容器镜像服务

实践教程

产品文档

腾讯云

文档目录

实践教程
个人版迁移
个人版迁移至企业版完全指南

最近更新时间：2023-02-17 11:08:09

操作场景

当前容器镜像服务 TCR 同时提供个人版服务和企业版服务。个人版服务面向个人开发者，仅提供容器镜像存储分发的基础功能。企业版服务可为企业客户提供安全、独享的高性能云原生应用制品托管分发服务。个人版与企业版服务区别可参见 规格说明。
本文主要介绍企业客户如何将容器镜像数据及业务配置从个人版迁移至企业版，实现业务的平滑迁移。

前提条件

从个人版服务迁移至企业版，您需要确认并完成以下准备工作：
已开通并使用个人版服务，且迁移操作账号具有拉取个人版镜像仓库内所有镜像的权限，请参考 个人版授权方案示例 提前为子账号授予个人版的全部管理权限。
已 购买企业版实例，且迁移操作账号具有向该企业版实例内推送镜像的权限，请参考 企业版授权方案示例 提前为子账号授予对应实例的容器镜像、Helm Chart 推送权限，建议将容器镜像服务全读写权限授予配置同步的子账号。
已设置迁移工具运行的运行环境。建议在私有网络 VPC 内执行该迁移任务，以提升迁移速度，并避免公网流量成本。
在私有网络 VPC 内运行迁移工具：在目标企业版实例的内网访问中添加迁移工具运行服务器所在的私有网络。详情可参见 内网访问控制。
在公网环境内运行迁移工具：开启目标企业版实例的公网访问入口，并放通访问来源。详情可参见 公网访问控制。

数据迁移

准备基础运行环境

1. 在实际容器业务的主要部署地域购买企业版实例。
2. 在同地域内准备一台用于镜像迁移的云服务器 CVM，并尽量选择 CPU/内存配置高、内网带宽高的机型。云服务器启动后，安装最新 Docker 客户端，或选择已安装 Docker 的操作系统。
3. 将 CVM 所在 VPC 接入至该企业版实例，并开启自动内网解析，详情可参见 内网访问控制。

4. 获取该实例的访问凭证，并在迁移专用 CVM 上执行 `Docker Login`，确认在该 CVM 上可通过内网正常访问该实例并登录成功。

准备迁移配置信息

1. 获取镜像仓库访问凭证

个人版镜像仓库访问凭证：用户名为需迁移镜像所属腾讯云账号 UIN，密码为初始化个人版服务时所设置密码。如忘记密码，可前往 容器镜像服务控制台 > **实例列表**，选择个人版实例，进入更多中单击**重置登录密码**来重置密码。

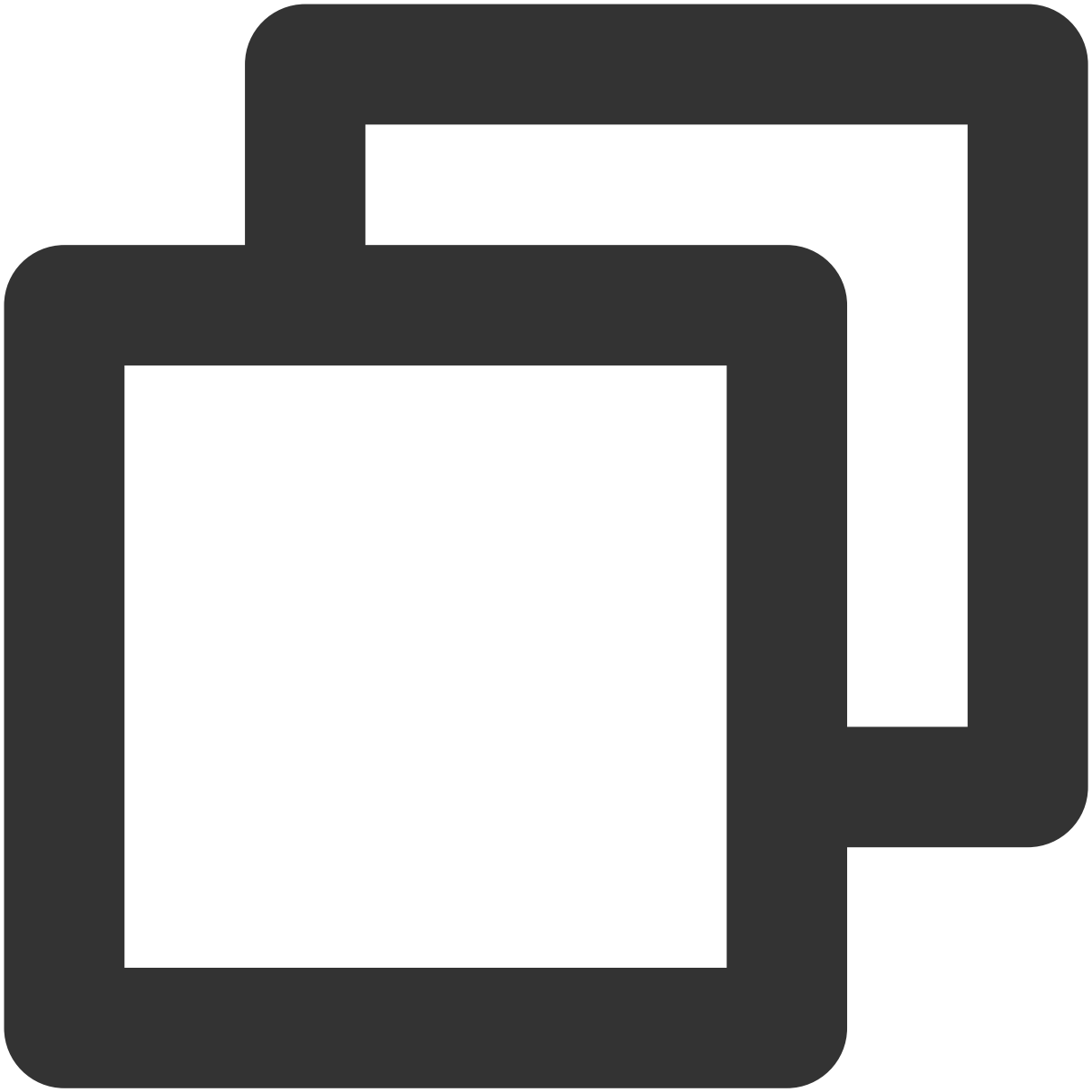
企业版镜像仓库访问凭证：可前往 容器镜像服务控制台 > **访问凭证**，选择已创建的企业版实例，单击**新建**，生成迁移专用的长期访问凭证，已包含用户名及密码。请注意，生成该访问凭证用户需具备该实例的全读写权限。

2. 获取 API 调用凭证

迁移镜像过程中将自动在企业版实例内新建命名空间及镜像仓库，需调用腾讯云 API 完成该操作。您可前往访问管理控制台 > **访问密钥** > **API密钥管理** 新建密钥或查看已有密钥。请谨慎保管该密钥信息。

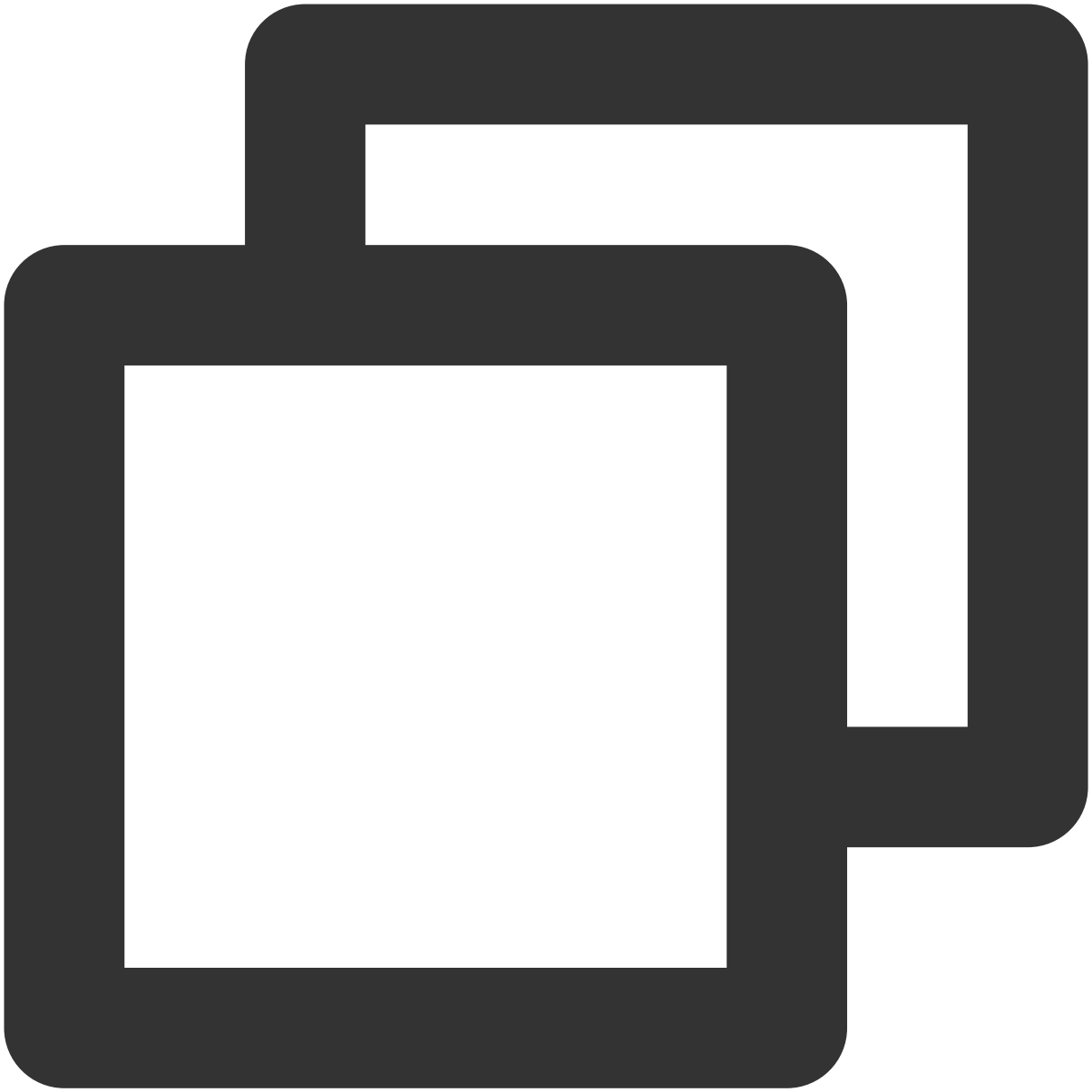
下载并执行迁移工具

执行如下命令，下载迁移专用容器镜像：



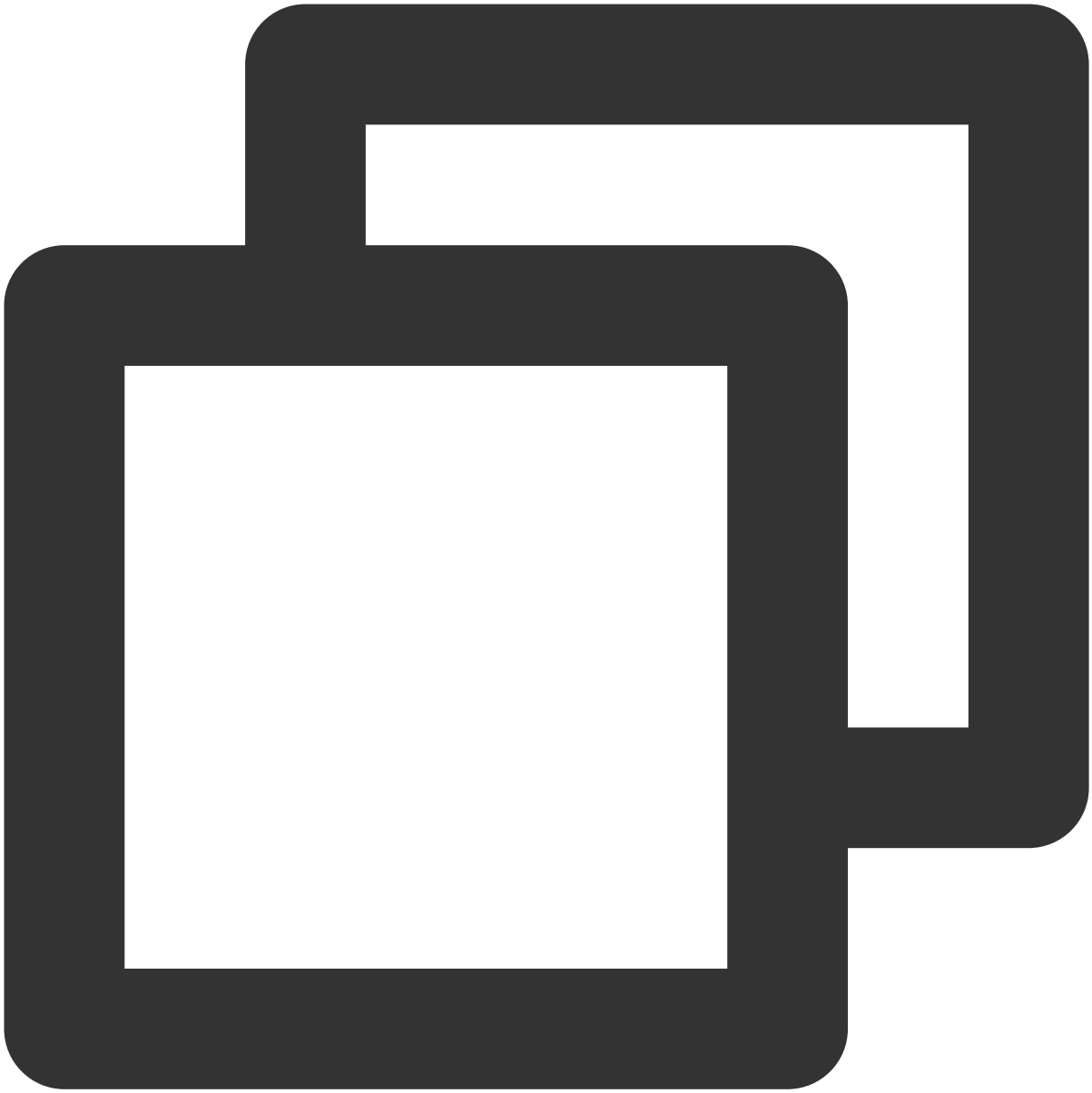
```
docker pull ccr.ccs.tencentyun.com/tcrimages/image-transfer:ccr2tcr
```

执行如下命令，查看该工具使用说明：



```
docker run --network=host --rm ccr.ccs.tencentyun.com/tcrimages/image-transfer:ccr2
```

执行如下命令，修改配置信息，并正式执行迁移任务：



```
docker run --network=host --rm ccr.ccs.tencentyun.com/tcrimages/image-transfer:ccr2
```

参数说明

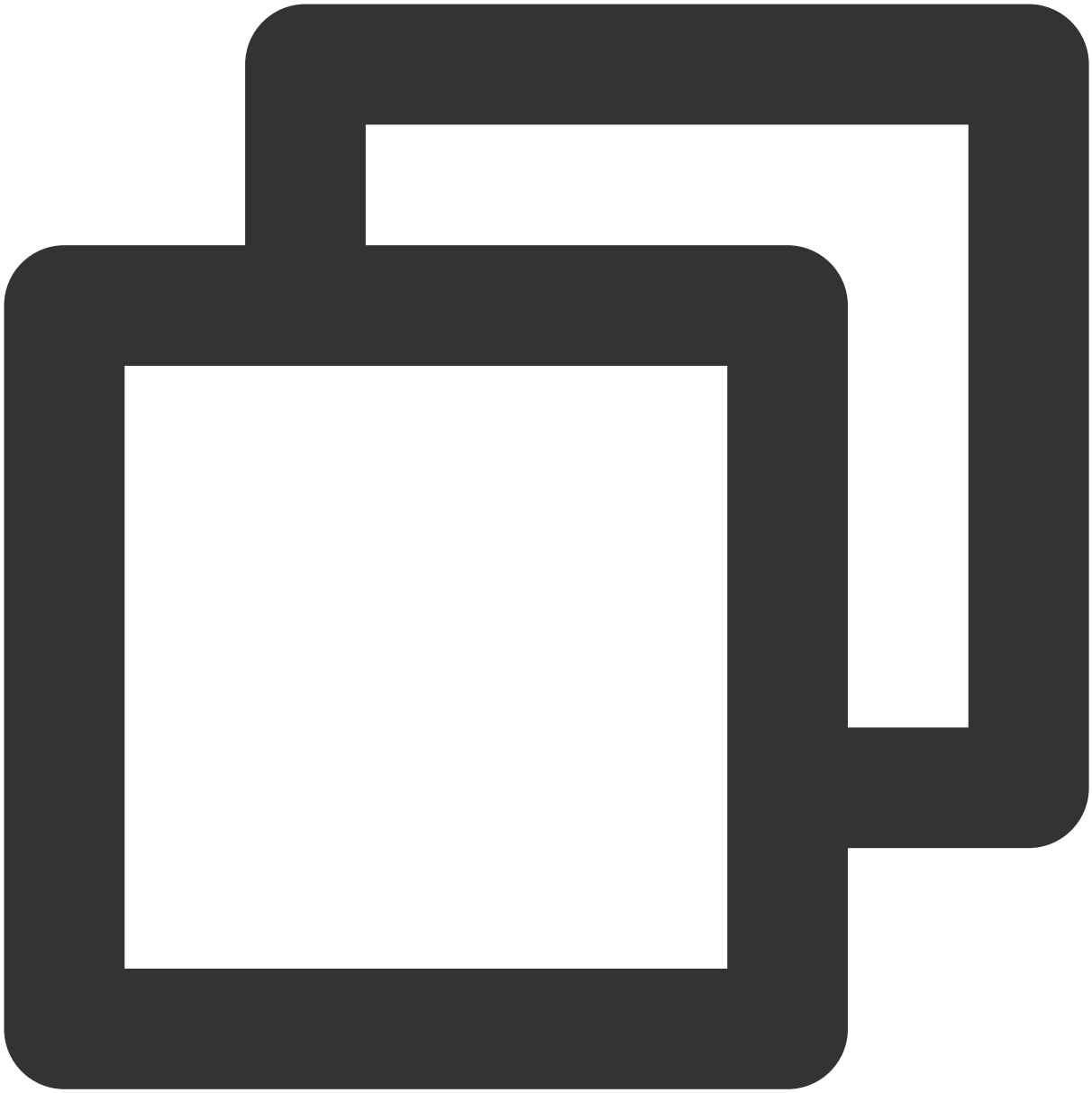
参数	参数说明
tcrName	目标迁移企业版实例的名称
ccrRegionName、ccrRegionName	实例地域，ccr 国内默认为 ap-guangzhou, tcr 需按照实际地域填写，例如 ap-shanghai

ccrAuth、tcrAuth	镜像仓库访问凭证，格式：username:password,如 username、password 中包含特殊字符，需要进行转义处理，如 ? 应写为 \\?
ccrSecretId、ccrSecretKey、tcrSecretId、tcrSecretKey	腾讯云 API 调用密钥，如果是同账号下迁移，ccr 及 tcr 调用密钥相同
tagNum	指定仅迁移镜像仓库内最新 N 个版本镜像

查看及确认运行结果

因个人版迁移至企业版默认使用全量迁移模式，迁移时间直接与当前个人版内镜像仓库数量及大小有关，请耐心等待。

若运行后展示如下代码，即表示全量迁移成功。否则请重新运行该迁移工具进行重试。您可以通过 提交工单 申请协助。



```
################## Finished, 0 transfer jobs failed, 0 normal urlPair generate faile
```

业务迁移

网络环境切换

容器镜像服务个人版无网络访问控制功能，国内地域内服务器默认均可内网访问该服务。容器镜像服务企业版支持网络访问控制，需将集群所在 VPC 接入实例内，允许内网访问。

个人版网络配置：无需配置，默认所有网络环境均可访问该服务，上传/下载镜像。
企业版网络配置：
内网访问（推荐）：主动将集群或弹性集群所在 VPC 接入目标实例，并开启 VPC 内自动解析或自行管理 DNS 解析，详情可参见 内网访问控制。
公网访问：不建议开启，建议仅在测试时，或有面向外部团队分发镜像时开放，且配置访问白名单。

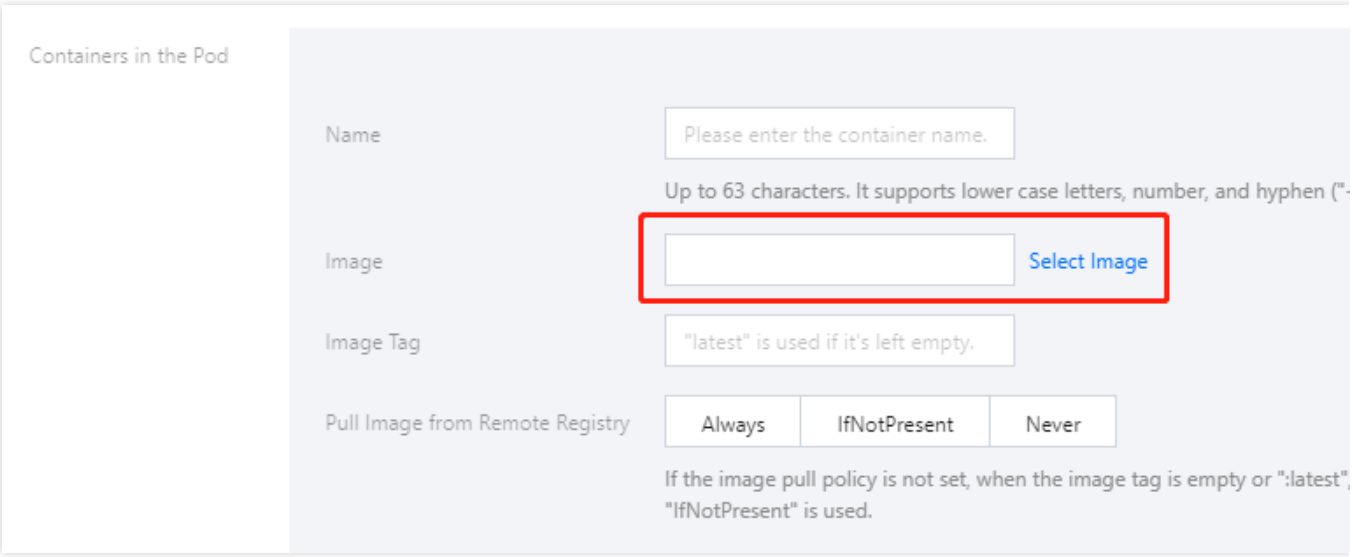
复用个人版镜像配置

可参考子目录文档：**使用个人版域名访问企业版实例**，使用此功能将无需变更 TKE 集群、CI/CD 平台内已有镜像仓库地址及访问凭证配置，方便客户最小成本切换至企业版服务。
长期使用，建议逐渐将个人版访问配置切换至企业版配置，避免后续因个人版服务变更导致访问异常。

使用企业版镜像配置

访问地址切换

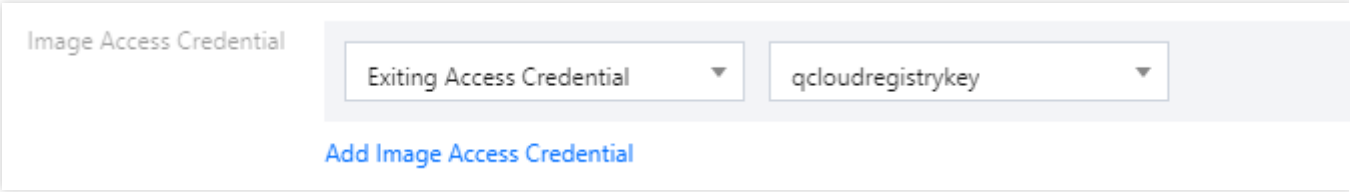
进入集群或弹性集群的详情页，选择左侧的“工作负载”，并选择新建/更新工作负载，在“实例内容器”中选择/填写镜像地址，或直接修改 YAML 中 **image** 参数。如下图所示：



个人版地址：默认为 `ccr.ccs.tencentyun.com/namespace/repo:tag` ，默认地域服务覆盖除中国香港以外的其他国内可用地域，如北京、上海、广州等，中国香港前缀域名为 hkccr。不支持多级路径。
企业版地址：可自定义实例名 `user-define` ，例如 `user-define.tencentcloudcr.com/namespace/repo:tag` 。支持自定义域名，例如 `xxx-company.com/namespace/repo:tag` 。支持多级路径，镜像地址可为 `xxx-company.com/ns/sub01/sub02/repo:tag` 。

访问凭证切换

进入集群或弹性集群的详情页，选择左侧的“工作负载”，并选择新建/更新工作负载，在“镜像访问凭证”中切换访问凭证，或直接修改 YAML 中 **imagePullSecret** 参数。如下图所示：



个人版访问凭证：新建命名空间默认会下发个人版访问凭证，即 **qcloudregistrykey**，选择该凭证即可。
企业版访问凭证：
推荐方案：使用 TCR 企业版专用插件自动下发并配置访问凭证，实现免密拉取。此方案无需配置镜像访问凭证，请将此参数已有值删除，保持为空。（仅支持 TKE）
手动配置：可在 TCR 企业版实例内创建长期访问凭证，并下发至命名空间内，或在创 建工作负载时新建镜像访问凭证。

企业版入门最佳实践

本文档仅面向个人版迁移至企业版场景提供部分最佳实践说明。

多实例规划

可根据实际业务需要，在多个地域内创建一个或多个实例，并配置同步复制策略，并使用自定义域名统一管理实例访问地址。详情可参见 TCR 企业版实例同步， TCR 企业版实例复制，从自建 Harbor 同步镜像到 TCR 企业版。

安全合规

操作合规
建议为使用企业版的子账号授予最小权限。支持仓库级权限配置，及指定某个子账号仅能拉取/管理指定镜像仓库，或更细粒度的 API 调用权限。操作详情可参见 企业版授权方案示例。
针对不同使用场景，可创建专用的长期访问凭证，单个账号创建的所有长期访问凭证均与只用于登录，权限与该账号在 CAM 侧配置的权限一致。
临时访问实例建议使用临时访问凭证（1小时有效），操作详情可参见 获取临时登录指令。
网络安全
请避免开通公网访问入口，避免外部非授权对象访问实例，或是自身业务通过公网下载镜像，产生公网访问费用。可选为实例绑定自定义域名，并管理该域名的公网及 VPC 内解析。

镜像管理

仓库规划
建议使用命名空间来隔离业务、团队等，方便后期权限管理及配置同步规则。
支持多级路径，可根据需要创建多层级仓库，避免创建过多命名空间。

支持推送镜像自动创建仓库，可在命名空间层级配置公开/私有等默认属性。

请注意：命名空间，镜像仓库等均是路径标记，后端数据存储无隔离。

版本命名

请避免在生产环境内使用 latest 更新镜像版本，可能影响服务更新及回滚。

建议使用 CI 工具为镜像进行自动化命名，便于后续版本管理及镜像同步等。

请注意：删除指定版本镜像时，相同 digest 镜像将会同时被删除。

CI/CD

使用企业版自带服务

企业版 CI/CD 能力完全基于腾讯云 CODING DevOps 产品，需开通该产品，并完成基础配置。

支持镜像构建，代码源可选 Github、Gitlab、工蜂、码云、CODING 等。

支持交付流水线，可自动部署镜像至集群、弹性集群及边缘集群。

对接外部服务

可使用触发器（webhook）功能对接已有 CI/CD 系统，推送镜像自动触发 webhook 通知，消息体包含镜像基础信息。详情可参见 管理触发器。

可直接使用 CODING DevOps 完整服务，已内置容器镜像服务 TCR 相关模板。

使用个人版域名访问企业版实例

最近更新时间：2023-06-14 15:50:42

操作场景

之前已在生产环境稳定使用个人版共享服务的客户如果希望升级到独享的企业版实例，一方面需要将个人版内已有镜像数据导入至企业版实例内，另一方面也需要变更现有构建、发布系统中的镜像地址配置，来访问企业版实例。在实际生产场景中，镜像地址会被应用在构建平台、发布平台、Kubernetes 集群内应用 YAML 定义等多个环节，统一修改成本较高。
针对以上场景和问题，企业版推出个人版服务域名兼容功能，支持客户使用已有的个人版镜像地址及访问凭证来推送、拉取企业版实例内镜像，并支持智能回源，在企业版内无对应镜像时，自动回源请求个人版服务内对应镜像，最大限度降低镜像仓库迁移给客户运维、研发带来的负担，加速客户尽快切换至更加服务稳定、功能强大、高性能的企业版服务。

前提条件

已创建企业版实例。具体操作，请参见创建企业版实例。
已将个人版实例中的数据迁移到企业版实例中。具体操作，请参见 个人版实例镜像导入到企业版实例。
当前只有白名单用户才可以使用个人版域名访问企业版实例功能，您需要 提交工单 申请使用。

基础知识

个人版实例和企业版实例支持的域名如下所示：
个人版实例域名
不区分公网及内网域名，VPC 私有网络内访问，默认为内网链路。
主服务地域（广州、上海、南京、北京、成都、重庆）：ccr.ccs.tencentyun.com
其他地域：具有独立服务及域名，如 中国香港地域：hkccr.ccs.tencentyun.com
企业版实例域名
区分公网及私网域名，并支持自定义域名
默认域名：{企业版实例名称}.tencentcloudcr.com。
内网专用域名：{企业版实例名称}-vpc.tencentcloudcr.com。
自定义域名：支持注册自定义域名。
以在广州地域个人版服务内命名空间 team-a 下 nginx:latest 镜像，迁移至企业版实例 company-a 为例：
个人版访问地址：ccr.ccs.tencentyun.com/team-a/nginx:latest。

企业版访问地址：company-a.tencentcloudcr.com/team-a/nginx:latest。

原理介绍

新建企业版实例时会默认下发支持个人版域名的证书，并支持处理个人版的认证鉴权请求。
客户仅需在私有网络环境内，将个人版域名解析至企业版的内网访问入口（请参考：配置内网访问控制），即可在私有网络内访问个人版镜像仓库地址时，自动访问企业版服务，并使用个人版服务的用户名+密码完成认证和鉴权。
客户可选择使用 私有域解析 PrivateDNS 产品或是自行管理集群节点 Host 配置来实现域名解析。
当客户不再需要使用个人版域名访问企业版实例时，仅需取消私有网络内的强制解析，即可正常访问个人版服务。

使用限制

1. 在同一个地域只允许一个企业版实例开启使用个人版域名兼容功能。
2. 如果您使用的是公网环境，您需要手动配置域名解析到企业版实例访问入口。
3. 在使用个人版域名访问企业版服务时，会优先请求企业版里对应命名空间内的镜像仓库，因此请避免在企业版实例内使用 library、tke、public 等特殊命名空间名称，否则将导致 TKE 集群无法访问产品官方镜像造成基础服务异常。

操作指南

确认基础环境

1. 已开启个人版服务并使用。
2. 已购买企业版服务，并将个人版服务内部分镜像同步至企业版实例内。
3. 已有 TKE 集群（含 TKE Serverless 集群），且集群所在 VPC 已接入企业版实例，具体可参考 配置内网访问控制。
4. 已验证可在 TKE 集群内正常通过内网拉取个人版及企业版内镜像。

配置私有域解析

1. 前往 私有域解析 PrivateDNS控制台
2. 新建私有域
2.1 域名：tencentyun.com。
2.2 关联 VPC：选择企业版已接入的 VPC。
2.3 子域名递归解析：保持开启。
2.4 其他选项保持默认即可。
3. 配置私有域解析

3.1 点击新建的私有域进入详情页。
3.2 在 **解析记录** 中添加记录，配置如下
主机记录：如在使用主服务地域，则配置为 **ccr.ccs**，其他地域请填写对应的域名前缀，如 hkccr.ccs。
记录类型：CNAME。
记录值：企业版实例的域名，使用默认域名或自定义域名即可，需要确认 默认域名或自定义域名 已经在产品控制台内已配置自动解析。
其他保持默认即可。
3.3 其他选项保持默认即可。

验证访问效果

完成上述配置后，即可验证使用个人版域名访问企业版实例。

场景 1 ：使用个人版域名拉取已迁移至企业版实例内镜像

1. 使用同步工具或手动推送镜像至企业版实例，如：company-a.tencentcloudcr.com/team-a/nginx:latest，对应个人版镜像仓库地址为：ccr.ccs.tencentyun.com/team-a/nginx:latest。
2. 登录集群节点手动拉取镜像，或通过创建新的工作负载来执行镜像拉取，需要注意：
镜像地址保持为：ccr.ccs.tencentyun.com/team-a/nginx:latest。
访问凭证保持为已配置的个人版访问凭证。
3. 验证集群可正常拉取到该镜像。

场景 2：使用个人版域名拉取尚未迁移至企业版实例内镜像

1. 个人版内已有镜像：ccr.ccs.tencentyun.com/team-b/apache:latest，尚未将该镜像同步至企业版内。
2. 登录集群节点手动拉取镜像，或通过创建新的工作负载来执行镜像拉取，需要注意：
镜像地址保持为：ccr.ccs.tencentyun.com/team-b/apache:latest。
访问凭证保持为已配置的个人版访问凭证。
3. 验证集群可正常拉取到该镜像。

场景 3：使用个人版域名推送镜像至企业版实例

1. 使用 Docker CLI 或是 CI 平台推送镜像，使用个人版地址：ccr.ccs.tencentyun.com/team-a/nginx:latest。
2. 若企业版实例内已有 team-a 命名空间，则可推送成本，否则将直接报错失败。

使用建议

适用场景

建议仅在以下场景中使用域名兼容功能：
构建环境、项目代码、部署应用中大量使用个人版镜像，切换到企业版独立域名成本高。
镜像构建、分发环境固定，一次性设置域名解析成本低。

如镜像分发场景较为复杂，且需要支持第三方用户、复杂网络场景访问企业版内镜像，不建议使用个人版域名兼容功能，避免扰乱生产环境部署。

灰度切换

建议在最初使用个人版域名访问企业版实例内镜像时，同时向个人版及企业版内推送镜像，以便在解析配置出现异常时，集群仍可临时切换至访问个人版服务。后续请逐渐将已有个人版镜像地址配置调整为企业版地址，并最终停止使用域名兼容功能。

使用交付流水线实现容器 DevOps

最近更新时间：2023-03-03 16:33:01

操作场景

在云原生时代，DevOps 理念已被广泛接受，而容器技术的兴起和普及加速了 DevOps 的落地。基于容器 DevOps 实现持续集成和持续部署，可显著提升企业的业务应用创建和交付速度，提升企业的竞争力。

本文将介绍如何通过使用 TCR 交付流水线功能，与容器服务 TKE、CODING DevOps 服务联合为用户提供简单易上手的容器 DevOps 能力，可实现 推送代码自动触发镜像构建和应用部署 或 本地推送镜像后自动触发部署

前提条件

- 已有容器镜像服务 TCR 企业版实例，并已创建镜像仓库。详情可参见 购买企业版实例、创建镜像仓库。
- 已有容器服务 TKE 集群，并已部署容器应用。详情可参见 创建集群。
- 已开通 CODING DevOps 服务。

> 说明：
>
> 当前容器服务 TKE 已支持在控制台内选择容器镜像服务 TCR 企业版镜像创建工作负载。同时，TKE 标准集群可安装 TCR 专属插件，实现内网及免密拉取 TCR 企业版内镜像，详情可参见 使用 TCR 企业版实例内容器镜像创建工作负载。

操作步骤

场景1：推送代码后自动触发镜像构建和应用部署

支持用户配置流水线，在代码变更后，自动构建镜像，并触发自动部署到容器平台。

配置交付流水线

1. 登录容器镜像服务控制台，选择左侧导航栏中的交付流水线。

2. 在“交付流水线”页面中，单击**新建**。

3. 在“基本信息”步骤中，配置以下参数，单击**下一步：镜像配置**。

- **流水线名称**：设置交付流水线名称。
- **流水线描述**：为交付流水线添加描述信息，创建后可修改。

4. 在“镜像配置”步骤中，配置以下参数，单击**下一步：应用部署**。

- **镜像仓库**：选择交付流水线关联的镜像仓库，将自动配置镜像构建及推送，用于托管应用部署所需要的镜像。
- **镜像版本过滤**：支持对执行交付流水线中镜像的版本进行限制，可以过滤不需要执行部署的镜像版本。
  - **直接部署任意版本**：推送到镜像仓库的任意版本镜像都会被部署。
  - **仅部署指定名称版本**：需指定镜像版本，多个版本可以使用逗号分隔，非指定版本不会部署。
  - **仅部署指定规则版本**：需输入正则表达式。
  - **镜像来源**：支持平台构建镜像和本地推送镜像。本场景以选择“平台构建镜像”为例。
  - **平台构建镜像**：允许用户关联不同代码托管平台的代码仓库，当代码变动时自动触发交付流水线，完成自动构建、推送镜像以及应用部署。
  - **本地推送镜像**：支持用户在手动推送镜像时可以触发应用部署。
  - **代码源、代码仓库**：选择用于构建镜像的代码仓库，流水线将拉取该代码仓库内源代码进行编译及构建，首次选择需要授权。目前已支持 GitHub、公有GitLab、私有GitLab、码云以及工蜂等代码托管平台。
  - **触发规则**：镜像构建被自动触发的规则条件。目前支持以下四种场景：
    - **推送到指定分支触发**：需指定分支。
    - **推送新标签时触发构建**：新建标签并推送时触发。
    - **推送到分支时触发构建**：推送至任意分支时触发，无需指定分支。

- **符合分支或标签规则时构建**：需输入正则表达式，例如 `^refs/heads/master$` ，可匹配 master 分支进行触发。

- **Dockerfile 路径**：镜像构建执行的操作基于代码仓库内的 Dockerfile，需指定该 Dockerfile 文件的路径。如不指定，默认为代码仓库根目录下名为 Dockerfile 的文件。

- **构建目录**：镜像构建执行的工作目录，即上下文环境（context），默认为代码仓库的根目录。

- **版本规则**：定义镜像构建生成的镜像名称，即镜像版本（tag）。支持配置自定义前缀，并组合加入“分支/标签”，“更新时间”，“commit 号” 三个环境变量。其中，更新时间为执行 docker tag 指令时构建服务的系统时间。

5. 在“应用部署”步骤中，配置以下参数，单击**完成**。

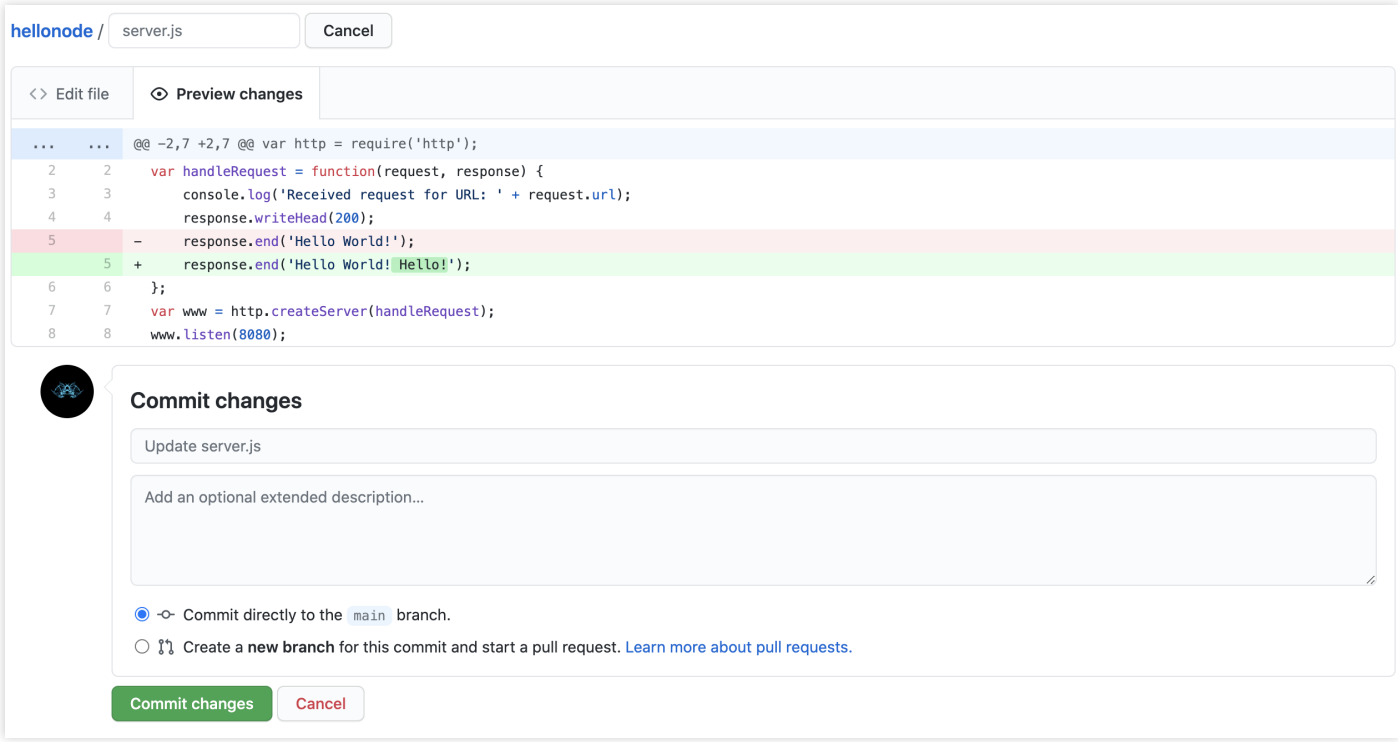
- **部署平台**：交付流水线同时支持容器服务 TKE、弹性容器服务 EKS 及边缘容器服务 Edge。本场景以容器服务 TKE 为例。
- **部署地域**：目标集群所在地域。选择已创建的 TKE 标准集群所在地域。
- **部署集群**：目标集群。选择已创建的 TKE 标准集群。
- **部署方式**：当前仅支持 “更新已有工作负载”。
- **命名空间**：已部署应用所在的命名空间。
- **工作负载**：已部署应用的关联工作负载。
- **Pod 容器**：已部署应用的工作负载内的 Pod 容器，该容器内使用了上步骤中关联镜像仓库内的镜像。

6. 完成以上配置后，可在“交付流水线” 列表页查看新建的流水线。

更新容器应用

完成以上配置后，即可在更新应用代码后，自动触发镜像构建，推送及应用更新。

1. 更新源代码
   更新源代码，并提交至远端代码仓库。如下图所示：



2. 执行流水线

源代码推送完成后，如符合镜像配置中镜像构建的触发条件，将触发流水线执行。可单击流水线查看该流水线执行记录，并查看具体步骤进度。

- **Checkout**：检出代码。
- **Docker Build**：基于镜像构建配置进行镜像构建，并为生成的镜像打上指定规则的 Tag。例如，`v-{tag}-{date}-{commit}`。
- **Docker Push**：推送镜像，自动推送至关联镜像仓库内。
- **Deploy To TKE**：使用最新推送的镜像更新关联工作负载及Pod 内同名镜像。

3. 查看应用更新状态

3.1 登录容器服务控制台，选择左侧导航栏中的集群。

3.2 单击需查看应用更新状态的集群 ID，进入集群的“工作负载”页面。

3.3 在 “Deployment” 页中，选择实例名称，进入实例的详情页面。

3.4 在“修订历史”页签中，即可查看应用更新状态。
您也可以直接访问该应用服务，查看是否已更新。通过 Service 暴露到公网的地址，查看服务更新结果。

场景2：本地推送镜像后自动触发部署

在某些场景中不需要使用 TCR 镜像自动构建能力，但又希望在推送镜像后能够自动部署到容器平台。TCR 支持用户配置本地推送镜像后，通过触发器自动触发镜像部署。

配置交付流水线

1. 登录容器镜像服务控制台，选择左侧导航栏中的 **交付流水线** 。

2. 在“交付流水线”页面中，单击**新建**。

3. 在“基本信息”步骤中，配置以下参数，单击**下一步：镜像配置**。

- **流水线名称**：设置交付流水线名称。
- **流水线描述**：为交付流水线添加描述信息，创建后可修改。

4. 在“镜像配置”步骤中，配置以下参数，单击**下一步：应用部署**。

- **镜像仓库**：选择交付流水线关联的镜像仓库，将自动配置镜像构建及推送，用于托管应用部署所需要的镜像。
- **镜像版本过滤**：支持对执行交付流水线中镜像的版本进行限制，可以过滤不需要执行部署的镜像版本。
  - **直接部署任意版本**：推送到镜像仓库的任意版本镜像都会被部署。
  - **仅部署指定名称版本**：需指定镜像版本，多个版本可以使用逗号分隔，非指定版本不会部署。
  - **仅部署指定规则版本**：需输入正则表达式。
  - **镜像来源**：支持平台构建镜像和本地推送镜像。本场景以选择“本地推送镜像”为例。
  - **平台构建镜像**：允许用户关联不同代码托管平台的代码仓库，当代码变动时自动触发交付流水线，完成自动构建、推送镜像以及应用部署。
  - **本地推送镜像**：支持用户在手动推送镜像时可以触发应用部署。

5. 在“应用部署”步骤中，配置以下参数，单击**完成**。

- **部署平台**：交付流水线同时支持容器服务 TKE、弹性容器服务 EKS 及边缘容器服务 Edge。本场景以容器服务 TKE 为例。
- **部署地域**：目标集群所在地域。选择已创建的 TKE 标准集群所在地域。
- **部署集群**：目标集群。选择已创建的 TKE 标准集群。
- **部署方式**：当前仅支持 “更新已有工作负载”。
- **命名空间**：已部署应用所在的命名空间。
- **工作负载**：已部署应用的关联工作负载。
- **Pod 容器**：已部署应用的工作负载内的 Pod 容器，该容器内使用了上步骤中关联镜像仓库内的镜像。

更新容器应用

完成以上配置后，即可在本地使用命令行指令推送镜像，触发自动部署。

1. 本地推送镜像

2. 登录 容器镜像服务控制台，选择左侧导航栏中的**镜像仓库**。
   在“镜像仓库”页面即可查看当前实例内的镜像仓库列表。如需切换实例，请在页面上方的“实例名称”下拉列表中进行选择。

3. 单击实例右侧的**快捷指令**，在弹窗中查看快捷指令。

4. 执行流水线
   本地推动镜像完成后，如符合镜像配置中镜像构建的触发条件，将触发流水线执行。由于此时镜像已经准备好，因此流水线只需要执行自动部署。

5. 查看应用更新状态

   5.1 登录容器服务控制台，选择左侧导航栏中的集群。

   5.2 单击需查看应用更新状态的集群 ID，进入集群的“工作负载”页面。

   5.3 在 “Deployment” 页中，选择实例名称，进入实例的详情页面。

5.4 在“修订历史”页签中，即可查看应用更新状态。

您也可以直接访问该应用服务，查看是否已更新。通过 Service 暴露到公网的地址，查看服务更新结果。如下图所示：

TKE 集群使用 TCR 插件内网免密拉取容器镜像

最近更新时间：2023-02-09 16:02:40

操作场景

本文介绍如何在 容器服务 TKE 中，通过使用 TCR 插件，实现内网免密拉取企业版实例内容器镜像，并创建工作负载。

前提条件

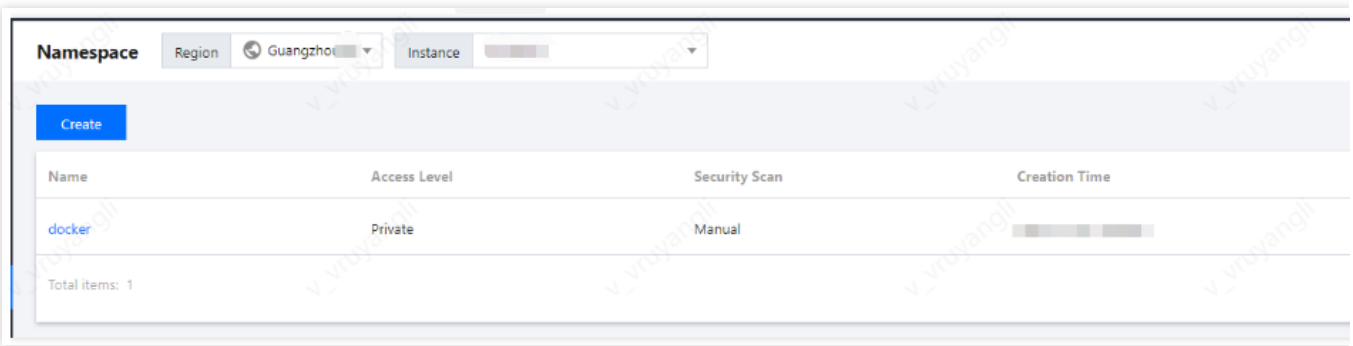
在使用容器镜像服务 TCR 企业版内托管的私有镜像进行应用部署前，您需要完成以下准备工作：
已成功 购买企业版实例。
已成功 创建 TKE 集群。
如使用子账号进行操作，请参考 企业版授权方案示例 提前为子账号授予对应实例的操作权限。
如使用已有 TKE 集群，请确认操作子账号具有集群相关权限，请参考 TKE 集群权限管理。

操作步骤

准备容器镜像

步骤1：创建命名空间

新建的 TCR 企业版实例内无默认命名空间，且无法通过推送镜像自动创建。请参考 创建命名空间 按需完成创建。
建议命名空间名使用项目或团队名，本文以 `docker` 为例。创建成功后如下图所示：

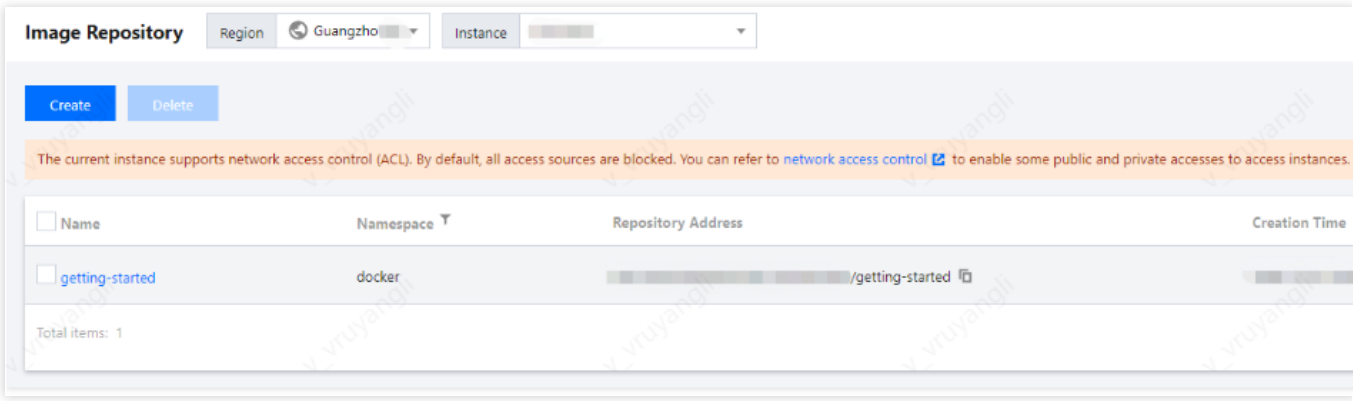


步骤2：创建镜像仓库（可选）

容器镜像托管在具体的镜像仓库内，请参考 创建镜像仓库 按需完成创建。镜像仓库名称请设置为期望部署的容器镜像名称，本文以 `getting-started` 为例。创建成功后如下图所示：

说明：

通过 docker cli 或其他镜像工具，例如 jenkins 推送镜像至企业版实例内时，若镜像仓库不存在，将会自动创建，无需提前手动创建。

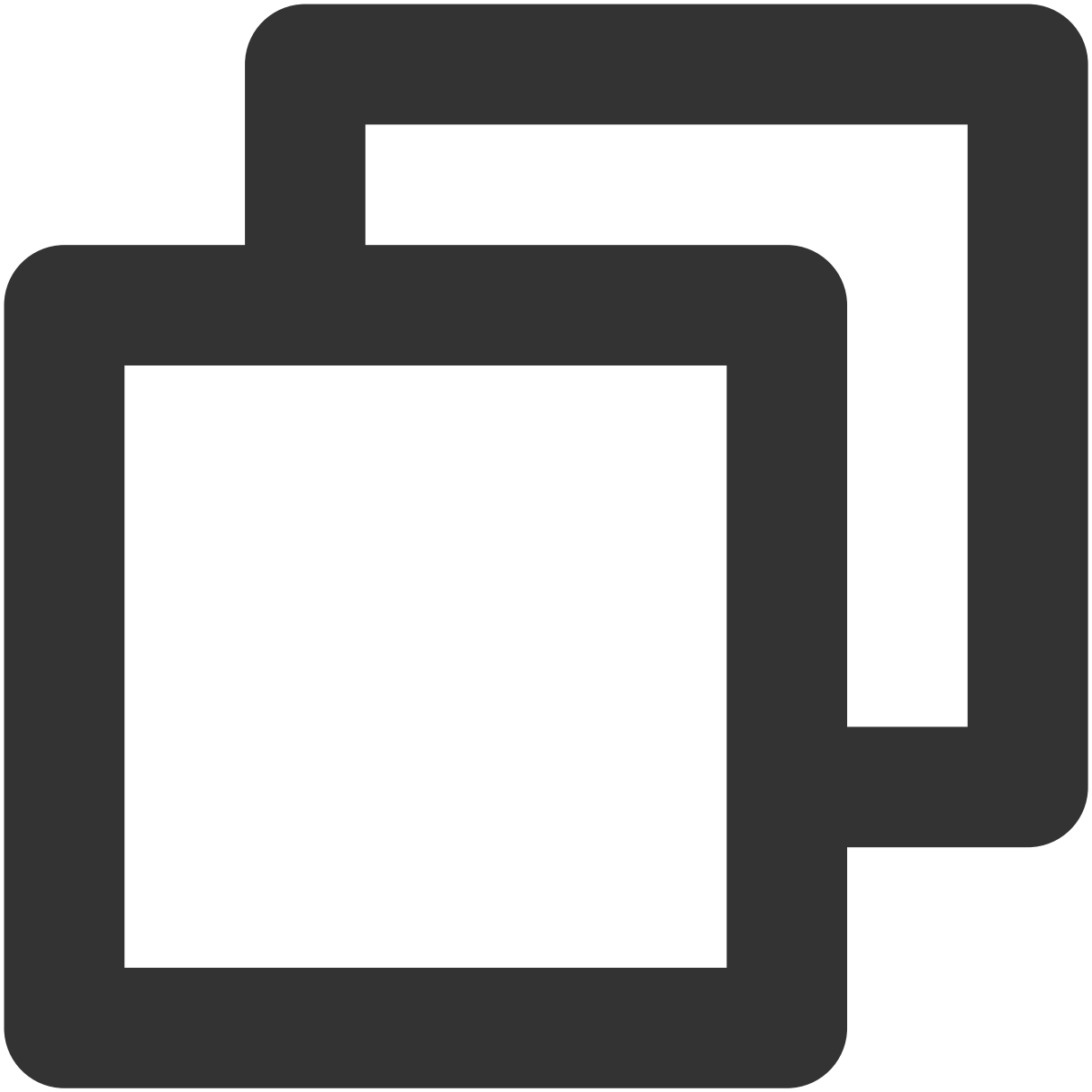


步骤3：推送容器镜像

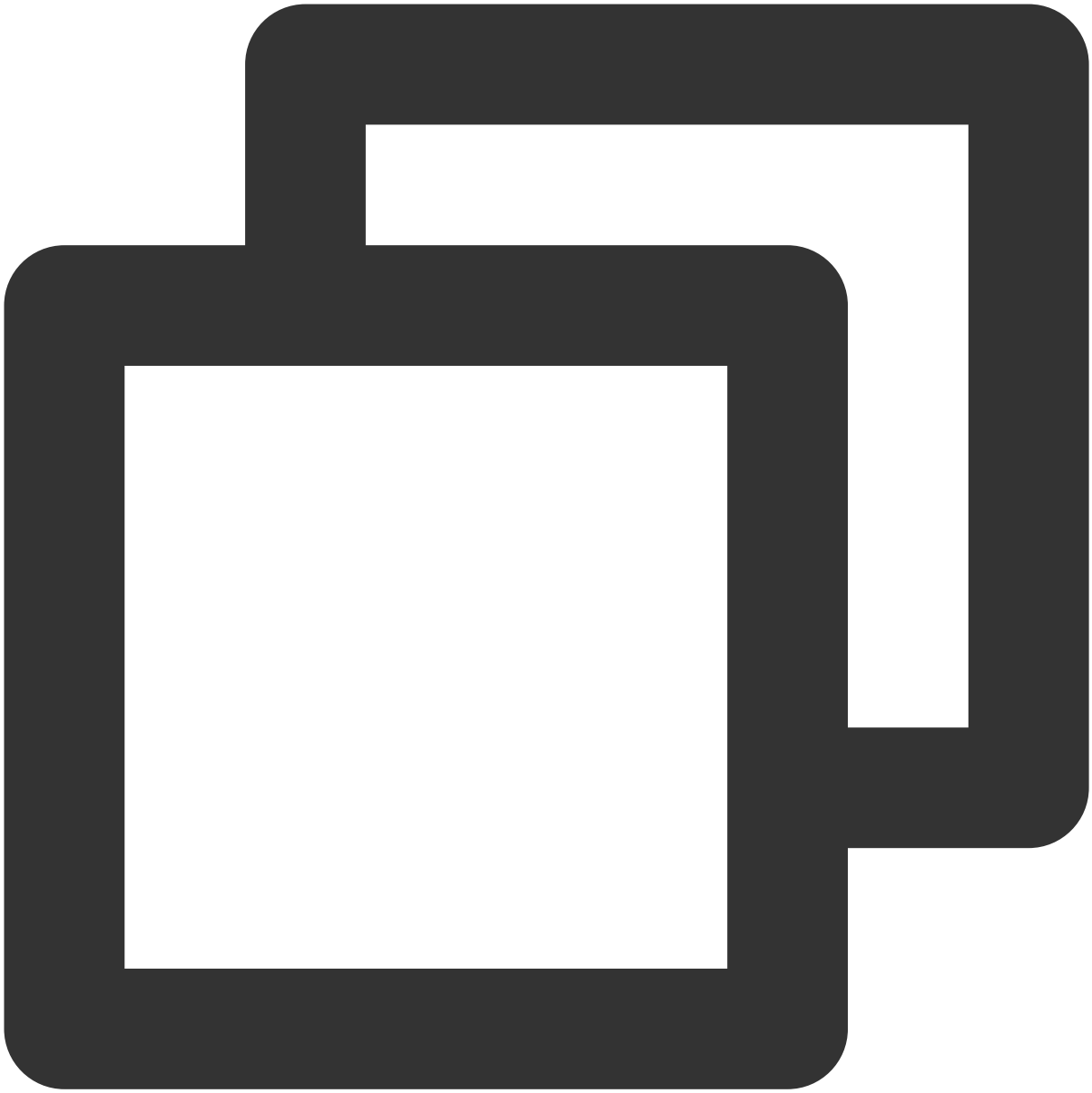
您可通过 docker cli 或其他镜像构建工具（例如 jenkins）推送镜像至指定镜像仓库内，本文以 docker cli 为例。此步骤需要您使用一台安装有 Docker 的云服务器或物理机，并确保访问的客户端已在 配置网络访问策略 定义的公网或内网允许访问范围内。

1. 参考 获取实例访问凭证 获取登录指令，并进行 Docker Login。
2. 登录成功后，您可在本地构建新的容器镜像或从 DockerHub 上获取一个公开镜像用于测试。

本文以 DockerHub 官方的 Nginx 最新镜像为例，在命令行工具中依次执行以下指令，即可推送该镜像。请将 demo-tcr、docker 及 getting-started 依次替换为您实际创建的实例名称、命名空间名称及镜像仓库名。



```
docker tag getting-started:latest demo-tcr.tencentcloudcr.com/docker/getting-starte
```



```
docker push demo-tcr.tencentcloudcr.com/docker/getting-started:latest
```

推送成功后，即可前往控制台的 “镜像仓库” 页面，选择仓库名并进入详情页面查看。

配置 TKE 集群访问 TCR 实例

TCR 企业版实例支持网络访问控制，默认拒绝全部来源的外部访问。您可根据 TKE 集群的网络配置，选择通过公网或内网访问指定实例，拉取容器镜像。若 TKE 集群与 TCR 实例部署在同一地域，建议通过内网访问方式拉取容器镜像，该方式可提升拉取速度，并节约公网流量成本。

步骤1：在 TCR 实例中关联集群 VPC

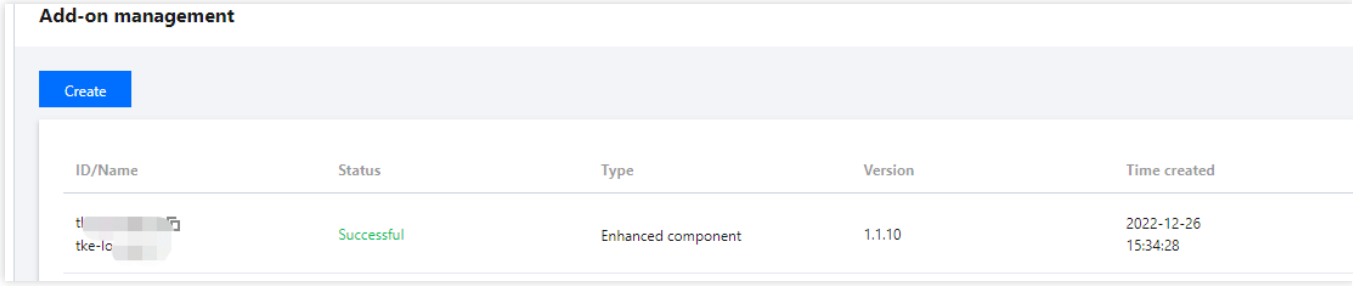
为保障用户数据安全，新建的 TCR 实例默认拒绝全部来源的访问。为允许指定 TKE 集群可访问 TCR 实例拉取镜像，需将集群所在的 VPC 关联至 TCR 实例，并配置相应的内网域名解析。

1. 新建内网访问链路
2. 配置域名内网解析

步骤2：在 TKE 集群中安装 TCR 插件

如果当前您正在使用容器服务 TKE，请参考 TCR 说明 在 TKE 集群中安装 TCR 插件，并在 “TCR组件参数设置”窗口中勾选"启用内网解析功能"。该插件可自动为集群内节点配置关联 TCR 实例的内网解析，可实现内网免密拉取实例内镜像。

插件安装完成后，集群将具备内网免密拉取该关联实例内镜像的能力，无需额外配置。如下图所示：



说明：

当前 TCR 组件暂只支持 K8S 版本为 1.12、1.14、1.16、1.18、1.20 的集群，如集群版本暂不支持，请采用手动配置方式。

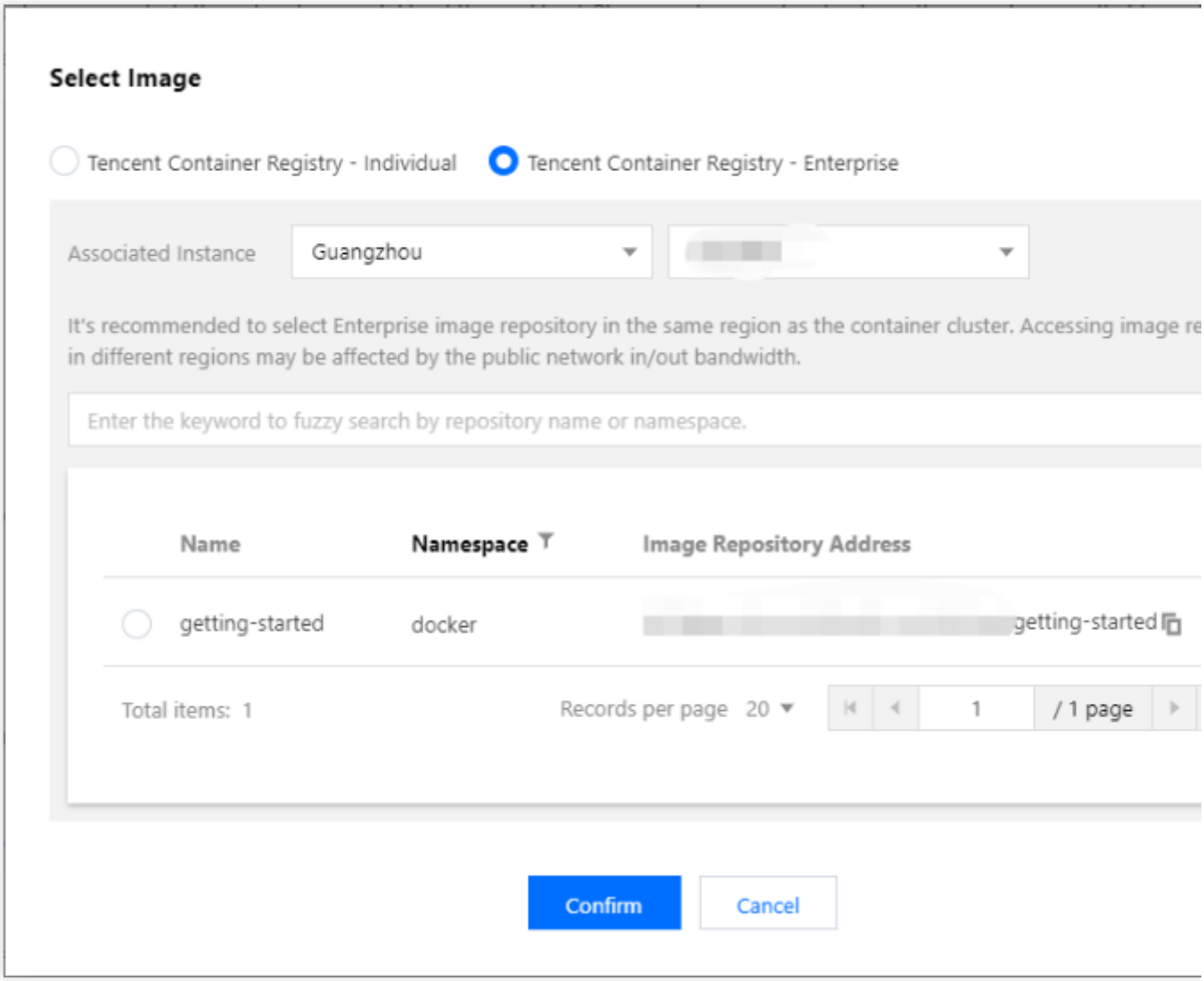
使用 TCR 实例内容器镜像创建工作负载

1. 登录容器服务控制台，选择左侧导航栏中的**集群**。
2. 选择需要创建工作负载的集群 ID，进入集群详情页。
3. 在集群详情页面，选择左侧**工作负载** > **Deployment**。
4. 进入“Deployment” 页面，并单击**新建**。
5. 进入“新建Workload” 页面，根据以下主要参数信息，创建工作负载。

命名空间：根据需要选择。请确认安装 TCR 插件时，配置支持免密拉取的命名空间已包含此时需要的命名空间。

实例内容器：

镜像：单击**选择镜像**，并在弹出的“选择镜像”窗口中，选择容器镜像服务企业版，再根据需要选择地域、实例和镜像仓库。如下图所示：

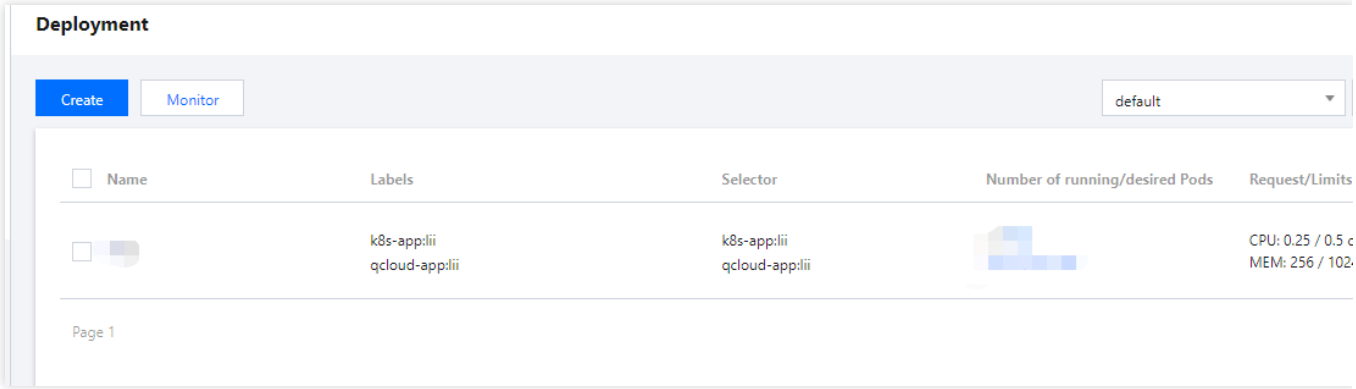


镜像版本：选择好镜像后，单击**选择镜像版本**，在弹出的“选择镜像版本”窗口中，根据需要选择该镜像仓库的某个版本。若不选择则默认为latest。

镜像访问凭证：如集群已安装 TCR 扩展组件，无需显式配置。**请避免选择其他访问凭证，选择其他访问凭证将导致此工作负载无法加载 TCR 插件的免密拉取配置。**

6. 完成其他参数设置后，单击**创建workload**，查看该工作负载的部署进度。

部署成功后，可在 “Deployment” 页面查看该工作负载的“运行/期望Pod数量”为“1/1”。如下图所示：


Deployment
Create
Monitor
default
Name
Labels
Selector
Number of running/desired Pods
Request/Limits
k8s-app:lii
qcloud-app:lii
k8s-app:lii
qcloud-app:lii
CPU: 0.25 / 0.5 c
MEM: 256 / 102
Page 1

从自建 Harbor 同步镜像到 TCR 企业版

最近更新时间：2023-02-09 11:55:37

操作场景

当用户将在 IDC 内自建的容器集群迁移至云上容器服务时，也可选择将自建的容器镜像托管服务一同迁移至云上进行托管。将自建的镜像仓库服务迁移至腾讯云容器镜像服务 TCR 后，一方面减少了用户自行搭建及维护的运维管理成本，并提供云上专业稳定的托管服务及技术支持。另一方面实现了与云上容器服务的联动使用，用户可享受容器上云的一致性使用体验，可使用容器集群内网拉取镜像，降低了公网带宽成本。

Harbor 是 VMware 公司开源的企业级 Docker Registry 项目，在开源 Docker Distribution 能力基础上扩展了例如 RBAC、镜像安全扫描及镜像同步等能力。当前已成为自建容器镜像托管及分发服务的首选。本文介绍如何将 IDC 或云上服务器内已搭建的 Harbor 中的容器镜像或 Helm Chart，同步至云上容器镜像服务企业版实例。

前提条件

在将自建 Harbor 内数据同步至云上容器镜像服务实例内，您需要首先确认并完成以下准备工作：

- 已搭建 Harbor 服务，且仅支持 Harbor v1.8.0 及以上版本。
- 确认自建 Harbor 可通过专线、公网或私有网络访问容器镜像服务。
- 已在云上容器集群所在地域或邻近地域成功 购买企业版实例。
- 如果使用子账号进行操作，请参考 企业版授权方案示例 提前为子账号授予对应实例的容器镜像，Helm Chart 推送权限，建议将容器镜像服务全读写权限授予配置同步的子账号。

操作步骤

配置自建 Harbor 服务可访问容器镜像服务企业版实例

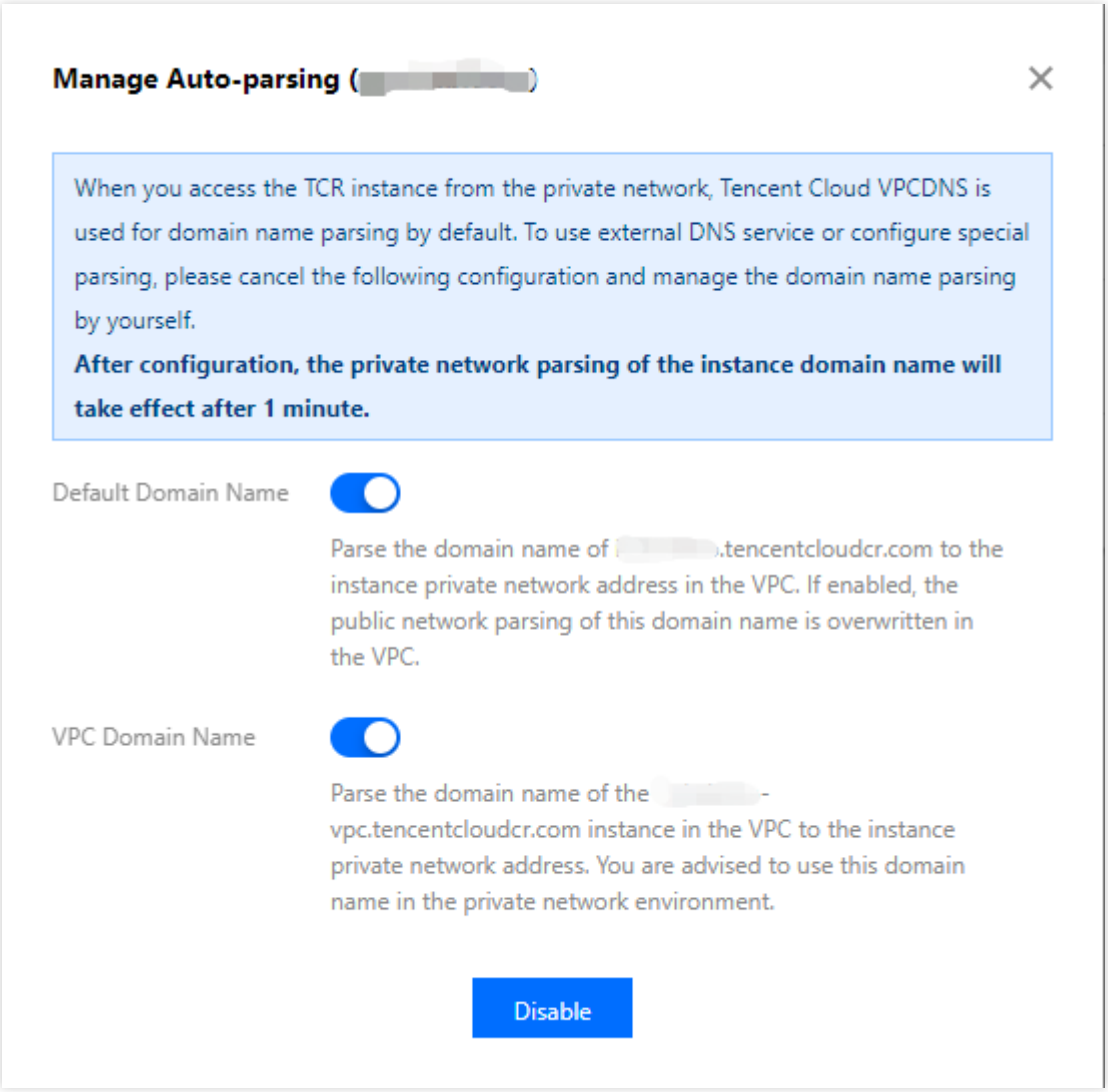
您可根据自建 Harbor 服务的实际网络情况，选择 通过腾讯云私有网络进行访问 或 通过公网进行访问 方案配置访问容器镜像服务企业版实例。

- 通过腾讯云私有网络进行访问
- 通过公网进行访问

若当前自建 Harbor 服务部署在腾讯云私有网络环境内，或已通过专线打通至腾讯云私有网络，则可通过内网进行数据同步。通过内网进行数据同步可提升数据同步速度，并节省公网流量费用。

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**访问控制>内网访问**。

2. 在页面上方的**实例名称**下拉列表中，选择需要进行数据同步的实例。
3. 单击**新建**，在弹出的“新建内网访问链路”窗口中配置新建内网访问链路以允许自建 Harbor 服务通过内网访问该实例。其中：
   - **所属实例**：当前已选择实例，即需要进行数据同步的实例。
   - **私有网络**：自建 Harbor 服务所在的私有网络，或已通过专线接入的私有网络。
   - **子网**：新建内网访问链路将占用所选私有网络的一个内网 IP，请选择私有网络下的一个子网以分配该内网 IP 所属的子网。
4. 完成以上配置后，可获得内网访问链路的目标访问 IP。为在私有网络环境中将实例域名解析至该内网 IP，请管理该内网访问链路的自动解析，开启默认域名的自动解析，如下图所示。详情可参见 管理内网解析。



您也可以在自建 Harbor 服务所在云服务器上配置 Host。如果选择手动配置，可在云服务器上执行以下命令，配置 Host。如果当前正在使用独立的 DNS 服务，也可在 DNS 服务中配置。

```
echo x.x.x.x harbor-sync.tencentcloudcr.com >> /etc/hosts
```

创建企业版实例访问凭证

容器镜像服务企业版支持创建、管理多个访问凭证，建议您为数据同步操作创建独立的访问凭证，完成数据同步后及时删除，避免实例访问权限泄露。

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**实例列表**。
2. 在“实例列表”页面中选择需要进行数据同步的实例，进入实例详情页。
3. 选择**访问凭证**页签，并单击实例列表上方的**新建**。
4. 在弹出的“新建访问凭证”窗口中，按照以下步骤进行获取：
   i. 在“新建访问凭证”步骤中，输入凭证“用途描述”并单击**下一步**。用途描述可填写为“自建 Harbor 数据同步专用”。
   ii. 在“保存访问凭证”步骤中，单击**保存访问凭证**下载凭证信息。**请妥善保管访问凭证，仅一次保存机会**。创建完成后即可在**访问凭证**页签中查看。当数据同步完成后，请及时进行访问凭证的禁用及删除操作。

配置 Harbor 同步仓库及同步规则

Harbor 支持添加第三方 Registry 并配置数据复制规则，本文以 Harbor v2.1.2 为例进行操作说明。

1. 使用管理员账号登录至自建 Harbor 服务，可查看并进行**系统管理**。
2. 选择左侧导航栏中的**系统管理>仓库管理**，进入“仓库管理”页面。
3. 在“仓库管理”页面中，单击**新建目标**，参考以下信息添加企业版实例。
   - **提供者**：选择 “Tencent TCR”。
   - **目标名**：自定义该同步目标名称，例如 tencent-tcr。
   - **描述**：该同步目标的描述。
   - **目标 URL**：企业版实例访问域名，例如 `https://harbor-sync.tencentcloudcr.com` 。
   - **访问 ID**：填写已在**访问管理> API密钥管理** 中获取的 SecretId。
   - **访问密码**：填写已在**访问管理> API密钥管理** 中获取的 SecretKey。
   - **验证远程证书**：保持默认设置。
4. 单击**测试连接**。
   - 如显示“测试连接成功”，则说明当前自建 Harbor 服务可以正常访问该企业版实例。
   - 如显示“测试连接失败”，则请确认 配置自建 Harbor 服务可访问容器镜像服务企业版实例。
5. 单击**确定**新建该目标仓库。

> 注意：
> 如果自建 Harbor 版本较低，提供者选项中无 “Tencent TCR”，请在创建新的目标仓库时，选择提供者为 "Docker Registry"，且访问 ID、访问密码分别填写在实例管理中获取的镜像仓库长期访问凭证（用户名 + 密码），而不是腾讯云的 SecretId，SecretKey。在此配置下，暂不支持在 TCR 侧自动新建命名空间。

6. 选择左侧导航栏中的**系统管理>复制管理**，并单击**新建规则**，参考以下信息创建同步规则。

- **名称**：同步规则名称，可根据具体使用场景填写。
- **描述**：该复制规则的描述。
- **复制模式**：默认为 Push-based 模式，仅当前使用 “Tencent TCR” 插件（Harbor 版本 ≥ 2.1.2）时，可选择 Pull-based。其中，Push-based 指将 Harbor 内新增镜像同步至 TCR，Pull-based 指将 TCR 内新增镜像同步至 Harbor。
- **源资源过滤器**：可过滤选择需要同步的资源，不填写则默认选择自建 Harbor 内全部容器镜像及 Helm Chart 资源。
- **目的 Registry**：选择 步骤3 中已创建的目标仓库。
- **目的 Namespace**：指定目的端的命名空间，不填写则默认同名命名空间，建议保持默认设置。
- **触发模式**：默认手动触发，如需在有新容器镜像或 Helm Chart 推送时自动同步，请选择 “事件驱动”，同时建议不要勾选“删除本地镜像时同时也删除远程的镜像”。
- **覆盖**：默认覆盖同名资源。

触发同步并查看同步日志

向自建 Harbor 服务内推送容器镜像及 Helm Chart，若同步规则中的触发模式设置为“事件驱动”，则新推送的资源将自动同步至企业版实例内。可选择该同步规则查看同步日志，并可进入企业版实例控制台查看是否同步成功。此步骤以向自建 Harbor 服务内手动推送 `nginx:latest` 容器镜像并触发同步为例：

1. 推送容器镜像并查看
   使用 docker 客户端推送本地的 `nginx:latest` 容器镜像，并进入自建 Harbor 控制台内查看已推送的镜像。
2. 查看同步记录及进度
   选择左侧导航栏中的**系统管理>复制管理**，选择在 步骤6 中已创建的同步规则，即可查看该同步规则的复制任务。
3. 在容器镜像服务内查看同步镜像
   进入容器镜像服务控制台的“镜像仓库”页面，并选择与自建 Harbor 服务进行同步的实例，即可查看已同步成功的容器镜像。

TKE Serverless 集群拉取 TCR 容器镜像

最近更新时间：2023-05-08 16:20:40

操作场景

本文介绍如何在容器服务 TKE Serverless 集群中拉取 TCR 企业版实例内的容器镜像，并创建工作负载。

前提条件

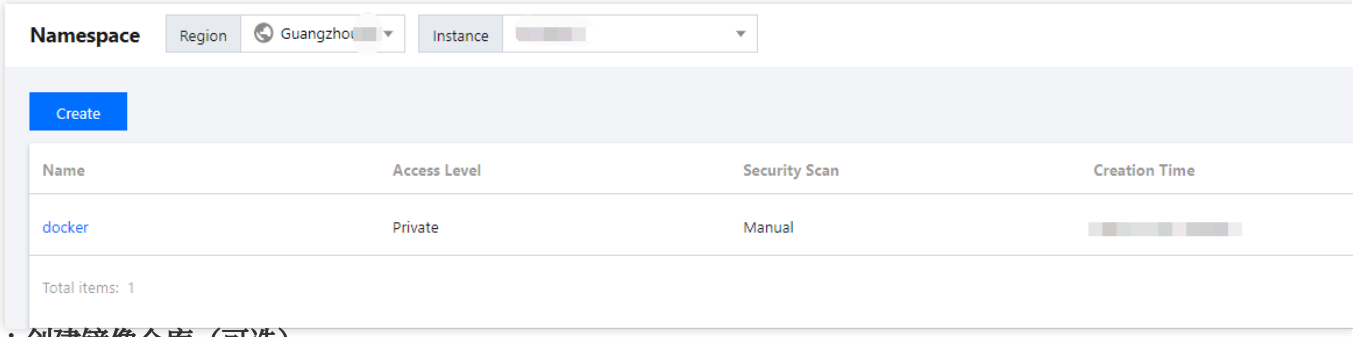
在使用容器镜像服务 TCR 企业版内托管的私有镜像进行应用部署前，您需要完成以下准备工作：
已成功 购买企业版实例。
已成功 创建 TKE Serverless 集群。
如使用子账号进行操作，请参见 企业版授权方案示例 提前为子账号授予对应实例的操作权限。

操作步骤

准备容器镜像

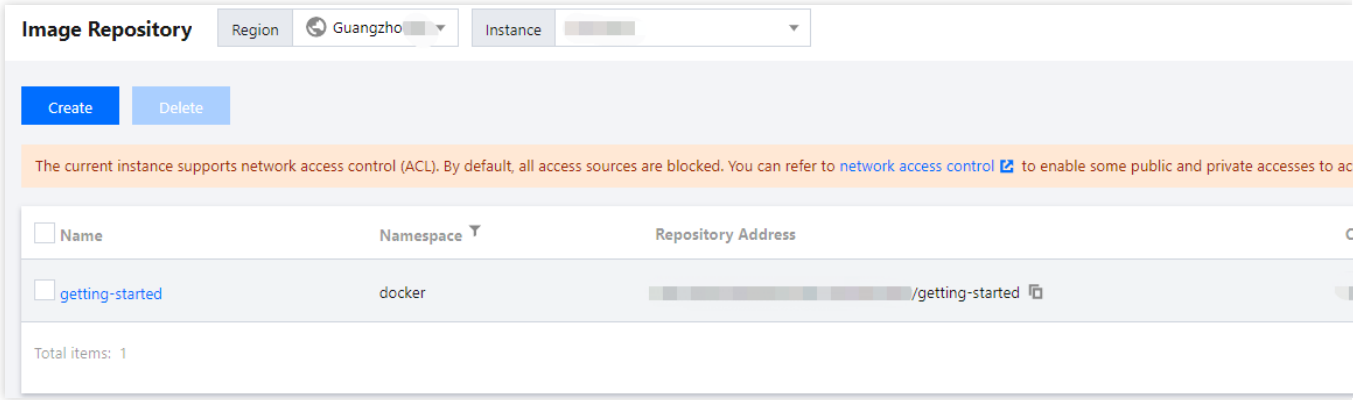
步骤1：创建命名空间

新建的 TCR 企业版实例内无默认命名空间，且无法通过推送镜像自动创建。请参见 创建命名空间 按需完成创建。建议命名空间名使用项目或团队名，本文以 `docker` 为例。创建成功后如下图所示：



步骤2：创建镜像仓库（可选）

容器镜像托管在具体的镜像仓库内，请参见 创建镜像仓库 按需完成创建。镜像仓库名称请设置为期望部署的容器镜像名称，本文以 `getting-started` 为例。创建成功后如下图所示：



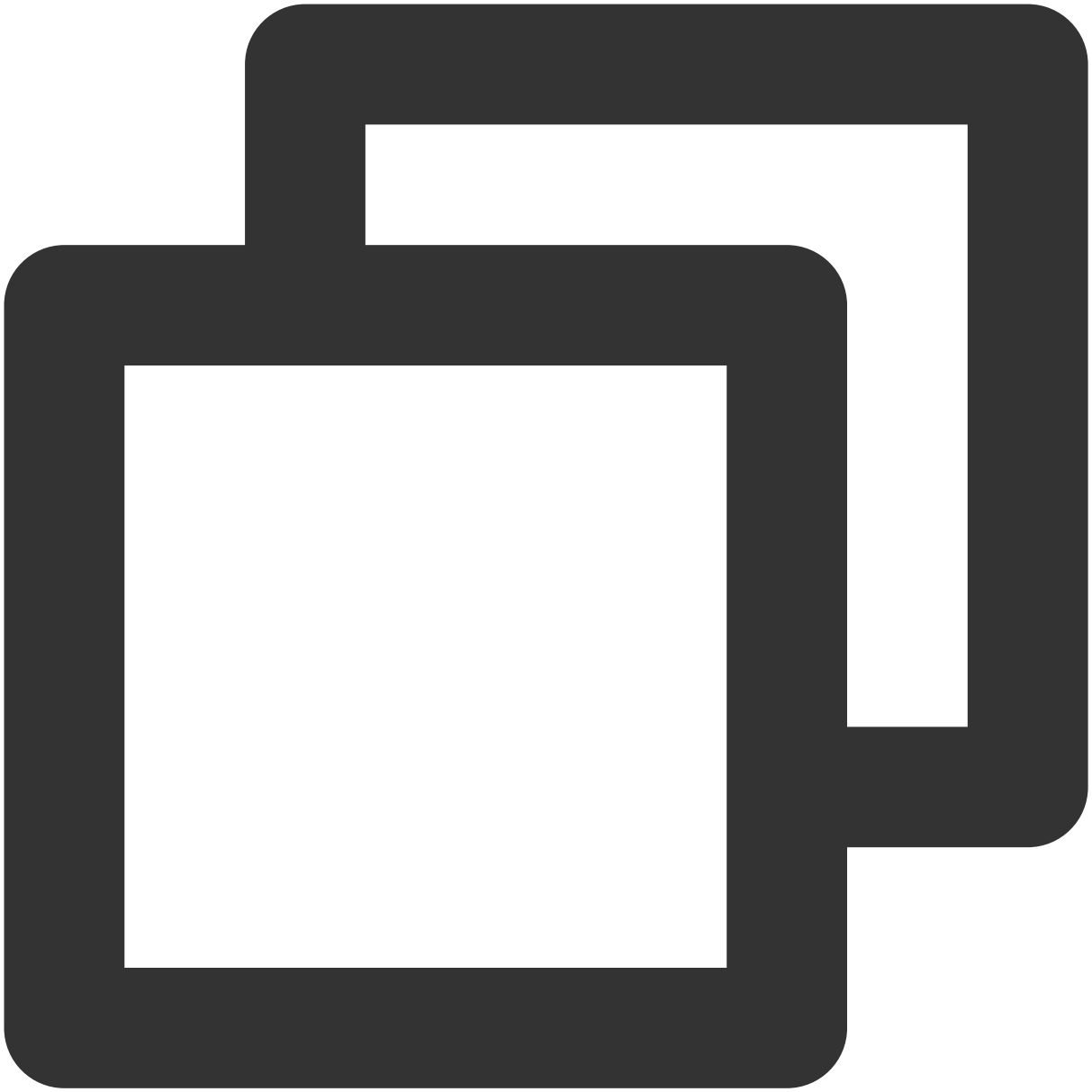
说明

通过 `docker cli` 或其他镜像工具，例如 jenkins 推送镜像至企业版实例内时，若镜像仓库不存在，将会自动创建，无需提前手动创建。

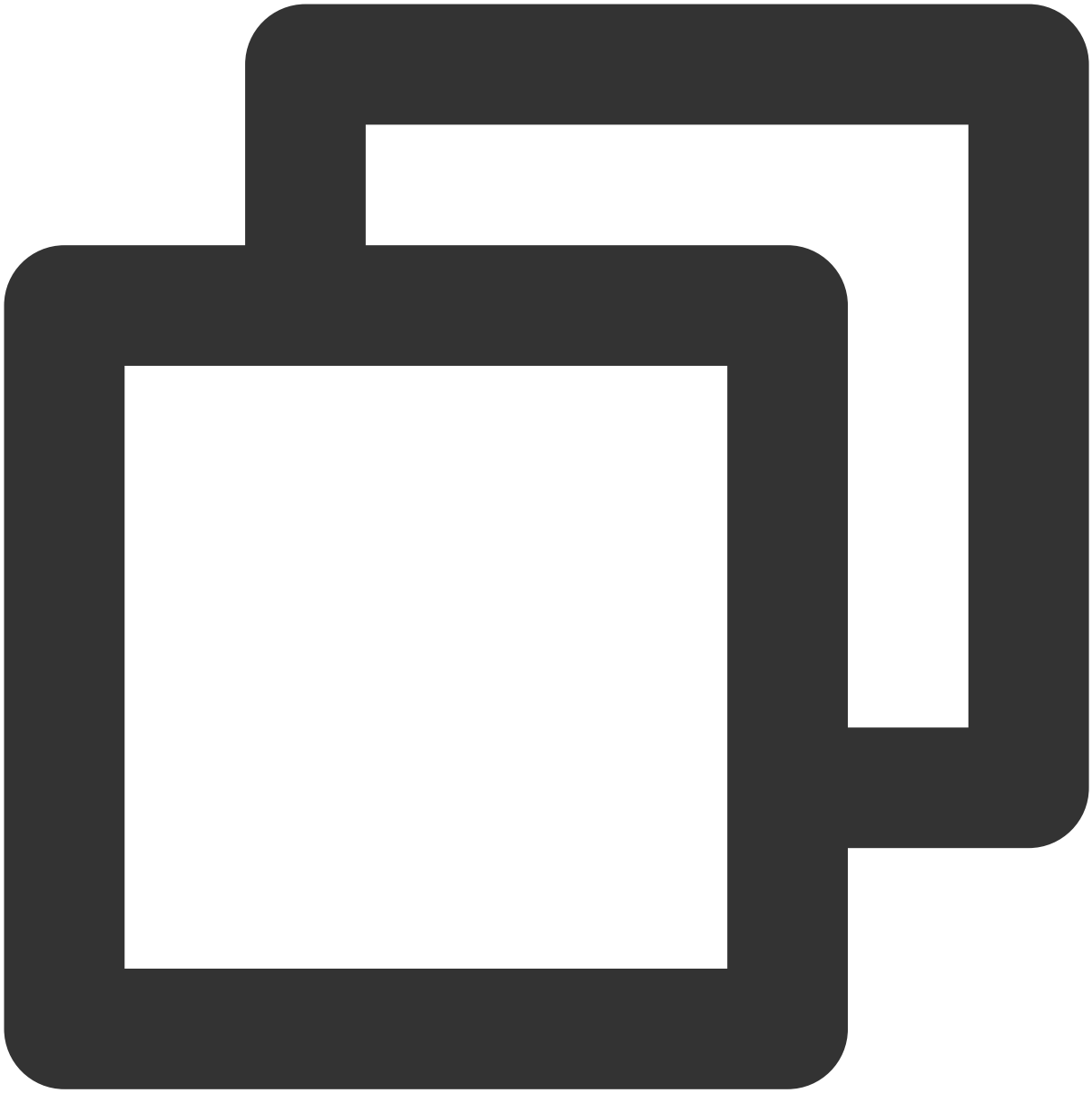
步骤3：推送容器镜像

1. 您可通过 `docker cli` 或其他镜像构建工具（例如 jenkins）推送镜像至指定镜像仓库内，本文以 `docker cli` 为例。此步骤需要您使用一台安装有 Docker 的云服务器或物理机，并确保访问的客户端已在 配置网络访问策略 定义的公网或内网允许访问范围内。
2. 参考 获取实例访问凭证 获取登录指令，并进行 Docker Login。
3. 登录成功后，您可在本地构建新的容器镜像或从 DockerHub 上获取一个公开镜像用于测试。

本文以 DockerHub 官方的 Nginx 最新镜像为例，在命令行工具中依次执行以下指令，即可推送该镜像。请将 demo-tcr、docker 及 getting-started 依次替换为您实际创建的实例名称、命名空间名称及镜像仓库名。



```
docker tag getting-started:latest demo-tcr.tencentcloudcr.com/docker/getting-starte
```



```
docker push demo-tcr.tencentcloudcr.com/docker/getting-started:latest
```

4. 推送成功后，即可前往控制台的 镜像仓库 页面，选择仓库名并进入详情页面查看。

配置 TKE Serverless 集群访问 TCR 实例

为保护您的数据安全，TCR 和 TKE Serverless 初始默认拒绝全部公网及内网访问。在准备将 TCR 的镜像部署至 TKE Serverless 之前，请先进行网络访问策略配置。

TCR 企业版实例支持网络访问控制，您可根据 TKE Serverless 集群的网络配置，选择通过公网或内网访问指定实例，拉取容器镜像。若 TKE Serverless 集群与 TCR 实例部署在同一地域，建议通过内网访问方式拉取容器镜像，该方式可提升拉取速度，并节约公网流量成本。
下文将介绍通过内网访问的方式，若要通过外网访问，请参见 通过 NAT 网关访问外网。

步骤1：在 TCR 实例中关联集群 VPC

为保障用户数据安全，新建的 TCR 实例默认拒绝全部来源的访问。为允许指定 TKE Serverless 集群可访问 TCR 实例拉取镜像，需将集群所在的 VPC 关联至 TCR 实例，并配置相应的内网域名解析。
1. 新建内网访问链路
2. 配置域名内网解析

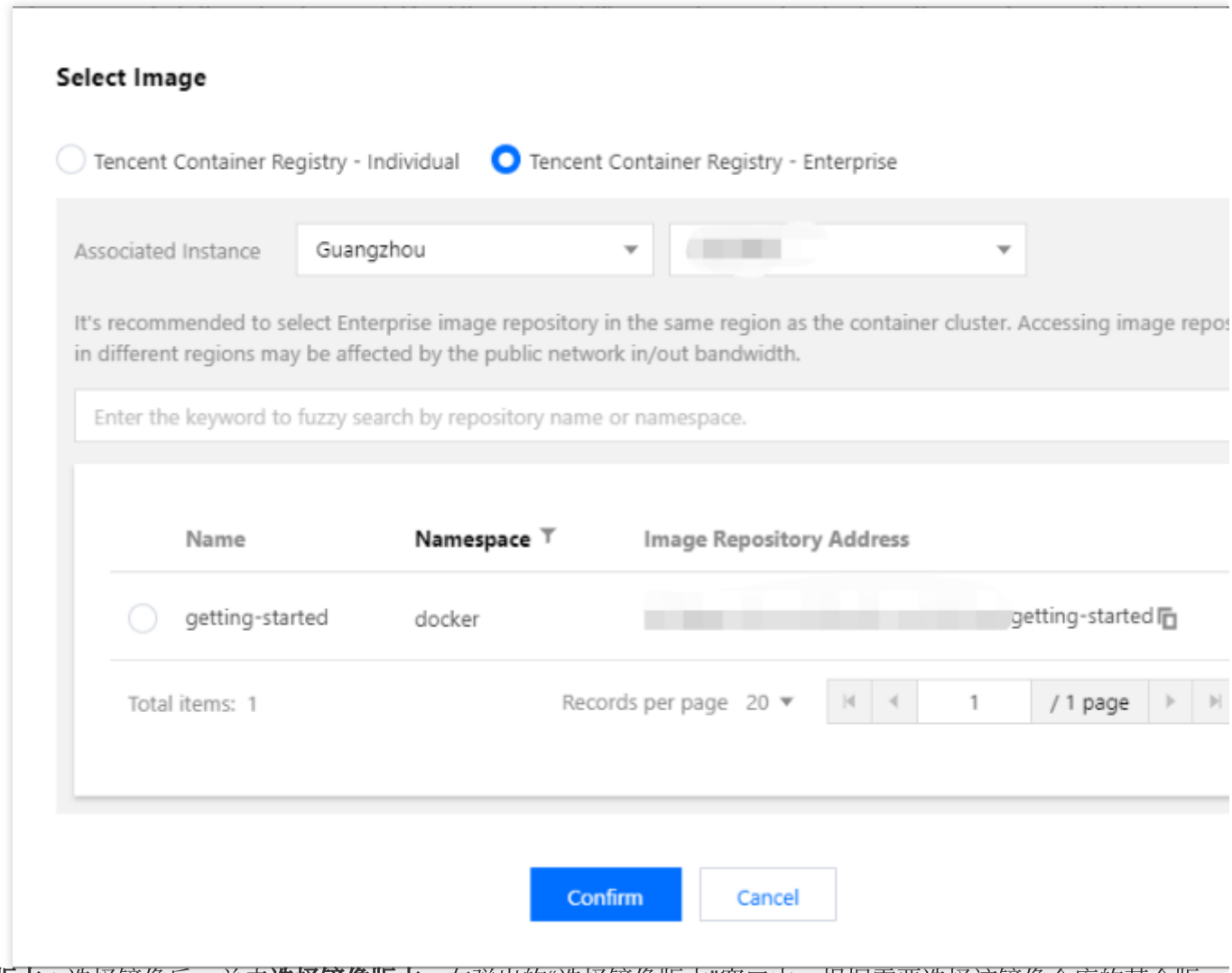
步骤2：获取 TCR 实例访问凭证

从 TCR 实例中拉取容器镜像需要首先使用凭证信息登录至实例。请参见 获取实例访问凭证，保存该实例的长期访问凭证，用于之后配置部署 TCR 镜像。

使用 TCR 实例内容器镜像创建工作负载

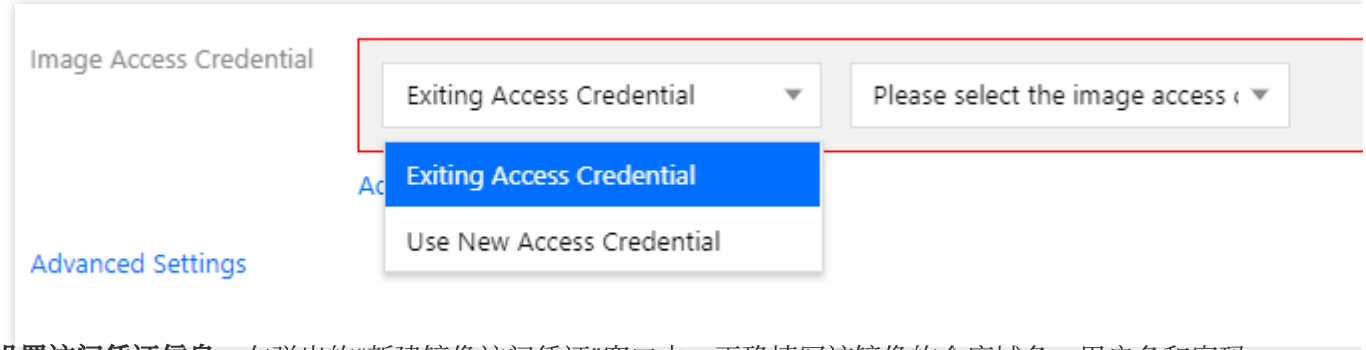
1. 登录 容器服务控制台。
2. 在**集群列表**中，选择 Serverless 集群 ID，进入集群详情页。
3. 在**集群详情**页面，选择左侧**工作负载** > **Deployment**。
4. 在 **Deployment** 页面，单击**新建**。
5. 在 **新建Deployment** 页面，参考以下主要的参数信息，创建工作负载。

命名空间：根据需要选择集群的命名空间。
实例内容器：
镜像：单击**选择镜像**，并在弹出的“选择镜像”窗口中，选择**容器镜像服务 企业版**，再根据需要选择地域、实例和镜像仓库。如下图所示：



镜像版本：选择镜像后，单击**选择镜像版本**，在弹出的“选择镜像版本”窗口中，根据需要选择该镜像仓库的某个版本。若不选择则默认为 latest。

镜像访问凭证：单击**添加镜像访问凭证**，下拉框中选择**使用新的访问凭证**。如下图所示：



单击**设置访问凭证信息**，在弹出的“新建镜像访问凭证”窗口中，正确填写该镜像的仓库域名、用户名和密码。

仓库域名：登录 容器镜像服务 控制台，选择左侧导航栏中的**镜像仓库**，即可获得所需镜像的仓库地址。

用户名：前往 账号信息 获取账号 ID，账号 ID 即为用户名。

密码：在上述 步骤2：获取 TCR 实例访问凭证中获取的访问凭证即为密码。

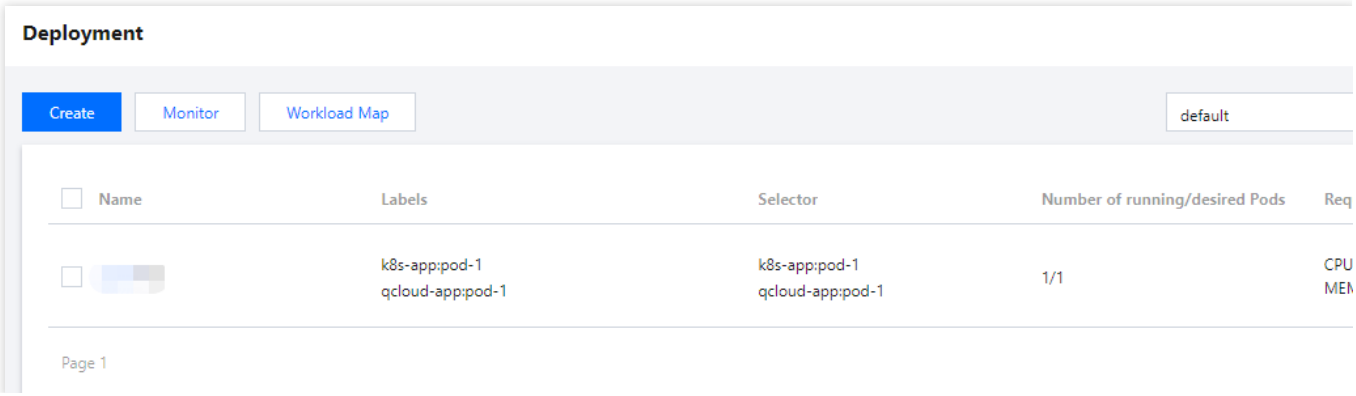
访问设置（Service）：用户在 Kubernetes 中可以部署各种容器，其中一部分是通过 HTTP、HTTPS 协议对外提供七层网络服务，另一部分是通过 TCP、UDP 协议提供四层网络服务。而 Kubernetes 定义的 Service 资源可用于管理集群中四层网络的服务访问。参考以下主要的参数信息，完成访问设置。

Service：勾选**启用**。

服务访问方式：选择**VPC内网访问**。

6. 完成其他参数设置后，单击**创建 Deployment**，查看该工作负载的部署进度。

部署成功后，可在 **Deployment** 页面查看该工作负载的“运行/期望Pod数量”为“1/1”。如下图所示：



混合云下的多平台镜像数据同步复制

最近更新时间：2023-02-13 15:12:02

操作场景

在用户的开发运维过程中，存在需要同时用到多个容器镜像仓库的场景，这些仓库可能跨主账号、跨地域、跨国、跨平台。用户可以通过手动完成实例间的推送、分发任务，但是会存在运维成本较高、同步不及时、不便于管理等问题。

基于该场景，目前 TCR 提供了同步复制功能，以及开源的镜像迁移工具。其中：

- 实例同步功能支持用户基于规则的配置来**按需同步**实例的镜像，详情请参见 配置实例同步。
- 实例复制功能支持用户从主实例**全量复制**实例镜像数据至从实例，详情请参见 配置实例复制。
- 镜像迁移工具支持**多种镜像仓库**的 Docker 镜像数据迁移，详情请参见 镜像迁移工具：image-transfer。
- 同时，用户从其他镜像仓库服务迁移至 TCR 时，还可以为 TCR 实例配置自定义域名，继续沿用原有域名，保持服务的连续性，详情请参见 配置自定义域名。

本文将介绍混合云大背景下，不同镜像仓库之间镜像数据的同步复制的经典使用场景以及对应的最佳实践。

前提条件

在创建并管理 TCR 企业版实例的复制实例前，您需要完成以下准备工作：

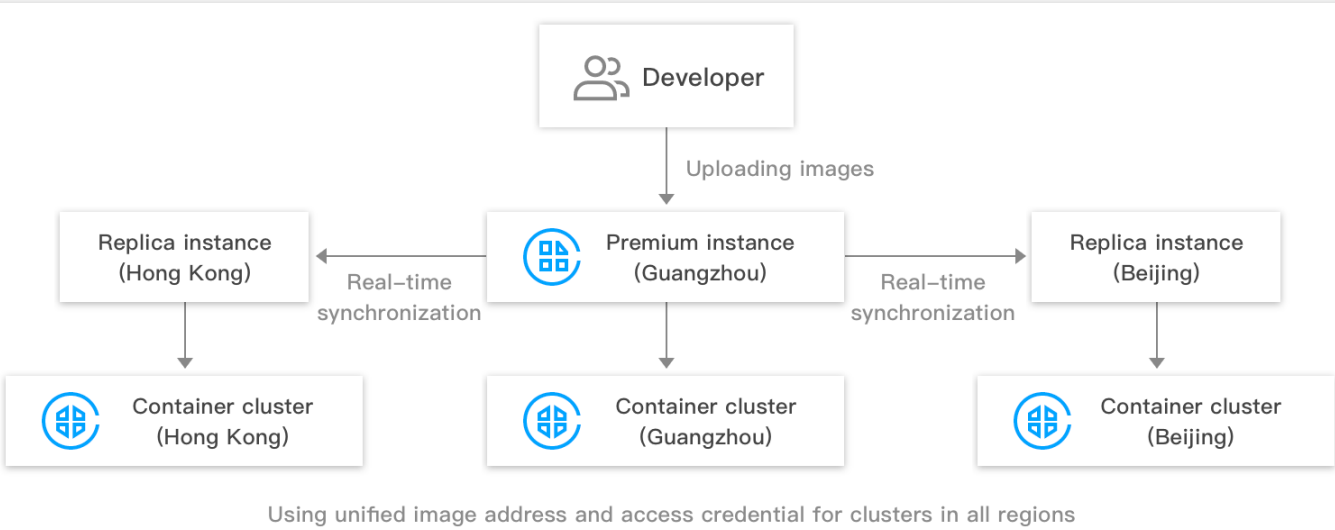
- 已成功 购买企业版实例，实例同步功能需要实例规格为标准版或高级版，实例复制功能需要实例规格为高级版。
- 如果使用子账号进行操作，请参见 企业版授权方案示例 提前为子账号授予对应实例的操作权限。

操作步骤

场景1：跨地域 TCR 实例复制

国内跨地域实例复制

当用户存在跨地域业务时，用户可以通过使用 实例复制 的功能实现单地域上传、多地域高速实时同步、就近内网拉取。相较于实例同步功能，该功能可统一多地域集群的发布配置，并提高云原生应用制品的跨地域同步速度。



跨国跨地域实例同步复制

但若当跨地域业务涉及跨国的情况时，用户还需结合 实例同步 功能的使用。出于安全合规的考虑，目前暂不支持跨国的实例复制。

1. 用户需要在国内外各购买一个 TCR 高级版实例后，首先 创建同步规则，实现跨国数据的按需同步。
2. 在两个实例里分别 创建并管理复制实例 ，实现国内和国外的单点上传、多地域实时复制、就近内网拉取。

注意：

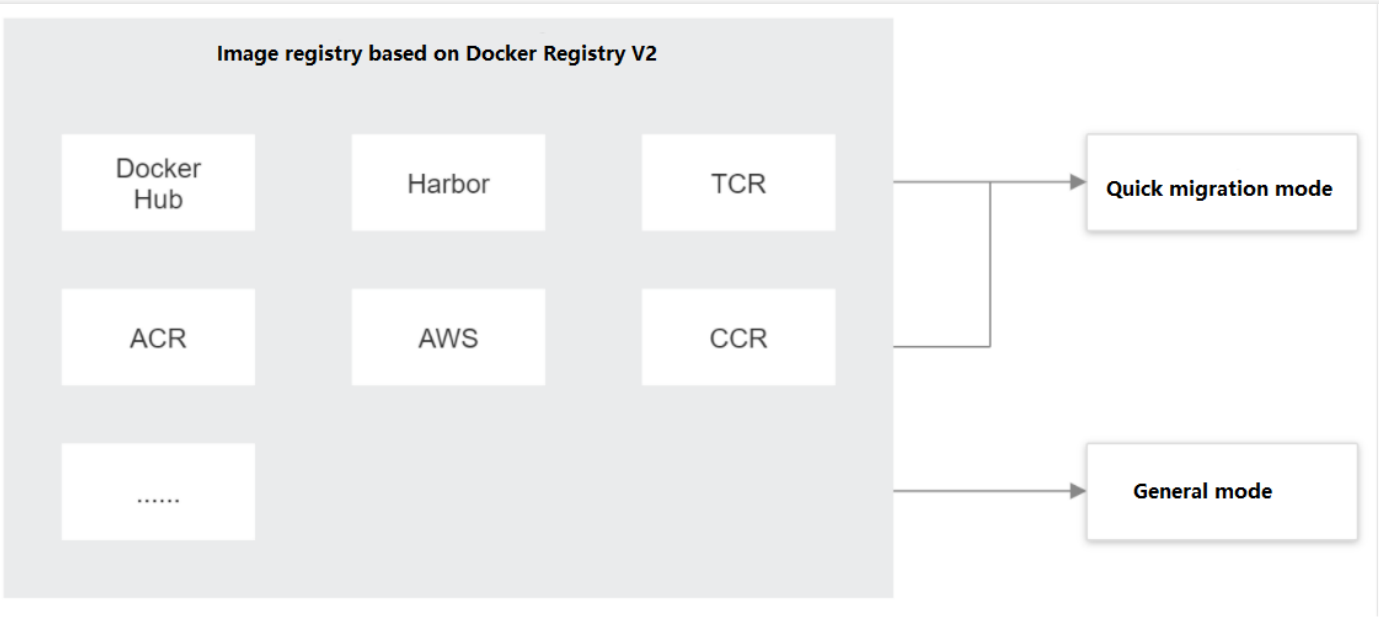
为实现就近内网拉取，需要用户手动将复制地域内的私有网络 VPC 依次接入该实例。详情请参见 内网访问控制，选择复制地域内的私有网络。

场景2：跨平台镜像迁移或同步

当用户同时使用公有云镜像仓库和自建镜像仓库，或是多家公有云镜像仓库时，往往存在跨平台的镜像迁移或同步的需求。在跨平台场景下，用户可以选择使用 TCR 的自定义域名功能，通过单一配置实现多平台的统一访问，以保证服务的连续性，详情请参见 配置自定义域名。

跨平台镜像迁移

image-transfer 是腾讯云针对镜像迁移的开源工具，支持多种镜像仓库中的 Docker 镜像之间的批量迁移，只需仓库是基于 Docker Registry V2 搭建的 Docker 镜像仓库服务（例如腾讯云 TCR 个人版（CCR）/ TCR 企业版、Docker Hub、 Quay、 阿里云镜像服务ACR、 Harbor 等）。该工具具有两种使用模式，通用模式以及用于腾讯云的一键迁移模式，如下图所示：



- 通用模式
- 一键迁移模式

使用 image-transfer 的通用模式可以实现多个镜像仓库对多个镜像仓库的镜像迁移，用户只需配置好认证鉴权文件以及迁移规则文件即可开始迁移。关于工具的下载、安装、使用方法请参见 image-transfer。

跨平台镜像同步

在跨平台的场景下，除了数据的批量迁移外，用户往往还存在跨平台镜像的实时同步需求。

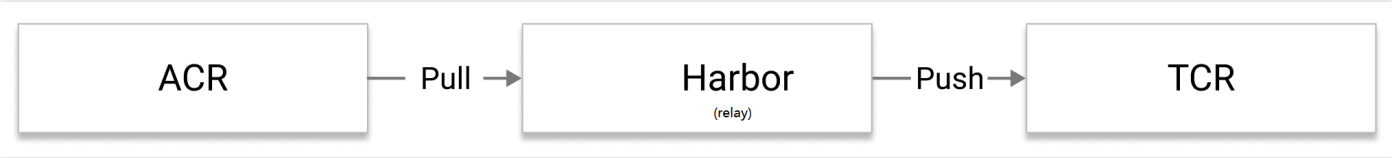
从自建 Harbor 同步镜像至 TCR 企业版，详情请参见 从自建 Harbor 同步镜像到 TCR 企业版。在 Harbor 侧配置同步规则。从自建的容器镜像服务转向使用 TCR，一方面可以减少用户自行搭建及维护的运维管理成本，并提供云上专业稳定的托管服务及技术支持。另一方面可以实现与云上容器服务的联动使用，用户可享受容器上云的一致性使用体验，可使用容器集群内网拉取镜像，降低公网带宽成本。同理，用户可以通过在 Harbor 侧配置规则，同步镜像至其他第三方仓库服务平台。除 Harbor 本身外，目前 Harbor 支持的镜像仓库服务如下：

- Docker Hub
- Docker registry
- AWS Elastic Container Registry
- Azure Container Registry
- Ali Cloud Container Registry
- Google Container Registry
- Huawei SWR
- Artifact Hub
- Gitlab
- Quay
- Jfrog Artifactory
- Tencent Container Registry

用户还可以通过将自建 Harbor 仓库作为中转仓库，实现第三方仓库服务平台之间的镜像同步。

如下图所示，以**将阿里云 ACR 的镜像实时同步至腾讯云 TCR**为例：

1. 在 Harbor 里配置 Pull-based 复制策略，将 ACR 的镜像实时拉取至 Harbor 中，作为中转。
2. 在 Harbor 里配置 Push-based 复制策略，将 Harbor 内来自 ACR 的镜像实时推送至 TCR 中。



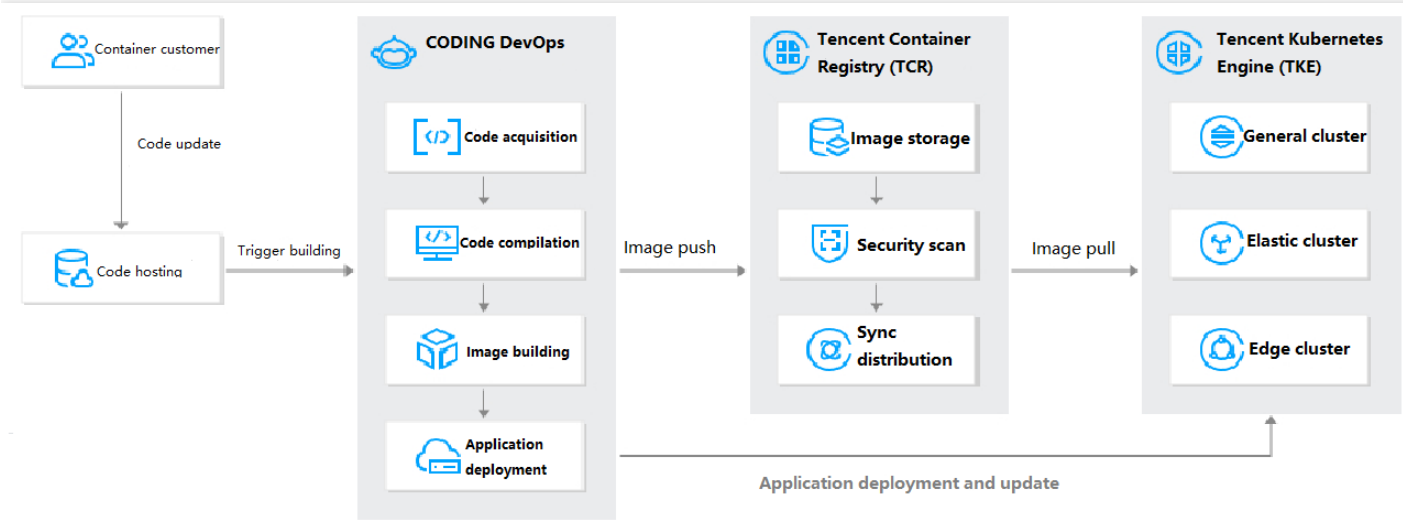
以此便实现了将镜像从阿里云 ACR 同步至腾讯云 TCR，其他平台之间的镜像同步也同理。

场景3：DevOps 镜像流转

在开发和运维过程中，一个应用从开发到上线往往要经历多个步骤：开发、测试、进入准生产环境、最终上线进入生产环境，相应的镜像也要经过多个步骤的流转。

用户可以利用 TCR 实例同步功能搭建上述的 DevOps 流水线实现镜像的流转。若上述不同环境所属的主账号不同，请在配置实例同步规则时开启“支持跨主账号实例同步”。

用户还可以使用交付流水线功能实现推送代码自动触发镜像构建和应用部署或本地推送镜像后自动触发部署。



注意：

目前 TCR 的交付流水线功能仅支持预置的固定流水线，如果用户有上述更加复杂的 DevOps 流水线的需求，可以使用 CODING DevOps。CODING DevOps 是腾讯云的一站式 DevOps 研发实践工具，TCR 的交付流水线功能依赖于 CODING DevOps 的持续集成与持续部署功能。

全球多地域间同步镜像实现就近访问

最近更新时间：2023-02-09 17:28:26

场景介绍

当企业将容器业务拓展至多个地域时，希望能够就近拉取容器镜像，以提高拉取速度，降低跨地域公网流量成本；或需要在多个地域内实现热备份，以及在同个地域内多个镜像仓库服务间传递镜像，如跨团队共享，从开发仓库流转至生产仓库等。上述场景下，常规最佳实践是在一个或多个地域内同时创建并维护多个容器镜像仓库服务（Docker Registry），并编写脚本调用 Docker Push/Pull 实现跨仓库复制镜像。容器镜像服务 TCR 企业版同时提供容器镜像跨实例按需同步和单实例多地复制的能力，用户可灵活选择或结合使用两项能力，满足上述场景的需求。其中，两项能力具有如下优势：

实例同步

在多个实例间（可在同一地域或多个地域）间自动按需同步指定镜像。

- 按需同步，基于自定义规则实现对目标实例，需要同步镜像的精确匹配选择。
- 自动同步，需要同步的镜像推送至源实例后，自动触发同步至目标实例。
- 跨主账号同步，可在同一集团内多个主账号下的实例间同步公共镜像。
- Helm Chart 及容器镜像筛选，可选仅同步一种类型的云原生制品。
- 可查询同步日志，并可与触发器配合使用，实现同步成功事件周知。

实例复制

为单个实例在多个地域内配置副本（子实例）并提供就近访问能力。

- 单一实例，多个地域内访问时，可使用同一个镜像仓库/版本名称，保持容器配置统一。
- 就近访问，在多地域部署场景中，就近拉取同地域内镜像数据，提高部署的效率及稳定性。
- 降低成本，就近内网拉取镜像可避免跨地域访问镜像仓库带来的公网流量费用或专线费用。
- 简化管理，无需管理多个实例，并配置实例间的同步规则，无需关心指定镜像的同步状态。
- 高速同步，镜像 Layer 数据实时跨地域流式复制，可实现单地镜像推送，即可多地域拉取。

使用案例

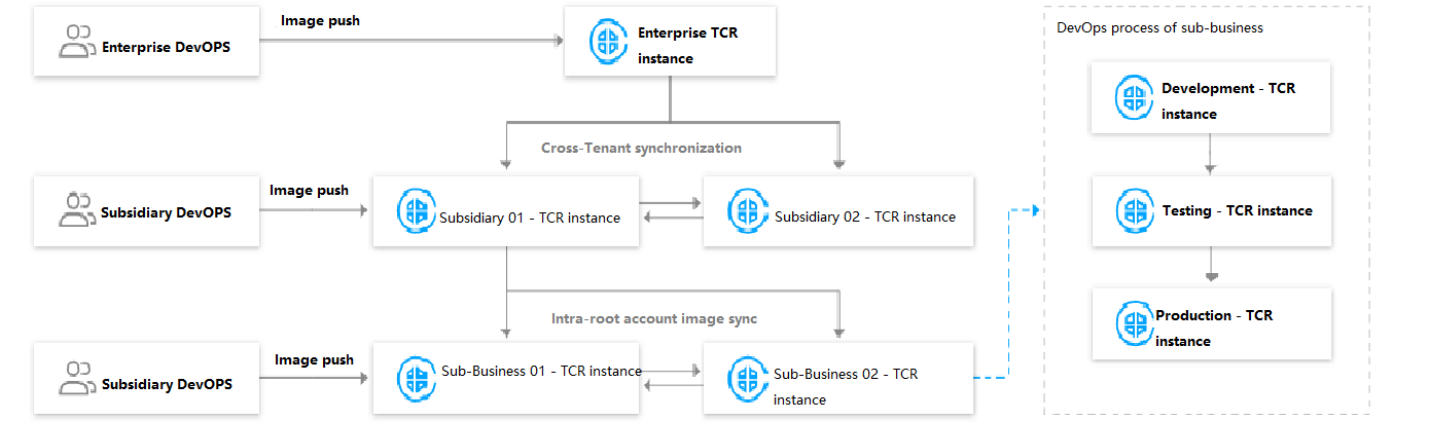
场景1：出海业务实现全球多地域就近访问

一家游戏开发商希望在全球多个地域内同时部署容器化游戏业务，需要实现容器镜像的全球多地域同步及就近访问。同时出于数据合规限制，需要对中国及境外数据进行独立管理，控制数据传输。该客户采用如下方案，实现了全球多地域的数据同步及就近访问，并保持了统一配置，显著提高了业务发布效率和稳定性。

在此方案中，客户在北京及法兰克福同时创建两个独立实例，并配置实例同步规则，按需同步面向生产发布的镜像。同时在北京，法兰克福实例内，均配置多个复制实例，如北京实例内包含上海，成都，广州三个子实例。当需要发布最新游戏版本时，北京研发团队推送国内及境外最新版本的容器镜像，其中境外版本自动同步至法兰克福，而后实时复制至硅谷，弗吉尼亚，孟买，新加坡等地。新加坡容器集群更新最新镜像时，通过内网就近访问新加坡的复制实例，实现生产容器的快速稳定更新。

场景2：大型集团内多个子公司及业务间流转镜像

一家大型企业内有多家子公司/BG，且某个子公司内具有多个业务方向，并配置独立的 IT 团队。为独立管理云上资源的权限及成本，多个子公司及业务间使用不同的腾讯云主账号。该客户采用了以下方案，实现了全集团内基础镜像的共享及多个业务间的镜像共享。



在此方案中，多个子公司账号下实例间配置了跨主账号实例同步，实现了公共镜像的共享；在单个子公司内，由基础平台的管理员统一配置各个业务实例间的基础镜像同步；在部分业务内，拟采用多个实例独立管理业务开发，测试及生产阶段的镜像，并基于镜像版本（tag）实现业务镜像在各个生产阶段的自动流转。

> 注意：
> 以上两个场景均是较为复杂的使用场景，常规业务可仅选取案例中部分方案满足自身需求，如跨地域热备份，国内多地域就近访问，同地域内多实例间业务镜像流转等。
> 同时，企业版实例支持使用自定义域名，结合 DNS 服务，可实现多个实例共用同一个域名，进而实现镜像发布配置统一及多地域就近内网访问，在实例管理上更加灵活。

操作指南

前提条件

- 已成功 购买企业版实例，实例同步功能需要实例规格为标准版或高级版，实例复制功能需要实例规格为高级版。
- 如果使用子账号进行操作，请参见 企业版授权方案示例 提前为子账号授予对应实例的操作权限。

配置实例同步

具体操作指南请参考 同步复制-配置实例同步。
其中，实例同步支持跨主账号同步，可在创建同步规则时进行配置。

配置实例复制

具体操作指南请参考 同步复制-配置实例复制。
其中，实例复制暂不支持国内及境外地域内复制，如无法为北京地域内高级版实例配置硅谷的复制实例。

配置自定义域名

具体操作指南请参考配置自定义域名。
其中，自定义域名解析需要独立配置，国内站可使用 PrivateDNS 产品，国际站该产品暂不支持，建议使用自建 DNS 服务。

排障指南

1. 实例同步失败，该如何处理？

可前往产品控制台，查看相关规则及同步日志，并手动触发同步；如果同步过慢或仍同步失败，请通过 提交工单 联系我们。

2. 实例复制失败，该如何处理？

当前实例复制暂不支持查看具体仓库的同步日志，请耐心等待实例复制过程，待状态更新为“同步成功”后再尝试访问镜像。如实例复制状态始终无法更新为同步成功，或同步成功后仍无法领取镜像，请通过 提交工单 联系我们。

3. 如何确定指定镜像已被复制到某个子实例内？

当前实例复制支持查看历史同步任务，可通过任务详细日志判断指定镜像仓库或镜像的同步状态。

4. 如何提高跨地域实例同步的速度？

当前暂不支持单独提高指定账号或实例的跨地域同步速度，该速度受限于跨地域云联网的带宽，且在多租户间共享，如需特殊保障，请通过 提交工单 联系我们。

使用自定义域名及云联网实现跨地域内网访问

最近更新时间：2023-02-28 16:35:24

操作场景

容器镜像服务 TCR 企业版支持网络访问控制，支持用户接入指定的私有网络 VPC，允许该 VPC 内 Docker 客户端通过内网访问镜像数据。随着多云/分布式云的概念普及及实践落地，用户的容器集群不再仅位于腾讯云指定地域单个私有网络 VPC 内，而可能分布在多个云厂商，IDC 的复杂网络内，而这些复杂网络可能通过云联网、对等连接的网络产品实现互通。此背景下，用户需要多地域、多私有网络同时接入 TCR 企业版单个实例，并实现正常的内网推送、拉取镜像。

本文主要介绍企业客户如何使用自定义域名，并配合云联网、对等连接，PrivateDNS 产品实现多私有网络 VPC 同时支持接入 TCR 实例，并正常通过内网分发容器镜像。

特别说明，如您的业务分布在多云、多地域，为实现数据的容灾备份、就近访问，建议您同时参考 混合云下的多平台镜像数据同步复制 、 全球多地域间同步镜像实现就近访问 最佳实践，综合业务需要选择最佳方案。

前提条件

您需要确认并完成以下准备工作：

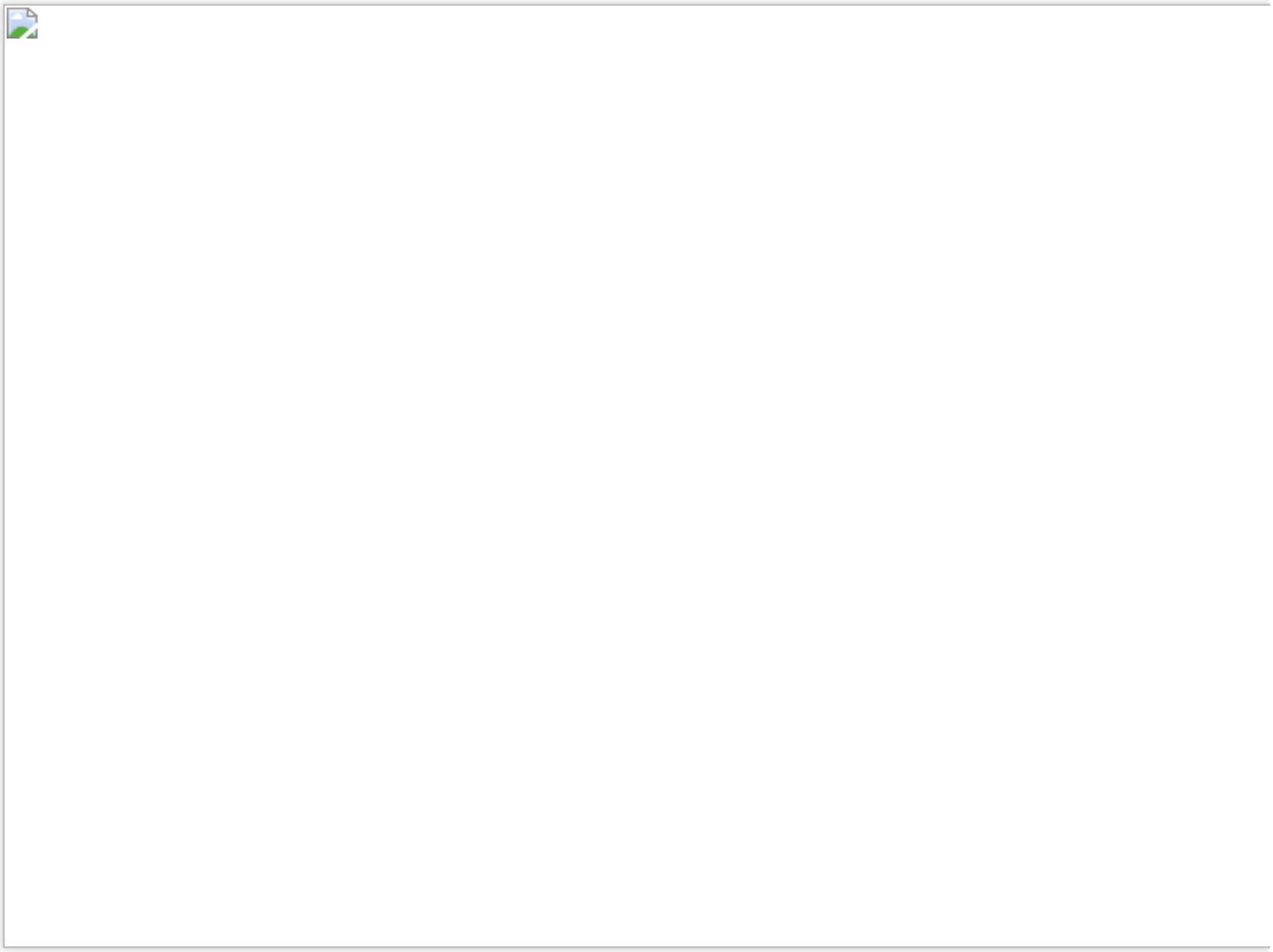
已 购买企业版实例，且操作人具有实例管理权限，如 QcloudTCRFullAccess。

具有合法的域名，具体请参考 配置自定义域名 中相关说明。

已开通云联网、对等连接等服务，并接入多个私有网络 VPC。

整体架构

客户在广州、上海均部署容器化业务，并同时使用位于广州的 TCR 企业版实例托管分发容器镜像。



配置详情

创建 TCR 企业版实例，并绑定自定义域名

1. 在容器业务部署地域购买企业版实例，具体请参考 购买企业版实例，本最佳实践选择 广州(ap-guangzhou、gz) 地域。
2. 初始化实例，上传首个镜像，具体请参考 企业版快速入门。此步骤中即接入指定私有网络 vpc-gz-01，并通过内网推送镜像。
3. 配置自定义域名，具体请参考 配置自定义域名。

使用云联网关联多个私有网络 VPC

1. 前往 私有网络控制台，新建云联网，关联广州、上海多个私有网络 VPC。

2. 可选使用 对等连接 功能关联上述私有网络 VPC。

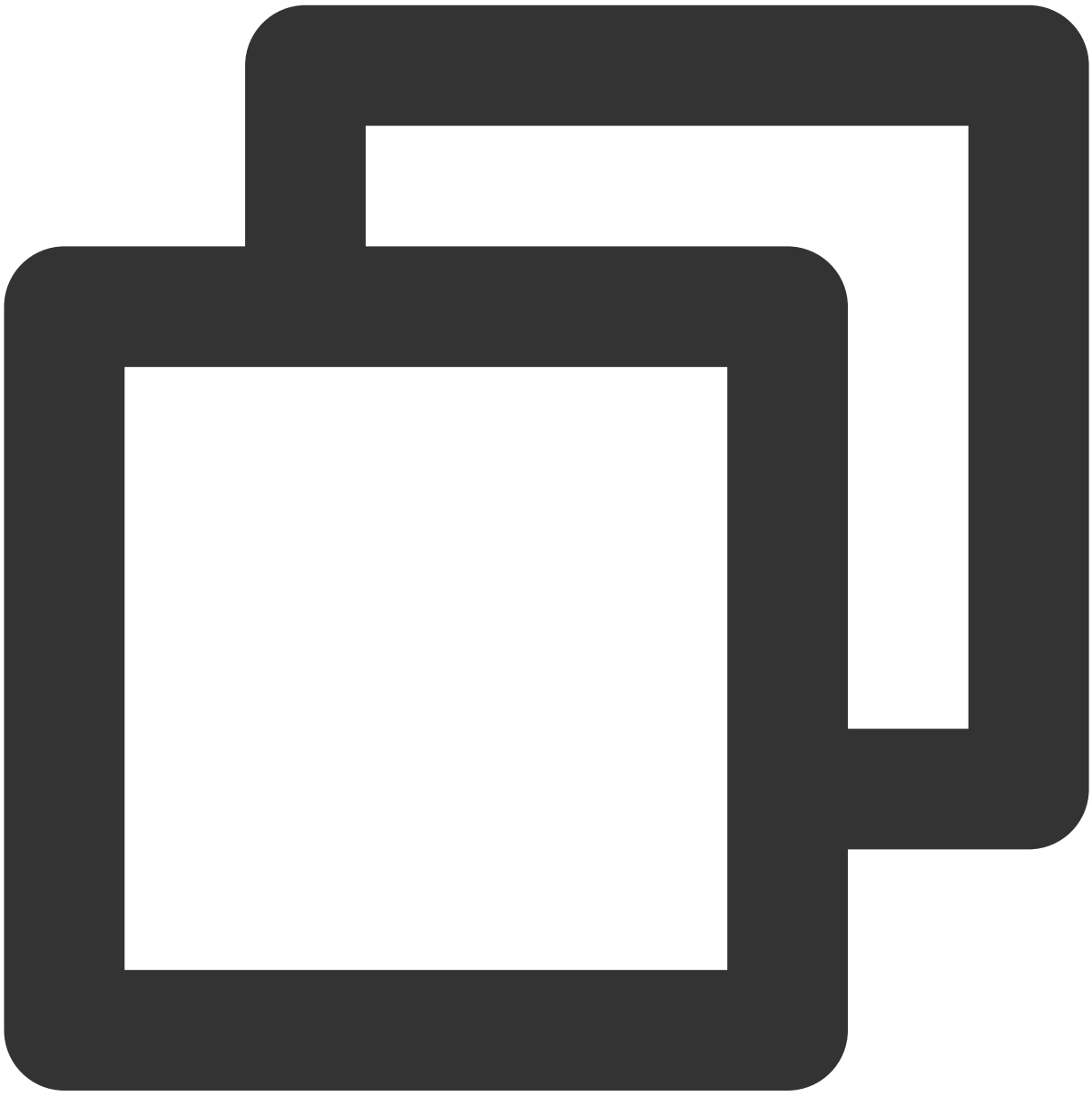
配置自定义域名的私有域解析

1. 前往 Private DNS 控制台，使用已绑定的自定义域名，新建 Private Zone，关联上述私有网络 VPC。
2. 配置解析记录，选择 A 记录，使用 @ - 直接解析主域名，并配置记录为已接入的私有网络对应的内网解析 IP。

场景验证

验证已接入实例的私有网络 VPC

1. 在广州的已接入的私有网络 VPC 内新建云服务器，并安装 Docker 客户端。
2. 登录至云服务器，并尝试拉取镜像，参考以下指令，其中 demo-tcr.cn 可替换为实际绑定的自定义域名，并将 demo/nginx:latest 替换为实际的惊镜像地址，其中 demo 是命名空间。

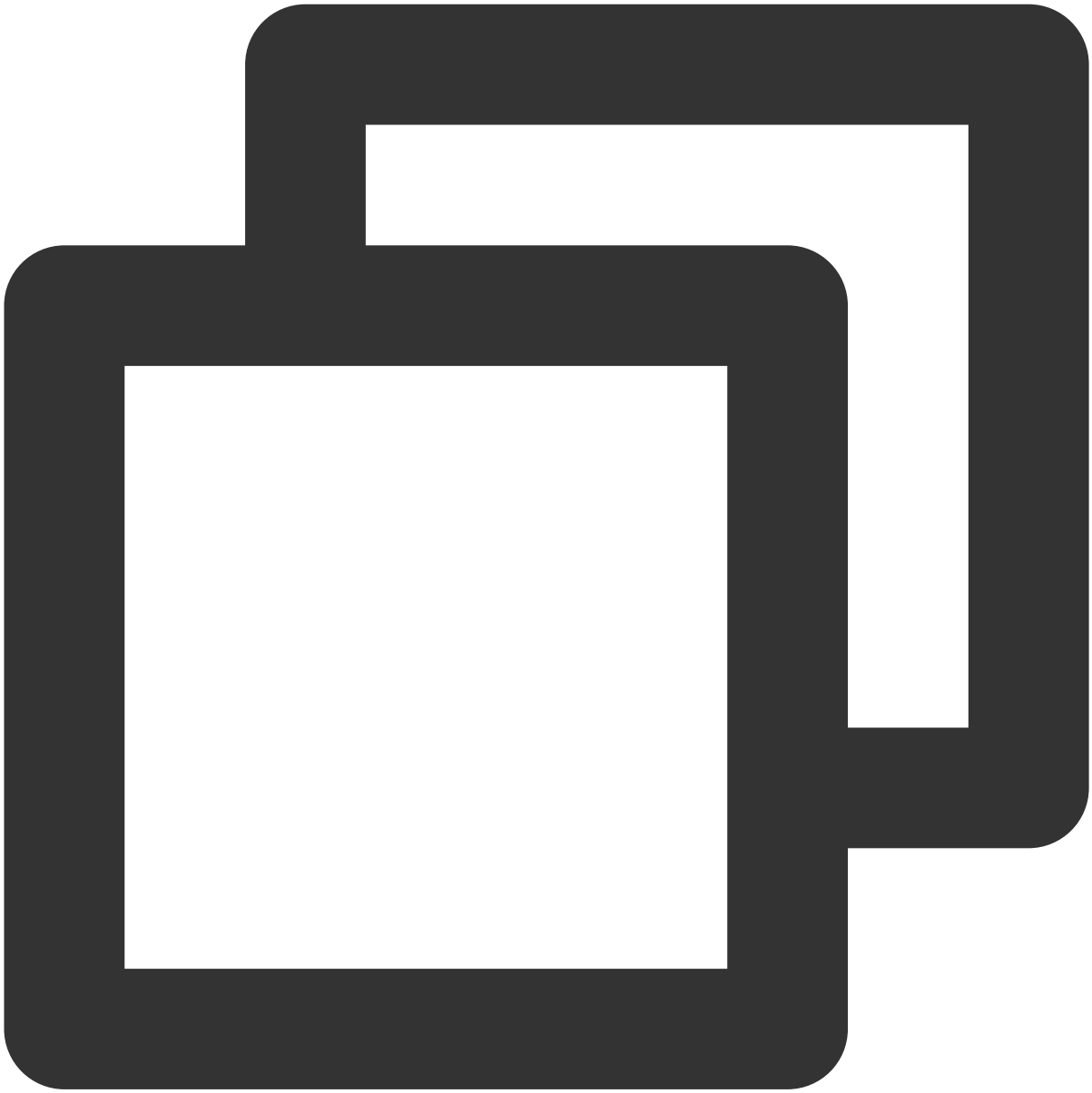


```
# 在位于广州的容器集群内拉取镜像
docker pull demo-tcr.cn/demo/nginx:latest
```

镜像拉取成功则说明 私有网络接入、自定义域名、私有域解析 配置正常，广州 VPC 内容器集群已可使用自定义域名通过内网拉取镜像。

验证已接入云联网的其他私有网络 VPC

1. 在上海的已接入云联网的私有网络 VPC 内新建云服务器，并安装 Docker 客户端。
2. 登录至云服务器，并尝试拉取镜像，可使用相同路径，直接拉取位于广州的企业版实例。



```
# 在位于上海的容器集群内拉取镜像
docker pull demo-tcr.cn/demo/nginx:latest
```

镜像拉取成功则说明云联网配置正常，上海 VPC 内容器集群已可使用自定义域名跨地域通过内网拉取镜像。