SoftWare Repository for Container(Enterprise Edition)

User Guide

Issue	01
Date	2025-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Repository Management

1.1 Purchasing a Repository

Scenarios

To use SWR Enterprise Edition, you first need to buy a repository. SWR Enterprise Edition provides enterprise-class, secure hosting services for container images and other cloud native artifacts that comply with the Open Container Initiative (OCI) specifications.

CAUTION

- By default, access to new repositories is blocked to ensure data security.
- Repositories are regional resources. If you need to use a repository in multiple regions, purchase it in each region. SWR Enterprise Edition is only available in regions CN East-Shanghai1, CN North-Ulanqab1, CN North-Beijing4, AP-Singapore, CN South-Guangzhou, CN Southwest-Guiyang1, CN East 2, CN-Hong Kong, AF-Johannesburg, TR-Istanbul, CN Northwest-Karamay, and AP-Jakarta.

Prerequisites

- You can access the Virtual Private Cloud (VPC), Object Storage Service (OBS), Key Management Service (KMS), and VPC Endpoint (VPCEP) services.
- SWR Enterprise Edition has been authorized to access VPC, OBS, and other related resources.

Procedure

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 In the upper right corner, click **Create Repository**. Configure the parameters as follows.

- **Billing Mode**: Only **pay-per-use** is available.
- **Project**: Select the region or project where the repository is. The region or project cannot be changed after repository purchase.
- **Repository Name**: Enter a repository name. The name will be used as part of the access address of the repository and cannot be changed after repository purchase.
- **Package Specifications**: Select specifications for the repository. The repository capabilities and quotas vary with different specifications.
- **VPC**: Select the VPC where the repository is. If there is no VPC available, create one by referring to **Creating a VPC**.
- **Subnet**: Select the subnet where the repository is.
- **Custom OBS Bucket**: Enabling this option allows you to select an OBS bucket from the list. You are advised to select a 3-AZ bucket for high availability.
- **OBS Bucket Encryption** (encryption at rest): Key Management Service (KMS) keys are used to automatically encrypt images uploaded to OBS buckets. This will improve data security.

  NOTE

  OBS bucket encryption may affect repository performance.
- **SM Encryption**: If you enable this option, SM algorithms will be used to secure image push, image signatures, and login passwords.
- **Tag**: Tags can be used to categorize cloud resources for easier resource management.
- **Description**: Describe the repository.

Step 3 Click **Next**.

Step 4 On the repository management page, check the creation progress. If the repository status is **Running**, the repository creation is complete.

NOTE

If the repository stays **Creating** or is not displayed in the list, click **Operation Records** in the upper left corner to view the failure cause. If the fault cannot be located, **submit a service ticket**.

----End

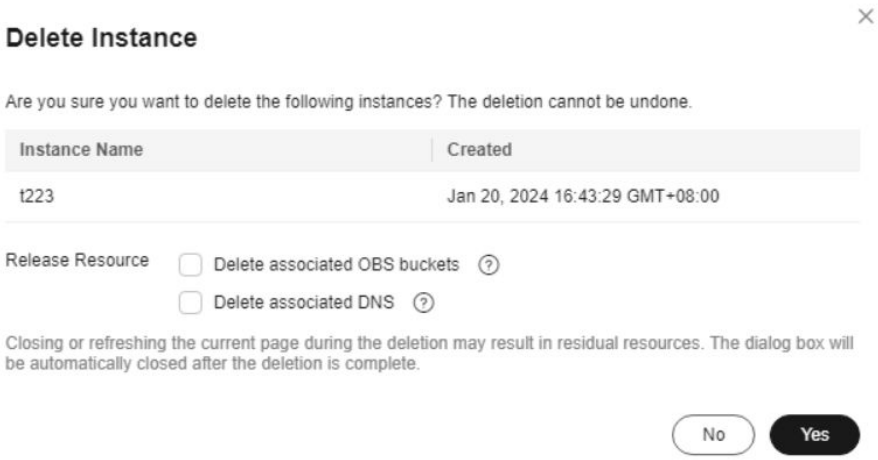
1.2 Deleting a Repository

You can delete a repository if you do not need it any longer.

Procedure

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Locate the repository and click **Delete**. You can choose whether to delete the OBS buckets and DNS resources associated with this repository.



Step 3 Click **Yes**.

----End

CAUTION

- A deleted repository cannot be restored.
- Do not close the **Delete Repository** dialog box or refresh the page during the deletion, or residual resources may be left. The dialog box will be automatically closed when the deletion is complete.

1.3 Tag Management

1.3.1 Overview

What Is a Tag

A tag is an identifier you assign to a cloud resource. When you have many cloud resources, you can use tags to categorize them in different ways (for example, by purpose, owner, or environment).

In SWR Enterprise Edition, you can use tags to identify repositories or namespaces so that you can find and manage them easier.

Application Scenarios

You can use tags to facilitate the following operations:

- **Central management of resources**

  If you have a lot of cloud resources, you can use tags to quickly identify resources of the same type to check, modify, or delete them.
- **Resource migration**

You can define a tag to identify the resources to be migrated. This improves migration efficiency and avoids errors caused by repeatedly creating tags.

- **Custom billing**

  In a billing system, to collect and analyze bills faster and more precisely, you can query resources with specific tags.

Naming Rules

Each tag consists of a key and a value. For each resource, their tag keys must be unique, and each tag key can have only one tag value. If the tag value you add is the same as an existing one for the resource, the new value overwrites the old one.

Table 1-1 Key and value

Parameter	Rule	Example
Key	• Cannot be omitted. • Cannot start with _**sys**_. • Contains 1 to 128 characters. • Consists of letters, digits, underscores (_), and hyphens (-). • Can contain UTF-8 letters, digits, spaces, and the following characters: _.:=+-@	Test Department
Value	• Can be omitted. • Cannot be empty or null for a predefined tag. • Contains 0 to 255 characters. • Consists of letters, digits, underscores (_), and hyphens (-). • Can contain UTF-8 letters, digits, spaces, and the following characters: _.:/=+-@	Shanghai

1.3.2 Adding a Repository Tag

Constraints

Table 1-2 Maximum number of tags allowed for a single repository

Item	Quota
Number of tags for a single repository	20

Adding a Tag When Purchasing a Repository

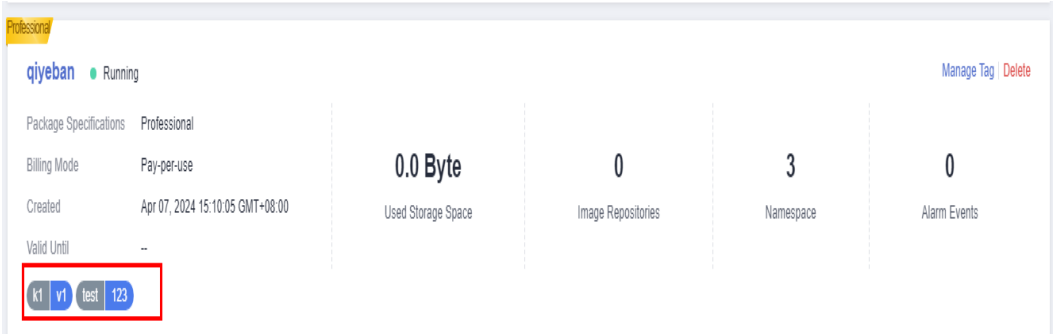
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the upper right corner, click **Create Repository**.

Step 2 On the repository purchase page, click + to add a tag. Enter a key and value as instructed in **Naming Rules**.

Step 3 Click **Next**.

Step 4 After the purchase is complete, check the new repository with tags on the repository management page.

Figure 1-1 Repository with tags



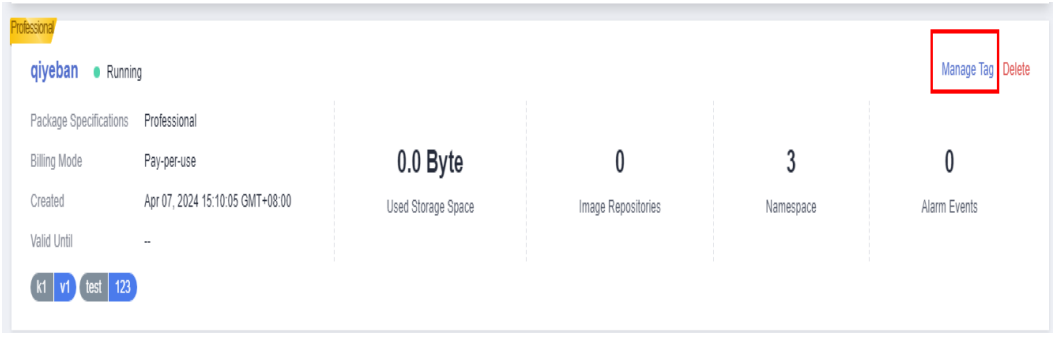
----End

Adding a Tag After Purchasing a Repository

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

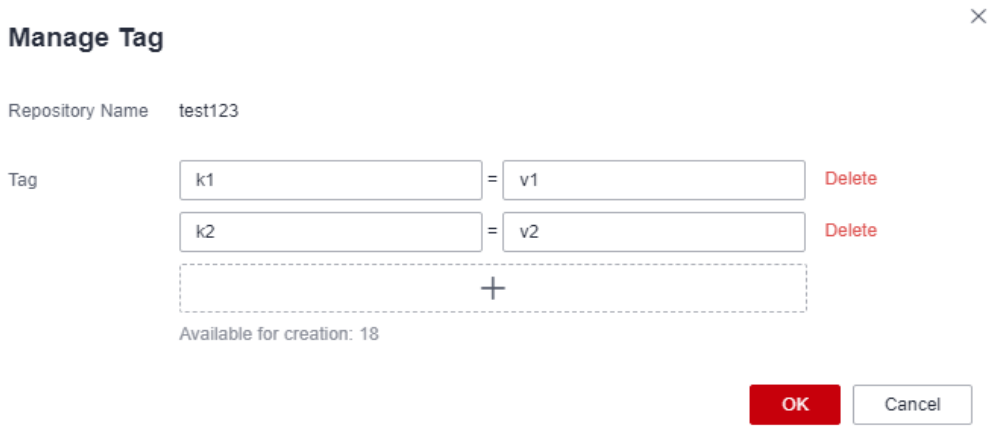
Step 2 On the repository management page, locate the repository you want to add a tag for and click **Manage Tag**.

Figure 1-2 Adding a tag for an existing repository



Step 3 In the **Manage Tag** dialog box, click + . Enter a key and a value.

Figure 1-3 Adding a tag



----End

1.3.3 Deleting a Repository Tag

You can delete tags on the SWR or TMS console.

- **Deleting a Tag on the SWR Console**
- **Deleting Tags in a Batch on the TMS Console**

Deleting a Tag on the SWR Console

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 On the repository management page, locate the repository whose tag needs to be deleted and click **Manage Tag**.

Step 3 In the **Manage Tag** dialog box, locate the tag to be deleted and click **Delete**.

----End

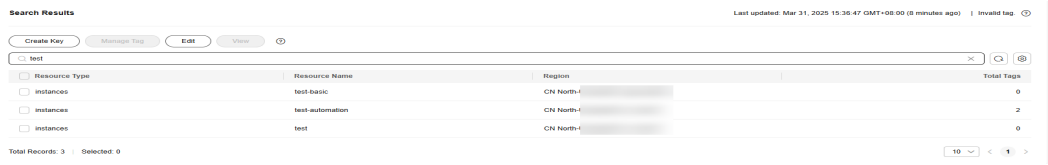
Deleting Tags in a Batch on the TMS Console

Step 1 Log in to the TMS console.

Step 2 Choose **Resource Tags** > **Tag Management**, select the target region, set **Resource Type** to **SWR**, and click **Search**. All SWR resources in this region will be returned.

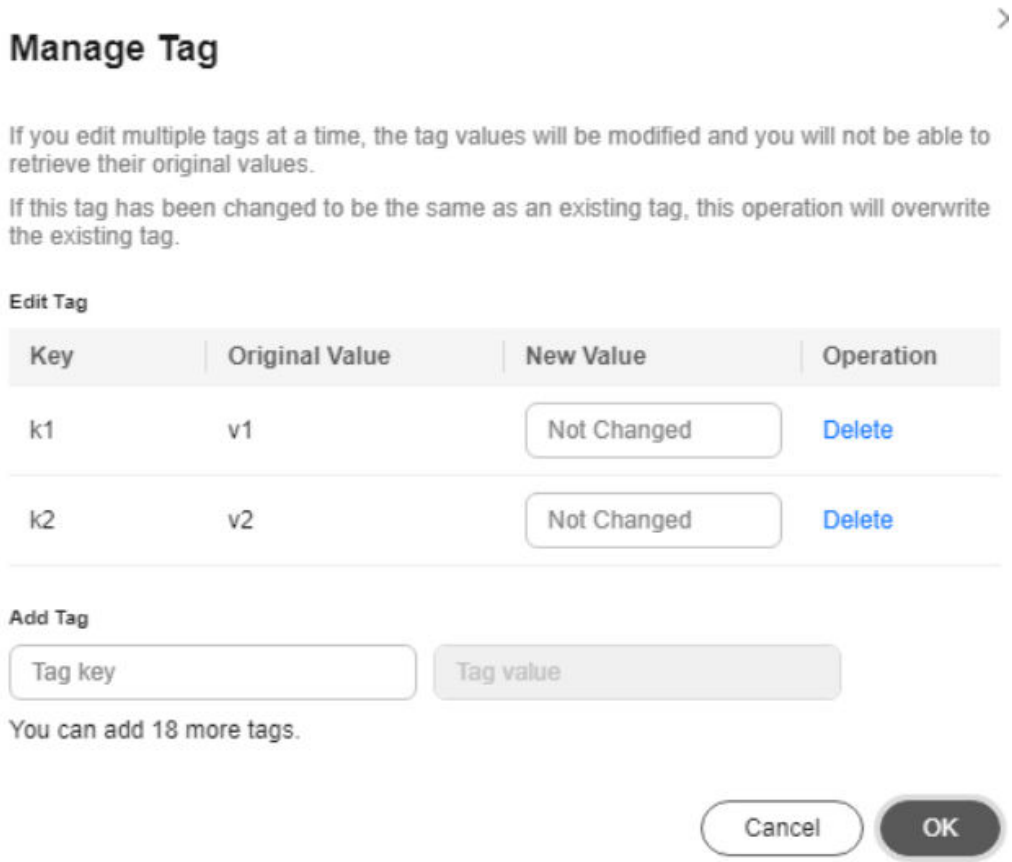
Step 3 Locate the repositories whose tags need to be deleted. Click **Manage Tag** above the list.

Figure 1-4 Tag search result



Step 4 Locate each tag to be deleted, click **Delete** in the **Operation** column, and click **OK**.

Figure 1-5 Managing tags



Step 5 (Optional) Click  in the upper right corner of the **Search Result** area.

The tag list is refreshed.

----End

1.3.4 Modifying a Repository Tag

You can modify tags on the SWR or TMS console.

Modifying a Tag on the SWR Console

Modifying Tags in a Batch on the TMS Console

Modifying a Tag on the SWR Console

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 On the repository management page, locate the repository you want to modify a tag for and click **Manage Tag**.

Step 3 In the **Manage Tag** dialog box, locate the tag to be modified and enter a new key and value.

----End

Modifying Tags in a Batch on the TMS Console

Step 1 Log in to the TMS console.

Step 2 Choose **Resource Tags** > **Tag Management**, select the target region, set **Resource Type** to **SWR**, and click **Search**. All SWR resources in this region will be returned.

Step 3 Locate the repositories whose tags need to be modified. Click **Manage Tag** above the list.

Step 4 In the **New Value** column, set new values for the tags. Click **OK**.

----End

1.3.5 Querying Repositories by Tag

You can quickly query repositories by tag on the SWR or TMS console.

Querying Repositories on the SWR Console

Querying Repositories on the TMS Console

Querying Repositories on the SWR Console

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 On the repository management page, select one or more tags from the drop-down list on the right to search for the repositories associated with any of these tags.

----End

Querying Repositories on the TMS Console

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Choose **Resource Tags** > **Tag Management**, select the target region, set **Resource Type** to **SWR**, and click **Search**. All SWR resources in this region will be returned.

----End

1.3.6 Managing Namespace Tags

Scenarios

A namespace is used to group container images into a category instead of storing them. A namespace is usually created for a project or department of an enterprise. You can add tags for namespaces to facilitate the search and management.

Prerequisites

A namespace has been created.

Constraints

Table 1-3 Maximum number of tags allowed for a single namespace

Item	Quota
Number of tags for a namespace	20

Adding a Namespace Tag

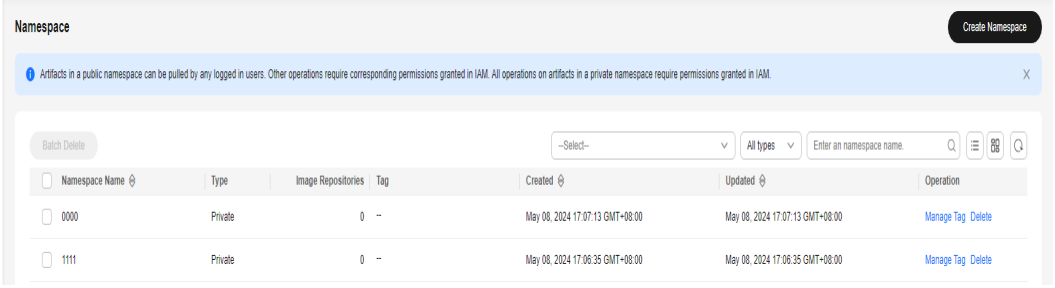
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Locate the repository you want to add a namespace tag for and click the repository name. The repository details page is displayed.

Step 3 In the navigation pane, choose **Namespaces**. Click  in the upper right corner of the page. The namespaces are listed.

Step 4 Locate the namespace you want to add a tag for and click **Manage Tag** in the **Operation** column.

Figure 1-6 Namespace management



Step 5 In the **Manage Tag** dialog box, click  to add a tag.

Figure 1-7 Tag management

Step 6 Enter a tag key and value.

----End

Modifying a Namespace Tag

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Locate the repository you want to modify a namespace tag for and click the repository name. The repository details page is displayed.

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

Step 4 Locate the namespace you want to modify a tag for and click **Manage Tag** in the **Operation** column.

Step 5 Enter one or more new keys or values.

----End

Deleting a Namespace Tag

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Locate the repository whose namespace tag needs to be deleted and click the repository name. The repository details page is displayed.

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

Step 4 Locate the namespace whose tag needs to be deleted and click **Manage Tag** in the **Operation** column.

Step 5 Click **Delete** on the right of the tag.

----End

Querying Namespaces by Tag

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Locate the repository you want to query the namespaces of and click the repository name. The repository details page is displayed.

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

Step 4 Configure one or more search filters. The search result will be displayed in the list below.

----End

2 Image Management

2.1 Image Repositories

Scenarios

An image repository manages container images. You can push and pull images to and from a repository and view the image build history.

Prerequisites

Before using an image repository, ensure that:

- You have **purchased a repository**.
- You have access to repositories. For details, see **Overview**.
- You have **created an access credential**.

Pushing an Image

Step 1 Prepare a computer that meets the following requirements:

- The container engine 1.11.2 or later is installed.
- The computer can be used within the network access range defined in **Access Control**.

Step 2 Log in to the computer as **root**.

Step 3 Use the access credential obtained in **Access Credentials** to log in to the registry and access a repository.

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

Step 4 Run the following command to tag the image:

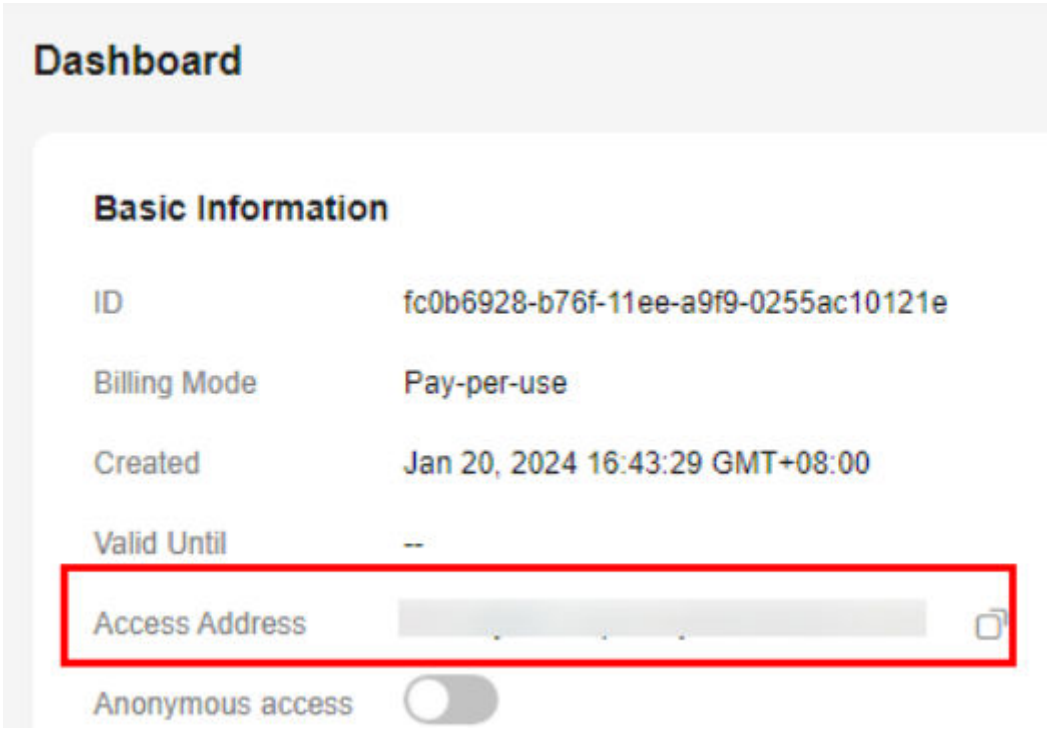
docker tag *[Image name 1:Tag 1] [Repository address]/[Namespace name]/[Image name 2:Tag 2]*

In the preceding command:

- *[Image name 1:Tag 1]*: name and tag of the image to be pushed.
- *[Repository address]*: address for accessing the repository where the image is stored. To obtain the address, perform the following operations:

  Log in to the **SWR console**. In the upper left corner, switch to your region. Click the repository name. On the **Dashboard** page, obtain the access address, as shown in **Figure 2-1**.

  Figure 2-1 Repository access address

- *[Namespace name]*: namespace you created in **Creating a Namespace**.
- *[Image name 2:Tag 2]*: new name and tag for the image.

Example:

docker tag nginx:latest test-01-2v8iom.swr.cn-east-3.myhuaweicloud.com/library/nginx:1.1.1

Step 5 Push the image to a repository.

docker push *[Repository address]/[Namespace name]/[Image name:Tag name]*

Example:

docker push test-01-2v8iom.swr.cn-east-3.myhuaweicloud.com/library/nginx:1.1.1

The following information will be returned upon a successful push:

```
fbce26647e70: Pushed
fb04ab8effa8: Pushed
8f736d52032f: Pushed
009f1d338b57: Pushed
678bbd796838: Pushed
d1279c519351: Pushed
f68ef921efae: Pushed
v1: digest: sha256:0cdfc7910db531bfa7726de4c19ec556bc9190aad9bd3de93787e8bce3385f8d size: 1780
```


To view the image information, go to the repository details page and choose **Images** from the navigation pane.

NOTE

After an image is pushed, you can use it to create a workload on the CCE console.

----End

Obtaining an Image Pull Address

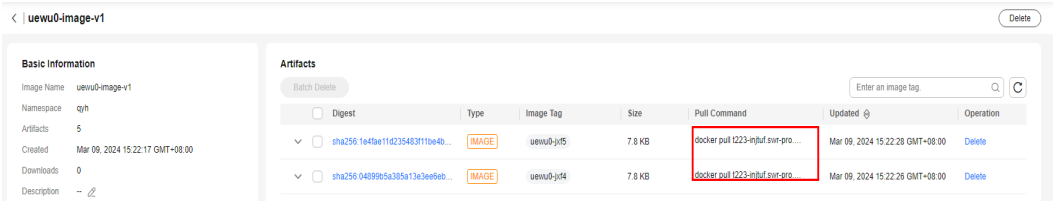
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Choose **Images** from the navigation pane.

Step 3 Click an image to go to its details page.

Step 4 Locate a desired image tag and obtain the image pull command in the **Pull Command** column.

Figure 2-2 Image pull command



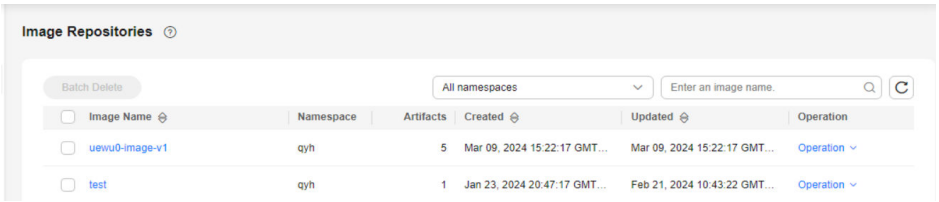
----End

Other Operations

- Searching for an image

  Search for an image by namespace or name.

  Figure 2-3 Searching for an image

- Deleting an image

  To delete an image, locate the image and click **Delete**. To avoid deleting important data by mistake, you need to enter **DELETE** to confirm the deletion.

  CAUTION

  Deleting an image will delete all its tags.

- Deleting an image tag

To delete an image tag, click the desired image name to go to its details page. Locate the target image tag, and click **Delete**. To avoid deleting important data by mistake, you need to enter **DELETE** to confirm the deletion.

Follow-up Operations

After images are pushed to a repository, you can:

- Configure an image signature policy so that images can be automatically signed. For details, see **Signing an Image**.
- Configure an image replication policy so that images can be replicated to another registry automatically. For details, see **Image Replication**.
- Configure an image retention policy to automatically delete unnecessary images. For details, see **Image Retention**.

3 Namespace Management

Scenarios

A namespace is used to group container images into a category instead of storing them. A namespace is usually created for a project or department of an enterprise.

NOTE

After a repository is created, a public namespace **library** will be automatically created for it.

Creating a Namespace

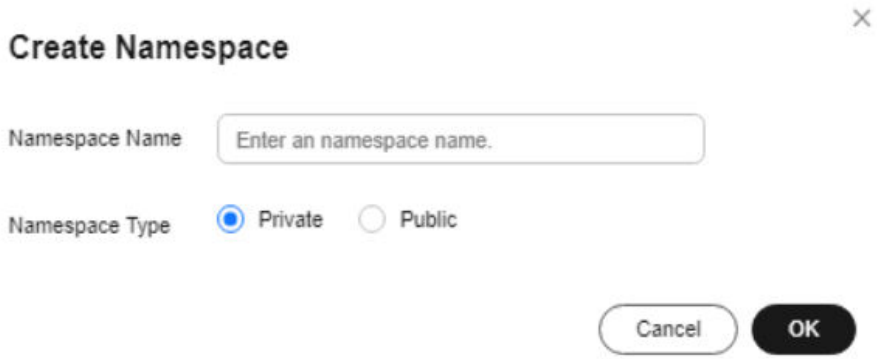
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the navigation pane, choose **Repositories**. Click your repository name.

Step 2 In the navigation pane, choose **Namespaces**.

Step 3 Click **Create Namespace** in the upper right corner.

Step 4 Enter a namespace name and select a namespace type.

Figure 3-1 Creating a namespace



- **Public**: Any user can pull artifacts from the namespace after login. If other operations on the artifacts are required, authorize users on the IAM console.
- **Private**: Only users authorized on the IAM console can perform operations on artifacts in the namespace.

Step 5 Click **OK**.

After a namespace is created, you can check its details in the list or card view.

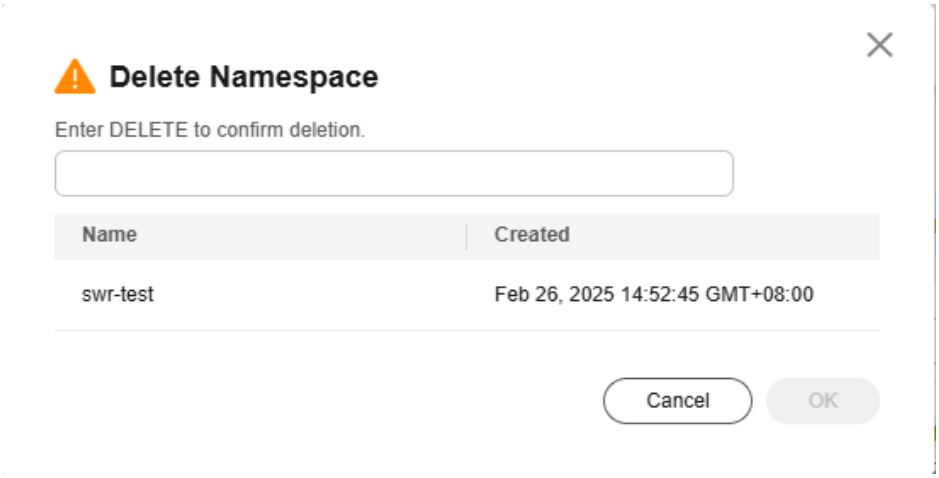
Click  or  in the upper right corner to switch the view.

----End

Deleting a Namespace

- List view: Select a namespace and click **Delete** in the **Operation** column. In the displayed dialog box, enter **DELETE** and click **OK**.
- Card view: Select a namespace and click  . In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 3-2 Deleting a namespace



NOTE

To avoid deleting important data by mistake, namespaces containing container images cannot be deleted. You need to delete the images first before deleting the namespaces.

4 Access Management

4.1 Access Credentials

Scenarios

Image repositories can only be accessed after you have obtained an access credential. Access credentials can be long-term valid or temporary.

- Long-term credentials: permanently valid after being created and can be disabled or deleted. A long-term credential can be used for preliminary tests, CI/CD pipelines, and image pull to container clusters.

  CAUTION

  Keep long-term credentials safe after they are created. If they are lost, disable or delete them in a timely manner.

- Temporary credentials: valid for 24 hours and cannot be disabled or deleted after being created. A temporary credential can be used for temporary use, one-time authorization, or other purposes. For example, it can also be used in production clusters that require high security, if it is periodically refreshed.

Creating a Long-Term Credential

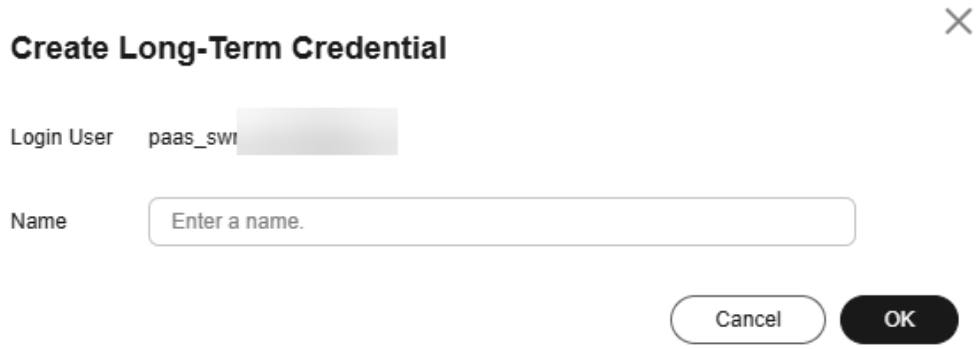
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the navigation pane, choose **Repositories**. Click your repository name.

Step 2 In the navigation pane, choose **Access** > **Access Credentials**.

Step 3 On the **Long-Term Credentials** tab page, click **Create Long-Term Credential**.

Step 4 In the displayed dialog box, enter a credential name.

Figure 4-1 Creating a long-term credential



Step 5 Click **OK**.

A long-term credential in .csv format will be automatically downloaded.

For container images, a credential is a Docker command that is used to access image repositories. For details about how to use an image repository, see **Image Repositories**.

----End

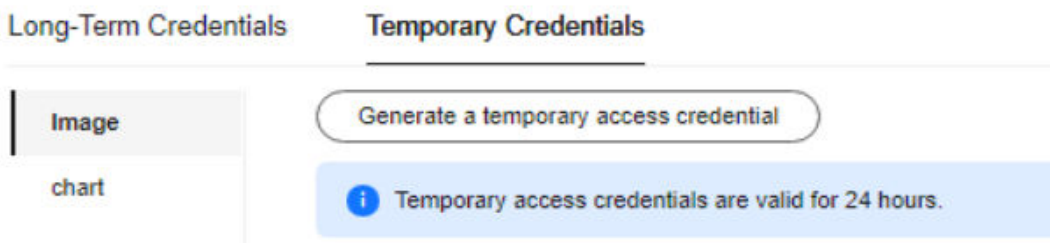
Creating a Temporary Credential

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 In the navigation pane, choose **Access** > **Access Credentials**. Click the **Temporary Credentials** tab.

Step 3 Choose **Image** or **chart** and click **Generate a temporary access credential**.

Figure 4-2 Generating a temporary access credential



The generated credential is displayed on the current page. You can copy and use it.

For container images, a credential is a Docker command that is used to access image repositories. For details about how to use an image repository, see **Image Repositories**.

----End

Follow-up Operations

- Image Repositories

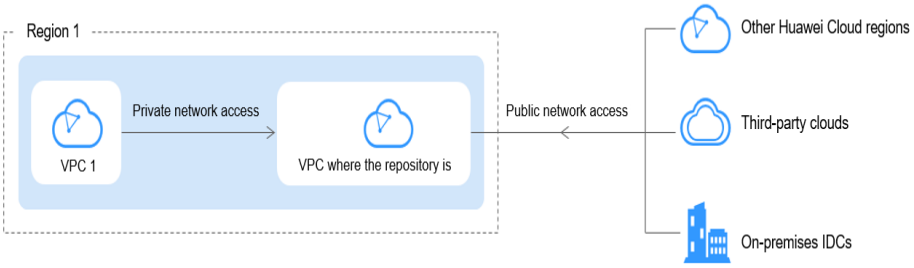
4.2 Access Control

4.2.1 Overview

By default, access to new SWR Enterprise Edition repositories is blocked for data security. You can configure control policies to allow only required access to repositories.

You can access repositories from the public network or a private network. The permissions are granted separately.

Figure 4-3 Accessing a repository



- Public network access: A whitelist is used to control which IP address CIDR blocks can access repositories.
- Private network access: You can access a repository from any VPC in the region where the repository is. For example, if a repository is in **Shanghai1**, you can access it from any VPC in Shanghai1.

  By default, you can access a repository from a VPC where the repository is. On the **Access Control** > **Private Network Access** page, you can see a default rule to allow the access.

For more information, see:

- Public Network Access
- Private Network Access

Constraints

To obtain the subnet list of a VPC, IAM users must have the **VPC ReadOnlyAccess** permission. Use your account to log in to IAM and grant this permission to IAM users.

4.2.2 Public Network Access

Scenarios

By default, new repositories cannot be accessed through the Internet. You can configure a whitelist to allow access to a repository through the Internet.

Procedure

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the navigation pane, choose **Repositories**. Click your repository name.

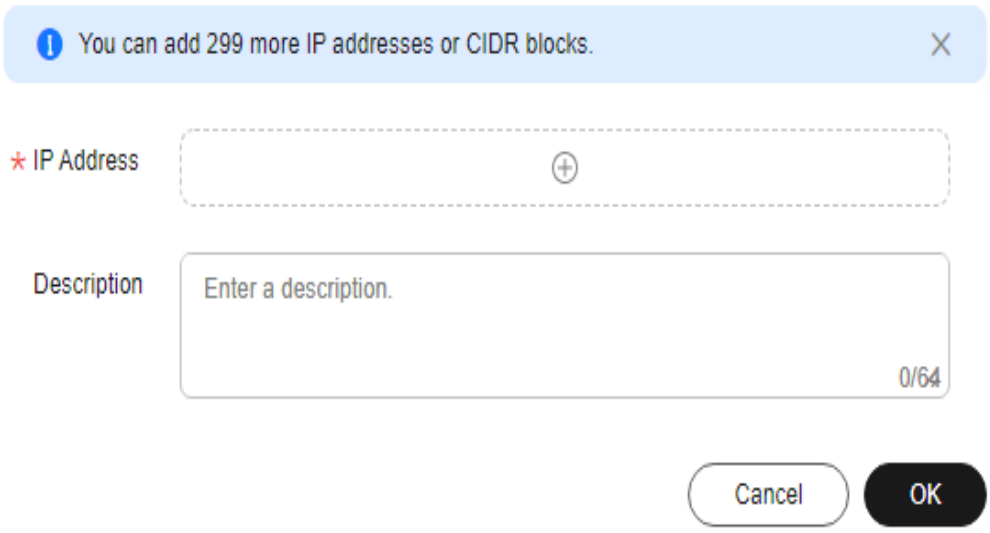
Step 2 In the navigation pane, choose **Access > Access Control**.

Step 3 Click the **Public Access** tab and click **Enable Public Network Access**. Read the message in the dialog box and click **OK**.

Figure 4-4 Enabling public network access

Step 4 Click **Create Public Network Access Rule** in the upper right corner. In the displayed dialog box, click ⊕. Enter the IP address CIDR block you want to add to the whitelist, as shown in **Figure 4-5**. If you need to add multiple CIDR blocks in a batch, click +.

Figure 4-5 Configuring a whitelist



NOTE

To reduce the risk of attacks, you are advised to add IP addresses one by one instead of adding an IP address CIDR block.

Step 5 Click **OK**.

NOTE

The whitelist cannot be modified. You can only delete it and create a new one.

----End

Follow-up Operations

To access a repository, you also need to create an access credential. For details, see **Access Credentials**.

4.2.3 Private Network Access

Scenarios

You can configure a rule to allow certain access to a repository through a private network.

This way, you can pull images to certain cloud servers over VPC.

NOTE

By default, you can access a repository from a VPC where the repository is. On the **Access Control** > **Private Network Access** page, you can see a default rule to allow the access.

Procedure

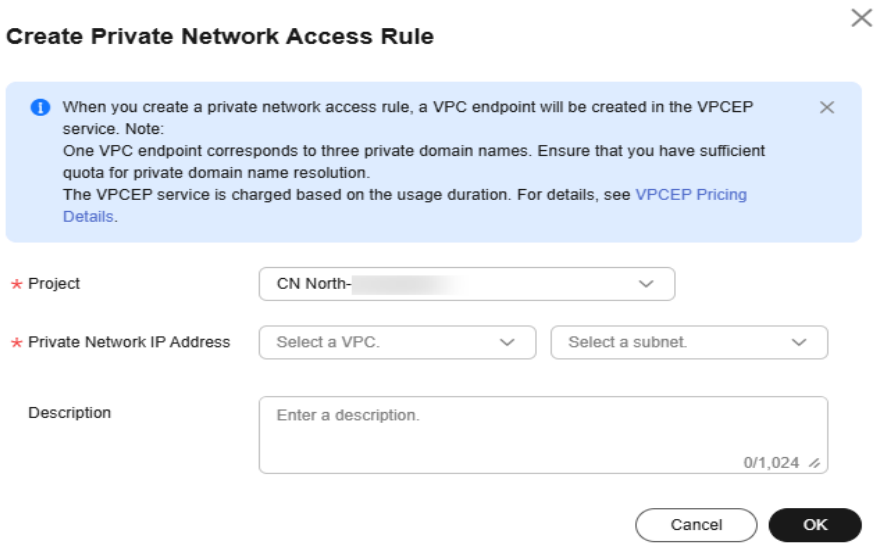
Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the navigation pane, choose **Repositories**. Click your repository name.

Step 2 In the navigation pane, choose **Access > Access Control**.

Step 3 Click the **Private Network Access** tab, and click **Create Private Network Access Rule** in the upper right corner.

Step 4 In the displayed dialog box, select a project, VPC, and subnet.

Figure 4-6 Creating a private network access rule



NOTE

If the project you select is not the default one, you need to switch to the project and authorize access to required services in this project before you can continue to create the rule.

Step 5 Click **OK**.

If the **status** changes to **Normal** and there are IP addresses displayed, the private network access rule has been created.

Figure 4-7 Private network access

Then, you can access the repository from any IP address within the CIDR block of the subnet you selected.

When you create a private network access rule, a VPC endpoint will be created in VPCEP. Do not delete that VPC endpoint.

----End

Follow-up Operations

To access a repository, you also need to create an access credential. For details, see **Access Credentials**.

4.3 Domain Names

There are two types of domain names for SWR Enterprise Edition:

- Default domain name: It is automatically created for each new repository.
- Custom domain name: It is created by a user.

You can create custom domain names when:

- You want to use the domain names planned by your company.
- Repositories are migrated from other registry services and you need to continue to use their original domain names for service continuity.

A repository can have multiple custom domain names in addition to its default domain name. To use a custom domain name, you need to provide the SSL certificate associated with it and access the repository over HTTPS. This section describes how to use a custom domain name to access a repository.

NOTE

A repository can have a maximum of five custom domain names. After a domain name is added or deleted, it takes 60s to 90s to take effect.

Prerequisites

- Domain Name Service (DNS) and Cloud Certificate Manager (CCM) cloud services have been enabled.
- You must have permission to query a certificate list (**scm:cert:list**) and permission to export certificates (varying depending on the IAM console edition).
  - New IAM console: **scm:cert:export**
  - Old IAM console: **scm:cert: download**
- A certificate has been issued for the domain name. You can purchase a certificate using the CCM service and associate the certificate with the domain name.

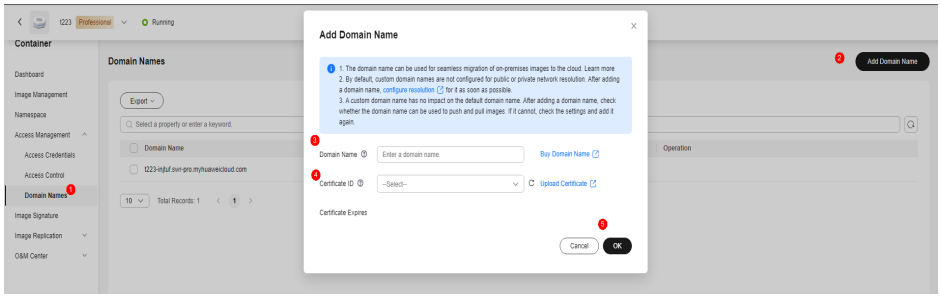
Adding a Domain Name

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. In the navigation pane, choose **Repositories**. Click your repository name.

Step 2 In the navigation pane, choose **Access** > **Domain Names**.

Step 3 Click **Add Domain Name**.

Step 4 In the displayed dialog box, enter a domain name, select the certificate issued for it, and click **OK**.



----End

Updating a Domain Name Certificate

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Click your repository name.

Step 3 In the navigation pane, choose **Access** > **Domain Names**.

Step 4 Locate a domain name, click **Edit** in the **Operation** column.

Step 5 Select the certificate to be updated and click **OK**.

----End

Deleting a Custom Domain Name

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region.

Step 2 Click your repository name.

Step 3 In the navigation pane, choose **Access** > **Domain Names**.

Step 4 Locate a domain name, click **Delete** in the **Operation** column.

Step 5 Enter **DELETE** and click **OK**.

----End

Configuring Domain Name Resolution

- **Public network access**

  You can configure **access control** and domain name resolution to access a repository through the Internet using a custom domain name. The following describes how to configure domain name resolution.

Step 1 Log in to the DNS console.

Step 2 In the navigation pane, select **Public Zones**.

Step 3 (Optional) If there is no public domain name with a custom suffix, click **Create Public Zone** in the upper right corner, enter a domain name, and click **OK**.

Step 4 Click your domain name to go to its details page.

Step 5 Click **Add Record Set**. Set parameters and click **OK**.

Table 4-1 Parameters for adding a record set

Parameter	Description
Name	Enter the prefix of the domain name to be resolved.
Type	Type of the record set. Select **CNAME**.
Line	Resolution line. It indicates whether the DNS server will return resolution results based on visitors' carrier networks or geographical locations. **Default** means that, if no lines are matched, the default resolution result will be returned.
TTL	Cache duration of the record set. A shorter TTL is useful for domains whose records change frequently. The default value is 5 minutes.
Value	Set it to the default domain name of the repository.

----End

- **Private network access**

You can configure **access control** and domain name resolution to pull images from a repository over VPC. The following describes how to configure domain name resolution.

Step 1 Log in to the DNS console.

Step 2 In the navigation pane, select **Private Zones**.

Step 3 (Optional) If there is no private zone with a custom suffix, click **Create Private Zone** in the upper right corner to create one. Enter a domain name, select a region and VPC, and click **OK**.

Step 4 Click your domain name to go to its details page.

Step 5 Click **Add Record Set**. Set parameters and click **OK**.

Table 4-2 Parameters for adding a record set

Parameter	Description
Name	Enter the prefix of the domain name to be resolved.

Parameter	Description
Type	Type of the record set. Select **CNAME**.
Line	Resolution line. It indicates whether the DNS server will return resolution results based on visitors' carrier networks or geographical locations. **Default** means that, if no lines are matched, the default resolution result will be returned.
TTL	Cache duration of the record set. A shorter TTL is useful for domains whose records change frequently. The default value is 5 minutes.
Value	Set it to the default domain name of the repository.

----End

5 Image Signatures

5.1 Signing an Image

Scenarios

You can use keys created in Data Encryption Workshop (DEW) to sign images. This will ensure image consistency during distribution and deployment and prevent man-in-the-middle (MITM) attacks or unauthorized image use and updates. An image can be automatically signed based on a policy after it is pushed. Before signing images, create an asymmetric key in Data Encryption Workshop (DEW). Then, create a signature rule, and set parameters. Images will be manually or automatically signed based on the rule.

Constraints

- Only V1.23 and later clusters are supported.
- Only key algorithms listed in **Table 5-1** can be used.
- A repository can have a maximum of 100,000 image tags and a maximum of 300 image tags can be signed per minute. After the verification plug-in is installed, the signatures of a maximum of 300 image tags can be verified per minute.

Prerequisites

You have **purchased a repository**.

You have **purchased a CCE cluster**.

Creating an Asymmetric Key

Step 1 Log in to the DEW console.

Step 2 In the navigation pane, choose **Key Management Service**. Click **Create Key** in the upper right corner.

Step 3 In the displayed dialog box, configure the parameters and click **OK**.

Asymmetric key algorithms are required by image signatures. So, select an EC, RSA, or SM2 algorithm for **Key Algorithm**. For details, see **Table 5-1**. For details about other parameters, see **Creating a Key**.

Figure 5-1 Creating a key

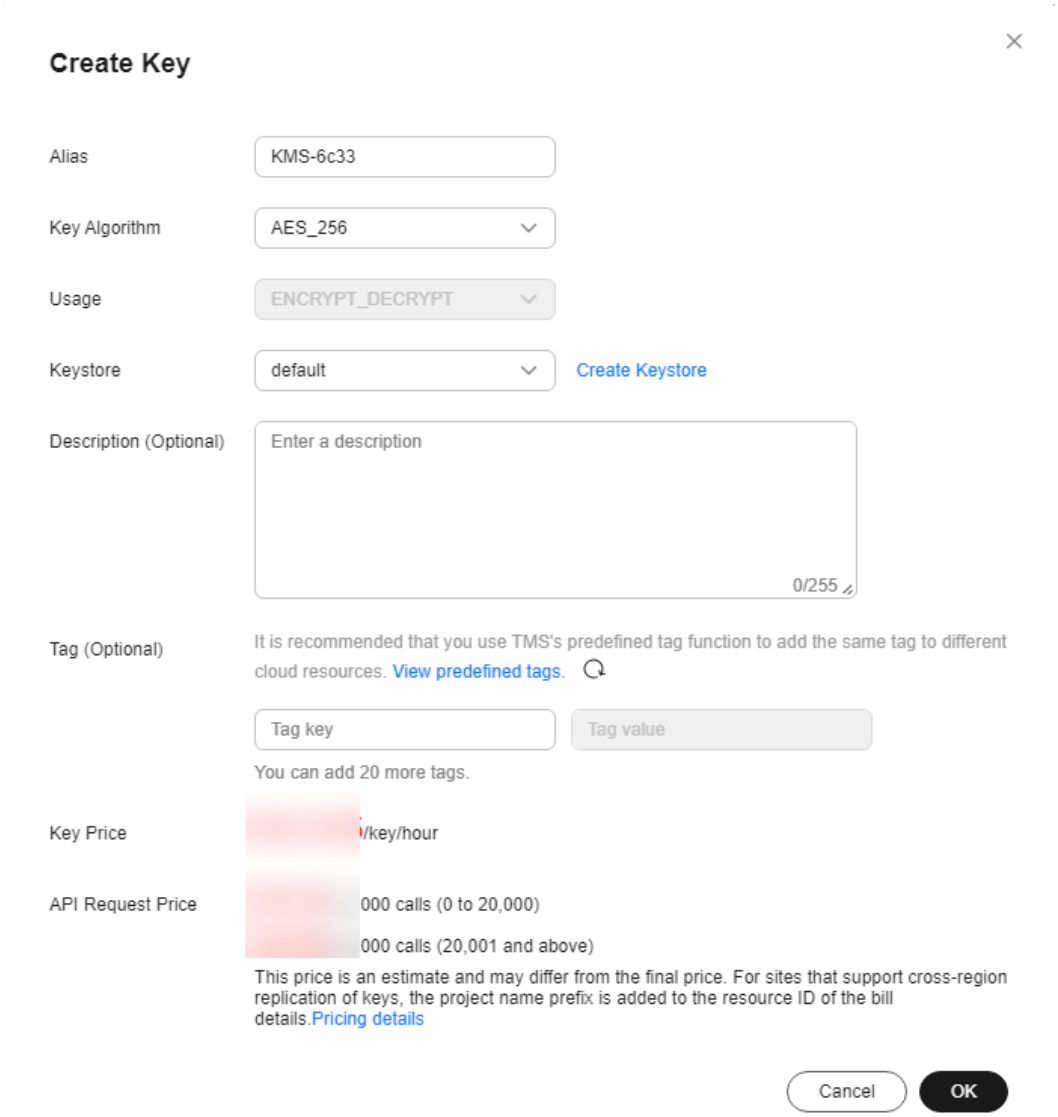


Table 5-1 Key algorithms supported by SWR

Key	Algorithm	Specifications	Description	Used For
Asymmetric	RSA	• RSA_2048 • RSA_3072 • RSA_4096 – RSASSA_PSS_SHA_256 – RSASSA_PSS_SHA_384 – RSASSA_PSS_SHA_512 – RSASSA_PKCS1_V1_5_SHA_256 – RSASSA_PKCS1_V1_5_SHA_384 – RSASSA_PKCS1_V1_5_SHA_512	RSA asymmetric key	Encrypting and decrypting a small amount of data, or creating digital signatures
Asymmetric	ECC	• EC_P256 – ECDSA_SHA_256 • EC_P384 – ECDSA_SHA_384	NIST Elliptic Curve Cryptography (ECC)	Creating digital signatures
Asymmetric	SM2	SM2	SM2 asymmetric key	Encrypting and decrypting a small amount of data, or creating digital signatures

----End

Creating a Signing Policy

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 2 In the navigation pane, choose **Image Signature**.

Step 3 Click **Create Signing Policy** in the upper right corner.

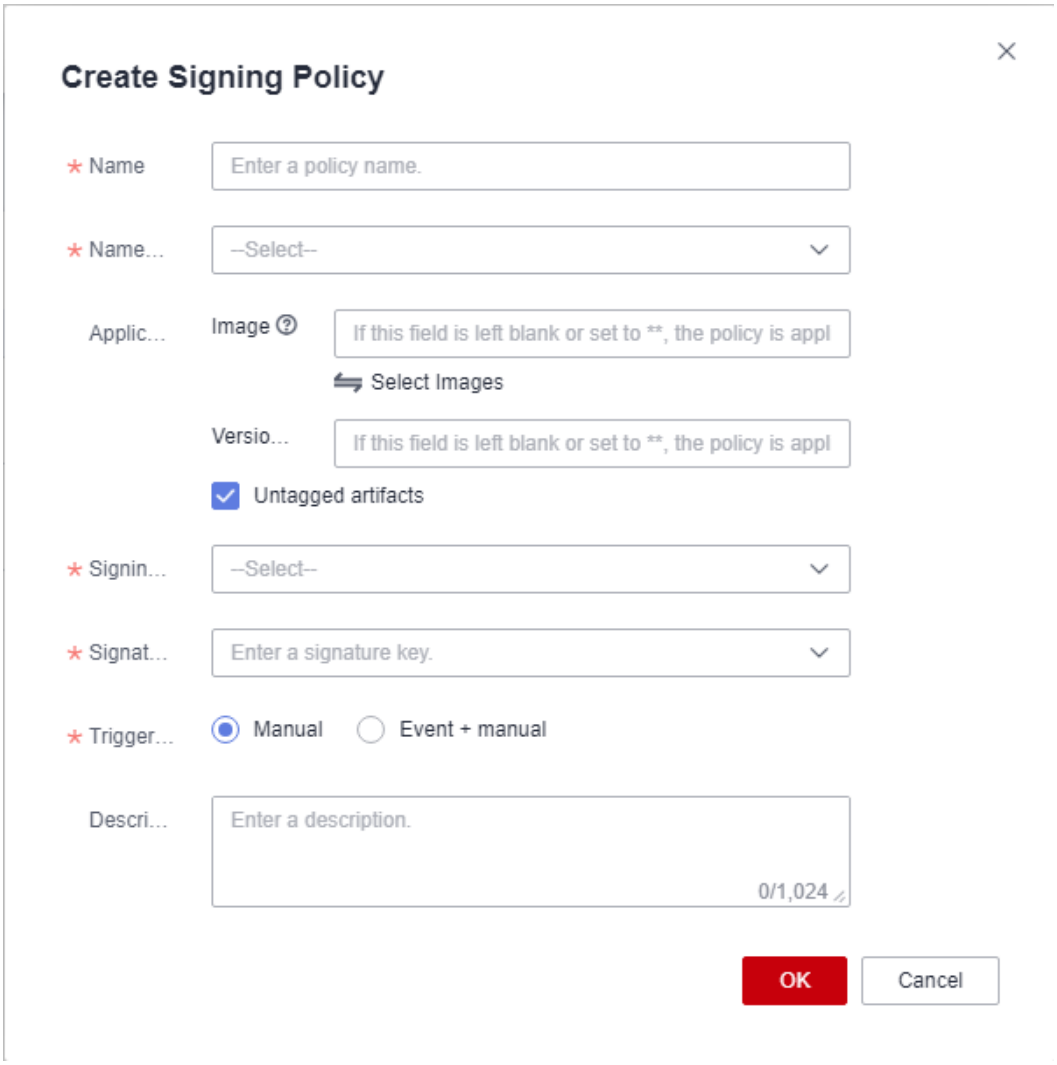
Step 4 In the displayed dialog box, configure the parameters.

Table 5-2 Parameter description

Parameter	Description	Example
Name	Policy name.	SignatureRule

Parameter	Description	Example
Namespace	Select the namespace where the image is.	library
Application Scope	**Image**: Image name. By default, a regular expression is used. Alternatively, you can click  to select images. The regular expression can be **nginx-*** or **{***repo1***, *repo2***}**. • ***: 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 any of the options. **Tag**: image tag. A regular expression is used.	**nginx-***: matches images starting with **nginx-**.
Signing Method	Select **KMS**.	KMS
Signature Key	Select the key created in **Creating an Asymmetric Key**.	key1
Trigger Mode	• **Manual**: You need to manually trigger image signing. • **Event + manual**: When a new image is pushed to a repository and the image matches the regular expression, image signing will be triggered.	Event + manual
Description	Enter a description for the policy.	-

Figure 5-2 Creating a signing policy



Step 5 Click **OK**.

----End

Verifying Image Signing

Log in to the SWR console. In the navigation pane, choose **Enterprise Edition**. Click a repository name to go to its details page. Choose **Image Signature**. Create a signing policy and execute it. After the execution is successful, go to the **Images** page. Click the signed image. The attachment in the **Artifacts** area is the signature file of the image.

5.2 Verifying an Image Signature

Scenarios

To verify image signatures, you need to install the swr-cosign add-on. This section describes how to install the add-on.

Installing swr-cosign

Step 1 Log in to the CCE console.

Step 2 In the navigation pane, choose Add-ons.

Step 3 In the search box, enter **cosign**.

Step 4 Locate the **Container Image Signature Verification** add-on in the search result and click **Install**.

Step 5 Set the following parameters:

- **Cluster**: Select the cluster where the image will be used. Only K8s V1.23 or later clusters are supported.

NOTICE

Before verifying image signatures in a namespace of a cluster, you need to add the **policy.sigstore.dev/include:true** label for the namespace.

- **Version**: Select an add-on version.
- **Specifications**:
  - **Single**: The add-on can be used only in one repository.
  - **HA**: The add-on can be used in two repositories.
  - **Custom**: You can customize the number of repositories, CPU quota, and container quota.

Table 5-3 swr-cosign specifications

Parameter	Description
Add-on Specifications	The value can be **Single**, **HA**, or **Custom**.
Pods	Number of pods that will be created to match the selected add-on specifications. If you selected **Custom** for **Specifications**, you can adjust the number of pods as needed.
Containers	If you selected **Custom** for **Specifications**, you can adjust the container specifications as needed.

- **Parameters**
  - **KMS Key**: Select a key created in **Creating an Asymmetric Key**.
  - **Signature Verification Image**: Click + and select the images whose signatures need to be verified.

Table 5-4 swr-cosign parameters

Parameter	Description
KMS Key	Select a key. Only EC_P256, EC_P384, and SM2 keys are supported. You can create a key using KMS.
Signature Verification Image	Enter a regular expression. For example, if you enter **docker.io/****, the signatures of all the images in the **docker.io** repository will be verified. To verify the signatures of all images, enter ****.

Step 6 Click **Install**.

After the installation is complete, select the cluster and click **Add-ons** in the navigation pane. On the displayed page, you can see the installed swr-cosign.

----End

Verifying an Image Signature

Log in to the CCE console and click the name of a cluster where swr-cosign has been installed. In the navigation pane, choose **Workloads** and click **Create Workload**. Select a namespace with the **policy.sigstore.dev/include:true** label and an unsigned image. Select an image access credential and continue to create the workload. The image will fail the signature verification because it has no signature.

6 Image Replication

Scenarios

You can replicate images between registries. In this way, images in one registry can be used in other registries for quick container deployment and updates globally. You can replicate artifacts between SWR Enterprise Edition and:

- SWR Shared Edition
- An SWR Enterprise Edition registry in another region or a private registry built based on open-source Harbor

You can create a policy to customize a replication. For example, you can customize the artifact type (images, Helm charts, or all), source images and tags (using a regular expression), and whether to overwrite existing artifacts.

6.1 Target Registries

Adding a Target Registry

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 2 In the navigation pane, choose **Image Replication** > **Target Registries**.

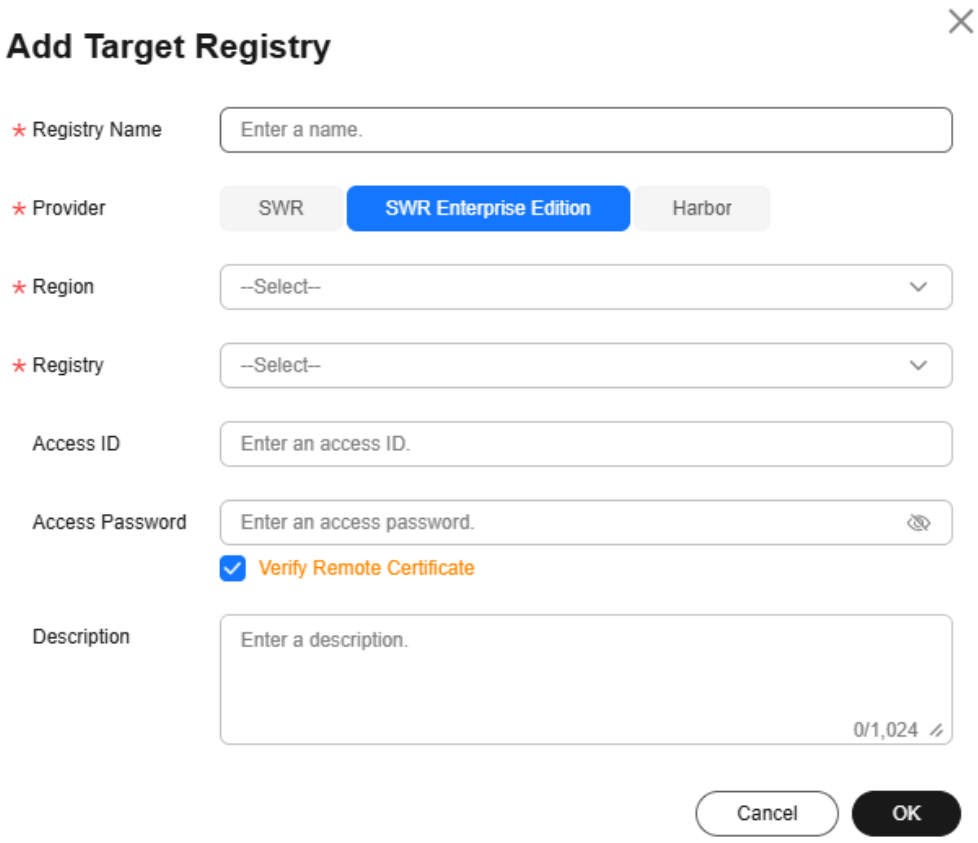
Step 3 In the upper right corner, click **Add Target Registry**.

Table 6-1 Parameter description

Parameter	Description	Example
Registry Name	Target registry name.	remote-registry

Parameter	Description	Example
Provider	Location of the target registry. The value can be: • **SWR**: SWR Shared Edition • **SWR Enterprise Edition**: **Huawei Cloud** indicates SWR Enterprise Edition in another region and **Other** indicates other registry provider. • **Harbor**: the image repository built using **Harbor**	SWR Enterprise Edition
Registry Address	Target registry address.	swr.cn-east-3.myhuaweicloud.com
Access ID Access Password	ID and password used to access the target registry. The ID and password are the user name and password in the docker login command.	-
Verify Remote Certificate	If you select this option, the system will check whether the remote certificate is released by an authorized organization. If you do not, it will not be checked.	-
Region	Region of the target registry. This parameter is available when the provider is **SWR Enterprise Edition**.	CN East-Shanghai1
Project	Project of the target registry. This parameter is available when the provider is **SWR Enterprise Edition**.	CN East-Shanghai1
Registry	Repository name. This parameter is available when the provider is **SWR Enterprise Edition**.	-
Hosts	The backend can only resolve the public domain name of the current region. If other domain names are used, such as domain names of registries or OBS buckets, you need to configure **Hosts**.	-
Description	Describe the target registry.	-

Figure 6-1 Adding a target registry



Step 4 Click **OK**.

You can check the health status in the target registry list and modify target registries.

----End

6.2 Replication Policies

Creating a Replication Policy

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 2 In the navigation pane, choose **Image Replication** > **Replication Policies**.

Step 3 Click **Add Replication Policy** in the upper right corner.

Step 4 In the displayed dialog box, configure the parameters.

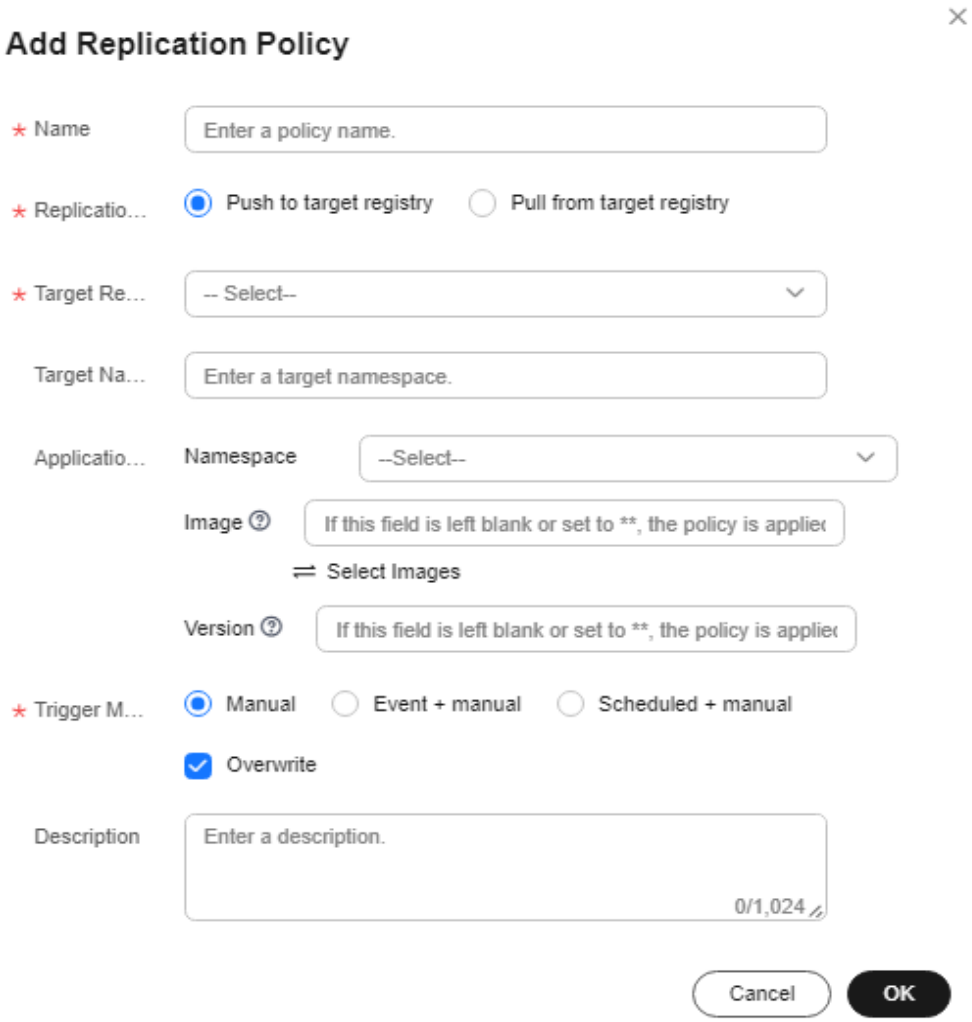
Table 6-2 Parameter description

Parameter	Description	Example
Name	Replication policy name.	SyncRule
Replication Direction	• **Push to target registry**: Push images to the target registry. • **Pull from target registry**: Pull images from the target registry.	Push to target registry
Target Registry	Select the target registry added in **Adding a Target Registry**.	-
Destination Namespace (for push to target registry)	Namespace that images will be pushed to. A namespace may be called a project on other clouds. If you omit it here, images will be pushed to the same namespace as in the source registry by default. If no such a namespace exists at the destination, replication may fail.	library1
Destination Namespace (for pull from target registry)	Namespace that images will be pulled to. A namespace may be called a project on other clouds. If you omit it here, images will be pulled to the same namespace as in the source registry by default. If no such a namespace exists at the destination, replication may fail.	library1

Parameter	Description	Example
Source Resource Filter (for push to target registry)	**Namespace**: Select a namespace. **Image**: You can use a regular expression to specify images. Alternatively, you can click  to select images. The regular expression can be **nginx-*** or *{repo1, repo2}*. ● *****: 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 any of the options. **Tag**: Image tag. You can use a regular expression to specify tags. The matching rules are the same with those for images. **NOTE** This parameter is available only when the replication direction is **Push to target registry**.	library2 nginx-* **
Source Resource Filter (for pull from target registry)	**Namespace**: You can use a regular expression to specify namespaces. **Image**: You can use a regular expression to specify images. The regular expression can be **nginx-*** or *{repo1, repo2}*. ● *****: 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 any of the options. **Tag**: Image tag. You can use a regular expression to specify tags. The matching rules are the same with those for images. **NOTE** This parameter is available only when the replication direction is **Pull from target registry**.	library2 nginx-* **

Parameter	Description	Example
Trigger Mode	• **Manual**: You need to manually trigger image replication. • **Event + manual**: Image replication is triggered when a new image is pushed or pulled and the image meets the regular expression. • **Scheduled + manual**: **Scheduled** means image replication is triggered periodically.	Scheduled + manual
Scheduled	This parameter is available only when **Trigger Mode** is set to **Scheduled + manual**.	-
Overwrite	Whether to overwrite images at the destination with the same name.	-
Description	Enter a description for the policy.	-

Figure 6-2 Creating a replication policy



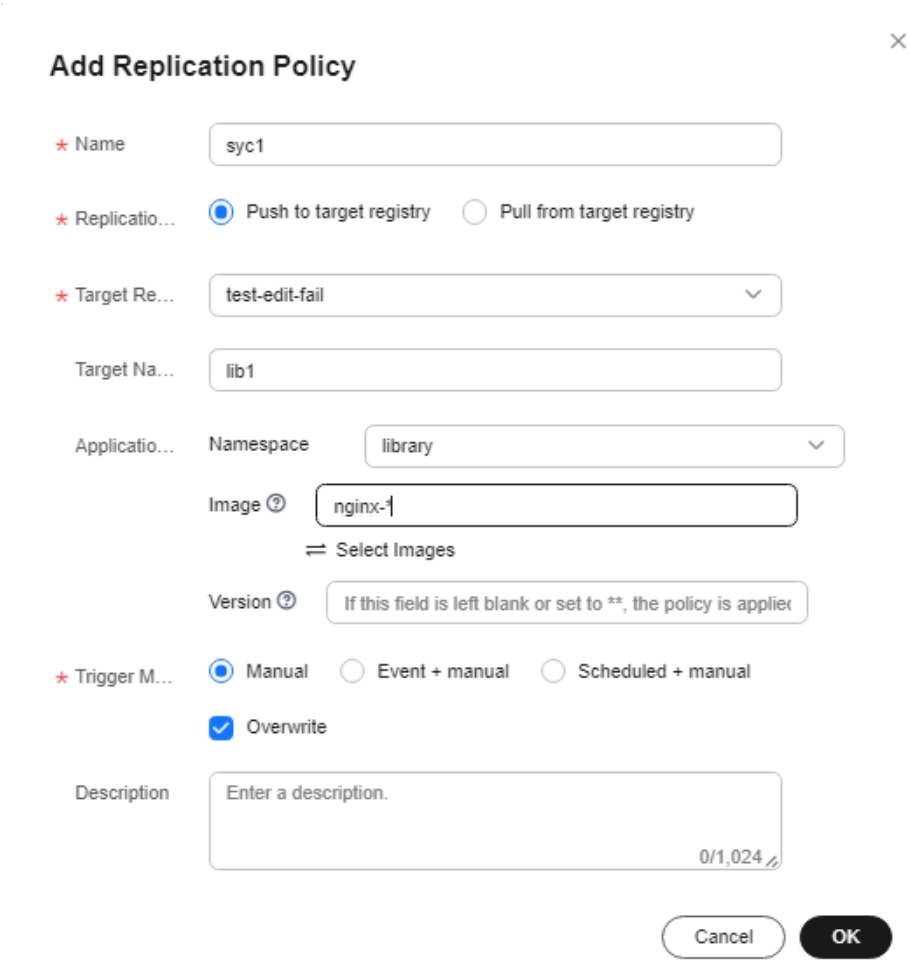
Step 5 Click **OK**.

----End

Replication Policy Examples

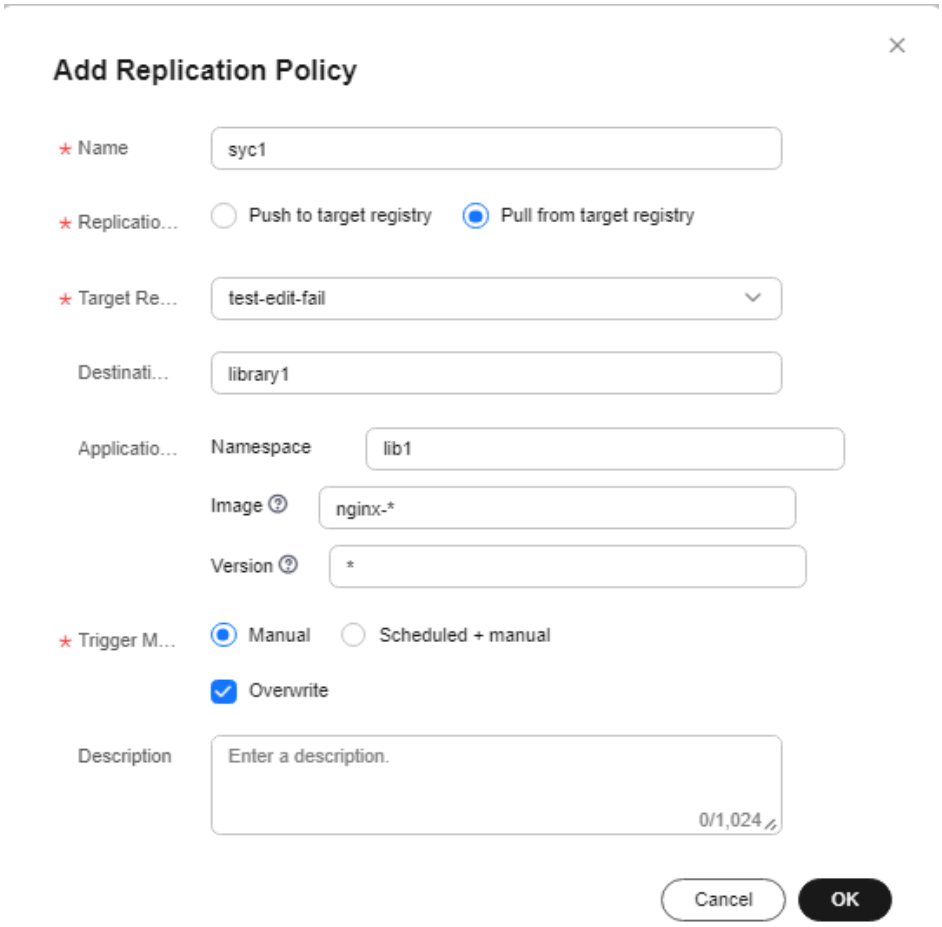
- Push to target registry

  Push all images starting with **nginx-in** from the **library** namespace of the local repository to the **lib1** namespace of the target repository **test-edit-fail**. The replication needs to be triggered manually and images with the same name will be overwritten.



- Pull from target registry

  Pull all images starting with **nginx-in** from the **lib1** namespace of the target repository **test-edit-fail** to the **library1** namespace of the local repository. The replication needs to be triggered manually and images with the same name will be overwritten.



Managing Replication Policies

You can manage your replication policies as follows.

Figure 6-3 Replication policies

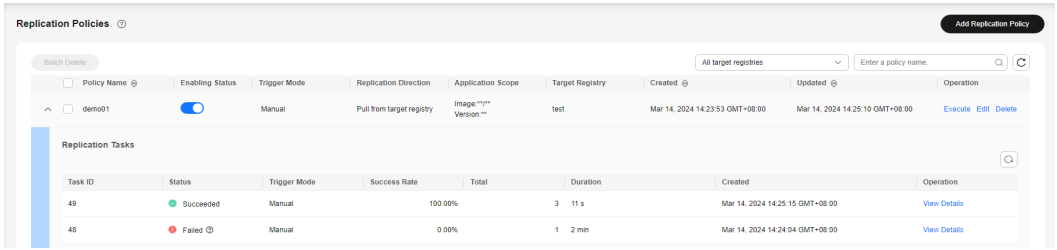
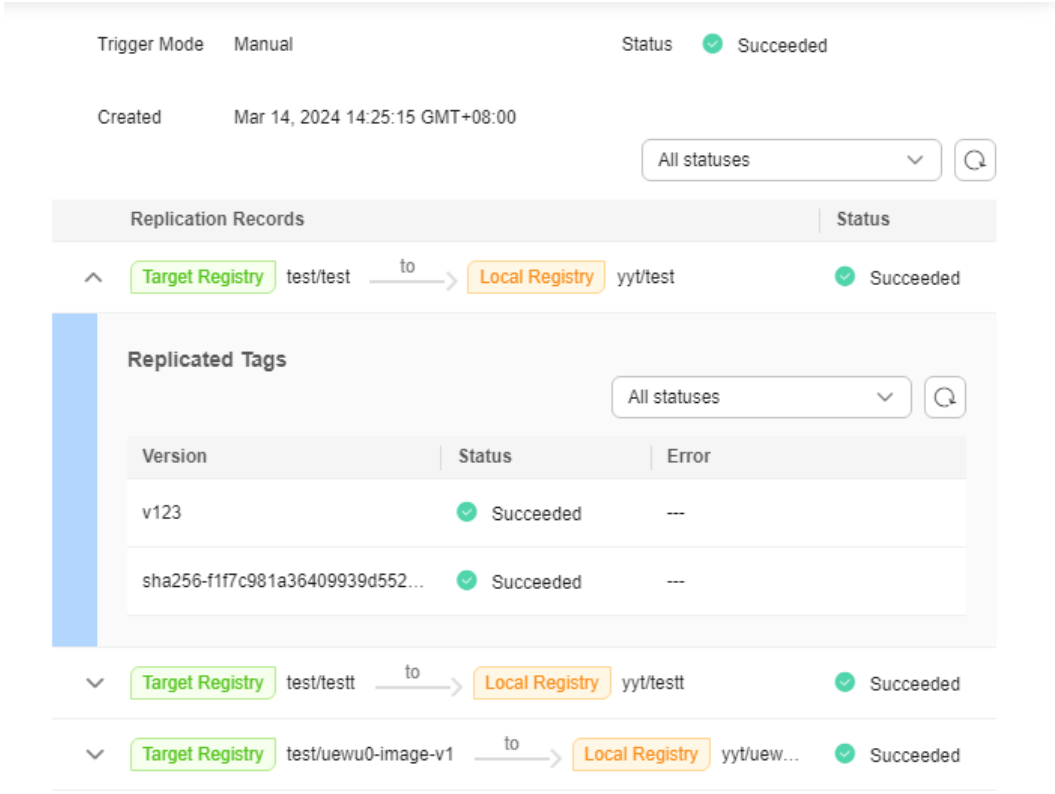


Figure 6-4 Task details



- Enable or disable a replication policy.  indicates a policy is enabled and  indicates the policy is disabled. A new policy is enabled by default.
- Manually execute a replication policy.
- Modify a replication policy.
- Delete a replication policy.
- View a replication task. When a replication policy is triggered, the images that meet the policy will be replicated. The following table describes details about a replication task.

Table 6-3 Replication task parameters

Parameter	Description
Task ID	Unique ID of a replication task for a repository.
Status	Task status.
Trigger Mode	The value is **Manual** or **Automatic**. If you click **Execute**, the trigger mode is **Manual**. If the replication is executed periodically based on a schedule, the trigger mode is **Automatic**.

Parameter	Description
Success Rate	The percentage of images that are successfully replicated to the total number of images that need to be replicated.
Total	Total number of images to be replicated in the current task.
Duration	Time required to complete a task.
Created	Time when a replication task was triggered.
Operation	**View Details**: You can check the replicated images in the right pane after clicking this button.

6.3 Replicating Images

Procedure

Step 1 Purchase a repository. For details, see **Purchasing a Repository**.

Step 2 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 3 In the navigation pane, choose **Image Replication** > **Target Registries**.

Step 4 Configure a target registry as described in **Table 6-1**.

Step 5 In the navigation pane, choose **Image Replication** > **Replication Policies** to create a replication policy. For details, see **Creating a Replication Policy**. Images will be manually or automatically replicated based on the policy.

----End

7 O&M Center

7.1 Image Retention

Scenarios

In modern software development, images are generated in pipelines and updated in each iteration. When images of earlier versions are no longer needed, you can delete them by using image retention policies, which can be, manually or periodically triggered. The rules in a policy can be used separately or in a combination.

Constraints

There can only be one retention policy in a given namespace. Each policy has 1 to 15 rules.

Creating an Image Retention Policy

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 2 In the navigation pane, choose **O&M Center** > **Image Retention**.

Step 3 Click **Add Retention Policy** in the upper right corner.

Step 4 In the displayed dialog box, configure the parameters.

Table 7-1 Parameter description

Parameter	Description	Example
Name	Retention policy name.	AgingRule
Namespace	Namespace where the retention policy will be applied.	library1

Parameter	Description	Example
Trigger Mode	• **Manual**: Image retention is manually triggered. • **Scheduled + manual**: **Scheduled** means image retention is triggered periodically.	Scheduled + manual
Scheduled	This parameter is available only when **Trigger Mode** is set to **Scheduled + manual**.	-
Image	You can: • Enter a regular expression. Example: **nginx-*** or *{repo1, repo2}*. – *: matches any field that does not contain the path separator /. – **: matches any field that contains the path separator /. – ?: matches any single character except /. – *{ repo1, repo2, ...}*: matches any of the options. Note: If this parameter is left blank or set to **, all images will be matched. • Select images from a list.	nginx-*
Tag	Image tag. Enter a regular expression. Example: **v1*** or *{v1, v2}*. • *: matches any field that does not contain the path separator /. • **: matches any field that contains the path separator /. • ?: matches any single character except /. • *{v1, v2}*: matches any of the options.	v1

Parameter	Description	Example
Condition	Retention condition. The options are as follows: • Retain the # image tags pushed most recently • Retain the # image tags pulled most recently • Retain image tags pushed within the last # days • Retain image tags pulled within the last # days *#* indicates the number of tags or days.	Retain the 10 image tags pushed most recently
Enable	Whether to enable or disable a retention rule.	-
Operation	You can delete a retention rule.	-

Figure 7-1 Creating an image retention policy

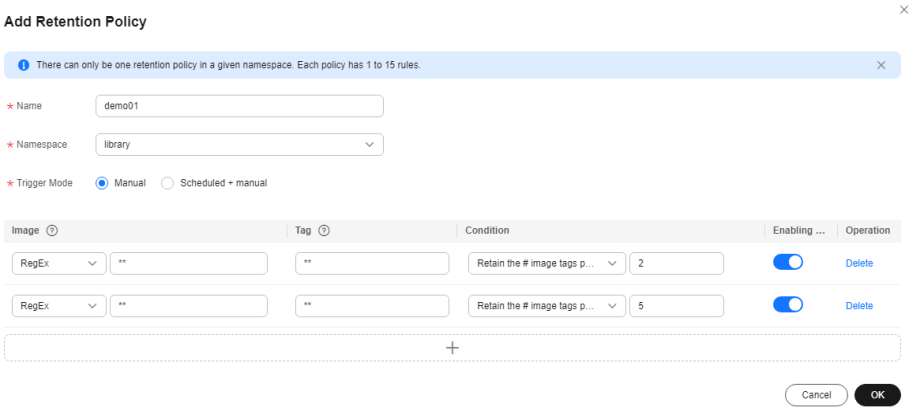
Step 5 Click **OK**.

----End

Retention Policy Examples

- Example 1:

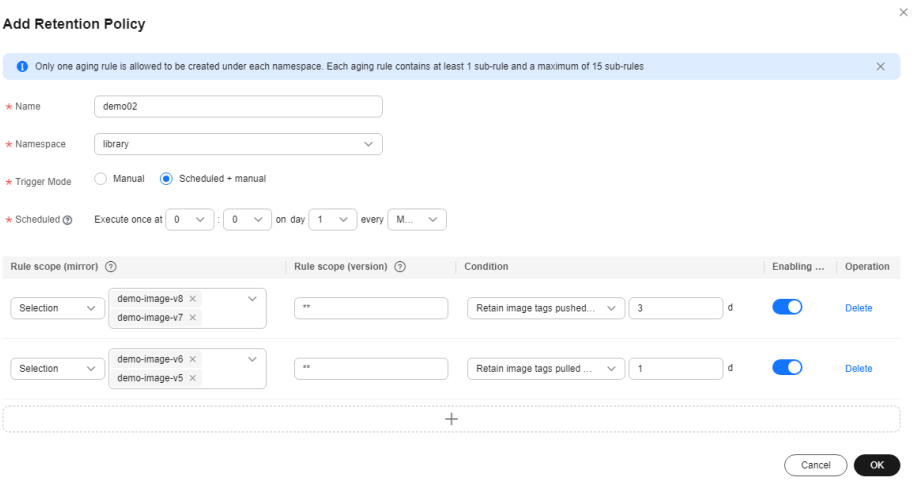
  In the **library** namespace, for all images, retain the 2 most recently pushed and the 5 most recently pulled tags. The policy needs to be manually triggered.



For example, there are 10 image tags. Image tags 9 and 10 are most recently pushed. Image tags 1 to 5 are most recently pulled. Based on the policy, image tags 6 to 8 will be deleted.

- Example 2:

  In the **library** namespace, retain the tags pushed in the last 3 days for the **demo-image-v8** and **demo-image-v7** images and the tags pulled in the last day for the **demo-image-v6** and **demo-image-v5** images. The policy is executed at 00:00 of the first day every month but can also be triggered manually.

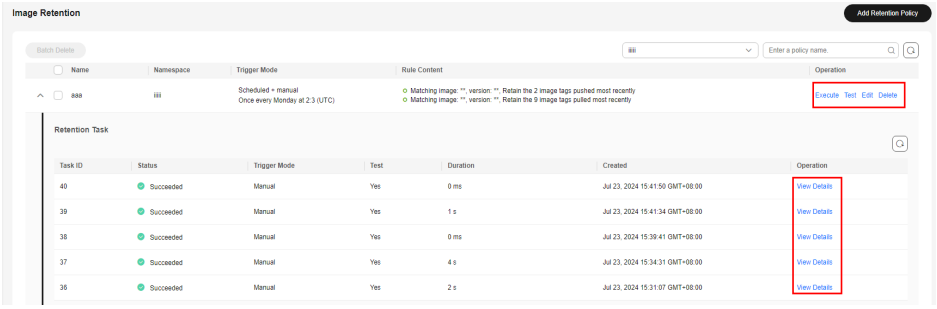


Managing Retention Policies

You can:

- Execute a retention policy. To prevent misoperations, you are advised to test a retention policy before executing it for the first time.
- Test a retention policy. You can use it to check whether a policy is in effect but no image tags will be deleted in the test.
- Modify a retention policy. All parameters except **Namespace** can be modified.
- Delete a retention policy.

Figure 7-2 Managing retention policies

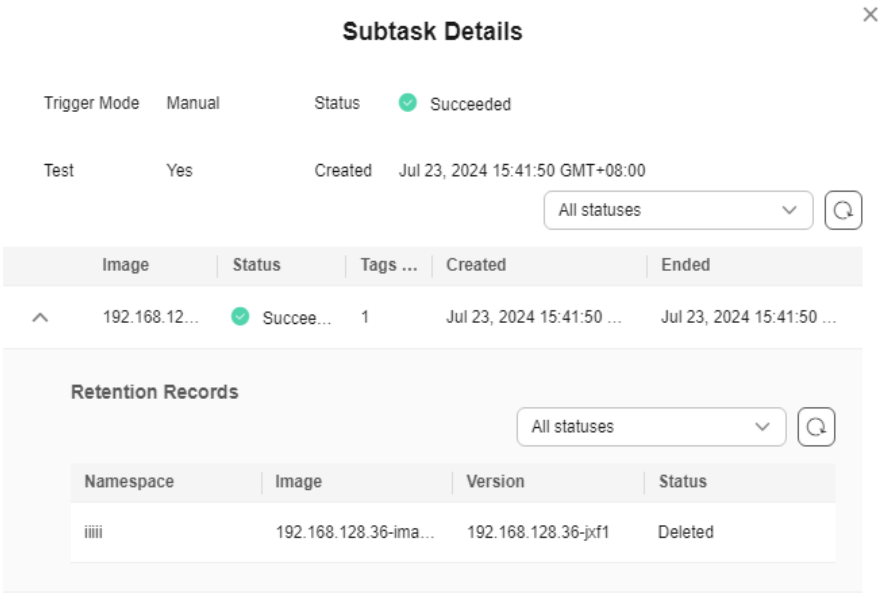


- View a retention task. When a retention policy is triggered, only the images that meet the policy will be retained. The following table describes details about a retention task.

  Table 7-2 Retention task parameters

Parameter	Description
Trigger Mode	The value is **Manual** or **Automatic**. If you click **Execute** or **Test**, the trigger mode is **Manual**. If the replication is executed periodically based on a schedule, the trigger mode is **Automatic**.
Status	Task status.
Test	The value can be **Yes** or **No**. If you click **Test**, the value is **Yes**. If you click **Execute**, the value is **No**. You can use **Test** to check whether a policy is in effect but no image tags will be deleted in the test.
Tags Deleted	Number of image tags that are deleted based on the policy.
Created	Time when a retention task was triggered.
Ended	Time when a retention task was ended.
Retention Records	Retention records of each image tag, such as the namespace, tag name, and retention results.

Figure 7-3 Task details



7.2 Triggers

Scenarios

You can create a trigger to automatically execute the defined HTTP POST requests. For example, when an image is pushed, the CI/CD pipeline will automatically pull and deploy the image to a cluster. In this way, you can quickly connect to the CI/CD pipeline for container DevOps.

Image push can trigger a request.

Creating a Trigger

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click a repository name to go to its details page.

Step 2 In the navigation pane, choose **O&M Center** > **Triggers**.

Step 3 Click **Add Trigger** in the upper right corner.

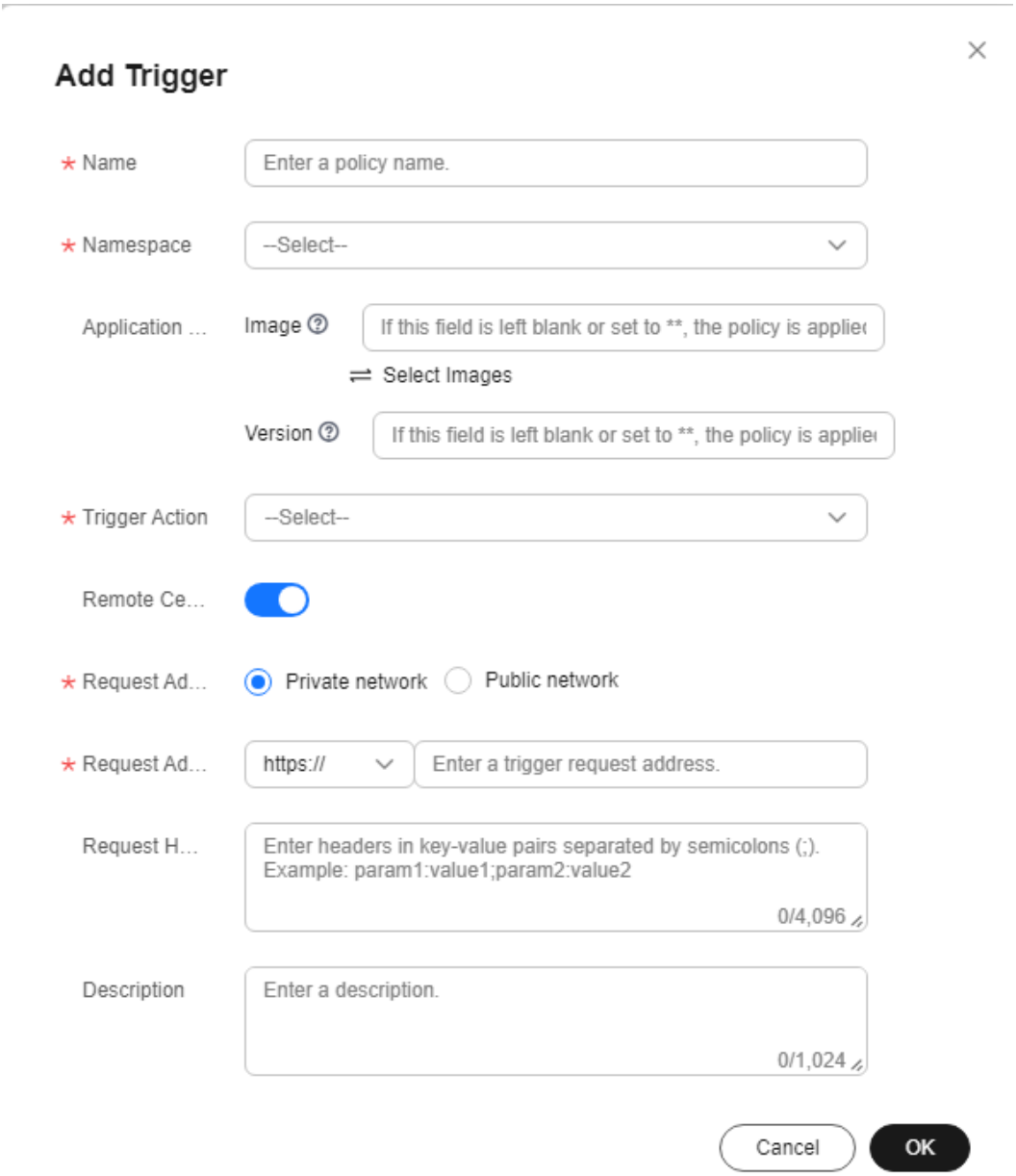
Step 4 In the displayed dialog box, configure the parameters.

Table 7-3 Parameter description

Parameter	Description	Example
Name	Trigger name.	TriggerRule
Namespace	Namespace where a trigger will be created.	library1

Parameter	Description	Example
Application Scope	**Image**: You can use a regular expression to specify images. Alternatively, you can click Select Images to select images. The regular expression can be **nginx-*** or *{repo1, repo2}*. ● *****: 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 any of the options. **Tag**: Image tag. You can use a regular expression to specify tags. The matching rules are the same with those for images.	nginx-*
Trigger Action	You can set the following action as a trigger: ● Pushing an image	Pushing an image
Remote Certificate Verification	If you select this option, the system will check whether the remote certificate is released by an authorized organization. If you do not, it will not be checked.	-
Request Address Type	● Private network ● Public network	Private network
Request Address	IP address the trigger will send a POST request to. **CAUTION** The IP address must fall into the default VPC network CIDR block you specified when you purchased the repository.	-
Request Header	When a trigger sends a POST request, the header information can be in **Key:Value** format. Example: **Authentication:** *xxxxxxx*. Use semicolons (;) to separate multiple headers, for example, *param1*:*value1*;*param2*:*value2*.	-

Figure 7-4 Creating a trigger



Step 5 Click **OK**.

----End

Managing Triggers

You can manage your triggers as follows.

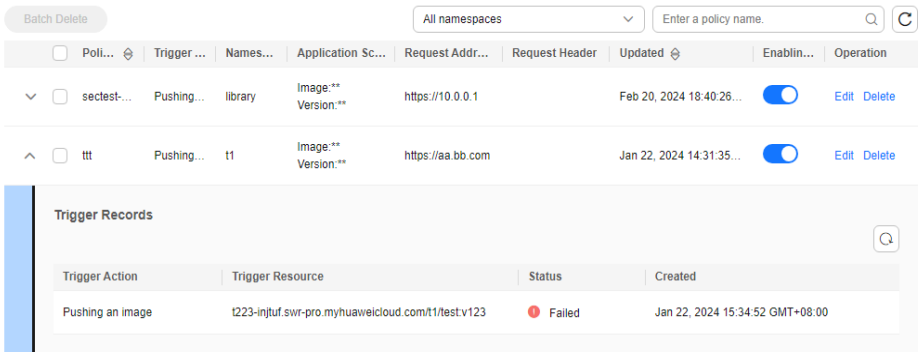
- Enable or disable a trigger. indicates a trigger is enabled and indicates the trigger is disabled. A new trigger is enabled by default.
- Modify a trigger. All parameters except **Namespace** and **Request Address** can be modified.

- Delete a trigger.
- View a trigger. When the action specified in a trigger is executed, the trigger will send a request. You can click ⌄ to view trigger records.

Table 7-4 Trigger records

Parameter	Description
Trigger Action	Action that triggers a request.
Trigger Resource	Repository resource on which the action was performed.
Status	Status of the Webhook request sent by a trigger.
Created	Time when the Webhook request was sent.

Figure 7-5 Managing triggers



7.3 Image Tag Immutability

Scenarios

To ensure end-to-end trust and prevent existing images from being overwritten if a set of access credentials gets leaked, you can configure an immutability policy for images in a namespace. If you attempt to push an image with a tag that is already in the namespace, an error will be returned.

Constraints

Only one immutability policy can be created for each namespace.

Creating an Image Tag Immutability Policy

Step 1 Log in to the **SWR console**. In the upper left corner, switch to your region. Click your repository name.

Step 2 In the navigation pane, choose **O&M Center** > **Image Tag Immutability**.

Step 3 Click **Create Immutability Policy** in the upper right corner.

Step 4 In the displayed dialog box, configure the parameters.

Table 7-5 Image tag immutability policies

Parameter		Description
Namespace		Namespace where an immutability policy will be created. It can be a public or private namespace.
Application Scope	Image	Select one or more images in the namespace.
	Tag	Specify the image tags that the policy will be applied to. If this parameter is omitted or set to ******, the policy will be applied to all image tags.

NOTE

- For **Image**, you can select one or more images from the list.
- Alternatively, you can enter a regular expression.
  The regular expression can be **nginx-*** or *{repo1, repo2}*.
  - *****: 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 any of the options.

Step 5 Click **OK**.

----End

Managing Image Tag Immutability Policies

You can manage your immutability policies as follows.

- Enable or disable an immutability policy.  indicates a policy is enabled and  indicates the policy is disabled. A new policy is enabled by default.
- Modify an immutability policy. All parameters except **Namespace** can be modified.
- Delete an immutability policy.

8 Auditing

8.1 SWR Operations Supported by CTS

Scenarios

Cloud Trace Service (CTS) is a log audit service provided by Huawei Cloud and intended for cloud security. It allows you to collect, store, and query cloud resource operation records and use these records to analyze security, audit compliance, track resources, and locate faults.

With CTS, you can record operations related to SWR for future query, audit, and backtrack.

Key Operations Recorded by CTS

Table 8-1 SWR Enterprise Edition operations recorded by CTS

Operation	Resource Type	Trace Name
Creating an instance	instance	createInstance
Deleting an instance	instance	deleteInstance
Creating a namespace	namespace	createNamespace
Deleting a namespace	namespace	deleteNamespace
Modifying a namespace	namespace	updateNamespace
Deleting a repository	repository	deleteRepository
Updating a repository	repository	updateRepository
Creating a retention policy	retention	createRetention
Modifying a retention policy	retention	updateRetention

Operation	Resource Type	Trace Name
Deleting a retention policy	retention	deleteRetention
Executing a retention policy	retention	executeRetention
Deleting a trigger	triggerPolicy	deleteTriggerPolicy
Creating a trigger policy	triggerPolicy	createTriggerPolicy
Modifying a trigger	triggerPolicy	updateTriggerPolicy
Creating a replication registry	registry	createRegistry
Deleting a replication registry	registry	deleteRegistry
Modifying a replication registry	registry	updateRegistry
Creating a replication policy	replication	createReplicationPolicy
Deleting a replication policy	replication	deleteReplicationPolicy
Modifying a replication policy	replication	updateReplicationPolicy
Executing a replication policy	replication	executeReplicationPolicy
Stopping a replication policy	replication	stopReplicationExecution
Creating a scan policy	scan	createScanPolicy
Deleting a scan policy	scan	deleteScanPolicy
Modifying a scan policy	scan	updateScanPolicy
Executing a scan policy	scan	executeScanPolicy
Creating a blocking policy	block	createBlockPolicy
Deleting a blocking policy	block	deleteBlockPolicy
Modifying a blocking policy	block	updateBlockPolicy
Enabling public network access	endpointPolicy	enableEndpointPolicy

Operation	Resource Type	Trace Name
Disabling public network access	endpointPolicy	disableEndpointPolicy
Updating the whitelist for public network access	endpointPolicy	updateEndpointPolicy
Obtaining a temporary access credential	TempCredentialAuth	createTempCredentia-lAuthPolicy
Creating a long-term access credential	LongTermCredentialAuth	createLongTermCreden-tialAuthPolicy
Deleting a long-term access credential	LongTermCredentialAuth	deleteLongTermCreden-tialAuthPolicy
Enabling or disabling a long-term access credential	LongTermCredentialAuth	updateLongTermCreden-tialAuthPolicy
Creating a private network access	IntranetEndpoint	createInternalEndpoint
Deleting a private network access	IntranetEndpoint	deleteInternalEndpoint
Creating a signature policy	signaturePolicy	createSignaturePolicy
Deleting a signature policy	signaturePolicy	deleteSignaturePolicy
Modifying a signature policy	signaturePolicy	updateSignaturePolicy
Executing a signature policy	signaturePolicy	executeSignaturePolicy
Uploading a chart	Chart	uploadChart
Deleting a chart	Chart	deleteChart
Deleting a chart version	Chart	deleteChartVersion
Creating an agency	agency	createAgency
Updating quotas	quota	updateQuota
Updating internal quotas for Harbor	quota	CACUpdateQuota
Adding a namespace tag	resourceTag	createResourceTags
Deleting a namespace tag	resourceTag	deleteResourceTags
Adding an instance tag	tms	createResourceTags

Operation	Resource Type	Trace Name
Deleting an instance tag	tms	deleteResourceTags
Deleting an artifact	artifact	deleteArtifact
Creating an image tag immutability policy	immutableRule	createImmutableRule
Deleting an image tag immutability policy	immutableRule	deleteImmutableRule
Modifying an image tag immutability policy	immutableRule	updateImmutableRule
Adding a domain name	addDomainName	addDomainName
Updating a domain name	updateDomainName	updateDomainName
Deleting a domain name	deleteDomainName	deleteDomainName
Creating an order	instance	createOrder
Deleting a job	job	deleteJob

8.2 Viewing Logs in CTS

Scenarios

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, 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 **All trace statuses**, **Normal**, **Warning**, or **Incident**.
- Time range: You can select **Last 1 hour**, **Last 1 day**, **Last 1 week**, or **Customize** in the upper right corner.

Step 4 Locate a record and click ⌄ to view its details.

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

----End