SoftWare Repository for Container

Best Practices

Issue 01

Date 2025-11-07

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 Automatically Adding Image Retention Policies Using Cloud Custodian

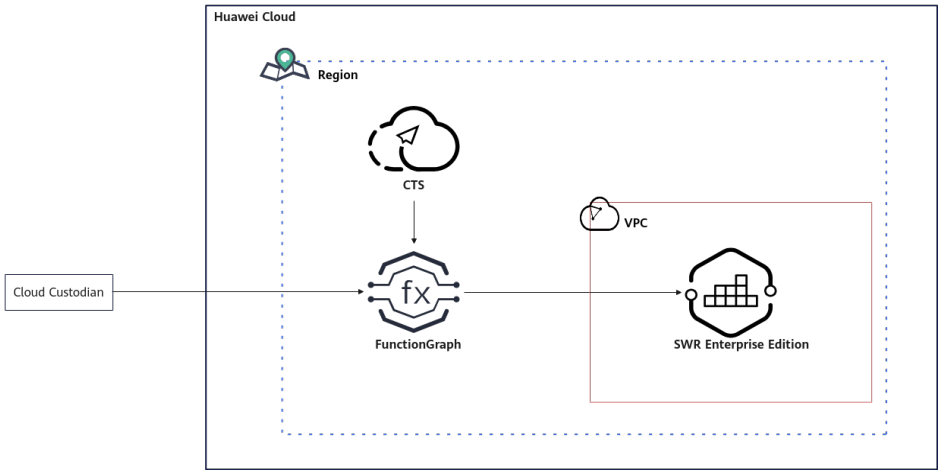
NOTE

This section applies only to SWR Enterprise Edition.

Many enterprises use cloud services provided by different cloud vendors. In such a hybrid cloud environment, alongside the security approaches provided by each cloud vendor, enterprises need strict governance over the cloud infrastructure. SWR is an important container service, and its security is critical. It is necessary to monitor SWR to prevent any access and permission vulnerabilities.

Cloud Custodian provides an open-source rule engine that can automatically check and govern cloud resources based on predefined security policies and compliance requirements. It can be used to control access to and govern resources in SWR. Cloud Custodian allows you to set rules to verify the environment based on the defined security and compliance standards. It helps follow security rules, manage tags, recycle unused resources, and control costs. It also provides an interface for you to easily implement consistent security policies and operational specifications in hybrid cloud environments.

Figure 1-1 Architecture of how Cloud Custodian is used to manage SWR resources



In this figure, there are the following cloud services:

- CTS records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.
- FunctionGraph hosts and computes event-driven functions in a serverless context while ensuring high availability, high scalability, and zero maintenance. All you need to do is write your code and set conditions.
- SWR Enterprise Edition provides secure and dedicated hosting services. You can host cloud native artifacts that comply with the OCI standard, such as container images and Helm charts.

Procedure

Step 1 Install Python. This is the running environment Cloud Custodian depends on.

NOTE

You are advised to use Python 3.11 and develop the Python application in a virtual environment.

For other Python versions, install them according to the official Python documentation. If you use native Python 3.11, run the commands below to create and activate a virtual environment.

```
# Create a virtual environment.
python -m venv custodian
# Activate a virtual environment (Linux).
source custodian/bin/activate
# Activate a virtual environment (Windows).
custodian\Scripts\activate.bat
If you use Conda or Miniconda, you can also run the commands below to create and activate a virtual environment.
# Create a virtual environment.
conda create -n custodian python=3.11
# Activate a virtual environment.
conda activate custodian
```

Step 2 Install Cloud Custodian.

1. Download Cloud Custodian.
   ```
   git clone https://github.com/huaweicloud/cloud-custodian.git
   cd cloud-custodian
   ```
2. Install Python dependencies.
   ```
   pip install -e .
   pip install -e tools/c7n_huaweicloud/.
   ```

For more details, see **Cloud Custodian official documentation**.

Step 3 Check whether Cloud Custodian is installed.

```
custodian schema huaweicloud.swr-ee
```

If the following information is displayed, the installation is successful.

```
$ custodian schema huaweicloud.swr-ee

Help
----

Huawei Cloud SWR Enterprise Edition Resource Manager.

This class manages SWR Enterprise Edition repositories on HuaweiCloud.
It provides functionality for discovering, filtering, and managing SWR repositories.

huaweicloud.swr-ee:
  actions:
  - notify-message
  - notify-message-structure
  - notify-message-template
  - webhook
  filters:
  - age
  - event
  - exempted
  - list-item
  - reduce
  - restricted
  - value

(custodian)
```

Step 4 Define a Cloud Custodian policy.

```
policies:
  - name: swr-ee-event
    resource: huaweicloud.swr-ee-namespace
    mode:
      type: cloudtrace
      xrole: fgs_default_agency
      events:
        - source: 'SWR.namespace'
          event: 'createNamespace'
          ids: 'resource_name'
    actions:
      - type: set-lifecycle
        rules:
          - template: latestPushedK
            params:
              latestPushedK: 50
            scope_selectors:
              repository:
                - kind: doublestar
                  pattern: '**'
            tag_selectors:
              - kind: doublestar
                decoration: matches
                pattern: '**'
```

NOTE

When you create a namespace of SWR Enterprise Edition, the policy automatically sets a retention policy for the namespace to retain the latest 50 artifact tags.

The following are two example policies for your reference:

Policy 1: Retain images in images repositories that have been created for more than 90 days.

```
policies:
  - name: swr-ee-repos
    resource: huaweicloud.swr-ee
    filters:
      - type: age
        days: 90
        op: gt
```

Policy 2: Retain images whose artifact tags match **release***.

```
policies:
  - name: swr-ee-set-immutability-rules
    resource: huaweicloud.swr-ee-namespace
```



```
actions:
  - type: set-immutability
    state: True
    scope_selectors:
      repository:
        - kind: doublestar
          pattern: '**'
    tag_selectors:
      - kind: doublestar
        decoration: matches
        pattern: '{release*}'
```

For more policy configurations, see **Cloud Custodian official documentation**.

Step 5 Run the custodian command to enable the policy.

1. Before executing the policy, configure environment variables in the terminal. The commands below are used in Linux. In Windows, replace **export** with **set**.

   ```
   # Configure the AK/SK of the Huawei Cloud account.
   export HUAWEI_ACCESS_KEY_ID={your-ak}
   export HUAWEI_SECRET_ACCESS_KEY={your-sk}
   # Configure the default region where resources are located, for example, ap-southeast-1. You can obtain the region from the web page URL.
   export HUAWEI_DEFAULT_REGION={your-region}
   ```

2. Enable the policy.

   ```
   custodian run --output-dir=<output_directory> <policy_name>.yaml
   ```

----End

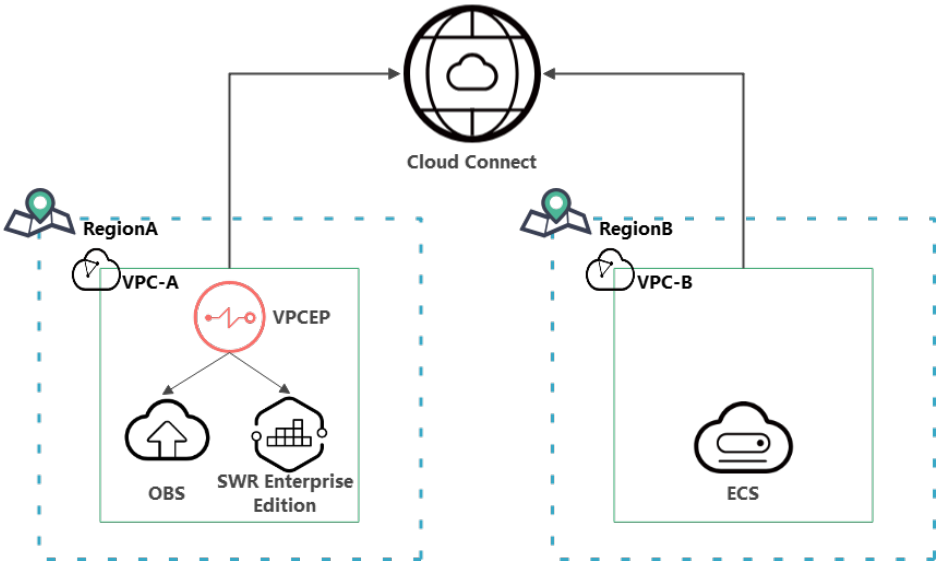
2 Accessing an SWR Enterprise Edition Instance Across Regions over the Private Network

Scenario

In SWR Enterprise Edition, if you need to push or pull images across regions, the VPC in the source region and the VPC in the region of the target SWR Enterprise Edition instance must be able to communicate with each other. You can take the following steps to enable mutual communication between the two VPCs:

1. **Configure Cloud Connect to enable network communication across regions.**
2. **Obtain the required information for network connectivity.**
3. **Configure a VPC endpoint to access OBS.**
4. **Configure the IP address ranges in Cloud Connect for forwarding OBS requests.**
5. **Configure private DNS resolution to access the target SWR Enterprise Edition instance.**
6. **Verify that images can be downloaded across regions.**

After completing these steps, you can push images to or pull images from the target SWR Enterprise Edition instance.



The following uses the resources of the same tenant to describe how to access an SWR Enterprise Edition instance in the CN South-Guangzhou region from an ECS in the CN East-Shanghai1 region. The environment information is as follows:

- **vpc-10**
  - Region: CN East-Shanghai1
  - IPv4 CIDR block: 10.0.0.0/8
  - IP address of ECS 1: 10.0.0.10 (ECS 1 is used to verify the image upload and download.)
- **vpc-default**
  - Region: CN South-Guangzhou
  - IPv4 CIDR block: 192.168.0.0/16
  - IP address of ECS 2: 192.168.0.18 (ECS 2 is used to obtain the IP address mapped to the OBS domain name.)
  - Access IP address of the SWR Enterprise Edition instance: 192.168.0.17

Constraints

Docker or containerd has been installed on ECS 1.

Procedure

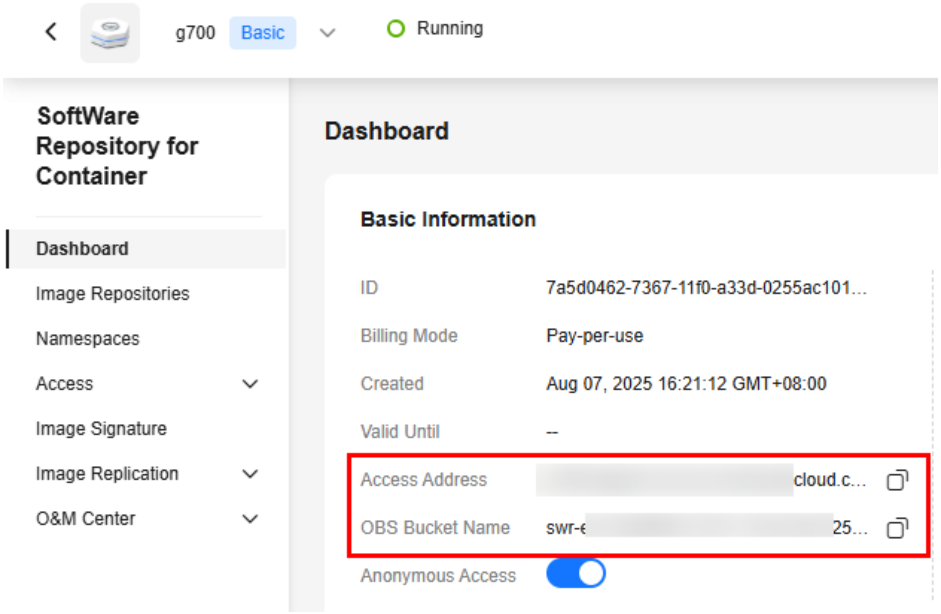
Step 1 Configure cross-region network connectivity.

Enable network connectivity between **vpc-10** in CN East-Shanghai1 and **vpc-default** in CN South-Guangzhou using Cloud Connect. For details, see **Using a Cloud Connection to Connect VPCs in the Same Account But Different Regions**.

Step 2 Obtain the domain name, OBS bucket name, and IP address of the target instance.

1. Access the **SWR console** and switch to the CN South-Guangzhou region.
2. In the navigation pane, choose **Enterprise Edition**. On the **Repositories** page, click the name of the target repository to go to the repository details page.

3. On the **Dashboard** page, obtain the access address and OBS bucket name.



4. In the navigation pane, choose **Access** > **Access Control** > **Private Network Access**. On the displayed page, locate the row that contains **vpc-default** in the **VPC** column, and record the value in the **IP** column.
5. Obtain the IP address of the OBS bucket in **vpc-default**.

   Run the **ping** command to obtain the IP address of the OBS domain name and record it. Ping the OBS domain name for several times to obtain multiple IP addresses.

Table 2-1 Information about the target instance

SWR Enterprise Edition Instance ID	Bucket Name	Domain Name (IP address) of SWR Enterprise Edition Instance	OBS Domain Name (IP Address)
${instance-id}	swr-ee-${instance-id}-registry	xxx.swr-pro.myhuaweicloud.com (192.168.0.17)	swr-ee-${instance-id}-registry.obs.${region-id}.myhuaweicloud.com (100.*.*.6, 100.*.*.7)

Step 3 Configure a VPC endpoint for accessing OBS.

1. Access the **management console**.
2. Click in the upper left corner and select the CN South-Guangzhou region.
3. Click in the upper left corner and choose **Networking** > **VPC Endpoint**.
4. On the VPC Endpoint console, click **Buy VPC Endpoint**. Set **Service Category** to **Cloud services**, and select **com.myhuaweicloud.{region_id}.swr**. If this service is not found, select **Find a service by name** for **Service Category**. Configure other parameters as needed.

- **VPC Endpoint Service Name**: Based on the OBS bucket name of the target instance, **submit a service ticket** or contact OBS O&M personnel to obtain the name of the OBS VPC endpoint service of the gateway type. Enter the OBS endpoint service name and click **Verify**.
- **VPC**: Select **vpc-default**.
- **Route Table**: Use the default route table of **vpc-default**.

Step 4 Configure the IP address ranges in Cloud Connect for forwarding OBS requests.

1. In the route table of **vpc-default**, view the routes for accessing OBS through the VPC endpoint.

   On the VPC Endpoint console, select the CN South-Guangzhou region. Then choose **Virtual Private Cloud** > **Route Tables**. Locate the row that contains the default route table **rtb-vpc-default** and click the name. On the displayed page, locate the route whose next hop type is **VPC endpoint**.

2. Click the number in the **IP Addresses** column to view all IP address ranges that can access OBS. Record the values in the **Destination** column.

3. On the **management console**, click in the upper left corner and select the CN East-Shanghai1 region. Click in the upper left corner and choose **Networking** > **Cloud Connect**. Click the name of the cloud connection created in **Step 1**. On the **Network Instances** tab, locate vpc-default and click **Modify VPC CIDR Block**.

4. In the **Other CIDR Block** area, add the IP address ranges obtained in **Step 4.2**.

Step 5 In the CN East-Shanghai1 region, configure private DNS resolution to access the target SWR Enterprise Edition instance and OBS domain name from **vpc-10**.

1. Go to the **Private Zones** page.
2. Click in the upper left corner and select the CN East-Shanghai1 region.
3. In the upper right corner of the page, click **Create Private Zone**.
4. Configure the private domain name used to access the target SWR Enterprise Edition instance.
5. Enter the domain name of the target SWR Enterprise Edition instance and configure other parameters. For details, see **Creating a Private Zone**.

   Domain Name: **xxx.swr-pro.myhuaweicloud.com**

   Region: **CN East-Shanghai1**

   VPC: **vpc-10**

   Locate the created private zone, click **Manage Record Sets** in the **Operation** column, and click **Add Record Set** to add the IP address of the target instance. In this example, the IP address is 192.168.0.17.
6. Repeat **Step 5.4** and **Step 5.5** to create a private zone for the OBS domain name.

   Domain Name: **swr-ee-${instance-id}-registry.obs.${region-id}.myhuaweicloud.com**

   Region: **CN East-Shanghai1**

VPC: **vpc-10**

Locate the created private zone, click **Manage Record Sets** in the **Operation** column, and click **Add Record Set** to add the IP addresses of OBS. In this example, the IP addresses are 100.*.*.6 and 100.*.*.7.

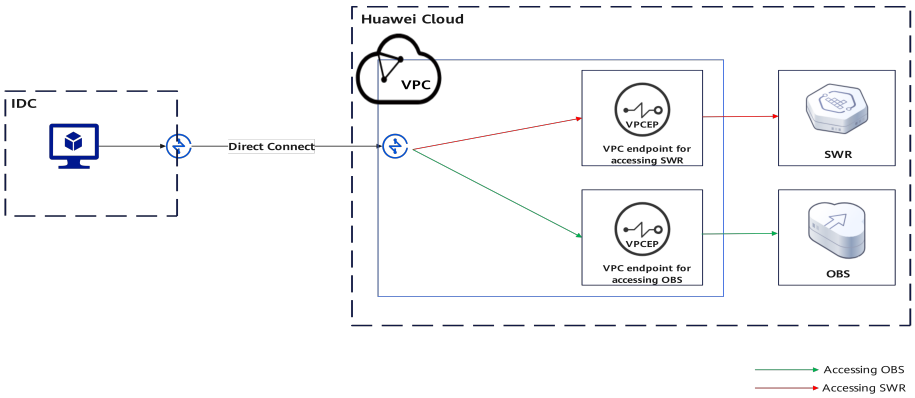
Step 6 Log in to ECS 1 in CN East-Shanghai1 and verify that the image in the image repository in CN South-Guangzhou can be downloaded.

----End

3 Accessing SWR Enterprise Edition from an On-Premises Data Center Over the Private Network

Scenario

If your on-premises data center needs to access SWR Enterprise Edition, you can connect to the VPC using Direct Connect or VPN and access cloud services over VPC endpoints. This method does not require the Internet and greatly improves the access speed.



Prerequisites

- A VPC is available. For details, see **Creating a VPC with a Subnet**.
- You have purchased the required VPC endpoints. For details, see **Buying a VPC Endpoint**.
- You have created a Direct Connect connection or VPN to connect the data center to the VPC. For details, see **Using Direct Connect to Connect an On-Premises Data Center to the Cloud** or **VPN**.

Procedure

Step 1 Obtain the domain name and IP address of the target SWR Enterprise Edition instance.

1. Access the **SWR console** and select the desired region.
2. In the navigation pane, choose **Enterprise Edition**. On the **Repositories** page, click the name of the target repository to go to the repository details page.
3. On the **Dashboard** page, record the access address (or the access domain name) of the instance.
4. In the navigation pane, choose **Access** > **Access Control**. On the **Private Network Access**, and record the private IP address of the instance.

Step 2 Configure the **hosts** file on on-premises servers using either of the following methods:

Configuring the /etc/hosts file directly

Configuring the on-premises DNS server (recommended)

Table 3-1 Comparison between two methods

Configuration Method	Scenario	Advantage and Disadvantage
Configuring the **/etc/hosts** file directly	The scenario where no DNS server is available in the on-premises data center	**Advantage**: No DNS server needs to be deployed in the on-premises data center. **Disadvantage**: You need to configure the **hosts** file on each on-premises servers. This is inconvenient.
Configuring the on-premises DNS server (recommended)	The scenario where a DNS server is available in the on-premises data center	**Advantage**: You need to configure the DNS server only once. This is easy to complete. **Disadvantage**: A DNS server needs to be deployed in the on-premises data center.

- Configuring the **/etc/hosts** file directly

  The following are steps in Linux:

  a. Log in to an on-premises server and run the following command to open **/etc/hosts**:
  ```
  sudo vim /etc/hosts
  ```
  b. Add a custom domain name. The address in **hosts** consists of the IP address and private domain name of the corresponding VPC endpoint, for example, *xx.xx.xx.xx xxxx*.swr-pro.myhuaweicloud.com.

  NOTE

  xx.xx.xx.xx is the node IP address queried in **Step 1.4**, and xxxx.swr-pro.myhuaweicloud.com is the repository access address queried in **Step 1.3**.

  c. Run the following command to restart the network:
  ```
  sudo/etc/init.d/networking restart
  ```


- Configuring the on-premises DNS server

  Configure forwarding rules on the on-premises DNS server.

  The method of configuring DNS forwarding rules varies depending on OSs. For details, see the operation guide of the corresponding DNS software.

  The following uses Linux and the common DNS software Bind as an example:

  a. Edit the **/etc/named.conf** file to add a zone.

  ```
  zone " xxxx.swr-pro.myhuaweicloud.com " IN {
    type master;
    file " /var/named/xxxx.swr-pro.myhuaweicloud.com.zone";
  };
  ```

  NOTE

  xxxx.swr-pro.myhuaweicloud.com is the repository access address obtained in **Step 1.3**.

  b. Configure the DNS server to map the custom domain name to the corresponding IP address. Create the file **/var/named/xxxx.swr-pro.myhuaweicloud.com.zone** corresponding to the file in **Step 2.a**.

  ```
  $TTL    604800
  @ IN     SOA     xxxx.swr-pro.myhuaweicloud.com. root.localhost. (
                        2         ; Serial
                   604800         ; Refresh
                    86400         ; Retry
                  2419200         ; Expire
                   604800 )       ; Negative Cache TTL
  ;
  @    IN   NS   xxxx.swr-pro.myhuaweicloud.com.
  xxxx.swr-pro.myhuaweicloud.com.    IN   A     xx.xx.xx.xx
  ```

  c. Run the following command to restart the service:

  ```
  /sbin/service named restart
  ```

  NOTE

  - You can query SWR endpoints in different regions in **Regions and Endpoints**.
  - If no DNS server is available in the on-premises data center, add the endpoint IP address for accessing DNS to the **/etc/resolv.conf** file on the on-premises servers.

Step 3 Verify that the configuration is successful.

Log in to any on-premises server, run the **ping xxxx.swr-pro.myhuaweicloud.com** command, and check the command output.

- Successful configuration: A message similar to "Reply from..." is displayed. You can then access SWR using xxxx.swr-pro.myhuaweicloud.com.
- Failed configuration: If "Request timed out" or "Destination host unreachable" is displayed, **submit a service ticket** to contact Huawei O&M engineers.

----End

CAUTION

The preceding configuration only allows you to push images. To pull images, you also need to **configure a VPC endpoint for accessing the private IP address of OBS**.

4 Cross-Region DR Using SWR Enterprise Edition

4.1 Using SWR Enterprise Edition to Implement Cross-Region DR for Self-Built Harbor

If you need to implement remote DR for Harbor, you can use SWR Enterprise Edition. By leveraging the replication capability of Harbor, you can copy image artifacts from Harbor at a site to SWR Enterprise Edition at another site. If Harbor is abnormal, you can pull the image artifacts replicated by SWR Enterprise Edition for remote DR. To achieve this, you can take the following steps:

1. Synchronize images from Harbor to SWR Enterprise Edition.

2. Configure a custom domain name for remote DR.

Prerequisites

- You have purchased an SWR Enterprise Edition instance. For details, see **Buying a Repository**.
- You have set up Harbor, and the network between Harbor and SWR Enterprise Edition is connected.
- The custom domain name of the SWR Enterprise Edition instance is the same as the Harbor domain name. For details about how to configure a custom domain name, see **Domain Names**.

Procedure

1. Synchronize images from Harbor to SWR Enterprise Edition.

Step 1 Create a namespace.

1. Log in to the **SWR console**. In the upper left corner, switch to your region.
2. In the navigation pane, choose **Namespaces**. In the upper right corner, click **Create Namespace**.
3. Enter the name of the target project in Harbor and select the namespace type.

4. Click **OK**.

Step 2 Configure the destination image registry on Harbor.

1. Create a registry endpoint.

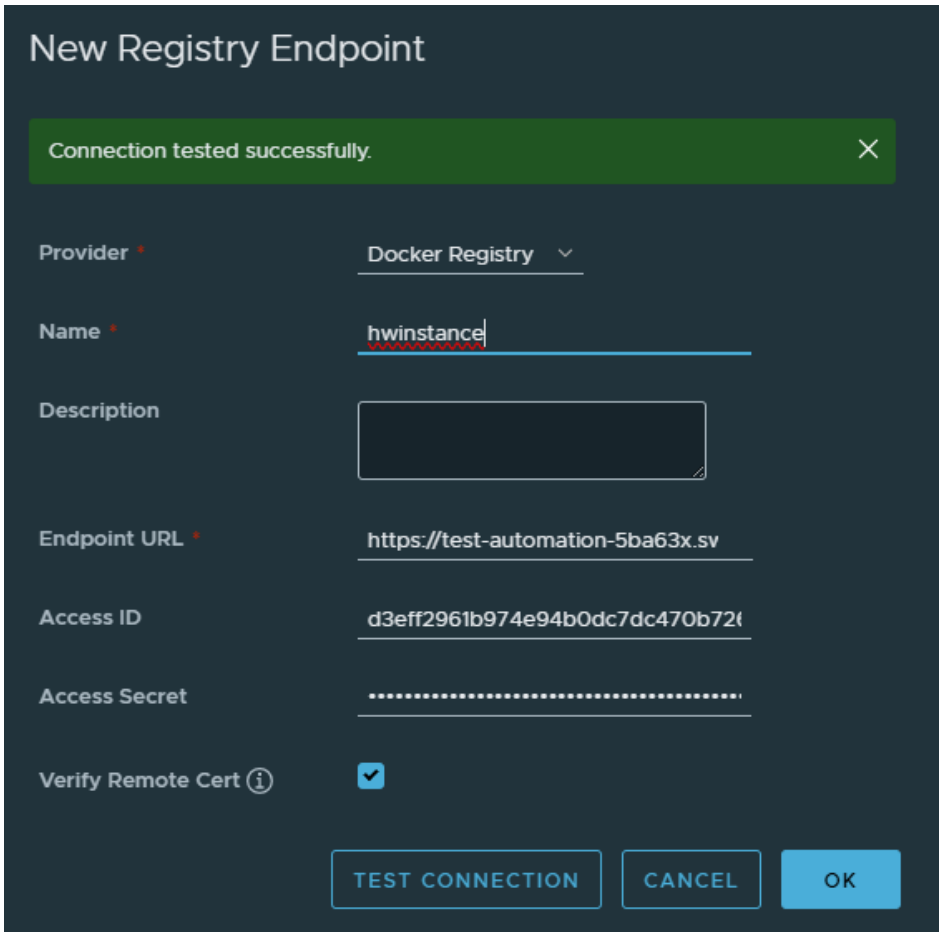


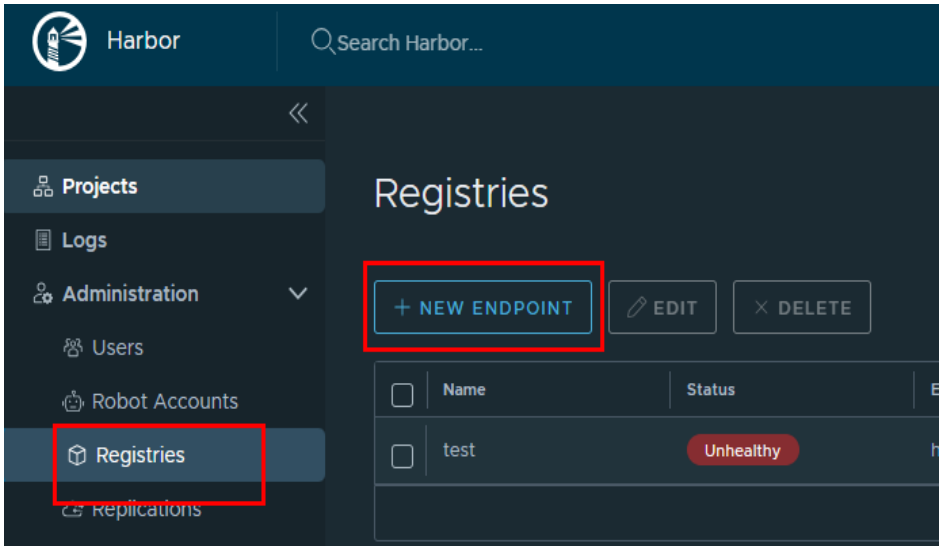
Table 4-1 Parameters for creating a registry endpoint

Parameter	Description
Provider	Select **Docker Registry**.
Name	Enter a custom name.
Description	Enter a description as needed.
Endpoint URL	Enter the domain name of the target SWR Enterprise Edition instance in the format of https://*{address-of-of-the-SWR-Enterprise-Edition-instance}*. To obtain the address, log in to the **SWR console**, switch to the target region in the upper left corner of the page. On the displayed page, click the name of the target repository to go to the repository details page. In the **Basic Information** area of the **Dashboard** page, obtain the access address.

Parameter	Description
Access ID	Username for accessing the instance. You can obtain the username from the table downloaded in **Creating a Long-Term Credential**.
Access Secret	Password for accessing the instance. You can obtain the password from the table downloaded in **Creating a Long-Term Credential**.
Verify Remote Cert	You are advised to deselect this option.

Step 3 Configure a replication rule.

1. Choose **Administration** > **Registries** and then click **NEW ENDPOINT**.



2. Configure the parameters.

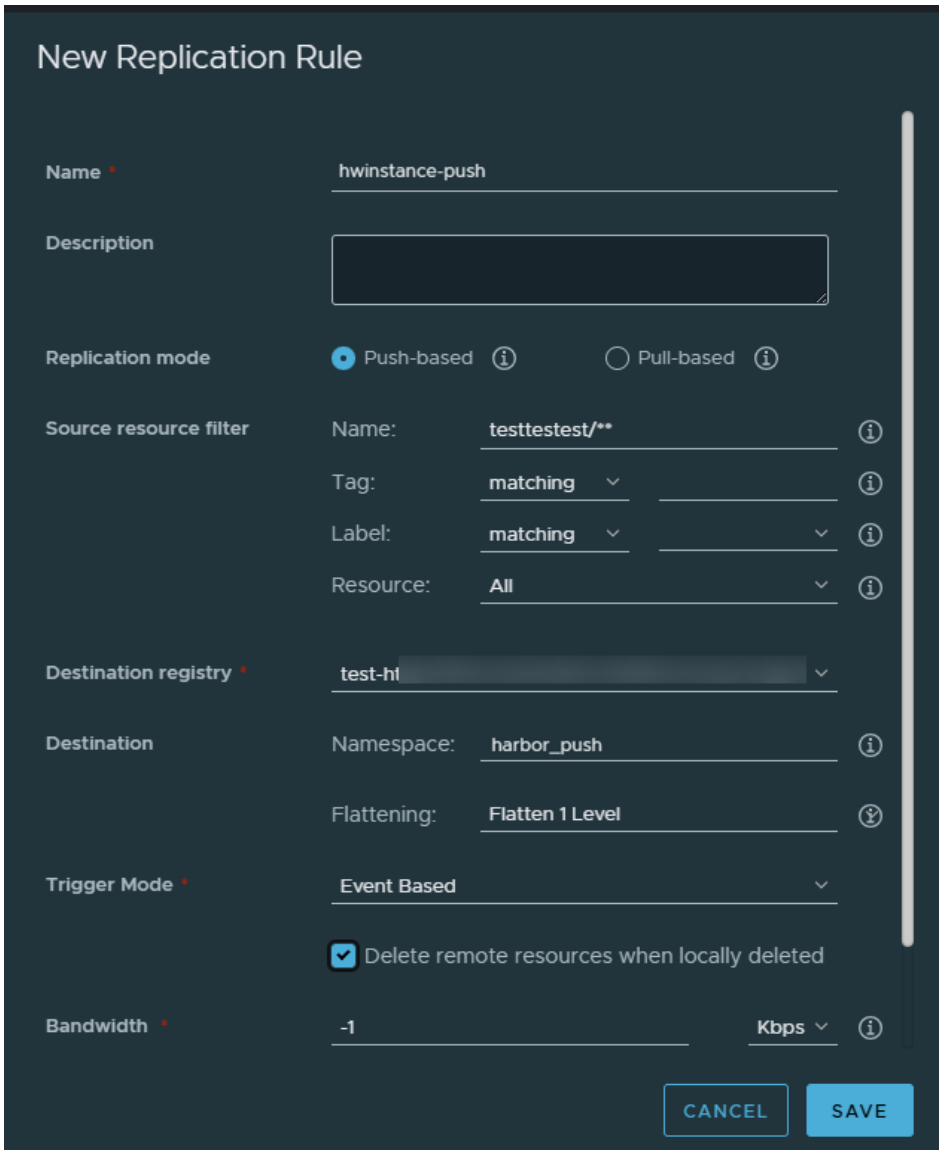


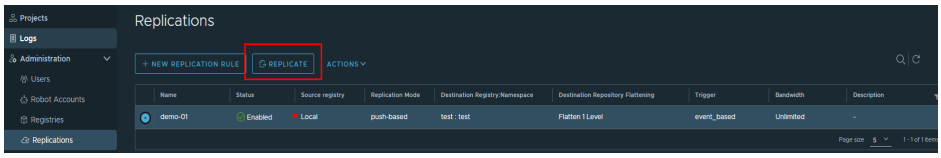
Table 4-2 Parameters for creating a replication rule

Parameter	Description
Name	Enter a custom name.
Description	Enter a description as needed.
Replication mode	Select **Push-based**. Images are pushed from the local Harbor to the destination registry.
Source resource filter	Filters images in Harbor based on the configuration. All resources are selected by default.
Destination registry	Select the registry endpoint created in **Step 2.1**.

Parameter	Description
Destination	Enter the name of the namespace created in **Step 1**. Flattening reduces the registry hierarchy during image replication. You are advised to select **Flatten 1 Level**.
Triggering Mode	Select an option as needed. You are advised to select **Event Based**.
Bandwidth	Set it to the maximum network bandwidth. **–1** indicates that the network bandwidth is not limited.
Overwrite	If there are resources with the same name, specify whether to overwrite the resources at the destination.

For more information, see the **Harbor official website**.

Step 4 Select the replication rule and click **REPLICATE** to replicate images.



----End

2. Configure a custom domain name for remote DR.

The following three scenarios are provided based on the network relationship between Harbor and SWR Enterprise Edition.

Assume that the SWR Enterprise Edition instance is in Guangzhou and the Harbor repository is in Shanghai. The table below describes three example scenarios.

Table 4-3 Remote DR scenarios

Scenario	Description	Remote DR Solution
Scenario 1	Harbor is deployed on Huawei Cloud, and SWR Enterprise Edition is accessed over the public network.	If Harbor in Shanghai becomes faulty and images cannot be pushed or pulled, you can modify the DNS settings of the custom domain name to pull images from SWR Enterprise Edition in Guangzhou. The detailed operations are as follows: 1. Log in to the **DNS console**. Switch to the CN East-Shanghai region. 2. In the navigation pane, choose **Private Zones**. 3. Locate the private zone created for the custom domain name of the SWR Enterprise Edition instance and associated with your VPC. 4. On the **Record Sets** page, click the target record set. 5. In the **Modify Record Set** dialog box, configure the parameters, and then click **OK**. • **Type**: Select **CNAME**. • **Name**: Enter the prefix of the custom domain name. • **Value**: Enter the default domain name of the SWR Enterprise Edition instance in the CN South-Guangzhou region. • **TTL**: Retain the default value.
Scenario 2	Harbor is not deployed on Huawei Cloud, and SWR Enterprise Edition is accessed over the public network.	If Harbor becomes faulty, you cannot push or pull images. In this case, take the following steps: 1. Access the SWR Enterprise Edition instance over the public network. For more information, see **Public Network Access**. 2. Configure the DNS resolution to map the domain name to the public IP address of the SWR Enterprise Edition instance. 3. Set the custom domain name of the SWR Enterprise Edition instance to the domain name used by Harbor.
Scenario 3	Harbor is not deployed on Huawei Cloud, and SWR Enterprise Edition is accessed over a private network.	If Harbor becomes faulty, you cannot push or pull images. In this case, take the following steps: 1. Obtain the IP address of the SWR Enterprise Edition instance. 2. Configure the routes and DNS resolution. 3. Point the domain name of Harbor to the IP address of the SWR Enterprise Edition instance.

4.2 Using SWR Enterprise Edition Across Regions for Remote DR

If you want to implement remote DR for image artifacts in an SWR Enterprise Edition instance in a region, you can synchronize the image artifacts to an SWR Enterprise Edition instance in a different region.

Prerequisites

- You have purchased an SWR Enterprise Edition instance named **S1** in one region (for example, region A) and an SWR Enterprise Edition instance named **S2** in another region (for example, region B). For details, see **Buying a Repository**.
- You have configured the same custom domain name for the SWR Enterprise Edition instances. For details about how to configure a custom domain name, see **Domain Names**.

Procedure

Step 1 Configure image synchronization rules for the two SWR Enterprise Edition instances.

Configure an image synchronization rule for each SWR Enterprise Edition instance. For details, see **Image Synchronization**.

Step 2 Configure access control for the two SWR Enterprise Edition instances.

- If the two instances access each other through the private network, you need to configure private network access for them.
- If the two instances access each other through the public network, you need to configure public network access for them. For details, see **Public Network Access**.

Step 3 Switch the DNS resolution for DR.

If instance **S1** is abnormal and you cannot push or pull images, you can modify the DNS settings of the custom domain name associated with the VPC of instance **S2** to pull the same images from instance **S2** across regions. The detailed operations are as follows:

1. Log in to the **DNS console**. Switch to region A.
2. In the navigation pane, choose **Private Zones**.
3. Locate the private zone created for the custom domain name of the SWR Enterprise Edition instance and associated with your VPC.
4. On the **Record Sets** page, click the target record set.
5. In the **Modify Record Set** dialog box, configure the parameters and then click **OK**.

Table 4-4 Modifying a record set

Parameter	Description
Record Set Type	– If the two instances access each other through the public network, select **CNAME**. – If the two instances access each other through the private network, select **A**.
Record Set Name	Enter the prefix of the custom domain name.
Record Set Value	– If the two instances access each other through the public network, set this parameter to the public domain name of instance **S2**. – If the two instances access each other through the private network, set this parameter to a private IP address in the VPC where instance **S2** is deployed.
TTL	Retain the default value.

----End