容器镜像服务

最佳实践（企业版）

文档版本 01

发布日期 2025-11-07

华为技术有限公司

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 通过 Cloud Custodian 自动增加镜像老化策略

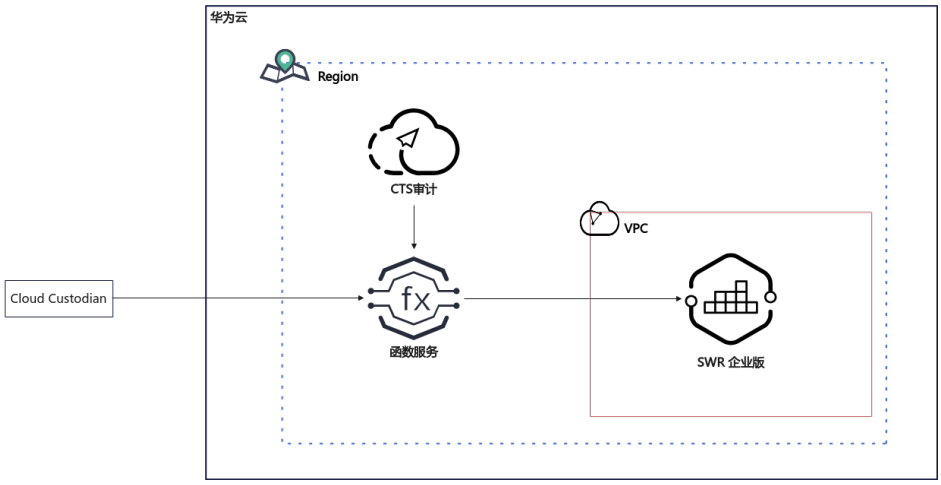
说明

该实践仅适用于容器镜像服务企业版。

当前很多企业会同时使用多个不同的云厂商提供的云服务。在这样的混合云环境中，除了各个云厂商提供的安全机制外，云基础设施还需要严格的云治理。容器镜像服务SWR是容器域中一个重要的服务，其安全性至关重要。必须对其进行监控以防存在任何访问和权限漏洞。

Cloud Custodian 提供了一套开源规则引擎，能够根据预定义的安全策略和合规要求，对云资源进行自动化检查和治理。可用于华为云容器镜像服务 SWR的资源的访问限制以及资源治理。借助 Cloud Custodian，您可设置规则，根据定义的安全和合规标准对环境进行验证。您可使用 Cloud Custodian 来管理您的云环境，帮助确保遵守安全政策、标签政策、未使用资源的垃圾回收和成本管理。借助 Cloud Custodian，其统一的治理界面使企业在混合云环境中能够轻松实施一致的安全策略和运营规范。

图 1-1 使用 Cloud Custodian 对 SWR 服务进行监管的架构



架构图中的服务是我们使用Cloud Custodian必须依赖的服务：

- CTS审计：即云审计服务，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。
- FunctionGraph：函数工作流FunctionGraph是华为云提供的一款无服务器（Serverless）计算服务，作为事件驱动型的函数托管平台，用户只需编写业务函数代码并设置运行的条件，无需配置和管理服务器等基础设施，函数以弹性、免运维、高可靠的方式运行。
- SWR企业版：SWR企业版作为容器镜像服务的企业版，为用户提供企业级专属安全托管服务，支持托管容器镜像、Helm Chart等符合OCI标准的云原生制品。

操作步骤

步骤1 安装Python运行环境。此为Cloud Custodian依赖的运行环境。

说明

python建议使用Python 3.11版本，建议使用虚拟环境进行开发。

如果使用原生Python 3.11，使用以下命令创建和激活虚拟环境。其他版本Python请根据Python官方文档进行安装。

```
# 创建虚拟环境
python -m venv custodian
# 激活虚拟环境（Linux）
source custodian/bin/activate
# 激活虚拟环境（Windows）
custodian\Scripts\activate.bat
如果使用Conda或者Miniconda，也可以使用以下命令创建和激活虚拟环境：
# 创建虚拟环境
conda create -n custodian python=3.11
# 激活虚拟环境
conda activate custodian
```

步骤2 安装Cloud Custodian。

1. 下载Cloud Custodian
   ```
   git clone https://github.com/huaweicloud/cloud-custodian.git
   cd cloud-custodian
   ```
2. 安装python依赖
   ```
   pip install -e .
   pip install -e tools/c7n_huaweicloud/.
   ```

更详细的安装指导请参考 **Cloud Custodian 官方文档**。

步骤3 执行下述命令检查cloud custodian是否安装正常。

```
custodian schema huaweicloud.swr-ee
```

回显如下表示安装成功


```
$ custodian schema huaweicloud.swr-ee

Help
----

Huawei Cloud SWR Enterprise Edition Resource Manager.

This class manages SWR Enterprise Edition repositories on HuaweiCloud.
It provides functionality for discovering, filtering, and managing SWR repositories.

huaweicloud.swr-ee:
  actions:
  - notify-message
  - notify-message-structure
  - notify-message-template
  - webhook
  filters:
  - age
  - event
  - exempted
  - list-item
  - reduce
  - restricted
  - value

(custodian)
```

步骤4 定义Cloud Custodian策略，策略如下：

```
policies:
  - name: swr-ee-event
    resource: huaweicloud.swr-ee-namespace
    mode:
      type: cloudtrace
      xrole: fgs_default_agency
      events:
        - source: 'SWR.namespace'
          event: 'createNamespace'
          ids: 'resource_name'
    actions:
      - type: set-lifecycle
        rules:
          - template: latestPushedK
            params:
              latestPushedK: 50
            scope_selectors:
              repository:
                - kind: doublestar
                  pattern: '**'
            tag_selectors:
              - kind: doublestar
                decoration: matches
                pattern: '**'
```

说明

当你在SWR企业版上新建一个命名空间的时候，该策略会自动在该命名空间上设置老化策略，老化策略为保留最近推送的50个制品版本。

下面给出如下两种场景的策略参考以供您参考：

策略1：查询超过创建时间90的镜像仓库：

```
policies:
  - name: swr-ee-repos
    resource: huaweicloud.swr-ee
    filters:
      - type: age
        days: 90
        op: gt
```

策略2：制品Tag匹配release*的设置镜像不可变规则:

```
policies:
  - name: swr-ee-set-immutability-rules
    resource: huaweicloud.swr-ee-namespace
    actions:
```



```
- type: set-immutability
  state: True
  scope_selectors:
    repository:
      - kind: doublestar
        pattern: '**'
  tag_selectors:
    - kind: doublestar
      decoration: matches
      pattern: '{release*}'
```

如果想要了解更多的策略配置请参考 **Cloud Custodian 官方文档**。

步骤5 执行Custodian命令启用策略。

1. 执行策略之前请先在Terminal中配置环境变量，以下为linux环境下的配置命令，windows环境下的配置只需将export改为set即可。

```
# 配置华为云账号ak/sk
export HUAWEI_ACCESS_KEY_ID={your-ak}
export HUAWEI_SECRET_ACCESS_KEY={your-sk}
# 配置资源默认所在region，例如ap-southeast-1，可从网页URL中获取
export HUAWEI_DEFAULT_REGION={your-region}
```

2. 执行custodian run命令启用策略。

```
custodian run --output-dir=<output_directory> <policy_name>.yaml
```

----结束

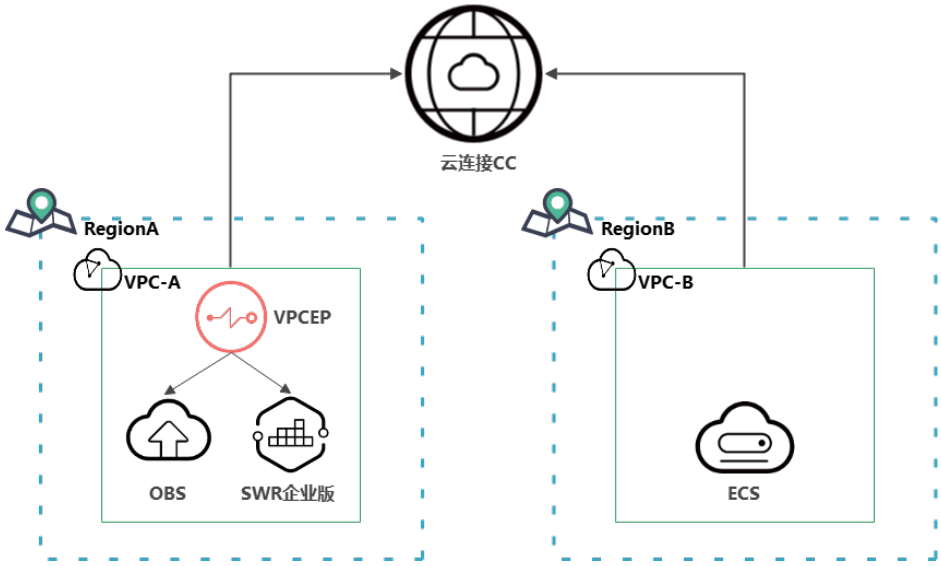
2 跨地域通过华为云内网访问 SWR 企业版仓库实例

操作场景

当您需要跨地域推送或拉取 SWR 企业版镜像时，需要让源端 VPC 与目标 SWR 企业版仓库实例的 VPC 网络互通，可以通过以下步骤实现：

1. **通过云连接配置跨区域网络互通**。
2. **获取打通网络所需信息**。
3. **配置访问OBS服务的VPCEP**。
4. **云连接中配置转发OBS的IP网段**
5. **配置到目标企业仓库的内部域名解析**。
6. **验证可跨地域下载镜像**。

完成以上配置后，您即可通过源端 VPC 推送或拉取目标地域的 SWR 企业版镜像，实现异地无缝访问。



下面以一个示例来演示如何实现同一个租户下，使用华东-上海一下的ECS1节点跨地域访问华南-广州局点的SWR企业版仓库实例。环境信息如下：

- vpc-10
  - 地域：华东-上海一
  - IPv4网段：10.0.0.0/8
  - ECS1地址：10.0.0.10（ECS1用于验证上传下载镜像）
- vpc-default
  - 地域：华南-广州
  - IPv4网段：192.168.0.0/16
  - ECS2地址：192.168.0.18（ECS2用于探测OBS域名的IP）
  - 企业仓库实例的访问IP: 192.168.0.17

约束与限制

ECS1节点已安装Docker或者containerd容器引擎客户端。

操作步骤

步骤1 配置跨区域网络互通。

请参考**同账号下跨区域的VPC互通**，通过云连接CC的方式打通华东-上海一vpc-10与华南-广州的的vpc-default之间的网络。

步骤2 获取要访问的目标企业仓库实例的域名访问地址、OBS桶名以及IP信息。

1. 登录**容器镜像服务控制台**，切换到华南-广州区域。
2. 单击左侧菜单栏的“企业版”，在新打开的“仓库管理”页面，单击仓库名称进入仓库详情页面。
3. 在总览页面获取访问地址与OBS桶名。

4. 依次单击“访问管理->访问控制->内网访问”，找到所属VPC列的值为vpc-default的记录，记录IP列的值。
5. 获取OBS Bucket在vpc-default中的IP。

使用ping命令获取相应的OBS域名对应的IP并记录，多ping几次可以获取得到obs域名的多个IP。

表 2-1 获取的目标仓库实例的信息记录

企业仓库实例ID	桶名称	企业仓库实例域名(IP)	OBS域名(IP)
${instance-id}	swr-ee-${instance-id}-registry	xxx.swr-pro.myhuaweicloud.com（192.168.0.17）	swr-ee-${instance-id}-registry.obs.${region-id}.myhuaweicloud.com（100.*.*.6、100.*.*.7）

步骤3 创建访问OBS服务的VPCEP。

1. 登录**管理控制台**。
2. 在管理控制台左上角单击图标，区域选择华南-广州。
3. 单击左上角图标，选择“网络”>“VPC终端节点”。
4. 在终端节点页面，单击“购买终端节点”，服务类别选择“云服务”，选择服务参数请勾选名称com.myhuaweicloud.{region_id}.swr的选项。如果选不到，服务类别请选择择“按名称查找服务”进行查找。其他参数根据需要填写。
   - 服务名称：根据企业仓库实例的OBS桶名，请**提交工单**或联系OBS服务运维人员获取“网关”型的OBS终端节点服务名称。然后输入OBS终端节点服务名称，单击“验证”确认生效。
   - 虚拟私有云：选择vpc-default。
   - 路由表：使用vpc-default的默认路由表。

步骤4 云连接中配置转发OBS的IP网段。

1. 从vpc-default 路由表查看 VPCEP 访问OBS的路由信息。

   在VPCEP终端节点控制台，区域选择华南-广州，进入“虚拟私有云-路由表” 页面。找到类型为“默认路由表”，名称为rtb-vpc-default的记录，单击名称后在新打开的页面找到下一跳类型列为VPC终端节点的记录。

2. 单击IP地址数列的数字链接，可以查询出来所有的访问OBS的IP网段。请记录目的地址列的值。

3. 登录**管理控制台**，在管理控制台左上角单击图标，区域选择华东-上海一。单击左上角图标，选择“网络”>“云连接 CC”。单击**步骤1**创建的CC连接，进入网络实例页签，单击vpc-default下的“修改VPC CIDR”。

4. 单击“其他网段”，把OBS的ip网段（即**2**中查询出来的）增加到其他网段中。

步骤5 在华东-上海一局点对vpc-10配置到目标企业仓库实例域名以及OBS域名的内部域名解析。

1. 进入**内网域名列表页面**。
2. 请单击管理控制台左上角的图标，区域选择华东-上海一。
3. 在页面右上角，单击“创建内网域名”。
4. 在“创建内网域名”页面中，配置一条到目标企业仓库实例域名的内部域名解析规则。
5. 输入目标企业仓库的域名及相关参数。详细添加域名指导请参考**创建内网域名**。

   域名：xxx.swr-pro.myhuaweicloud.com

   区域：华东-上海一

   VPC: vpc-10

   配置完成后进入配置的内网域名详情页面，依次单击“管理解析->添加记录集”，添加目标仓库实例IP记录值：上述示例中该值为192.168.0.17。
6. 重复**4**和**5**再配置一条到OBS域名的内部域名解析规则。

   域名：swr-ee-${instance-id}-registry.obs.${region-id}.myhuaweicloud.com

   区域：华东-上海一

   VPC: vpc-10

   配置完成后进入配置的内网域名详情页面，依次单击“管理解析->添加记录集”，添加OBS的IP记录值：上述示例中该值为100.*.*.6和100.*.*.7。

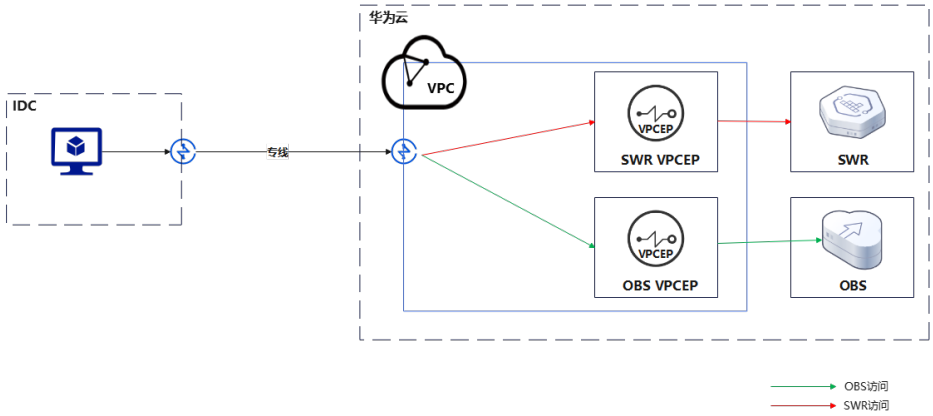
步骤6 登录华东-上海一下的ECS1节点，验证可成功下载华南-广州下的镜像仓库中的镜像。

----结束

3 云下数据中心 IDC 通过华为云内网访问 SWR 企业版仓库实例

操作场景

如有您的云下数据中心想要访问SWR企业版，那么您可以使用专线或VPN方式与VPC连接后，通过终端节点实现高速访问华为云服务，无需经过公网，提高用户的访问效率。



前提条件

- 已创建VPC，详细步骤请参考**创建虚拟私有云和子网**。
- 已购买VPC终端节点，详细步骤请参见**购买终端节点**。
- 已创建云专线或者虚拟专有网络使得数据中心能通过专线/VPN连接VPC，详细步骤请参考**云专线**或**VPN**。

操作步骤

步骤1 获取SWR企业版仓库实例的域名与IP。

1. 登录**容器镜像服务控制台**，选择您所在的区域。
2. 单击左侧菜单栏的“企业版”，在新打开的“仓库管理”页面，单击仓库名称进入仓库详情页面。
3. 在总览页面获取仓库实例的访问地址，记录访问地址的值。即SWR企业版仓库实例的访问域名。

4. 依次单击“访问管理->访问控制->内网访问”，记录IP列的值。即SWR企业版仓库实例的内网访问IP。

步骤2 在用户本地数据中心节点上配置hosts，具体配置hosts的方式有如下2种：

直接配置/etc/hosts文件

自定义DNS Hosts（推荐）

表 3-1 配置 hosts 的 2 种方式对比

配置方式	适用场景	配置优缺点
直接配置/etc/hosts文件	适用于您的本地数据中心IDC没有DNS解析服务器	**优点**：不需要用户本地数据中心部署有DNS服务器。 **缺点**：需要在用户本地数据中心的每一个节点上进行配置。 配置不够便捷。
自定义DNS Hosts（**推荐**）	适用于您的本地数据中心IDC已有DNS解析服务器	**优点**：仅需在用户本地数据中心的DNS服务器配置一次。 配置便捷。 **缺点**：需要用户本地数据中心部署有DNS服务器。

- **直接配置/etc/hosts文件**

  Linux操作系统配置步骤如下：

  a. 登录用户本地数据中心节点，运行以下命令，打开/etc/hosts。
  ```
  sudo vim /etc/hosts
  ```
  b. 添加自定义域名，hosts地址由两部分组成，节点IP和内网域名。如：xx.xx.xx.xx xxxx.swr-pro.myhuaweicloud.com。

  说明

  xx.xx.xx.xx为4中查询到的节点IP，xxxx.swr-pro.myhuaweicloud.com为3中查询到的仓库实例访问地址。

  c. 配置完成后执行如下命令重启网络。
  ```
  sudo/etc/init.d/networking restart
  ```

- **自定义DNS Hosts**。

  在用户本地数据中心的DNS服务器配置相应的DNS转发规则。

  不同操作系统中配置DNS转发规则的方法不同，具体操作请参考对应DNS软件的操作指导。

  下文以Linux操作系统，常见的DNS软件Bind为例介绍：

  a. 配置/etc/named.conf，新增zone：
  ```
  zone " xxxx.swr-pro.myhuaweicloud.com " IN {
    type master;
    file " /var/named/xxxx.swr-pro.myhuaweicloud.com.zone";
  };
  ```


说明

xxxx.swr-pro.myhuaweicloud.com为3中查询到的仓库实例访问地址。

b. 配置自定义的域名到IP的正向解析配置。新建一个a中file对应的文件：/var/named/xxxx.swr-pro.myhuaweicloud.com.zone

```
$TTL    604800
@ IN     SOA     xxxx.swr-pro.myhuaweicloud.com. root.localhost. (
                      2         ; Serial
                 604800         ; Refresh
                  86400         ; Retry
                2419200         ; Expire
                 604800 )       ; Negative Cache TTL
;
@    IN   NS   xxxx.swr-pro.myhuaweicloud.com.
xxxx.swr-pro.myhuaweicloud.com.    IN   A     xx.xx.xx.xx
```

c. 执行如下命令重启服务。

```
/sbin/service named restart
```

说明

- 您可以从地区和终端节点中查询不同区域SWR的Endpoint信息。
- 用户本地数据中心若无DNS服务器，需要将连接DNS服务的终端节点的节点IP增加到用户本地数据中心节点的/etc/resolv.conf文件中。

步骤3 验证配置是否成功。

登录您的本地数据中心IDC中的任一节点后台，执行命令：ping xxxx.swr-pro.myhuaweicloud.com，查看返回结果。

- 成功：显示类似 Reply from ... 的消息，表示可以ping通。后续通过域名:xxxx.swr-pro.myhuaweicloud.com访问SWR即可。
- 失败：显示 Request timed out 或 Destination host unreachable，请提交工单联系华为运维工程师解决。

----结束

注意

上述配置仅可实现通过容器镜像服务上传镜像，当您需要下载镜像时，您还需要配置访问OBS服务内网地址的终端节点。

4 企业版仓库实例的异地容灾

4.1 使用 SWR 企业版仓库实例实现自建 Harbor 实现异地容灾

如果您需要对您的Harbor进行异地容灾，那么可通过SWR企业版仓库实例来实现。您可使用Harbor的远程复制功能将A局点自建Harbor上的镜像制品复制到B局点的SWR企业版仓库实例中，当您的Harbor异常的时候可以通过拉取SWR企业版复制的镜像制品实现异地容灾。具体可通过以下步骤实现：

1.Harbor同步镜像至SWR企业版仓库实例

2.配置自定义域名实现异地容灾

前提条件

- 已购买容器镜像服务企业版仓库实例。具体操作，请参见**购买仓库**。
- 已自行搭建Harbor。并且已打通Harbor和容器镜像服务企业版仓库实例之间的网络。
- 容器镜像服务企业版仓库实例的自定义域名与配置的与Harbor的域名一致。如何配置自定义域名，请参见**通过自定义域名访问容器镜像服务企业版仓库实例**。

操作步骤

1. **Harbor同步镜像至SWR企业版仓库实例**

步骤1 创建命名空间

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。
2. 在左侧导航栏单击“命名空间”。在右上角单击“创建命名空间”。
3. 命名空间名称填入Harbor中需要同步的项目名称，并选择命名空间类型。
4. 单击“确定”。

步骤2 在Harbor上配置目标镜像仓库

1. 新建目标并填写参数。

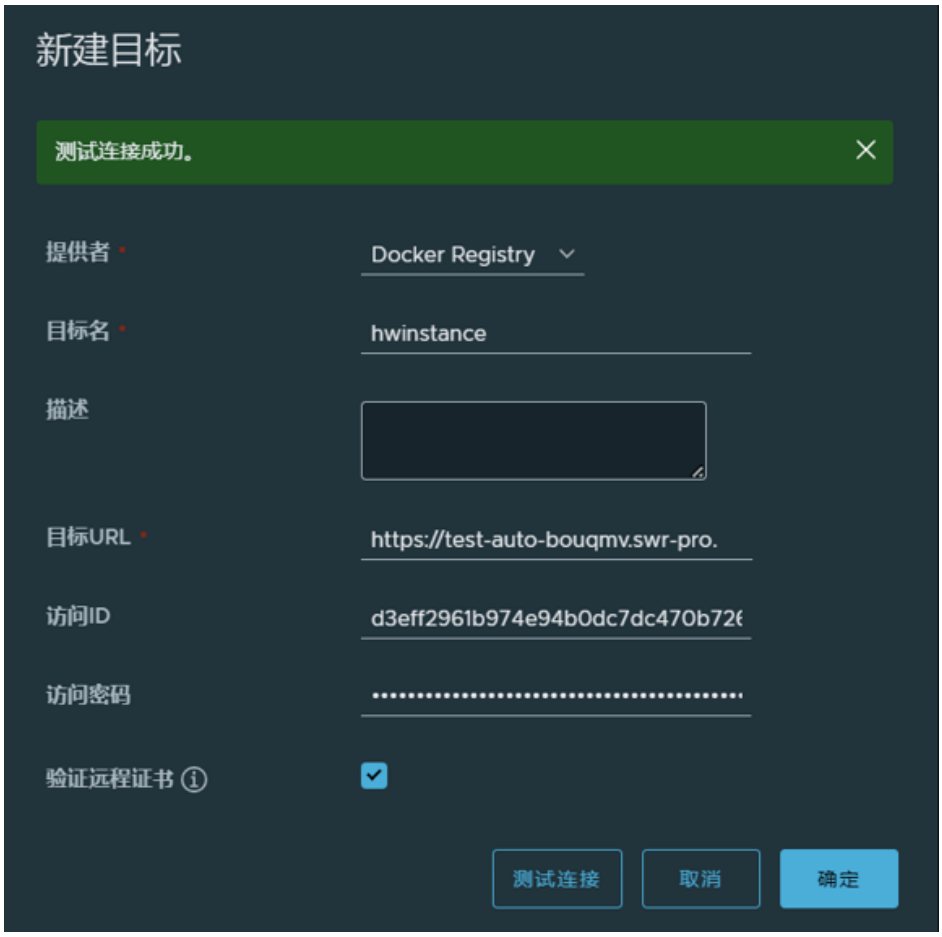


表 4-1 新建目标参数解释

参数	说明
提供者	选择Docker Registry。
目标名	自定义填写。
描述	自定义填写。
目标URL	填写SWR企业版仓库实例目标仓库域名地址，格式为https://{*SWR镜像仓库地址*}。 镜像仓库地址获取方法：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，单击仓库名称进入仓库详情页面，在“总览-基本信息”页面获取访问地址。
访问ID	访问镜像仓库实例的用户名，获取方法见**获取长期访问凭证**中的下载的表格中的用户名的值。
访问密码	访问镜像仓库实例的密码，获取方法见**获取长期访问凭证**中的下载的表格中的密码的值。

参数	说明
验证远程证书	建议取消勾选。

步骤3 配置同步规则。

1. 在左侧系统管理-复制管理页面新建规则。

2. 填写如下参数。

表 4-2 新建复制规则参数解释

参数	说明
名称	自定义。
描述	自定义。
复制模式	选择Push-based。表示把镜像由本地Harbor推送到远端仓库。
源资源过滤器	根据填写的规则过滤Harbor上的镜像。默认为全部资源。
目标仓库	选择择2.1创建的目标。
目标	填写1.1创建的命名空间名称,仓库扁平化用以在复制镜像时减少仓库的层级结构，推荐选择替换1级。

参数	说明
触发模式	自定义。建议选择事件驱动。
带宽	设置执行该条同步规则时的最大网络带宽，“-1”表示无限制。
覆盖	如果存在具有相同名称的资源，请指定是否覆盖目标上的资源。

更详细的参数解释请参考**Harbor官网文档**。

步骤4 创建完成后，选中后单击“复制”即可完成同步。

----结束

2. **配置自定义域名实现异地容灾**

根据Harbor和容器镜像服务企业版仓库实例部署位置的网络关系，给出下面三种场景。

以SWR企业版仓库实例在广州，Harbor实例在上海为示例分下述三种场景进行说明。

表 4-3 异地容灾场景

场景	场景描述	实现异地容灾的方案
场景一	Harbor部署在华为云，业务通过公网访问SWR企业版仓库实例	若位于上海的Harbor发生故障导致无法推拉镜像，您可以通过修改自定义域名解析实现拉取位于广州的SWR企业版仓库实例。 具体操作方式如下。 1. 登录**云解析服务 DNS控制台**。切换到上海region。 2. 在左侧导航栏选择内网域名。 3. 找到您给swr企业版仓库实例配置的自定义域名记录，单击关联您的VPC的那条实例记录。 4. 在解析设记录页签，单击目标记录名称的超链接。 5. 在修改记录对话框，设置参数。单击确定。 • 记录类型：选择CNAME。 • 主机记录：输入自定义域名的前缀。 • 记录值：设置为广州的SWR企业版仓库实例的默认域名。 • TTL时间：默认值即可。

场景	场景描述	实现异地容灾的方案
场景二	Harbor未部署在华为云，业务通过公网访问SWR企业版仓库实例	若自建的Harbor发生故障导致无法进行镜像的推送或拉取操作，请按照以下步骤进行处理： 1. 通过公网访问SWR企业版仓库实例。更多内容请参见**通过公网访问SWR企业版仓库实例**。 2. 需要修改域名解析，解析到SWR企业版仓库实例的公网IP。 3. 将SWR企业版仓库实例的自定义域名设置为自建Harbor使用的域名。
场景三	Harbor未部署在华为云，业务通过专有网络访问SWR企业版仓库实例	若自建Harbor服务出现故障导致无法进行镜像的推送或拉取操作，请按照以下步骤进行处理： 1. 首先获取SWR企业版仓库实例的IP地址。 2. 配置路由规则和域名解析设置。 3. 将自建Harbor使用的域名解析指向SWR企业版仓库实例的IP地址。

4.2 使用 SWR 企业版多地域实例实现异地容灾

如果您需要对A局点的SWR企业版某镜像仓库实例的镜像制品设置异地容灾，那么可以通过将A局点的镜像制品同步推送到B局点的另一SWR企业版仓库实例来实现。

前提条件

- A局点已购买容器镜像服务企业版仓库实例S1,B局点已购买容器镜像服务企业版仓库实例S2。具体操作，请参见**购买仓库**。
- 两个局点两个SWR企业版仓库实例已配置了相同的自定义域名。如何配置自定义域名，请参见**通过自定义域名访问容器镜像服务企业版仓库实例**。

操作步骤

步骤1 配置两企业仓库实例的镜像同步规则

分别为企业版仓库实例S1和S2实例配置镜像同步规则。具体操作，请参见**镜像同步**。

步骤2 配置两企业仓库实例的访问控制

- 两个实例之间通过内网访问，需要为实例配置内网访问。
- 两个实例之间通过公网访问，需要为实例配置公网访问。具体操作，请参见**公网访问**。

步骤3 切换域名解析实现容灾

若S1实例出现异常无法推拉镜像时，您可以通过修改使用VPC对应的自定义域名解析来实现跨地域拉取实例S2的同镜像。具体操作如下。

1. 登录**云解析服务 DNS控制台**。切换到A局点。
2. 在左侧导航栏选择内网域名。

3. 找到您给SWR企业版仓库实例配置的自定义域名记录，单击关联您的VPC的那条实例记录。
4. 在解析设记录页签，单击目标记录名称的超链接。
5. 在修改记录对话框，设置参数。单击确定。

表 4-4 修改记录集

参数	说明
记录类型	– 如果您两个实例之间通过公网访问，选择CNAME。 – 如果您两个实例之间通过内网访问，选择A。
主机记录	输入自定义域名的前缀。
记录值	– 如果您两个实例之间通过公网访问，请设置为实例S2的公网域名。 – 如果您两个实例之间通过内网访问，请设置为实例S2所在的VPC中的内网地址。
TTL时间	默认值即可。

----结束