SoftWare Repository for Container

User Guide

Issue	07
Date	2021-09-02

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

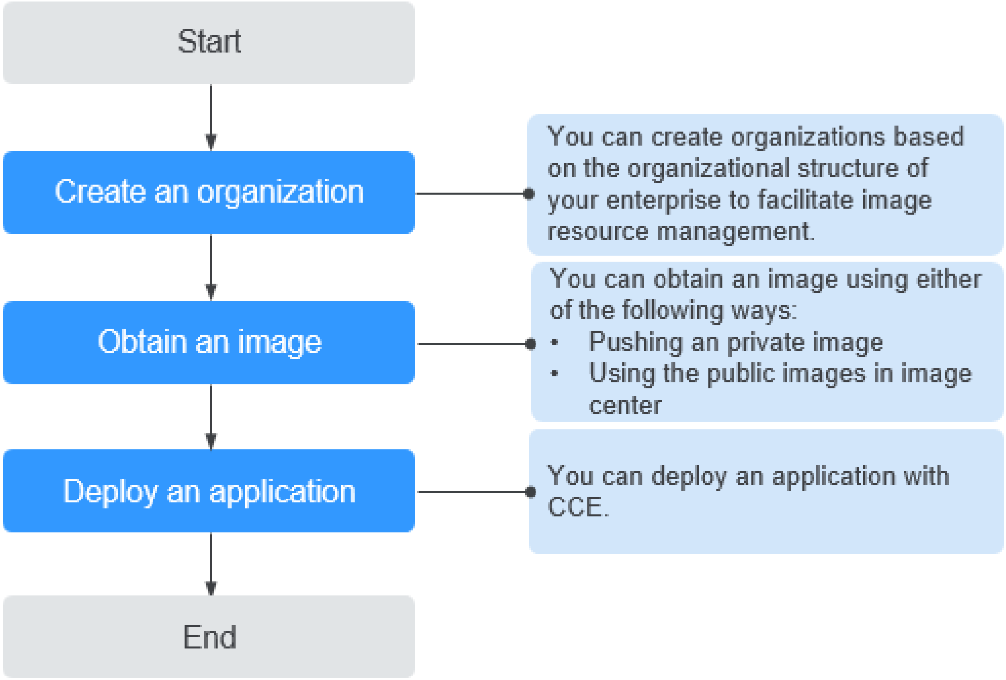
1 Introduction

SoftWare Repository for Container (SWR) provides easy, secure, and reliable management of container images throughout their lifecycles, featuring image push, pull, and deleting.

SWR provides private image repositories and fine-grained permission management, allowing you to grant different access permissions, namely, read, write, and edit, to different users. You can also use triggers to automatically update applications when images are updated. Simply set a trigger to the desired image. Every time the image is updated, the application deployed in Cloud Container Engine (CCE) with this image will be automatically updated.

You can access SWR on the **Console** or through **APIs**.

Figure 1-1 How SWR works


Start
Create an organization
Obtain an image
Deploy an application
End
You can create organizations based on the organizational structure of your enterprise to facilitate image resource management.
You can obtain an image using either of the following ways:
• Pushing an private image
• Using the public images in image center
You can deploy an application with CCE.

2 Permissions Management

2.1 Creating a User and Granting SWR Permissions

System-defined permissions in role/policy-based authorization provided by **Identity and Access Management (IAM)** let you control access to your SWR resources. With IAM, you can:

- Create IAM users or user groups for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing SWR resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your SWR resources.

If your Huawei Cloud account does not require individual IAM users for permissions management, you can skip this section.

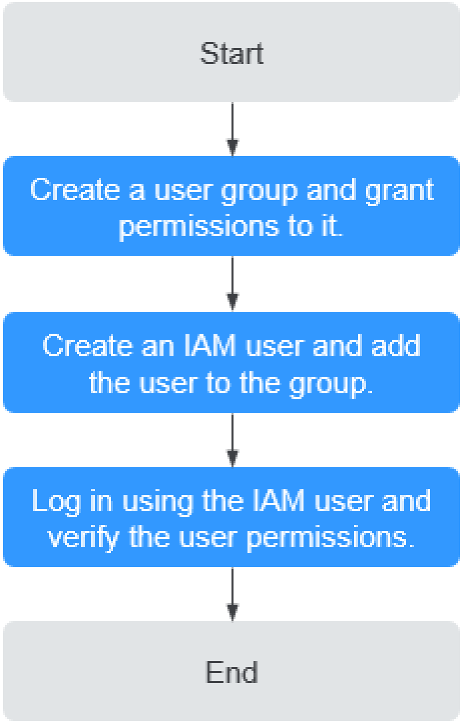
This section describes the procedure for granting user permissions.

Prerequisite

Before granting permissions to user groups, learn about system-defined permissions in **Role/Policy-based Permissions Management**. To grant permissions for other services, learn about all **system-defined permissions** supported by IAM.

Process Flow

Figure 2-1 Process of granting SWR permissions


Start
Create a user group and grant permissions to it.
Create an IAM user and add the user to the group.
Log in using the IAM user and verify the user permissions.
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and grant the **SWR Administrator** permissions to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console using the IAM user. Switch to the authorized region. If the following permissions can be successfully performed, the permissions are assigned successfully:

   a. Choose **Service List** > **SoftWare Repository for Container**. The SWR console is displayed.

   b. In the navigation pane on the left, choose **Organization Management**, click **Create Organization** in the upper right corner, and enter an organization name to create an organization.

   c. In the navigation pane on the left, choose **My Images** and click **Upload Through SWR** in the upper right corner. Select the organization created in the previous step and a local image file. The image is successfully uploaded.

3 Basics of the Container Engine

The container engine is an open source engine which allows you to create a lightweight, portable, and self-sufficient container for any application.

Preparations Before Installation

Before installing the container engine, you should understand the basic knowledge of the container engine. For details, see **Docker Documentation**.

Selecting an Edition of Container Engine

The container engine is compatible with almost all operating systems. Select an edition that best suits your needs. If you are not sure which edition to use, see **https://docs.docker.com/engine/install/**.

📖 NOTE

- It is advised to install container engine 1.11.2 or later because earlier versions do not support image push to SWR.
- If the container engine client is in a private network, bind an elastic IP address (EIP) to the client. This EIP will allow the client to download container engine installation packages from the website.

Installing the Container Engine

You can select either of the following installation procedures based on your OS.

Linux OS

EulerOS

- **Linux OS**

  Run the following commands to quickly install the latest edition. To install a specific edition, see **Docker Engine installation overview**.

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

- **EulerOS**

  The procedure of installing the container engine in EulerOS is as follows:

a. Log in to ECS where you want to install the container engine.

b. Configure a yum repository.

   If you have not configured a yum repository on the host, configure one. For details, see **How Can I Use an Automated Tool to Configure a Huawei Cloud Image Source (x86_64 and Arm)?** If you have configured one, skip this step.

c. Install and run the container engine.

   i. Run the following command to obtain the **docker-engine** package from the yum repository.

      ```
      yum search docker-engine
      ```

   ii. Run the **yum install -y** command to install the **docker-engine** package obtained in the previous step. The following is an example in the x86 architecture:

      ```
      yum install docker-engine.x86_64 -y
      ```

   iii. Set the container engine to start at system startup.

      ```
      systemctl enable docker
      ```

   iv. Start the container engine.

      ```
      systemctl start docker
      ```

d. Check the installation result.

   ```
   docker --version
   ```

   If information similar to the following is displayed, the container engine is successfully installed:

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

Building a Container Image

This section walks you through the steps of using a Dockerfile to build a container image for a simple web application. Dockerfile is a text file that contains all the instructions a user can call on the command line to build an image. A container image is a stack consisting of multiple layers. Each instruction creates a layer.

When using a browser to access a containerized application built from a Nginx image, you will see the default Nginx welcome page. In this section, you will build a new image based on the Nginx image to change the welcome message to **Hello, SWR!**

Step 1 Log in to the container engine as the **root** user.

Step 2 Run the following commands to create an empty file named **Dockerfile**:

```
mkdir mynginx
```

```
cd mynginx
```

```
touch Dockerfile
```

Step 3 Edit the Dockerfile.

```
vim Dockerfile
```

Add the following instructions to the Dockerfile:

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

In the preceding instructions:

- **FROM**: creates a layer from the base image. A valid Dockerfile must start with a **FROM** instruction. In this example, the **Nginx** image is used as the base image.
- **RUN**: executes a command to create a layer. One of its syntax forms is **RUN <command>**. In this example, the **echo** command is executed to display **Hello, SWR!**

Press **Esc** and enter **:wq** to save the settings and exit.

Step 4 Run **docker build** [*option*] <*context path*> to build an image.

docker build -t nginx:v1 .

- **-t nginx:v1**: specifies the image name and tag.
- **.**: indicates the path where the Dockerfile is located. All contents in this path are packed and sent to the container engine to build an image.

Step 5 Run the following command to check the created image. The command output shows that the **Nginx** image has been created with a tag of **v1**.

docker images

----End

Creating an Image Package

This section describes how to compress a container image into a .tar or .tar.gz package.

Step 1 Log in to the container engine as the **root** user.

Step 2 Run the following command to check images:

docker images

Check the name and tag of the image to be compressed.

Step 3 Run the following command to compress the image into a package:

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

NOTE

OPTIONS: You can set this to **--output** or **-o**, indicating that the image is exported to a file.

The file should be in either **.tar** or **.tar.gz**.

When using **docker save** to create an image package, use *{image}:{tag}* instead of *image id*. Otherwise, the package cannot be uploaded on the SWR page.

Example:

```
$ 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 # Packages all Nginx versions.
$ docker save -o nginx-latest.tar nginx:latest
```

----End

Importing an Image File

This section describes how to import an image package as an image using the **docker load** command.

There are two modes:

docker load < ***Path/File name.tar***

docker load --input ***Path/File name.tar*** or **docker load -i** ***Path/File name.tar***

Example:

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

4 Image Management

4.1 Uploading an Image Through a Container Engine Client (Recommended)

Scenario

Uploading an image through a container engine client is to run **docker push** on the server where the client is installed to push the image to SWR.

If your container engine client is an ECS or CCE node, you can push an image over two types of networks.

- If your client and the image repository are in the same region, you can push an image over private networks.
- If your client and the image repository are in different regions, you can push an image over public networks and the client needs to be bound to an EIP.

Notes and Constraints

- Each image layer cannot exceed 10 GB.
- Your container engine client version must be 1.11.2 or later.

Prerequisite

You have created an organization in SWR. For details, see **Creating an Organization**.

Procedure

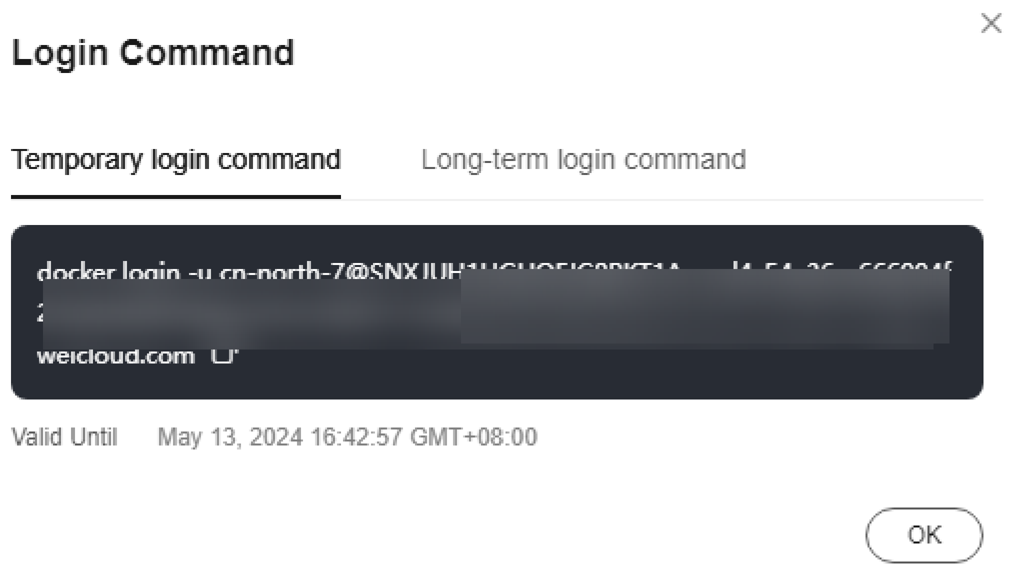
Step 1 **Building a Container Image** or **Importing an Image File**.

Step 2 Access SWR.

1. Log in to the **SWR console**.

2. In the navigation pane on the left, choose **Dashboard** and click **Generate Login Command** in the upper right corner. On the displayed page, click ⧉ to copy the login command.

Figure 4-1 Generating a login command



Login Command

```
docker login -u cn-north-7@SNXJUH[redacted]weicloud.com
```

Valid Until May 13, 2024 16:42:57 GMT+08:00

NOTE

- A temporary login command is valid for 6 hours. For details about how to obtain a login command that will remain valid for a long term, see **Obtaining a Long-Term Valid Login Command**. After you obtain a long-term valid login command, your temporary login commands will still be valid as long as they are in their validity periods.
- The domain name at the end of the login command is the image repository address. Record the address for later use.

3. Run the login command on your container engine client.

   The message **Login Succeeded** will be displayed upon a successful login.

Step 3 Run the following command on the device where the container engine is installed to label the **Nginx** image:

docker tag [*Image name 1*:*tag 1*] [*Image repository address*]/[*Organization name*]/[*Image name 2*:*tag 2*]

In the preceding information:

- [Image name 1:tag 1]: Replace it with the actual name and tag of the image to be uploaded.
- [Image repository address]: You can query the address on the SWR console, that is, the domain name at the end of the login command in **Step 2.2**.
- [Organization name]: Replace it with the name of the organization created.
- [Image name 2:tag 2]: Replace it with the desired image name and tag.

Examples:

docker tag nginx:v1 swr.ap-southeast-1.myhuaweicloud.com/cloud-develop/nginx:v1

Step 4 Run the following command to push the image to the image repository:

docker push [*Image repository address*]/[*Organization name*]/[*Image name 2*:*tag 2*]

Examples:

docker push swr.ap-southeast-1.myhuaweicloud.com/cloud-develop/nginx:v1

The following information will be returned upon a successful push:

```
The push refers to repository [swr.ap-southeast-1.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
```

To view the pushed image, refresh the **My Images** page.

----End

FAQ

Why Does an Image Fail to Be Uploaded Through a Container Engine Client?

4.2 Obtaining a Long-Term Valid Login Command

Scenario

This section describes how to obtain a login command that is permanently valid.

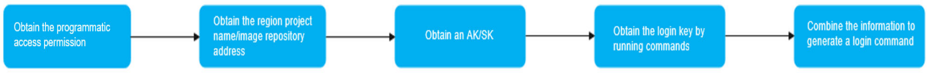
NOTE

- For security purposes, it is advised to obtain the login command in the development environment.
- Before logging in to the IAM console, ensure that you have the permission for accessing IAM service. For details about the authorization mode, see **Creating a User Group and Assigning Permissions**.

Process

You can obtain a long-term valid login command as the following process:

Figure 4-2 Process

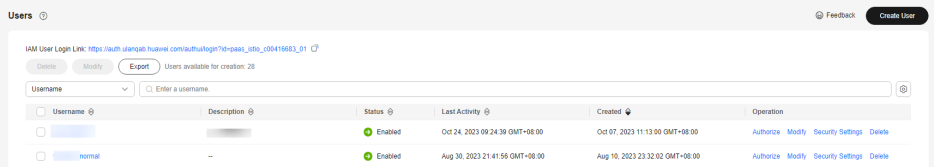

Obtain the programmatic access permission
Obtain the region project name/image repository address
Obtain an AK/SK
Obtain the login key by running commands
Combine the information to generate a login command

Procedure

Step 1 Obtain the programmatic access permission. (If the current user has the permission, skip this step.)

1. Log in to the management console as an administrator.
2. Click in the upper left corner and select a region and a project.
3. Click ☰ in the navigation pane on the left and choose **Management & Governance** > **Identity and Access Management**.
4. Enter the name of the user to whom you want to grant the programmatic access permission in the search box on the **Users** page.

Figure 4-3 User list

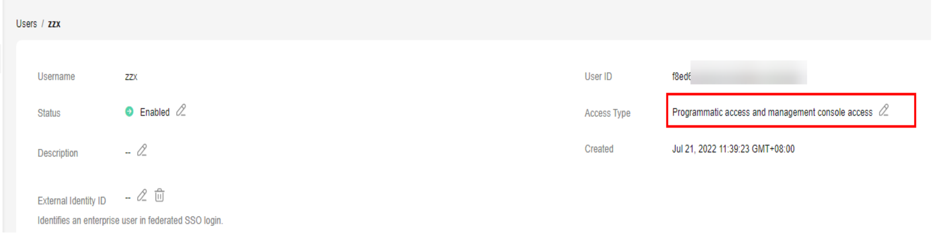


Users
IAM User Login Link: https://auth.ulanqab.huawei.com/authui/login?id=paas_istio_c00416683_01
Users available for creation: 28
Username | Enter a username.

Username	Description	Status	Last Activity	Created	Operation
[redacted]	[redacted]	Enabled	Oct 24, 2023 09:24:39 GMT+08:00	Oct 07, 2023 11:13:00 GMT+08:00	Authorize Modify Security Settings Delete
[redacted]normal	--	Enabled	Aug 30, 2023 21:41:56 GMT+08:00	Aug 10, 2023 23:32:02 GMT+08:00	Authorize Modify Security Settings Delete

5. Click the user to go to its details page.
6. Click next to **Access Type**.

Figure 4-4 Changing access type



Users / zzx

Username zzx

Status Enabled

Description --

External Identity ID --

Identifies an enterprise user in federated SSO login.

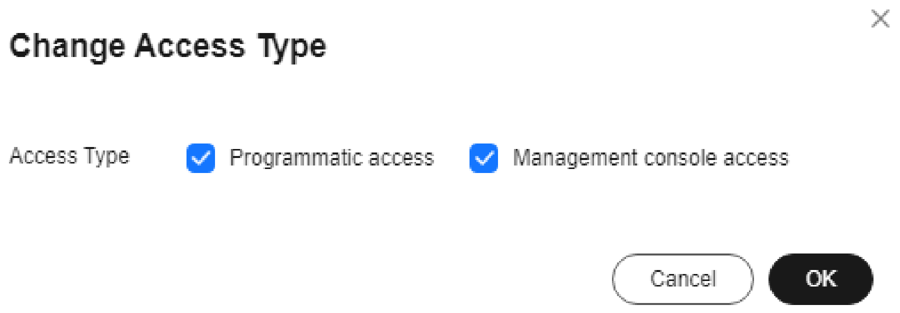
User ID f8ed6[redacted]

Access Type Programmatic access and management console access

Created Jul 21, 2022 11:39:23 GMT+08:00

7. Select **Programmatic access**. (You can select only programmatic access or both access types.)

Figure 4-5 Changing the access type



Change Access Type

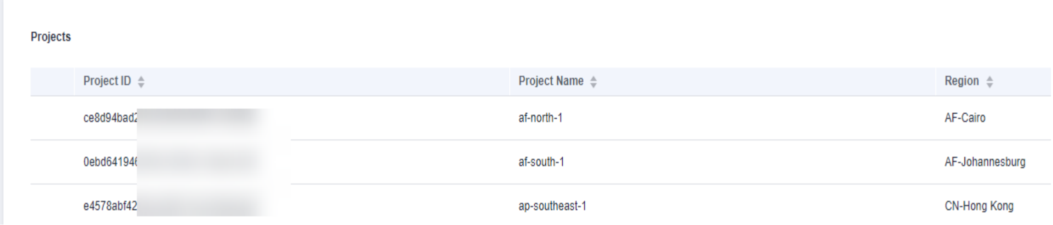
Access Type ☑ Programmatic access ☑ Management console access

Step 2 Obtain the regional project name and image repository address.

1. Log in to the IAM console.
2. Hover the cursor over the username in the upper right corner.

3. Choose **My Credentials** from the drop-down list.
4. In the project list, find the region and project to which your VM belongs.

Figure 4-6 Region and project



Projects

Project ID	Project Name	Region
ce8d94bad2[redacted]	af-north-1	AF-Cairo
0ebd64194[redacted]	af-south-1	AF-Johannesburg
e4578abf42[redacted]	ap-southeast-1	CN-Hong Kong

Step 3 Obtain an AK/SK.

NOTE

The access key ID (AK) and secret access key (SK) are a pair of access keys used together to authenticate users who wish to make API requests. The AK/SK pair provides functions similar to a password. If you already have an AK/SK, skip this step.

1. Log in to the IAM console, hover over your username, and click **My Credentials**.
2. In the navigation pane on the left, choose **Access Keys** and click **Create Access Key**.
3. Enter a description, and click **OK**.
4. In the displayed dialog box, click **Download**.

   After the certificate is downloaded, obtain the AK and SK information from the **credentials** file.

Table 4-1 *credentials file*

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

NOTE

Keep the AK/SK file confidential to prevent information leakage.

Step 4 Log in to a Linux PC and run the following command to obtain the login key**:**

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

Replace **AK** with the *Access Key Id* and **SK** with *Secret Access Key* in the **credentials** file in **Step 3**.

Examples:

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

After the command is executed, the following login key is obtained:

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

NOTE

The preceding key is only an example.

Step 5 **Use the information you obtained to generate a long-term valid login command in the following format:**

docker login -u [*Regional project name*]**@**[*AK*] **-p** [*Login key*] [*Image repository address*]

In the command, the regional project name and image repository address are obtained in **Step 2**, the AK in **Step 3**, and the login key in **Step 4**.

Examples:

```
docker login -u ap-southeast-3@RVHVMX****** -p cab4ceab4a1545*************** swr.ap-
southeast-3.myhuaweicloud.com
```

If the **Login Succeeded** message is displayed, it indicates that the login is successful.

NOTE

- The login key is encrypted and cannot be decrypted. Therefore, other users cannot obtain the SK from **-p**.
- The login command can be used on other devices.

Step 6 **(Optional) When you log out the repository, run the following commands to delete your authentication information.**

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

Step 7 Run the **history -c** command to clear the operation records.

----End

4.3 Uploading an Image Through SWR Console

Scenario

This section walks you through the steps of uploading an image to SWR through the SWR console.

Notes and Constraints

- A maximum of 10 files can be uploaded at a time. The size of a single file (including the decompressed files) cannot exceed 2 GB.
- The image package is created using container engine 1.11.2 or later.

Prerequisites

- You have created an organization in SWR. For details, see **Creating an Organization**.
- The image has been saved as a **.tar** or **.tar.gz** file. For details, see **Creating an Image Package**.

Procedure

Step 1 Log in to the **SWR console**.

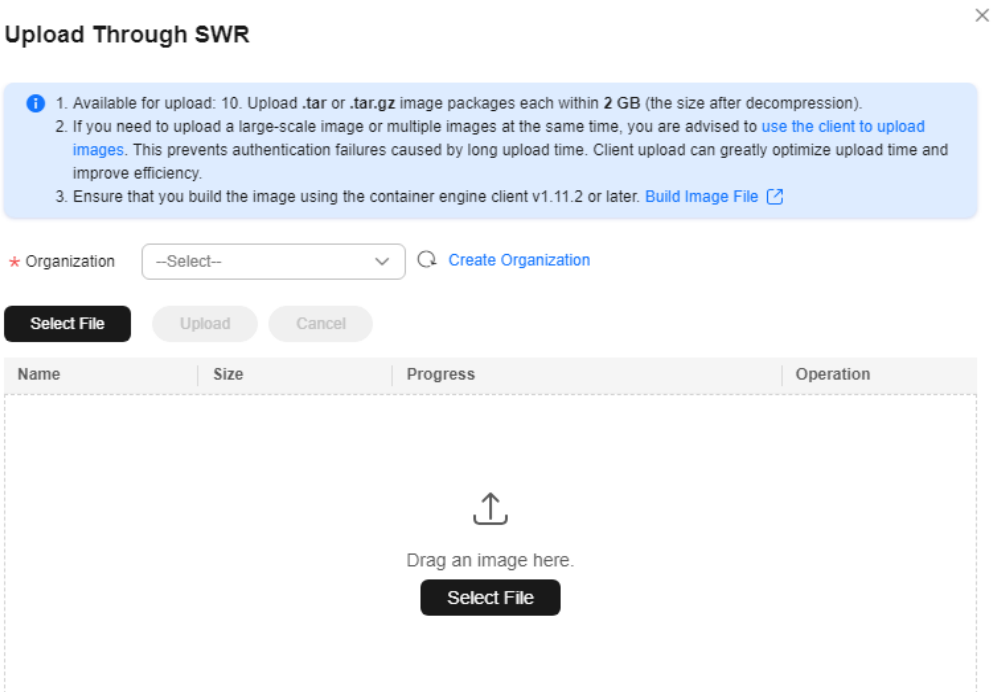
Step 2 In the navigation pane on the left, choose **My Images**. Then, click **Upload Through SWR**.

Step 3 On the page displayed, select an organization. Then, click **Select File** to upload the desired image file.

NOTE

If you select multiple images to upload, the system uploads them one by one. Concurrent upload is not supported.

Figure 4-7 Uploading an image through SWR console



Upload Through SWR

1. Available for upload: 10. Upload **.tar** or **.tar.gz** image packages each within **2** GB (the size after decompression).
2. If you need to upload a large-scale image or multiple images at the same time, you are advised to use the client to upload images. This prevents authentication failures caused by long upload time. Client upload can greatly optimize upload time and improve efficiency.
3. Ensure that you build the image using the container engine client v1.11.2 or later. Build Image File

Step 4 Click **Upload**.

If **Completed** is displayed, the image is successfully uploaded.

----End

FAQ

Why Does an Image Fail to Be Uploaded Through SWR Console?

4.4 Pulling an Image

Scenario

You can run the **docker pull** command to pull images from SWR.

Prerequisite

- Before pulling an image, ensure that your network connection is normal.
- Before pulling an image, contact the administrator to grant the SWR pull permission on the IAM console. For details, see **Permissions Management**.
- On the **My Images** page, **Private Images** list your own images in your organization and **Shared Images** list private images shared by other users in the organization.
- After an IAM user is created, the administrator needs to grant permissions to the user in the organization so that the user can read and edit images in the organization. For details, see **User Permissions**.

Pulling an Image from My Images

Step 1 Log in to the VM running the container engine as the **root** user.

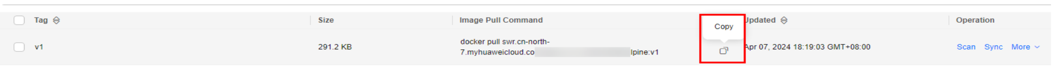
Step 2 Obtain a login command by referring to **Step 2** and access SWR.

Step 3 Log in to the **SWR console**.

Step 4 In the navigation pane, choose **My Images** and click the name of the target image.

Step 5 On the **Image Tags** tab page, in the same row as the target image tag, click ⧉ in the **Image Pull Command** column to copy the command.

Figure 4-8 Obtaining the image pull command



□	Tag ⇕	Size	Image Pull Command		pdated ⇕	Operation
□	v1	291.2 KB	docker pull swr.cn-north-7.myhuaweicloud.co[redacted]lpine:v1	Copy ⧉	pr 07, 2024 18:19:03 GMT+08:00	Scan Sync More ⌄

Step 6 Run the image pull command obtained in **Step 5** on the VM.

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

Run the **docker images** command to check whether the image is successfully pulled.

```
# 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
```

Step 7 (Optional) Run the following command to save the image as an archived file:

docker save [*Image name:tag name*] > [*Archived file name*]

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

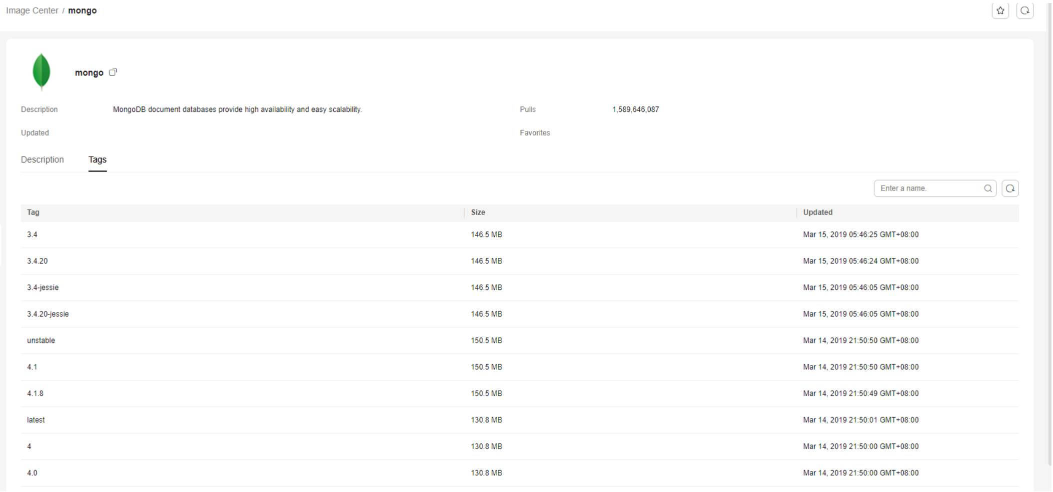
----End

Pulling an Image from the Image Center

You can directly pull an image from the Image Center without specifying a repository address. For example, you can **connect the VM where the container engine resides with SWR** and run the following command to directly pull the **mongo** image:

docker pull mongo:*4.1*

Figure 4-9 mongo image details



Description MongoDB document databases provide high availability and easy scalability.

Pulls 1,589,646,087

Updated

Favorites

Tag	Size	Updated
3.4	146.5 MB	Mar 15, 2019 05:46:25 GMT+08:00
3.4.20	146.5 MB	Mar 15, 2019 05:46:24 GMT+08:00
3.4-jessie	146.5 MB	Mar 15, 2019 05:46:05 GMT+08:00
3.4.20-jessie	146.5 MB	Mar 15, 2019 05:46:05 GMT+08:00
unstable	150.5 MB	Mar 14, 2019 21:50:50 GMT+08:00
4.1	150.5 MB	Mar 14, 2019 21:50:50 GMT+08:00
4.1.8	150.5 MB	Mar 14, 2019 21:50:49 GMT+08:00
latest	130.8 MB	Mar 14, 2019 21:50:01 GMT+08:00
4	130.8 MB	Mar 14, 2019 21:50:00 GMT+08:00
4.0	130.8 MB	Mar 14, 2019 21:50:00 GMT+08:00

4.5 Setting Image Attributes

Scenario

After pushing an image, you can set image attributes, including its type (private by default), category and description.

Public images can be pulled by all users; whereas the access to private images requires corresponding permissions. You can add permissions, namely, read, write, or manage, to allow users to access your private images. For details, see **Granting Permissions of a Specific Image**.

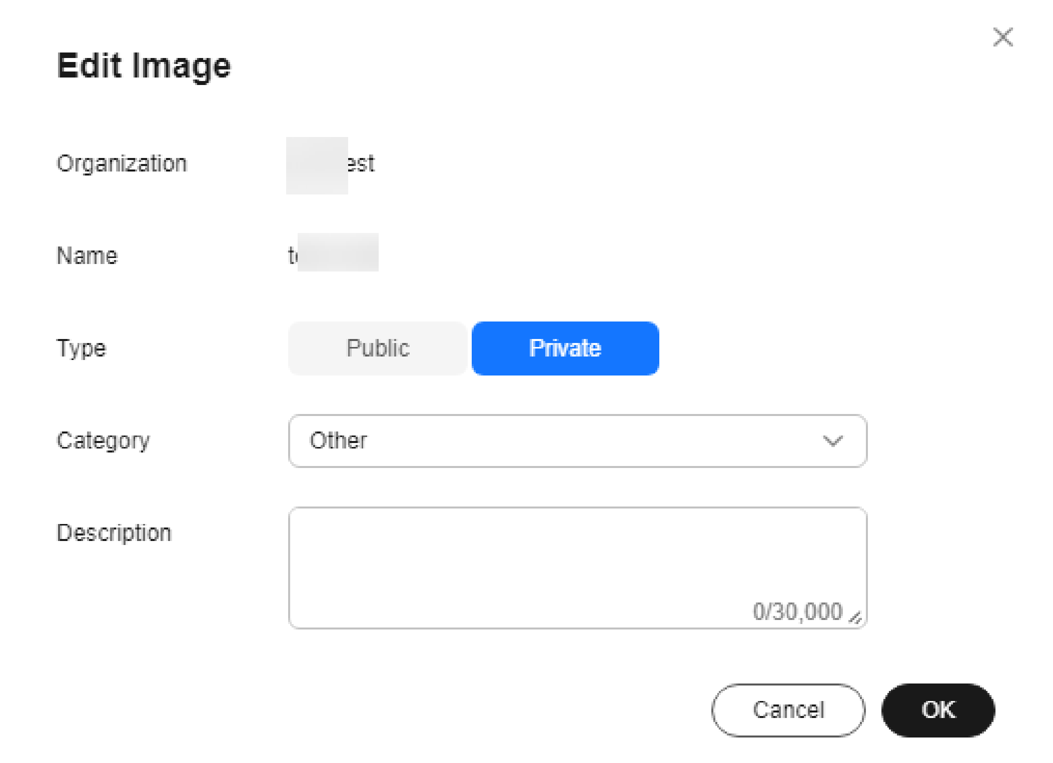
Procedure

Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane, choose **My Images** and click the desired image.

Step 3 On the details page, click **Edit** in the upper right corner. In the dialog box displayed, set **Sharing Type** (**Public** or **Private**), **Category**, and **Description**, and click **OK**.

Figure 4-10 Editing an image



Edit Image

Organization [redacted]est

Name t[redacted]

Type: Public / [✓ Private]

Category: Other

Description: 0/30,000

Table 4-2 Editing an image

Parameter	Description
Organization	The organization to which the image belongs
Image	Image name
Sharing Type	The following options are available: - Public - Private **NOTE** Public images can be pulled and used by all users. - If your machine and the image repository are in the same region, you can access the image repository through private networks. - If your machine and the image repository are in different regions, the node must have access to the public network to pull images from the image repository.

Parameter	Description
Category	The following options are available: ● Application server ● Linux ● Arm ● Framework & Application ● Database ● Language ● Others
Description	Image description. Enter a maximum of 30,000 characters.

----End

4.6 Sharing a Private Image

Scenario

You can share your **private images** with other users and grant the accounts permissions to pull the images.

A user under the account with which you shared the image can then log in to the **SWR console** to view the image on the **My Images > Shared Images** page. On the tab page, the user can click the target image to check its detailed information, including the image tag and image pull command.

Notes and Constraints

- Only private images can be shared. Public images cannot be shared.
- Only IAM users authorized to manage the private images can share images. The users with whom you share your images only have the read-only permission, which only allows them to pull the images.
- You can share images only with accounts in the same region. Cross-region image sharing is not supported.
- A private image can be shared with a maximum of 500 tenants.

Procedure

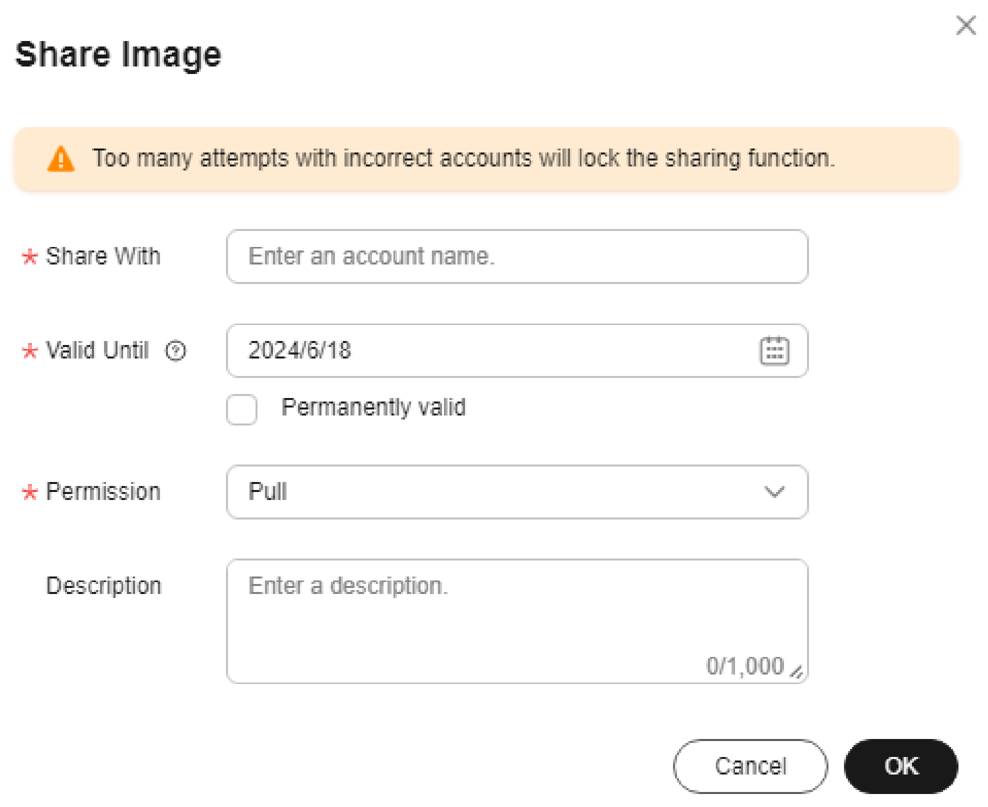
Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane, choose **My Images** and click the target image.

Step 3 On the details page, click the **Sharing** tab.

Step 4 Click **Share Image**. Set parameters based on **Table 4-3**, and click **OK**.

Figure 4-11 Sharing an image



Share Image

Too many attempts with incorrect accounts will lock the sharing function.

* Share With: Enter an account name.

* Valid Until: 2024/6/18

□ Permanently valid

* Permission: Pull

Description: Enter a description.

0/1,000

Table 4-3 Sharing an image

Parameter	Description
Sharing Type	Account name, account ID, or organization
Share With	Enter an account ID.
Valid Until	Set a validity period. If you want the image to be permanently accessible to the account, select **Permanently valid**.
Permission	Only the **Pull** permission is supported currently.
Description	Enter a maximum of 1,000 characters.

Step 5 To view all the shared images, choose **My Images** in the navigation pane, click the **Private Images** tab, and select **Display only shared images**.

----End

4.7 Adding a Trigger

Scenario

SWR works with Cloud Container Engine (CCE) to enable automatic application updates. This could be realized by adding a trigger to the desired images.

Prerequisite

A containerized application has been created on CCE by using an image from SWR.

If no applications have been created, log in to the CCE console and create one. For details, see **Creating a Deployment** or **Creating a StatefulSet**.

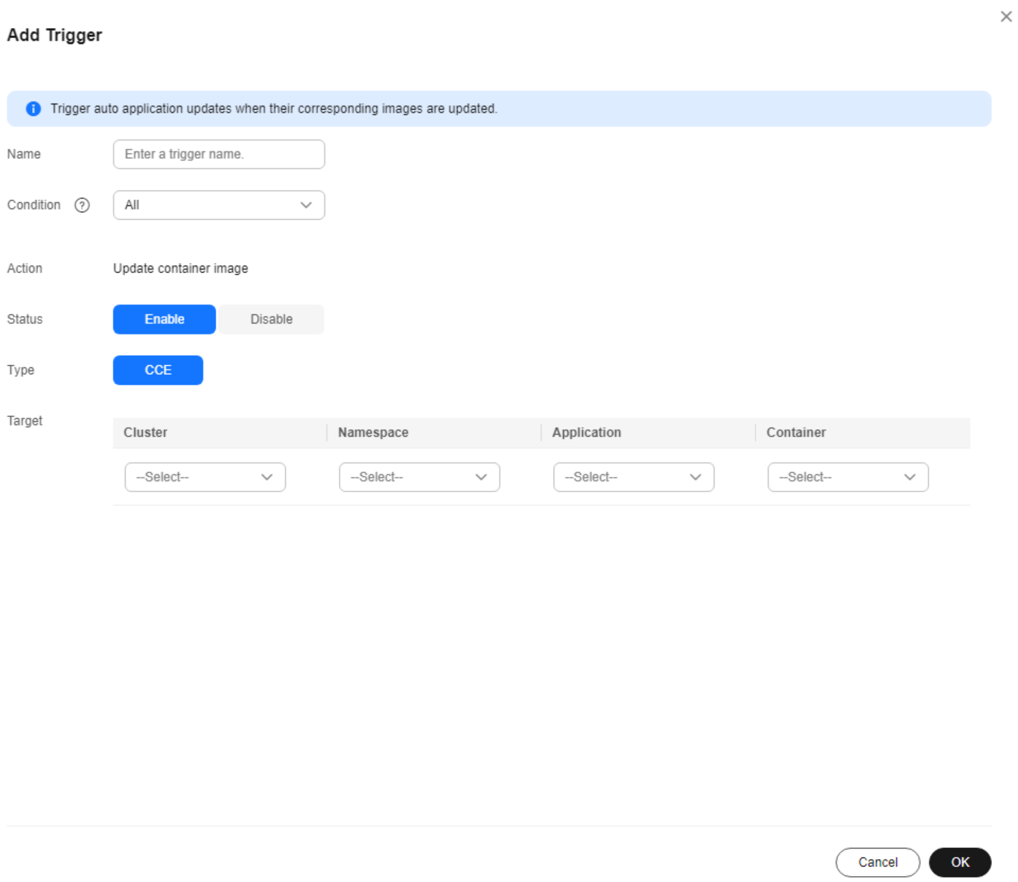
Procedure

Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane on the left, choose **My Images**, and click the target image.

Step 3 Click the **Triggers** tab, then click **Add Trigger**. On the page displayed, configure the following parameters according to **Table 4-4** and click **OK**.

Figure 4-12 Adding a trigger



Add Trigger

Trigger auto application updates when their corresponding images are updated.

Name: Enter a trigger name.

Condition: All

Action: Update container image

Status: Enable | Disable

Type: CCE

Target:

Cluster	Namespace	Application	Container
--Select--	--Select--	--Select--	--Select--

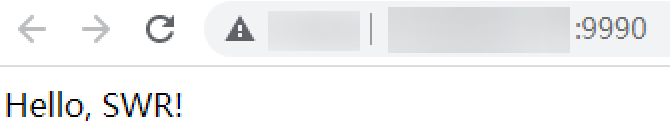
Table 4-4 Trigger

Parameter	Description
Name	The name of a trigger. The name can contain 1 to 64 characters, and must start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed. The name cannot end with an underscore or hyphen. Consecutive underscores or hyphens are not allowed and an underscore cannot be placed next to a hyphen.
Condition	The following trigger conditions are supported: ● All tags: Deployment is triggered when any image tags are generated or updated. ● Specific tag: Deployment is triggered when a specific image tag is generated or updated. ● Tags matching regular expression: Deployment is triggered when an image tag that matches the regular expression is generated or updated. The regular expression rules are as follows: – *****: matches any field that does not contain the path separator **/**. – ******: matches any field that contains the path separator **/**. – **?**: matches any single character except **/**. – **{option 1, option 2, ...}**: matches multiple options.
Operation	Currently, only operation of updating images will be triggered. You need to specify the application to be updated and the container of the application.
Status	Select **Enable**.
Trigger Type	Select **CCE**.
Application	Select the container whose image you want to update.

----End

Example 1: The trigger condition is All tags.

A Deployment named **nginx** is created using the Nginx image v1. The Deployment provides service to external systems with a welcome page displaying **Hello, SWR!**



[redacted] | [redacted]:9990

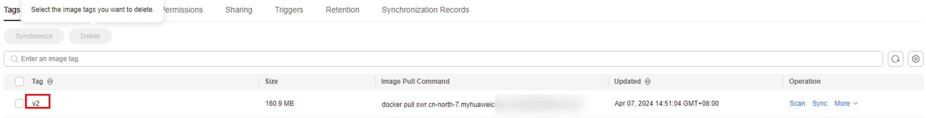
Hello, SWR!

1. Add a trigger to the Nginx image.

Set **Name** as **All_tags**, **Condition** as **All tags**, and select the application and all its containers that use the Nginx image.

2. Push the Nginx image v2 to SWR. The welcome page of the Deployment created using this new image should display **Hello, SoftWare Repository for Container!**

Figure 4-13 Image tag v2

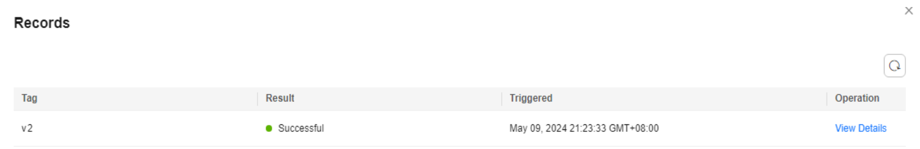


Tag	Size	Image Pull Command	Updated	Operation
v2	160.9 MB	docker pull swr.cn-north-7.myhuaweic [redacted]	Apr 07, 2024 14:51:04 GMT+08:00	Scan Sync More

3. Check whether the deployment is triggered successfully.

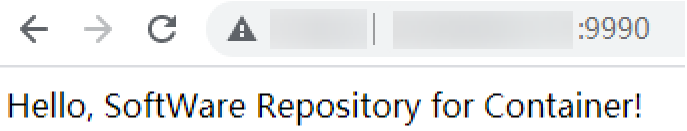
   On the **Triggers** tab page, locate the trigger and click **Records** to check whether the trigger is successful.

Figure 4-14 Result


Records

Tag	Result	Triggered	Operation
v2	● Successful	May 09, 2024 21:23:33 GMT+08:00	View Details

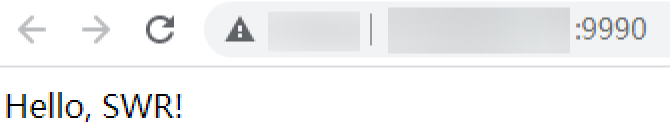
The welcome page of the Deployment displays **Hello, SoftWare Repository for Container!**


[redacted] | [redacted] :9990

Hello, SoftWare Repository for Container!

Example 2: The trigger condition is Tags matching regular expression.

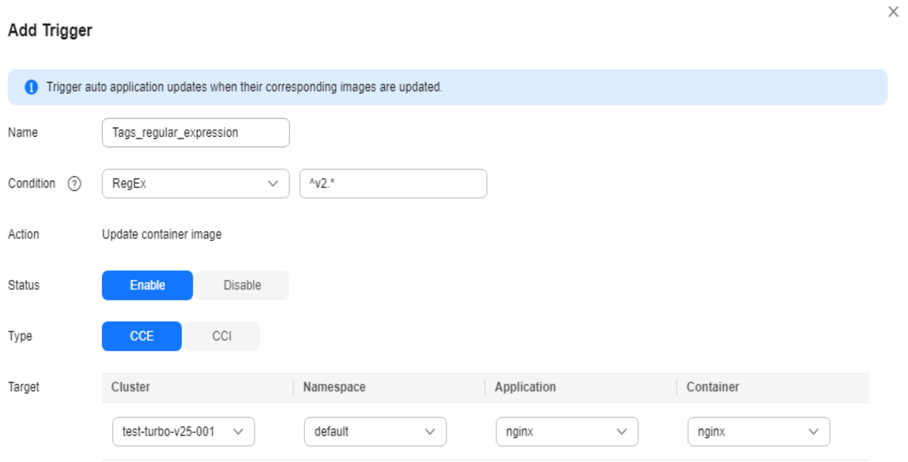
A Deployment named **nginx** is created using the Nginx image v0. The Deployment provides service to external systems with a welcome page displaying **Hello, SWR!**


[redacted] | [redacted] :9990

Hello, SWR!

1. Add a trigger to the Nginx image.

   Set **Name** to **Tags_regular_expression**, **Condition** to **Tags matching regular expression**, regular expression to **^v2.***, and select the application and all its containers that use the Nginx image.



Add Trigger

Trigger auto application updates when their corresponding images are updated.

Name: Tags_regular_expression

Condition: RegEx ^v2.*

Action: Update container image

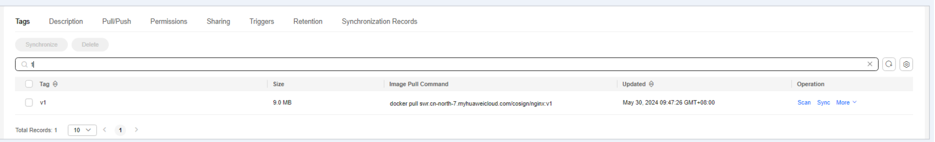
Status: Enable | Disable

Type: CCE | CCI

Target:

Cluster	Namespace	Application	Container
test-turbo-v25-001	default	nginx	nginx

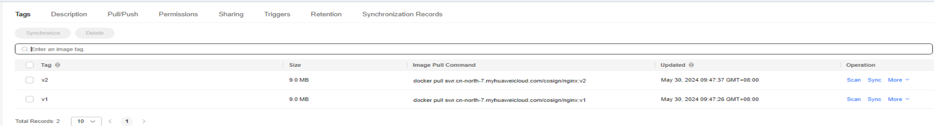
2. Push the Nginx image v1 to SWR. The welcome page of the Deployment created using this new image should display **Hello, SWR! (v1)**.



Tag	Size	Image Pull Command	Updated	Operation
v1	9.0 MB	docker pull swr.cn-north-7.myhuaweicloud.com/cosign/nginx:v1	May 30, 2024 09:47:26 GMT+08:00	Scan Sync More

Total Records: 1

3. Push the Nginx image v2 to SWR. The welcome page of the Deployment created using this new image should display **Hello, SWR! (v2)**.



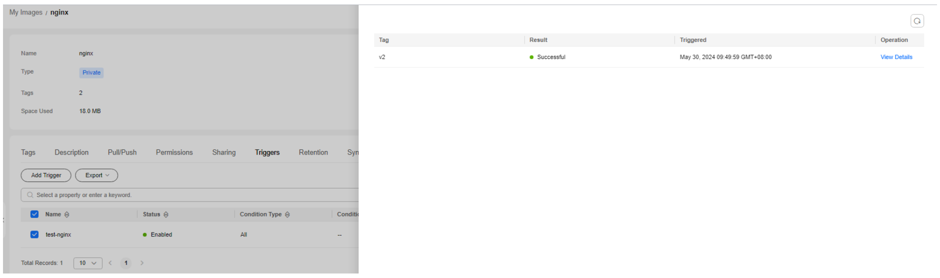
Tag	Size	Image Pull Command	Updated	Operation
v2	9.0 MB	docker pull swr.cn-north-7.myhuaweicloud.com/cosign/nginx:v2	May 30, 2024 09:47:37 GMT+08:00	Scan Sync More
v1	9.0 MB	docker pull swr.cn-north-7.myhuaweicloud.com/cosign/nginx:v1	May 30, 2024 09:47:26 GMT+08:00	Scan Sync More

Total Records: 2

4. Check whether the deployment is triggered successfully.

On the **Triggers** tab page, click ˅ to check the result. As shown in **Figure 4-15**, only the deployment of the Nginx image v2 is triggered.

Figure 4-15 Result



Name: nginx

Type: Private

Tags: 2

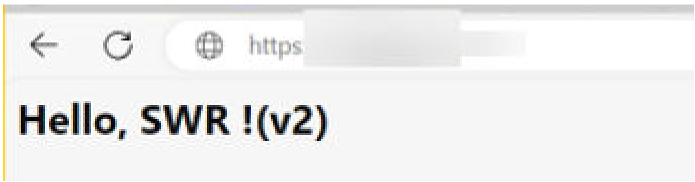
Space Used: 18.0 MB

Name	Status	Condition Type	Conditi
test-nginx	● Enabled	All	--

Total Records: 1

Tag	Result	Triggered	Operation
v2	● Successful	May 30, 2024 09:49:59 GMT+08:00	View Details

The welcome page of the Deployment displays **Hello, SWR! (v2)**.



Hello, SWR !(v2)

4.8 Adding an Image Retention Policy

Scenario

You can add a retention policy to an image in SWR to automatically delete any unused image tags. The policy takes effect immediately after you set it. There are two types of policies:

- Number of days: keeping only image tags that have been pushed to SWR within a certain number of days.
- Number of tags: keeping only a certain number of the most recent image tags.

You can configure filters for your retention policy to prevent certain image tags from being affected by the retention policy.

Notes and Constraints

Only one retention rule can be added to an image. If you want to add a new retention policy, you must delete the existing policy.

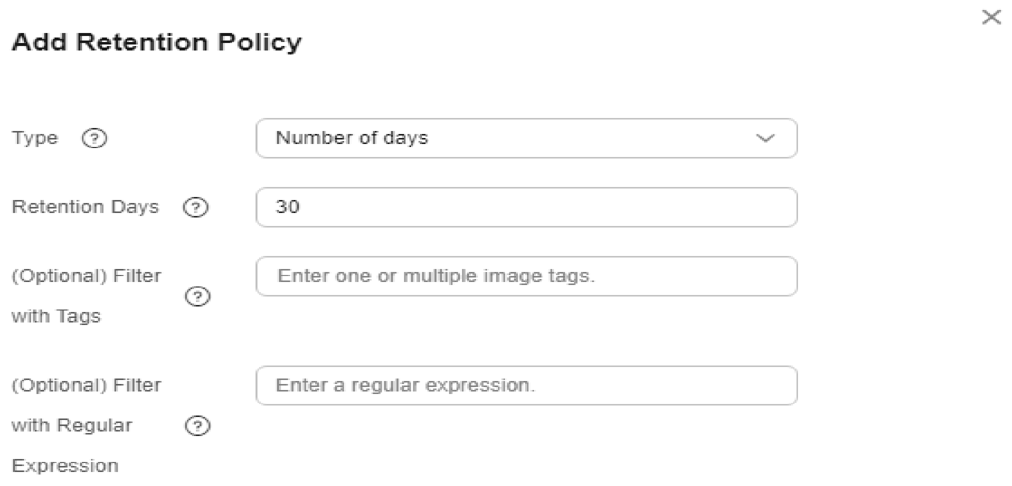
Procedure

Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane on the left, choose **My Images**, and click the desired image to enter its details page.

Step 3 On the **Retention** tab page, click **Add Retention Policy**. Configure the policy based on **Table 4-5** and click **OK**.

Figure 4-16 Adding a retention policy



Add Retention Policy

Type: Number of days

Retention Days: 30

(Optional) Filter with Tags: Enter one or multiple image tags.

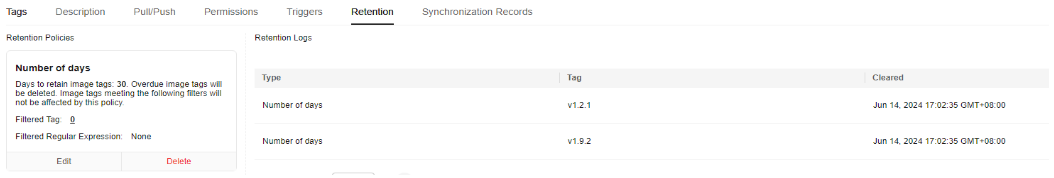
(Optional) Filter with Regular Expression: Enter a regular expression.

Table 4-5 Parameters for adding an image retention policy

Parameter	Description
Policy Type	There are two types of retention policies: ● Number of days: keeping only image tags that have been pushed to SWR within a certain number of days. ● Number of tags: keeping only a certain number of the most recent image tags.
Count Limit (Number of days)	When you set **Policy Type** to **Number of days**, the value of **Count Limit** indicates the maximum number of the most recent image tags to be retained. The value should be an integer ranging from 1 to 365.
Count Limit (Number of tags)	When you set **Policy Type** to **Number of tags**, the value of **Count Limit** indicates the maximum number of the most recent image tags to be retained. The value should be an integer ranging from 1 to 1,000.
Tag Filter	Enter image tags that you do not want this retention policy to apply to.
Regular Expression Filter	Enter a regular expression. Image tags meeting this regular expression will not be affected by this retention policy.

After the retention policy is added, SWR immediately applies the policy and displays deleted image tags (if any) in the **Retention Logs** area.

Figure 4-17 Checking the retention policy and logs



Number of days

Days to retain image tags: **30**. Overdue image tags will be deleted. Image tags meeting the following filters will not be affected by this policy.

Filtered Tag: 0

Filtered Regular Expression: None

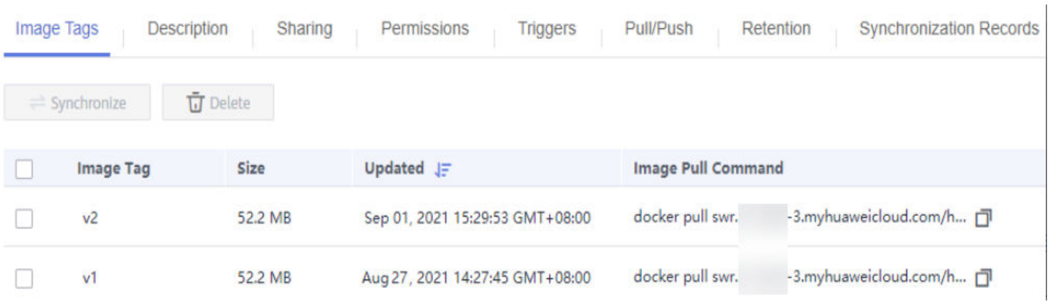
Type	Tag	Cleared
Number of days	v1.2.1	Jun 14, 2024 17:02:35 GMT+08:00
Number of days	v1.9.2	Jun 14, 2024 17:02:35 GMT+08:00

----End

Example 1: Set Policy Type to Number of Days

The update time of Nginx v1 image and Nginx v2 image is shown in the following figure.

Figure 4-18 Image tags

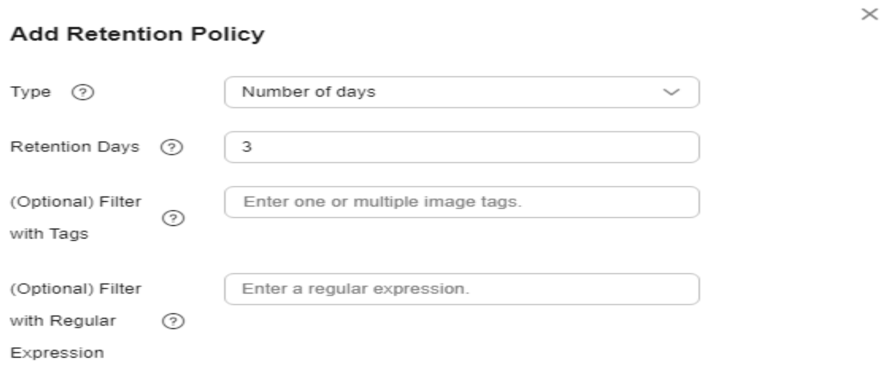


□	Image Tag	Size	Updated	Image Pull Command
□	v2	52.2 MB	Sep 01, 2021 15:29:53 GMT+08:00	docker pull swr.[redacted]-3.myhuaweicloud.com/h...
□	v1	52.2 MB	Aug 27, 2021 14:27:45 GMT+08:00	docker pull swr.[redacted]-3.myhuaweicloud.com/h...

1. Add a retention policy.

   Set **Policy Type** to **Number of days**, and **Count Limit** to **3**.

   Figure 4-19 Adding a retention policy

   Add Retention Policy

   Type: Number of days

   Retention Days: 3

   (Optional) Filter with Tags: Enter one or multiple image tags.

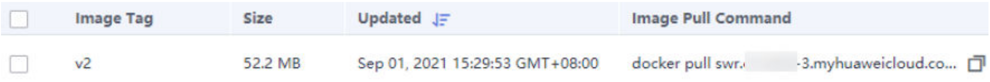
   (Optional) Filter with Regular Expression: Enter a regular expression.

2. Check whether the retention policy has taken effect.

   Check **Retention Logs**. Nginx v1 image has been stored for more than three days (the current time is 2021/09/01 16:00:00). Therefore, it is automatically removed.

   Check **Image Tag**. Only Nginx v2 image is left.

   Figure 4-20 Image tag v2

□	Image Tag	Size	Updated	Image Pull Command
□	v2	52.2 MB	Sep 01, 2021 15:29:53 GMT+08:00	docker pull swr.[redacted]-3.myhuaweicloud.co...

   The retention policy has taken effect.

Example 2: Set Policy Type to Number of Tags, and Specify Regular Expression Filter

Click **Image Tags** tab page. Nginx v1 image, Nginx v2 image, Nginx v1.0.0 image and Nginx v2.0.0 image are shown in **Image tags**.

Figure 4-21 Nginx image tags

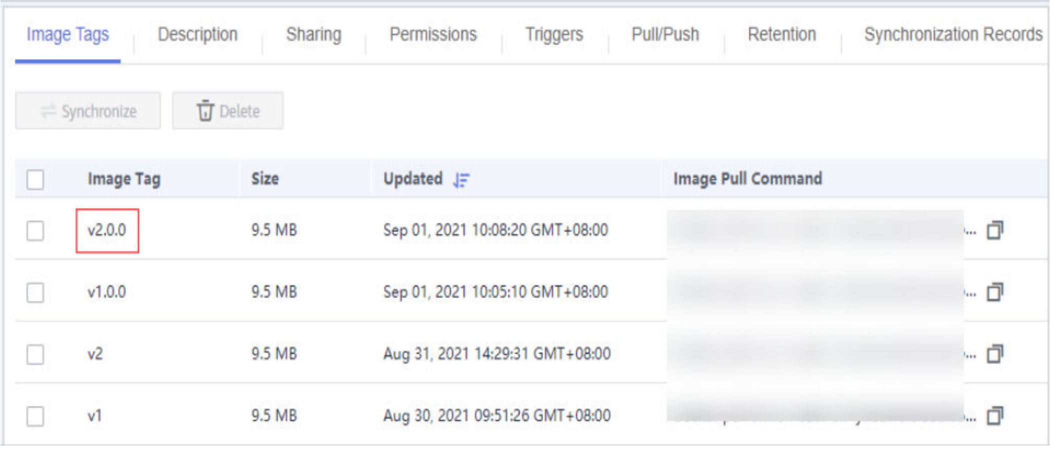


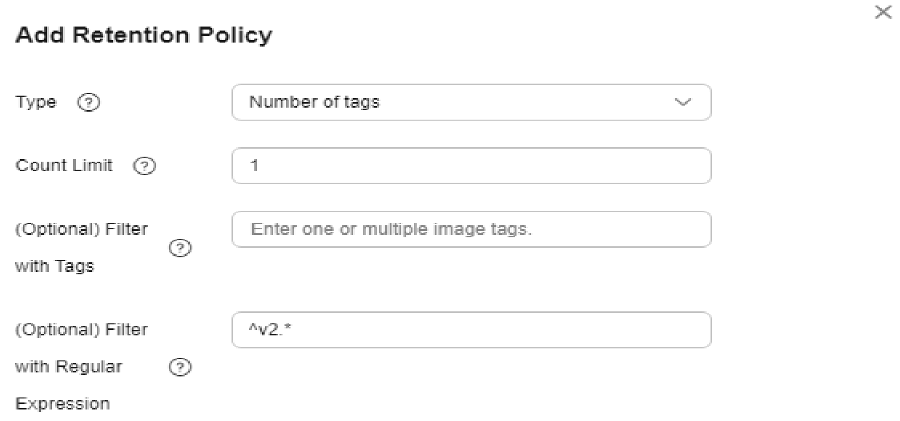
Image Tags | Description | Sharing | Permissions | Triggers | Pull/Push | Retention | Synchronization Records
⇄ Synchronize
Delete

□	Image Tag	Size	Updated	Image Pull Command
□	v2.0.0	9.5 MB	Sep 01, 2021 10:08:20 GMT+08:00	[redacted]...
□	v1.0.0	9.5 MB	Sep 01, 2021 10:05:10 GMT+08:00	[redacted]...
□	v2	9.5 MB	Aug 31, 2021 14:29:31 GMT+08:00	[redacted]...
□	v1	9.5 MB	Aug 30, 2021 09:51:26 GMT+08:00	[redacted]...

1. Add a retention policy.

   Set **Policy Type** to **Number of tags**, **Count Limit** to **1**, and **Regular Expression Filter** to **^v2.***.

   Figure 4-22 Adding a retention policy

   Add Retention Policy

   Type: Number of tags

   Count Limit: 1

   (Optional) Filter with Tags: Enter one or multiple image tags.

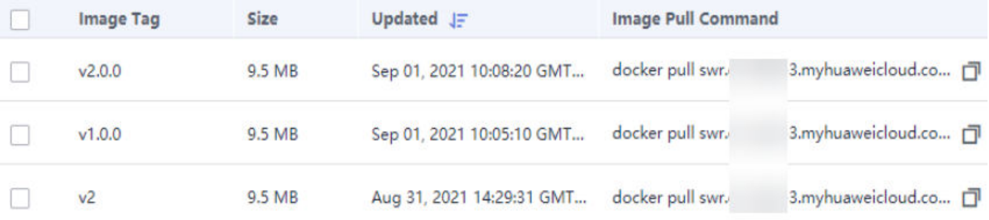
   (Optional) Filter with Regular Expression: ^v2.*

2. Check whether the retention policy has taken effect.

   Before the retention policy takes effect, Nginx v2 image and Nginx v2.0.0 image are filtered for matching the regular expression. Only one of Nginx v1 image and Nginx v1.0.0 image will be stored. Nginx v1 image will be removed because it is older.

   Check **Retention Logs** and **Image Tag**. If Nginx v1 image is removed, the retention policy has taken effect.

   Figure 4-23 Image tags

□	Image Tag	Size	Updated	Image Pull Command
□	v2.0.0	9.5 MB	Sep 01, 2021 10:08:20 GMT...	docker pull swr.[redacted]3.myhuaweicloud.co...
□	v1.0.0	9.5 MB	Sep 01, 2021 10:05:10 GMT...	docker pull swr.[redacted]3.myhuaweicloud.co...
□	v2	9.5 MB	Aug 31, 2021 14:29:31 GMT...	docker pull swr.[redacted]3.myhuaweicloud.co...

The following regular expressions are for your reference:

- ^[0-9]*$: filters out tags consisting of numbers.
- ^.{2,5}$: filters out tags with a length ranging from 2 to 5 characters.
- ^[a-z]+$: filters out tags consisting of lowercase letters.
- ^[A-Za-z0-9]+$: filters out tags consisting of letters and numbers.

⚠ CAUTION

If there is an OR (|) operator in a regular expression, enclose the OR part in parentheses, or the regular expression will be parsed incorrectly and all tags of the image will be removed.

For example, if you only want to retain tags containing a or s, the regular should be (.*a.*|.*s.*).

4.9 Configuring Automatic Image Synchronization Between Regions

Scenario

You can configure newly pushed images to be automatically synchronized to image repositories in other regions.

NOTE

After you configure automatic image synchronization, image updates will also be synchronized to target repositories. However, images that were pushed to repositories before automatic image synchronization was enabled will not be automatically synchronized.

For details on how to synchronize pushed images before you set the automatic synchronization, see **Can Existing Images be Automatically Synchronized**.

Notes and Constraints

- Only accounts and users with administrator permissions can configure automatic image synchronization.
- Currently, images can be synchronized only among the following regions: CN North-Beijing1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN North-Ulanqab1, CN-Hong Kong, AP-Singapore, AP-Bangkok, and AF-Johannesburg.

Procedure

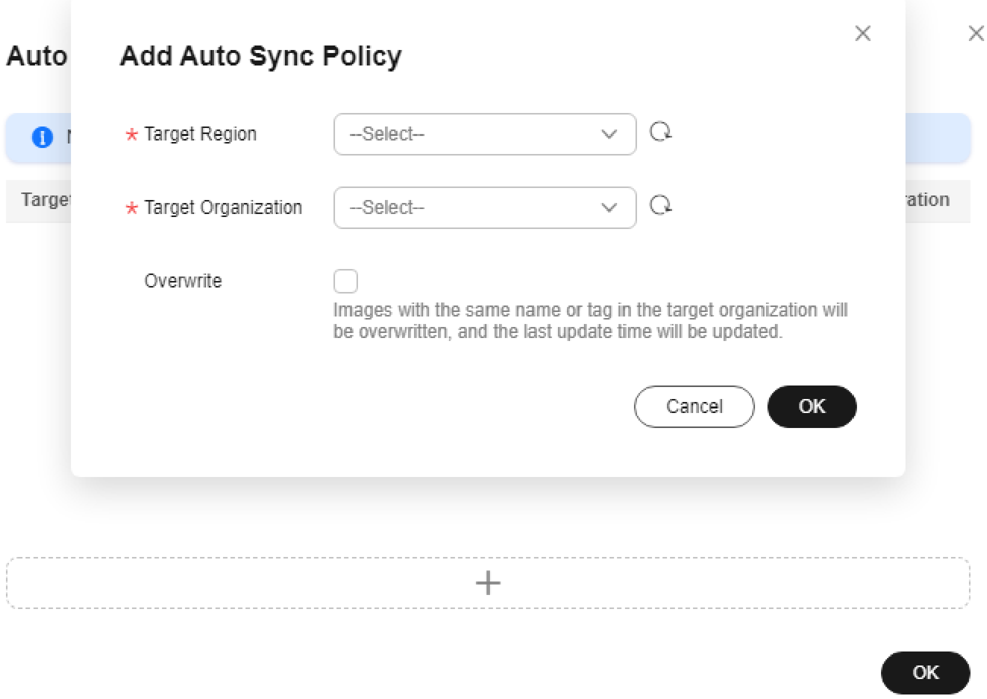
Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane, choose **My Images** and click the target image.

Step 3 On the image details page, click **Set Auto Sync** in the upper right.

Step 4 Click +. Select a target region and a target organization. Click **OK**.

Figure 4-24 Configuring automatic image synchronization



Images with the same name or tag in the target organization will be overwritten, and the last update time will be updated.

- **Target Region**: The target region for image synchronization, for example, CN-Hong Kong.
- **Target Organization**: The target organization to which the image will be synchronized.
- **Overwrite**:

  Select this option if you want to overwrite any image with the same name and tag in the target organization.

  Deselect this option if you do not want to overwrite images in the target organization. If the image you are synchronizing has a duplicate name and tag with an image in the target organization, the synchronization will be canceled and you will receive a notification.

Step 5 On the **Synchronization Records** tab page of image details page, you can view the details of each synchronization task, including the start time, image tag, task status, type, and duration.

----End

4.10 Image Center

Scenario

SWR provides a large number of public images. You can add public container images to your favorites and push them to your repository.

Notes and Constraints

This function is not supported in the CN North-Ulanqab1, AP-Jakarta, LA-Mexico City1, LA-Mexico City2, and LA-Sao Paulo1 regions.

Adding an Image to Favorites

Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane, choose **Image Resources** > **Image Center**.

Step 3 In the image list, select the desired image and click ☆ on the right.

You can view all your favorite images on the **My Favorites** page.

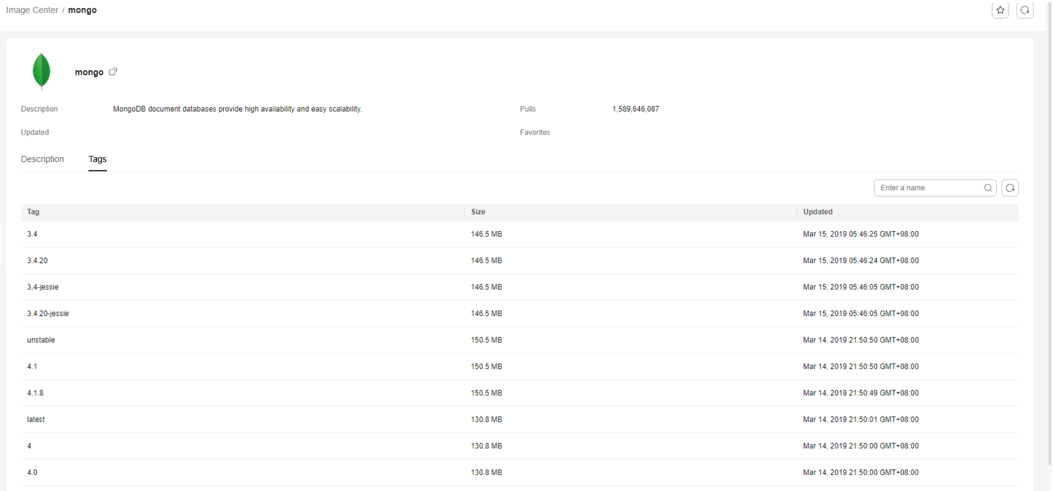
----End

Pulling an Image from the Image Center

You can directly pull an image from the Image Center without specifying a repository address. For example, you can **connect the VM where the container engine resides with SWR** and run the following command to directly pull the **mongo** image:

docker pull mongo:*4.1*

Figure 4-25 mongo image details



Description MongoDB document databases provide high availability and easy scalability.
Pulls 1,589,646,087
Updated
Favorites

Description Tags

Tag	Size	Updated
3.4	146.5 MB	Mar 15, 2019 05:46:25 GMT+08:00
3.4.20	146.5 MB	Mar 15, 2019 05:46:24 GMT+08:00
3.4-jessie	146.5 MB	Mar 15, 2019 05:46:05 GMT+08:00
3.4.20-jessie	146.5 MB	Mar 15, 2019 05:46:05 GMT+08:00
unstable	150.5 MB	Mar 14, 2019 21:50:50 GMT+08:00
4.1	150.5 MB	Mar 14, 2019 21:50:50 GMT+08:00
4.1.8	150.5 MB	Mar 14, 2019 21:50:49 GMT+08:00
latest	130.8 MB	Mar 14, 2019 21:50:01 GMT+08:00
4	130.8 MB	Mar 14, 2019 21:50:00 GMT+08:00
4.0	130.8 MB	Mar 14, 2019 21:50:00 GMT+08:00

For details about image pull, see **Pulling an Image**.

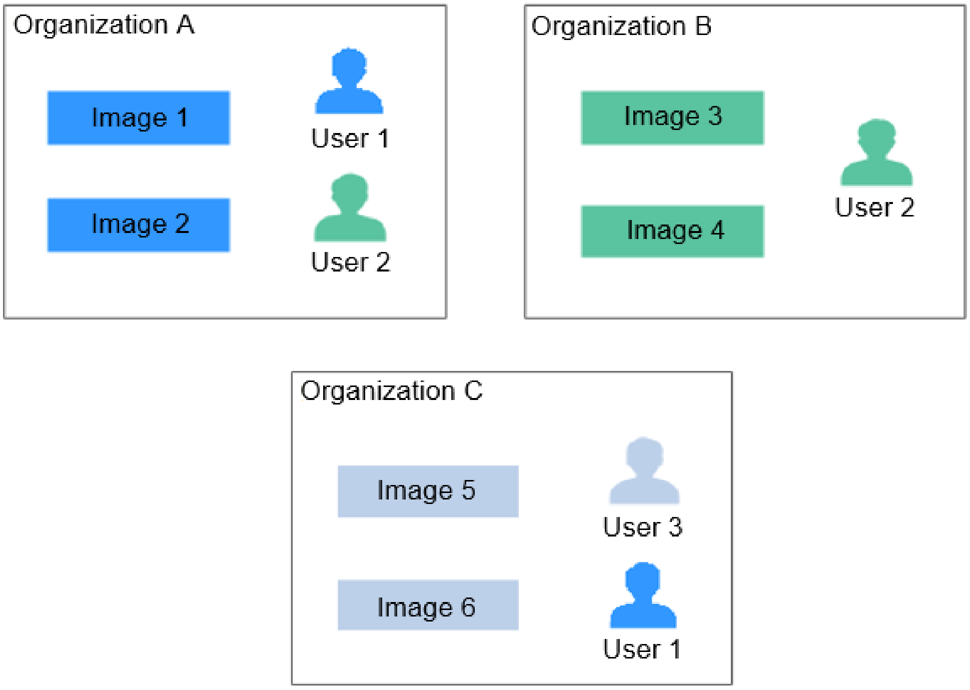
5 Organization Management

Scenario

Organizations enable efficient management of images. Organizations are used to isolate image repositories. With each organization being limited to one company or department, images can be managed in a centralized and efficient manner. An image name needs to be unique within an organization. The same IAM user can access different organizations as long as the user has sufficient permissions, as shown in **Figure 5-1**.

You can grant different permissions, namely, read, write, and manage, to IAM users under the same account. For details, see **User Permissions**.

Figure 5-1 Organization



Creating an Organization

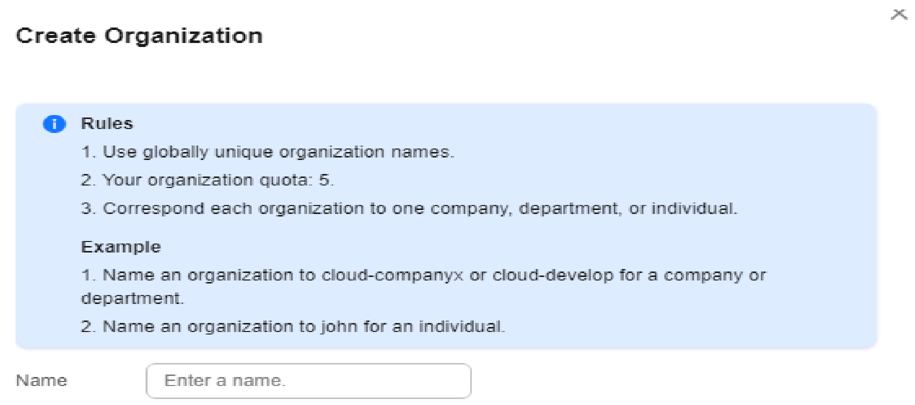
You can create organizations based on the organizational structure of your enterprise to facilitate image resource management. Create an organization before you push an image.

Step 1 Log in to the **SWR console**.

Step 2 Click 📍 in the upper left corner and select the desired region and project.

Step 3 Click **Organizations** in the navigation pane.

Step 4 Click **Create Organization** in the upper right corner of the page. In the dialog box that is displayed, enter the **Name** and click **OK**.



Create Organization

Rules

1. Use globally unique organization names.
2. Your organization quota: 5.
3. Correspond each organization to one company, department, or individual.

Example

1. Name an organization to cloud-companyx or cloud-develop for a company or department.
2. Name an organization to john for an individual.

Name: Enter a name.

NOTE

- The organization name must be globally unique. If a message is displayed indicating that the organization already exists, the organization name may have been used by another user. Use another organization name.
- A user can create organizations only after being granted the **SWR Admin** or **Tenant Administrator** policy in IAM.

----End

Viewing the Images of an Organization

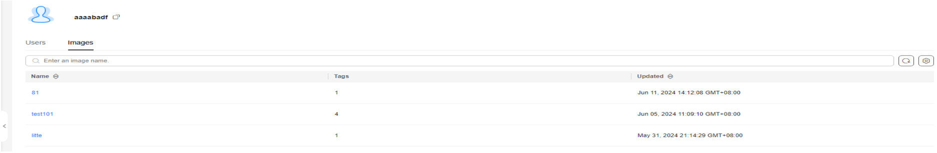
After you create an organization and push images to it, you can view the image list of the organization.

Step 1 Log in to the **SWR console**.

Step 2 Click 📍 in the upper left corner and select the desired region and project.

Step 3 In the navigation pane, choose **Organizations**. On the page displayed, click the desired organization name in the list.

Step 4 To view the images of this organization, click the **Images** tab.



aaaabadf

Name	Tags	Updated
81	1	Jun 11, 2024 14:12:08 GMT+08:00
test101	4	Jun 05, 2024 11:09:10 GMT+08:00
litte	1	May 31, 2024 21:14:29 GMT+08:00

----End

Deleting an Organization

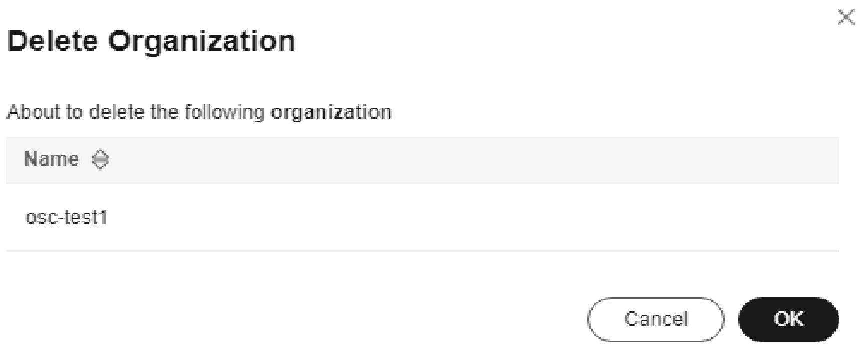
Before deleting an organization, delete all the images in the organization.

Step 1 Log in to the **SWR console**.

Step 2 Click ⌖ in the upper left corner and select the desired region and project.

Step 3 In the navigation pane, choose **Organizations**.

Step 4 In the upper right corner of the organization, click **Delete**. Then, click **OK**.



Delete Organization

About to delete the following organization

Name
osc-test1

----End

6 User Permissions

Scenario

To manage SWR permissions, you can use Identity and Access Management (IAM). For details about how to set permissions, see **Creating a User and Granting SWR Permissions**. If you have the SWR Admin or Tenant Administrator permission, you become an admin user of SWR. You can grant permissions to other IAM users in SWR.

NOTE

An admin user is granted image management permission of all organizations by default, even if the user is not in the authorized user list of the organizations.

If you are not an SWR admin user, you can request an SWR admin user to grant you permissions to read, write, or manage a specific image or images in a specific organization.

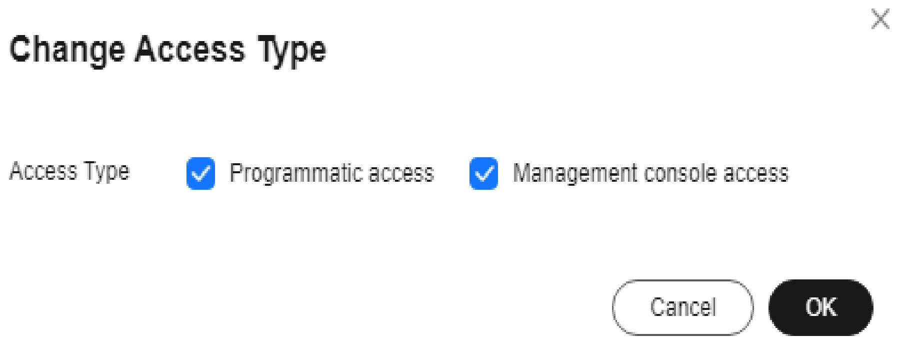
Scenarios

- Example 1: An IAM user having the ServiceStage Developer permission (SWR read-only permission) wants to pull the **Nginx** image created by the SWR administrator in the **group** organization.

  Solution: The SWR administrator grants the **read** permission on the **Nginx** image details page to the IAM user and then the image can be pulled.
- Example 2: An SWR administrator wants to grant an external user the permission to push images to the organization, but the user is not allowed to log in to the console and can only push images through the container engine client.

  Solution: The SWR administrator grants the **edit** permission to the user on the **Users** tab page of the organization details page and set **Access Type** to **Programmatic access** in IAM.

Figure 6-1 Changing the access type



Change Access Type

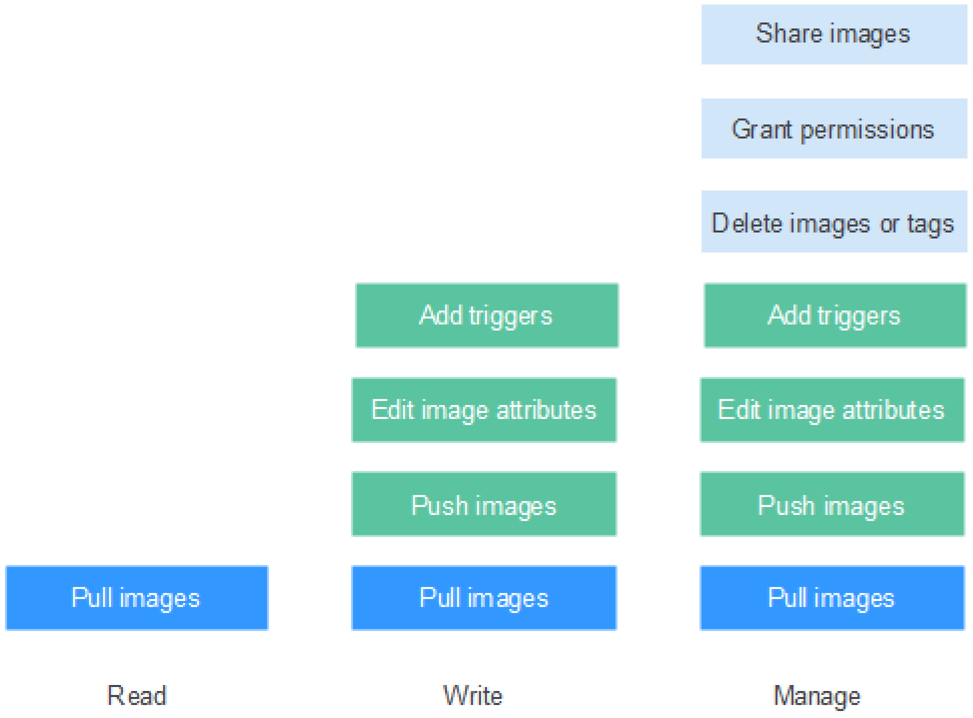
Access Type ☑ Programmatic access ☑ Management console access

Authorization Methods

IAM users in SWR can have permissions by using either of the following methods:

- **Grant permissions of a specific image** to allow IAM users to read, write, and manage the image.
- **Grant permissions of an organization** to allow IAM users to read, write, and manage all the images in the organization.

Figure 6-2 User permissions



You can add the following three types of permissions to users:

- Read: Users can only pull images.
- Write: Users can pull and push images, edit image attributes, and add triggers.
- Manage: Users can pull and push images, delete images or tags, edit image attributes, grant permissions, add triggers, and share images with other users.

NOTE

To upload images to an organization, you require the write or manage permission for the organization to which images are uploaded. Write and manage permissions added on the image details pages will not be sufficient to upload images.

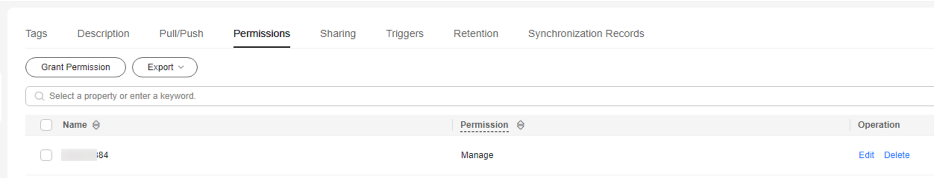
Granting Permissions of a Specific Image

To allow IAM users of your account to read, write, and manage a specific image, add the required permissions to the users on the details page of this image.

Step 1 Log in to the **SWR console**.

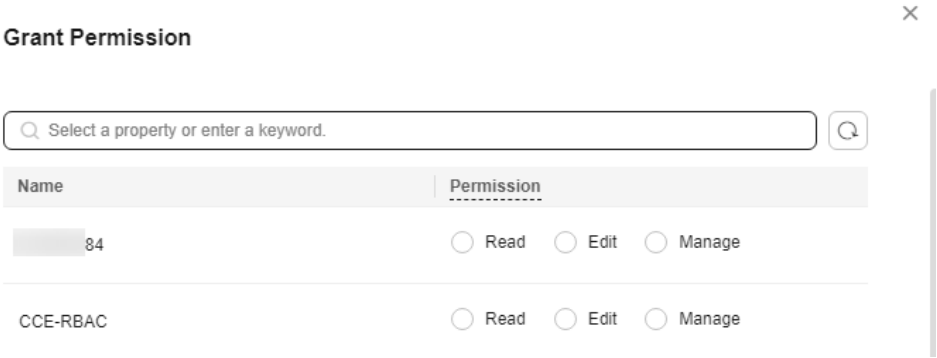
Step 2 In the navigation pane, choose **My Images** and click the desired image.

Step 3 On the image details page, click the **Permissions** tab.



Name	Permission	Operation
[redacted]84	Manage	Edit Delete

Step 4 Click **Add Permission**. On the page displayed, enter an IAM username, and then click **Read, Write, or Manage**. Click **OK** to confirm.



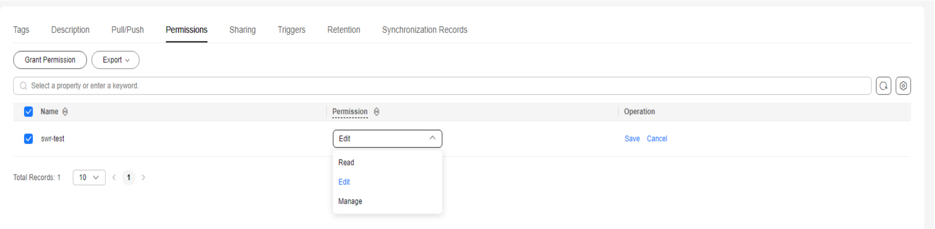
Name	Permission
[redacted]84	○ Read ○ Edit ○ Manage
CCE-RBAC	○ Read ○ Edit ○ Manage

----End

Modifying or Deleting Permissions of a Specific Image

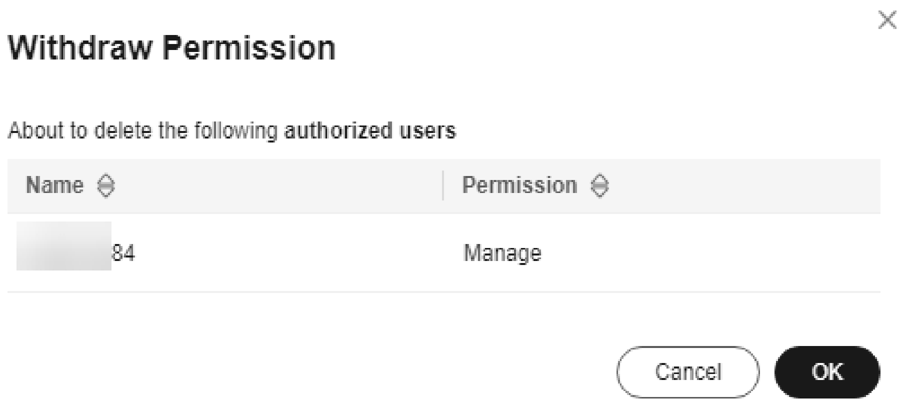
You can also modify or delete user permissions on the image details page.

- To modify permissions, click the **Permissions** tab on the image details page, and click **Edit** in the row of the desired username. Select a permission in the **Permission** drop-down list, and click **Save** in the **Operation** column.



	Name	Permission	Operation
☑	swr-test	Edit	Save Cancel

- To delete permissions, click **Delete** in the row of the desired username on the **Permissions** tab page, and then click **OK**.



Withdraw Permission

About to delete the following authorized users

Name	Permission
[redacted]84	Manage

Granting Permissions of an Organization

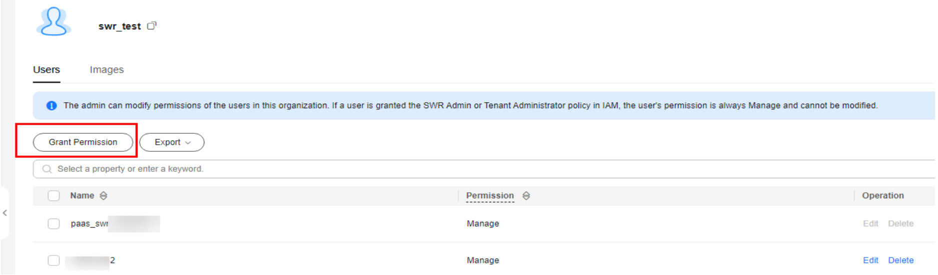
After an IAM user is created, the administrator needs to grant permissions to the user in the organization so that the user can read, edit, and manage images in the organization.

Only accounts and IAM users who have the **Manage** permission can add permissions for other users.

Step 1 Log in to the **SWR console**.

Step 2 In the navigation pane, choose **Organizations**. Then click **View Details** in the row of the desired organization.

Step 3 On the **Users** tab page, click **Add Permission**. In the dialog box displayed, enter an IAM username, select permissions for the user and click **OK**.



swr_test

The admin can modify permissions of the users in this organization. If a user is granted the SWR Admin or Tenant Administrator policy in IAM, the user's permission is always Manage and cannot be modified.

Select a property or enter a keyword.

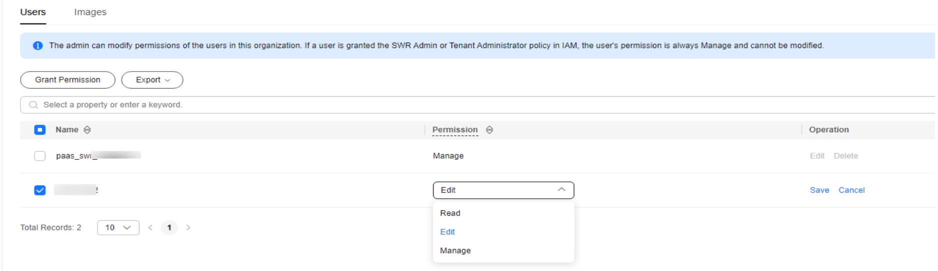
Name	Permission	Operation
paas_swr[redacted]	Manage	Edit Delete
[redacted]2	Manage	Edit Delete

----End

Modifying or Deleting Permissions of an Organization

You can also modify and delete user permissions of an organization.

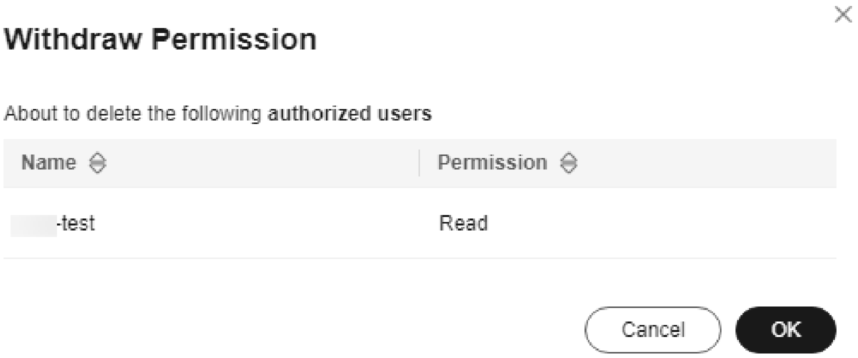
- To modify permissions, click **Edit** in the row of the desired username on the **Users** tab page. Select a permission in the **Permission** drop-down list, and click **Save** in the **Operation** column.



The admin can modify permissions of the users in this organization. If a user is granted the SWR Admin or Tenant Administrator policy in IAM, the user's permission is always Manage and cannot be modified.

	Name	Permission	Operation
□	paas_swr_[redacted]	Manage	Edit Delete
☑	[redacted]	Edit	Save Cancel

- To delete permissions, click **Delete** in the row of the desired username on the **Users** tab page, and then click **OK**.



Withdraw Permission

About to delete the following authorized users

Name	Permission
[redacted]-test	Read

7 Auditing

7.1 SWR Operations Supported by CTS

Scenario

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

With CTS, you can record operations associated with SWR for future query, audit, and backtrack operations.

Key Operations Recorded by CTS

Table 7-1 SWR Shared Edition operations recorded by CTS

Operation	Resource Type	Trace Name
Creating namespace permissions	usernamespaceauth	createUserNamespaceAuth
Modifying namespace permissions	usernamespaceauth	updateUserNamespaceAuth
Deleting namespace permissions	usernamespaceauth	deleteUserNamespaceAuth
Creating a software package	package	createPackage
Modifying a software package	package	updatePackage
Deleting a software package	package	deletePackage
Creating a repository	repository	createRepository

Operation	Resource Type	Trace Name
Modifying a repository	repository	updateRepository
Deleting a repository	repository	deleteRepository
Creating a version	version	createVersion
Modify a version	version	updateVersion
Deleting a version	version	deleteVersion
Uploading an image package	image	uploadImagePackage
Uploading a file	file	uploadFile
Downloading a file	file	downloadFile
Deleting a file	file	deleteFile
Creating an organization	usernamespace	createUserNamespace
Deleting an organization	usernamespace	deleteUserNamesapce
Adding an image to favorites	usercollections	createUserCollections
Removing an image from favorites	usercollections	deleteUserCollections
Creating a trigger	trigger	createTrigger
Modifying a trigger	trigger	updateTrigger
Deleting a trigger	trigger	deleteTrigger
Granting permissions of an image repository	userrepositoryauth	createUserRepositoryAuth
Modifying permissions of an image repository	userrepositoryauth	updateUserRepositoryAuth
Deleting permissions of an image repository	userrepositoryauth	deleteUserRepositoryAuth
Creating an image repository	imagerepository	createImageRepository
Modifying an image repository	imagerepository	updateImageRepository

Operation	Resource Type	Trace Name
Deleting an image repository	imagerepository	deleteImageRepository
Deleting an image tag	imagetag	deleteImageTag
Generating a login command	dockerlogincmd	createDockerConfig
Creating a shared image	imagerepositoryaccess-domain	createImageRepositoryAccess-Domain
Modifying a shared image	imagerepositoryaccess-domain	updateImageRepositoryAccessDomain
Deleting a shared image	imagerepositoryaccess-domain	deleteImageRepositoryAccess-Domain
Downloading an image layer	downloadimagelayer	downloadimagelayer

7.2 Viewing Logs in CTS

Scenario

After you enable CTS, the system starts recording operations performed on SWR resources. CTS stores operation records generated within a week.

This section describes how to view the records on the CTS console.

Procedure

Step 1 Log in to the CTS console. In the upper right corner of the page, click "Go to Old Edition".

Step 2 In the navigation pane, choose **Trace List**.

Step 3 Set the filter criteria and click **Query**.

The following filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

  Select the desired filter criteria from the drop-down lists, and set **Trace Type** to **Management** and **Trace Source** to **SWR**.

  If you set **Search By** to **Resource ID**, you need to enter a resource ID. Only whole word match is supported.

- **Operator**: Select a specific operator from the drop-down list.
- **Trace Status**: Select one of **All trace statuses**, **Normal**, **Warning**, and **Incident**.
- Time range: You can select **Last 1 hour**, **Last 1 day**, **Last 1 week**, or **Customize** in the upper right corner.

Step 4 On the left of the target record, click ⌄ to view details.

Step 5 Click **View Trace** in the **Operation** column. The trace structure details are displayed.

----End

A Change History

Release Date	Description
2021-09-02	This issue is the seventh official release, which incorporates the following change: Added configuration examples of adding triggers and a retention policy in **Adding a Trigger** and **Adding an Image Retention Policy**.
2021-06-30	This issue is the sixth official release, which incorporates the following change: Revised the descriptions in **Obtaining a Long-Term Valid Login Command** and **User Permissions**.
2019-11-30	This issue is the fifth official release, which incorporates the following change: Supported an image retention policy. For details, see **Adding an Image Retention Policy**.
2019-02-28	This issue is the fourth official release, which incorporates the following change: Added automatic image synchronization between regions. For details, see **Configuring Automatic Image Synchronization Between Regions**.
2018-07-30	This issue is the third official release, which incorporates the following change: Added the image center. For details, see **Image Center**.
2018-04-10	This issue is the second official issue, which incorporates the following changes: Added image sharing between accounts. For details, see **Sharing a Private Image**.
2018-03-02	This issue is the first official release.