容器镜像服务(企业版)

用户指南

文档版本 01

发布日期 2025-02-18

华为云计算技术有限公司

商标声明


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 2
1.3 标签管理 3
1.3.1 标签概述 3
1.3.2 新增仓库标签 6
1.3.3 删除仓库标签 7
1.3.4 修改仓库标签 8
1.3.5 通过标签查找仓库 9
1.3.6 命名空间标签管理 9
2 镜像管理 12
2.1 镜像仓库 12
3 命名空间 16
4 访问管理 18
4.1 访问凭证 18
4.2 访问控制 19
4.2.1 访问控制概述 20
4.2.2 公网访问 20
4.2.3 内网访问 22
4.3 域名管理 23
5 镜像签名与验签 27
5.1 镜像签名 27
5.2 镜像验签 31
6 镜像同步 34
6.1 目标仓库 34
6.2 同步规则 36
6.3 镜像同步 43
7 运维中心 44
7.1 镜像老化 44
7.2 触发器 48
8 审计 52

8.1 支持云审计的关键操作 52
8.2 查看云审计日志 54

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。
- 仓库是按照region购买的。如果需要在多个region使用，请分别在每个region完成购买。企业版目前支持“华东-上海一、华北-乌兰察布一、华北-北京四、亚太-新加坡、华南-广州、西南-贵阳一、华东二、华东-芜湖二零一、中国-香港、非洲-约翰内斯堡、土耳其-伊斯坦布尔、西北-克拉玛依、印尼-雅加达”区域。

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。在页面左上角切换Region到您所在的Region。

步骤2 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：

- **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。
- **自定义OBS桶**：可手动指定仓库的OBS桶，建议选择3AZ高可用的OBS桶。
- **OBS桶加密**（静态数据存储加密）：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。

  说明

  开启OBS桶加密会降低仓库实例性能，请您按需选择。
- **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。
- **标签：**标签是对云上资源的一种标识。
- **描述**：输入仓库的描述。

步骤3 单击右下角“立即购买”。

步骤4 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。

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**，在页面左上角切换Region到您所在的Region。

步骤2 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”。

步骤3 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 1-1 标签示例 1

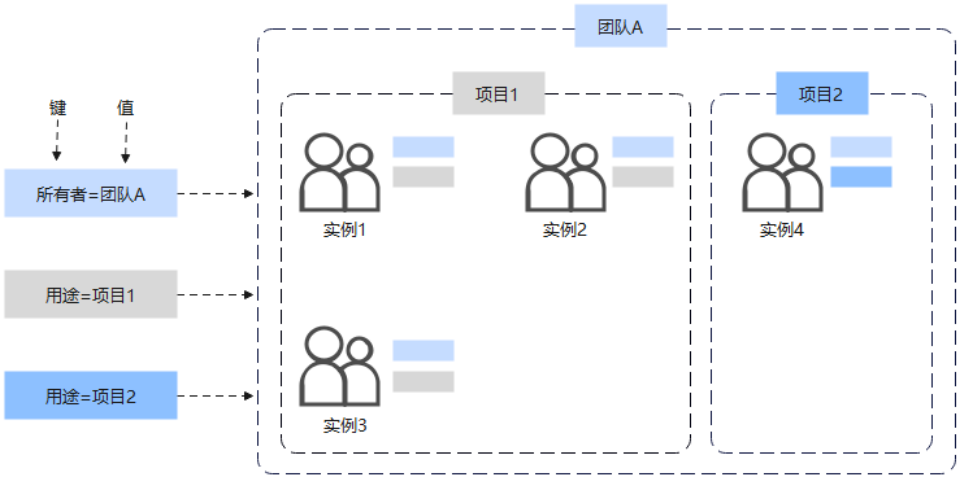


图 1-2 标签示例 2

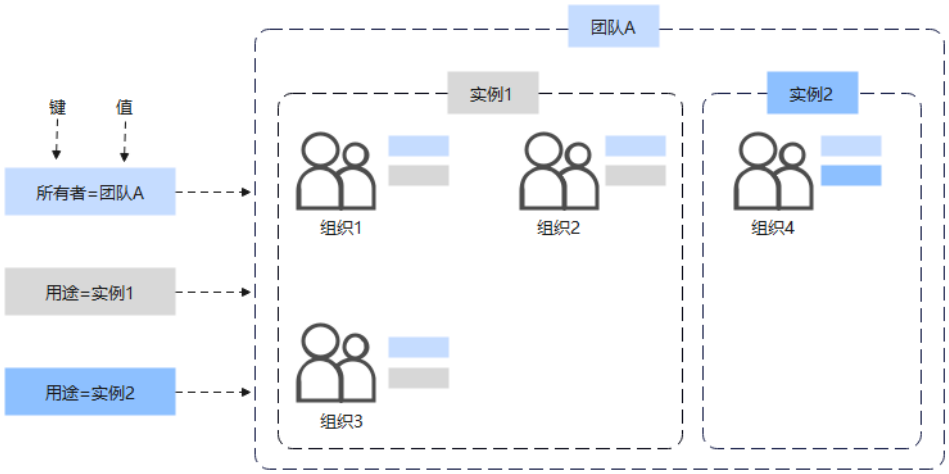


图1 图2说明了标签的工作方式。在此示例中，您为每个仓库分配了两个标签，每个标签都包含您定义的一个“键”和一个“值”，一个标签使用键为“所有者”，另一个使用键为“用途”，每个标签都拥有相关的值。

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

当您在使用容器镜像服务时，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	● 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	● 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**，在页面左上角切换Region到您所在的Region。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 1-3 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**，在页面左上角切换Region到您所在的Region。

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 1-4 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 1-5 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，在页面左上角切换Region到您所在的Region。

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 1-6 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 1-7 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**，在页面左上角切换Region到您所在的Region。

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**，在页面左上角切换Region到您所在的Region。

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**容器镜像服务控制台**，在页面左上角切换Region到您所在的Region。

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**，在页面左上角切换Region到您所在的Region。

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。

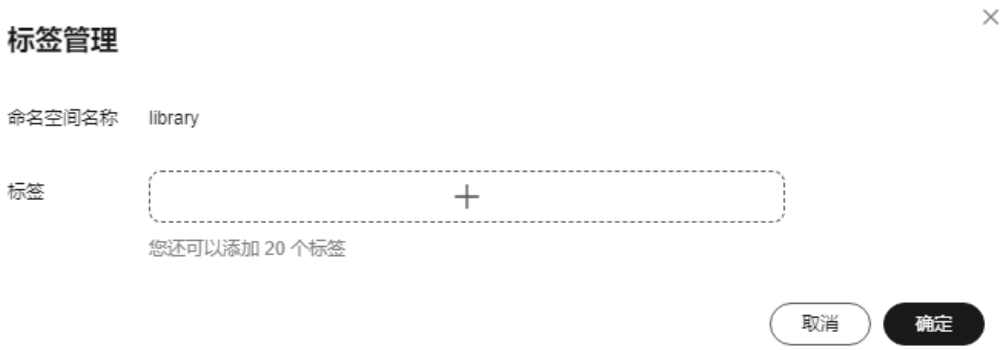
步骤3 单击仓库详情页左侧导航栏“命名空间”，进入命名空间列表页。单击页面右上角的 图标，以列表形式展示命名空间列表。

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 1-8 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 1-9 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**，在页面左上角切换Region到您所在的Region。

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**，在页面左上角切换Region到您所在的Region。

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**，在页面左上角切换Region到您所在的Region。

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。

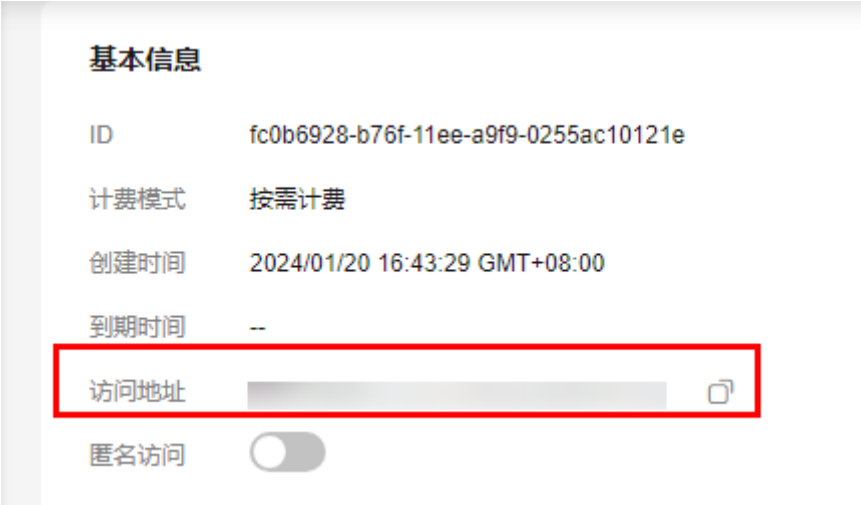
docker tag [镜像名称1:版本名称1] [镜像仓库地址]/[命名空间名称]/[镜像名称2:版本名称2]

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**，在页面左上角切换Region到您所在的Region，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

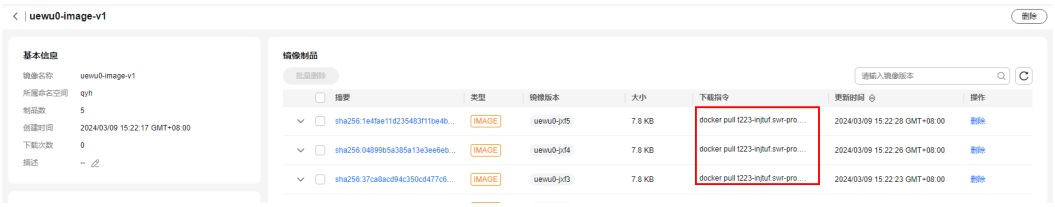
步骤1 登录**容器镜像服务控制台**，在页面左上角切换Region到您所在的Region。

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。

  注意

  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**。

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**，在页面左上角切换Region到您所在的Region。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

- 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

为避免您删除重要数据，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**，在页面左上角切换Region到您所在的Region。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

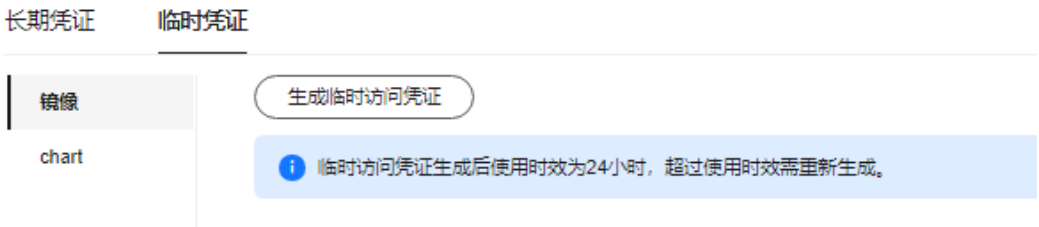
创建临时凭证

步骤1 登录**容器镜像服务控制台**，在页面左上角切换Region到您所在的Region。

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**

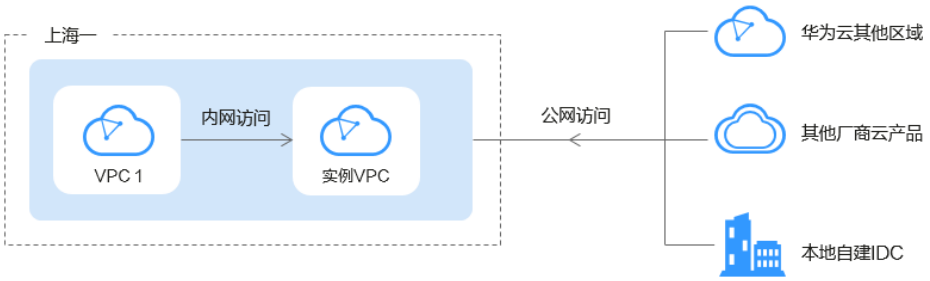
4.2 访问控制

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。

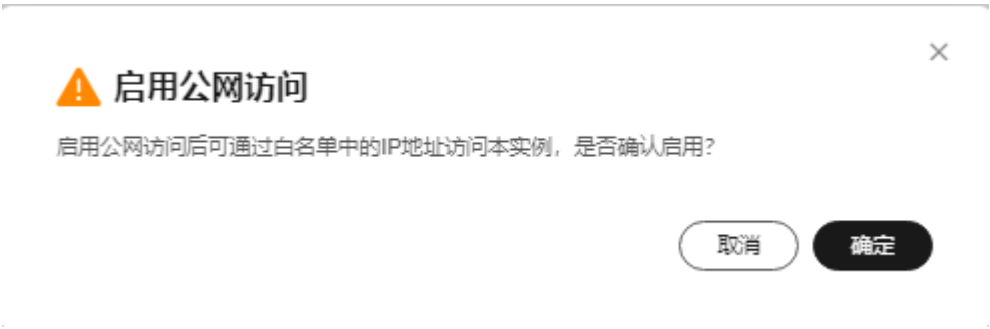
操作步骤

步骤1 登录**容器镜像服务控制台**，在页面左上角切换Region到您所在的Region。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”，在弹出的窗口中单击⊕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**，在页面左上角切换Region到您所在的Region。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

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

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。证书导出权限在IAM新版本控制台和旧版本控制台的权限不同。具体如下：
  - IAM新版控制台：（scm:cert:export)
  - IAM旧版控制台：（scm:cert:download))
- 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**，在页面左上角切换Region到您所在的Region。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**，在页面左上角切换Region到您所在的Region。

步骤2 单击仓库名称进入。

步骤3 在左侧导航栏中单击“访问管理 > 域名管理”。

步骤4 在域名管理页面单击目标域名操作列下的“修改”。

步骤5 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**，在页面左上角切换Region到您所在的Region。

步骤2 在仓库管理页面单击目标仓库。

步骤3 在左侧导航栏中单击“访问管理 > 域名管理”。

步骤4 在域名管理页面单击目标域名操作列下的“删除”。

步骤5 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

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

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	• 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	小量数据的加解密或数字签名。
非对称密钥	ECC	• 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	小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**，在页面左上角切换Region到您所在的Region。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	**镜像**：镜像名称，默认使用正则表达式。单击 ⇌ 切换成选择模式 可手动选择镜像。 正则表达式规则可填写如nginx-*、{repo1, repo2} 等，其中： ● *****：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。 **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。	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	● 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

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**，在页面左上角切换Region到您所在的Region。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。 • 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	提供者为“容器镜像服务 企业版”时需要选择。	华东-上海一
所属项目	提供者为“容器镜像服务 企业版”时需要选择。	华东-上海一
所属仓库	提供者为“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

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，在页面左上角切换Region到您所在的Region。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	• 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	**命名空间**：命名空间名称范围。 **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。 正则表达式规则可填写如nginx-* 、{repo1, repo2} 等，其中： • *：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。 **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。 **说明** 当同步模式是“推送到目标仓库”时有该参数。	library2 nginx-* **

参数名称	说明	示例
目标仓库拉取范围	**命名空间**：命名空间名称范围。 **镜像**：镜像名称，使用正则表达式匹配。 正则表达式规则可填写如nginx-* 、{repo1, repo2} 等，其中： ● *****：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。 **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。 **说明** 当同步模式是“从目标仓库拉取”时有该参数。	library2 nginx-* **
触发模式	● 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

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。

- 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。

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

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**，在页面左上角切换Region到您所在的Region。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。镜像老化规则支持多个老化子规则组合生效。

约束与限制

每个命名空间下仅允许创建1个老化规则，每个老化规则至少包含1个子规则，至多包含15个子规则。

创建老化规则

步骤1 登录**容器镜像服务控制台**，在页面左上角切换Region到您所在的Region。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
触发模式	● 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。	-
子规则范围（镜像）	有如下两种模式： ● 正则输入模式 正则表达式规则可填写如 nginx-*，{repo1，repo2} 等 。 – *****：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。 – **{repo1，repo2, ...}**：同时匹配多个选项。 注意：不填或者填**默认为匹配全部。 ● 选择模式 可直接选择镜像。	nginx-*
子规则范围（版本）	镜像的版本，同样使用正则表达式匹配。 正则表达式规则可填写如 v1*，{v1，v2} 等。 ● *****：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。 ● **{v1，v2, ...}**：同时匹配多个版本。	v1
老化条件	选择执行的老化条件，有如下条件可选择： ● 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 其中“#”为变量，为具体的版本数和保留天数，请自行设置。	保留最近推送的10个镜像版本

参数名称	说明	示例
启用	可启用或不启用本条老化子规则	-
操作	可删除本条老化子规则	-

图 7-1 创建老化规则

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，匹配所有版本的所有镜像，保留符合最近推送的2个与最近拉取的5个的并集条件的镜像，其余镜像删除，且需要手动触发执行。

  示例解读：假设library命名空间空间下有10个镜像Image1 ~ Image10，其中Image9和Image10是最近推送的2个镜像，Image1~Image5是最近拉取的5个镜像，那么保留的就是Image1~Image5以及Image9和Image10，老化的是Image6~Image8。

- 示例2：

  选择library命名空间中，demo-image-v8和demo-image-v7保留最近3天被推送过的所有版本的镜像以及demo-image-v6和demo-image-v5保留最近1天被拉取过的镜像所有版本的镜像的并集，其余镜像全部删除，该规则每月1号 0时0分定时执行，且可以手动触发执行。

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。

- 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。

图 7-2 管理老化规则

- 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
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。
状态	任务完成状态。

参数	说明
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。
老化数	老化删除了多少个镜像，这里是按照镜像版本统计不是镜像制品。
创建时间	老化任务被触发的时间。
结束时间	老化任务执行结束的时间。
老化信息	老化了哪个命名空间下的哪些版本的镜像，删除是否成功。

图 7-3 任务详情

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**，在页面左上角切换Region到您所在的Region。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	**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。 正则表达式规则可填写如nginx-* 、{repo1, repo2} 等，其中： ● ***：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。 **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。	nginx-*
触发动作	触发器支持如下触发动作： ● 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	● 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。	-

参数名称	说明	示例
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

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。

- 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。

图 7-5 管理触发器

8 审计

8.1 支持云审计的关键操作

操作场景

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SWR相关的操作事件，便于日后的查询、审计和回溯。

支持审计的关键操作列表

表 8-1 云审计服务支持的企业版 SWR 操作列表

操作名称	资源类型	事件名称
创建实例	instance	createInstance
删除实例	instance	deleteInstance
创建命名空间	namespace	createNamespace
删除命名空间	namespace	deleteNamespace
修改命名空间	namespace	updateNamespace
删除镜像仓库	repository	deleteRepository
更新镜像仓库	repository	updateRepository
创建老化策略	retention	createRetention
修改老化策略	retention	updateRetention
删除老化策略	retention	deleteRetention
执行老化策略	retention	executeRetention

操作名称	资源类型	事件名称
删除触发器	triggerPolicy	deleteTriggerPolicy
创建触发器策略	triggerPolicy	createTriggerPolicy
修改触发器策略	triggerPolicy	updateTriggerPolicy
创建同步仓库	registry	createRegistry
删除同步仓库	registry	deleteRegistry
修改同步仓库	registry	updateRegistry
创建同步策略	replication	createReplicationPolicy
删除同步策略	replication	deleteReplicationPolicy
修改同步策略	replication	updateReplicationPolicy
执行同步策略	replication	executeReplicationPolicy
停止同步策略	replication	stopReplicationExecution
创建扫描策略	scan	createScanPolicy
删除扫描策略	scan	deleteScanPolicy
修改扫描策略	scan	updateScanPolicy
执行扫描策略	scan	executeScanPolicy
创建阻断策略	block	createBlockPolicy
删除阻断策略	block	deleteBlockPolicy
修改阻断策略	block	updateBlockPolicy
开启公网访问	endpointPolicy	enableEndpointPolicy
关闭公网访问	endpointPolicy	disableEndpointPolicy
更新公网访问白名单	endpointPolicy	updateEndpointPolicy
获取临时访问凭证	TempCredentialAuth	createTempCredentialAuthPolicy
创建长期访问凭证	LongTermCredentialAuth	createLongTermCredentialAuthPolicy
删除长期访问凭证	LongTermCredentialAuth	deleteLongTermCredentialAuthPolicy
启用/停用长期访问凭证	LongTermCredentialAuth	updateLongTermCredentialAuthPolicy
新增内网访问	IntranetEndpoint	createInternalEndpoint
删除内网访问	IntranetEndpoint	deleteInternalEndpoint
创建签名策略	signaturePolicy	createSignaturePolicy

操作名称	资源类型	事件名称
删除签名策略	signaturePolicy	deleteSignaturePolicy
修改签名策略	signaturePolicy	updateSignaturePolicy
执行签名策略	signaturePolicy	executeSignaturePolicy
上传chart包	Chart	uploadChart
删除chart仓库	Chart	deleteChart
删除chart版本	Chart	deleteChartVersion
创建委托	agency	createAgency
更新配额数据	quota	updateQuota
更新Harbor内部配额	quota	CACUpdateQuota
添加子资源标签	resourceTag	createResourceTags
删除子资源标签	resourceTag	deleteResourceTags
添加资源标签	tms	createResourceTags
删除资源标签	tms	deleteResourceTags
删除制品	artifact	deleteArtifact
创建不可变镜像规则	immutableRule	createImmutableRule
删除不可变镜像规则	immutableRule	deleteImmutableRule
修改不可变镜像规则	immutableRule	updateImmutableRule
增加域名	addDomainName	addDomainName
更新域名	updateDomainName	updateDomainName
删除域名	deleteDomainName	deleteDomainName
创建订单	instance	createOrder
删除任务	job	deleteJob

8.2 查看云审计日志

操作场景

开启了云审计服务（CTS）后，系统开始记录SWR相关的操作。CTS会保存最近1周的操作记录。

本小节介绍如何在CTS管理控制台查看最近1周的操作记录。

操作步骤

步骤1 登录CTS管理控制台，单击页面右上角“返回旧版”。

步骤2 选择左侧导航栏的“事件列表”，进入事件列表页面。

步骤3 事件记录了云资源的操作详情，设置筛选条件，单击“查询”。

当前事件列表支持四个维度的组合查询，详细信息如下：

- 事件类型、事件来源、资源类型和筛选类型。
  在下拉框中选择查询条件。其中，“事件类型”选择“管理事件”，“事件来源”选择“SWR”。

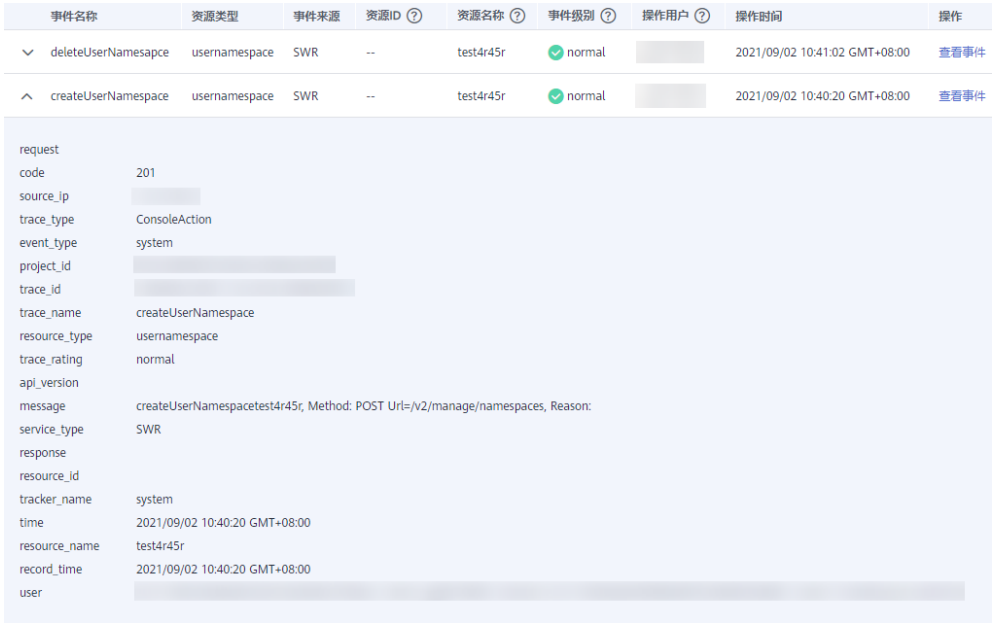
  图 8-1 设置筛选条件

  其中，筛选类型选择“按资源ID”时，还需手动输入某个具体的资源ID，目前仅支持全字匹配模式的查询。
  筛选类型选择“按资源名称”时，选框下拉列表会自动显示符合筛选条件的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选项为“最近1小时”、“最近1天”、“最近1周”和“自定义时间段”，本示例选择“最近1周”。

步骤4 在需要查看的事件左侧，单击 图标展开该事件的详细信息。

图 8-2 展开事件



步骤5 在需要查看的事件右侧，单击“查看事件”，弹出一个窗口，显示了该操作事件结构的详细信息。

关于云审计事件结构的关键字段详解，请参见**事件结构**。

----结束

