

容器镜像服务(企业版)
23.12.0

用户指南

文档版本 01
发布日期 2023-12-30



版权所有 © 华为云计算技术有限公司 2024。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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 管理仓库	1
1.1 购买仓库	1
1.2 删除仓库	3
1.3 标签管理	4
1.3.1 标签概述	4
1.3.2 新增仓库标签	6
1.3.3 删除仓库标签	8
1.3.4 修改仓库标签	9
1.3.5 通过标签查找仓库	10
1.3.6 命名空间标签管理	10
2 镜像管理	13
2.1 镜像仓库	13
2.2 Helm Chart 仓库	16
3 命名空间	18
4 访问管理	20
4.1 访问凭证	20
4.2 访问控制	21
4.2.1 访问控制概述	22
4.2.2 公网访问	22
4.2.3 内网访问	24
4.3 域名管理	25
5 镜像签名与验签	29
5.1 镜像签名	29
5.2 镜像验签	33
6 镜像同步	36
6.1 目标仓库	36
6.2 同步规则	38
6.3 镜像同步	45
7 运维中心	46
7.1 镜像老化	46
7.2 触发器	52

7.3 镜像版本不可变.....	55
------------------	----

1 管理仓库

1.1 购买仓库

操作场景

使用容器镜像服务企业仓库前，您首先需要购买仓库。企业仓库提供企业级的云原生制品安全托管服务，提供容器镜像等符合OCI规范的云原生制品托管。

注意

仓库支持访问控制，新创建的仓库默认阻断全部访问来源，请参考[访问控制](#)开通访问控制，避免无法正常访问仓库。

前提条件

- 已开通容器镜像服务所依赖的云服务：虚拟私有云 VPC、对象存储 OBS、密钥管理服务 KMS、VPC终端节点 VPCEP。
- 已为容器镜像服务企业版授权您的虚拟私有云、对象存储等资源权限。

操作步骤

- 步骤1** 登录容器镜像服务控制台。
- 步骤2** 在页面左上角切换Region到您所在的Region。单击左侧菜单栏的“企业版”进入企业版页面。
- 步骤3** 单击页面右上角“创建仓库”，进入购买界面。输入以下参数，具体参数含义如下：

< 容器镜像服务企业版

* 计费模式 按需计费

* 所属项目 华北-乌兰察布-二零三

* 实例名称 请输入名称

* 套餐规格

基础版	企业版
<ul style="list-style-type: none"> ✓ 免费镜像存储: 500GB ✓ 免费镜像传输: 100GB ✓ 并发上传镜像层数: 40 ✓ 并发下载镜像层数: 500 	<ul style="list-style-type: none"> ✓ 免费镜像存储: 1TB ✓ 免费镜像传输: 100GB ✓ 并发上传镜像层数: 60 ✓ 并发下载镜像层数: 1000

* 虚拟私有云 vpc-lyy(192.168.0.0/24) 创建虚拟私有云

* 子网 subnet-lyyyy(192.168.0.0/29) 创建子网

OBS桶加密
上传对象时自动进行加密, 提高数据存储安全。但是会影响仓库性能, 请慎选。

国密加密
使用国密算法进行加密, 提高数据存储安全。

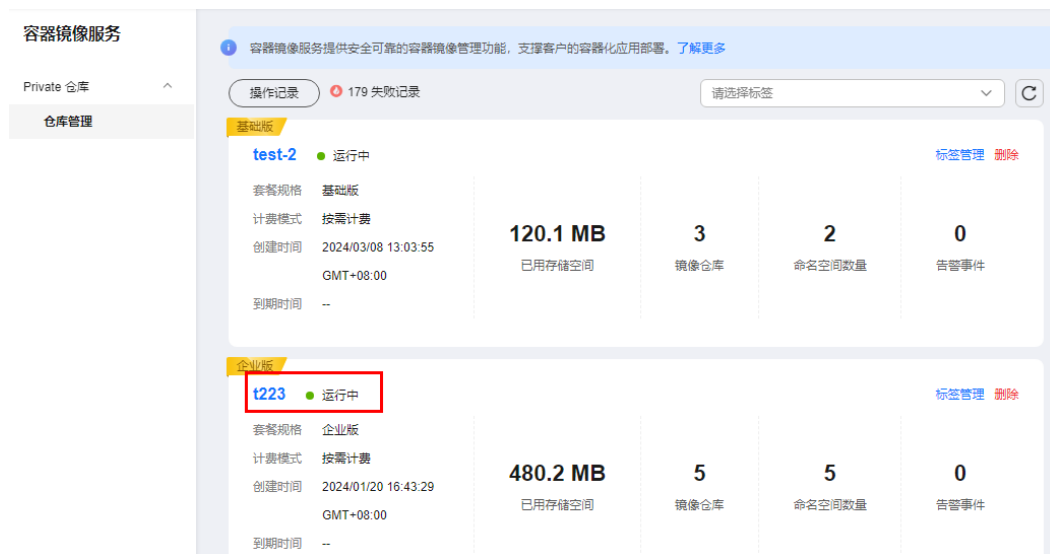
标签 +

- **计费模式**: 当前仅支持按需计费模式。
- **所属项目**: 选择仓库所在区域或项目。仓库购买后区域或项目将无法更改, 请根据容器集群所在地进行选择。
- **仓库名称**: 输入仓库名称。该名称将直接应用于该仓库的访问地址, 购买后不可修改, 请谨慎填写。
- **套餐规格**: 选择仓库规格。不同仓库规格具有不同的功能及配额, 请参考界面上的规格对比进行选择。
- **虚拟私有云**: 选择仓库所在虚拟私有云。如果没有选项可参见[创建虚拟私有云和子网](#)创建。
- **子网**: 选择仓库所在子网。
- **OBS桶加密**: 仓库购买后默认在您账号下创建OBS桶, 用来托管容器镜像。开启OBS桶加密后, 上传对象时自动进行加密, 以提高数据存储安全。但同时会影响仓库性能, 请您谨慎选择。
- **国密加密**: 仓库支持国密算法加密, 保证数据存储安全。开启此功能后, 镜像上传、镜像签名及登录口令均启用国密加密算法。当前支持的国密算法详见[表5-1](#)。
- **标签**: 标签是对云上资源的一种标识。关于标签的详细介绍请参考[标签管理](#)
- **描述**: 输入仓库的描述。

步骤4 单击右下角“立即购买”。

步骤5 返回仓库管理, 查看创建进度。当仓库状态为“运行中”时, 表示当前仓库已处于可用状态。

图 1-1 仓库管理



说明

若仓库一直处于“创建中”，或者从列表中消失，请单击列表左上方的“操作记录”查看失败原因。若无法定位，您可[新建工单](#)联系我们。

---结束

1.2 删除仓库

仓库创建后，用户也可以对它进行删除操作。

操作步骤

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏里的“企业版”。
- 步骤2** 在页面左上角切换Region到您所在的Region。
- 步骤3** 单击您要删除的仓库后面的“删除”按钮。您可以根据需要，选择是否勾选“删除仓库关联的OBS桶”和“删除仓库关联的DNS”。

删除实例

您确定要删除以下实例吗？删除操作无法恢复，请谨慎操作

实例名称	创建时间
t223	2024/01/20 16:43:29 GMT+08:00

- 资源释放 删除实例关联的OBS桶
- 删除实例关联的DNS

* 注：删除中时请勿关闭当前弹窗或刷新页面，删除完成后弹框会自动关闭，否则可能导致部分资源残留

否 是

步骤4 单击“确认”按钮，完成删除。

----结束

注意

- 仓库一旦删除，便无法恢复，请谨慎操作。
- 删除中时请勿关闭当前弹窗或刷新页面，删除完成后弹框会自动关闭，否则可能导致部分资源残留。

1.3 标签管理

1.3.1 标签概述

什么是标签？

标签是对云上资源的一种可视化的标识。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

图 1-2 标签示例 1

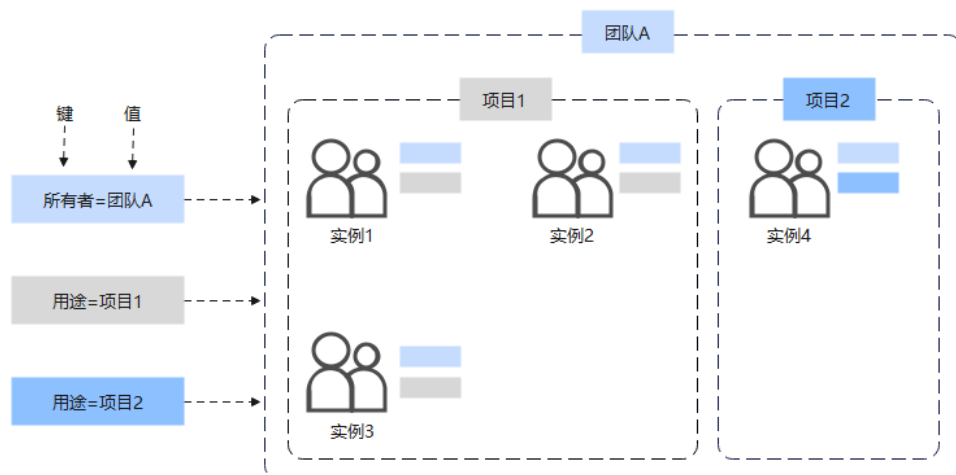


图 1-3 标签示例 2

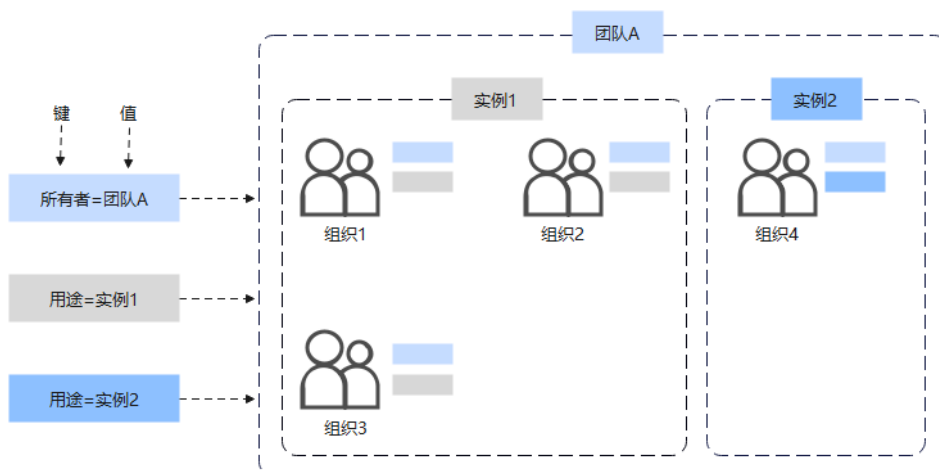


图1 图2说明了标签的工作方式。在此示例中，您为每个仓库分配了两个标签，每个标签都包含您定义的一个“键”和一个“值”，一个标签使用键为“所有者”，另一个使用键为“用途”，每个标签都拥有相关的值。

在容器镜像服务中，您可以使用标签对企业仓库中的仓库/命名空间进行标识，以便于对其进行快速查找和管理。

标签的使用场景

当您在容器镜像服务中使用时，若存在以下需求，建议您使用标签来快速完成任务：

- **资源集中处理**
对于拥有大量云资源的用户，可以通过使用标签，快速查找标识有某标签的所有云资源，可对这些资源统一进行检视、修改、删除等操作。
- **资源迁移**
资源迁移过程中，用户可以将迁移资源与预定义标签关联，避免大量重复建立标签过程中产生的错误率与效率低下的问题。
- **自定义计费**
您可以在计费系统中查询已打标签的仓库，从而快速对账单进行精细化的统计和分析。

标签命名规则

每个标签都是由一个键值对构成。对于每个资源，每个标签“键”都必须是唯一的，每个标签“键”只能有一个“值”。如果您添加的标签的“值”与该资源上现有标签的“值”相同，新值将覆盖旧值。具体填写规则如下：

表 1-1 键和值填写说明

填写参数	规则	示例
键	<ul style="list-style-type: none"> 不能为空 不能以_sys_开头 键的长度为1~128个字符（中文也可以输入128个字符） 可以由英文字母、数字、下划线、中划线、中文字符组成 可用 UTF-8 格式表示的字母(包含中文)、数字和空格，以及以下字符：_ . : = + - @ 	Test Department
值	<ul style="list-style-type: none"> 资源标签值可以为空 预定义标签值不可以为空 值的长度为0~255个字符（中文也可以输入255个字符） 可以由英文字母、数字、下划线、中划线、中文字符组成 可用 UTF-8 格式表示的字母(包含中文)、数字和空格，以及以下字符：_ . : / = + - @ 	Shanghai

1.3.2 新增仓库标签

约束与限制

表 1-2 单个仓库最多可添加的标签数量

资源类型	配额
单个仓库的标签数量	20个

购买仓库时添加标签

步骤1 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，单击右上角“创建仓库”。

- 步骤2** 进入仓库购买页面，单击 **+** 添加标签，请按照**标签命名规则**，在标签输入框设置标签的“键”和“值”。
- 步骤3** 单击“立即购买”。
- 步骤4** 系统自动进入仓库管理页，购买的仓库页签已显示刚刚添加的标签。

图 1-4 已购买的仓库

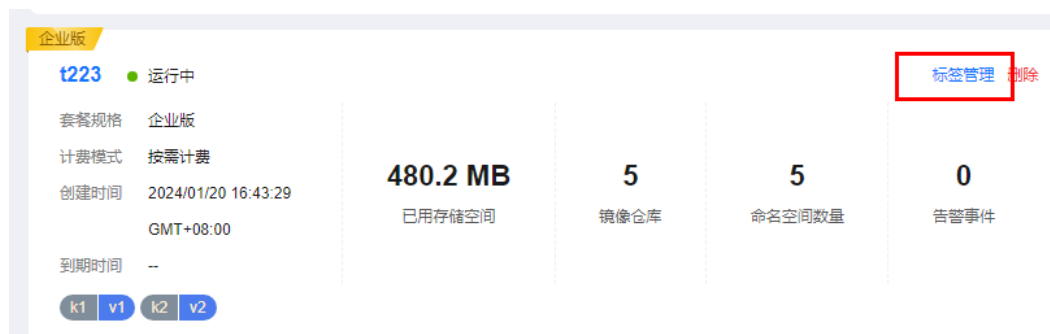


----结束

购买后给仓库添加标签

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 在仓库管理页，选中要添加标签的仓库，单击该仓库右上角“标签管理”。

图 1-5 购买仓库后添加标签



- 步骤3** 在标签管理页，单击 **+** ，在标签输入框设置标签的“键”和“值”，即可添加一个标签。

图 1-6 添加标签



----结束

1.3.3 删除仓库标签

删除标签可在容器镜像服务完成，也可以登录进入标签管理服务控制台进行操作，具体操作方式有3种：

- [在容器镜像服务删除标签](#)
- [批量删除标签](#)

在容器镜像服务删除标签

步骤1 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。

步骤2 在仓库管理页，选中要删除标签的仓库，单击该仓库右上角“标签管理”。

步骤3 进入标签管理页，在要删除的标签的右侧，单击“删除”。

----结束

在标签管理服务批量删除标签

步骤1 登录标签管理服务控制台。

步骤2 在“资源标签->资源配置标签”页面，“区域”勾选资源所在的区域，“资源类型”请选择SWR，单击“搜索”。搜索结果将展示SWR在所选区域下所有资源。

步骤3 勾选待删除标签的资源，单击列表上方的“管理标签”，进入管理标签页面。


图 1-7 标签搜索结果



步骤4 单击待删除标签所在行的“删除”，单击“确认”，资源标签删除完成。

图 1-8 管理标签



步骤5 （可选）单击搜索结果区域右侧刷新按钮 。

资源标签列表刷新为最新状态，并更新列表刷新时间。

----结束

1.3.4 修改仓库标签

修改标签可在容器镜像服务完成，也可以登录进入标签管理服务控制台进行操作，具体操作方式有3种：

[在容器镜像服务修改](#)

[批量修改标签](#)

在容器镜像服务修改

步骤1 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。

步骤2 在仓库管理页，选中要修改标签的仓库，单击该仓库右上角“标签管理”。

步骤3 进入标签管理页，选中要修改的标签，重新输入“键”和“值”。

----结束

批量修改标签

步骤1 登录标签管理服务控制台。

步骤2 在“资源标签->资源配置标签”页面，“区域”勾选资源所在的区域，“资源类型”请选择SWR，单击“搜索”。搜索结果将展示SWR在所选区域下所有资源。

步骤3 勾选待修改标签的云资源，单击列表上方的“管理标签”，进入管理标签页面。

步骤4 在“新值”区域，设置标签的新值，单击“确定”。

----结束

1.3.5 通过标签查找仓库

当您所管理的各种资源已添加标签后，您可以通过标签来对资源进行快速检索，具体方式有2种：

[在容器镜像服务中查找](#)

[在标签管理服务中查找](#)

在容器镜像服务查找仓库

步骤1 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。

步骤2 在仓库管理页，从下拉复选框选中要查找的标签（可多选），即可筛选出标识该标签的仓库。

----结束

在标签管理服务中查找

步骤1 登录标签管理服务控制台。

步骤2 在“资源标签”页面，勾选资源所在的区域，“资源类型”请选择SWR，单击“搜索”。搜索结果将展示SWR在所选区域下所有资源。

----结束

1.3.6 命名空间标签管理

操作场景

命名空间用于管理多个具有关联属性的镜像，不直接存储容器镜像，可对应企业内部的一个产品项目或部门。当公司部门繁多时，我们可以通过添加命名空间标签，方便后续通过标签对命名空间进行查找及管理。

前提条件

[命名空间已创建](#)

约束与限制

表 1-3 单个命名空间最多可添加的标签数量

资源类型	配额
单个命名空间的标签数量	20个

添加命名空间标签


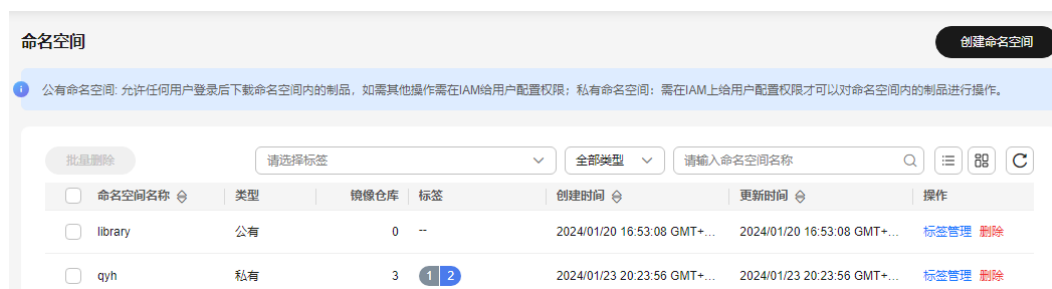
- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 选中要添加命名空间标签的仓库，单击仓库名称，进入仓库详情页。
- 步骤3** 单击仓库详情页左侧导航栏“命名空间”，进入命名空间列表页。单击页面右上角的  图标，以列表形式展示命名空间列表。
- 步骤4** 选择要添加标签的命名空间，单击右侧“标签管理”，进入标签管理页面。

图 1-9 命名空间管理列表页




- 步骤5** 在标签管理页面，单击 ，新增一个标签。

图 1-10 标签管理



- 步骤6** 参考标签命名规则，填写标签的键和值。

----结束

修改命名空间标签

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 选中命名空间所在仓库，单击仓库名称，进入仓库详情页。
- 步骤3** 单击仓库详情页左侧导航栏“命名空间”，进入命名空间列表页。
- 步骤4** 选择要修改标签的命名空间，单击右侧“标签管理”，进入标签管理页面。
- 步骤5** 重新输入单个或多个键或值。
----结束

删除指定命名空间标签

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 选中命名空间所在仓库，单击仓库名称，进入仓库详情页。
- 步骤3** 单击仓库详情页左侧导航栏“命名空间”，进入命名空间列表页。
- 步骤4** 选择要删除标签的命名空间，单击右侧“标签管理”，进入标签管理页面。
- 步骤5** 单击命名空间标签右侧“删除”按钮。
----结束

通过标签查找命名空间

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 选中命名空间所在仓库，单击仓库名称，进入仓库详情页。
- 步骤3** 单击仓库详情页左侧导航栏“命名空间”，进入命名空间列表页。
- 步骤4** 配置1项或多项筛选条件。搜索结果即展示在下方列表中。
----结束

2 镜像管理

2.1 镜像仓库

操作场景

镜像仓库直接管理容器镜像，您可以上传镜像、下载镜像，查看镜像构建历史。

前提条件

使用镜像仓库前，您需要完成如下工作：

- 已经[购买仓库](#)。
- 已经设置了仓库的访问权限，具体请参见[访问控制概述](#)。
- 已经[创建访问凭证](#)。

上传镜像

步骤1 准备一台计算机，需满足如下要求：

- 安装的容器引擎版本必须为1.11.2及以上。
- 这台计算机已在[访问控制](#)中定义的公网或内网允许访问范围内。

步骤2 以root用户登录这台计算机。

步骤3 使用[访问凭证](#)创建的访问凭证获取的镜像访问凭证登录镜像仓库。

登录成功会显示“Login Succeeded”。

步骤4 执行以下命令为镜像打标签。

```
docker tag [镜像名称1:版本名称1] [镜像仓库地址]/[命名空间名称]/[镜像名称2:版本名称2]
```

其中：

- **[镜像名称1:版本名称1]**请替换为您所要上传的实际镜像的名称和版本名称。
- **[镜像仓库地址]**为仓库的访问地址，获取方式如下：

登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面，在“总览”页面获取访问地址，如图2-1所示。

图 2-1 访问地址



- [命名空间名称]请替换为您在[创建命名空间](#)中创建的命名空间。
- [镜像名称2:版本名称2]请替换为您期待的镜像名称和版本名称。

样例如下：

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

步骤5 上传镜像至镜像仓库。

```
docker push [镜像仓库地址]/[命名空间名称]/[镜像名称:版本名称]
```

样例如下：

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

终端显示如下信息，表明上传镜像成功。

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

在仓库详情页面“镜像管理”中可查看到对应的镜像信息。

📖 说明

镜像上传以后，您可以在CCE控制台创建工作负载。

----**结束**

查看镜像下载地址

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”。
- 步骤2** 在左侧导航栏选择“镜像管理”。
- 步骤3** 单击镜像名称进入镜像详情。
- 步骤4** 在对应镜像版本“下载指令”一列可以获取镜像下载指令，如图2-2所示。

图 2-2 下载指令



---结束

镜像仓库其他操作

- **搜索镜像**
支持根据命名空间和镜像名称搜索镜像。

图 2-3 搜索镜像



- **删除镜像**
单击镜像所在行的“删除”即可删除镜像。为避免您误删重要数据，删除镜像时需要输入DELETE进行二次确认。



删除镜像会同时删除镜像下的所有版本，请谨慎操作。

- **删除镜像版本**
单击镜像名称进入镜像详情，在镜像版本所在行单击“删除”即可删除镜像版本。为避免您误删重要数据，删除镜像版本时需要输入DELETE进行二次确认。

后续操作

镜像上传到镜像仓库后，您还可以对镜像进行一系列的操作，包括：

- 配置镜像签名规则，根据规则自动对镜像签名。具体请参见[镜像签名](#)。
- 配置镜像同步规则，根据规则与目标仓库自动同步镜像。具体请参见[镜像同步](#)。

- 配置镜像老化规则，根据规则自动清理不需要的镜像。具体请参见[镜像老化](#)。

2.2 Helm Chart 仓库

操作场景

容器镜像服务企业版支持托管[Helm Chart](#)。您可以在同一个命名空间内同时管理容器镜像和Helm Chart，实现在业务项目内同时使用容器镜像和Helm Chart。

背景信息

Kubernetes提供了统一模式的API，能以YAML格式的文件定义Kubernetes集群中的资源，包括Pod、Service、Deployment、StatefulSet、Job等等。这些资源种类繁多，且分散的kubernetes应用配置文件难以管理、编辑和更新，因此云原生社区衍生了一个更高维度的概念及其实现工具，即Chart和Helm。

- Chart是描述相关的一组Kubernetes集群内资源的文件集合。
- Helm是一个命令行程程序，用于管理这些Chart，以及其运行态Release。

容器镜像服务企业版支持Helm客户端实现Chart的上传和下载。

使用 Helm 客户端上传及下载 Helm Chart

安装Helm客户端

本文以在Linux操作系统的节点上安装为例，如在其他平台安装请下载对应安装包。

- 步骤1** 依次执行以下命令，下载并安装Helm客户端。关于安装Helm的更多信息，请参见[Installing Helm](#)。

```
curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3
```

```
chmod 700 get_helm.sh
```

```
./get_helm.sh
```

📖 说明

“get_helm.sh”脚本会自动拉取最新的Helm版本进行安装，如需安装其他版本，请从官方下载需要的[Helm版本](#)。

----结束

推送Helm Chart

- 步骤1** 安装Helm Push插件。

📖 说明

在安装Helm Push插件前，需要预先安装Git。

```
helm plugin install https://github.com/chartmuseum/helm-push
```

- 步骤2** 在节点上执行如下命令，创建一个Chart。

```
helm create [Chart名称]
```

示例: **helm create chart-demo**

步骤3 执行如下命令, 推送指定目录至Chart仓库。

helm push [Chart名称] [本地仓库名称]

示例:

```
helm push chart-demo group
```

您还可以将Chart文件打包为tgz压缩包, 然后直接上传。

helm push [Chart名称]-[Chart版本].tgz [本地仓库名称]

示例:

```
tar zcvf chart-demo-1.0.0.tgz chart-demo/ # 压缩Chart文件  
helm push chart-demo-1.0.0.tgz group # 上传Chart压缩包
```

----结束

下载Helm Chart

步骤1 在节点上执行如下命令, 更新本地仓库Chart信息。

helm repo update

步骤2 下载指定版本Chart。

helm pull [本地仓库名称]/[Chart名称] --version [Chart版本]

示例:

```
helm pull group/chart-demo --version 1.0.0
```

----结束

3 命名空间

操作场景

命名空间用于管理多个具有关联属性的镜像，不直接存储容器镜像，可对应企业内部的一个产品项目或部门。

📖 说明

仓库创建成功后，默认会创建一个名为“library”的公有命名空间。

创建命名空间

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏的“企业版”，在“仓库管理”页面单击您的仓库名称进入仓库。
- 步骤2** 在左侧导航栏单击“命名空间”。
- 步骤3** 在右上角单击“创建命名空间”。
- 步骤4** 填写命名空间名称，选择命名空间类型。

图 3-1 创建命名空间

创建命名空间

命名空间名称

命名空间类型 私有 公有

取消 确定

- 公有命名空间：允许任何用户登录后下载命名空间内的制品，如需其他操作需在IAM上为用户授权。
- 私有命名空间：需在IAM上为用户授权才可以对命名空间内的制品进行操作。

步骤5 单击“确定”。

命名空间创建成功后，您可以选择列表视图或卡片视图查看命名空间详情，在右上角

单击  或  图标进行视图切换。

----结束

删除命名空间


- 列表视图：选择需要删除的命名空间，单击操作列的“删除”，在弹出的对话框中输入“DELETE”，单击“确定”。
- 卡片视图：选择需要删除的命名空间，单击  图标，在弹出的对话框中输入“DELETE”，单击“确定”。

图 3-2 删除命名空间



说明

为避免你删除重要数据，命名空间下有镜像的命名空间无法删除，需要先删除掉镜像，才能删除命名空间

4 访问管理

4.1 访问凭证

操作场景

镜像仓库需要使用访问凭证才能访问。访问凭证分为长期凭证和临时凭证：

- 长期凭证：生成后永久有效，支持禁用及删除。长期凭证可应用在前期测试、CICD流水线及容器集群拉取镜像等场景中。

注意

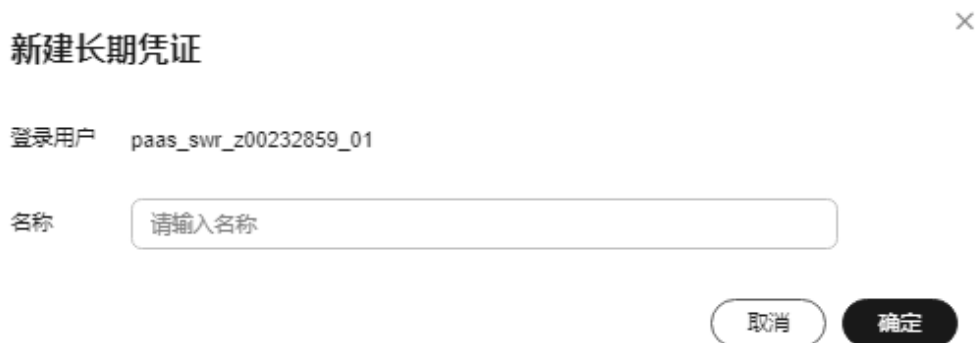
长期凭证没有时效限制，生成后请妥善保管，如果遗失请及时禁用或删除。

- 临时凭证：24小时内有效，生成后无法禁用及吊销。临时凭证可应用在临时使用，对外单次授权等场景中，对安全性要求较高的生产集群也可通过定时刷新的方式进行使用。

创建长期凭证

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏的“企业版”，在“仓库管理”页面单击您的仓库名称进入。
- 步骤2** 在左侧导航栏选择“访问管理 > 访问凭证”。
- 步骤3** 选择“长期凭证”页签，单击“新建长期凭证”。
- 步骤4** 在弹出的窗口中填写凭证名称，如[图4-1](#)所示。

图 4-1 新建长期凭证



步骤5 单击“确定”。

单击确定后会自动下载一个“长期凭证名称.csv”文件。

镜像访问凭证是docker命令，用于访问镜像仓库，镜像仓库的使用详细说明请参见[镜像仓库](#)。

----结束

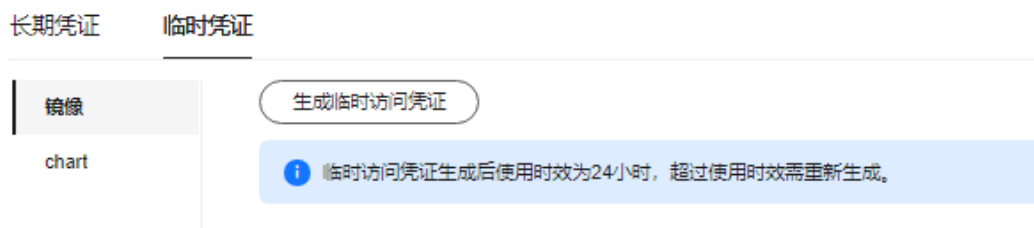
创建临时凭证

步骤1 登录容器镜像服务控制台，单击左侧菜单栏的“企业版”。

步骤2 在左侧导航栏选择“访问管理 > 访问凭证”。选择“临时凭证”页签。

步骤3 选择“镜像”或“chart”，单击“生成临时访问凭证”，如[图4-2](#)所示。

图 4-2 生成临时访问凭证



临时凭证会直接显示在页面上，您可以复制后使用。

镜像访问凭证是docker命令，用于访问镜像仓库，镜像仓库的使用详细说明请参见[镜像仓库](#)。

----结束

后续操作

- [镜像仓库](#)

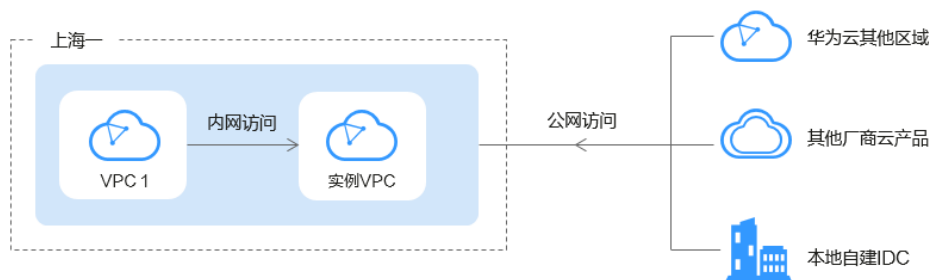
4.2 访问控制

4.2.1 访问控制概述

容器镜像服务企业版支持访问控制，新创建的仓库默认阻断全部访问来源，以确保您的镜像仓库内的数据安全。您可以根据业务需要配置访问控制策略，以最小范围放通业务客户端访问仓库。

仓库支持从公网访问和从华为云内网访问，并能分别控制公网和内网访问权限。

图 4-3 仓库访问示意图



- 公网访问：仓库支持从公网访问，通过白名单策略控制哪些公网IP网段可以访问仓库。
- 内网访问：仓库支持从所在区域的内部网络的任一VPC中访问，如仓库在“上海一”区域，则可从上海一的任一VPC中访问仓库。

每个仓库所在VPC默认能访问仓库，您可以在内网访问页面看到一条默认的内网访问规则。

详情请参见：

- [公网访问](#)
- [内网访问](#)

约束与限制

IAM用户使用访问控制功能时，需要拥有“VPC ReadOnlyAccess”权限，从而能够获取到VPC的子网列表。请使用账号登录IAM为IAM用户授权。

4.2.2 公网访问

操作场景

容器镜像服务企业版支持公网访问，可基于白名单策略限制来自公网环境的客户端对仓库的访问，保障仓库内的数据安全。新创建的仓库默认不开启公网访问入口。

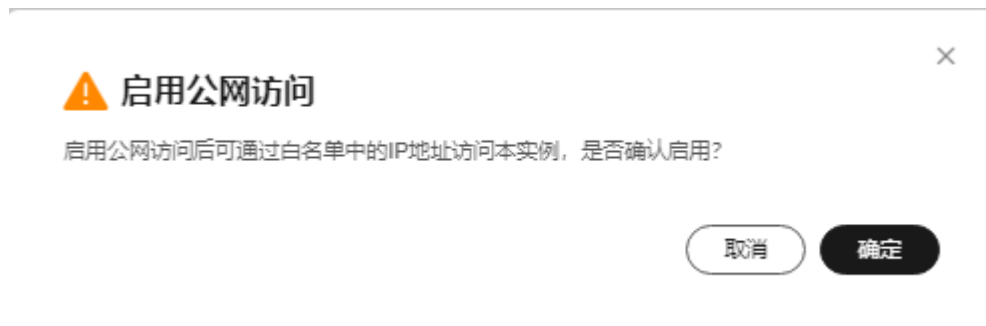
本文档介绍如何为仓库配置公网访问。

操作步骤

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏里的“企业版”，在“仓库管理”页面单击您的仓库名称进入。
- 步骤2** 在左侧导航栏选择“访问管理 > 访问控制”。

步骤3 选择“公网访问”页签，单击“启用公网访问”。阅读弹窗中的提示信息，并单击“确定”。

图 4-4 启用公网访问



步骤4 单击右上角“创建公网访问”，在弹出的窗口中填写白名单IP网段，如图4-5所示。如果一次需要添加多个网段，可单击+进行添加。

图 4-5 添加白名单



📖 说明

【注意】公网白名单，建议以单IP的形式增加放通白名单，减少网段放通过大，增加被攻击的风险。

步骤5 单击“确定”，该白名单IP添加成功并生效。

📖 说明

如需修改该白名单信息，可删除后再次新建。

----结束

后续操作

创建公网访问后，您还需要创建访问凭证，才可以访问仓库。访问凭证的获取方法请参见[访问凭证](#)。

4.2.3 内网访问

操作场景

容器镜像服务企业版支持内网访问，可基于内网访问链路限制私有网络内的客户端访问仓库。

本文档介绍如何为仓库配置内网访问。完成以下配置后，您可使用指定VPC内的云服务器通过内网拉取仓库中的镜像。

📖 说明

每个仓库所在VPC默认能访问仓库，您可以在内网访问页面看到一条默认的内网访问规则。

操作步骤

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”进入，在“仓库管理”页面单击您的仓库名称进入。
- 步骤2** 在左侧导航栏选择“访问管理 > 访问控制”。
- 步骤3** 选择“内网访问”页签，单击右上角“创建内网访问”。
- 步骤4** 在弹出的窗口中选择所属项目、内网IP所属VPC和子网，如[图4-6](#)所示。

图 4-6 创建内网访问

创建内网访问

1 创建1个内网访问会在VPC终端节点（VPCEP）服务下创建1个对应的VPCEP。请注意：
1. 1个VPCEP对应3条内网域名，请确保内网域名解析配额足够。
2. VPCEP会根据使用时长收取一定费用，具体请参考VPC终端节点价格详情。

* 所属项目 华北-乌兰察布-二零三

* 内网IP 请选择所属VPC 请选择子网

描述 请输入描述 0/1,024

取消 确定

说明

如果下拉框需要选择的“所属项目”不是默认项目，请先切换到该项目下，访问企业仓库页面，进行授权后，再进该页面选择对应项目开通内网访问。

步骤5 单击“确定”。

等待“状态”变为“正常”，且“IP”不为空时，则说明内网访问已创建成功。

图 4-7 内网访问

<input type="checkbox"/>	所属项目	所属VPC	子网	IP	VPC 终端节点	状态	描述	操作
<input type="checkbox"/>	华北-乌兰察布-二零三	vpcvp55c-6a33755a	subnet-7c24(172.16.3.0/24)		000f1d07-d711-41fd-91be-1...	正常	--	删除
<input type="checkbox"/>	华北-乌兰察布-二零三	vpc-fde7(172.16.0.0...	subnet-7c24(172.16...	17	4d8cda02-9c8e-41c8-89ce-e...	正常	--	删除
<input type="checkbox"/>	华北-乌兰察布-二零三	testgitip(192.168...	subnet1612666974...	19	9a099f2e-89a6-4165-ba37-2...	正常	instance[fc0b6928-b...	删除

创建完成后，就可以从已添加的内网IP网段访问仓库。

创建内网访问会在VPC终端节点（VPCEP）服务下创建一个对应的VPC终端节点，请勿删除，否则会影响访问。

----结束

后续操作

创建内网访问后，您还需要创建访问凭证，才可以访问仓库。访问凭证的获取方法请参见[访问凭证](#)。

4.3 域名管理

SWR仓库的域名包含以下两类：

- 默认域名：默认域名，创建仓库自动生成的域名。
- 自定义域名：自定义的域名。

其中，自定义域名功能适用场景：

- 用户欲使用公司统一规划的域名访问服务。
- 从其他镜像仓库服务迁移至本产品时，可继续使用原有域名，保持业务的连续性。

在 SWR仓库中，所有规格的仓库均支持配置多个自定义域名，且不影响仓库已有的默认域名的正常使用。使用自定义域名需要提供域名关联的 SSL 证书，并通过 HTTPS 协议访问仓库。本章节介绍如何通过自定义域名访问容器镜像服务仓库。

说明

仓库当前默认支持最多支持增加5个自定义域名。增加或者删除域名后，需要等待60s~90s才能生效，请您稍候。

前提条件

- 需要开通云服务：云解析服务 DNS、云证书管理服务（Cloud Certificate Manager, CCM）。
- 欲使用域名管理功能，您的账户需要具备查询证书列表权限（scm:cert:list）以及证书导出的权限（scm:cert:export）。
- 已拥有域名。您可以通过[域名注册](#)服务注册域名，详细介绍请参见[什么是域名注册服务？](#)。

📖 说明

- 如果您的SWR仓库在中国境内，那么如果您要在公网环境中使用自定义域名，则域名需要备案。如果您的SWR仓库在境外，则域名无需备案。
- 已为域名签发证书。您可通过云证书管理CCM服务购买证书，并确认已绑定仓库需要使用的自定义域名。

添加自定义域名

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏里的“企业版”，在“仓库管理”页面单击您的仓库名称进入。
- 步骤2** 在左侧导航栏选择“访问管理 > 域名管理”。
- 步骤3** 在域名管理页面单击“添加域名”。
- 步骤4** 在添加域名对话框中输入域名并选择相应的证书ID，单击“确定”。



----结束

更新域名证书

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏里的“企业版”。
- 步骤2** 在顶部菜单栏，选择目标地域。
- 步骤3** 单击仓库名称进入。
- 步骤4** 在左侧导航栏中单击“访问管理 > 域名管理”。
- 步骤5** 在域名管理页面单击目标域名操作列下的“修改”。
- 步骤6** 选择您要更新的证书，单击“确定”。

----结束

删除自定义域名

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏里的“企业版”。
 - 步骤2** 在顶部菜单栏，选择目标地域。
 - 步骤3** 在仓库管理页面单击目标仓库。
 - 步骤4** 在左侧导航栏中单击“访问管理 > 域名管理”。
 - 步骤5** 在域名管理页面单击目标域名操作列下的“删除”。
 - 步骤6** 输入“DELETE”单击“确定”。
- 结束

设置访问控制与域名解析

- **公网访问**

设置公网访问控制和域名解析，您可以使用公网并通过自定义域名的方式访问SWR仓库。配置公网的访问控制，详情请参考[配置公网访问](#)。

- 步骤1** 进入云解析服务控制台。
- 步骤2** 在左侧树状导航栏，选择“公网域名”，进入域名列表页面。
- 步骤3** 【可选】如果没有自定义域名后缀的公网域名，单击右上角的“创建公网域名”，输入域名，单击“确定”。
- 步骤4** 单击您的域名名称进入详情页。
- 步骤5** 单击“添加记录集”，进入“添加记录集”页面设置参数，然后单击“确定”。

表 4-1 添加记录集参数设置

参数	配置
主机记录	输入自定义域名的前缀。
类型	CNAME。
线路类型	指域名访问者所在的地区和使用的运营商网络，本例中为全网默认。
TTL	为缓存时间，数值越小，修改记录各地生效时间越快，默认为5分钟。
值	设置为仓库的默认域名。

----结束

- **内网访问**

设置内网访问控制和内网域名，您可以在指定VPC内的云服务器通过内网拉取SWR仓库中的镜像。配置内网访问控制，详情请参考[配置内网访问](#)。

- 步骤1** 进入云解析服务控制台。

- 步骤2** 在左侧树状导航栏，选择“内网域名”，进入域名列表页面。
- 步骤3** 【可选】如果没有自定义域名后缀的内网域名，单击右上角的“创建内网域名”，输入域名，选择区域，以及与仓库打通网络的VPC，单击“确定”。
- 步骤4** 单击您的域名名称进入详情页。
- 步骤5** 单击“添加记录集”，进入“添加记录集”页面设置参数，然后单击“确定”。

表 4-2 添加记录集参数设置

参数	配置
主机记录	输入自定义域名的前缀
类型	CNAME
线路类型	指域名访问者所在的地区 and 使用的运营商网络，本例中为全网默认。
TTL	为缓存时间，数值越小，修改记录各地生效时间越快，默认为5分钟。
值	设置为仓库的默认域名。

---结束

5 镜像签名与验签

5.1 镜像签名

操作场景

容器镜像服务企业版支持使用数据加密服务（DEW）中创建的密钥对镜像进行签名，保障镜像分发部署过程中的一致性，避免中间人攻击和非法镜像更新及运行。支持命名空间级别的自动镜像签名，容器镜像上传后都会根据签名规则自动签名。在使用镜像签名功能时，请先在数据加密服务（DEW）中创建非对称密钥，然后创建签名规则，设置参数。之后根据规则设置的触发模式完成手动或者自动签名。

约束与限制

- 镜像验签功能仅支持V1.23及以上集群版本
- 当前支持密钥算法类型见[表1](#)
- 单个仓库最多同时支持100000 tag，单个仓库的签名速度为1分钟300个tag本；验签插件安装后，验签速度为1分钟300个镜像版本。

前提条件

[已购买企业版实例](#)

[已购买CCE集群](#)

创建非对称密钥

步骤1 登录数据加密服务控制台。

步骤2 在左侧导航栏选择“密钥管理”，单击右上角的“创建密钥”。

步骤3 在“创建密钥”对话框中配置参数，然后单击“确定”。

镜像签名功能需要非对称密钥算法的支持，创建密钥时，密钥算法需选择EC、RSA或SM2类型，详情请见[表1](#)。其他参数配置请参见[创建密钥](#)。

图 5-1 创建密钥

×

创建密钥

别名

密钥算法

密钥用途

所属密钥库 [新建密钥库](#)

描述 (可选) 0/255

标签 (可选) 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。 [查看预定义标签](#)

您还可以创建20个标签。

密钥实例费用 /小时

API请求费用 万次 (小于等于20,000次)
 万次 (大于20,000次)

参考价格，具体扣费请以账单为准。支持密钥跨region复制的局点，费用账单详情资源ID会统一加上项目名称前缀。 [了解计费详情](#)

表 5-1 容器镜像服务支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	用途
非对称密钥	RSA	<ul style="list-style-type: none"> • 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非对称密钥	少量数据的加解密或数字签名。
非对称密钥	ECC	<ul style="list-style-type: none"> • EC_P256 - ECDSA_SHA_256 • EC_P384 - ECDSA_SHA_384 	椭圆曲线密码，使用NIST推荐的椭圆曲线	数字签名
非对称密钥	SM2	SM2	国密SM2非对称密钥	少量数据的加解密或数字签名。

----结束

创建签名规则

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。
- 步骤2** 在左侧导航栏选择“镜像签名”。
- 步骤3** 在右上角单击“创建签名规则”。
- 步骤4** 填写具体规则。

表 5-2 参数说明

参数名称	说明	示例
规则名称	镜像签名规则的名称。	SignatureRule
命名空间	选择要签名的镜像所在的命名空间。	library


参数名称	说明	示例
规则范围	<p>镜像: 镜像名称, 默认使用正则表达式。单击  切换到选择模式 可手动选择镜像。</p> <p>正则表达式规则可填写如nginx-*、{repo1, repo2} 等, 其中:</p> <ul style="list-style-type: none"> • *: 匹配不包含路径分隔符“/”的任何字段。 • **: 匹配包含路径分隔符“/”的任何字段。 • ?: 匹配任何单个非“/”的字符。 • {选项1, 选项2, ...}: 同时匹配多个选项。匹配上其中一个即可。 <p>版本: 镜像的版本, 同样使用正则表达式, 匹配规则与镜像名称相同。</p>	nginx-*: 表示匹配“nginx-”开头的镜像。
签名方式	当前支持使用KMS签名。	KMS
签名Key	选择在 创建非对称密钥 中创建的密钥。	key1
触发模式	<ul style="list-style-type: none"> • 手动: 手动触发, 规则创建完成后需要您手动单击执行。 • 事件触发 + 手动: 事件触发指当有新镜像上传到仓库且符合匹配规则时触发镜像签名。 	事件触发 + 手动
规则描述	规则的描述信息。	-

图 5-2 创建签名规则

创建签名规则

* 规则名称: test

* 命名空间: library

规则范围: 镜像 --请选择镜像--
[切换成正则输入模式](#)

版本: 请输入版本范围, 不填或填*默认为匹配全部
 无版本的制品

* 签名方式: KMS

* 签名Key: 请输入签名Key

* 触发模式: 手动 事件触发 + 手动

规则描述: 请输入描述 (0/1,024)

取消 确定

步骤5 单击“确定”完成规则创建。

----结束

签名功能生效验证

登录容器镜像服务SWR控制台，进入“企业版”，单击仓库名称进入仓库实例，单击“镜像签名”创建签名规则并执行。执行成功之后进入“镜像管理”，查看镜像签名选择的镜像可以发现“镜像制品”下面的存在附件，该附件即该镜像的签名文件。

5.2 镜像验签

操作场景

容器镜像服务是通过swr-cosign插件实现镜像签名验证的，使用镜像验签功能需要安装swr-cosign插件即可。下面介绍如何安装验签插件swr-cosign。

操作步骤

- 步骤1** 登录云容器引擎CCE控制台。
- 步骤2** 在左侧导航栏上单击“插件市场”。
- 步骤3** 在插件市场页面上方搜索框输入“cosign”并搜索。
- 步骤4** 在下方的搜索结果中找到“容器镜像签名验证”插件，单击“安装”。
- 步骤5** 填写“安装插件”页面的相关参数。
 - **选择集群**：选择镜像所在集群。该插件只能在K8S V1.23及以上版本集群上安装。

须知

对集群某个命名空间进行镜像验签时，需要先为该命名空间添加 policy.sigstore.dev/include:true 标签。

- **选择版本**：选择插件版本
- **规格配置**
 - 单仓库：当前插件只支持在1个仓库上使用。
 - 高可用：当前插件支持在2个仓库上使用。
 - 自定义：自定义仓库数、CPU配额、容器配额。

表 5-3 swr-cosign 插件规格配置

参数	参数说明
插件规格	该插件可配置“单实例”、“高可用”或“自定义”规格。
实例数	选择上方插件规格后，显示跟插件规格匹配的实例数。 选择“自定义”规格时，您可根据需求调整插件实例数。
容器	选择“自定义”规格时，您可根据需求调整插件实例的容器规格。


- **参数配置**
 - KMS密钥：选择一个[创建非对称密钥](#)中创建好的密钥。
 - 验签镜像：单击 ，选择需要验签的镜像。

表 5-4 swr-cosign 插件参数配置

参数	参数说明
KMS密钥	选择一个密钥，仅支持 EC_P256、EC_P384、SM2 类型的密钥。 您可以前往密钥管理服务新增密钥。

参数	参数说明
验签镜像	验签镜像地址通过正则表达式进行匹配，例如填写 docker.io/** 表示对docker.io镜像仓库的镜像进行验签。如需对所有镜像验签，请填写**。

步骤6 填写完成后，单击“安装”。

待插件安装完成后，选择对应的集群，然后单击左侧导航栏的“插件中心”，可筛选“已安装插件”查看相应的插件。

----结束

验签功能生效验证

登录云容器引擎CCE控制台，单击已安装验签插件的集群名称进入集群，进入“工作负载”界面，单击“创建工作负载”，选择已打验签标签policy.sigstore.dev/include:true的命名空间，选择一个未签名的镜像，勾选镜像访问凭证继续创建工作负载，此时会发现验签不通过，原因是容器镜像验签插件会对当前命名空间下的创建负载的容器镜像进行验签，说明验签功能已生效。

6 镜像同步

操作场景

容器镜像服务企业版支持与其他仓库之间同步容器镜像，可实现单点推送及全球自动同步分发，方便企业在全全球多个地域快速部署更新容器业务。当前支持与如下类型仓库之间同步：

- 容器镜像服务：即SWR共享仓库中的镜像。
- 容器镜像服务企业版：支持华为云不同地域的企业仓库以及客户基于开源harbor搭建的私有仓库。

镜像同步功能允许用户自定义创建同步规则，可指定某个仓库内的部分资源同步至另一个仓库内的命名空间。例如，用户可选择同步资源类型（容器镜像、Helm Chart、或是全部同步），通过正则表达式过滤镜像及版本，可选择是否覆盖已有的同名镜像，避免历史数据覆盖丢失。

6.1 目标仓库

添加目标仓库

步骤1 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。

步骤2 在左侧导航栏选择“镜像同步 > 目标仓库”。

步骤3 在右上角单击“添加目标仓库”。

表 6-1 参数说明

参数名称	说明	示例
仓库名	目标仓库名称。	remote-registry

参数名称	说明	示例
提供者	选择目标仓库所在位置。 <ul style="list-style-type: none"> 容器镜像服务：即SWR共享仓库中的镜像。 容器镜像服务 企业版：其他仓库，可以是不同地域的企业仓库。 	容器镜像服务 企业版
仓库地址	目标仓库的地址。	swr.cn-east-3.myhuaweicloud.com
访问ID 访问密码	目标仓库的访问ID和密码。 ID和密码对应docker login命令中的用户名和密码。	-
验证远程证书	校验证书是否为授信单位发布，不勾选则不校验。	-
所属区域	提供者“容器镜像服务 企业版”时需要选择。	华东-上海一
所属项目	提供者“容器镜像服务 企业版”时需要选择。	华东-上海一
所属仓库	提供者“容器镜像服务 企业版”时需要选择。	-
hosts配置	后台服务只能解析当前局点的公共域名，若涉及其他域名请配置host参数，如仓库域名与OBS桶域名。	-
描述	目标仓库的描述信息。	-

图 6-1 添加目标仓库

添加目标仓库

* 仓库名

* 提供者

* 类型 华为云 其他

* 所属区域

* 所属实例

访问ID

访问密码 验证远程证书

描述 0/1,024

步骤4 单击“确定”。

创建完成后，界面会显示目标仓库的健康状态，您还可以对目标仓库的信息进行修改。


----结束

6.2 同步规则

创建同步规则

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。
- 步骤2** 在左侧导航栏选择“镜像同步 > 同步规则”。
- 步骤3** 在右上角单击“创建同步规则”。
- 步骤4** 填写具体规则。

表 6-2 参数说明

参数名称	说明	示例
规则名称	镜像同步规则的名称。	SyncRule
同步模式	<ul style="list-style-type: none"> 推送到目标仓库：将本仓库中镜像推送到目标仓库中。 从目标仓库拉取：从目标仓库中拉取镜像到本仓库中。 	推送到目标仓库
目标仓库	选择上面 添加目标仓库 步骤中添加的目标仓库。	-
目标命名空间	同步至目标仓库后所在的命名空间（其他云厂商可能被称作项目等），不填写则默认是与本仓库中同名的命名空间，如果目标仓库中没有该命名空间同步可能会失败。	library1
本地命名空间	从目标仓库拉取到本仓库，镜像所在的命名空间，不填写则默认是与目标仓库中同名的命名空间（其他云厂商可能被称作项目等），如果没有命名空间将新建。	library1
本地仓库推送范围	<p>命名空间：命名空间名称范围。</p> <p>镜像：镜像名称，默认使用正则表达式匹配。单击  切换成选择模式 可手动选择镜像。</p> <p>正则表达式规则可填写如Nginx-*、{repo1, repo2} 等，其中：</p> <ul style="list-style-type: none"> *：匹配不包含路径分隔符“/”的任何字段。 **：匹配包含路径分隔符“/”的任何字段。 ?: 匹配任何单个非“/”的字符。 {选项1, 选项2, ...}：同时匹配多个选项。 <p>版本：镜像的版本，同样使用正则表达式匹配，匹配规则与镜像相同。</p> <p>说明 当同步模式是“推送到目标仓库”时有该参数。</p>	library2 nginx-* **

参数名称	说明	示例
目标仓库拉取范围	<p>命名空间: 命名空间名称范围。</p> <p>镜像: 镜像名称, 使用正则表达式匹配。</p> <p>正则表达式规则可填写如nginx-*、{repo1, repo2} 等, 其中:</p> <ul style="list-style-type: none"> • *: 匹配不包含路径分隔符“/”的任何字段。 • **: 匹配包含路径分隔符“/”的任何字段。 • ?: 匹配任何单个非“/”的字符。 • {选项1, 选项2, ...}: 同时匹配多个选项。 <p>版本: 镜像的版本, 同样使用正则表达式匹配, 匹配规则与镜像相同。</p> <p>说明 当同步模式是“从目标仓库拉取”时有该参数。</p>	<p>library2</p> <p>nginx-*</p> <p>**</p>
触发模式	<ul style="list-style-type: none"> • 手动: 手动触发, 规则创建完成后需要您手动单击执行。 • 事件触发 + 手动: 事件触发指推送和被拉取一方有新增镜像且符合匹配规则时触发同步。 • 定时 + 手动: 定时即为设置周期性定时同步。 	定时 + 手动
定时	触发模式为“定时 + 手动”时可以设置。	-
覆盖	当同步相同版本的镜像时, 是否覆盖。	-
规则描述	规则的描述信息。	-

图 6-2 创建同步规则

创建同步规则

* 规则名称

* 同步模式 推送到目标仓库 从目标仓库拉取

* 目标仓库

本地命名...

规则范围

命名空间

镜像

版本

* 触发模式 手动 定时 + 手动

覆盖

规则描述 0/1,024

步骤5 单击“确定”完成规则创建。

----结束

同步规则示例

- 推送到目标仓库
将本仓库中library命名空间中以“nginx-”名称开头的所有版本镜像，推送到目标仓库test-edit-fail的lib1命名空间下，触发模式为手动触发，且覆盖相同名称版本的镜像。

创建同步规则

×

* 规则名称

* 同步模式 推送到目标仓库 从目标仓库拉取

* 目标仓库

目标命名...

规则范围 命名空间

镜像
⇌ 切换成选择模式

版本

* 触发模式 手动 事件触发 + 手动 定时 + 手动

覆盖

规则描述
0/1,024

- 从目标仓库拉取
将目标仓库test-edit-fail的lib1命名空间中以“nginx-”名称开头的所有版本镜像，拉取到本仓库library1命名空间中，触发方式为手动触发，且覆盖相同名称版本的镜像。

创建同步规则

* 规则名称

* 同步模式 推送到目标仓库 从目标仓库拉取

* 目标仓库

本地命名...

规则范围 命名空间

镜像

版本

* 触发模式 手动 定时 + 手动

覆盖

规则描述

0/1,024

管理同步规则

成功创建后即可在“同步规则”页面查看已创建的同步规则，您可以执行以下操作管理同步规则。

图 6-3 同步规则

规则名称	启用	触发模式	同步模式	同步范围	目标仓库	创建时间	更新时间	操作
demo01	<input checked="" type="checkbox"/>	手动	从目标仓库拉取	镜像"nginx- 版本"	test	2024/03/14 14:23:53 GMT+08:00	2024/03/14 14:25:10 GMT+08:00	执行 编辑 删除

任务ID	状态	触发模式	成功百分比	总数	持续时间	创建时间	操作
49	成功	手动	100.00%	3	11秒	2024/03/14 14:25:15 GMT+08:00	详情
48	失败	手动	0.00%	1	2分钟	2024/03/14 14:24:04 GMT+08:00	详情

图 6-4 任务详情





- 启用： 表示规则启用， 表示规则关闭。新创建的同步规则默认为启用状态，您可以自行调整。
- 执行：手动触发同步规则。
- 编辑：重新编辑同步规则，所有参数均可编辑。
- 删除：删除该同步规则。
- 查看同步任务：当同步规则被触发时，符合规则范围的镜像将被同步。同步任务包含的信息如下：

表 6-3 同步任务

参数	说明
任务ID	仓库内唯一的同步执行任务ID。
状态	任务完成状态。
触发模式	手动或自动。 单击“执行”为手动方式，通过规则定义的周期自动执行，则为自动方式。
成功百分比	同步成功的镜像数占总数的百分比。
总数	当前任务需要同步的镜像总数。
持续时间	完成一次任务消耗的时间。

参数	说明
创建时间	同步任务被触发的时间。
操作	详情：任务详细信息，单击后在侧边栏可查看哪些镜像被同步。

6.3 镜像同步

操作步骤

- 步骤1** 购买仓库，详细操作步骤请参考[购买仓库](#)。
- 步骤2** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面
- 步骤3** 在左侧导航栏选择“镜像同步” > “目标仓库”。
- 步骤4** 按照表格填写相关参数，配置目标仓库，参数填写说明请参考[表1](#)。
- 步骤5** 在左侧导航栏选择“镜像同步” > “同步规则”，创建一个仓库同步规则，详细操作步骤请参考[创建同步规则](#)。镜像将根据创建的规则自动或手动同步。

----结束

7 运维中心

7.1 镜像老化

操作场景

现代软件开发多采用流水线生成镜像，随着版本不断向前迭代，将会不断生成新的镜像版本。新版本镜像的生成意味着老旧版本的镜像变得不再需要，如何方便快速的删除这些老旧版本镜像成为了新的问题。容器镜像服务企业版提供镜像老化功能，您可以创建镜像老化规则，手动或定时触发该规则，根据规则老化删除不需要的镜像。

约束与限制

每个命名空间下仅允许创建一个老化规则。

创建老化规则

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。
- 步骤2** 在左侧导航栏选择“运维中心 > 镜像老化”。
- 步骤3** 在右上角单击“创建老化规则”。
- 步骤4** 填写具体规则。

表 7-1 参数说明

参数名称	说明	示例
规则名称	老化规则的名称。	AgingRule
命名空间	选择要老化的镜像所在的命名空间。	library1


参数名称	说明	示例
规则范围	<p>镜像： 镜像名称，默认使用正则表达式匹配。单击  切换成选择模式 可手动选择镜像。</p> <p>正则表达式规则可填写如nginx-*、{repo1, repo2} 等，其中：</p> <ul style="list-style-type: none"> • *：匹配不包含路径分隔符“/”的任何字段。 • **：匹配包含路径分隔符“/”的任何字段。 • ?：匹配任何单个非“/”的字符。 • {选项1, 选项2, ...}：同时匹配多个选项。 <p>版本： 镜像的版本，同样使用正则表达式匹配，匹配规则与镜像相同。</p>	nginx-*
老化条件	<p>选择执行的老化条件，有如下条件可选择：</p> <ul style="list-style-type: none"> • 保留最近推送的#个镜像版本 • 保留最近拉取的#个镜像版本 • 保留最近#天被推送过的 • 保留最近#天被拉取过的 <p>其中“#”为变量，取值为下面“版本数”和“保留天数”的值。</p>	保留最近推送的#个镜像版本
版本数	老化条件为“保留最近推送的#个镜像版本”和“保留最近拉取的#个镜像版本”需设置。	10
保留天数	老化条件为“保留最近#天被推送过的”和“保留最近#天被拉取过的”需设置。	10
触发模式	<ul style="list-style-type: none"> • 手动：手动触发，规则创建完成后需要您手动单击执行。 • 定时 + 手动：定时即为设置周期性定时老化。 	定时 + 手动
定时	触发模式为“定时 + 手动”时可以设置。	-

图 7-1 创建老化规则

创建老化规则

每个命名空间下仅允许创建一个老化规则。

* 规则名称

* 命名空间

规则范围 **镜像**
 切换成选择模式

版本

* 老化条件

* 触发模式 手动 定时 + 手动

步骤5 单击“确定”完成规则创建。

----结束

老化规则示例

- 示例1:
选择library命名空间中, 名称以“nginx-”开头所有版本的镜像(版本*表示选择所有版本), 保留最近拉取的10个镜像版本, 其余镜像全部删除, 且需要手动触发执行。

创建老化规则

×

i 每个命名空间下仅允许创建一个老化规则。

* 规则名称

* 命名空间

规则范围 镜像 [切换成选择模式](#)

版本

* 老化条件

* 版本数

* 触发模式 手动 定时 + 手动

确定 **取消**

- 示例2:
选择library命名空间中，nginx和busybox所有版本的镜像（版本不填写表示选择所有版本），保留最近10天被推送过的镜像，其余镜像全部删除，每周日0时0分执行该规则，且可以手动触发执行。

创建老化规则



每个命名空间下仅允许创建一个老化规则。

* 规则名称

* 命名空间

规则范围 镜像
切换成选择模式

版本

* 老化条件

* 保留天数 天

* 触发模式 手动 定时 + 手动

* 定时 时 分执行一次

确定

取消

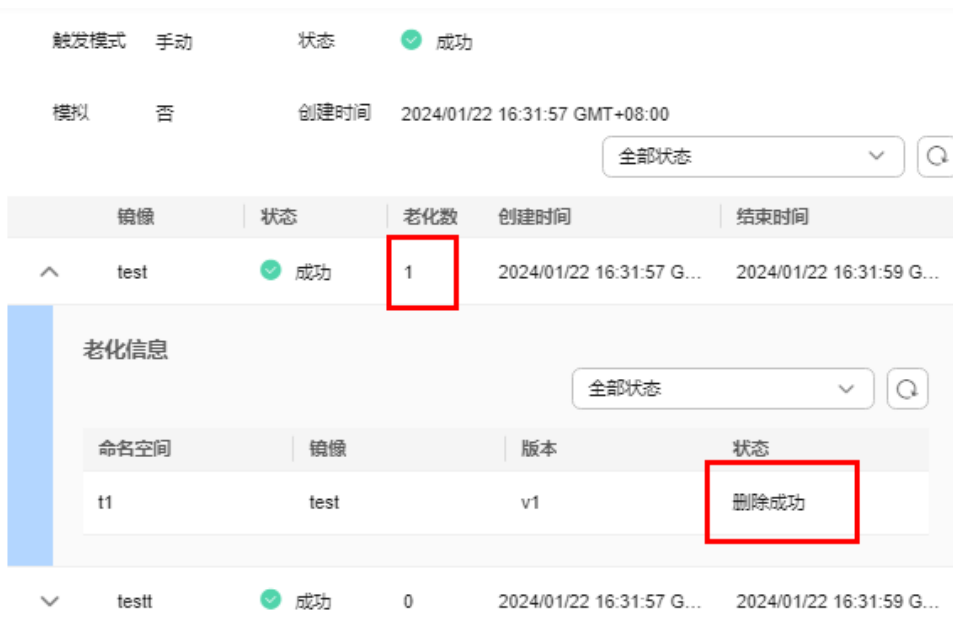
管理老化规则

成功创建后即可在“镜像老化”页面查看已创建的老化规则，您可以执行以下操作管理老化规则。

图 7-2 老化规则





图 7-3 任务详情



- 查看老化任务：当老化规则被触发时，符合规则范围的镜像将被删除。老化任务包含的信息如下：

表 7-2 老化任务

参数	说明
任务ID	仓库内唯一的老化执行任务ID。
状态	任务完成状态。
触发模式	手动或自动。 单击“执行”或“模拟”为手动方式，通过规则定义的周期自动执行，则为自动方式。
模拟	是或否。 单击“模拟”则为是，单击“执行”则为否。模拟可用于确认规则是否生效，但不实际清理镜像版本。
持续时间	完成一次任务消耗的时间。
创建时间	老化任务被触发的时间。
操作	详情：任务详细信息，单击后在侧边栏可查看哪些镜像被删除（“老化数”非0，说明有镜像被删除）。

- 修改规则状态： 表示规则启用， 表示规则关闭。新创建的老化规则默认为启用状态，您可以自行调整。
- 执行：真实执行。为避免误操作，建议在首次执行老化规则前模拟执行。

- 模拟：模拟执行。可用于确认规则是否生效，但不实际清理镜像版本。
- 编辑：重新编辑老化规则，除“命名空间”外，其余参数均可编辑。
- 删除：删除该老化规则。

7.2 触发器

操作场景


容器镜像服务企业版支持配置并使用触发器功能。您可以通过创建触发器，当有触发动作（如上传镜像）发生时，自动执行您定义的HTTP POST请求（如让流水线下载镜像并部署）。使用触发器，您可以快速接入现有研发流程及CI/CD平台，实现容器DevOps场景。

触发器支持上传镜像的触发动作。

创建触发器

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。
- 步骤2** 在左侧导航栏选择“运维中心 > 触发器”。
- 步骤3** 在右上角单击“创建触发器”。
- 步骤4** 填写具体规则。

表 7-3 参数说明

参数名称	说明	示例
规则名称	触发器规则的名称。	TriggerRule
命名空间	选择要创建触发器的命名空间。	library1
规则范围	<p>镜像：镜像名称，默认使用正则表达式匹配。单击  切换成选择模式 可手动选择镜像。</p> <p>正则表达式规则可填写如nginx-*、{repo1, repo2} 等，其中：</p> <ul style="list-style-type: none"> • *：匹配不包含路径分隔符“/”的任何字段。 • **：匹配包含路径分隔符“/”的任何字段。 • ?：匹配任何单个非“/”的字符。 • {选项1, 选项2, ...}：同时匹配多个选项。 <p>版本：镜像的版本，同样使用正则表达式匹配，匹配规则与镜像相同。</p>	nginx-*

参数名称	说明	示例
触发动作	触发器支持如下触发动作： <ul style="list-style-type: none">• 上传镜像	上传镜像
验证远程证书	勾选则校验证书是否是授信单位发布，不勾选则不校验。	-
请求地址类型	<ul style="list-style-type: none">• 内网• 公网	内网
请求地址	触发器被触发后，发起请求的目标地址。触发器将向该地址发起POST请求。 注意 请确保该地址的后端服务的IP在购买仓库时选择的VPC默认网段范围内，不支持配置VPC默认网段范围之外的IP地址。	-
请求头域	触发器发起POST请求时，支持以Key:Value形式输入可携带的Header信息。例如，Authentication:xxxxxxx。 多个Header之间用英文分号(;)分隔，例如， param1:value1;param2:value2。	-

图 7-4 创建触发器

✕

创建触发器

* 规则名称	请输入规则名称
* 命名空间	--请选择命名空间--
规则范围	镜像 ② 请输入镜像仓库范围，不填或填**默认为匹配全部 ≡ 切换到选择模式
版本	版本 ② 请输入版本范围，不填或填**默认为匹配全部
* 触发动作	--请选择触发动作--
验证远程证书	<input checked="" type="checkbox"/>
* 请求地址类型	<input checked="" type="radio"/> 内网 <input type="radio"/> 公网
* 请求地址	https:// 请输入触发请求地址
请求头域	自定义Header，仅支持Key:Vaule格式，用;号分隔，例： param1:value1;param2:value2 0/4,096
规则描述	请输入描述 0/1,024

取消确定

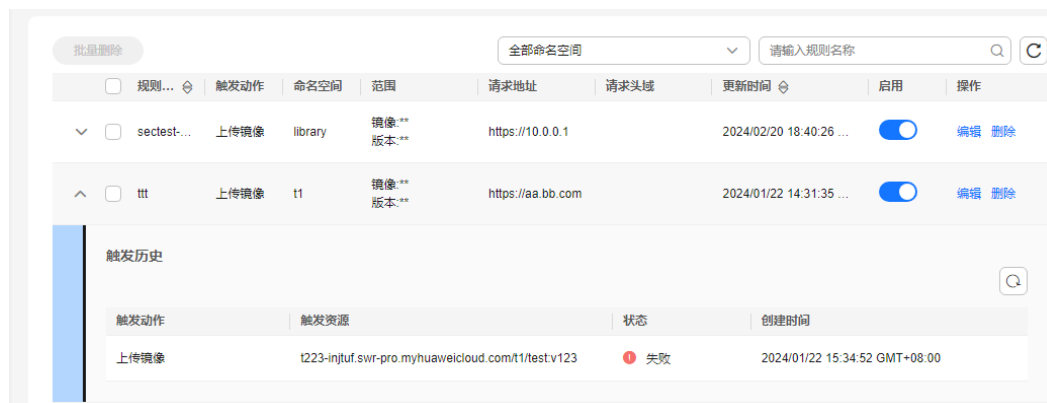
步骤5 单击“确定”完成创建。

---结束

管理触发器

成功创建后即可在“触发器”页面查看已创建的触发器规则，您可以执行以下操作管理触发器。

图 7-5 管理触发器






- 修改规则状态： 表示规则启用， 表示规则关闭。新创建的触发器规则默认认为启用状态，您可以自行调整。
- 编辑：重新编辑触发器规则，除“命名空间”和“请求地址”外，其余参数均可编辑。
- 删除：删除该触发器规则。
- 查看触发历史：当有符合触发器规则的动作发生时，自动触发该规则，您可以单击图标查看触发历史。包含信息如下：

表 7-4 触发历史

参数	说明
触发动作	产生该次触发的触发动作。
触发资源	产生该次触发动作的仓库资源。
状态	触发器执行Webhook请求的状态。
创建时间	该次触发的启动时间，即发起Webhook请求的时间。

7.3 镜像版本不可变

操作场景

容器镜像服务企业版支持配置并使用镜像版本不可变规则。容器镜像服务为了实现端到端可信，规避访问凭证泄漏后，现有镜像被覆盖的问题，容器镜像服务新增镜像版本不可变功能，通过对命名空间下的镜像设置不可变规则，保证该镜像版本不可变。

约束与限制

每个命名空间下仅允许创建一个不可变规则。

创建镜像不可变规则

- 步骤1** 登录容器镜像服务控制台，单击左侧菜单栏“企业版”，然后单击仓库名称进入仓库详情页面。
- 步骤2** 在左侧导航栏选择“运维中心 > 镜像版本不可变”。
- 步骤3** 单击右上角“创建不可变规则”。
- 步骤4** 填写具体规则。

表 7-5 镜像不可变规则

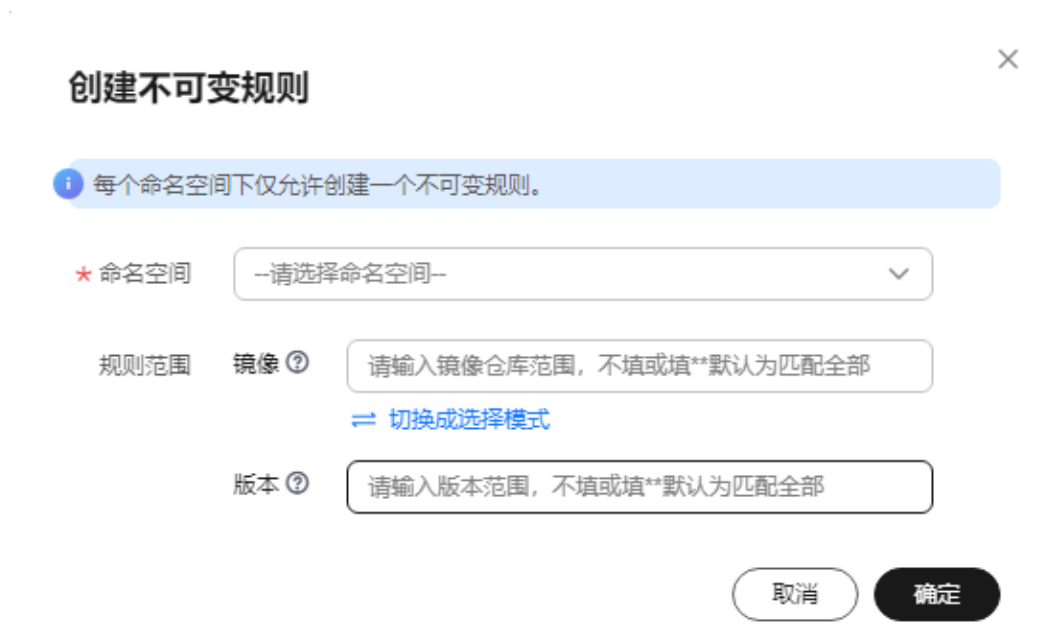
参数名称		说明
命名空间		仓库下创建的命名空间，包括公有命名空间和私有命名空间。
规则范围	镜像	选择选择该命名空间下的一个或多个镜像。
	版本	输入需要创建不可变规则的镜像版本范围，若不填或者填**，则默认匹配全部版本。

说明

- 在选择模式下，镜像范围可以勾选该命名空间下的镜像，如[表7-5](#)。
- 在正则输入模式下：
正则表达式规则可填写如 `nginx-*`，`{repo1, repo2}` 等，其中：
 - `*`：匹配不包含 `'/'` 的任何字段。
 - `**`：匹配包含 `'/'` 的任何字段。
 - `?`：匹配任何单个非 `'/'` 的字符。
 - `{选项1,选项2,...}`：同时匹配多个选项。

- 步骤5** 单击“确定”，完成不可变规则创建。

图 7-6 创建不可变规则





----结束

管理镜像版本不可变规则

成功创建后即可在“镜像版本不可变”页面查看已创建的不可变规则，您可以执行以下操作管理镜像不可变规则。

图 7-7 管理镜像不可变



- 修改规则状态： 表示规则启用， 表示规则关闭。新创建的不可变规则默认为启用状态，您可以自行调整。
- 编辑：重新编辑不可变规则，除“命名空间”外，其余参数均可编辑。
- 删除：删除该不可变规则。