SoftWare Repository for Container

FAQs

Issue 01

Date 2025-09-19

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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

 Copyright © Huawei Technologies Co., Ltd.

1 General FAQ

1.1 What Is SWR?

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

With SWR, you can securely host and efficiently distribute images on the cloud without building or maintaining image repositories by yourselves. In addition, SWR can work with **Cloud Container Engine (CCE)** to smoothly run your applications in containers.

For more information, see **Service Overview**.

1.2 SWR Overview

Is SWR Free?

SWR Basic Edition is free but SWR Enterprise Edition is not.

Can I Query the CPU Architecture (x86 or Arm) of an Image in SWR?

- For a public image, you can log in to the **SWR console**, go to the image center, search for an image, and view its details, including the architectures supported by this image.
- For a private image, you can run **docker inspect** *[Image name:Tag name]* to query the image architecture.

Example: *docker inspect openjdk:7*

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Example

How Many Images Can Be Stored in SWR?

SWR imposes a quota on the maximum number of images that can be stored. For details, see swr_faq_0006.xml#swr_faq_0006/section626111350212.

What Is the Bandwidth of SWR?

The bandwidth of SWR dynamically changes based on actual usage.

Why Cannot I See the ContainerOps Console?

ContainerOps subscription is now suspended. If you have subscribed to ContainerOps before June 25, 2020, you can continue to use it. Sorry for any inconvenience caused.

1.3 How Do I Create a Container Image?

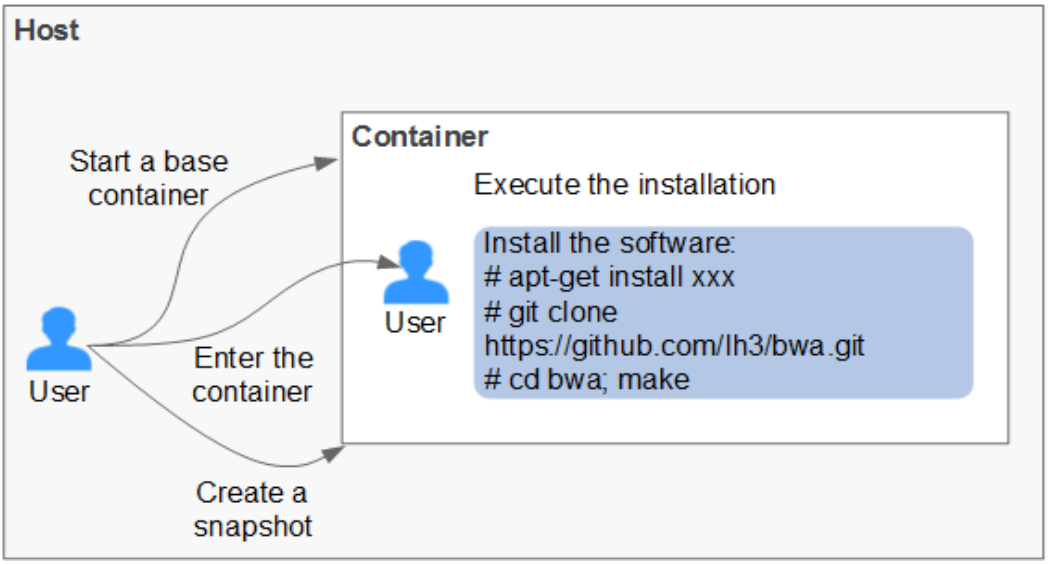
The following two approaches are for you to consider. Approach 1 is for images that will only be updated occasionally whereas approach 2 is for images that will be frequently updated.

- Approach 1: creating a snapshot. This approach involves three key steps: (1) Install a container engine. (2) Start a base container from a base image (for example, Ubuntu image) and install applications. (3) Create a snapshot of the container.
- Approach 2: creating a Dockerfile. This approach involves two key steps: (1) Write software installation instructions into a Dockerfile. (2) Run **docker build** to build an image from the Dockerfile.

Approach 1: Creating a Snapshot

This approach is suitable for images that will only be updated occasionally.

Copyright © Huawei Technologies Co., Ltd.



Procedure:

1. Install a container engine on a host.
2. Start an empty base container in the interactive mode.

   For example, start a CentOS container in the interactive mode.

   docker run -it centos
3. Run the following commands to install the target software:

   yum install XXX

   git clone https://github.com/lh3/bwa.git

   cd bwa;make

   NOTE

   Install Git in advance and check whether an SSH key is set on the local host.
4. Run the **exit** command to exit the container.
5. Create a snapshot.

   docker commit -m "xx" -a "test" container-id test/image:tag

   - **-a**: indicates the author of the base image.
   - **container-id**: indicates the ID of the container you have started in step 2. You can run the **docker ps -a** command to query the container ID.
   - **-m**: indicates the commit message.
   - **test/image:tag**: indicates the repository name/image name:tag name.
6. Run the **docker images** command to list the built container image.

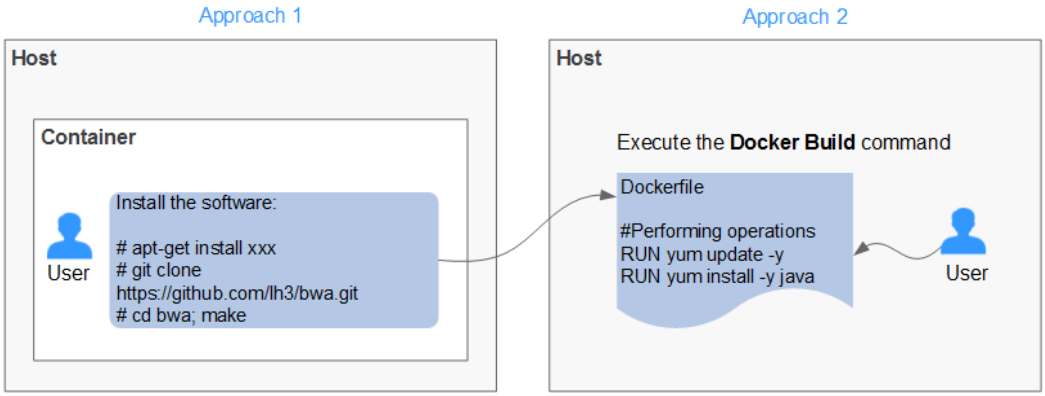
Approach 2: Creating a Dockerfile

This approach is suitable for images that will be frequently updated. In **Approach 1**, you create a snapshot of the whole container. This could be demanding if you need to frequently update your images. In this case, **Approach 2** is put forward to automate the image build process.

The idea behind **Approach 2** is to write the process of **Approach 1** into a Dockerfile and then run the **docker build -t test/image:tag.** command to

 Copyright © Huawei Technologies Co., Ltd.

automatically build an image from the Dockerfile. The period (.) in this command indicates the path to the Dockerfile.



Example Dockerfile:

NOTE

If an external network is required, ensure that network connectivity is available.

```
#Version 1.0.1
FROM centos:latest

# Setting the root user as the executor of subsequent commands
USER root

# Performing operations
RUN yum update -y
RUN yum install -y java

# Using && to concatenate commands
RUN touch test.txt && echo "abc" >>abc.txt

# Setting an externally exposed port
EXPOSE 80 8080 1038

# Adding a network file
ADD https://www.baidu.com/img/bd_logo1.png /opt/

# Setting an environment variable
ENV WEBAPP_PORT=9090

# Setting a work directory
WORKDIR /opt/

# Setting a start command
ENTRYPOINT ["ls"]

# Setting start parameters
CMD ["-a", "-l"]

# Setting a volume
VOLUME ["/data", "/var/www"]

# Setting the trigger operation for a sub-image
ONBUILD ADD . /app/src
ONBUILD RUN echo "on build executed" >> onbuild.txt
```

Basic Syntax of Dockerfile

- FROM:

 Copyright © Huawei Technologies Co., Ltd.

It is used to specify the parent image (base image) from which you are building a new image. Except annotations, a Dockerfile must start with a FROM instruction. Subsequent instructions run in this parent image environment until the next FROM instruction appears. You can create multiple images in the same Dockerfile by adding multiple FROM instructions.

- MAINTAINER:

  It is used to specify the information about the author who creates an image, including the username and email address. This parameter is optional.

- RUN:

  It is used to modify an image. Generally, RUN commands are executed to install libraries, and install and configure programs. After a **RUN** command is executed, an image layer will be created on the current image. The next command will be executed on the new image. The RUN statement can be in one of the following formats:

  - **RUN yum update**: Command that is executed in the **/bin/sh** directory.
  - **RUN ["yum", "update"]**: Directly invoke **exec**.
  - **RUN yum update && yum install nginx**: Use **&&** to connect multiple commands to a RUN statement.

- EXPOSE:

  It is used to specify one or more network ports that will be exposed on a container. If there are multiple ports, separate them by spaces.

  When running a container, you can set **-P** (uppercase) to map the ports specified in EXPOSE to random ports on a host. Other containers or hosts can communicate with the container through the ports on the host.

  You can also use **-p** (lowercase) to expose the ports that are not listed in EXPOSE.

- ADD:

  It is used to add a file to a new image. The file can be a host file, a network file, or a folder.

  - First parameter: source file (folder)
    - If a relative path is used, this path must correspond to the directory where the Dockerfile is located.
    - If a URL is used, the file needs to be downloaded first and then added to the image.
  - Second parameter: target path
    - If the source file is in the .zip or .tar file, the container engine decompresses the file and then adds it to the specified location of the image.
    - If the source file is a compressed network file specified by a URL, the file will not be decompressed.

- VOLUME:

  It is used to create a mount point for a specified path (file or folder) in the image. Multiple containers can share data through the same mount point. Even if one of the containers is stopped, the mount point can still be accessed.

 Copyright © Huawei Technologies Co., Ltd.

- WORKDIR:

  It is used to specify a new work directory for the next command. The directory can be an absolute or a relative directory. WORKDIR can be specified multiple times as required. When a container is started, the directory specified by the last WORKDIR command is used as the current work directory of the container.

- ENV:

  It is used to set an environment variable for running the container. When running the container, you can set **-e** to modify the environment variable or add other environment variables.

  Example:

  docker run -e WEBAPP_PORT=8000 -e WEBAPP_HOST=www.example.com ...

- CMD:

  It is used to specify the default command for starting a container.

- ENTRYPOINT:

  It is used to specify the default command for starting a container. Difference: For ENTRYPOINT, parameters added to the image during container running will be spliced. For CMD, these parameters will be overwritten.

  – If the Dockerfile specifies that the default command for starting a container is **ls -l**, the default command **ls -l** will be run accordingly. For example:

    ▪ **ENTRYPOINT ["ls", "-l"]**: The program and parameter for starting a container are set to be **ls** and **-l** respectively.

    ▪ **docker run centos**: The **docker run centos ls -l** command is run by default for starting a CentOS container.

    ▪ **docker run centos -a**: When the **-a** parameter is added for starting a CentOS container, the **docker run centos ls -l -a** command is run by default.

  – If the Dockerfile specifies that the default command for starting a container is **--entrypoint** but you need to replace the default command, you can add **--entrypoint** to replace the configuration specified in Dockerfile. Example:

    docker run gutianlangyu/test --entrypoint echo "hello world"

- USER:

  It is used to specify the user or UID for running the container, and running the RUN, CMD, or ENTRYPOINT command.

- ONBUILD:

  Trigger command. During image build, the image builder of the container engine saves all commands specified by the ONBUILD command to the image metadata. These commands will not be executed in the process of building the current image. These commands will be executed only when a new image uses the FROM instruction to specify the parent image as the current image.

  Using the FROM instruction to build a child image based on the parent image created by the Dockerfile:

 Copyright © Huawei Technologies Co., Ltd.

ONBUILD ADD. /app/src: The **ADD. /app/src** command is automatically executed.

1.4 How Do I Create an Image Package?

Run the **docker save** command to make the container image into a .tar or .tar.gz package. The command format is as follows:

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

[OPTIONS] can be set to **--output** or **-o**, indicating that the image is exported to a file.

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

1.5 Are There Quotas for SWR Resources?

No quotas are imposed on SWR images. You can push as many images as you need.

Quotas are imposed on the number of organizations a user can create, as shown in **Table 1-1**.

Table 1-1 SWR resource quotas

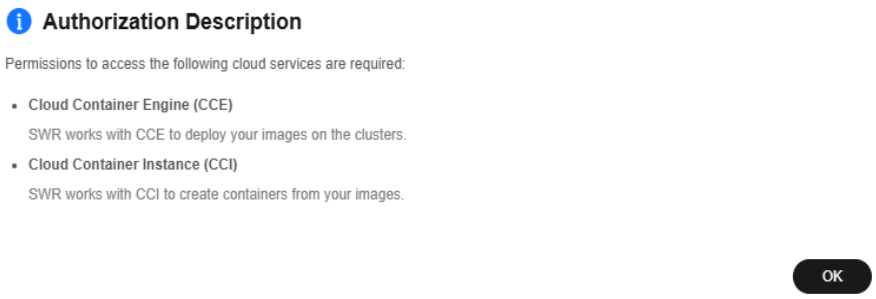
Resource type	Quota
Organization	5

Copyright © Huawei Technologies Co., Ltd.

2 Logins

What Do I Do If Authorization Failure Occurs When I Log In to the SWR Console for the First Time?

Symptom: When you log in to the SWR console for the first time, after you click **OK** in the **Authorization Description** dialog box, the authorization failed.



Solution

- If you have not completed real-name authentication, complete it.
- If your account is in arrears, **renew** it.

What Are the Differences Between Long-Term and Temporary Login Commands?

- Temporary login commands expire 6 hours after they are generated. A temporary login command can be used for temporary use or one-time authorization. For production clusters that require high security, it can be used with periodic refresh.
- Long-term login commands are permanently valid. A long-term login command can be used for preliminary tests, CI/CD pipelines, and image pull to container clusters.
- After you obtain a long-term login command, your temporary login commands can still be valid as long as they are in their validity periods.
- Both long-term and temporary login commands can be used by multiple users at the same time.

 Copyright © Huawei Technologies Co., Ltd.

3 Image Push

How Do I Push an Image to SWR by Calling an API?

Currently, SWR does not provide an API for pushing images. You can push images through the SWR console. For details, see **Pushing an Image**.

Why Is an Image Pushed to SWR Using a Container Engine Client Different in Size from One Uploaded Through the SWR Console?

Symptom

Assume that a nginx image of v2.0.0 is created on the local Docker client. The **docker images** command is run to query **SIZE** of the image. The size is 22.8 MB.

```
$ docker images
REPOSITORY                    TAG          IMAGE ID       CREATED       SIZE
nginx                         v2.0.0       22f2bf2e2b4f   9 days ago    22.8MB
```

1. Run **docker push** to push the image to SWR. The size of the image is **9.5 MB**.
2. On the local Docker client, pack the image into a **.tar** package. Download the **nginx.tar** package to the local host, and upload the package to SWR. The size of the package is **23.2 MB**.

The size of the image pushed through the client is different from that of the image uploaded through the SWR console.

Possible Cause

Image layers are compressed into .tgz packages when images are pushed to SWR using a container engine client, whereas when they are uploaded through the SWR console, they are only packed without being compressed. Therefore, the same image will be of different sizes when it is uploaded in these two different ways.

Can I Push Arm-based Container Images to SWR?

SWR has no restriction on the kernel architecture of images. There is no difference between pushing an Arm-based image and an x86-based image to SWR.

 Copyright © Huawei Technologies Co., Ltd.

What Protocol Is Used to Push Images to SWR When I Run the docker push Command?

HTTPS is used.

Will an Existing Image Be Overwritten If I Push an Image That Has the Same Name and Tag with It?

Yes. The existing image will be overwritten.

What Is the Maximum Size of an Image Layer?

If you use the container engine client to push images to SWR, each image layer cannot exceed 10 GB.

What Is the Rate Limit for a Tenant to Push Images over the Internet?

To avoid mutual interference between tenants when they push SWR images, the image push traffic for a single tenant is limited to 20 QPS. The traffic exceeding this value will be blocked. In this case, Docker will receive 503 and automatically retry traffic control requests.

Does SWR Support Resumable Image Push?

No.

 Copyright © Huawei Technologies Co., Ltd.

4 Image Pull

How Do I Pull an Image from SWR by Calling an API?

Currently, SWR does not provide an API for pulling images. You can use a container engine client to pull images. For Docker, run **docker pull**. For containerd, run **crictl pull**.

Where Are the Images Pulled by docker pull Stored?

Images pulled by running the **docker pull** command are stored on your local hosts. You can run the **docker save** command to save images into TAR archive files.

Can I Pull Images from Another Region?

Cross-region image pull over public network is supported.

Cross-region image pull over public network is supported. Ensure that you have obtained the correct login command.

Can I Access SWR over a Private Network? Will I Be Charged for Pushing and Pulling Images over a Private Network?

If your machine and the image repository are in the same region, you can access the image repository over private networks. No additional fees are charged for private network access because you have paid for your servers and EIPs.

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.

Can I Pull Images on the SWR Console to a Local PC?

Images stored in SWR cannot be directly downloaded through the console. You can perform the following operations to pull the images:

1. Obtain the image pull command on the image details page.
2. Run the obtained command on the device where the Docker client is installed.

   Example:

   docker pull swr.ap-southeast-1.myhuaweicloud.com/group/nginx:v1

 Copyright © Huawei Technologies Co., Ltd.

3. Save the image as a TAR or TAR.GZ file.

   Example:

   docker save nginx:v1 > nginx.tar

4. Download the file to the local host.

What Are the Possible Causes of Slow Image Pull?

1. The network is abnormal.
2. There are multiple image layers.
3. Image pull tasks are serially executed. A task cannot be executed until the previous task is complete. The timeout interval for a pull task is 30 minutes.

Will a Pulled Image Overwrite an Existing Image with the Same Name and Tag?

If they have the same manifest, the existing image will not be overwritten. Otherwise, it will be overwritten.

 Copyright © Huawei Technologies Co., Ltd.

5 Synchronizing Images

5.1 Can I Synchronize Images Across Regions?

- Cross-region image synchronization is only available in the following regions: CN North-Beijing1, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, and AF-Johannesburg.
- For other regions, you can pull an image to your local PC first and then push it to the desired region.

5.2 Why Cannot IAM Users Configure Image Synchronization?

Currently, only accounts and IAM users with administrator permissions can configure image synchronization.

5.3 Can Existing Images Be Automatically Synchronized?

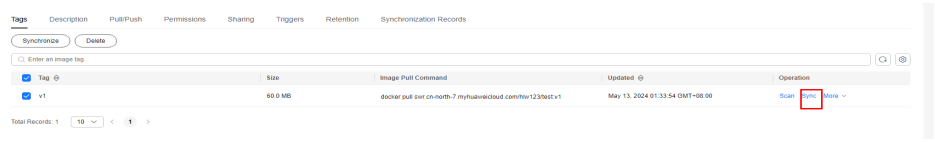
Setting image synchronization enables you to automatically synchronize newly pushed images to the target organizations in the target regions you specified. When images are updated, corresponding images in the target organization are automatically updated, accordingly.

To synchronize images pushed before you configure image synchronization, perform the following operations:

1. On the **Tags** tab of the image details page, select an image tag and click **Sync** in the **Operation** column.

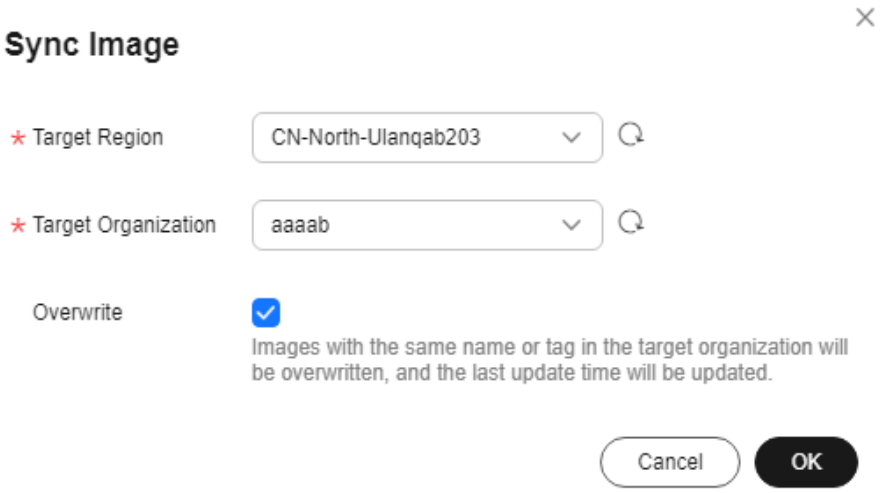
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Synchronizing existing images



2. In the dialog box displayed, select the target region, target organization, and whether to overwrite any image that has the same name and tag in the target organization. Click **OK**.

Figure 5-2 Synchronizing images



5.4 Can I Synchronize Images Shared by Other Users?

No. You cannot synchronize the images shared by other users.

For images that other users shared with you, you only have read permission on them. Specifically, you can only pull them. To synchronize them, you must have administrator permissions.

5.5 Why Can't I See Images Synchronized to the Target Region After Configuring Image Synchronization?

Symptom

After configuring automatic image synchronization, you cannot see images synchronized to the region you specified. For example, you created an automatic synchronization task to synchronize the **nginx_01** image from region A to region B. After the synchronization was successful, the **nginx_01** image was not found in region B.

Possible Cause

Automatic synchronization for an image can be executed only when the image is updated.

 Copyright © Huawei Technologies Co., Ltd.

In this example, you will find image **nginx_01** synchronized to region B after you add a new tag for **nginx_01**. If you want an image to be synchronized immediately, synchronize it manually.

 Copyright © Huawei Technologies Co., Ltd.

6 Troubleshooting

6.1 Why Does the Login Command Fail to Be Executed?

Possible causes are as follows:

1. The container engine is not properly installed, in which case the following error is reported:

   docker: command not found

   Solution: Reinstall the container engine. For details, see **Installing a Container Engine**.

   - Only Docker 18.06 or later is supported. Download the corresponding version.
   - 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.

2. The temporary login command has expired, or the regional project name, access key (AK), or login key in the command is incorrect, in which case the following error is reported:

   unauthorized: authentication required

   Solution: Log in to the SWR console. In the navigation pane, choose **My Images**. Click **Upload Through Client** in the upper right corner. In the displayed dialog box, click **Generate Login Command**.

   a. To obtain a temporary login command: On the **Temporary Login Command** tab page, click  to copy the login command.

   b. To obtain a long-term login command: On the **Long-Term Login Command** tab page, import or enter the AK and SK to generate a login command. For details, see **Obtaining a Long-Term Login Command**.

3. The image registry address in the login command is incorrect, in which case the following error is reported:

   Error logging in to v2 endpoint, trying next endpoint: Get https://{{endpoint}}/v2/: dial tcp: lookup {{endpoint}} on xxx.xxx.xxx.xxx:53 : no such host

   Solutions:

 Copyright © Huawei Technologies Co., Ltd.

a. Change the image registry address in the login command.

   The image registry address format is as follows: swr.*regional project name*.myhuaweicloud.com. For example, the image registry address for CN North-Beijing4 is **swr.cn-north-4.myhuaweicloud.com**.

b. Generate a temporary login command. For detailed instructions, see **2**.

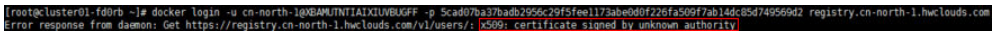
4. **x509: certificate has expired or is not yet valid**

   The preceding error is reported when the AK/SK in the login command with long-term validity is deleted. In this case, use a valid AK/SK to generate a login command.

5. **x509: certificate signed by unknown authority**

   Possible Causes:

   The container engine client communicates with SWR through HTTPS. The client verifies the server certificate. If the server certificate is not issued by an authoritative organization, the following error message is displayed: "x509: certificate signed by unknown authority"

   Solutions:

   If you trust the server and skip certificate authentication, manually configure Docker startup parameters as follows:

   – CentOS:

     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": ["{image-registry-address}"]
     }
     ```

   – Ubuntu:

     Modify the **/etc/default/docker** file and add the following content to **DOCKER_OPTS**:

     ```
     DOCKER_OPTS="--insecure-registry {image registry address}"
     ```

   – EulerOS:

     Modify the **/etc/sysconfig/docker** file and add the following content to **INSECURE_REGISTRY**:

     ```
     INSECURE_REGISTRY='--insecure-registry {image-registry-address}'
     ```

   NOTE

   The image registry address can be a domain name or an IP address.

   - Domain name: swr.*[regional-project-name]*.myhuaweicloud.com. For example, the image registry address for CN North-Beijing4 is **swr.cn-north-4.myhuaweicloud.com**.
   - To obtain the image registry address in IP address format, ping the image registry address in domain name format.

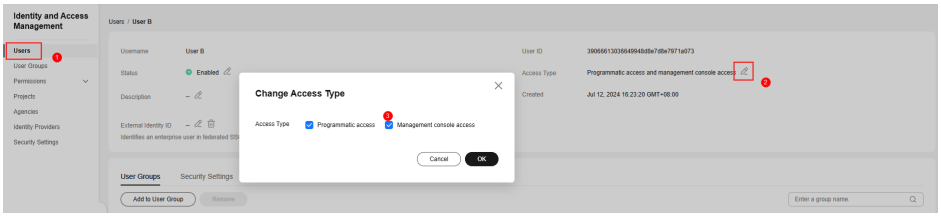
   After the configuration, run the **systemctl restart docker** command to restart the container engine.

6. **denied: Authenticate Error**

   The user does not have programmatic access. To grant programmatic access to this user, log in to **IAM** as an administrator. Click the name of this user to go to its details page. Click next to **Access Type**. Select both

 Copyright © Huawei Technologies Co., Ltd.

Programmatic access and **Management console access**. For more information about IAM, see **IAM Service Overview**.



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

denied: you do not have the permission

Symptom: When you push an image to SWR through your container engine client, the operation fails with the following information returned:

denied: you do not have the permission

Possible causes:

- The organization name you specified has already been used by another user or the maximum number of organizations that you are allowed to create has been reached.
- The **docker login** command you used to log in to SWR is generated using the AK and SK of an IAM user who does not have the permission of the target organization.

Solutions:

- If the organization name has been used by other users, create an organization with another name first, and then push the image to it. For details about how to create an organization, see **Creating an Organization**.
- If the maximum number of organizations (5 per user) you are allowed to create has been reached, you can push the image to an existing organization.
- If the IAM user does not have the permission of the target organization, you can authorize this user on either the SWR or IAM console.

  Method 1: Log in to the SWR console as an SWR administrator. In the organization list, locate the organization. On the details page of the organization, grant the IAM user the permission to manage this organization. For details, see **User Permissions**.

  Method 2: Use IAM fine-grained authorization to assign a custom policy to this IAM user. This policy contains the permission to push images.

  a. Log in to the **management console**.

  b. Select a region, click ☰ in the upper left corner, and choose **Management & Governance** > **Identity and Access Management**.

  c. In the navigation pane, choose **Permissions** > **Policies/Roles**. Click **Create Custom Policy**. Enter a policy name and set **Policy View** to **JSON**. Enter the policy content as follows (replace *namespace1* with the organization name) and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "swr:repo:upload"
         ],
         "Resource": [
            "SWR:*:*:repo:namespace1/*"
         ]
      },
   ]
}
```

d. In the navigation pane, choose **User Groups**. Click the name of the user group that the IAM user belongs to. Click **Authorize**. Select the policy created in **c** for the user group.

e. Wait for 1 minute. After the policy takes effect, push the image again.

denied: Image organization does not exist, you should create it first

Symptom: When you push an image to SWR through your container engine client, the operation fails with the following information returned:

denied: Image organization does not exist, you should create it first

Possible cause: The organization name in the **docker push** command does not exist.

Solution: Create an organization and upload the image again.

"tag does not exist: xxxxxx" or "An image does not exist locally with the tag: xxxxxx" Displayed

Symptom: When you push an image to SWR through your container engine client, the operation fails with the following information returned:

tag does not exist: xxxxxx

Or

An image does not exist locally with the tag: xxxxxx

Possible cause: The image or image tag to be pushed does not exist.

Solution: Run the **docker images** command to view all the local images. Check the target image name and tag, and push the image again.

name invalid: 'repository' is invalid

Symptom: When you push an image to SWR through your container engine client, the operation fails with the following information returned:

name invalid: 'repository' is invalid

Possible cause: The organization name or image name does not comply with the naming rules.

Solution: The regular expressions of the organization (namespace) name and image (repository) name are as follows:

 Copyright © Huawei Technologies Co., Ltd.

namespace: The value contains a maximum of 64 characters and must meet regular expression **^([a-z]+(?:(?:(?:_|__|[-]*)[a-z0-9]+)+)?)$**.

repository: The value contains a maximum of 128 characters and must meet regular expression **^([a-z0-9]+(?:(?:(?:_|__|[-]*)[a-z0-9]+)+)?)$**.

Specify a valid organization name or image name, and push the image again.

Image Push Occasionally Times Out

Symptom: Image push occasionally times out.

Possible cause: When you push an image from a server in Chinese mainland to a server outside Chinese mainland, the network may be unstable.

6.3 Why Does an Image Fail to Be Uploaded on the SWR Console?

SWR has strict requirements on image name and address format. Invalid image names or addresses could lead to upload failures.

Invalid Image Format or Authentication Failed

Symptom: When you upload an image to SWR through the SWR console, an error message is displayed, indicating that the image format is invalid.

Possible causes:

1. The upload takes longer than 15 minutes, after which the token has expired.
2. The image address format is invalid.

   The image tag, which is at the end of an image address, can be omitted. When it is omitted, the latest version of the image will be pushed. Other parts of the image address cannot be omitted. Ensure that they are all correctly configured.

   Example: *swr.regionid.*******.com/repo_namespace/repo_name:tag*

   - *swr.regionid.*******.com*: SWR image registry address.
   - *repo_namespace*: organization name. It contains 1 to 64 characters and must match the regular expression **^([a-z]+(?:(?:(?:_|__|[-]*)[a-z0-9]+)+)?)$**.
   - *repo_name:tag*: image name and tag. The image name contains 1 to 128 characters and must match the regular expression **^([a-z0-9]+(?:(?:(?:_|__|[-]*)[a-z0-9]+)+)?)$**.

   To view the image address, decompress the image. Open the **manifest.json** file, and check the value of **RepoTags**.

 Copyright © Huawei Technologies Co., Ltd.

Solutions:

1. If the token has expired, you are advised to use a **container engine client** to push the image.
2. If the image address is invalid, tag the image again based on the naming rules, run **docker save** to save the image, and upload it on the console again.

NOTICE

It is the image name in the **repositories** and **manifest.json** files that should be checked and modified rather than the name of the image file you select and upload on the SWR console.

Stuck at the Upload Page Until It Times Out

Symptom: When you upload an image to SWR through the SWR console, the upload progress is stuck and the upload task times out at the end.

Possible Causes:

- Invalid image name leads to upload failure.
- If you upload an image using the SWR console, it is uploaded over public networks. Unstable networks can lead to upload failure.

Solutions:

- Modify the image name according to the naming rules, and try uploading the image again.
- Change the network environment or use the container engine client to upload the image.

6.4 Why Does the docker pull Command Fail to Be Executed?

x509: certificate signed by unknown authority

Symptom: When you run **docker pull** to pull an image, error message "x509: certificate signed by unknown authority" is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Possible causes:

- The container engine client communicates with SWR through HTTPS. The client verifies the server certificate. If the root certificate installed on the client is incomplete, the error message "x509: certificate signed by unknown authority" is displayed.
- A proxy is configured on the container engine client.

Solutions:

- If you trust the server, skip certificate authentication. Specifically, manually configure the container engine startup parameters using either of the following two methods. Replace *Image registry address* with the actual SWR registry address.
  - Add the following configuration to the **/etc/docker/daemon.json** file. If the file does not exist, manually create it. Ensure that two-space indents are used in the configuration.
    ```
    {
      "insecure-registries":["Image registry address"]
    }
    ```
  - /etc/sysconfig/docker:
    ```
    INSECURE_REGISTRY='--insecure-registry=Image registry address'
    ```

  After configuration, run the **systemctl restart docker** or **service restart docker** command to restart the container engine.
- Run the **docker info** command to check whether the proxy is correctly configured. If not, modify the configuration.

Error: remote trust data does not exist

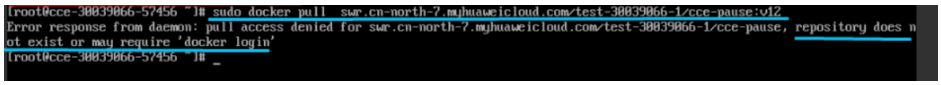
Problem: When you run the **docker pull** command to pull an image from SWR, message "Error: remote trust data does not exist" is displayed.

Possible cause: The image signature verification is enabled on the client. However, the image to be pulled does not contain a signature layer.

Solution: Check whether the environment variable **DOCKER_CONTENT_TRUST** is set to **1** in the **/etc/profile** file. If yes, change the value to **0** and run **source /etc/profile** for the setting to take effect.

pull access deny

Symptom: When you pull an image, an error occurs.



Possible cause: You do not have the **swr:repo:download** permission to pull images from the target organization.

Solutions

On either the SWR or IAM console, grant the required permission to the IAM user you are using.

Method 1: Log in to the SWR console as an SWR administrator. In the organization list, locate the organization. On the details page of the organization,

 Copyright © Huawei Technologies Co., Ltd.

grant the IAM user the permission to manage this organization. For details, see **User Permissions**.

Method 2: Use IAM fine-grained authorization to assign a custom policy to the user. This policy contains the permission to pull images.

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

Step 2 Select a region, click ☰ in the upper left corner, and choose **Management & Governance** > **Identity and Access Management**.

Step 3 In the navigation pane, choose **Permissions** > **Policies/Roles**. Click **Create Custom Policy**. Enter a policy name and set **Policy View** to **JSON**. Enter the policy content as follows (replace *namespace1* with the organization name) and click **OK**.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "swr:repo:download"
      ],
      "Resource": [
        "SWR:*:*:repo:namespace1/*"
      ]
    },
  ]
}
```

Step 4 In the navigation pane, choose **User Groups**. Click the name of the user group that the IAM user belongs to. Click **Authorize**. Select the policy created in **Step 3** for the user group.

Step 5 Wait for 1 minute. After the policy takes effect, pull the image again.

----End

6.5 What Should I Do If Images Cannot Be Downloaded from Private Networks?

This is usually caused by incorrect DNS configurations. You can solve the problem by taking either of the following approaches:

- Approach 1:

  Add a private DNS server address to the **/etc/resolv.conf** file. If you are not sure which private DNS server address to use in your region, see **What Are the Private DNS Servers Provided by the HUAWEI CLOUD DNS Service**.

  NOTE

  The newly added DNS server address must be placed before all existing DNS server addresses.

  Updates to DNS configurations take effect immediately after the **/etc/resolv.conf** file is saved.

- Approach 2:

  Restarting an Elastic Cloud Server (ECS) will invalidate updates to the **/etc/resolv.conf** file on this ECS. You will have to update the file again. To avoid

 Copyright © Huawei Technologies Co., Ltd.

the repetitive modifications, take the following steps to change the DNS server address of the VPC subnet to the private DNS server address available in your region.

NOTICE

Any changes to a VPC subnet will affect all ECSs in this subnet.

a. On the management console, click **Service List**, and choose **Network** > **Virtual Private Cloud** to launch the VPC console.
b. Change the DNS server address of the VPC subnet. For details, see **How Do I Change Default DNS Servers of an ECS to Private DNS Servers Provided by the DNS Service**.
c. Restart the ECS, and check whether the private DNS server address is contained in the **/etc/resolv.conf** file and whether this address is placed before other DNS server addresses.

6.6 Why Does Organization Creation Fail?

Symptom: The creation of an organization failed, and a message is displayed indicating that the organization already exists. However, the organization is not found in the organization list.

Possible cause: Each organization name must unique in a region. The name of the new organization may have been used by another user.

Solution: Change the name of the organization and create it again.

 Copyright © Huawei Technologies Co., Ltd.

7 Other FAQ

7.1 Why Does a CCE Workload Cannot Pull an Image from SWR and a Message "Not Logged In" Is Displayed?

If a CCE workload cannot pull an SWR image and a message "Not logged in" is displayed, check whether the YAML file of the workload contains the **imagePullSecrets** field and whether the value of **name** is fixed to **default-secret**.

Example:

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  strategy:
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - image: nginx
        imagePullPolicy: Always
        name: nginx
      imagePullSecrets:
      - name: default-secret
```

7.2 How Many Tenants Can I Share an SWR Private Image With?

500

 Copyright © Huawei Technologies Co., Ltd.

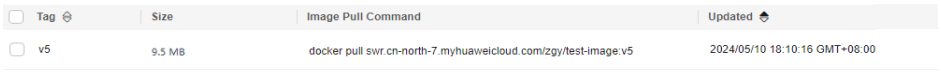
7.3 Why Is an Image Pushed Using a Container Engine Client to SWR Different in Size From One Uploaded Through the SWR Console?

Symptom

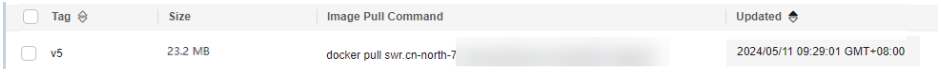
Assume that a nginx image of v5 is created on the local Docker client. The **docker images** command is run to query **SIZE** of the image. The size is 22.8 MB.

```
$ docker images
REPOSITORY                    TAG             IMAGE ID       CREATED         SIZE
nginx                         v5              22f2bf2e2b4f   9 days ago      22.8MB
```

1. Run the **docker push** command to push the image to SWR. The size of the image is 9.5 MB.



2. On the local Docker client, pack the image into a .tar package. Download the **nginx.tar** package to the local host, and upload the package to SWR. The size of the package is 23.2 MB.



The size of the image pushed through the client is different from that of the image uploaded through the SWR console.

Possible Cause

Image layers are compressed into .tgz packages when images are pushed to SWR using a container engine client, whereas when they are uploaded through the SWR console, they are only packed without being compressed. Therefore, the same image will be of different sizes when it is uploaded in these two different ways.

7.4 Can I Pull Images on the SWR Console to a Local PC?

Images stored in SWR cannot be directly downloaded through the console. You can perform the following operations to pull the images:

1. Obtain the image pull command on the image details page.
2. Run the obtained command on the device where the Docker client is installed.

   Example:

   docker pull swr.ap-southeast-1.myhuaweicloud.com/group/nginx:v1
3. Save the image as a TAR or TAR.GZ file.

   Example:

 Copyright © Huawei Technologies Co., Ltd.

docker save nginx:v1 > nginx.tar

4. Download the file to the local host.

 Copyright © Huawei Technologies Co., Ltd.