

容器镜像服务

产品介绍

文档版本 07
发布日期 2025-01-27



版权所有 © 华为技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 什么是容器镜像服务.....	1
2 产品优势.....	3
3 应用场景.....	4
4 安全.....	5
4.1 责任共担.....	5
4.2 身份认证与访问控制.....	6
4.2.1 身份的认证与管理.....	6
4.2.2 访问控制.....	7
4.3 数据保护技术.....	8
4.4 审计与日志.....	9
5 基本概念.....	11
6 约束与限制.....	13
7 权限管理.....	14
8 与其他云服务的关系.....	17

1 什么是容器镜像服务

产品简介

容器镜像服务（SoftWare Repository for Container，简称SWR）是一种支持镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助您快速部署容器化服务。

通过使用容器镜像服务，您无需自建和维护镜像仓库，即可享有云上的镜像安全托管及高效分发服务，并且可配合[云容器引擎 CCE](#)使用，获得容器上云的顺畅体验。

容器镜像服务共享版免费。

产品功能

- 镜像全生命周期管理
容器镜像服务支持镜像的全生命周期管理，包括镜像的上传、下载、删除等。
- 私有镜像仓库
容器镜像服务提供私有镜像库，并支持细粒度的权限管理，可以为不同用户分配相应的访问权限（读取、编辑、管理）。
- 镜像加速
容器镜像服务通过华为自主专利的镜像下载加速技术，使CCE集群下载镜像时在确保高并发下能获得更快的下载速度。
- 镜像仓库触发器
容器镜像服务支持容器镜像版本更新自动触发部署。您只需要为镜像设置一个触发器，通过触发器，可以在每次镜像版本更新时，自动更新使用该镜像部署的应用。

访问方式

华为云提供了Web化的服务管理平台（即管理控制台）和基于HTTPS请求的API（Application programming interface）管理方式。

- API方式
如果用户需要将容器镜像服务集成到第三方系统，用于二次开发，请使用API方式访问容器镜像服务。具体操作请参见《[容器镜像服务API参考](#)》。
- 管理控制台方式

其他相关操作，请使用管理控制台方式访问容器镜像服务。如果用户已在云平台注册，可直接登录管理控制台，从主页选择“容器镜像服务”。

如果未注册，请参考[注册账号](#)，进行账号注册。

2 产品优势

简单易用

- 无需自行搭建和运维，即可快速推送拉取容器镜像。
- 容器镜像服务的管理控制台简单易用，支持镜像的全生命周期管理。

安全可靠

- 容器镜像服务遵循HTTPS协议保障镜像安全传输，提供账号间、账号内多种安全隔离机制，确保用户数据访问的安全。
- 容器镜像服务依托华为专业存储服务，确保镜像存储更可靠。

镜像加速

- 容器镜像服务通过华为自主专利的镜像下载加速技术，使CCE集群下载时在确保高并发下能获得更快的下载速度。

3 应用场景

镜像生命周期管理

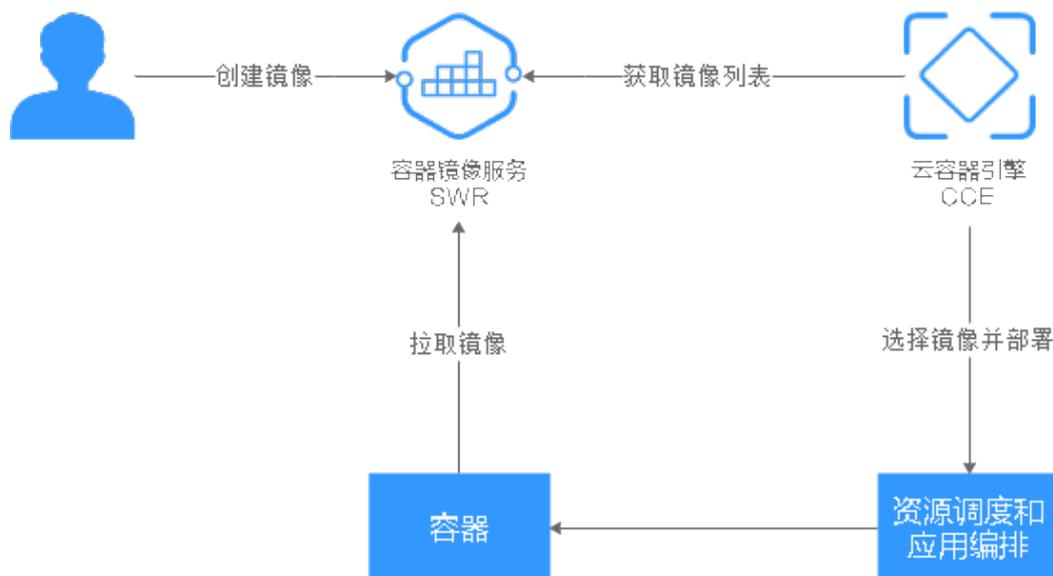
提供镜像构建、镜像上传、下载、同步、删除等完整的生命周期管理能力。

优势

- 镜像下载加速：华为自主专利的加速下载技术，提升华为云容器拉取镜像的速度。
- 高可靠的存储：依托华为OBS专业存储，确保镜像的存储可靠性高达11个9。
- 更安全的存储：细粒度的授权管理，让用户更精准的控制镜像访问权限。

建议搭配使用

云容器引擎CCE



4 安全

4.1 责任共担

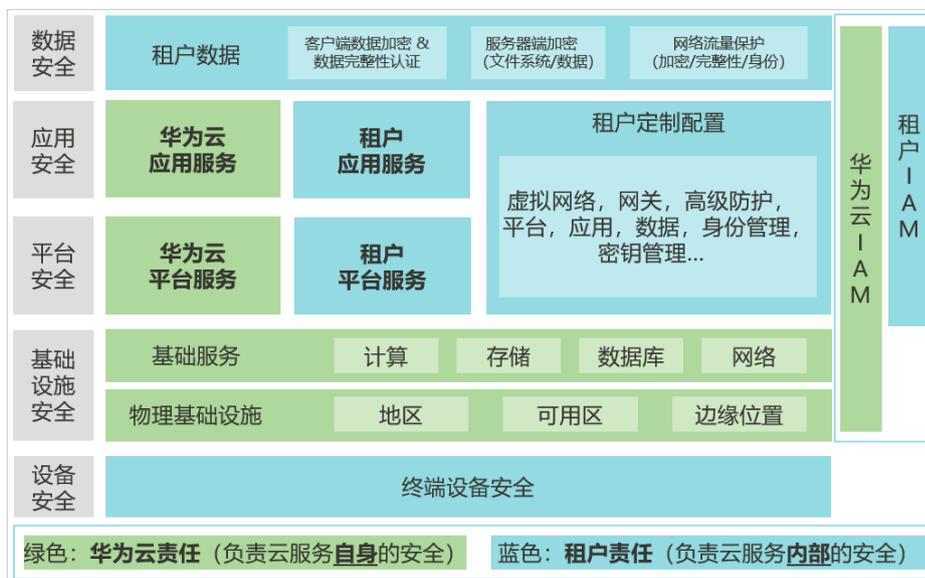
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如[图4-1](#)所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 4-1 华为云安全责任共担模型



4.2 身份认证与访问控制

4.2.1 身份的认证与管理

统一身份认证 (Identity and Access Management, 简称IAM) 是华为云提供权限管理的免费基础服务, 它可以帮助您安全地控制云服务和资源的访问权限。IAM 管理员控制谁可以通过身份验证 (登录) 和授权 (具有权限) 使用SWR资源。

使用身份进行身份验证

如果您想使用华为云上的服务和资源, 首先必须注册成为IAM用户。

账号

当您首次使用华为云时注册的账号, 该账号是您的华为云资源归属、资源使用计费的主体, 对其所拥有的资源及云服务具有完全的访问权限, 可以重置用户密码、分配用户权限等。账号统一接收所有IAM用户进行资源操作时产生的费用账单。

账号不能在IAM中修改和删除, 您可以在账号中心修改账号信息, 如果您需要删除账号, 可以在账号中心进行注销。

IAM 用户

IAM用户是由账号在IAM中创建的用户, 是云服务的使用人员, 具有独立的身份凭证 (密码和访问密钥), 根据账号授予的权限使用资源。IAM用户不进行独立的计费, 由所属账号统一付费。

用户组

用户组是用户的集合, IAM可以通过用户组功能实现用户的授权。您创建的IAM用户, 加入特定用户组后, 将具备对应用户组的权限。当某个用户加入多个用户组时, 此用户同时拥有多个用户组的权限, 即多个用户组权限的全集。

IAM角色

IAM 角色是华为云账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您还可以根据业务的需要，在不同角色中切换。

使用策略管理访问

您将创建策略并将其附加到华为云身份，以控制华为云中的访问。策略是华为云中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，华为云将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略存储为JSON 文档。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。

4.2.2 访问控制

访问方式

用户访问SWR的方式有多种，包括管理控制台、命令行工具、API、SDK，无论访问方式封装成何种形式，其本质都是通过SWR提供的REST风格的API接口进行请求。

SWR的接口既支持认证请求，也支持匿名请求。匿名请求通常仅用于需要公开访问的场景，例如静态网站托管。除此之外，绝大多数场景是需要经过认证的请求才可以访问成功。经过认证的请求总是需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子，结合请求体携带的特定信息计算而成。通过访问密钥（AK/SK）认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。关于访问密钥的详细介绍及获取方式，请参见[获取长期有效登录指令](#)。

控制策略

用户访问SWR，无论采用何种方式，都会受到SWR访问控制策略的制约。SWR目前支持以下几种控制策略：

表 4-1 表 1 SWR 访问控制方式

访问控制方式		简要说明	详细介绍
权限控制	IAM权限	IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予SWR所需的权限，用户加入到用户组后，该用户将拥有该用户组的所有权限。	IAM权限介绍
	镜像权限	镜像的权限指的是该镜像的读取、编辑、管理权限。除了在IAM中给用户授权外，SWR还支持管理员在镜像详情中为IAM用户添加或修改、删除权限。	在镜像详情中添加授权
	组织权限	组织用于隔离镜像仓库，每个组织可对应一个公司或部门，将其拥有的镜像集中在该组织下。在不同的组织下，可以有同名的镜像。同一IAM用户可属于不同的组织。	组织管理

4.3 数据保护技术

容器镜像服务通过多种数据保护手段和特性，保障存储数据的安全可靠。

表 4-2 容器镜像服务的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密 (HTTPS)	为保证数据传输的安全性, SWR仅支持传输更安全的HTTPS协议。	构造请求
镜像数据加密存储	SWR企业仓库支持使用系统托管的KMS密钥对镜像进行加密。SWR使用OBS进行镜像存储, 开启OBS桶加密功能, SWR可以在上传镜像时使用系统托管的KMS密钥自动进行数据加密, 以提高数据存储安全。	/
数据冗余存储	SWR用户元数据及镜像数据默认使用数据冗余存储, 存储在同区域的多个AZ中。当某个AZ不可用时, 仍然能够从其他AZ正常访问数据, 适用于对可靠性要求较高的数据存储场景。	/
数据完整性校验 (Sha256)	镜像在上传下载过程中, 有可能会因为网络劫持、数据缓存等原因, 存在数据不一致的问题。SWR提供通过计算Sha256值的方式对上传下载的数据进行一致性校验。	客户端上传镜像
跨区域复制	跨区域复制是指通过创建跨区域复制规则, 将源仓库的镜像自动、异步地复制到不同区域的另外一个仓库中。跨区域复制能够为用户提供跨区域数据容灾的能力, 满足用户数据复制到异地进行备份的需求。	自动同步镜像
镜像老化规则	您可以在单个镜像中保留多个版本的对象, 使您更方便地检索和还原各个版本, 在意外操作或服务故障时快速恢复数据。	镜像老化规则介绍和配置方法

4.4 审计与日志

审计

云审计服务 (Cloud Trace Service, CTS), 是华为云安全解决方案中专业的日志审计服务, 提供对各种云资源操作记录的收集、存储和查询功能, 可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

通过云审计服务, 您可以记录与容器镜像服务相关的操作事件, 便于日后的查询、审计和回溯。

CTS的详细介绍和开通配置方法, 请参见[CTS快速入门](#)。

CTS支持追踪SWR的操作列表, 请参见[支持云审计的关键操作](#)。

5 基本概念

镜像 (Image)

容器镜像是一个模板，是容器应用打包的标准格式，在部署容器化应用时可以指定镜像。例如一个容器镜像可以包含一个完整的Ubuntu操作系统环境，里面仅安装了用户需要的应用程序及其依赖文件。容器镜像用于创建容器。容器引擎 (Docker) 本身提供了一个简单的机制来创建新的镜像或者更新已有镜像，您也可以下载其他人已经创建好的镜像来使用。

容器 (Container)

一个通过容器镜像创建的运行实例，一个节点可运行多个容器。容器的实质是进程，但与直接在宿主机执行的进程不同，容器进程运行于属于自己的独立命名空间。

镜像 (Image) 和容器 (Container) 的关系，就像是面向对象程序设计中的类和实例一样，镜像是静态的定义，容器是镜像运行时的实体。容器可以被创建、启动、停止、删除、暂停等。

镜像仓库 (Repository)

镜像仓库 (Repository) 用于存放容器镜像。单个镜像仓库可对应单个具体的容器应用，并托管该应用的不同版本。

组织

组织用于隔离镜像仓库，每个组织可对应一个公司或部门，将其拥有的镜像集中在该组织下。同一用户可属于不同的组织。支持为账号下不同用户分配相应的访问权限 (读取、编辑、管理) 。

图 5-1 组织



6 约束与限制

配额

容器镜像服务对单个组织可承载的镜像数量及大小没有限制，只对单个用户可添加的组织数量限定了配额，如表6-1所示。

表 6-1 配额

资源类型	配额(单位/个)
组织	5

上传镜像限制

- 使用客户端上传镜像，单个租户同时上传镜像layer总数不大于20个。
- 使用客户端上传镜像，镜像的每个layer大小不能超过10G。
- 使用页面上传镜像，每次最多上传10个文件，单个文件大小（含解压后）不得超过2G。

7 权限管理

如果您需要对华为云上购买的容器镜像服务（SWR）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有容器镜像服务（SWR）的使用权限，但是不希望他们拥有删除SWR等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用SWR，但是不允许删除SWR的权限，控制他们对SWR资源的使用范围。

如果华为云账号已经能满足您的使用要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用SWR服务的其他功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见[IAM产品介绍](#)

SWR 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

SWR部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如中国-香港）对应的项目（ap-southeast-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问SWR时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业

对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

SWR目前有共享版和企业版两个版本，SWR共享版的权限如下：

如表1和表2所示，包括了SWR共享版的所有系统策略和系统角色。

表 7-1 SWR 系统策略（推荐）

名称	描述	类型
SWR FullAccess	容器镜像仓库所有权限	系统策略
SWR OperateAccess	容器镜像仓库操作权限	系统策略
SWR ReadOnlyAccess	容器镜像仓库只读权限	系统策略

表 7-2 SWR 系统角色

名称	描述	类型
SWR Admin	容器镜像服务的管理员权限，拥有该服务下的所有权限。	系统角色
Tenant Administrator	除IAM服务外，其他所有服务的管理员权限，拥有容器镜像服务下的所有权限。	系统角色
ServiceStage Developer	应用管理与运维平台（ServiceStage）开发者，拥有容器镜像服务下载镜像等权限。	系统角色

下表列出了SWR常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 7-3 SWR 常用操作与系统权限关系

操作	SWR FullAccess	SWR OperateAccess	SWR ReadOnlyAccess	SWR Admin	Tenant Administrator
上传/推送镜像	√	√	x	√	√
下载/拉取镜像	√	√	√	√	√
添加触发器	√	√	x	√	√
编辑镜像属性	√	√	x	√	√
共享镜像	√	√	x	√	√
添加授权	√	√	x	√	√

操作	SWR FullAccess	SWR OperateAccess	SWR ReadOnlyAccess	SWR Admin	Tenant Administrator
删除镜像或版本	√	√	x	√	√
镜像同步	√	√	x	√	√
创建组织	√	√	x	√	√
删除组织	√	√	x	√	√

📖 说明

在容器镜像服务中进行[授权管理](#)，可以添加对某个镜像或组织中所有镜像的读取、编辑或管理权限。

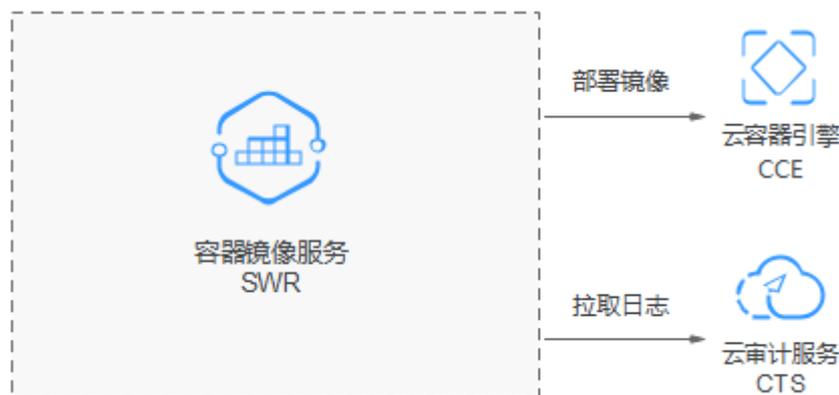
相关链接

- [IAM产品介绍](#)
- 创建用户组、用户并授予SWR权限请参考：[创建用户并授权使用SWR](#)。

8 与其他云服务的关系

容器镜像服务需要与其他云服务协同工作，容器镜像服务和其他云服务的关系如图 8-1。

图 8-1 容器镜像服务和其他云服务的关系



- 云容器引擎
云容器引擎（Cloud Container Engine，简称CCE）提供高可靠高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。
容器镜像服务能无缝对接CCE，您可以将容器镜像服务中的镜像部署到CCE中。
- 云审计服务
云审计服务（Cloud Trace Service，简称CTS）为您提供云服务资源的操作记录，记录内容包括您从公有云管理控制台或者开放API发起的的云服务资源操作请求以及每次请求的结果，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。
通过CTS，您可以记录与容器镜像服务相关的操作事件，便于日后的查询、审计和回溯。CTS支持的SWR操作列表参见[容器镜像服务的关键操作列表](#)。