SoftWare Repository for Container

Service Overview

Issue 03

Date 2022-11-07

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 Introduction

Overview

SoftWare Repository for Container (SWR) provides easy, secure, and reliable management of container images throughout their lifecycle, facilitating the deployment of containerized applications.

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

SWR Shared Edition is free of charge.

Features

- Full lifecycle management of images

  SWR manages the full lifecycle of your container images, including push, pull, and deletion.
- Private image repository

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

  Acceleration technology developed by Huawei brings faster image pull for CCE clusters during high concurrency.
- Automatic deployment update through triggers

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

Access Mode

You can access SWR using a web-based console or through HTTPS-based application programming interfaces (APIs).

- APIs

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

- Console

  If you do not want to integrate SWR into a third-party system, use the console to access SWR. If you already have an account on the cloud platform, log in to the console and choose **SoftWare Repository for Container**.

  If you do not have an account, create one as instructed in **Signing Up with Huawei Cloud**.

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 of container images.

Security and Reliability

- SWR uses HTTPS to secure image transmission, and provides multiple isolation mechanisms between and inside accounts to control access to images.
- Based on professional storage services provided by Huawei, SWR provides highly reliable storage service for your container images.

Faster Image Pull

- Huawei's acceleration technology makes image pull faster for CCE clusters during high concurrency.

3 Application Scenarios

Image Lifecycle Management

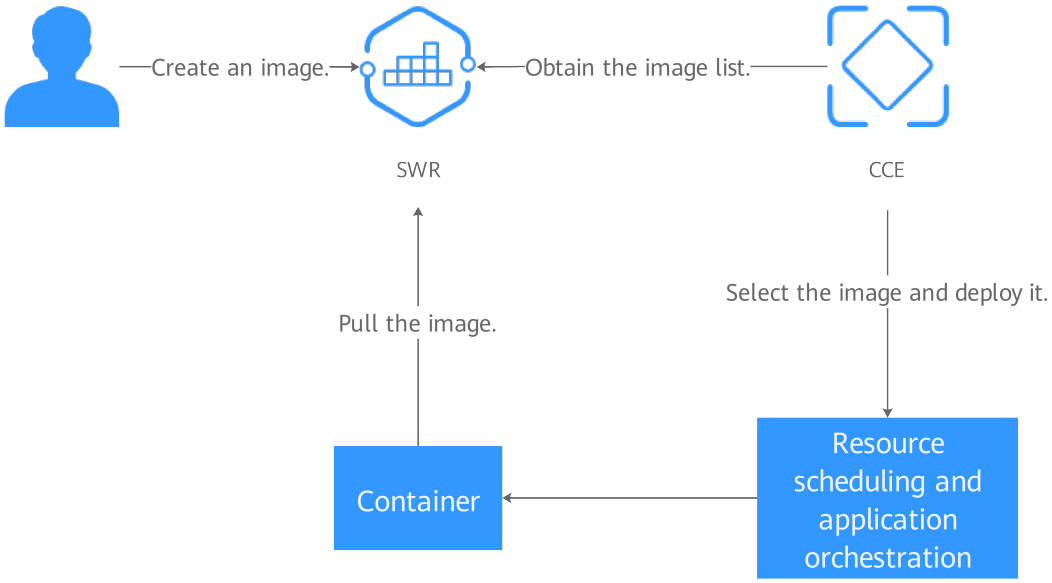
You can use SWR to build, push, pull, synchronize, and delete container images.

Advantages

- Proprietary acceleration makes image pull faster during high concurrency.
- Up to 99.999999999% image storage reliability is achieved by working with Huawei Cloud Object Storage Service (OBS).
- Fine-grained authorization allows you to control access to specific images and images in specific organizations.

Related Services

You can use SWR together with CCE in this scenario.



4 Security

4.1 Shared Responsibilities

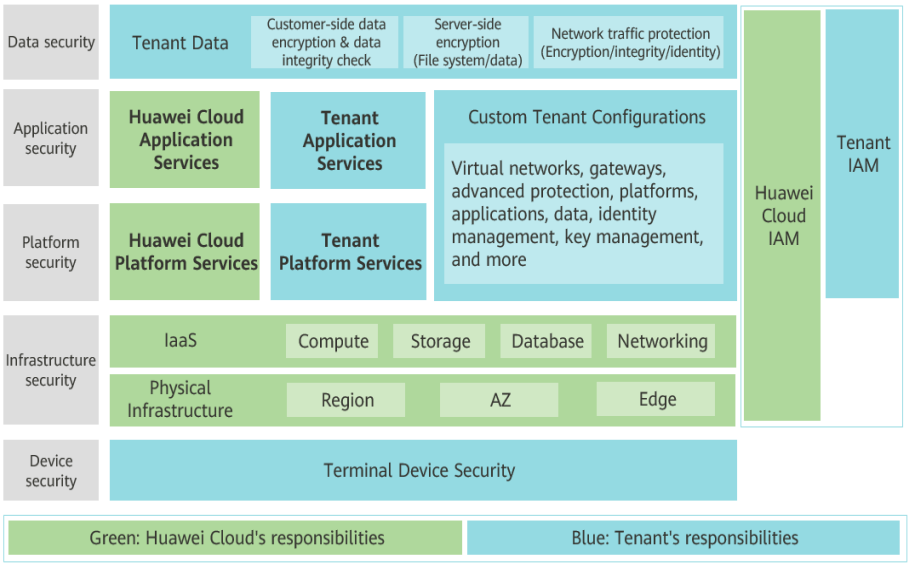
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system 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 and 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 controls who can access 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

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

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

An identity-based policy is defined in a JSON document of an identify (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 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.	**Basic Concepts**
	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 of 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 a Container Engine 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

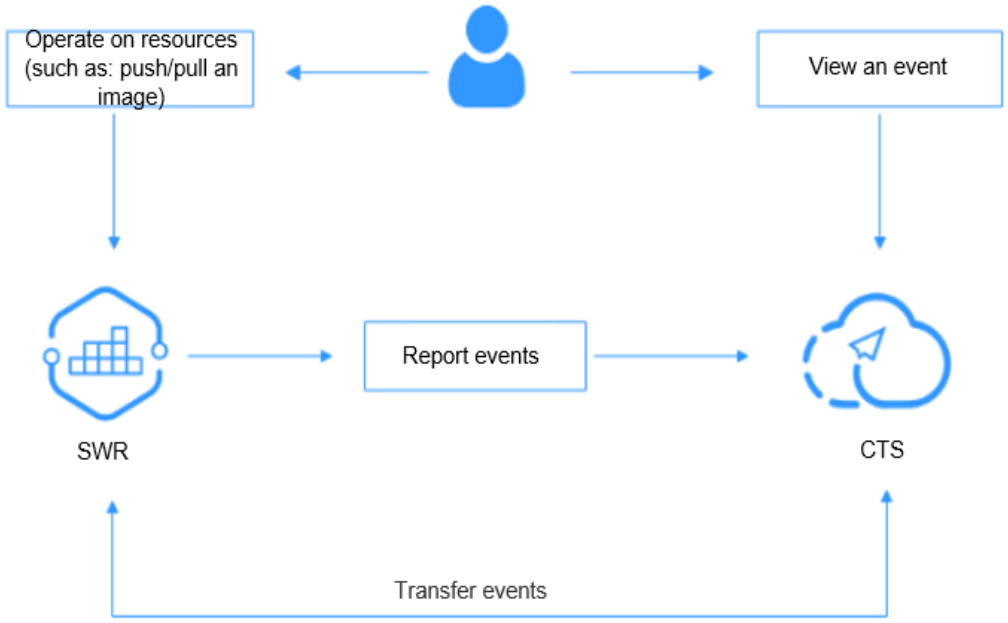
Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

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

Container images are like templates that include everything needed to run applications. When deploying containerized applications, you can use images from image centers and your private image registries. For example, a container image can contain a complete Ubuntu operating system, in which only the required programs and dependencies are installed. Container images are used to create containers. A container engine 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 container 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. Containers are created from images. Containers can be created, started, stopped, deleted, and suspended.

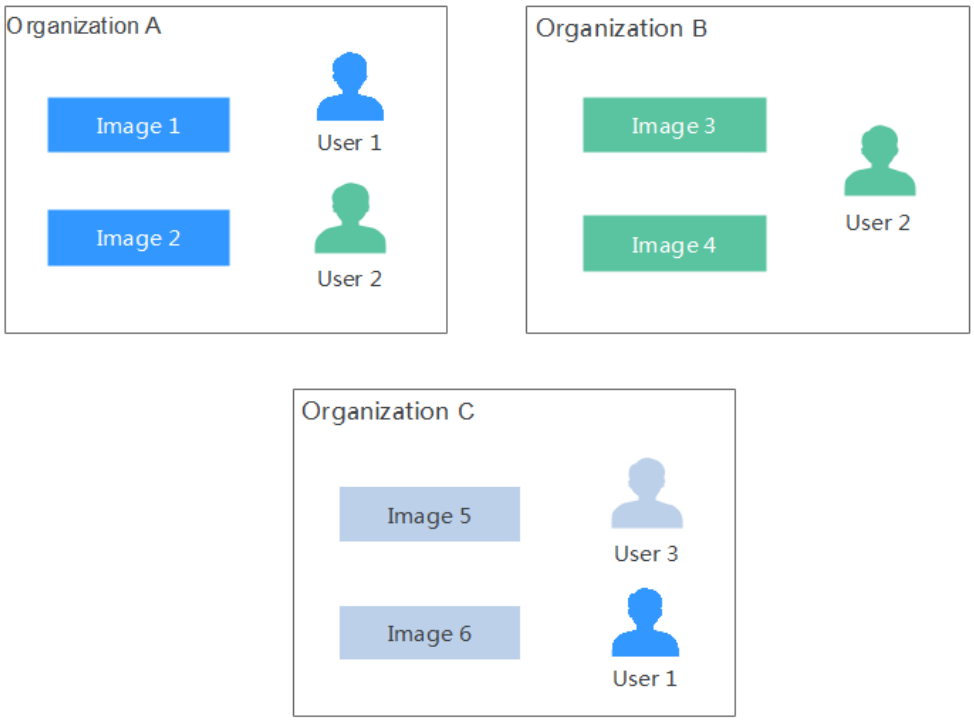
Repository

Image repositories are used for storing container 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 not on the number and size of images in an organization, but on the number of organizations a user can create, as shown in **Table 6-1**.

Table 6-1 Quotas

Resource Type	Quota
Organization	5

Requirements on Uploading Images

- If you run **docker push** to push images, the total number of image layers cannot exceed 20 at a time.
- If you run **docker push** to push images, 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 grant your enterprise personnel permission to access your SWR resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your Huawei Cloud resources.

With IAM, you can create IAM users and grant them permission to access only specific resources. For example, if you want some software developers in your enterprise to be able to use SWR resources but not be able to delete the resources or perform any other high-risk operations, you can create IAM users and grant permission to use SWR resources but not permission to delete them.

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

IAM is a free service. You only pay for the resources in your account.

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

SWR Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

SWR is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-1**) in the specified regions (for example, **CN-Hong Kong**), the users only have permissions for SWR resources in the selected projects. When accessing SWR, the users need to switch to the authorized region.

Table 7-1 System-defined permissions for SWR

Role/Policy Name	Description	Type
SWR Admin	Administrator permissions for SWR. Users with this role can perform all operations on SWR resources.	System-defined role

Role/Policy Name	Description	Type
Tenant Administrator	Administrator permissions for all services except IAM.	System-defined role
Tenant Guest	Read-only permissions for all services except IAM. For example, users with this role can pull images.	System-defined role
ServiceStage Developer	ServiceStage developer permissions. For example, users with this role can pull images.	System-defined role

NOTE

- You can **grant permissions** (read, write, and manage permissions), to different users for them to access either a specific image or images in a specific organization.
- In addition to the roles listed in the table, SWR has system-defined policies, such as SWR FullAccess, SWR OperateAccess, and SWR ReadOnlyAccess. However, the three policies are only available for SWR Enterprise Edition. Only users of SWR Enterprise Edition can be assigned with these policies.

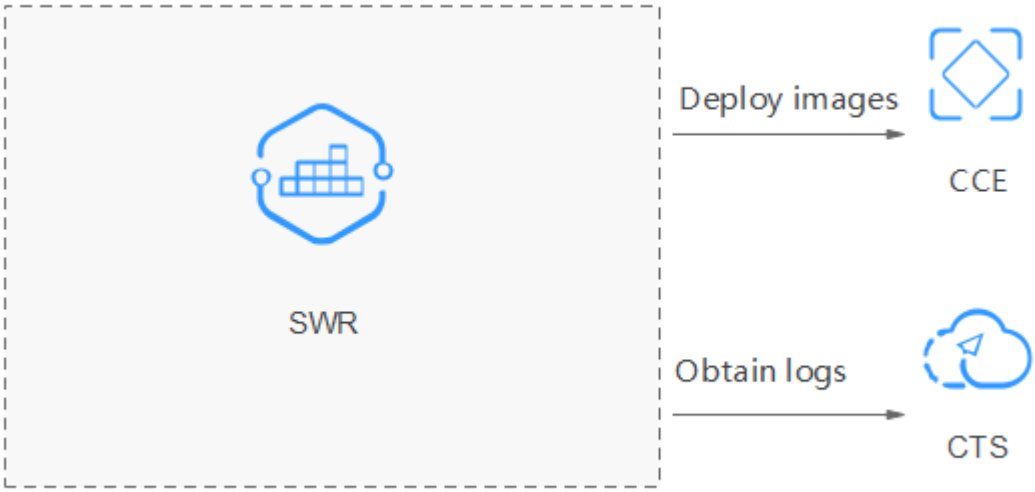
Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting SWR Permissions**.

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 and high-reliability service through which enterprises can manage containerized applications. It supports Kubernetes-native applications and tools, allowing you to easily set up a container runtime environment in 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. For details on the operations supported by CTS, see **Key Operations on SWR**.

A Change History

Date	Description
2022-11-07	This issue is the fifth official release. Added the following sections: **Shared Responsibilities** **Identity Authentication and Access Control** **Data Protection** **Audit and Logging**
2022-07-01	This issue is the fourth official release. Added the following section: SWR Quick Overview
2021-06-30	This issue is the third official release. Complemented the concept of image repository in **Basic Concepts**.
2018-07-30	This issue is the second official release. Added image pull acceleration to **Introduction**, **Advantages**, and **Application Scenarios**.
2018-03-02	This issue is the first official release.

