SoftWare Repository for Container

Service Overview

Issue	01
Date	2022-09-30

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

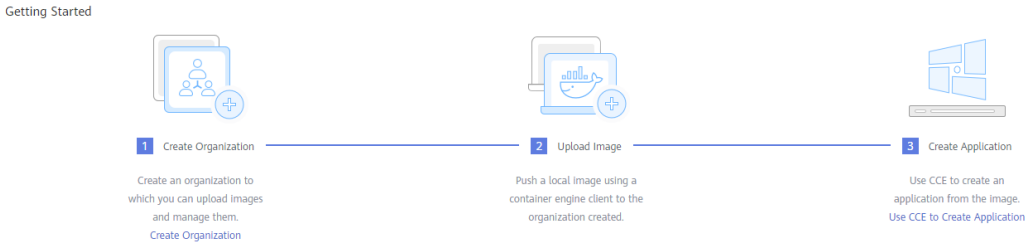
1 Introduction 1
2 Advantages 3
3 Application Scenarios 4
4 Security 5
4.1 Shared Responsibilities 5
4.2 Identity Authentication and Access Control 6
4.2.1 Identity Authentication and Management 6
4.2.2 Example of Identity-based Policy 7
4.2.3 Access Control 9
4.3 Data Protection 11
4.4 Audit and Logging 12
5 Basic Concepts 14
6 Notes and Constraints 16
7 Permissions 17
7.1 SWR Permissions 17
8 Related Services 19

1 Introduction

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

SWR can either work with CCE or be used as an independent container image repository.

Figure 1-1 How SWR works



Features

- **Full lifecycle management of images**

  SWR manages the whole lifecycle of your container images, including push, pull, and deletion.

- **Private image repository and access control**

  Private image repository and fine-grained permission management allow you to grant different access permissions, namely, read, write, and edit, to different users.

- **Large scale image distribution acceleration**

  SWR uses the image pull acceleration technology to ensure faster image pull for CCE clusters in high concurrency scenarios.

- **Automatic deployment update through triggers**

  Image deployment can be triggered automatically upon image update. Simply set a trigger to the desired image. Every time the image is updated, the application deployed with this image will be automatically updated.

Accessing SWR

The cloud platform provides a web-based management console and HTTPS-based APIs through which you can access the SWR service.

- Using APIs

  If you want to integrate SWR into a third-party system for secondary development, use APIs to access SWR. For details, see *SWR API Reference*.

- Using the management console

  Use this mode if you do not want to integrate SWR into a third-party system.

2 Advantages

Ease of Use

- You can directly push and pull container images without platform build or O&M.
- SWR provides an easy-to-use management console for full lifecycle management over container images.

Security and Reliability

- SWR supports HTTPS to ensure secure image transmission, and provides multiple security isolation mechanisms between and inside accounts.
- Based on professional storage services, SWR provides highly reliable storage service for your container images.

Image Acceleration

SWR uses the image pull acceleration technology to ensure faster image pull for CCE clusters in high concurrency scenarios.

3 Application Scenarios

Image Lifecycle Management

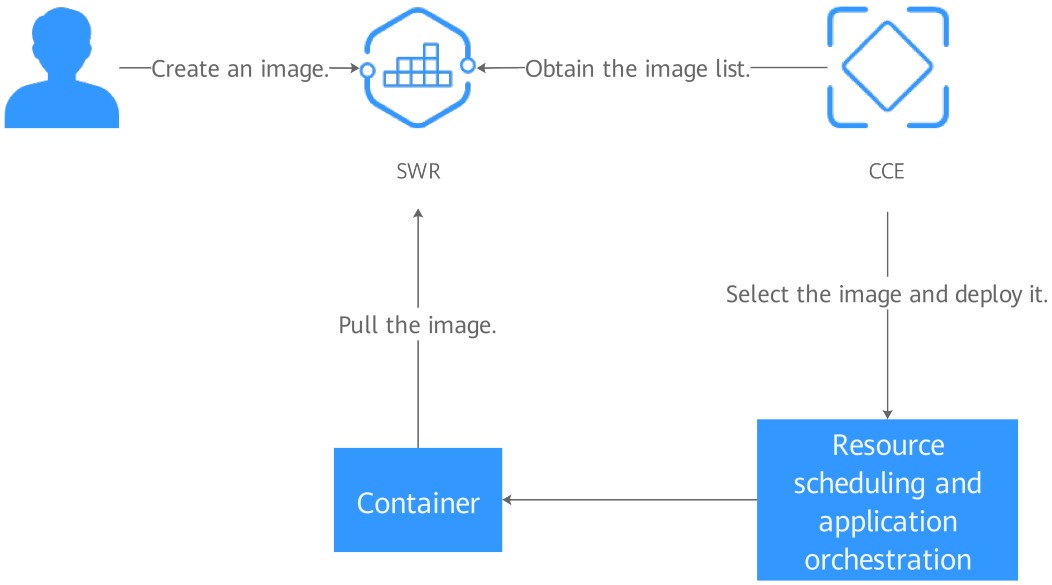
You can use SWR to build, push, pull, synchronize, and delete container images.

Advantages

- Pull acceleration ensures faster image pull for CCE clusters.
- Up to 99.999999999% image storage reliability is achieved by working with Object Storage Service (OBS).
- Fine-grained authorization allows you to control access to specific images and images in specific organizations.

Related service: Cloud Container Engine (CCE)

Figure 3-1 SWR working with CCE



4 Security

4.1 Shared Responsibilities

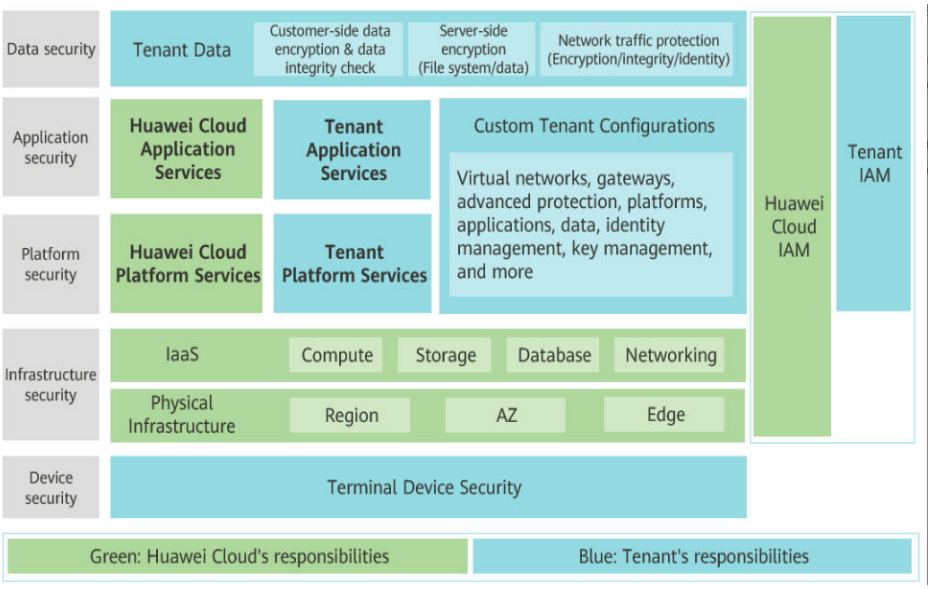
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 4-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 4-1 Huawei Cloud shared security responsibility model



4.2 Identity Authentication and Access Control

4.2.1 Identity Authentication and Management

The Identity and Access Management (IAM) service provides free permissions management for secure access to your cloud services and resources. The IAM administrator can assign users permissions for accessing SWR resources through *identity authentication* (logging in) and *authorization* (assigning permissions).

Identity Authentication

If you want to use Huawei Cloud services and resources, you must register as an IAM user.

Account

An account is created after you successfully register with Huawei Cloud, and you can use it to purchase Huawei Cloud resources. The account has full access permissions for your cloud resources and can be used to make payments for them. You can use the account to reset user passwords, assign permissions, and receive and pay all bills generated by your IAM users for their usage of resources.

You cannot modify or delete your account in IAM, but you can do so in My Account.

IAM User

IAM users are created with an account to use cloud services. Each IAM user has their own identity credentials (passwords and access keys) and uses cloud resources based on assigned permissions. IAM users cannot make payments themselves. You can use your account to pay their bills.

User Group

Users in the same user group have the same permissions. IAM users must be added to a user group to obtain the permissions assigned to the user group. If a user is added to multiple user groups, the user inherits the permissions assigned to all these groups.

IAM Roles

The IAM roles are IAM users with special permissions. But they are irrelevant to a specific account. You can switch between different roles as required.

Policy-based Permissions Management

You can create a policy and attach it to Huawei Cloud identities and resources to manage their permissions in Huawei Cloud. A policy is an object in Huawei Cloud. When a subject (user, root user, or role session) sends a request, Huawei Cloud will evaluate the request based on the permissions on these policies. Most policies are stored as JSON documents.

Identity-based Policy

Identity-based policies are JSON permission policy documents that can be attached to identities (IAM users, user groups, or roles). These policies manage the permissions of users and roles for operating on specific resources under specific conditions.

4.2.2 Example of Identity-based Policy

SWR provides some permissions for roles. You can assign these permissions to IAM users or user groups. With these roles, you can control access to SWR resources and operations at different levels.

Tenant Administrator

Administrator permissions for all services except IAM, including all SWR permissions. Its JSON policy document is as follows:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "obs:*:*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringNotEqualsIgnoreCase": {
                    "g:ServiceName": [
                        "iam"
                    ]
                }
            },
            "Action": [
                "*:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```


Tenant Guest

Read-only permissions for all services except IAM, including permissions such as image pull.

Its JSON policy document is as follows:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "obs:*:get*",
            "obs:*:list*",
            "obs:*:head*"
         ],
         "Effect": "Allow"
      },
      {
         "Condition": {
            "StringNotEqualsIgnoreCase": {
               "g:ServiceName": [
                  "iam"
               ]
            }
         },
         "Action": [
            "*:*:get*",
            "*:*:list*",
            "*:*:head*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

ServiceStage Developer

ServiceStage developer permissions, including permissions such as image pull.

Its JSON policy document is as follows:

```
{
   "Version": "1.0",
   "Statement": [
      {
         "Action": [
            "servicestage:*:*"
         ],
         "Effect": "Allow"
      }
   ],
   "Depends": [
      {
         "catalog": "BASE",
         "display_name": "Tenant Guest"
      }
   ]
}
```

SWR Admin

SWR administrator permissions, including all SWR permissions.

Its JSON policy document is as follows:


```
{
   "Version": "1.0",
   "Statement": [
      {
         "Action": [
            "SWR:software:*",
            "SWR:dockerimage:*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

4.2.3 Access Control

Access Mode

A bunch of tools, including console, command line tools, APIs, and SDKs, are provided for you to access SWR. No matter which method you use, you are accessing SWR through REST APIs.

The SWR APIs support both authenticated and anonymous requests. There will usually be anonymous requests in the scenarios that require public access, for example, accessing a hosted static website. In most cases, requests for SWR resources must be authenticated. An authenticated request must contain a signature value. The signature value is calculated based on the requestor's access keys (AK/SK) as the encryption factor and the specific information carried in the request body. AK/SK authentication uses AK/SK-based encryption to authenticate a request sender. For details about an AK/SK and how to obtain one, see **Obtaining a Long-Term Valid Login Command**.

Control Policy

Users' access to SWR in any mode is restricted by the SWR access control policy. Currently, SWR supports the following control policies:

Table 4-1 SWR access control modes

Access Mode		Description	Reference
Permissions control	IAM permissions	IAM permissions define which actions on your cloud resources are allowed and which actions are denied, to control access to your resources. After an IAM user is created, the administrator adds it to a user group. The administrator can assign the user group required SWR access permissions and all users in this group then inherit the assigned permissions.	**IAM Permissions**
	Image permissions	The image permissions refer to the permissions to read, edit, and manage an image. In addition to assigning permissions to users in IAM, the administrator can add, modify, and delete permissions for IAM users in the image details page on SWR console.	**Granting Permissions for a Specific Image**

Access Mode		Description	Reference
	Organization permissions	Organizations enable efficient management of images. Organizations are used to isolate image repositories. With each organization being limited to one company or department, images can be managed in a centralized and efficient manner. An image name needs to be unique within an organization. An IAM user can join different organizations.	**Organization Management**

4.3 Data Protection

SWR takes different measures to keep the data stored in SWR secure and reliable.

Table 4-2 Data protection measures

Measure	Description	Reference
Transmission encryption (HTTPS)	To ensure secure data transmission, SWR supports only HTTPS.	**Making an API Request**
Data redundancy	By default, SWR user metadata and image data are stored in multiple AZs in the same region. If one AZ becomes unavailable, data can still be properly accessed from the other AZs. The multi-AZ storage is ideal for scenarios that demand high reliability.	N/A

Measure	Description	Reference
Data integrity verification (SHA256)	During image push or pull, data may become inconsistent due to network hijacking, caching, and other reasons. SWR verifies data consistency by calculating the SHA256 value when data is uploaded or downloaded.	**Uploading an Image Through the Client**
Cross-region replication	You can configure cross-region replication rules to automatically, asynchronously replicate images from a source repository to a destination repository in another region. This provides you with disaster recovery across regions, catering to your needs for remote backup.	Configuring Automatic Image Synchronization Between Regions
Image retention policy	You can keep multiple tags of an image for quickly retrieving and restoring an image tag, or recovering data from both accidental actions and application failures.	**Adding an Image Retention Policy**

4.4 Audit and Logging

Audit

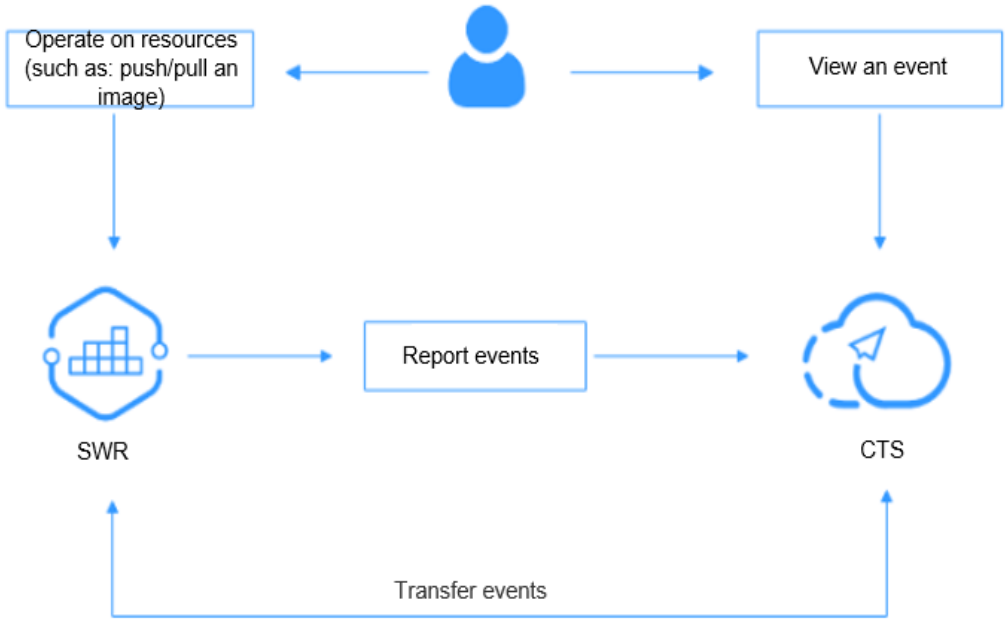
Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

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

For details about how to enable and configure CTS, see **Getting Started**.

For details about SWR operations supported by CTS, see **SWR Operations Supported by CTS** .

Figure 4-2 Audit process



Logging

Once CTS is enabled, the system starts recording operations on SWR and CTS stores operations within the latest week.

For details about how to view SWR audit logs, see **Viewing Logs in CTS**.

5 Basic Concepts

Image

Images are like templates that include everything needed to run applications. When deploying containerized applications, you can use images from the Docker image center and your private image registries. For example, an image can contain a complete Ubuntu operating system, in which only the required programs and dependencies are installed. Docker images are used to create Docker containers. Docker provides an easy way to create and update your own images. You can also pull images created by other users.

Container

A container is a running instance of a Docker image. Multiple containers can run on one node. Containers are actually software processes. Unlike traditional software processes, containers have separate namespaces and do not run directly on a host.

Images become containers at runtime, that is, containers are created from images. Containers can be created, started, stopped, deleted, and suspended.

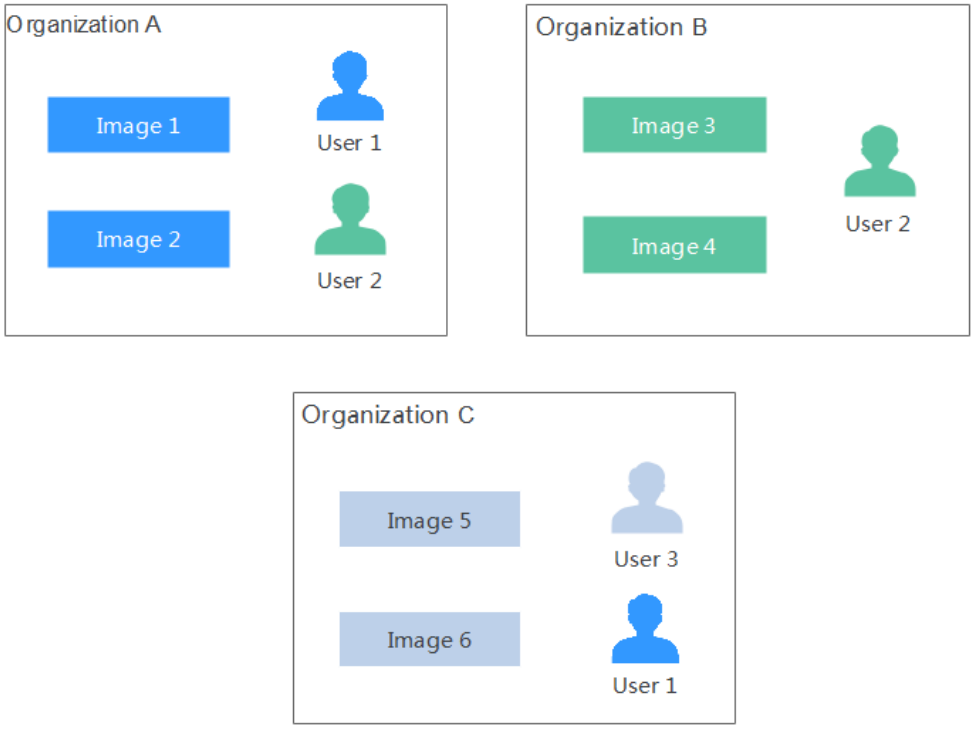
Repository

Image repositories are used for storing Docker images. An image repository hosts different versions of a specific containerized application.

Organization

Organizations are used to isolate image repositories. With each organization being limited to one company or department, images can be managed in a centralized and efficient manner. A user can access different organizations as long as the user has corresponding permissions. Different permissions, namely read, write, and manage, can be assigned to different users in the same account.

Figure 5-1 Organization



6 Notes and Constraints

Quotas

Quotas are imposed on the number of organizations a user can create. **Table 6-1** lists the quotas imposed by SWR.

Table 6-1 SWR resource quotas

Resource Type	Quota
Organization	5

Requirements on Images to Upload

- If you use the container engine client to push images to SWR, each image layer cannot exceed 10 GB.
- If you use the SWR console to upload images, a maximum of 10 files can be uploaded at a time. The size of a single file (including the decompressed files) cannot exceed 2 GB.

7 Permissions

If you need to assign different permissions to employees in your enterprise to access your SWR resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, enabling secure access to your cloud resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific cloud resources. For example, some software developers in your enterprise need to use SWR resources but should not be allowed to delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using SWR resources.

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

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

7.1 SWR Permissions

By default, new IAM users do not have any permissions granted. You need to add them to one or more groups and attach permissions policies or roles to these groups. In this way, the users can inherit permissions from the groups and perform operations on specific cloud resources.

SWR is a project-level service deployed and accessed in specific physical regions. To assign AOM permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing SWR, the users need to switch to a Region where they have been authorized to use this service.

Table 7-1 SWR permissions

Name	Description	Type
SWR Admin	SWR administrator permissions, including all SWR permissions.	System-defined role
Tenant Administrator	Administrator permissions for all services except IAM, including all SWR permissions.	System-defined role
Tenant Guest	Read-only permissions for all services except IAM, including permissions such as image pull.	System-defined role
ServiceStage Developer	ServiceStage developer permissions, including permissions such as image pull.	System-defined role

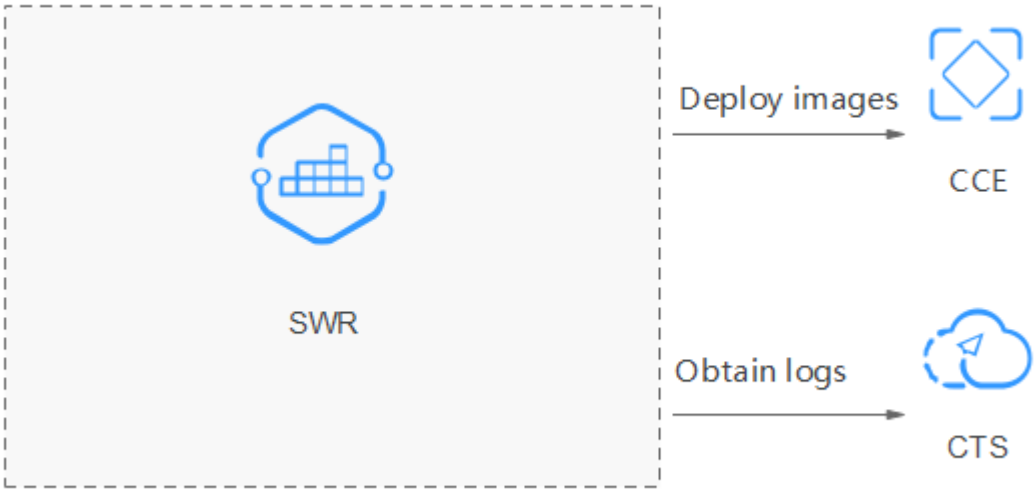
NOTE

- **Granting user permissions** enables you to grant different permissions, namely, read, write, and manage, to different users for them to access either a specific image or images of a specific organization.
- In addition, SWR has the **SWR FullAccess**, **SWR OperateAccess**, and **SWR ReadOnlyAccess** permissions. However, the three are available only for SWR Enterprise Edition, which OBT has been suspended .

8 Related Services

SWR works with other cloud services and requires permissions to access them. For details, see **Figure 8-1**.

Figure 8-1 Relationship between SWR and other services



- Cloud Container Engine (CCE)

  CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud.

  SWR works seamlessly with CCE to allow you to deploy your images held by SWR on CCE clusters.

- Cloud Trace Service (CTS)

  CTS generates traces to enable you to get a history of operations performed on cloud service resources. The content of a trace includes operation requests sent using the management console or open APIs as well as the operation

results. You can view all generated traces to query, audit, and backtrack performed operations.

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

