Software Repository for Container

User Guide

Issue 01

Date 2024-11-08

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

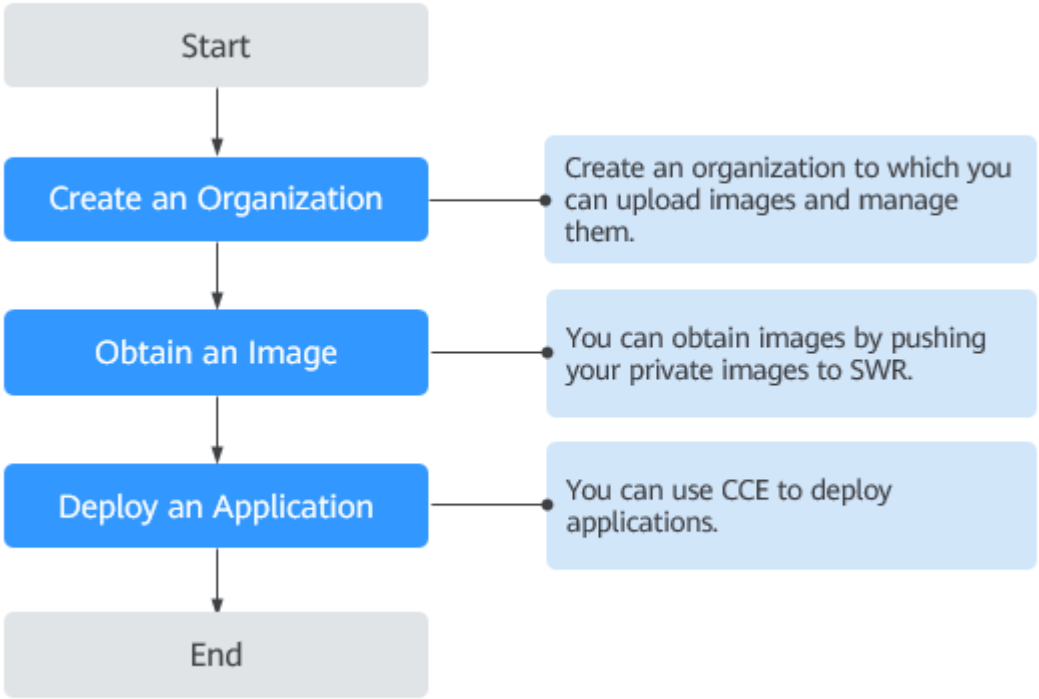
1 Overview....1
2 Permissions Management....2
2.1 Creating a User and Granting Permissions....2
3 Basics of Docker....4
4 Image Management....7
4.1 Pushing an Image Through a Container Engine Client....7
4.2 Obtaining a Long-Term Valid Docker Login Command....9
4.3 Obtaining a Long-Term Valid containerd Pull/Push Command....11
4.4 Uploading an Image Through the SWR Console....12
4.5 Pulling an Image....13
4.6 Setting Image Attributes....15
4.7 Sharing Private Images....16
4.8 Adding a Trigger....17
4.9 Adding an Image Retention Policy....19
4.10 Image Center....20
5 Organization Management....22
6 User Permissions....25
7 Auditing....28
7.1 SWR Operations Supported by CTS....28
7.2 Viewing Logs in CTS....30

1 Overview

SoftWare Repository for Container (SWR) allows you to easily manage the full lifecycle of container images and facilitates secure deployment of images for your applications.

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 use triggers to automatically update applications when images are updated.

Figure 1-1 How SWR works



2 Permissions Management

2.1 Creating a User and Granting Permissions

This section describes how to use **IAM** for fine-grained permission management on your SWR resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SWR resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a cloud account or cloud service to perform efficient O&M on your SWR resources.

If your account does not need individual IAM users, you may skip this section.

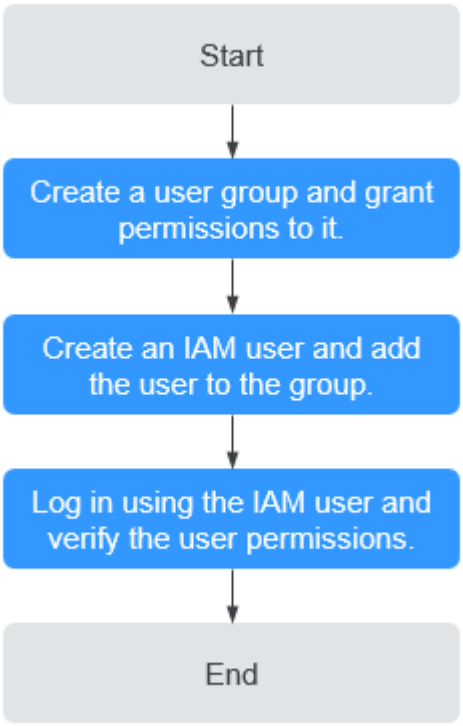
This section describes the procedure for granting permissions (see **Figure 2-1**).

Prerequisite

Learn about the permissions (see **Permissions Management**) supported by SWR and choose policies or roles according to your requirements.

Process Flow

Figure 2-1 Process for granting SWR permissions



1. **Create a user group and assign permissions**.
2. **Create an IAM user and add the user to a user group**.
3. **Log in** as the IAM user and verify permissions.

   Log in to the management console as the created user. Switch to the authorized region. Perform the following operations. If they can be successfully performed, the permissions are successfully granted.

   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**, 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 Docker

Docker is an open-source container engine which allows you to create a lightweight, portable, and self-sufficient container for any application. SWR is compatible with Docker, allowing you to use Docker CLI and APIs to manage your images.

Installing Docker

Before installing Docker, get a basic understanding of what Docker is and how it works. For more information, see **Docker Documentation**.

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

NOTE

- To use SWR, the Docker version must be between 1.11.2 (included) and 24.0.9 (included).
- Bind an elastic IP address first if your server runs in a private network as the installation requires Internet connection.

On a device running Linux, run the following commands to quickly install Docker:

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

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 device running Docker as a root user.

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

mkdir mynginx

cd mynginx

touch Dockerfile

Step 3 Edit 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 new layer. One of its syntax forms is RUN <command>. In this example, the **echo** command is executed to display **Hello, SWR!**

Save the changes 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 Docker 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 device running Docker as a root user.

Step 2 Run the following command to list 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.

Sample:

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

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

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

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

----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***

Sample:

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


4 Image Management

4.1 Pushing an Image Through a Container Engine Client

Scenario

You can run **docker push** (Docker) or **ctr push** (containerd) on the server where the container engine client is installed to push an image to SWR.

Notes and Constraints

- Each image layer cannot exceed 10 GB.
- The Docker version must be between 1.11.2 (included) and 24.0.9 (included).

Prerequisites

- You have created an organization in SWR. For details, see **Creating an Organization**.
- If you use an ECS that is not a CCE node to connect to SWR using a private network address, configure **insecure-registries** as follows:
  a. Modify the **/etc/docker/daemon.json** file. If the file does not exist, manually create it. Add the following content to the file:

```
{
   "insecure-registries": [
      "{Intranet address}"
   ]
}
```

  To obtain the value of {*Intranet address*}, log in to the SWR console. On the **Dashboard** page, click **Generate Login Command** and obtain the private network address in the private network command.

NOTE

If **insecure-registry** has been configured in the **DOCKER_OPTS** configuration item in the **/etc/default/docker** file, you do not need to modify the **/etc/docker/daemon.json** file.

Run the following command to add the private network IP address to the end of the **DOCKER_OPTS** configuration item:

vi /etc/default/docker

Example:

```
# Use DOCKER_OPTS to modify the daemon startup options. DOCKER_OPTS="--insecure-registry={existing configurations} --insecure-registry={Intranet address}"
```

b. Restart Docker for the configuration to take effect.

sudo systemctl daemon-reload

sudo systemctl restart docker

Docker

Take the **nginx:v1** image built in **Basics of Docker** as an example.

Step 1 Access SWR.

1. Log in to the SWR console and then the VM running Docker as the **root** user.
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.

   NOTE

   - A temporary login command is valid for 24 hours. For details about how to obtain a login command that will remain valid for a long term, see **Obtaining a Long-Term Valid Docker 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 **docker login** command on your Docker client (a device that has Docker installed).

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

Step 2 Run the following command on the device where Docker 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 command:

- [Image name 1:tag 1]: Replace it with the actual name and tag of the image to be pushed.
- [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 .
- [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.

Example:

Step 3 Push the image to the image repository by running the following command:

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

Example:

The following information will be returned upon a successful push:

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

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

----End

containerd

Step 1 Log in to the SWR console.

Step 2 In the navigation pane, choose **My Images** and click the name of your image.

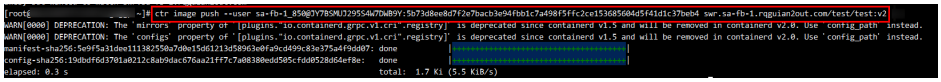
Step 3 On the **Pull/Push** tab page, click **Generate upload instructions** and copy the image push command.

NOTE

The command is only valid for six hours after it is generated. To obtain a long-term valid command, see **Obtaining a Long-Term Valid containerd Pull/Push Command**.

Step 4 Log in to the VM running containerd as the **root** user.

Step 5 Run the command copied in **Step 3** (replace *{Tag}* with the new image tag).



Step 6 Check whether the image is pushed successfully.

----End

FAQ

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

4.2 Obtaining a Long-Term Valid Docker Login Command

Scenario

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

NOTE

For security purposes, you are advised to obtain the command in a development environment.

Process

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

Figure 4-1 Process

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 & Deployment** > **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.
5. Click the user to go to its details page.
6. Click next to **Access Type**.
7. Select **Programmatic access**. (You can select only programmatic access or both access types.)

Step 2 Obtain the region, project name, and image repository address.

1. Log in to the management console, click your username in the upper right corner, and click **My Credentials**.
2. On the **Projects** tab page, search for the project corresponding to the current region.
3. Obtain the image repository address by referring to **Step 1.2**. The domain name at the end of the login command is the image repository address.

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/AS pair provides functions similar to a password. If you already have an AK/SK, skip this step.

1. Log in to the management console, click your username in the upper right corner, and click **My Credentials**.
2. On the **Access Keys** tab page, click **Add Access Key**.
3. Enter the login password and verification code sent to your mailbox or mobile phone.

4. Download the access key, which includes the AK and SK.

   NOTE

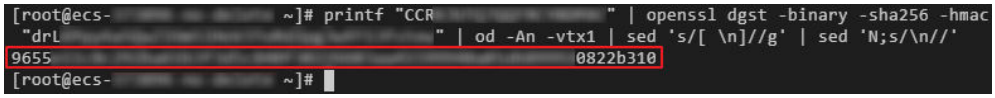
   Keep the access key secure and do not disclose it to any unauthorized personnel.

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//'

In the command, **$AK** and **$SK** indicate the AK and SK obtained in **Step 3** respectively.

Figure 4-2 Sample command output



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

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**.

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

----End

4.3 Obtaining a Long-Term Valid containerd Pull/Push Command

Scenario

This section describes how to obtain a containerd pull/push command that is permanently valid.

NOTE

- For security purposes, you are advised to obtain the commands in a development environment.
- Ensure that you have permission to access the IAM service.

Procedure

Step 1 Obtain the programmatic access permission by referring to **Step 1**.

Step 2 Obtain the resource space name, image repository address, AK, and login key by referring to **Step 2** to **Step 4**.

Step 3 Concatenate the obtained information to form a long-term valid containerd command.

1. Image pull command

ctr image pull --user *[Resource space name]* **@***[AK]***:** *[Login key] [Image repository address]*

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

2. Image push command

ctr image push --user *[Resource space name]* **@***[AK]***:** *[Login key] [Image repository address]*

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

NOTE

- The login key is encrypted and cannot be decrypted into an SK.
- The commands can be executed on other containerd clients to pull and push images.

----End

4.4 Uploading an Image Through the SWR Console

Scenario

This section describes how to upload 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.
- Only image file packages created by Docker 1.11.2 to 24.0.9 can be uploaded.

Prerequisite

- 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, 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.

Step 4 Click **Start Upload**.

When the upload progress is complete, the image is successfully uploaded.

----End

FAQ

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

4.5 Pulling an Image

Scenario

You can use Docker or containerd to pull images from SWR.

Prerequisites

- 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 **SWR Permissions**.
- 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**.

Docker

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

Step 2 Obtain a login command by referring to **Step 1** and access SWR.

Step 3 Log in to the SWR console.

Step 4 In the navigation pane, choose **My Images** and click 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.

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

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

```
# docker images
REPOSITORY                TAG      IMAGE ID       CREATED        SIZE
xxx/group/nginx           v2.0.0   22f2bf2e2b4f   5 hours ago    22.8MB
```


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

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

----End

containerd

Step 1 Log in to the SWR console.

Step 2 In the navigation pane, choose **My Images** and click the name of your image.

Step 3 On the **Tags** tab page, click **containerd command** in the **Operation** column to copy the image pull command. Alternatively, go to the **Pull/Push** tab page to copy the image pull command.

NOTE

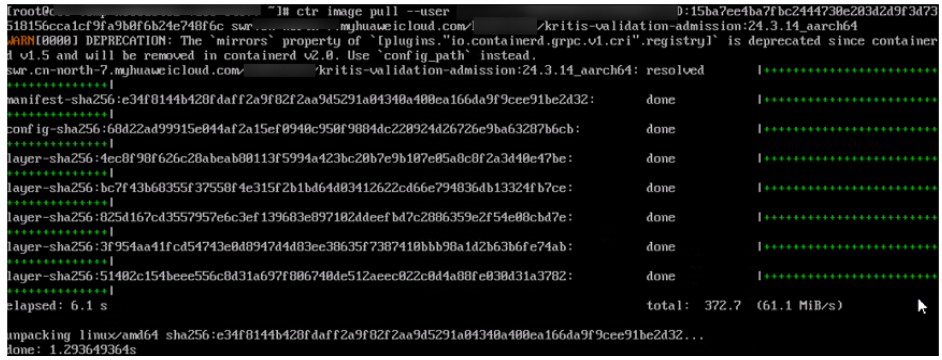
The command is only valid for six hours after it is generated. To obtain a long-term valid command, see **Obtaining a Long-Term Valid containerd Pull/Push Command**.

Step 4 Log in to the VM running containerd as the **root** user.

Step 5 Run the command copied in **Step 3**.

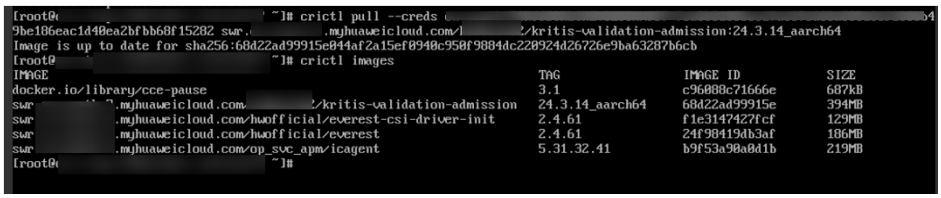
- If the command was copied from the **Operation** column, run it as follows.

- If the command was copied from the **Pull/Push** tab page, run it as follows (replace *{Tag}* with the new image tag).

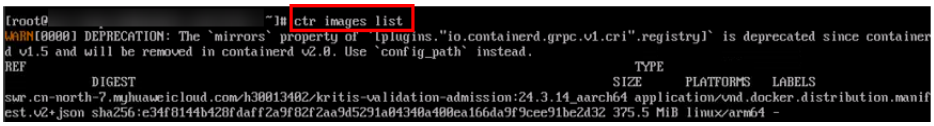


Step 6 Check whether the image is pulled successfully.

- If the command was copied from the **Operation** column, run **crictl images** to check whether the pull is successful.



- If the command was copied from the **Pull/Push** tab page, run **ctr images list** to check whether the pull is successful.



----End

4.6 Setting Image Attributes

Scenario

After uploading an image, you can set image attributes, including its type (public or private), 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, and manage, to allow users to access your private images. For details, see **Granting Permissions for 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. On the page displayed, set **Sharing Type** (**Public** or **Private**), **Category**, and **Description**, and click **OK**.

Table 4-1 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 over private networks. • If your machine and the image repository are in different regions, the node must have access to public networks to pull images from the image repository.

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

----End

4.7 Sharing Private Images

Scenario

You can share your **private images** with other accounts 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 by clicking **My Images** > **Shared Images**. 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 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.

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 4-2**, and click **OK**.

Table 4-2 Sharing an image

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

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

----End

4.8 Adding a Trigger

Scenario

SWR works with Cloud Container Engine (CCE) to achieve automatic application update. When images are updated, these new images can be automatically deployed to update the applications that use these images. You only need to add a trigger to the desired images. Every time these images are updated, they can trigger automatic updates of the applications that use them.

Prerequisite

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

To create an application, log in to the CCE console and create a workload.

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 4-3** and click **OK**.

Table 4-3 Trigger

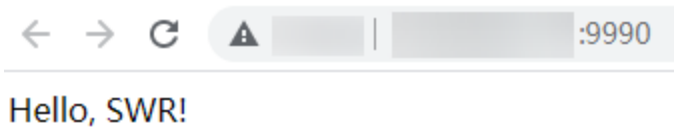
Parameter	Description
Name	The name can contain 1 to 64 characters, and must start with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed. The name cannot end with an underscore or hyphen. Consecutive underscores or hyphens are not allowed and an underscore cannot be placed next to a hyphen.
Condition	The following trigger conditions are supported: • All tags: Trigger when any image tags are generated or updated. • Specific tag: Trigger when a specific image tag is generated or updated. • Tags matching regular expression: Trigger when an image tag that matches the specified 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	Operation that will be triggered when the conditions you set are met. Currently, only application update is supported. You need to specify the application to be updated and the container image of the application.
Status	Select **Enable**.
Trigger Type	Select **CCE**.
Application	Select the container whose image you want to update.

----End

Example

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

Figure 4-3 Nginx deployment



1. Add a trigger to the Nginx image.

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

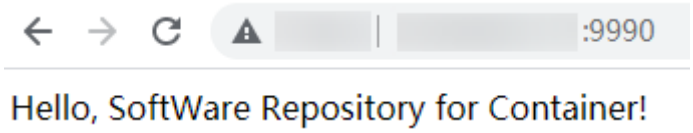
2. Check the image tags. The Nginx image v2 is pushed to SWR. The welcome page of the Deployment created using this new image should display **Hello, SoftWare Repository for Container!**

3. Check whether the deployment is triggered successfully.

   On the **Triggers** tab page, click ⌄ and the trigger is successful.

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

Figure 4-4 Updated Nginx



4.9 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 target image.

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

Table 4-4 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 how many days an image tag can be stored. 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 1000.
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.

----End

4.10 Image Center

Scenario

SWR provides a variety of public images, including official Docker images. You can add official Docker images to **My Favorites** for ease of use.

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, click ☆ next to an image to add the image to favorites.

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

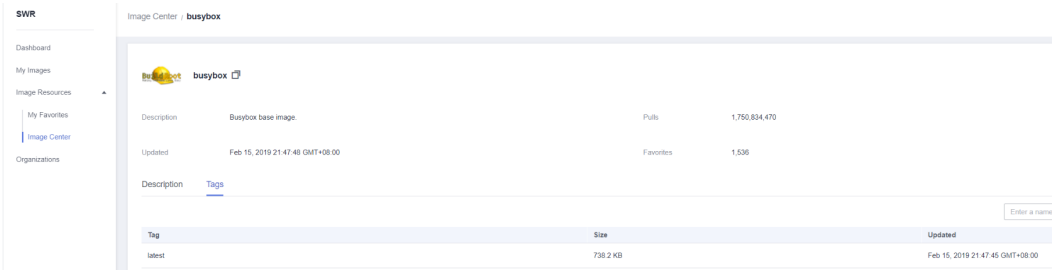
----End

Pulling an Image

You can pull an image without specifying a repository address. For example, you can run the following command to pull the busybox image:

docker pull busybox:latest

Figure 4-5 busybox image details



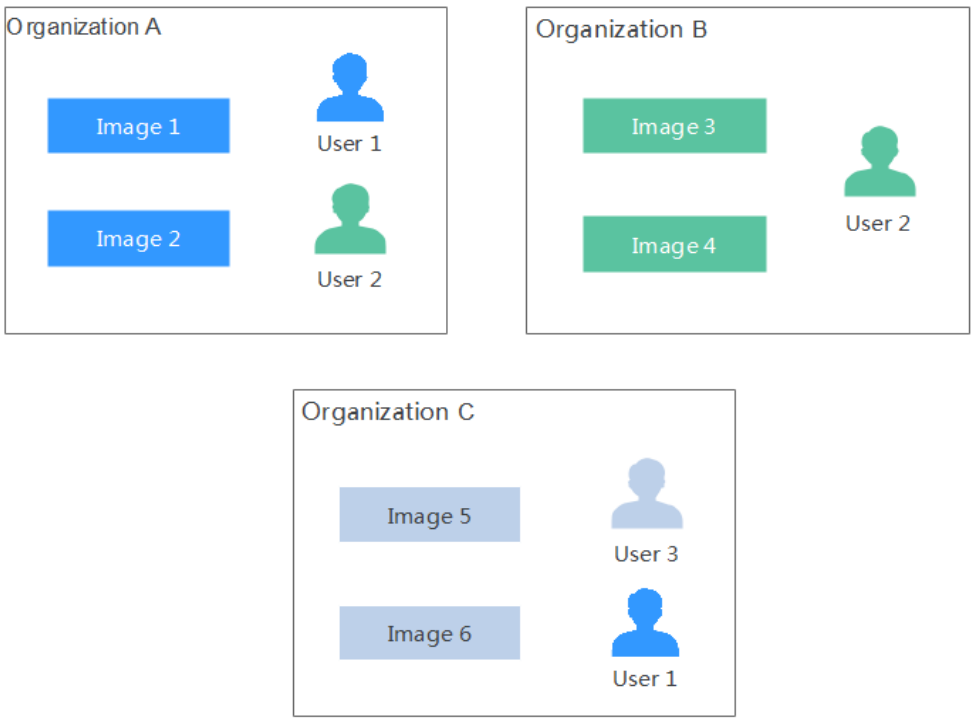
5 Organization Management

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 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 users created by 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 In the navigation pane on the left, choose **Organization Management** and click **Create Organization**. On the page displayed, specify **Organization Name** and click **OK**.

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.
- After a tenant is deleted, residual organization resources may exist. In this case, the message indicating that the organization already exists could also be displayed when you create an organization. Use another organization name.

----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 In the navigation pane, choose **Organization Management**. On the page displayed, click the desired organization name in the list.

Step 3 To view the images of this organization, click the **Images** tab.

----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 In the navigation pane, choose **Organization Management**. On the page displayed, click the desired organization name in the list.

Step 3 Click **Delete** in the upper right corner. In the displayed dialog box, enter **DELETE** as prompted and click **Yes**.

----End

NOTICE

Before you delete a tenant, delete its organizations first; otherwise, residual organization resources may exist. When you create an organization that has the same name with the residual organization, a message is displayed indicating that the organization already exists.

6 User Permissions

Scenario

To manage SWR permissions, you can use Identity and Access Management (IAM). If you have the SWR Administrator or Tenant Administrator permission, you become an admin user of SWR accounts. You can grant permissions to other IAM users in SWR.

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

NOTE

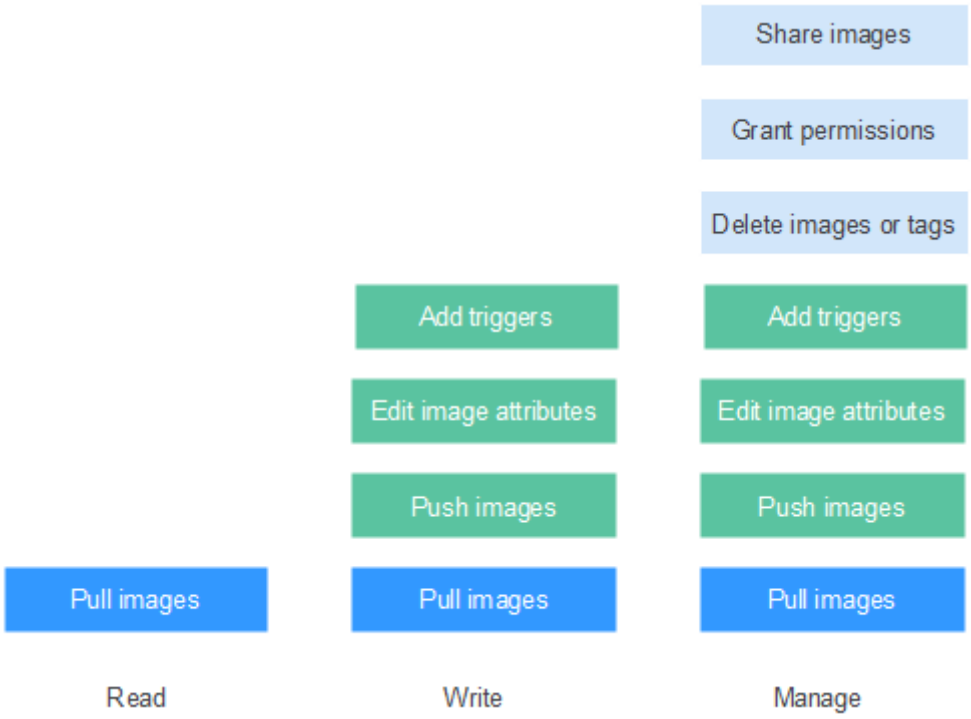
- An SWR account admin user is granted image management permission of all organizations by default, even if the user is not in the authorized user list of the organizations.

Authorization Method

You can grant permissions to users in SWR by using either of the following methods:

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

Figure 6-1 User permissions



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

- Read: Users can only pull images.
- Write: Users can pull and push images and edit image attributes.
- Manage: Users can pull and push images, delete images or tags, edit image attributes, grant permissions, 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 for a Specific Image

To allow users to read, write, and manage a specific image, grant corresponding permissions to them 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.

Step 4 Click **Add Permission**. On the page displayed, click **Read**, **Write**, or **Manage** in the row of the desired username. Click **OK** to confirm.

----End

Modifying or Deleting Permissions for a Specific Image

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

- To modify permissions, click **Modify** in the row of the desired username on the **Permissions** tab page. Select a permission in the **Permission** drop-down list, and click **Save** in the **Operation** column.
- To delete permissions, click **Delete** in the row of the desired username on the **Permissions** tab page, enter **DELETE** in the dialog box displayed, and then click **Yes**.

Granting Permissions for an Organization

To allow users to read, write, and manage all the images in an organization, grant corresponding permissions to them on the details page of this organization.

Only users with the **Manage** permission can grant permissions for other users.

Step 1 Log in to the SWR console.

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

Step 3 On the **Users** tab page, click **Add Permission**. In the dialog box displayed, select permissions for users and click **OK**.

----End

Modifying or Deleting Permissions for an Organization

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

- To modify permissions, click **Modify** 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.
- To delete permissions, click **Delete** in the row of the desired username on the **users** tab page, enter **DELETE** in the dialog box displayed, and then click **Yes**.

7 Auditing

7.1 SWR Operations Supported by CTS

Scenario

CTS records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit, 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 operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Granting permissions for an organization	usernamespaceauth	createUserNamespaceAuth
Modifying permissions for an organization	usernamespaceauth	updateUserNamespaceAuth
Deleting permissions for an organization	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
Granting permissions for an image repository	userrepositoryauth	createUserRepositoryAuth
Modifying permissions for an image repository	userrepositoryauth	updateUserRepositoryAuth
Deleting permissions for an image repository	userrepositoryauth	deleteUserRepositoryAuth
Creating an image repository	imagerepository	createImageRepository
Modifying an image repository	imagerepository	updateImageRepository
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

Operation	Resource Type	Trace Name
Modifying a shared image	imagerepositoryaccess-domain	updateImageRepositoryAccessDomain
Deleting a shared image	imagerepositoryaccess-domain	deleteImageRepositoryAccessDomain

7.2 Viewing Logs in CTS

Scenario

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

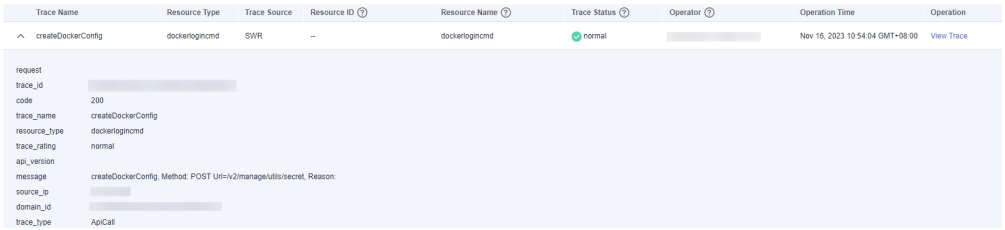
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Viewing Real-Time Traces in the Trace List

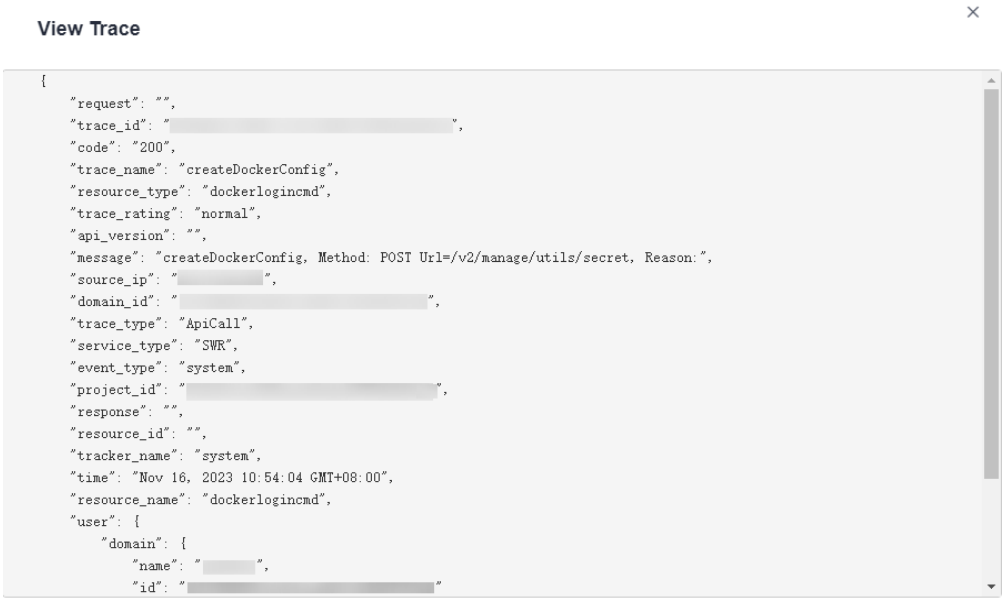
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
5. Click **Query**.
6. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

– Click to view the latest information about traces.

7. Click on the left of a trace to expand its details.



8. Click **View Trace** in the **Operation** column. The trace details are displayed.



9. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces" in the *CTS User Guide*.

