可以进一步对其他IAM非管理员用户的镜像访问操作进行授权。可授予读取或编辑或管理权限，这样实现了层级化的更精细的权限管理。
- **SWR控制台的权限依赖**：云上的服务之间往往协同完成某个功能，所以部分功能特性会依赖于其他的服务。SWR的镜像漏洞扫描和触发器功能就是如此，如果想使用这两个功能特性需要具备HSS、CCE或者CCI的权限，详情请参考**SWR控制台的权限依赖**。

5.2 配置 IAM 权限

5.2.1 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。

SWR已经在IAM中预置了**系统角色**和**系统策略**供您使用，如果系统预置的角色和策略无法满足您的需求，您还可以**自定义策略**。

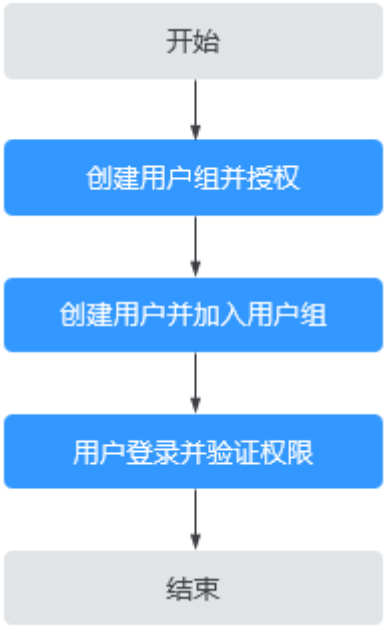
本章节为您介绍对用户授权的方法，操作流程如下图给用户授予SWR权限流程所示。

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 5-1 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 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（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。

系统角色

角色是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

IAM中预置的SWR系统角色为**SWR Admin**，即容器镜像服务(SWR)管理员,拥有该服务下的所有权限。

系统策略

IAM中预置的SWR系统策略当前包含**SWR FullAccess**、**SWR OperateAccess**和**SWR ReadOnlyAccess**三种策略：

- **SWR FullAccess**：系统策略，SWR容器镜像仓库所有权限。
- **SWR OperateAccess**：系统策略，SWR容器镜像仓库操作权限。
- **SWR ReadOnlyAccess**：系统策略，SWR容器镜像仓库只读权限

表 5-1 SWR FullAccess 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限。
	"scm:*:list*"	SCM（SSL证书管理服务）所有资源列表的查看权限。
	"scm:cert:download"	SCM（SSL证书管理服务）证书下载权限。
	"kms:*:get*"	KMS（数据加密服务）所有资源详情的查看权限。
	"kms:*:list*"	KMS（数据加密服务）所有资源列表的查看权限。
	"hss:image:*"	HSS（企业主机安全）容器镜像相关的所有权限。
	"cce:cluster:list*"	CCE（云容器引擎）集群资源列表的查看权限。
	"cci:namespace:list*"	CCI（云容器实例）namespace资源列表的查看权限。
	"cci:deployment:list*"	CCI（云容器实例）deployment资源列表的查看权限。
	"cci:namespaceSubResource:list*"	CCI（云容器实例）kubernetes资源列表的查看权限。
	"cci:deployment:get"	CCI（云容器实例）无状态负载资源详情的查看权限。

操作（Action）	Action详情	说明
	"cci:namespaceSubResource:get"	CCI（云容器实例）kubernetes资源详情的查看权限。

表 5-2 SWR ReadOnlyAccess 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"swr:*:get*"	SWR（云容器镜像）所有资源详情的查看权限。
	"swr:*:list*"	SWR（云容器镜像）所有资源列表的查看权限。
	"swr:*:download*"	SWR（云容器镜像）镜像下载权限。
	"swr:instance:createTempCredential"	SWR（云容器镜像）生成企业仓库临时登录凭证权限。
	"swr:system:createLoginSecret"	SWR（云容器镜像）生成共享仓库临时登录凭证权限。
	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限。
	"scm:*:list*"	SCM（SSL证书管理服务）所有资源列表的查看权限。
	"kms:*:get*"	KMS（数据加密服务）所有资源详情的查看权限。
	"kms:*:list*"	KMS（数据加密服务）所有资源列表的查看权限。
	"hss:image:list*"	HSS（企业主机安全）容器镜像列表的查看权限。
	"hss:image:vulnerabilities"	HSS（企业主机安全）容器镜像漏洞的查看权限。
	"cce:cluster:list*"	CCE（云容器引擎）集群资源列表的查看权限。

操作（Action）	Action详情	说明
	"cci:namespace:list*"	CCI（云容器实例）namespace资源列表的查看权限。
	"cci:deployment:list*"	CCI（云容器实例）deployment资源列表的查看权限。
	"cci:namespaceSubResource:list*"	CCI（云容器实例）kubernetes资源列表的查看权限。
	"cci:deployment:get"	CCI（云容器实例）无状态负载资源详情的查看权限。
	"cci:namespaceSubResource:get"	CCI（云容器实例）kubernetes资源详情的查看权限。

表 5-3 SWR OperateAccess 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"swr:repository:*"	SWR（云容器镜像）企业版仓库管理的所有权限。
	"swr:instance:get*"	SWR（云容器镜像）企业版实例详情的查看权限。
	"swr:instance:list*"	SWR（云容器镜像）企业版实例列表的查看权限。
	"swr:instance:execute*"	SWR（云容器镜像）企业版实例异步任务的的执行权限。
	"swr:instance:createTempCredential"	SWR（云容器镜像）生成企业仓库临时登录凭证权限。
	"swr:system:createLoginSecret"	SWR（云容器镜像）生成共享仓库临时登录凭证权限。
	"swr:repo:*"	SWR（云容器镜像）基础版仓库的所有权限。

操作（Action）	Action详情	说明
	"swr:namespace:get*"	SWR（云容器镜像）基础版命名空间所有资源的查看权限。
	"swr:namespace:list*"	SWR（云容器镜像）基础版命名空间的所有资源的列表权限。
	"swr:system:listQuotas"	SWR（云容器镜像）基础版配额信息的查看权限。
	"swr:system:getDomainOverview"	SWR（云容器镜像）基础版总览信息的查看权限。
	"swr:system:getDomainResourceReports"	SWR（云容器镜像）基础版仓库获取租户资源统计信息的权限。
	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限。
	"scm:*:list*"	SCM（SSL证书管理服务）所有资源列表的查看权限。
	"kms:*:get*"	KMS（数据加密服务）所有资源详情的查看权限。
	"kms:*:list*"	KMS（数据加密服务）所有资源列表的查看权限。
	"hss:image:*"	HSS（企业主机安全）容器镜像相关的所有权限。
	"cce:cluster:list*"	CCE（云容器引擎）集群资源列表的查看权限。

表 5-4 SWRFullAccessPolicy 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限。

操作（Action）	Action详情	说明
	"scm:cert:list"	SCM（SSL证书管理服务）所有证书列表的查看权限。
	"kms:cmk:get"	KMS（数据加密服务）密钥的详细信息的查看权限。
	"kms:cmk:list"	KMS（数据加密服务）密钥的列表信息的查看权限。
	"eps:enterpriseProjects:list"	EPS（企业项目管理服务）企业项目列表列表的查看权限。
	"iam:projects:list"	IAM（统一身份认证服务）项目列表列表的查看权限。

表 5-5 SWRReadOnlyAccessPolicy 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"swr:*:get*"	SWR（云容器镜像）所有资源详情的查看权限。
	"swr:*:list*"	SWR（云容器镜像）所有资源列表的查看权限。
	"swr:*:download*"	SWR（云容器镜像）所有资源列表的下载权限。
	"swr:instance:createTempCredential"	SWR（云容器镜像）企业仓临时登录凭证的生成权限。
	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限。
	"scm:cert:list"	SCM（SSL证书管理服务）所有证书列表的查看权限。
	"kms:cmk:get"	KMS（数据加密服务）密钥的详细信息的查看权限。

操作（Action）	Action详情	说明
	"kms:cmk:list"	KMS（数据加密服务）密钥的列表信息的查看权限。
	"eps:enterpriseProjects:list"	EPS（企业项目管理服务）企业项目列表列表的查看权限。
	"iam:projects:list"	IAM（统一身份认证服务）项目列表列表的查看权限。

表 5-6 SWROperateAccessPolicy 策略主要权限

操作（Action）	Action详情	说明
"swr:*:*"	"swr:*:get*"	SWR（云容器镜像）所有资源详情的查看权限。
	"swr:*:list*"	SWR（云容器镜像）所有资源列表的查看权限。
	"swr:*:download*"	SWR（云容器镜像）所有资源列表的下载权限。
	"swr:instance:createTempCredential"	SWR（云容器镜像）企业仓临时登录凭证的生成权限。
	"swr:repository:*"	SWR（云容器镜像）企业版仓库管理的所有权限。
	"swr:instance:execute*"	SWR（云容器镜像）企业版实例异步任务的的执行权限。
	"vpc:*:get*"	VPC（虚拟私有云）所有资源详情的查看权限。
	"vpc:*:list*"	VPC（虚拟私有云）所有资源列表的查看权限
	"scm:cert:list"	SCM（SSL证书管理服务）所有证书列表的查看权限。
	"kms:cmk:get"	KMS（数据加密服务）密钥的详细信息的查看权限。

操作（Action）	Action详情	说明
	"kms:cmk:list"	KMS（数据加密服务）密钥的列表信息的查看权限。
	"eps:enterpriseProjects:list"	EPS（企业项目管理服务）企业项目列表列表的查看权限。
	"iam:projects:list	IAM（统一身份认证服务）项目列表列表的查看权限。

自定义策略

如果系统预置的SWR策略，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限策略和授权项**。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。

5.2.2 SWR 自定义策略

如果系统预置的SWR权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

  具体创建步骤请参见**创建自定义策略**。本章为您介绍常用的SWR企业版自定义策略样例。

SWR自定义策略样例

- 示例1：授权允许下载镜像

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "swr:repo:download"
      ]
    },
```

```
  {
    "Effect": "Allow",
    "Action": [
      "swr::createLoginSecret"
    ]
  }
 ]
}
```

- 示例2：授权禁止下载镜像

```
{
 "Version": "1.1",
 "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "swr:repo:download"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "swr::createLoginSecret"
    ]
  }
 ]
}
```

示例3：授权允许指定sourcevpc下载

```
{
 "Version": "1.1",
 "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "swr:repo:download"
    ],
    "Condition": {
      "StringEquals": {
        "g:SourceVpc": [
          "0bfdf87b-7789-4851-801e-8e726b82beae"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "swr::createLoginSecret"
    ]
  }
 ]
}
```

5.2.3 SWR 资源

资源是服务中存在的对象。在SWR中，资源包括repo和namespace。您可以在创建自定义策略时，通过指定资源路径来选择特定资源。

表 5-7 SWR 的指定资源与对应路径

指定资源	资源名称	资源路径
repo	镜像仓库	【格式】 SWR:*:*:repo:镜像仓库名称。 其中第一个*是regionid，第二个*是domainid。 【说明】 对于镜像仓库资源，IAM自动生成资源路径前缀SWR:*:*:repo: 通过镜像仓库名称指定具体的资源路径，支持通配符*。例如： swr:*:*:repo:test/nginx*：test组织下，仓库名称以nginx开头的镜像仓库。 swr:*:*:repo:test/nginx：test组织下，仓库名称为nginx的镜像仓库。
namespace	组织	【格式】 SWR:*:*:namespace:组织名称。 其中第一个*是regionid，第二个*是domainid。 【说明】 对于组织资源，IAM自动生成资源路径前缀SWR:*:*:namespace:通过组织名称指定具体的资源路径，支持通配符*。例如： swr:*:*:namespace:test*：名称以test开头的组织。 swr:*:*:namespace:test：名称为test的组织。

5.3 配置镜像权限

5.3.1 镜像授权管理

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。上传镜像需要您拥有镜像的编辑或管理权限，下载私有镜像需要您拥有镜像的读取或编辑或管理权限，下载公开镜像不需要鉴权。

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。

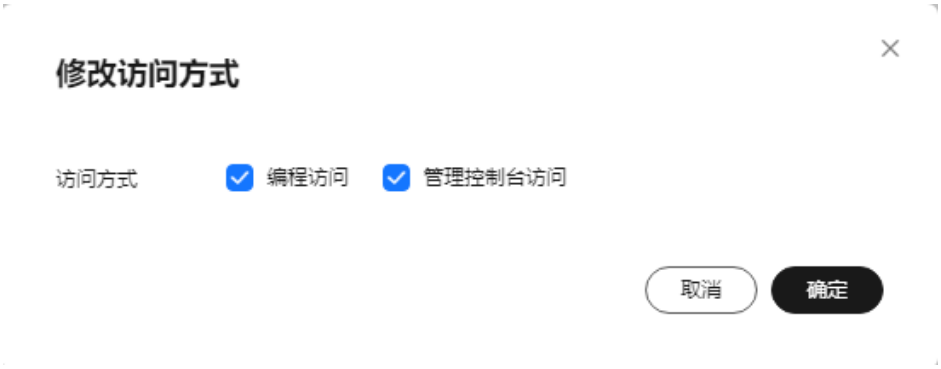
场景示例：

- 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 5-2 修改访问方式示例



约束与限制

联邦用户暂不支持在SWR的控制台进行镜像授权管理，请在IAM控制台添加自定义策略进行镜像授权管理。详情请参见**SWR自定义策略**。

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 5-3 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”。

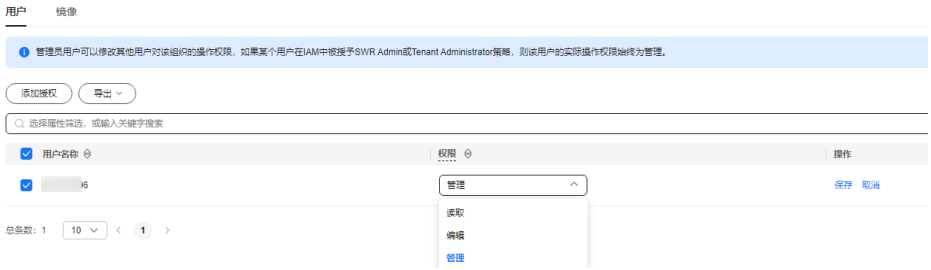
步骤3 在“用户”页签下单击“添加授权”，在弹出的窗口中为IAM用户选择权限，然后单击“确定”。

----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”。

5.4 SWR 控制台的权限依赖

SWR对其他云服务有依赖关系，因此在您开启IAM授权后，在SWR Console控制台的部分功能需要配置相应的服务权限后才能正常查看或使用。

依赖服务的权限配置均基于您已设置了IAM授权的SWR Administrator、SWR FullAccess、SWR OperateAccess或SWR ReadOnlyAccess策略权限。

依赖服务的权限设置

如果IAM用户需要在SWR Console控制台拥有相应功能的查看或使用权限，请确认已经对该用户所在的用户组设置了SWR Administrator、SWR FullAccess、SWR OperateAccess或SWR ReadOnlyAccess策略的权限，再按如下**表5-8**增加依赖服务的角色或策略。

表 5-8 SWR Console 中依赖服务的角色或策略

Console控制台功能	依赖服务	需配置角色/策略
镜像漏洞扫描	企业主机安全 HSS	**SWR HSS Access自定义策略**
触发器	云容器引擎 CCE 云容器实例 CCI	如果您的触发器类型为云容器引擎CCE，则需要配置云容器引擎 **SWR CCE Access自定义策略** 如果您的触发器类型为云容器实例CCI，则需要配置云容器实例 **SWR CCI Access自定义策略**

说明

以下授权操作需要拥有Security Administrator权限的用户手动进行授权。

HSS 细粒度授权操作

步骤1 登录**管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的☰，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤3 选择左侧导航树的“权限管理 > 权限”，单击右上角的“创建自定义策略”。填写策略参数。策略名称为“SWR HSS Access”，策略配置方式选择“JSON视图”。填写策略内容如下，配置完成后单击“确定”。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "HSS:*:*"
         ]
      }
   ]
}
```

步骤4 选择左侧导航树上的“用户组”，选择相应的用户组，单击用户组的授权操作。

步骤5 选择策略SWR HSS Access，选择所有资源，单击确定。

步骤6 显示授权成功后，单击“完成”后等待15分钟授权生效。

----结束

CCE 细粒度授权操作

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤3 选择左侧导航树的“权限管理 > 权限”，单击右上角的“创建自定义策略”。填写策略参数。策略名称为“SWR CCE Access”，策略配置方式选择“JSON视图”。填写策略内容如下，配置完成后单击“确定”。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cce:cluster:list"
      ]
    }
  ]
}
```

步骤4 选择左侧导航树上的“用户组”，选择相应的用户组，单击用户组的授权操作。

步骤5 选择策略SWR CCE Access，选择所有资源，单击确定。

步骤6 显示授权成功后，单击“完成”后等待15分钟授权生效。

步骤7 单击页面左上方的，选择“容器 > 云容器引擎CCE”。选择左侧导航树的“权限管理 ”，然后在集群选择框中选择对应的集群，单击右上角的“添加权限”

步骤8 输入以下参数，单击确定。

- 用户/用户组：选择你要授权的用户所在的用户组
- 命名空间：全部命名空间
- 权限类型：只读权限

步骤9 显示添加权限成功后，单击“确定”等待3到5秒待授权生效。

----结束

CCI 细粒度授权操作

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“管理与监管 > 统一身份认证服务 IAM”。

步骤3 选择左侧导航树的“权限管理 > 权限”，单击右上角的“创建自定义策略”。填写策略参数。策略名称为“SWR CCI Access”，策略配置方式选择“JSON视图”。填写策略内容如下，配置完成后单击“确定”。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
```



```
            "Action": [
              "cci:namespace:list",
              "cci:deployment:list",
              "cci:namespaceSubResource:list",
              "cci:deployment:get",
              "cci:namespaceSubResource:get"
            ]
        }
    ]
}
```

步骤4 选择左侧导航树上的“用户组”，选择相应的用户组，单击用户组的授权操作。

步骤5 选择策略SWR CCI Access，选择所有资源，单击确定。

步骤6 显示授权成功后，单击“完成”后等待15分钟授权生效。

----结束

5.5 SWR 支持的控制策略

5.5.1 控制策略概述

SWR服务支持多种控制策略：IAM权限控制、服务控制策略(SCP)、资源控制策略(RCP)、网络控制策略(NCP)以及通过VPCEP终端节点策略。用户可以根据不同的安全业务诉求，可以使用不同控制策略。

基于IAM的权限控制

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助您安全地控制云服务和资源的访问权限。如何使用IAM服务对SWR进行权限控制请参见**配置IAM权限**。

基于服务控制策略的权限控制

服务控制策略 (Service Control Policy，SCP) 是一种基于组织 Organizations的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。SCP可以关联到组织、OU和成员账号。当SCP关联到组织或OU时，该组织或OU下所有账号均受该策略影响。具体请参考**服务控制策略概述**。

说明

这里的组织是指组织 Organizations服务里面的组织，非容器镜像服务里面的组织。

基于资源控制策略的权限控制

资源控制策略RCP（Resource Control Policies）是组织 Organizations服务中提供的一种护栏控制策略，RCP策略可以限制一个资源所允许的最大权限，访问组织成员账号资源的操作会受到RCP护栏限制。组织管理员可以在组织中设置RCP策略，帮助访问组织成员账号资源时更好地满足业务的安全性和合规性需求。

说明

这里的组织是指组织 Organizations服务里面的组织，非容器镜像服务里面的组织。

基于网络控制策略的权限控制

网络控制策略NCP（Network Control Policies）是组织 Organizations服务中提供的一种护栏控制策略，NCP策略可以限制从一个VPC EP发起访问时所允许的最大权限，

当请求从组织内账号所创建的VPC EP发起访问时会收到NCP护栏限制。组织管理员可以在组织中设置NCP策略，帮助由组织内账号创建的VPC EP发起的访问更好地满足业务的安全性和合规性需求。

说明

这里的组织是指组织 Organizations服务里面的组织，非容器镜像服务里面的组织。

基于VPCEP策略的权限控制

VPC终端节点策略是一种基于资源的策略，您可以附加到VPC终端节点，以控制哪些华为云主体可以使用该终端节点访问华为云云服务。具体请参考**管理终端节点的策略**。

在云环境中，虚拟私有云VPC（Virtual Private Cloud）网络边界控制是一个非常重要的安全管理维度。当一个访问主体请求操作一个资源时，如果目标资源的API访问点是仅存在于账号的VPC内部，而在VPC网络之外不存在访问面，那么可以认为这种访问是发生在一个VPC内部（可以把VPC看作是一个网络安全域），网络攻击面较小，安全性相对可控。但是，当前云上提供的诸多云服务API访问点都是面向互联网开放，网络攻击面较大，安全性相对难控。

说明

配置控制策略后，匿名下载公开镜像也会受控制策略的管控。

5.5.2 服务控制策略(SCP)

本章节以配置示例的方式演示SCP策略如何配置。

配置示例：禁止某账号下载的某个组织下的镜像。

下面以禁止Organizations组织下的账号下载SWR组织为test-namespace，镜像仓库为test-repo内的镜像的场景为例演示如何配置。

配置方法：

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

步骤2 进入策略管理页，依次单击“服务控制策略-创建”，进入SCP创建页面。

步骤3 输入策略名称和策略描述，在策略内容左侧可以复制粘贴如下JSON格式的策略内容。单击“保存”。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "swr:repo:download"
      ],
      "Resource": [
        "swr:*:*:repo:test-namespace/test-repo"
      ]
    }
  ]
}
```

步骤4 把此策略绑定至组织的OU或者账号上，使其生效。这样该账号就无法下载。具体方法如下：

1. 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

2. 选中要绑定SCP的OU或者账号。
3. 在右侧详情页，选择策略页签，展开“服务控制策略”列表，单击列表上方的“绑定”。
4. 在弹窗中选择要添加的策略后，在文本框中输入“确认”，然后单击“绑定”，完成策略绑定。

----结束

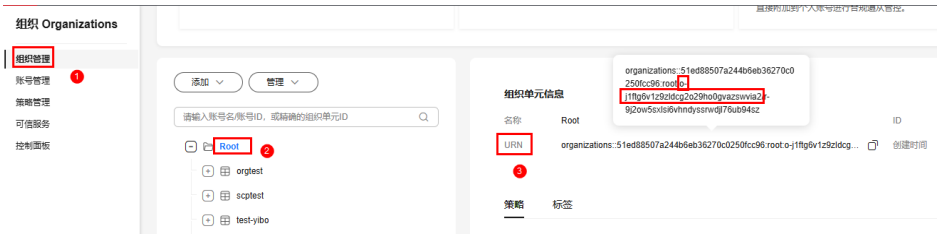
5.5.3 资源控制策略(RCP)

配置示例1：组织内的镜像只能由组织内的账号下载。

下面策略的含义：该策略绑定的OU或账号下的镜像不能被组织外的账号下载。只能由组织(o-j1ftg6v1z9zldcg2o29ho0gvazswvia2)内的账号账号下载。

说明

这里的组织是指组织服务里面的组织，非容器镜像服务里面的组织。该组织的id的获取方法如下：



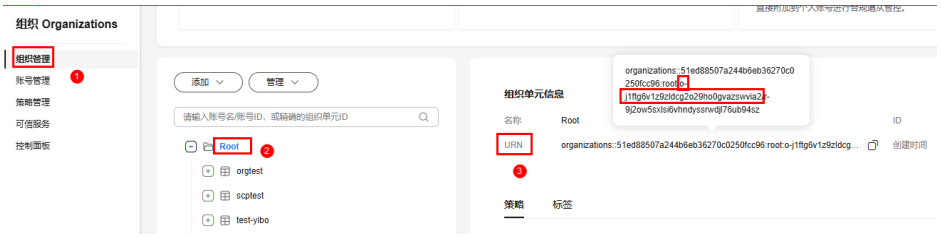

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "swr:repo:download"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "g:PrincipalOrgId": [
            "o-j1ftg6v1z9zldcg2o29ho0gvazswvia2"
          ]
        },
        "Bool": {
          "g:PrincipalIsService": [
            "false"
          ]
        }
      }
    }
  ]
}
```

配置示例2：除了公开镜像，组织内的镜像只能由组织内的账号账号下载。

下面策略的含义：该策略绑定的OU或账号下的私有镜像不能被组织外的账号下载。只能由组织(o-j1ftg6v1z9zldcg2o29ho0gvazswvia2)内的账号下载，公开镜像可以由任何账号账号下载。

说明

这里的组织是指组织服务里面的组织，非容器镜像服务里面的组织。该组织的id的获取方法如下：




```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "swr:repo:download"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "g:PrincipalOrgId": [
            "o-j1ftg6v1z9zldcg2o29ho0gvazswvia2"
          ]
        },
        "Bool": {
          "g:PrincipalIsService": [
            "false"
          ],
          "swr:RepositoryIsPublic": [
            "false"
          ]
        }
      }
    }
  ]
}
```

说明

配置方法同**服务控制策略(SCP)**章节的配置方法。

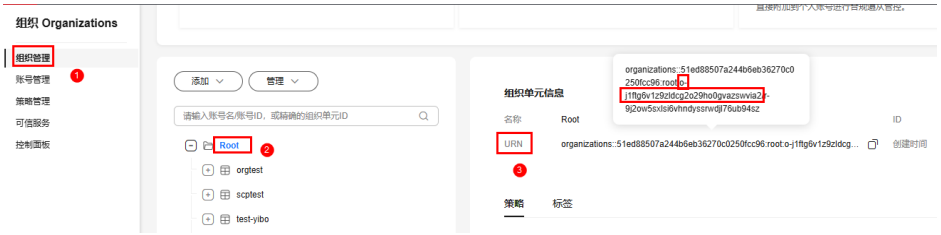
5.5.4 网络控制策略(NCP)

配置示例1：组织内的账号账号通过VPCEP只能下载组织内的私有镜像，可以下载任意公开镜像。

下面策略的含义：通过该策略绑定的OU或账号下的vpcep下载镜像，不允许被组织外的账号下载，只能由组织(o-j1ftg6v1z9zldcg2o29ho0gvazswvia2)内的账号账号下载。

说明

这里的组织是指组织服务里面的组织，非容器镜像服务里面的组织。该组织的id的获取方法如下：



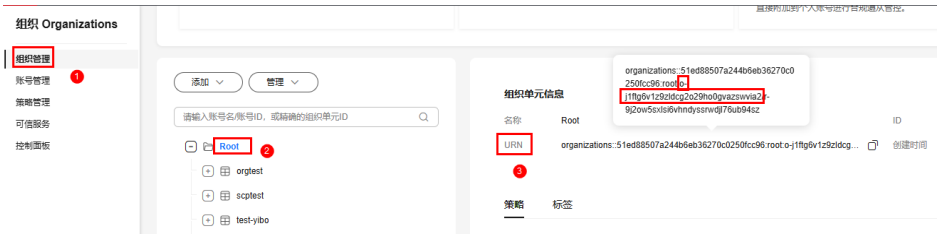

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "swr:repo:download"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Bool": {
          "g:PrincipalIsService": [
            "false"
          ]
        },
        "StringNotEquals": {
          "g:ResourceOrgId": [
            "o-j1ftg6v1z9zldcg2o29ho0gvazswvia2"
          ]
        }
      }
    }
  ]
}
```

配置示例2：组织内的账号账号通过VPCEP只能下载组织内的私有镜像，可以下载任意公开镜像。

下面策略的含义：通过该策略绑定的OU或账号下的vpcep下载镜像，私有镜像不允许被组织外的账号下载，只能由组织(o-j1ftg6v1z9zldcg2o29ho0gvazswvia2)内的账号账号下载，公开镜像可以由任何账号账号下载。

说明

这里的组织是指组织服务里面的组织，非容器镜像服务里面的组织。该组织的id的获取方法如下：




```
{
  "Version": "5.0",
  "Statement": [
    {
```

```
    "Effect": "Deny",
    "Principal": "*",
    "Action": [
      "swr:repo:download"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "Bool": {
        "g:PrincipalIsService": [
          "false"
        ],
        "swr:RepositoryIsPublic": [
          "false"
        ]
      },
      "StringNotEquals": {
        "g:ResourceOrgId": [
          "o-j1ftg6v1z9zldcg2o29ho0gvazswvia2"
        ]
      }
    }
  }
 ]
}
```

说明

配置方法同**服务控制策略(SCP)**章节的配置方法。

5.5.5 VPC 终端节点策略

SWR基础版可以通过VPC终端节点上传下载镜像，VPC终端节点支持配置策略，可以配置策略管控镜像的上传或者下载。创建VPC终端节点步骤请参见**通过VPCEP方式访问SWR**。配置VPC终端节点策略步骤请参见**管理终端节点的策略**。

配置示例1：配置VPC终端节点策略，只允许上传下载指定的镜像。

下面策略的含义：VPC1内的服务器只能上传下载SWR中组织为test-namespace、镜像仓库为test-repo下的镜像。

```
{
 "Version": "5.0",
 "Statement": [
  {
    "Action": [
      "swr:repo:upload",
      "swr:repo:download"
    ],
    "Resource": [
      "swr:*:*:repo:test-namespace/test-repo"
    ],
    "Effect": "Allow",
    "Principal": "*"
  }
 ]
}
```

配置示例2：配置VPC终端节点策略，只允许下载指定的私有镜像，可以下载所有的公开镜像。

下面策略的含义：VPC1内的服务器只能下载SWR中组织为test-namespace、镜像仓库为test-repo，公开镜像不受限制。

```
{
 "Version": "5.0",
```

```
 "Statement": [
  {
    "Action": [
      "swr:repo:download"
    ],
    "Resource": [
      "swr:*:*:repo:test-namespace/test-repo"
    ],
    "Effect": "Allow",
    "Principal": "*"
  },
  {
    "Action": [
      "swr:repo:download"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow",
    "Principal": "*",
    "Condition": {
      "Bool": {
        "swr:RepositoryIsPublic": [
          "true"
        ]
      }
    }
  }
 ]
}
```

6 镜像管理

6.1 镜像管理概述

容器镜像服务提供了一个免费的共享镜像仓库供您使用。镜像仓库针对您的镜像可提供全生命周期的镜像管理。

- **推送镜像**：推送镜像（也叫上传镜像），可以帮助您将本地的镜像推送到容器镜像服务的镜像仓库中，更方便地管理您的镜像。推送镜像到镜像仓库有两种方式：通过容器引擎客户端上传和通过SWR页面上传。容器引擎客户端目前支持**docker**容器引擎以及**containerd**容器引擎。
- **拉取镜像**：拉取镜像（也叫下载镜像），当您需要使用镜像仓库中的镜像时，您需要从镜像仓库拉取镜像。常搭配华为云产品云容器引擎CCE部署工作负载或者云容器实例CCI部署实例使用。
- **登录/连接镜像仓库**：使用容器引擎客户端推送或者拉取镜像时，需要先连接上镜像仓库。连接镜像仓库有临时登录指令和长期登录指令。
- **编辑镜像**：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。
- **共享镜像**：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。
- **镜像触发器**：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。
- **镜像老化**：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按照镜像存活时间和保留镜像版本数目两种老化处理规则，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。
- **镜像同步**：镜像上传后，您可以使用镜像同步功能帮助您把最新推送的镜像版本同步到其他区域镜像仓库内。支持自动同步和手动同步两种方式。
- **镜像漏洞扫描**：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。
- **镜像中心**：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。

- **设置镜像加速器**：由于运营商网络原因，会导致您拉取第三方镜像仓库的镜像(例如Docker Hub)变慢甚至下载失败。华为云容器镜像服务提供了镜像下载加速功能，对部分常用的开源镜像下载进行加速。

6.2 推送镜像到镜像仓库

操作场景

推送镜像（也叫上传镜像），可以帮助您将本地的镜像推送到容器镜像服务的镜像仓库中，更方便地管理您的镜像。推送镜像到镜像仓库有两种方式：通过容器镜像客户端上传和通过SWR页面上传。

- 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命令或者ctr命令将镜像上传到容器镜像服务的镜像仓库。如果是**docker**容器引擎客户端则使用docker push命令上传。如果是**containerd**容器引擎客户端则使用ctr push命令上传。适用于大镜像的上传。

  说明

  容器引擎客户端推送镜像既可走内网链路也可走外网链路。详情请参见**配置访问网络**。
- SWR页面上传镜像，是指直接通过SWR控制台页面将镜像上传到容器镜像服务的镜像仓库。适用于小镜像的上传。

前提条件

- 已创建组织，请参见**创建组织**。
- 已准备好容器引擎客户端。
- 使用页面上传镜像时请确保镜像已保存为tar或tar.gz文件，具体请参见**制作镜像压缩包**。

约束与限制

- 使用docker容器引擎客户端上传镜像时，需确保docker容器引擎客户端必须为18.06及以上的版本；
- 镜像的每个layer大小不能超过10G；
- 单个租户同时并发上传镜像layer总数不大于20个。
- 页面上传每次最多上传10个文件，单个文件大小（含解压后）不得超过2G。且仅支持上传18.06及以上的版本Docker容器引擎客户端制作的镜像压缩包。
- 单个租户可推送的镜像配额为500个，镜像版本配额为300个。超过配额将会推送失败。

推送镜像到镜像仓库

- 小镜像可以使用页面上传镜像，暂不支持断点续传。大镜像推荐使用客户端上传。
- SWR对存储的镜像数量有配额限制，请及时老化不再使用的镜像。

容器引擎客户端推送镜像（推荐）

docker容器引擎客户端

1. **制作容器镜像**或**导入镜像文件**
2. 连接容器镜像服务。
   a. 登录**容器镜像服务控制台**。
   b. 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 6-1 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**获取长期有效登录或推拉镜像指令**。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。
      - 临时登录指令过期后需清除浏览器缓存后重新生成登录指令。
      - 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。

   c. 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”。
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**2.b**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
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。

containerd容器引擎客户端

1. 登录**容器镜像服务控制台**。
2. 在左侧导航栏选择“我的镜像”，单击右侧镜像名称。
3. 在镜像详情页面中，进入“Pull/Push指南”页签，复制containerd容器引擎的镜像上传指令。

   说明

   该指令将于6个小时后过期。若需要长期有效的上传指令，请参见**获取containerd容器引擎通用型登录指令之长期有效的拉取、推送镜像指令**。
4. 以root用户登录containerd引擎所在的虚拟机。
5. 在虚拟机中执行**3**复制的镜像上传指令。

6. 检查镜像是否上传成功。

说明

- 如果上传的镜像达到配额，不能上传新的镜像，但是存量镜像如果镜像版本没有超过配额仍可继续上传。
- 如果上传的某个镜像版本达到配额，则该镜像不能继续上传，其他镜像不受影响。
- 并发推送镜像或镜像版本时，可能存在推送成功的镜像或镜像版本超过配额的场景。此时需先删除所有超出配额的镜像或镜像版本，然后删除镜像或镜像版本才能释放出可用配额。

常见问题

为什么使用客户端上传镜像失败?

推送镜像其他问题

页面上传镜像

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 6-2 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

说明

- 如果上传的镜像达到配额，不能上传新的镜像，但是存量镜像如果镜像版本没有超过配额仍可继续上传。
- 如果上传的某个镜像版本达到配额，则该镜像不能继续上传，其他镜像不受影响。
- 并发推送镜像或镜像版本时，可能存在推送成功的镜像或镜像版本超过配额的场景。此时需先删除所有超出配额的镜像或镜像版本，然后删除镜像或镜像版本才能释放出可用配额。

常见问题

为什么通过页面上传镜像失败?

推送镜像其他问题

6.3 获取长期有效登录或推拉镜像指令

操作场景

使用容器引擎客户端推送或者拉取镜像时，连接镜像仓库有临时登录指令和长期登录指令。

- 如果您使用的是Docker容器引擎客户端，且需要长期推送或者拉取镜像，那么您可以使用**获取docker容器引擎长期有效登录指令**来登录容器镜像仓库。如果您只是偶尔推送或者拉取镜像，使用临时登录指令即可。
- 如果您使用的是containerd容器引擎客户端，且需要长期推送或者拉取镜像，那么您可以使用**获取containerd容器引擎长期有效的拉取、推送镜像指令**来访问容器镜像仓库。

⚠ 注意

Docker容器的长期登录指令以及containerd容器的长期推送/拉取指令，请您务必妥善保管，防止信息泄露。

具体差异请参见**长期有效的登录指令与临时登录指令的区别是什么?**

本章节介绍如何获取docker容器引擎长期有效的登录指令以及containerd容器引擎长期推送、拉取镜像指令，长期有效登录指令的有效期为永久。

说明

临时登录指令6小时后会过期。提示过期后，需要清除浏览器缓存后重新生成登录指令。

为了与IAM新平面更好的兼容，新增了增强型指令，为了于区分以前的指令现叫做通用型指令。增强型指令简化了权限控制，去掉了冗余的SWR自有的镜像权限控制，完全支持IAM的权限控制并，更方便用户对镜像上传、下载的控制。两者的详细区别请参见**下表**:

表 6-1 通用型指令和增强型指令对比

差异	通用型登录指令	增强型登录指令
适用范围	无限制	开启了IAM新平面才支持，适用使用IAM新平面进行权限控制的场景
指令有效期	支持临时登录指令和长期登录指令，具体差异请参见**长期有效的登录指令与临时登录指令的区别是什么?**	为了安全考虑，不再支持长期登录指令，仅支持临时登录指令，其有效期为24小时。

差异	通用型登录指令	增强型登录指令
权限控制	支持IAM权限管理，详细内容请参见**配置IAM权限** 支持SWR自有的镜像权限控制（即本地授权），详细内容请参见**配置镜像权限**	仅支持IAM权限管理，详细内容请参见**配置IAM权限**。 增强型登录指令对iam条件键支持做了增强，请参见**下表**。
是否对接审计日志	是	是
支持的条件键	见**下表**	见**下表**

表 6-2 通用型登录指令与增强型登录指令对上传下载的 IAM 的条件键的支持不同

条件键名称	通用型登录指令是否支持		增强型临时登录指令是否支持
	临时登录指令	长期有效登录指令	
g:CalledVia	否	否	否
g:CalledViaFirst	否	否	否
g:CalledViaLast	否	否	否
g:PrincipalTag/tag-key	否	否	是
g:MFAAge	否	否	是
g:MFAPresent	否	否	是
g:SourceIdentity	否	否	是
g:TokenIssueTime	否	否	是
g:ViaService	否	否	是
g:DomainId	是	否	是
g:DomainName	是	否	是
g:PrincipalAccount	是	是	是
g:PrincipalUrn	是	是	是
g:PrincipalIsService	是	是	是
g:PrincipalIsRootUser	是	是	是
g:PrincipalServiceName	是	否	是

条件键名称	通用型登录指令是否支持		增强型临时登录指令是否支持
	临时登录指令	长期有效登录指令	
g:PrincipalType	是	是	是
g:PrincipalId	是	是	是
g:UserName	是	是	是
g:UserId	是	是	是
g:PrincipalOrgPath	是	是	是
g:PrincipalOrgId	是	是	是
g:PrincipalOrgManagementAccountId	是	是	是
g:ResourceOrgId	是	是	是
g:ResourceOrgPath	是	是	是
g:Referer	是	是	是
g:SecureTransport	是	是	是
g:SourceIp	是	是	是
g:SourceVpc	是	是	是
g:SourceVpce	是	是	是
g:UserAgent	是	是	是
g:RequestedRegion	是	是	是
g:RequestTag/tag-key	否	否	否
g:ResourceAccount	是	是	是
g:ResourceTag/tag-key	否	否	否
g:TagKeys	否	否	否
g:EnterpriseProjectId	否	否	否
g:SourceAccount	否	否	否
g:SourceUrn	否	否	否

条件键名称	通用型登录指令是否支持		增强型临时登录指令是否支持
	临时登录指令	长期有效登录指令	
g:CurrentTime	是	是	是

获取方式

下面来介绍如何获取docker容器引擎长期有效登录指令和获取containerd容器引擎长期有效的拉取、推送镜像指令的详细操作。

获取 docker 容器引擎通用型登录指令之长期有效登录指令

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。
5. 单击用户名称，进入用户详情页。单击“访问方式”后面的按钮。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 6-3 修改访问方式

步骤2 获取AK/SK访问密钥。(如果当前用户已获取AK/SK访问密钥，请忽略此步骤)

说明

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**。

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”。
5. 下载成功后，在“credentials.csv”文件中即可获取AK和SK信息。

表 6-3 *credentials.csv 文件示例*

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

说明

每个访问密钥文件仅能下载一次，请妥善保管。

步骤3 登录**容器镜像服务控制台**。

步骤4 依次单击页面的“登录指令->长期有效登录指令->导入访问密钥”，选择访问密钥文件credentials.csv或者手动输入***步骤2***中获取的 credentials.csv文件中的*Access Key Id*和*Secret Access Key*，单击“生成指令”后会自动生成长期有效的登录指令。到此获取完成，后面的步骤您无需执行。如果您的控制台的页面暂无长期有效登录指令页签，请跳过本步骤参考后面的步骤完成手动拼接长期有效登录指令。

步骤5 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 6-4 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 6-5 区域与项目

项目列表

项目ID	项目	所属区域
050b1255df800f572f8cc01f3740bed5	cn-north-1	华北-北京一
0574965613802674 2fecc01f996391ca	cn-north-4	华北-北京四
06fa03d01480252e2f86c01fffec3424	cn-east-3	华东-上海一
0574969f538026802f6bc01fdc762b9f	cn-east-2	华东-上海二
057496aa378010e62f1bc01f7ab9a012	cn-south-1	华南-广州
0573404491000f602fdac01fc170f683	cn-southwest-2	西南-贵阳一

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6 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2 *credentials文件*的*Access Key Id*，SK替换为2 *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7 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5**中获取，AK在**步骤2**中获取，登录密钥为**步骤6**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8 （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9 （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

获取 containerd 容器引擎通用型登录指令之长期有效的拉取、推送镜像指令

步骤1 已拥有编程访问权限。获取编程访问权限方式如下：

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。
5. 单击用户名称，进入用户详情页。单击“访问方式”后面的按钮。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 6-6 修改访问方式

步骤2 已获取AK/SK访问密钥，获取方式如下：

说明

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**。

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”。
5. 下载成功后，在“credentials.csv”文件中即可获取AK和SK信息。

表 6-4 *credentials.csv 文件示例*

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

说明

每个访问密钥文件仅能下载一次，请妥善保管。

步骤3 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 6-7 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 6-8 区域与项目

项目列表

	项目ID	项目	所属区域
⊞	050b1255df800f572f8cc01f3740bed5	cn-north-1	华北-北京一
	0574965138026742fecc01f996391ca	cn-north-4	华北-北京四
	06fa03d01480252e2f86c01fffec3424	cn-east-3	华东-上海一
	0574969f538026802f6bc01fdc762b9f	cn-east-2	华东-上海二
	057496aa378010e62f1bc01f7ab9a012	cn-south-1	华南-广州
	0573404491000f602fdac01fc170f683	cn-southwest-2	西南-贵阳一

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2****credentials.csv文件*的*Access Key Id*，**SK**替换为***步骤2****credentials.csv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长期拉取和推送镜像的指令。

1. 镜像拉取指令拼接

ctr image pull --user [项目名]@[*AK*]:[*登录密钥*] [*镜像仓库地址*]/{组织名称}/{镜像名称}:{版本名称}

其中，项目名和镜像仓库地址在**步骤3**中获取，AK*步骤2中获取的credentials.csv文件中的Access Key Id字段*，登录密钥为**步骤4**的执行结果。

2. 镜像推送指令拼接

ctr image push --user [项目名]@[*AK*]:[*登录密钥*] [*镜像仓库地址*]/{组织名称}/{镜像名称}:{版本名称}

其中，项目名和镜像仓库地址在**步骤3**中获取，AK*步骤2中获取的credentials.csv文件中的Access Key Id字段*，登录密钥为**步骤4**的执行结果。

说明

- 登录密钥字符串是经过加密的，无法将登录密钥字符串逆向解密成SK。
- 获取的指令可在其他机器上使用并进行镜像上传下载。

----结束

6.4 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。
- Docker容器引擎仅支持上传18.06及以上版本Docker容器引擎客户端制作的镜像压缩包。
- 单个租户可推送的镜像配额为500个，镜像版本配额为300个。超过配额将会上传失败。

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 6-9 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

说明

- 如果上传的镜像达到配额，不能上传新的镜像，但是存量镜像如果镜像版本没有超过配额仍可继续上传。
- 如果上传的某个镜像版本达到配额，则该镜像不能继续上传，其他镜像不受影响。
- 并发推送镜像或镜像版本时，可能存在推送成功的镜像或镜像版本超过配额的场景。此时需先删除所有超出配额的镜像或镜像版本，然后删除镜像或镜像版本才能释放出可用配额。

常见问题

为什么通过页面上传镜像失败?

6.5 拉取镜像到本地

操作场景

当您需要使用镜像仓库中的镜像时，您需要从镜像仓库拉取镜像。常搭配华为云产品云容器引擎CCE部署工作负载或者云容器实例CCI部署实例使用。拉取镜像也叫下载镜像。镜像类型有公开和私有两种。

- 公开镜像所有用户（即所有账户下的所有用户）默认都能下载。为了进一步提升镜像管理的安全性，SWR也支持对公开镜像的下载进行权限控制，可通过**相关控制策略**进行控制。
- 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**。

您可以使用Docker容器引擎也可以使用containerd容器引擎下载容器镜像服务中的镜像。

前提条件

- 在拉取镜像前，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**。
- IAM用户创建后，在拉取镜像前，请联系管理员为您添加对应组织权限，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**。
- “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）。

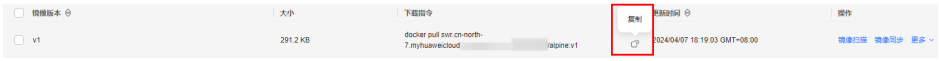
拉取“我的镜像”

您可以使用docker容器引擎也可以使用containerd容器引擎拉取容器镜像服务中的镜像。

docker容器引擎

1. 以root用户登录容器引擎所在的虚拟机。
2. 参考**容器引擎客户端推送镜像（推荐）**获取登录访问权限，连接容器镜像服务。
3. 登录**容器镜像服务控制台**。
4. 在左侧导航栏选择“我的镜像”，单击右侧镜像名称。
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 6-10 获取镜像下载指令

6. 在虚拟机中执行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.*******.*******.com/group/nginx         v2.0.0    22f2bf2e2b4f   5 hours ago     22.8MB
   ```

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**

containerd容器引擎

1. 登录**容器镜像服务控制台**。
2. 在左侧导航栏选择“我的镜像”，单击右侧镜像名称。

3. 在镜像详情页面中，复制操作列的“containerd指令”或者进入“Pull/Push指南”页签，复制containerd容器引擎的镜像下载指令。

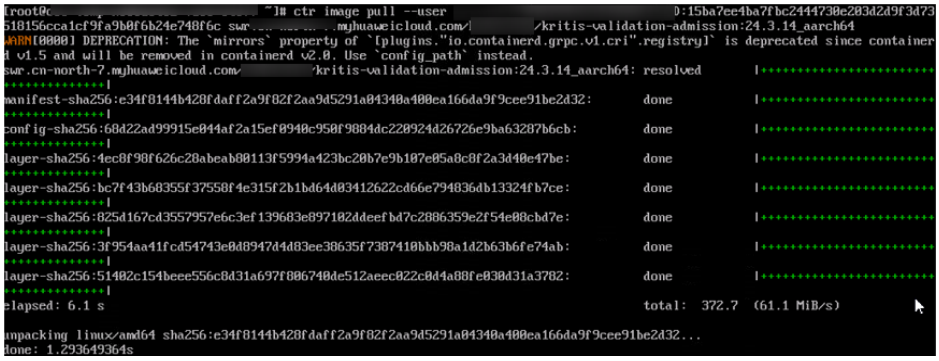
   说明

   该指令将于6个小时后过期。若需要长期有效的下载指令，请参见**获取containerd容器引擎通用型登录指令之长期有效的拉取、推送镜像指令**。

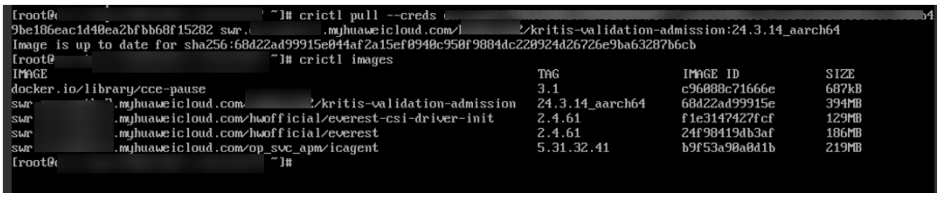
4. 以root用户登录containerd引擎所在的虚拟机。
5. 在虚拟机中执行**3**复制的镜像拉取指令。
   - 复制操作列的“containerd指令”的场景下执行：

   - 复制“Pull/Push指南”页签containerd容器指令的场景下执行：

6. 查看镜像是否拉取成功。
   - 复制操作列的“containerd指令”的场景下使用**crictl images** 命令查看是否拉取成功。

   - 复制“Pull/Push指南”页签containerd容器下载指令的场景下使用**ctr images list**命令查看是否拉取成功。

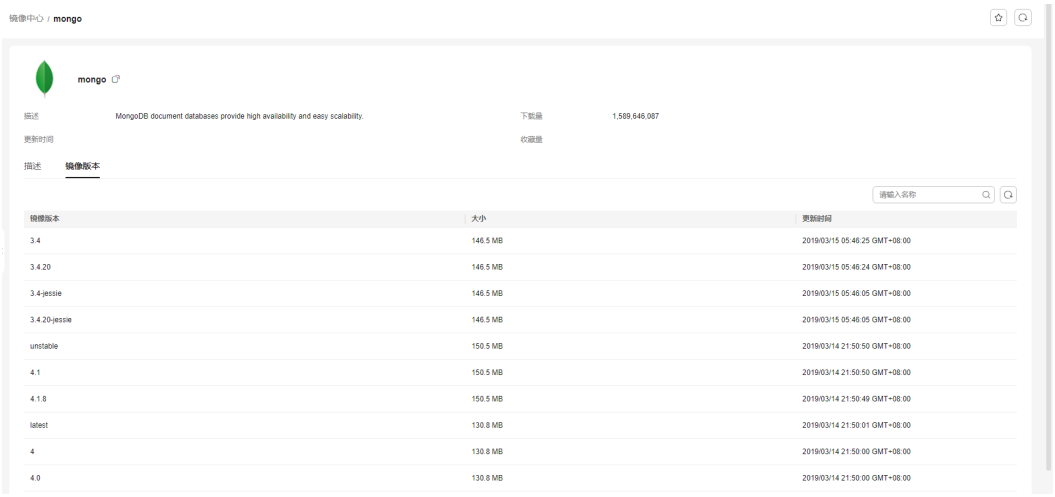
     

拉取镜像中心的镜像

镜像中心的镜像可直接拉取，无需添加仓库地址。如**图6-11**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拉取。

docker pull mongo:*4.1*

图 6-11 mongo 镜像详情示例



常见问题

下载镜像中心的镜像偶发失败，详情请参见**国内网络访问 DockerHub 镜像仓库异常通知**

6.6 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（即所有账户下的所有用户）都能下载，为了进一步提升镜像管理的安全性，SWR也支持对公开镜像的下载进行权限控制，可通过**相关控制策略**进行控制。

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 6-12 编辑镜像属性

表 6-5 编辑镜像

参数	说明
所属组织	镜像所属组织。
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。

参数	说明
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

6.7 将私有镜像共享给其他账号

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6-6**填写相关参数，然后单击“确定”。

图 6-13 共享镜像

表 6-6 共享镜像

参数	说明
共享给	账号名。
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。

说明

您也可以在“我的镜像-自有镜像”页面勾选多个镜像后单击“批量共享”按钮进行批量共享。

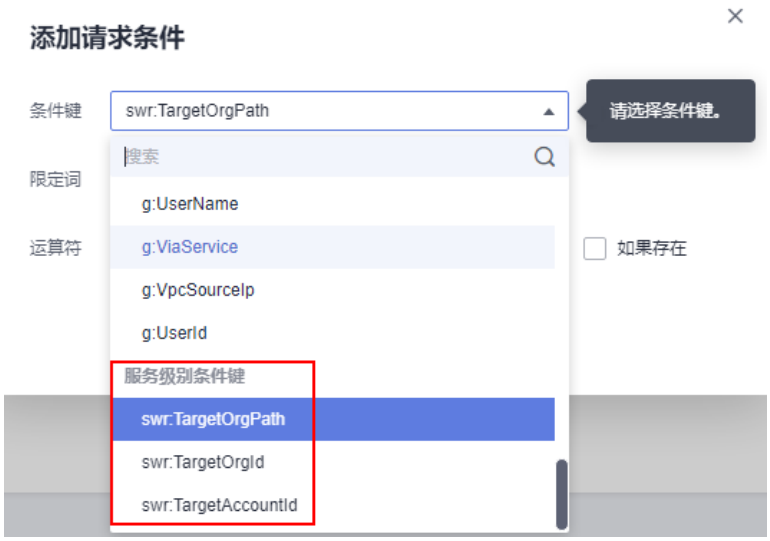
----结束

共享范围约束

将目标账号的OrgID或者OrgPath作为访问控制的条件，组织管理员即可通过SCP强制访问控制策略来约束组织内的共享共享范围，保证数据安全，防止数据泄露。

具体创建步骤请参见：**创建策略**。

图 6-14 添加请求条件



说明

- 策略内容：授予基础版仓库创建镜像共享规则的权限（swr:repo:createRepoShare）。
- 条件键：
  - swr:TargetOrgPath：按照共享目标账号所处的组织路径进行权限控制。
  - swr:TargetOrgId：按照共享目标账号所处的组织Id进行权限控制。
  - swr:TargetAccountId：按照共享目标账号Id进行权限控制。

6.8 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

- 用户需具备CCE或CCI相关权限，详细操作请参见**CCE细粒度授权操作 CCI细粒度授权操作**。

  说明

  在使用云容器引擎CCE或者云容器实例CCI进行镜像扫描时会根据其收费策略进行收费，CCE收费策略详见**CCE计费概述**，

  CCI收费策略详见**CCI计费概述**。

- 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6-7**填写相关参数，然后单击“确定”。

图 6-15 *添加触发器*

表 6-7 触发器

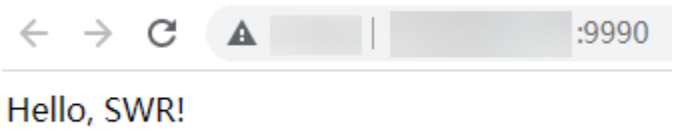
参数	说明
触发器名称	自定义触发器的名称。 字母开头，由字母、数字、下划线_、中划线-组成，下划线、中划线不能连续且不能作为结尾，1-64个字符。

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。 ● 全部触发：有新的镜像版本生成时，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。

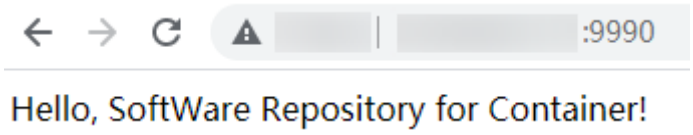
2. Nginx镜像新增一个v2版本，该版本的欢迎页面为“Hello, SoftWare Repository for Container!”。

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”。

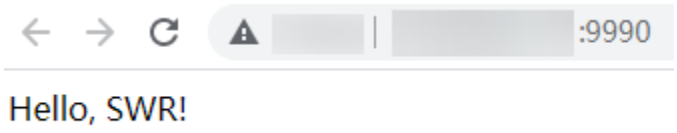
图 6-16 触发结果

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。

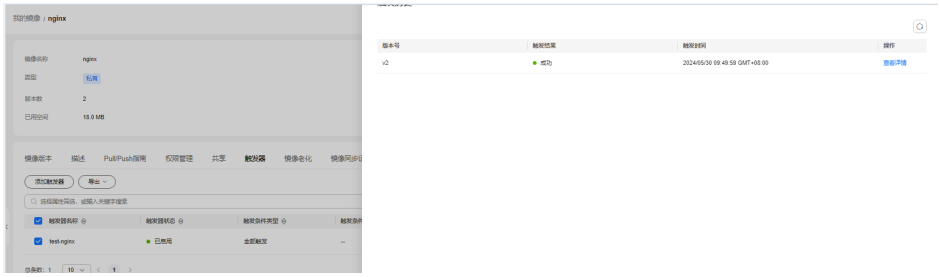
2. Nginx镜像新增一个v1版本，该版本的欢迎页面为“Hello, SWR! (v1)”。

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6-17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 6-17 触发结果示例



   工作负载的访问页面已变更为“Hello, SWR! (v2)”。

6.9 镜像老化

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。
- 镜像老化日志中只能查看近3个月以内的老化日志。

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6-8**填写相关参数，然后单击“确定”。

图 6-18 创建老化规则

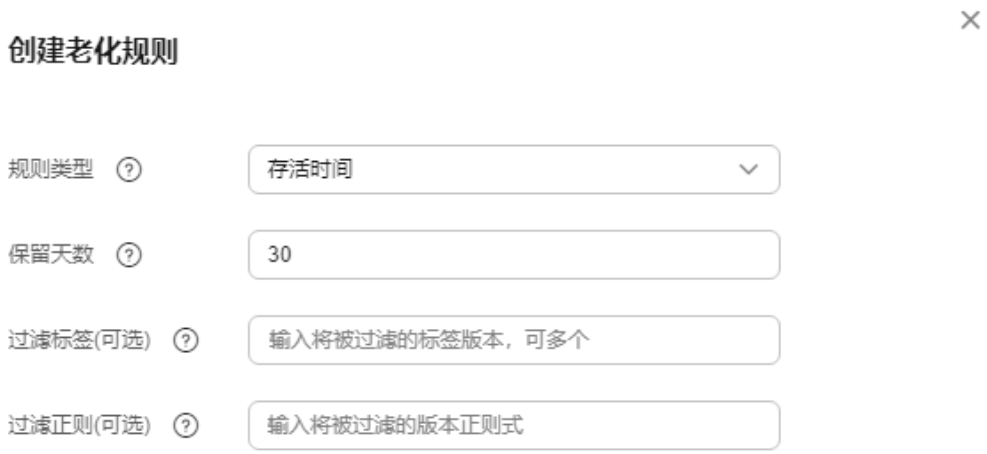


表 6-8 添加镜像老化规则

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。

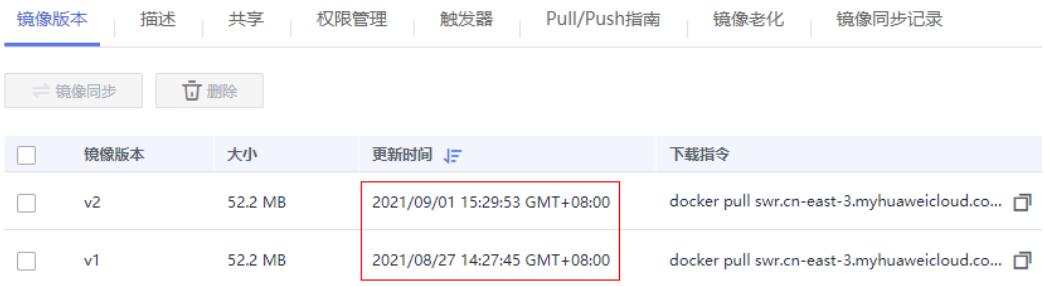
图 6-19 查看规则列表和老化日志

----结束

示例 1：规则类型为“存活时间”

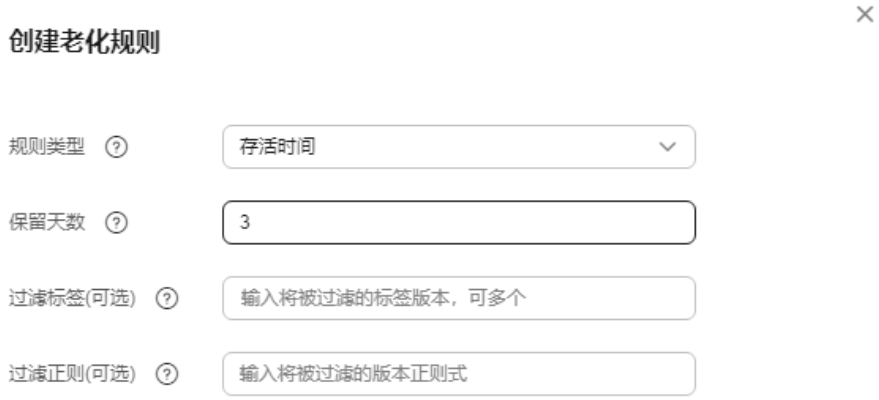
假设“nginx”镜像包含两个版本：v1和v2，更新时间如下图：

图 6-20 镜像版本



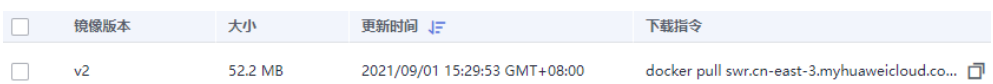
1. 添加老化规则。
   规则类型为“存活时间”，保留天数为“3”。

   图 6-21 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 6-22 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”

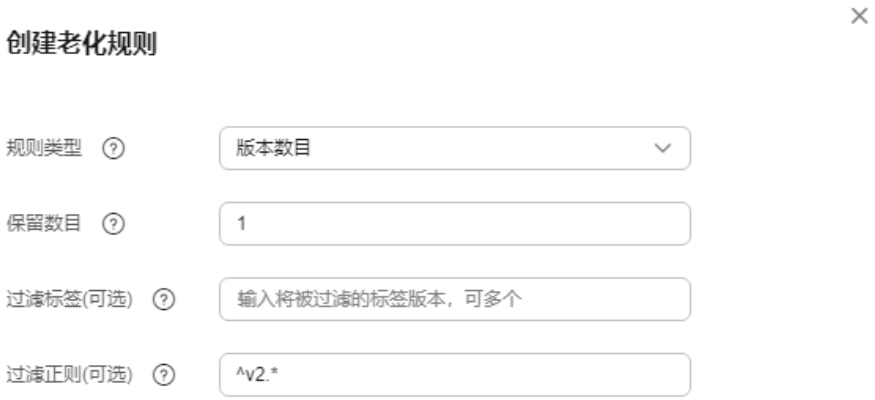
假设“nginx”镜像包含四个版本：v1、v2、v1.0.0、v2.0.0，如下图：

图 6-23 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 6-24 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 6-25 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.*)。

6.10 将镜像同步到其他区域

操作场景

镜像上传后，您可以使用镜像同步功能帮助您把最新推送的镜像版本同步到其他区域镜像仓库内。支持自动同步和手动同步两种方式。自动同步又支持单个镜像自动同步和多个镜像批量自动同步。

表 6-9 镜像同步的两种类型对比

镜像同步类型	自动同步	手动同步
适用范围	适用于后期镜像频繁有更新的场景。 已有的镜像不支持自动同步。	适用于后期不频繁更新，偶尔执行一两次的场景。 已有镜像支持手动同步。
执行时机	镜像有更新时自动触发	任何时候，单击“镜像同步”即触发。

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。
- 单个租户可推送的镜像配额为500个，镜像版本配额为300个。超过配额将会推送失败。
- 目前支持跨区域同步镜像的局点有：“华北-北京一”、“华北-北京四”、“华北-乌兰察布一”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”、“中国-香港”、“亚太-曼谷”、“亚太-新加坡”、“亚太-雅加达”、“非洲-约翰内斯堡”区域同步镜像。

单个镜像自动同步

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 6-26 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

批量镜像自动同步

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”，勾选要同步的镜像，单击“批量自动同步”按钮。

注意

单次可同步的镜像不能超过50个。

步骤3 在右侧滑出的窗口中确认待同步的镜像无误后，选择要同步的目标区域和目标组织，最后选择是否覆盖镜像，单击确定。

步骤4 单击镜像名称进入镜像详情页面，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。

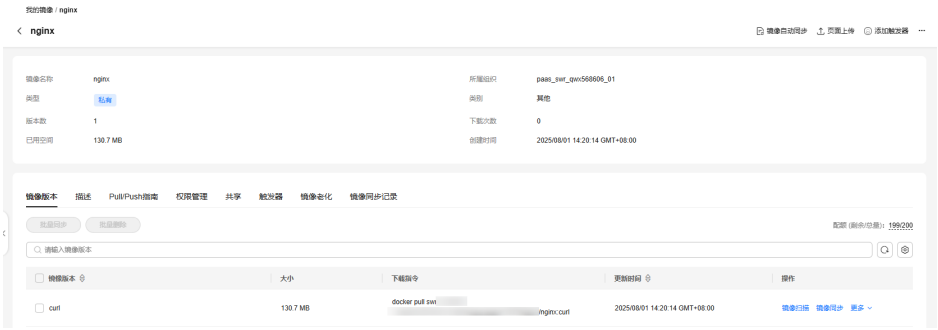
----结束

镜像手动同步

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”，单击要同步的镜像名称进入镜像详情页面。

步骤3 单击要同步的镜像版本操作列的“镜像同步”。并设置要同步到的目标区域和目标组织，最后选择是否覆盖镜像，单击确定。



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、同步耗时等。

----结束

镜像同步失败常见原因

表 6-10 镜像同步失败问题汇总

状态	可能原因	解决方案
失败	• 区域间管理面节点网络问题，导致镜像同步失败 • 目标仓库可推送的镜像配额超限。	• 请联系运维工程师确认网络是否存在异常 • **提交工单**申请增加配额。 • 请稍后重试
失败：同步超时	区域间管理面节点网络问题，导致镜像同步超时	• 请联系运维工程师确认网络是否存在异常 • 请稍后重试
失败：镜像已存在	镜像同步时“覆盖镜像”选项未勾选，而目标区域和组织已经存在同名的镜像	• 如果无需覆盖，无需处理，忽略此条记录即可 • 如果需要覆盖，需要删除同步规则，重新创建一个勾选“覆盖镜像”的同步规则

6.11 镜像漏洞扫描

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”，“华北-北京四”，“华东-上海一”，“华东-上海二”，“华南-广州”区域。
- 用户需具备企业主机安全HSS相关权限，详细操作请参见**HSS细粒度授权操作**。

  说明

  在使用企业主机安全HSS进行镜像扫描时会根据其收费策略进行收费，HSS收费策略详见**HSS计费概述**。
- 多架构镜像不支持镜像扫描。

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

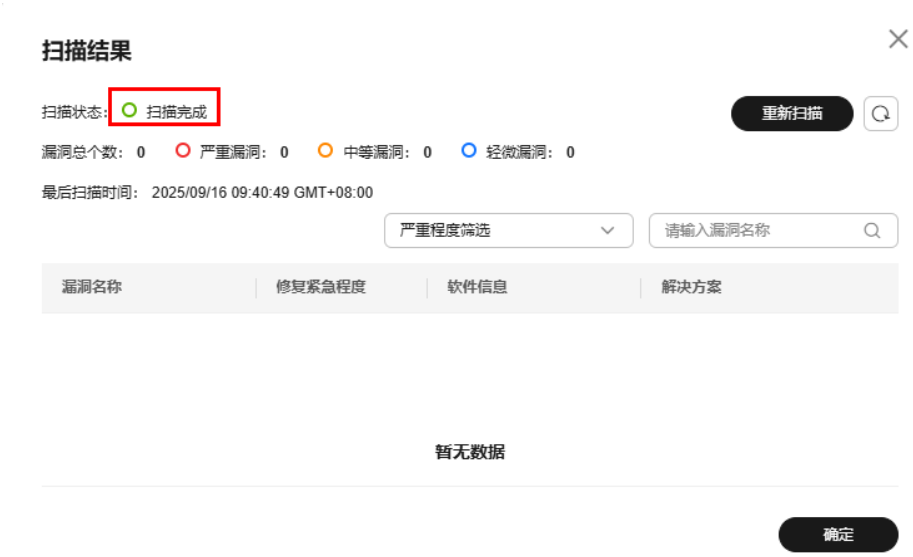
在执行镜像安全扫描任务前，请确保“我的镜像”中已经有1个以上的私有镜像。如果您当前账户下没有私有镜像，请参考**客户端上传镜像**，上传一个镜像到您的镜像仓库中。

步骤3 在“镜像版本”页签，选择待操作的镜像版本并单击操作列的“镜像扫描”。

说明

镜像同步到主机安全服务后才能执行镜像扫描。如果要扫描的镜像还没同步至主机安全服务，会弹出提示框。请单击“点此同步镜像”即可。

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。



- 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

如果遇到镜像扫描失败，请参见下表排查解决。

表 6-11 仓库镜像扫描失败原因及解决方案

失败原因	解决办法
访问SWR服务出错	请您**提交工单**，通过工单向技术人员寻求帮助。
缺少SWR授权	完成授权，授权方法请参见**SWR授权方法**。
获取镜像详细信息失败，镜像仓中可能已经不存在此镜像	请在主机/容器安全 HSS控制台的“风险预防-容器镜像安全-仓库镜像”页面，单击“同步镜像列表”，更新镜像列表信息，确认该镜像是否已经不存在。
镜像下载失败	请您**提交工单**，通过工单向技术人员寻求帮助。
镜像大小超限，不支持扫描	镜像总大小不能超过50G，建议精简镜像。
镜像层数超限，不支持扫描	镜像层数不能超过127层，单个镜像层不能超过10G。建议精简镜像。
Schema v1镜像不支持扫描	建议将Schema镜像升级到V2版本。

失败原因	解决办法
扫描镜像的时间超过3小时的超时时间，系统自动中止扫描。	建议精简镜像。

关于容器镜像镜像扫描如果想了解更多，请参见**仓库镜像安全扫描**。

6.12 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。

注意

镜像中心镜像由开源社区提供和维护，仅用于开发者测试，不支持商用环境使用。

约束与限制

仅以下区域支持“镜像中心”功能，其他区域暂不支持。

“华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”、“中国-香港”、“亚太-曼谷”、“亚太-新加坡”、“非洲-约翰内斯堡”和“拉美-圣地亚哥”。

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

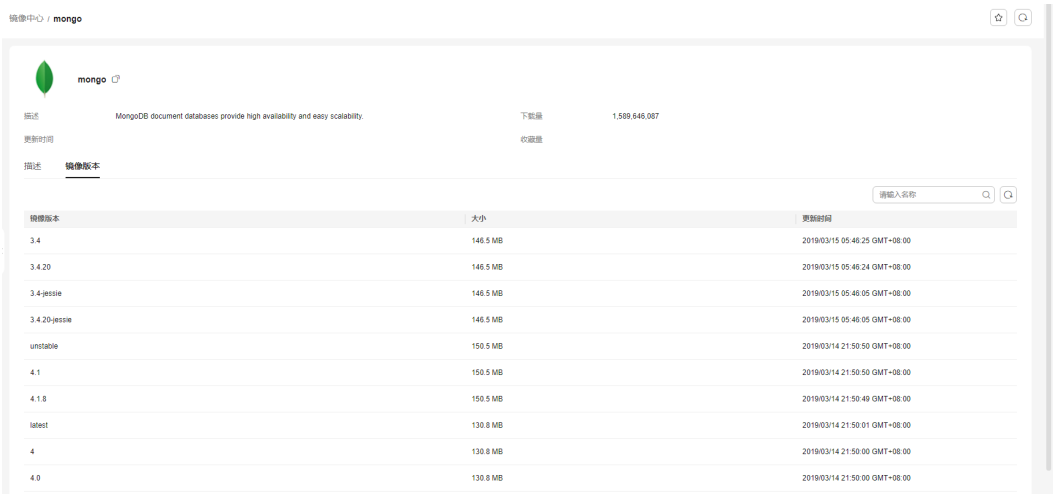
下载镜像中心的镜像

下面以下载镜像中心里的**mongo**镜像为例进行操作指导。

注意

下载镜像中心的镜像需要您的容器引擎客户端能够访问公网。

图 6-27 mongo 镜像详情示例



- 如果您的容器引擎客户端节点在以下局点，只需执行如下命令即可将其下载。

  “中国-香港”、“亚太-曼谷”、“亚太-新加坡”、“非洲-约翰内斯堡”和“拉美-圣地亚哥”。

  docker pull mongo:*4.1*

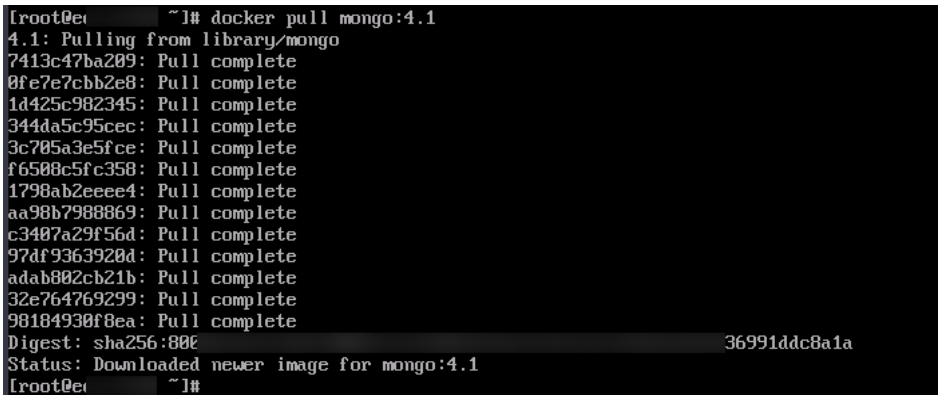
  ```
  [root@ec        ~]# docker pull mongo:4.1
  4.1: Pulling from library/mongo
  7413c47ba209: Pull complete
  0fe7e7cbb2e8: Pull complete
  1d425c982345: Pull complete
  344da5c95cec: Pull complete
  3c705a3e5fce: Pull complete
  f6508c5fc358: Pull complete
  1798ab2eeee4: Pull complete
  aa98b7988869: Pull complete
  c3407a29f56d: Pull complete
  97df9363920d: Pull complete
  adab802cb21b: Pull complete
  32e764769299: Pull complete
  98184930f8ea: Pull complete
  Digest: sha256:800                                                    36991ddc8a1a
  Status: Downloaded newer image for mongo:4.1
  [root@ec        ~]#
  ```

  说明

  此处**docker pull**后面的参数是镜像名称:镜像版本号。镜像名称可在镜像详情页单击镜像名称后的 按钮进行复制，镜像版本号请切换到镜像版本页签复制您要pull的版本号。

- 如果您容器引擎客户端节点在以下局点需要先**设置镜像加速器**再执行上述**docker pull**命令。

  “华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-广州”、“西南-贵阳一”



常见问题

拉取镜像中心的镜像失败，可能原因：**国内网络访问 DockerHub 镜像仓库异常通知**。如果您无法解决拉取失败的问题请**提交工单**。

6.13 设置镜像加速器

由于运营商网络原因，会导致您拉取第三方镜像仓库的镜像(例如Docker Hub)变慢甚至下载失败。华为云容器镜像服务提供了镜像下载加速功能，对部分常用的开源镜像下载进行加速。

⚠ 注意

- SWR镜像加速器是面向个人开发者的服务，仅限于支持个人开发场景，不允许有再次封装或商业用途。
- 面向生产环境使用场景，为避免Docker访问网络问题导致的镜像拉取失败，建议您在生产环境中慎重考虑对Docker Hub容器镜像的依赖，将需要的镜像从Docker Hub同步到SWR私有仓库使用。
- 仅支持通过镜像加速器拉取常用的开源镜像，镜像加速器无法保证一定拉取到所有的镜像版本，建议您将需要的镜像同步到SWR私有仓库使用。
- 暂不支持containerd容器引擎设置镜像加速器。

约束与限制

- 仅限华为云用户在华为云上的容器产品中使用该镜像加速能力。
- 仅支持通过镜像加速器拉取常用的开源镜像，不保证能够加速所有镜像，生产环境请谨慎使用。
- 构建镜像的客户端所安装的容器引擎（Docker）必须为18.06及以上版本。
- "华南-广州"、"华北-北京四"、"华东-上海一"和"西南-贵阳一"区域支持该功能。

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 6-28 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 6-29 Registry Mirrors 信息

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

----结束

常见问题

设置镜像加速器后还是拉取失败，可能原因：

- **国内网络访问 DockerHub 镜像仓库异常通知**。如果您无法解决拉取失败的问题请**提交工单**。

- 开源镜像源DockerHub中不存在您要拉取的镜像。
- 容器引擎所在的虚拟机节点配置异常，请**提交工单**进行处理。

7 使用 CTS 审计 SWR

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 云审计服务支持的基础版 SWR 操作列表

操作名称	资源类型	事件名称
镜像上传	images	postMultipartImagePackage
获取登录指令	dockerlogincmd	createDockerConfig
获取概览信息	overview	getDomainOverview
查询监控指标	overview	getDomainResourceReports
获取配额信息	quota	listQuotas
查询触发器详情	trigger	showTrigger
查询触发器列表	trigger	listTriggers
创建触发器	trigger	createTrigger
更新触发器	trigger	updateTrigger
删除触发器	trigger	deleteTrigger
创建组织	usernamespace	createUserNamespace

操作名称	资源类型	事件名称
删除组织	usernamespace	deleteUserNamespace
查询组织列表	usernamespace	listUserNamespaces
查询组织详情	usernamespace	showUserNamespace
创建组织授权	usernamespaceauth	createUserNamespaceAuth
删除组织授权	usernamespaceauth	deleteUserNamespaceAuth
查询组织授权	usernamespaceauth	showUserNamespaceAuth
更新组织授权	usernamespaceauth	updateUserNamespaceAuth
创建镜像仓库	imagerepository	createImageRepository
删除镜像仓库	imagerepository	deleteImageRepository
查询镜像仓库详情	imagerepository	showImageRepository
更新镜像仓库	imagerepository	updateImageRepository
查询镜像仓库列表	imagerepository	listImageRepositories
创建镜像tag	imagetag	createImageTag
删除镜像tag	imagetag	deleteImageTag
查询镜像tag列表	imagetag	listImageTags
创建镜像授权	userrepositoryauth	createUserRepositoryAuth
删除镜像授权	userrepositoryauth	deleteUserRepositoryAuth
查询镜像授权信息	userrepositoryauth	showUserRepositoryAuth
更新镜像授权信息	userrepositoryauth	updateUserRepositoryAuth
查询镜像授权列表	userrepositoryauth	listSharedReposDetails
创建按账号共享	imagerepositoryaccessdomain	createImageRepositoryAccessDomain
删除账号共享	imagerepositoryaccessdomain	deleteImageRepositoryAccessDomain
查询账号共享的详情信息	imagerepositoryaccessdomain	showImageRepositoryAccessDomain
更新账号共享	imagerepositoryaccessdomain	updateImageRepositoryAccessDomain
查询账号共享列表	imagerepositoryaccessdomain	listImageRepositoryAccessDomain
创建镜像共享	reposhare	createRepoShare
删除镜像共享	reposhare	deleteRepoShare

操作名称	资源类型	事件名称
查询镜像共享详情	reposhare	getRepoShare
更新镜像共享	reposhare	updateRepoShare
查询镜像共享列表	reposhare	listRepoShares
创建镜像自动同步	image-sync	setRImageSync
删除镜像自动同步	image-sync	unsetRImageSync
查询镜像自动同步列表	image-sync	listRImageSync
手动镜像同步	image-sync	manualImageSync
查询手动镜像同步job信息	image-sync	showSyncJob
创建镜像老化规则	retention	createRetention
删除镜像老化规则	retention	deleteRetention
查询镜像老化规则详情	retention	showRetention
更新镜像老化规则	retention	updateRetention
查询镜像老化规则列表	retention	listRetentions
查询镜像老化规则历史记录	retention	listRetentionHistories
创建镜像层	blob	createBlob
分片更新镜像层数据	blob	updateImageLayerChunk
更新镜像层	blob	updateImageLayer
下载镜像层	blob	downloadImageLayer
上传镜像manifest文件	manifest	uploadManifest

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。

约束与限制

默认只上报操作类的以及部分查询类的事件到云审计，如果需要上报全部的查询类事件到云审计请参考**配置特定云服务的查询类事件上报到云审计**进行配置。

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

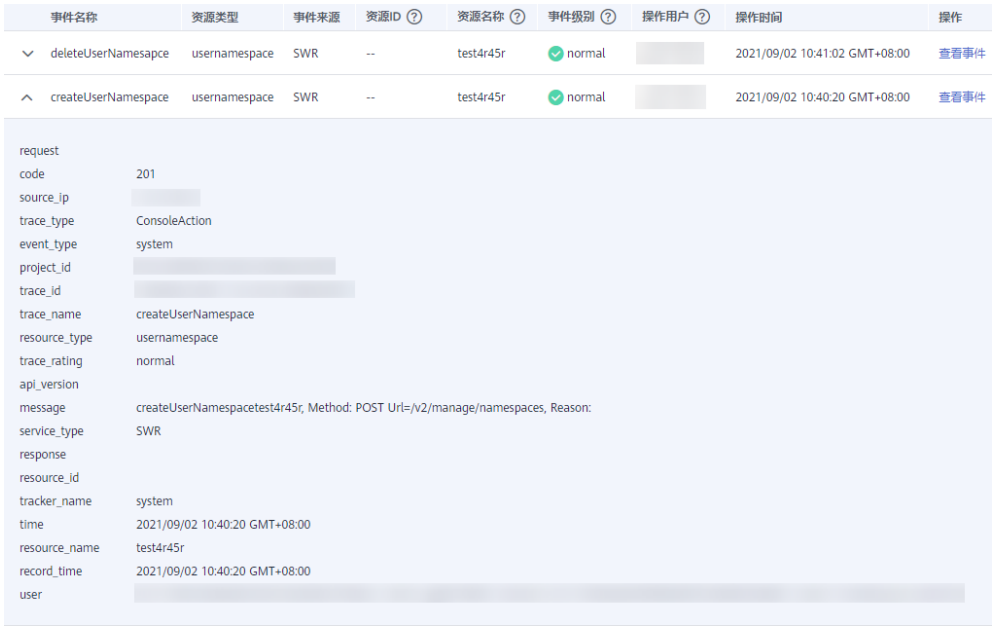
  

  其中，筛选类型选择“按资源ID”时，还需手动输入某个具体的资源ID，目前仅支持全字匹配模式的查询。

  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

