容器镜像服务

操作指南

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南
- 创建企业版实例
- 访问配置
  - 访问凭证配置
    - 用户级账号管理
    - 服务级账号管理
  - 访问网络控制
    - 访问网络控制概述
    - 配置公网访问控制
    - 配置内网访问控制
  - 访问权限配置
    - 访问权限管理概述
    - 基于 CAM 管理子账号权限
  - 访问域名配置
    - 配置自定义域名
- 镜像创建
  - 管理命名空间
  - 管理镜像仓库
- 镜像分发
  - 同实例多地域复制镜像
  - 跨实例（账号）同步镜像
  - 按需加载容器镜像
- 镜像安全
  - 容器镜像安全扫描
  - 镜像版本不可变
  - 高危镜像部署阻断
  - 容器镜像签名
- 镜像清理
  - 清理 COS 存储空间
  - 自动删除镜像版本
- DevOps
  - 触发器（Webhook）
  - 镜像自动部署
  - 镜像自动构建
- OCI 制品管理
  - OCI 制品管理概述
  - 托管 Helm Chart
- 个人版操作指南
  - 更新登录密码
  - 配置访问权限
    - 个人版接入 CAM 的 API 列表
    - 个人版授权方案示例
    - 个人版资源级 API 接口及授权方案变更指南
  - 设置镜像清理
- 销毁退还实例

版权所有：腾讯云计算（北京）有限责任公司

操作指南
创建企业版实例

最近更新时间：2024-03-25 11:04:31

操作场景

本文档介绍如何通过容器镜像服务购买页选购腾讯云容器镜像服务 TCR 企业版实例。

前提条件

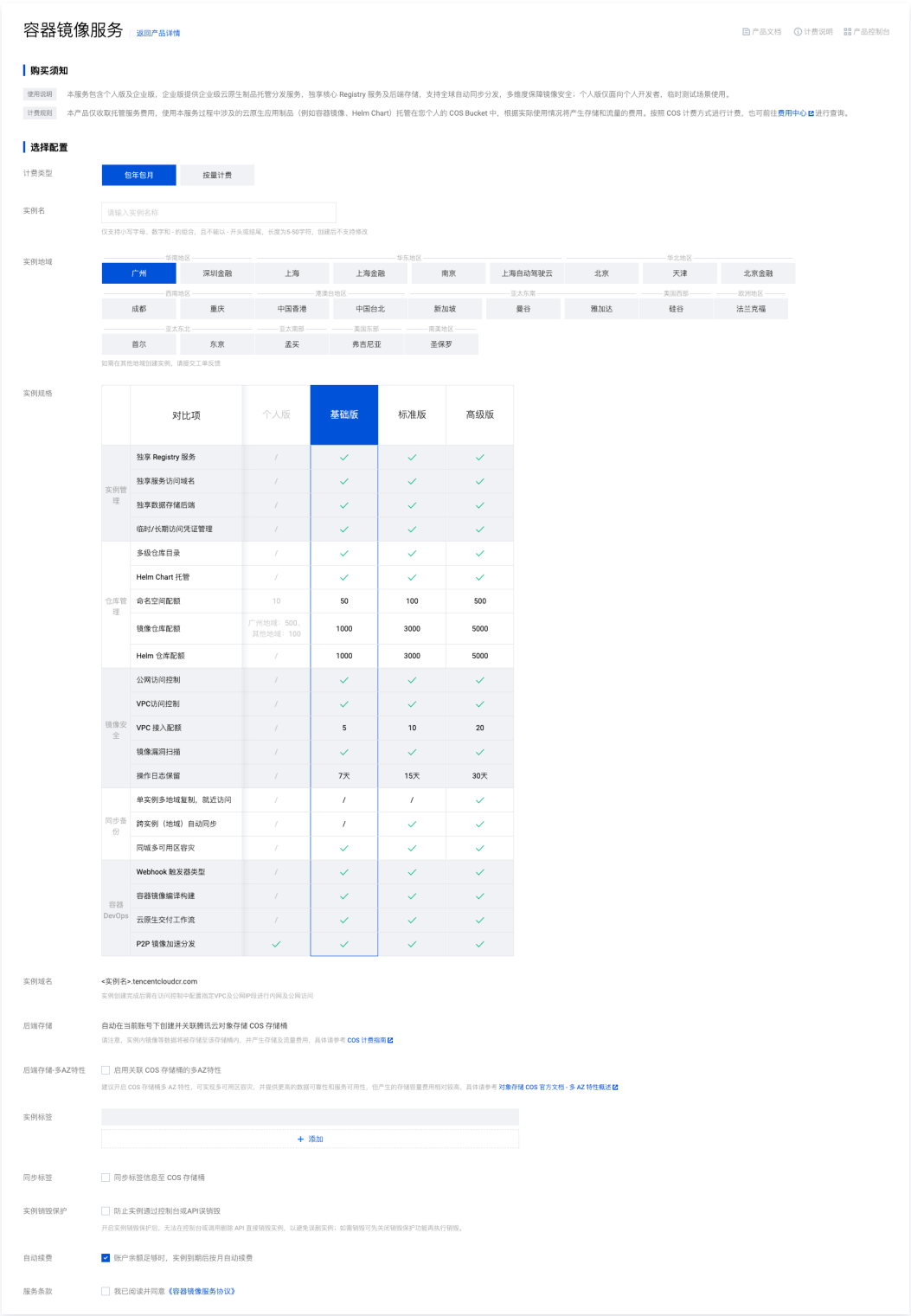
在购买 TCR 企业版实例前，您需要完成以下准备工作：

- 注册腾讯云账号，并完成 实名认证。
- 已开通容器镜像服务所依赖的云产品 对象存储，用于存储镜像数据。
- 已开通容器镜像服务所依赖的云产品 私有网络，私有域解析 PrivateDNS，用于在私有网络 VPC 环境内推送，拉取镜像。
- 已在控制台开通服务，并授权您的对象存储、私有网络等资源部分操作权限。

操作步骤

使用控制台创建

1. 登录 腾讯云官网，选择 容器镜像服务，**单击立即选购**，进入容器镜像服务控制台。
2. 选择左侧导航栏中的**实例管理**，进入**实例管理**页面并单击**新建**。
3. 在**容器镜像服务**购买页中，参考以下信息购买实例。如下图所示：



- **计费类型**：容器镜像服务 TCR 提供两种类型的计费方式：包年包月和按量计费。详情请参见容器镜像服务 计费概述 。
- **实例名**：输入自定义实例名称。该名称全局唯一，请避免与自己或他人现有实例名称重复。该名称将直接用于该实例 Registry 服务的访问域名，**购买后不可修改**，请谨慎选择。建议组合使用公司、实例所在地域或项目的缩写。
- **实例地域**：选择您希望部署该实例的地域。**实例购买后地域将无法更改**，请根据容器集群资源所在地进行选择。
- **实例规格**：选择您希望购买的实例规格。不同实例规格具有不同的实例性能及配额，请参考页面内规格对比进行选择。
- **实例域名**：自动生成的实例访问域名，前缀与实例名一致。**实例购买后，实例域名无法修改**。使用 `docker login` 命令登录实例时，即使用该域名。
- **后端存储**：实例购买时将自动在当前账号下购买并关联腾讯云对象存储 COS 存储桶，实例内镜像等数据将被存储至该存储桶内，并产生存储及流量费用，详情请参见 COS 计费指南 。您可在实例购买后前往 COS 控制台查看该存储桶，请避免误删该存储桶，否则实例内托管的镜像等数据将无法找回。
- **后端存储-多AZ特性**：可选启用关联 COS 存储桶的多AZ特性。建议开启 COS 存储桶多 AZ 特性，可实现多可用区容灾，并提供更高的数据可靠性和

服务可用性，但产生的存储容量费用相对较高，详情请参见 对象存储 COS 官方文档 – 多 AZ 特性概述 。

- **实例标签**：为新建的实例绑定腾讯云标签，也可在实例购买后在实例详情页进行绑定与编辑。

4. 阅读并勾选《容器镜像服务协议》。
   企业版实例按照实例所在地域及规格收取不同费用，请在配置完成基本信息后确认已选规格及配置费用。
5. 勾选该选项后可单击**立即购买**，购买已选配置的企业版实例。
6. 您可在“实例管理”页面查看实例购买进度，当实例状态为“运行中”时，则表示当前实例已成功购买并处于可用状态。

> **说明**
> 若实例购买花费时间过长，或显示状态为异常，您可通过 在线咨询 联系我们。

使用 API 创建

您还可以使用 CreateInstance 接口创建实例。详细信息请参见 创建实例 API 文档 。

注意事项

如选择使用按量计费模式购买企业版实例，实例创建后将按小时产生费用，具体费用金额为购买页展示的费用。您可前往 计费中心 查询本服务产生的费用。如对扣费产生疑问，请 在线咨询 联系我们。

访问配置
访问凭证配置
用户级账号管理

最近更新时间：2024-03-25 18:30:23

操作场景

推送拉取容器镜像需要首先使用凭证信息登录至实例，即在 Docker 客户端中执行 `docker login` 命令并输入用户名及密码，该用户名及密码仅用于该实例的登录及认证鉴权，不可用于其他场景。本文档介绍如何在企业版实例中管理与腾讯云账号关联的用户级账号。
当用户购买企业版实例后，若希望交由多个子账号同时管理使用，如推送/拉取镜像，可先由账号管理员配置各子账号权限（请参见 企业版授权方案示例 ），子账号登录产品控制台后，可生成用户级账号，即与自己身份关联的 Docker Registry 访问凭证（访问凭证的用户名与腾讯云子账号 ID 相同），并用于执行仓库登录，镜像推送、拉取。使用与子账号关联的用户级账号操作镜像时，读写行为将被记录，并可追溯至账号持有人，可用于内部审计。
在创建用户级账号时，可选创建临时访问凭证，或生成长期访问凭证。建议日常临时推送/拉取镜像时使用临时访问凭证，避免凭证泄漏造成数据安全风险。

- **长期访问凭证**：生成后永久有效，支持禁用及删除。长期访问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**
> 长期访问凭证生成后请妥善保管，如果遗失请及时禁用或删除。

- **临时登录指令**：1小时内有效，生成后无法禁用及吊销。临时登录指令可应用在临时使用，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。

前提条件

在获取 TCR 企业版实例访问凭证前，您需要完成以下准备工作：

- 已成功 购买企业版实例 。
- 如需通过 API 获取访问凭证，需获取 API 3.0 调用所需的 API 密钥 。

操作步骤

获取长期访问凭证

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**访问凭证**，并选择**用户级账号**。
2. 在**用户级账号**页面中选择地域及实例名称，并单击**新建**。
3. 在**新建访问凭证**页面中，按照以下步骤进行获取：
   3.1 在**新建访问凭证**步骤中，输入凭证用途描述并单击**下一步**。
   3.2 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**。

4. 创建完成后即可在**访问凭证**页签中查看，您还可进行访问凭证的禁用及删除操作。

获取临时登录指令

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**访问凭证**，并选择**用户级账号**。
2. 在**用户级账号**页面中选择地域及实例名称，并单击**生成临时登录指令**。
3. 在**临时登录指令**页面中，单击**复制登录指令**即可获取临时访问凭证。

使用 API 创建

您还可以使用 CreateInstanceToken 接口创建实例访问凭证，详细信息请参见 创建实例访问凭证 。

后续操作

请参考 登录 Registry 实例 登录企业版实例。

注意事项

使用部分功能时，将自动创建长期访问凭证，包含以下场景：

1. 在容器服务 TKE 集群中安装 TCR 插件，将会自动创建所选实例的长期访问凭证。该凭证暂不会随着插件删除而自动销毁，如不再需要使用，请手动删除自动创建的访问凭证。
2. 使用镜像构建，交付流水线功能时，将自动专用的访问凭证，并提供给 CODING DevOps 服务，用于推送自动构建的镜像，请勿直接删除该访问凭证，将会导致已有镜像构建配置失效。

服务级账号管理

最近更新时间：2024-03-06 17:05:51

操作场景

推送拉取容器镜像需要首先使用凭证信息登录至实例，即在 Docker 客户端中执行 `docker login` 命令并输入用户名及密码，该用户名及密码仅用于该实例的登录及认证鉴权，不可用于其他场景。本文档介绍如何在企业版实例中管理自定义的服务级账号，用于 CI/CD 等自动化场景。
当用户购买企业版实例后，可创建与腾讯云账号绑定的用户级账号，用户名与账号 ID 相同，密码为随机生成长字符串，具体可参考 用户级账号管理 。用户级账号与腾讯云账号关联，可基于 访问管理 CAM 功能精细化配置账户权限，并可追溯仓库登录，镜像推送、拉取操作。但当对应子账号被删除或禁用时（如账号使用者转岗或离职，需要注销对应子账号），关联的用户级账号也将失效。如果该用户级账号被使用在 CI/CD 等自动化系统中，或已配置在 Kubernetes 集群中，将可能导致镜像推送、拉取失败，进而影响业务。同时，基于访问管理 CAM 进行权限管理较为复杂，如需按照命名空间维度为各个团队配置权限，需要配置复杂的 CAM 策略。
如您遇到上述问题，可选择使用服务级账号功能。该功能支持：

- 创建管理服务级账号，可自定义用户名及密码。
- 可自定义权限范围，按照命名空间层级配置读写、只读权限。
- 可自定义过期时间，支持按天设置，并可临时禁用账号。

> **注意：**
> 1. 服务级账号支持操作审计，即操作审计日志中会记录上传、下载操作所使用的服务级账号，但平台无法验证、追溯服务级账号的实际使用者身份，请谨慎对外分发使用服务级账号。如需严格审计镜像拉取推送行为的操作者或是账号持有者，请选择用户级账号。
> 2. 服务级账号权限配置独立于访问管理 CAM，因此具有服务级账号创建权限的子账号，创建的服务级账号对部分命名空间的操作权限，可能超出该子账号关联的用户级账号权限，存在越权风险。因此，请严格限制服务级账号功能的授权范围，建议仅授予实例管理团队。

前提条件

在使用 TCR 企业版实例服务级账号功能前，您需要完成以下准备工作：

- 已成功 购买企业版实例。
- 如需通过 API 获取访问凭证，需获取 API 3.0 调用所需的 API 密钥。

操作步骤

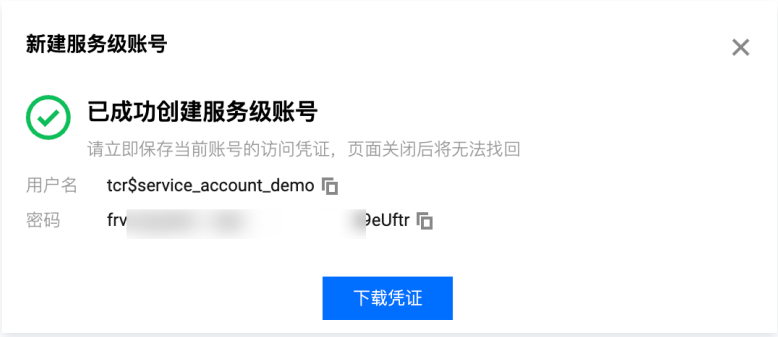
创建服务级账号

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**访问凭证**，并选择服务级**账号**。
2. 在服务级**账号**页面中选择地域及实例名称，并单击**新建**。
3. 在**新建**服务级**账号**页面中，按照以下步骤进行配置：
   - **名称**：由小写字符、数字和 ._- 组成，且至少1个字符并以字符或者数字开头。请注意，名称将自动增加前缀用于标记该账号为服务级账号，如填写 robot-demo，则实际使用的用户名为：tcr$robot-demo。

     > **说明：**
     > 部分开源 CI/CD 平台可能无法正确处理 tcr$ 前缀，如遇到问题请 提交工单 灰度更新实例，更新后可替换为 tcr@ 前缀。

   - **描述**：该账号的描述信息，支持中文。
   - **过期时间**：可选永不过期，或指定天数过期，默认为30天。
   - **权限配置**：支持选择多个命名空间，并独立配置各个命名空间的权限类型；建议按照最小权限原则仅选择必要的命名空间，并优先使用只读权限。
     - **命名空间**：支持选择多个命名空间。
     - **权限类型**：支持配置只读、读写，只读模式下不支持镜像推送。

4. 创建完成后请立即保存用户名及密码，该页面仅展示一次，页面关闭后将无法找回。



管理服务级账号

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**访问凭证**，并选择服务级**账号**。
2. 在服务级**账号**页面中选择地域及实例名称，并管理已有服务级账号，支持以下操作：
   - 查看已有服务级账号。
   - 查看指定服务级账号的权限范围。
   - 编辑指定服务级账号的配置，除名称不可调整外，其他配置均可修改。
   - 禁用指定服务级账号，禁用后可再启用。账号禁用时，将无法用于镜像推送、拉取，请谨慎操作。
   - 删除指定服务级账号，删除后不可恢复。账号删除后，将无法用于镜像推送、拉取，请谨慎操作。

容器镜像服务
实例管理
资源中心
镜像仓库
Helm Chart
命名空间
运维中心
触发器
镜像加速
同步复制
版本管理
域名管理
访问凭证
用户级账号
服务级账号
服务级账号
地域
广州 2
实例
training
容器镜像服务文档
服务级账号可使用自定义名称及密码，并支持指定权限生效范围及类型，可用于多租户管理，或配置在 CI/CD 系统中执行自动化操作。服务级账号生成并实际应用时，平台无法验证审计实际使用者身份，请谨慎对外分发使用服务级账号。如需严格追踪审计镜像拉取推送行为，请选择用户级账号。
新建
名称或命名空间
名称
描述
状态
账号权限
创建时间
过期时间
操作
tcr$robot-demo
演示机器人账号
已启用
已配置2个命名空间
2023-03-21 18:48:24
2023-04-20 18:48:23
禁用 编辑 删除

访问网络控制
访问网络控制概述

最近更新时间：2023-04-07 10:13:18

腾讯云容器镜像服务（Tencent Container Registry，TCR）为企业版实例提供了访问网络控制能力，为保障您的镜像仓库及 Helm Chart 内数据安全，新创建的企业版实例默认不开启公网及私有网络访问入口，即拒绝全部外部访问。
您可根据业务的具体需要，分别配置公网及内网访问控制策略，以最小范围放通业务客户端访问实例，推送或拉取镜像。详情请参见：

- 公网访问控制
- 内网访问控制

配置公网访问控制

最近更新时间：2023-10-20 16:21:21

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持公网访问控制，可基于白名单策略限制来自公网环境的客户端对实例的访问，保障实例内的数据隐私安全。新创建的 TCR 企业版实例默认不开启公网访问入口，即无法使用处在公网环境内的开发测试服务器直接进行镜像的推送，拉取操作。本文档介绍如何在 TCR 企业版实例中配置公网访问控制。

前提条件

在配置 TCR 企业版实例的公网访问控制前，您需要成功 购买企业版实例 。

操作步骤

开启公网访问入口

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 > 公网访问**。
2. 在**公网访问**页面，如果需要切换实例，请在页面上方选择实例所在地域，并在**实例**下拉列表中进行选择。
3. 选择**开启公网访问入口**即可开始开启入口。
   待该按钮变为**关闭公网访问入口**，且**添加公网白名单**为可选择状态，则说明入口已开启。如下图所示：
   入口开启后，仍默认拒绝全部来源的公网访问。

配置访问策略

1. 在**公网访问**页面，单击**添加公网白名单**并在弹出窗口中配置公网 IP 地址段及备注信息。如下图所示：

- **所属实例**：配置公网访问策略的目标实例，可在“公网访问”页面顶部的“实例名称”下拉框中修改。
- **规则来源**：支持选择手动配置公网 IP 地址或从已有安全组内导入公网 IP 列表。
  - **手动配置公网地址**：放通的公网 IP 地址段。支持单个 IPV4 地址或 CIDR，例如 `192.168.0.0/24`，不建议直接输入 `0.0.0.0/0` 以放开全部公网访问。
  - **导入已有安全组内来源地址**：安全组规则 – 入站规则内所有来源将被去重后导入至白名单地址，支持重复导入安全组，导入后可手动管理实例的公网白名单。请注意，再次修改安全组配置，不会自动同步，需要重新导入。
- **备注**：访问策略的备注信息，可选，支持输入中文。

2. 配置完成后单击**确定**，该公网访问白名单策略即被添加并生效。

若公网访问入口无法开启或白名单策略无法新建，您可 在线咨询 联系我们。

配置内网访问控制

最近更新时间：2023-10-20 16:30:51

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持内网访问控制，可基于内网访问链路限制私有网络内的客户端访问实例。在容器计算的实际生产场景中，通过内网拉取容器镜像可有效提升拉取速度，并避免公网带宽成本。TCR 支持将用户的私有网络接入至企业版实例中，以实现内网访问及网络访问控制。
本文档介绍如何在 TCR 企业版实例中配置内网访问控制。完成以下配置后，您可使用在指定私有网络 VPC 内的云服务器通过内网拉取指定 TCR 实例内镜像。或在 TKE 等容器集群中实现集群内网拉取容器镜像，详情请参见 TKE 集群使用 TCR 插件内网免密拉取容器镜像 。

前提条件

在配置 TCR 企业版实例的内网访问控制前，您需要完成以下准备工作：

- 已成功 购买企业版实例 。
- 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。
- 已开通 私有网络 VPC 服务，并在企业版实例所在地域具有可用的私有网络及子网。
- 已开通 私有域解析 PrivateDNS 服务。

操作步骤

新建访问链路

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**内网访问**页面中，单击**接入私有网络**。
3. 在弹出的**新建内网访问链路**窗口中，配置私有网络及子网信息。如下图所示：

   - **所属实例**：开启内网访问策略的目标实例，可在**内网访问**页面顶部的**实例**下拉框中修改。
   - **地域**：当前需要接入的私有网络所在的地域，默认与所属实例地域相同。如果当前实例已开启多地域复制特性，且在多个地域内配置了复制实例，此处可新选择复制实例所在地域，接入复制地域的私有网络。详情可参见 配置实例复制 。
   - **私有网络**：
     - 可接入的私有网络。在下拉列表中选择当前实例所在地域可用的私有网络。
     - 私有网络内任一子网。请选择该私有网络下内网 IP 仍有空余的子网。新建私有网络访问链路将占用该子网内的一个内网 IP 地址，并作为实例域名的内网解析目标地址。该子网仅用于分配内网访问地址，链路创建完成后，该私有网络下任意子网内云服务器均可通过该链路访问 TCR 企业版实例。
4. 配置完成并单击**确定**，该内网访问链路将启动新建。
   等待**访问链路状态**转变为**链路正常**时，且**内网解析IP**不为空时，则说明该内网访问链路已创建成功。

> **注意**
> 实例访问域名仅默认配置了公网解析，接入指定私有网络后，并获得内网解析IP后，请单击**管理自动解析**，配置实例域名在该私有网络内的专用内网解析。

管理内网解析

内网访问链路建立完成后，关联的私有网络 VPC 内云服务器访问该内网解析 IP ，即可通过内网访问该实例。默认情况下，实例默认域名（如 tcr-demo.tencentcloudcr.com ）及内网域名（如 tcr-demo-vpc.tencentcloudcr.com ）在该私有网络内不会自动解析至该内网解析 IP，需使用**管理自动解析**功能配置内网解析，或使用自建 DNS 服务自行管理。

使用私有域解析 PrivateDNS 自动配置（默认方式）

本产品默认使用腾讯云 私有域解析 PrivateDNS 服务配置私有网络内的域名解析，使用此功能需首先开通该服务。

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**内网访问**页面中，单击已创建成功的内网访问链路右侧的**管理自动解析**。
3. 在弹出的**管理自动解析**窗口中，配置该链路的域名解析。如下图所示：

- **解析服务**：当前 PrivateDNS 服务的开通状态。如尚未开通服务，请单击**开通服务**跳转至 PrivateDNS 开通服务。使用此功能不会在 PrivateDNS 产品侧产生额外费用。
- **解析配置**：默认不开启。单击可开启默认域名的自动解析。开启后，本实例域名在私有网络内将解析至内网 IP x.x.x.x ，不再默认解析至实例公网访问地址，用于内网推送，拉取镜像，无需手动或使用 TCR 插件配置此域名解析。
- **高级配置**：可配置自动解析 VPC 域名。VPC 域名是面向私有网络的专用域名，您可在私有网络内使用该专用域名，用于和公网环境内使用的默认域名进行区分。请注意，镜像仓库默认提供的是默认域名的访问地址及相关操作指引，如您选择使用 VPC 专用域名，请注意同时调整镜像仓库访问地址的相关配置。

4. 配置完成并单击**确认**。

使用 TCR 插件自动配置

此方案适用于 PrivateDNS 在容器服务 TKE 集群所在地域尚未提供服务时选用，默认不推荐使用。
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。

手动配置云服务器 Host

此方案适用于需要临时访问企业版实例的云服务器或在私有网络自建 Kubernetes 集群的节点。默认不推荐使用。
以 Linux 云服务器为例，登录至云服务器，并执行以下命令：

```
echo '172.16.1.95 techo-demo.tencentcloudcr.com' >> /etc/hosts
```

`172.21.17.69` 及 `demo.tencentcloudcr.com` 请替换为您实际使用的内网解析 IP 及 TCR 实例域名。

访问权限配置
访问权限管理概述

最近更新时间：2023-10-12 17:24:11

腾讯云容器镜像服务（Tencent Container Registry，TCR）为企业版实例提供了两种访问权限管理模式，支持实例管理者为使用实例的研发运维人员，及内部 CI/CD 等自动化系统分配独立的访问凭证，并精细化管理用户权限，保障实例的数据安全。

使用场景

人员权限管控

企业购买企业版实例后，一般会有多个业务团队同时使用该实例，并涉及到研发、运维、测试等多种角色，出于数据安全需要，不同团队和角色应在满足正常业务需求的前提下，配置最小权限，避免出现镜像误删、镜像泄漏等数据安全问题。
具体而言，需要对指定人员分配独立账号用于身份认证，并配置独立权限用于操作鉴权。在镜像仓库的使用场景下，即需要给指定人员分配登录镜像仓库（docker login）的访问凭证（username + password），并配置该账户权限，如仅能向镜像仓库 A 内推送拉取镜像，或仅能拉取镜像仓库 B 内镜像。同时，企业也需要人员对镜像仓库的操作进行审计，针对异常操作进行回溯定位。

系统权限管控

容器镜像的生产和部署也涉及到自动化系统，如 CI/CD 流水线。在自动化场景下，使用指定人员的账号将可能造成严重后果，如在发布系统中配置了某位运维人员的访问凭证用于集群拉取镜像，当该运维人员账号被误删、或是员工转岗、离职后，该镜像访问凭证将失效，导致发布异常。因此，在自动化场景中，应使用与指定人员无关的访问凭证，并可独立管理账号权限。

产品功能

针对上述两个典型场景，产品提供两种访问权限管理功能：用户级账号、服务级账号，您可组合使用，满足企业内权限管理需求。

用户级账号

用户级账号与腾讯云账号直接关联，并基于访问管理 CAM 管理账号权限。如需为企业内指定人员授予权限，需要在腾讯云主账号下新建一个该人员专用的子账号，并为账号在访问管理 CAM 中关联权限策略，具体请参见 基于 CAM 管理子账号权限 。
该用户使用子账号登录产品控制台，并前往**访问凭证-用户级账号**功能页，新建专属的访问凭证。该访问凭证与子账号关联，仅子账号可见可管理。用户可使用这个访问凭证登录镜像仓库，并推送、拉取镜像，实际操作受到关联的权限策略管控。

> **说明**
> 请注意，当子账号被禁用或删除时，关联的访问凭证也将失效，因此避免将子账号关联的访问凭证配置在自动化系统中。

关于用户级账号具体使用，请参见 用户级账号 。

服务级账号

服务级账号与腾讯云账号不直接关联，属于实例内资源，权限管理独立于访问管理 CAM。如需为自动化系统，如 CI/CD 流水线，Kubernetes 集群配置自动推送、拉取镜像的访问凭证，可在实例内新建服务级账号，并配置该访问凭证可访问的命名空间。

> **说明**
> 因服务级账号属于实例内资源，因此所有具有服务级账号功能相关 API 权限的子账号，均可查询管理服务级账号。同时，因为该账号权限独立于访问管理 CAM 权限体系，因此会出现越权风险，请严格控制相关 API 的授权范围。

关于服务级账号具体使用，请参见 服务级账号 。

版权所有：腾讯云计算（北京）有限责任公司

基于 CAM 管理子账号权限

最近更新时间：2024-01-04 09:53:01

本文将介绍如何通过访问管理 CAM 策略使子账户可以查看和使用容器镜像服务 TCR 企业版相关资源，包括具体的操作步骤以及常用的策略配置示例。

> **注意**
> 如您在容器镜像服务控制台中使用部分功能时需要外部权限，例如私有网络、操作审计、云标签等，请参见 支持 CAM 的产品 中对应产品的访问管理指南文档。

访问管理（CAM）简介

访问管理（Cloud Access Management，CAM）是腾讯云提供的一套 Web 服务，它主要用于帮助用户安全管理腾讯云账户下的资源的访问权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。
当您使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。更多关于 CAM 策略的基本信息，请参见 策略语法 。更多关于 CAM 策略的使用信息，请参见 策略 。
若您不需要对子账户进行 TCR 相关资源的访问管理，您可以跳过此章节，不会影响您对文档中其余部分的理解和使用。

TCR 基于 CAM 的资源级访问控制

资源级权限指的是能够指定允许用户对哪些资源具有执行操作的能力。容器镜像服务（TCR）支持基于 CAM 的资源级访问控制，控制颗粒度可至仓库级，即用户可通过配置 CAM 策略实现授权子账号仅能够操作指定镜像仓库或 Helm Chart 仓库资源。
TCR 在 CAM 中可授权的资源类型：

资源类型	授权策略中的资源描述方法
企业版实例相关	qcs::tcr:$region:$account:instance/*
企业版仓库相关	qcs::tcr:$region:$account:repository/*
个人版仓库相关	qcs::tcr:$region:$account:repo/*

- $region：描述地域信息，例如 ap-guangzhou 代表广州地域，若值为空则表示所有地域。具体地域列表及缩写请参见 地域和可用区 。
- $account：描述资源拥有者的主账号信息，表示为 uin/${uin}，例如 uin/12345678，若值为空则表示创建策略的 CAM 用户所属的主账号。
  关于授权策略中的资源描述方式，详情请参见 资源描述方式 。

操作步骤

本文以“授权子账号只读某个镜像仓库”为例，介绍如何完成创建策略操作。

- **实例 ID**：tcr-xxxxxxxx
- **命名空间**：team-01
- **镜像仓库**：repo-demo

通过策略生成器创建（推荐）

1. 登录 访问管理控制台 。
2. 左侧导航栏中，单击**策略**，进入策略管理页面。
3. 单击左上角的**新建自定义策略**。
4. 在弹出的选择创建方式窗口中，单击**按策略生成器创建**，进入编辑策略页面。
5. 在“可视化策略生成器”中选择服务的页面，补充以下信息，并编辑授权声明。
   - **效果（Effect）**：选择允许或拒绝，这里我们选择**允许**。
   - **服务（Service）**：选择要授权的产品，这里我们选择**容器镜像服务 (tcr)**。
   - **操作（Action）**：选择需要授权的操作，这里我们选择**读操作**。
   - **资源（Resource）**：选择全部资源或您要授权的特定资源，这里我们选择**特定资源**，并添加以下资源六段式来限制访问。
     - **repository**：选择仓库所属地域，并填写该仓库的资源路径，例如 tcr-xxxxxxxx/team-01/repo-demo/* 。您可在 镜像仓库 中获取资源路径。

- **repo**：此处置空。
- **instance**：选择仓库所属地域，并填写该仓库所属实例的实例 ID，例如 `tcr-xxxxxxxx` 。您可在 实例列表 中获取实例 ID。

- **条件**：此处置空。

6. 单击**下一步**，进入关联用户/用户组页面。
7. 在关联用户/用户组页面，补充策略名称和描述信息，可同时关联用户、用户组或角色快速授权。
8. 单击**完成**，完成按策略生成器创建自定义策略的操作。

通过策略语法创建

1. 登录 访问管理控制台 。
2. 左侧导航栏中，单击**策略**，进入策略管理页面。
3. 单击左上角的**新建自定义策略**。
4. 在弹出的选择创建方式窗口中，单击**按策略语法创建**，进入**选择策略模板**页面。
5. 在选择模板类型中，选择**空白模板**。
6. 单击**下一步**，进入**编辑策略**页面。
7. 在**编辑策略**页面，补充策略名称和描述信息，添加以下策略内容。

```
{
  "version": "2.0",
  "statement": [{
        "action": [
          "tcr:DescribeRepositories",
          "tcr:PullRepository",
          "tcr:DescribeNamespaces"
        ],
        "resource": [
          "qcs::tcr:::repository/tcr-xxxxxxxx/team-01/repo-demo/*"
        ],
        "effect": "allow"
      },
      {
        "action": [
          "tcr:DescribeInstance*"
        ],
        "resource": [
          "qcs::tcr:::instance/tcr-xxxxxxxx"
        ],
        "effect": "allow"
      }
  ]
}
```

8. 单击**完成**，完成按策略语法创建自定义策略的操作。

常用策略配置

若需要自定义编辑策略 JSON，请参见 企业版接入 CAM 的 API 列表 以及 策略语法 。

预设策略配置

- **QcloudTCRFullAccess**：容器镜像服务（TCR）全读写权限。
  子账号绑定该策略后，将具有 TCR 全部资源的全部操作权限，包含企业版及个人版。

```
{
  "version": "2.0",
  "statement": [{
```

```
      "action": [
        "tcr:*"
      ],
      "resource": "*",
      "effect": "allow"
    }]
}
```

- **QcloudTCRReadOnlyAccess**：TCR 只读权限。
  子账号绑定该策略后，将具有容器镜像服务全部资源的只读权限，包含企业版及个人版。

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "tcr:Describe*",
      "tcr:PullRepository*"
    ],
    "resource": "*",
    "effect": "allow"
  }]
}
```

典型场景策略配置

> **注意**
> 以下场景策略均只面向企业版使用场景。个人版场景策略请参见 个人版授权方案示例 。

- 授予子账号 TCR 企业版内全部资源的全读写操作权限。

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "tcr:*"
    ],
    "resource": [
      "qcs::tcr:::instance/*",
      "qcs::tcr:::repository/*"
    ],
    "effect": "allow"
  }]
}
```

- 授予子账号 TCR 企业版内全部资源的只读操作权限。

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "tcr:Describe*",
      "tcr:PullRepository*"
    ],
    "resource": [
      "qcs::tcr:::instance/*",
      "qcs::tcr:::repository/*"
    ],
    "effect": "allow"
  }]
}
```

- 授权子账号管理指定实例。例如 dev-guangzhou，其实例 ID 为 tcr-xxxxxxxx。

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "tcr:*"
    ],
    "resource": [
      "qcs::tcr:::instance/tcr-xxxxxxxx",
      "qcs::tcr:::repository/tcr-xxxxxxxx/*"
    ],
    "effect": "allow"
  }]
}
```

- 授权子账号管理指定实例内的指定命名空间。例如实例 tcr-xxxxxxxx 下 team-01。

```
{
  "version": "2.0",
  "statement": [{
      "action": [
        "tcr:*"
      ],
      "resource": [
        "qcs::tcr:::repository/tcr-xxxxxxxx/team-01",
        "qcs::tcr:::repository/tcr-xxxxxxxx/team-01/*"
      ],
      "effect": "allow"
    },
    {
      "action": [
        "tcr:DescribeInstance*"
      ],
      "resource": [
        "qcs::tcr:::instance/tcr-xxxxxxxx"
      ],
      "effect": "allow"
    }
  ]
}
```

- 授权子账号只读某个镜像仓库，仅能拉取该仓库内镜像，无法删除仓库、修改仓库属性及推送镜像。例如实例 tcr-xxxxxxxx 下 team-01 命名空间内的 repo-demo。

```
{
  "version": "2.0",
  "statement": [{
      "action": [
        "tcr:Describe*",
        "tcr:PullRepository"
      ],
      "resource": [
        "qcs::tcr:::instance/tcr-xxxxxxxx",
        "qcs::tcr:::repository/tcr-xxxxxxxx/team-01",
        "qcs::tcr:::repository/tcr-xxxxxxxx/team-01/repo-demo",
        "qcs::tcr:::repository/tcr-xxxxxxxx/team-01/repo-demo/*"
      ],
      "effect": "allow"
    }
  ]
```

```
}
```

访问域名配置

配置自定义域名

最近更新时间：2023-10-20 16:40:42

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持配置使用自定义域名，方便用户使用公司统一规划的域名访问服务，或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，保持服务的连续性。
在 TCR 企业版实例中，所有规格的实例均支持配置多个自定义域名，且不影响实例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 协议访问实例。本文介绍如何通过自定义域名访问容器镜像服务企业版实例。

基本概念

域名

域名，即网域名称（Domain Name），由一串用点分隔的字符组成。域名在容器镜像服务企业版中用于访问实例服务，且直接影响镜像仓库的访问地址。

SSL 证书

SSL 证书 用于遵守 HTTPS 协议，使得容器镜像服务企业版实例可通过 HTTPS 协议进行传输加密和身份认证，保证了传输过程的安全性。

腾讯云 DNSPod 服务

腾讯云 DNSPod 服务可以将自定义域名的访问路由至容器镜像服务企业版实例的相应 IP 地址。

前提条件

在配置使用自定义域名前，您需要完成以下准备工作：

- 已拥有域名。您可通过腾讯云 域名注册服务 注册域名，详情请参见 域名注册 。

> **注意**
> - 如果您希望在公网环境内使用自定义域名，则您的域名需要 备案 。
> - 如果您的容器镜像服务企业版实例位于境外，则您的域名无需备案。

- 已为域名签发证书。您可通过腾讯云 SSL证书 服务购买证书，并确认已绑定实例需要使用的自定义域名。
- 已开通腾讯云 DNSPod 服务。详情请参见 DNS 解析 和 Private DNS 解析 。

操作步骤

创建自定义域名

1. 登录 容器镜像服务控制台，选择左侧导航栏中的**域名管理**。
2. 在**域名管理**页面选择需要添加自定义域名的实例地域和实例 ID。
3. 单击**添加自定义域名**。在**添加域名**弹窗中，参考以下提示配置域名及证书信息。如下图所示：

- **域名：** 所需要使用自定义域名，建议使用常见域名后缀。
- **证书：** 已绑定自定义域名的证书，仅支持选择已在腾讯云 SSL 证书服务内托管的证书。

> **说明**
> 如果您的自定义域名已经在工信部 备案 且在 云解析 DNS 控制台 添加解析，请直接在“域名”输入框填写您的自定义域名，并选择证书。

4. 单击**确定**即可添加自定义域名。
   成功添加自定义域名后即可在**域名管理**页面查看，此时您可参考以下步骤对自定义域名进行管理。如下图所示：

设置访问控制和域名解析

您可以在公网或私有网络 VPC 内使用自定义域名服务，建议优先使用私有网络访问实例。

内网访问

配置内网访问控制

请参考 内网访问控制，配置私有网络 VPC 接入实例内，并确认已正常生成内网访问 IP。

配置私有域解析

请前往 PrivateDNS 控制台，使用已添加的自定义域名 创建私有域，并关联已接入的 VPC，并配置该私有域内解析。
1. 使用 CNAME，且记录值为实例的标准访问域名。请注意，需要在 TCR 内配置接入 VPC 时，开启自动解析。
2. 使用 A 记录，且记录值为已创建内网访问链路的内网访问 IP。请注意，后续如重新接入 VPC，内网访问 IP 可能变化。

详情请参见 私有域解析 Private DNS 。

公网访问

配置公网访问控制

请参考 公网访问控制，开通公网访问入口，并放通公网访问地址。

配置公网解析

请前往 DNS 解析 DNSPod 控制台，配置已添加自定义域名的云解析，记录类型请选择 “CNAME”，记录值请填写实例的默认域名。详情请参见 快速添加域名解析 。

更新域名证书

如因证书过期或升级证书等原因需要更新自定义域名所绑定的证书，您可在“域名管理”页面单击自定义域名所在行右侧的**更新证书**重新选择 SSL 证书。更新证书操作需要重新下发 SSL 证书，此期间自定义域名仍可正常访问。

删除自定义域名

在“域名管理”页面选择指定自定义域名所在行右侧的**删除**即可删除该自定义域名。删除自定义域名可能造成容器集群内已有容器镜像拉取配置无法使用，进而影响应用更新，请谨慎操作。

镜像创建
管理命名空间

最近更新时间：2023-12-12 10:05:31

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版中命名空间用于管理多个具有关联属性的镜像仓库及 Helm Chart，不直接存储容器镜像及 Helm Chart，可映射为企业内部的组织团队、产品项目或个人。
在 TCR 企业版实例中，因企业独享该实例，所以在创建命名空间无需担心所需命名空间被其他客户占用，但个人版实例中仍需避免与已有的命名空间命名冲突。
本文档介绍如何在 TCR 企业版实例内创建并管理命名空间。

前提条件

在创建并管理 TCR 企业版实例的命名空间前，您需要完成以下准备工作：

- 已成功 购买企业版实例 。
- 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。

操作步骤

创建命名空间

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**命名空间**。
2. 在**命名空间**页面即可查看当前实例内的命名空间列表。如果需要切换实例，请在页面上方的**实例**下拉列表中进行选择。
3. 单击**新建**，在**新建命名空间**窗口中，参考以下提示配置命名空间名称及访问级别。如下图所示：

   - **所属实例：**当前所选实例，新建的命名空间将属于该实例。
   - **名称：**命名空间名称，长度2 - 30个字符，只能包含小写字母、数字及分隔符 ._- ，且不能以分隔符开头、结尾或连续。建议使用组织团队、产品项目等进行命名，或使用个人姓名用作个人测试空间。单个实例内命名空间名称不可重复。
   - **访问级别：**可选择**私有**或**公开**，默认设置为私有。
     若选择设置为公开，该命名空间内所有的镜像仓库及 Helm Chart 均成为公开仓库。若实例同时开启匿名访问（默认开启），则任何可通过访问控制的客户端均无需登录即可拉取镜像及 Chart，请谨慎设置，该属性在新建后仍可再次修改。
   - **标签：**可绑定云标签，标签用于在命名空间维度对资源进行分类管理。如现有标签不符合您的要求，请前往控制台 管理标签 。
4. 单击**确认**即可创建命名空间。
   成功创建后即可在**命名空间**页面查看，此时您可参考以下步骤对命名空间进行管理。如下图所示：

切换访问级别

1. 单击命名空间名称，进入该命名空间基本信息页面。
2. 在**基本信息**中，单击**访问级别**中的，即可在弹出窗口中切换命名空间的公开、私有属性。

> **注意**
> 切换后命名空间下所有的镜像仓库及 Helm Chart 均将立即继承该切换，**请谨慎将私有命名空间切换为公开命名空间**。

切换安全扫描方式

1. 单击命名空间名称，进入该命名空间基本信息页面。
2. 在**基本信息**中，单击**安全扫描**中的，即可切换该命名空间下容器镜像的安全扫描属性。可设置为**手动扫描**或**自动扫描**状态。

> **注意**
> 切换安全扫描状态不会影响已经存在的安全扫描结果。

- **手动扫描**：您需要前往**镜像仓库**页面，选择镜像，并在**版本管理**页签中单击**扫描**才可对指定容器镜像进行安全扫描并查看结果。
- **自动扫描**：当该命名空间下所有镜像仓库内有新的镜像被推送至仓库内时，均将触发自动的安全扫描。

配置部署安全

企业版实例支持阻断部署高危镜像，请参见 高危镜像部署阻断 。

删除命名空间

选择指定命名空间所在行右侧的**删除**即可删除该命名空间。为避免您误删重要数据，当前内部仍有镜像仓库及 Helm Chart 的命名空间无法删除。

管理镜像仓库

最近更新时间：2023-10-20 16:58:41

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版中镜像仓库用于直接管理容器镜像，单个镜像仓库可包含不同版本的容器镜像。镜像仓库归属于命名空间，并从命名空间继承了公开、私有属性及安全扫描触发方式。
镜像仓库是 TCR 中进行权限管理的最小单位，实例管理员可授予子用户镜像仓库的管理或只读权限。例如，授权子账户 tom 仅能拉取镜像仓库 project-a-frontend 中的镜像，但无法推送或删除镜像的权限。更多权限管理及授权方式请参考 企业版授权方案示例 。本文档介绍如何在 TCR 企业版实例内创建并管理镜像仓库。

前提条件

在创建并管理 TCR 企业版实例的镜像仓库前，您需要完成以下准备工作：

- 已成功 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操作权限。

操作步骤

创建镜像仓库

1. 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**下拉列表中进行选择。
2. 单击**新建**，在**新建镜像仓库**窗口中，参考以下提示进行镜像仓库配置。如下图所示：

   - **所属实例**：当前所选实例，新建的命名空间将属于该实例。
   - **命名空间**：镜像仓库所属的命名空间，如果列表为空，请先在该实例内 新建命名空间 。
   - **名称**：镜像仓库名称，长度为2 - 200个字符，只能包含小写字母、数字及分隔符（ `.` 、 `_` 、 `-` 、 `/` ），且不能以分隔符开头、结尾或连续。名称支持多级路径，例如 `team-01/front/nginx` ，可根据业务需要灵活设置。
   - **简短描述**：简短描述镜像仓库信息。支持中文输入，最长为100个字符，可在创建后重新编辑。
   - **详细描述**：详细描述镜像仓库信息。支持 Markdown，最长为1000个字符，可在创建后继续编辑。
3. 单击**确认**即可创建镜像仓库。

镜像仓库相关操作

成功创建后即可在**镜像仓库**页面查看，此时您可执行以下操作对镜像仓库进行管理。如下图所示：

- **筛选命名空间**

  在“镜像仓库”列表中选择 命名空间 进行筛选，即可在下拉列表中选择仅需要查看的命名空间。

- **查看仓库详情**

  单击指定镜像仓库的名称即可进入该仓库的详情页面，可在详情页中管理镜像版本，编辑镜像仓库的基本信息。

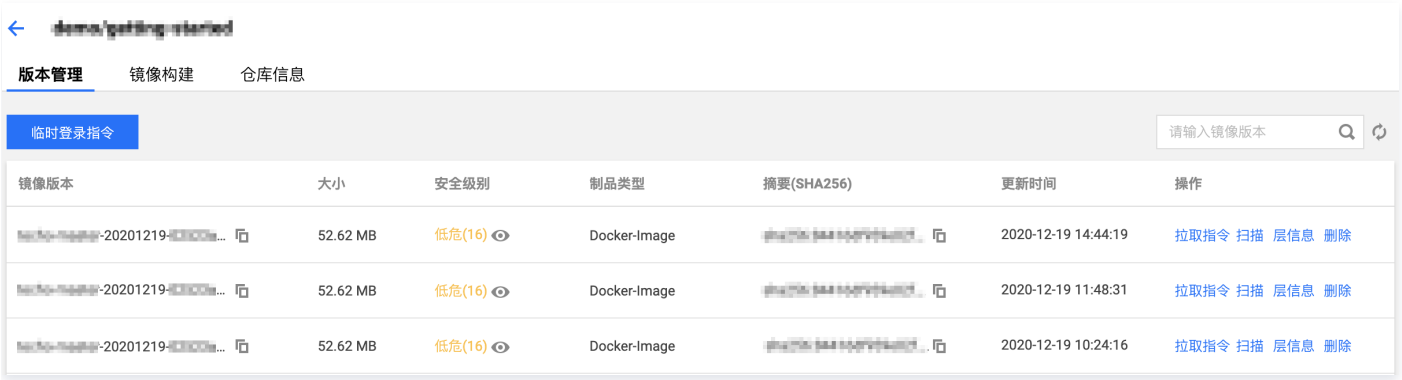
- **删除镜像仓库**

  单击指定镜像仓库所在行右侧的**删除**即可删除该镜像仓库。为避免您误删重要数据，删除镜像仓库时需要二次确认。

> **注意**
> 镜像仓库被删除后，**镜像仓库内的所有容器镜像均被直接删除**。

管理镜像版本

单击指定镜像仓库名称，即可进入该仓库的详情页面，默认选择**版本管理**页签。您可在此页面管理仓库内的镜像版本，并执行安全扫描，查看层信息等操作。如下图所示：



- **筛选镜像版本**

  在版本列表右上方搜索框中输入指定的镜像版本即可镜像搜索，支持模糊搜索。

- **获取拉取指令**

  选择指定镜像版本所在行右侧的**拉取指令**即可复制该镜像版本的拉取指令。

- **执行安全扫描**

  选择指定镜像版本所在行右侧的**扫描**即可主动触发安全扫描，待对应的“安全级别”属性出现扫描结果时，即可单击 查看结果详情。

- **查看镜像层信息**

  选择指定镜像仓库的所在行右侧的**层信息**即可在弹窗中查看该镜像的层信息。

- **删除镜像版本**

  选择指定镜像仓库的所在行右侧的**删除**即可删除该镜像版本。为避免您误删重要数据，删除镜像版本时需要二次确认。

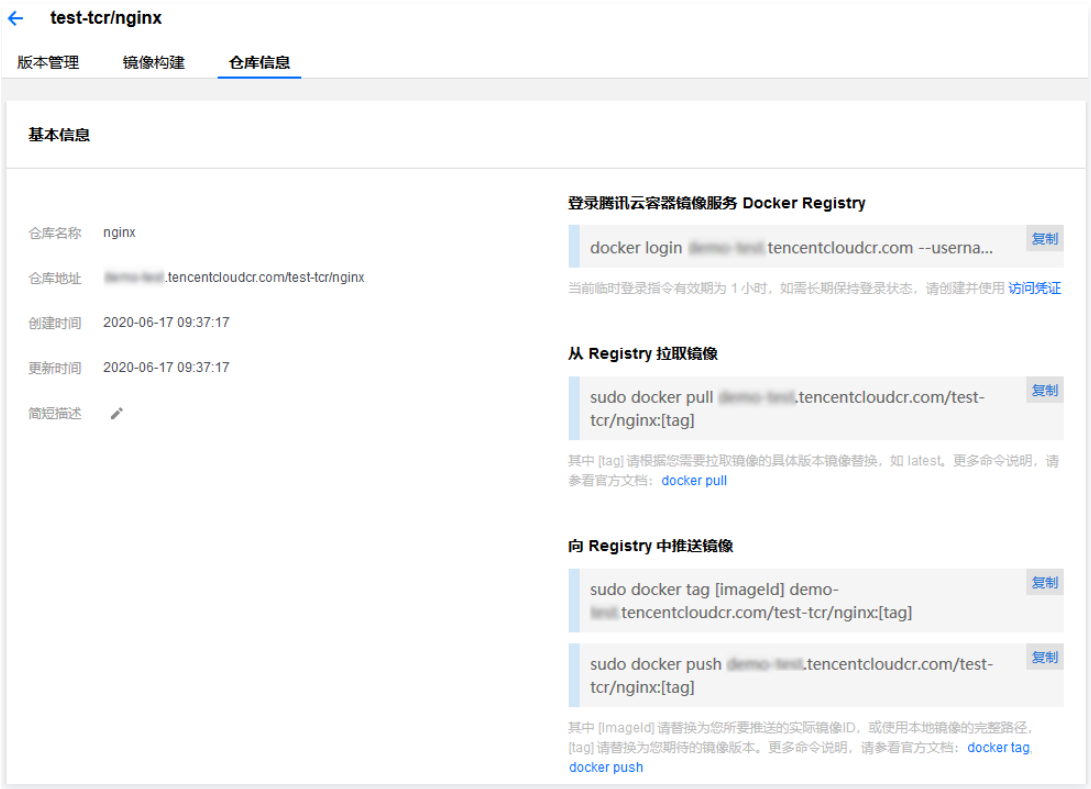
> **注意**
> 删除指定镜像版本可能会同时删除与其镜像 ID 相同的其它镜像版本，造成其它镜像版本不可用。

镜像构建

支持使用托管在 GitHub、GitLab.com、私有 Gitlab、Gitee 码云、腾讯工蜂 及 CODING 上的源代码进行编译构建，详情请参见 配置镜像构建 。

编辑仓库信息

在镜像仓库的详情页面选择**仓库信息**页签，即可查看并编辑仓库的基本信息。如下图所示：



- **编辑简短描述**

  选择“简短描述”后的 ，即可进入编辑状态，完成修改后单击**保存**即可完成编辑。

- **编辑详细描述**

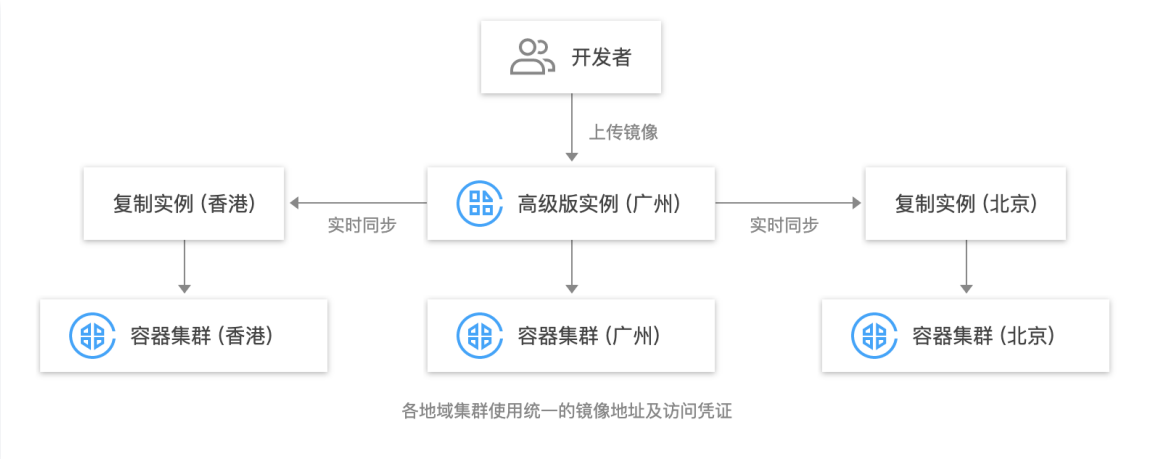
  选择“详细描述”后的 ，即可进入编辑状态，完成修改后单击**保存**即可完成编辑。详细描述支持 Markdown 语法，保存后可查看渲染后的文本效果。

镜像分发
同实例多地域复制镜像

最近更新时间：2024-03-29 15:41:31

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持高级版实例多地域复制镜像，使用统一的域名及访问凭证，可实现单地域上传、多地域高速实时同步、就近内网拉取。相对于跨实例同步功能，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，助力客户实现全球业务应用同步更新。
实例复制功能允许用户为高级版实例在多个地域内配置复制实例，复制实例将实时与该主实例进行数据同步，并可使用该主实例的访问域名及访问凭证进行内网访问。通过使用实例复制功能，可对多地域业务所使用的应用镜像进行统一管理，无需购买使用多个企业版实例，降低使用成本，即可提高容器镜像镜像分发速度，简化部署配置。



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，且实例规格为高级版。
- 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。

使用限制

- 从实例仅可拉取镜像，不可推送镜像，如需在多个地域同时推送、拉取镜像，请使用 跨实例（账号）同步镜像 功能，在多个地域内使用独立实例，并配置同步规则。
- 由于腾讯云国内外控制台有独立的账号体系，如果您要实现国内外之间的镜像传输，请使用 跨实例（账号）同步镜像 功能。

操作步骤

创建并管理复制实例

1. 登录 容器镜像服务控制台，选择左侧导航栏中的**同步复制** > **实例复制**。
2. 在**实例复制**页面中选择地域及实例名称，并单击**新建**。
3. 在弹出的**新建从实例**窗口中进行如下设置。

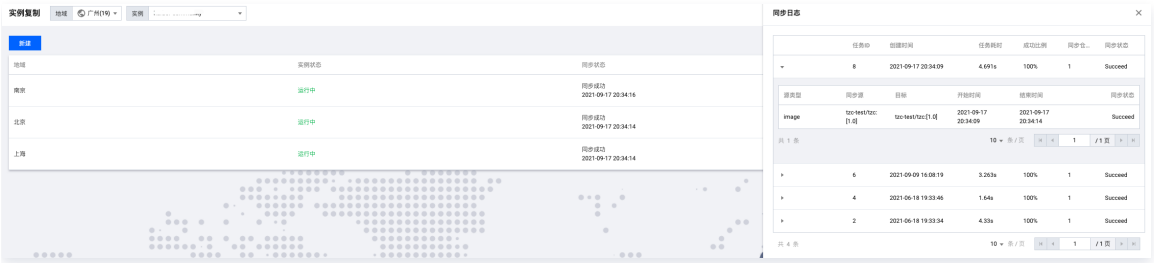
- **主实例名**：当前所选的高级版实例名称。
- **默认地域**：当前所选的高级版实例所在地域。
- **复制地域**：复制实例所在的地域，不可选择与当前主实例相同的地域。

4. 单击**确认**即可创建复制实例。

> **注意：**
> 如果不再需要指定地域的复制实例，可删除该复制实例。若高级版实例内已配置复制实例，您需要先删除所有复制实例以删除该高级版实例。

查看镜像复制日志

配置复制实例后，向主实例内推送镜像，将自动复制镜像数据至复制实例内。为确认镜像同步状态，可选择指定的复制实例，查看复制日志。



通过内网访问复制实例

1. 为能够使复制地域内的容器集群或云服务器可通过内网访问该实例，您需要将复制地域内的私有网络 VPC 依次接入该实例。请参见 内网访问控制 ，并选择复制地域内的私有网络。
2. 完成以上配置后，复制地域内的容器集群或云服务器即可通过内网访问该实例，镜像访问地址及访问凭证和在初始地域访问该高级版实例一致。

相关文档

您还可以使用 CreateReplicationInstance 接口创建从实例。详细信息请参见 创建从实例 API 文档 。

跨实例（账号）同步镜像

最近更新时间：2024-03-06 17:05:51

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持在不同地域的不同实例间同步容器镜像及 Helm Chart，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。
实例同步功能允许用户自定义创建同步规则，可指定某个实例内的部分资源同步至另一个实例内的指定位置。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）、可过滤同步资源路径，通过正则表达式过滤仓库及版本、可选择是否覆盖已有的同名镜像，避免历史数据覆盖丢失。目前实例同步功能已支持跨主账号间的实例同步，同步源侧的用户可以根据同步目标侧用户提供的实例 ID、账号 ID 和访问凭证来创建同步规则。

前提条件

在创建并管理 TCR 企业版实例的同步配置前，您需要完成以下准备工作：

- 已成功 购买企业版实例，且实例规格为标准版或高级版。
- 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操作权限。

使用限制

数据同步功能依赖于底层网络支持，受限于安全合规要求，因此，暂不支持中国台湾地域。

操作步骤

创建同步规则

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**同步复制** > **实例同步**。
2. 在**实例同步**页面中选择地域及实例名称，并单击**新建**。
3. 在**新建实例同步规则**中，参考以下提示进行规则配置。如下图所示：

- **名称**：实例规则名称，支持小写字母、数字及（-._）三种符号，且需以字母或数字开头。
- **描述**：规则描述，支持中文。
- **同步源**：
  - **源实例**：当前所选实例即为源实例，可返回**实例同步**页面修改。
  - **命名空间**：当前实例所需要同步的命名空间，暂不支持选择全部命名空间。
  - **仓库名称**：同步的仓库，不填写则默认是命名空间内全部仓库。
  - **版本Tag**：同步的版本，不填写则默认是符合条件的仓库内所有版本。
  - **仓库类型**：同步资源的类型，可同时同步容器镜像及 Helm Chart，或只同步其中一种资源。
- **同步目标**：选择是否开启跨主账号实例同步。

关闭

开关关闭，则创建同一主账号内的实例同步规则，配置以下字段。如下图所示：

- **目标实例**：数据同步的目标实例，可选择该主账号内的任一实例。
- **命名空间**：仓库同步至目标实例后所在的命名空间，不填写则默认是与源实例中同名的命名空间，如果没有命名空间将新建。

开启

开关打开，则创建跨主账号的实例同步规则，根据目标账号提供的信息配置以下字段，如下图所示：

- **目标实例**：数据同步的目标实例 ID，前往 实例管理 即可获得。
- **命名空间**：仓库同步至目标实例后所在的命名空间，不填写则默认是与源实例中同名的命名空间，如果没有命名空间将新建。
- **用户名**：登录同步目标实例的用户名。

> **注意：**
> 用户名只能填写 用户级账号，暂时不支持 服务级账号 。若输入服务级账号，则无效且会报错。

- **密码**：登录同步目标实例的密码。

> **注意**
> 请使用长期访问凭证，避免同步规则出现不可用的情况。同步规则的生命周期与该目标账号下最新添加的同步规则的访问凭证的生命周期保持一致。

- **镜像覆盖**：可选择是否覆盖目标实例内已有同名的容器镜像，建议不覆盖。

4. 单击**确定**即可创建同步规则。

管理同步规则

成功创建后即可在**实例同步**页面查看已创建的同步规则，您可执行以下操作管理同步规则。如下图所示：

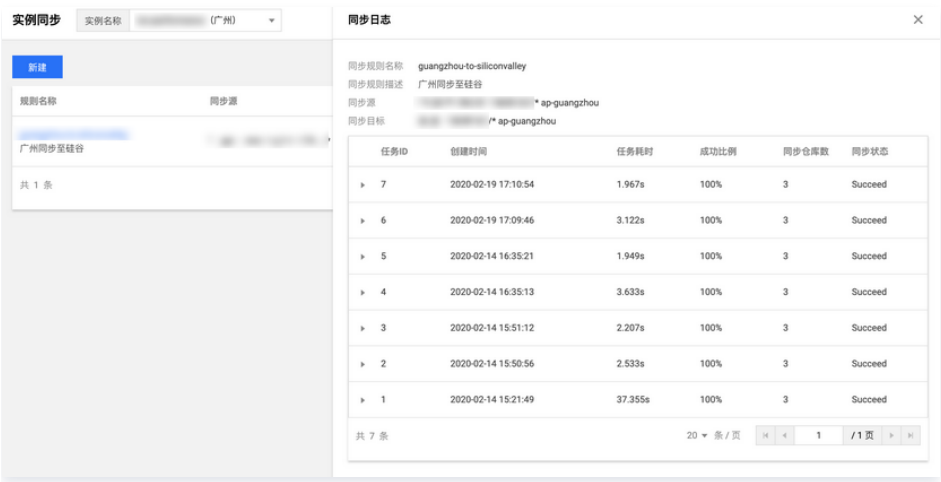
- **查看同步日志**：单击实例规则名称，即可查看该规则触发日志，详情请参见 查看同步日志 。
- **修改规则状态**：表示规则启用，表示规则关闭。新建的实例同步规则默认为启用状态，您可自行调整。
- **触发同步**：手动触发同步，将扫描实例内所有符合规则的仓库并进行同步。

> **注意：**
> 规则创建好之后，针对新推送的镜像，都会自动同步到其他实例，无需您手动触发。
> 手动触发主要针对一些历史镜像和异常情况。手动触发同步的操作会扫描实例内所有符合规则的仓库，需要一定的耗时，根据您镜像 tag 数决定。在同步的过程中，因为同步任务的执行，可能对其他镜像传输动作造成压力。请尽量避免同时手动触发多个同步规则。

- **配置**：重新配置实例同步规则，可配置全部参数。
- **删除**：删除该实例同步规则。

查看同步日志

单击指定实例同步规则名称，即可查看该规则的触发日志。如下图所示：



- **任务ID**：实例内唯一的同步任务 ID。
- **创建时间**：同步任务创建的时间。
- **任务耗时**：完成全部同步任务消耗的时间。
- **成功比例**：资源同步完成比例，单次同步任务可能同时同步多个仓库。
- **同步仓库数**：当前任务需要同步的仓库数量。
- **同步状态**：任务完成状态。如果单次同步任务所需同步的容器镜像及 Helm Chart 较多，可能同步状态会较长时间保持在 “InProgress”（同步中）状态。

相关文档

您还可以使用 ManageReplication 接口管理实例同步。详细信息请参见 管理实例同步 API 文档 。

按需加载容器镜像

最近更新时间：2024-03-25 10:36:00

操作场景

在使用容器镜像部署更新业务应用时，传统方案将下载全量的容器镜像数据并解压，一方面导致容器启动耗时较长，另一方面也可能因为集群规模过大，下载解压环节造成较大的网络，磁盘读写压力，进而导致大规模容器启动不符合部署预期。实际上在容器启动时，可能仅使用容器镜像内的部分数据。
容器镜像服务企业版支持按需加载功能，您可在业务部署中使用经转换的加速镜像版本，实现镜像数据免全量下载和在线解压，大幅提升应用分发效率，享受极致的弹性体验。本文介绍如何按需加载容器镜像。

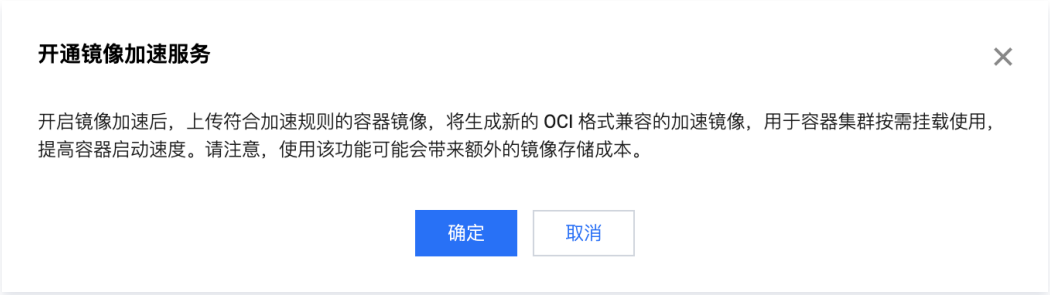
前提条件

- 已成功 创建容器集群 。当前按需加载功能仅面向腾讯云 容器服务TKE 提供适配支持，且需集群具备以下配置：
  - 集群 Kubernetes版本 在1.16及以上。
  - 集群 运行时组件 为 containerd，且版本为1.4.3。已创建的集群可修改运行时配置至 containerd 1.4.3，调整后添加的节点默认为此版本运行时。
  - 集群操作系统为 Ubuntu，TencentOS，CentOS。如果使用 CentOS，需要在集群节点上执行 `yum install -y fuse` 安装 fuse 应用。
- 已成功 购买企业版实例 。按需加载容器镜像功能当前仅限**高级版实例**开启使用。
- 容器集群所在私有网络 VPC 已接入至企业版实例，允许集群节点内网访问实例内镜像，具体配置可参考 配置私有网络的访问控制 。

准备加速镜像

开启镜像加速

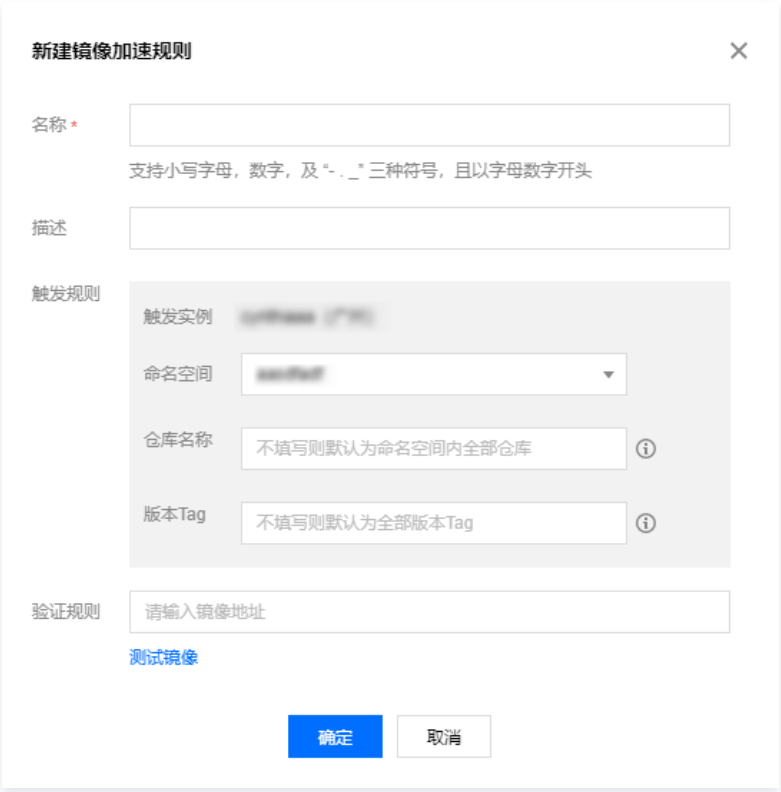
1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**镜像加速**。
2. 在“镜像加速”页面选择需要开启镜像加速的实例地域和实例名称，可查看当前实例镜像加速的状态及镜像加速规则列表。
3. 单击**开启镜像加速**，在“开通镜像加速服务”窗口中，请仔细阅读相关提示。如下图所示：



   - 开启镜像加速后，上传符合加速规则的容器镜像，将生成新的 OCI 格式兼容的加速镜像。
   - 请注意，开启并使用该功能后，同时存储普通镜像及加速镜像将带来额外的镜像存储成本。
4. 单击确定即可为当前实例开启镜像加速功能。

添加镜像加速规则

1. 单击**添加镜像加速规则**，在“新建镜像加速规则”窗口中，参考以下提示进行规则配置。如下图所示：



- **名称**：规则名称。
- **描述**：规则描述，支持中文。
- **触发规则**：
  - **触发实例**：当前所选实例即为触发实例。
  - **命名空间**：当前实例内需要加速分发的命名空间，暂不支持选择全部命名空间。
  - **仓库名称**：加速的仓库，支持正则表达式筛选。不填写则默认为命名空间内全部仓库。
  - **版本Tag**：加速的版本，支持正则表达式筛选。不填写则默认为符合条件的仓库内所有版本。
- **验证规则**：输入需要加速的镜像地址，验证当前规则下该镜像是否满足加速规则。

2. 单击**确定**即可为当前实例添加镜像加速规则。

推送镜像并自动转换

成功添加规则后，可在“镜像加速”页面查看已添加的镜像加速规则。确认规则状态为开启中，并向符合规则的镜像仓库内推送新的容器镜像，自动触发加速镜像格式转换，生成带有 -apparate 后缀的加速镜像。默认镜像的制品类型为 Docker-Image，经转换后的镜像制品类型为 OCI-Image-v1。

镜像版本	大小	安全级别	制品类型	摘要(SHA256)	更新时间	操作
nginx-apparate	56.14 MB	-	OCI-Image-v1	sha256:ca16135a610534...	2021-12-06 16:01:14	拉取指令 扫描 层信息 删除
nginx	54.1 MB	-	Docker-Image	sha256:4424e31f2c3661...	2021-12-06 16:00:54	拉取指令 扫描 层信息 删除

部署加速镜像

容器服务 TKE 是腾讯云官方提供的 Kubernetes 托管服务，与容器镜像服务 TCR 紧密结合，您可在 TKE 集群中安装 TCR 加速应用，部署加速镜像，提高业务启动速度。

配置集群节点

集群节点默认不支持使用加速镜像，节点若需优先使用加速镜像，您可通过命令行或容器服务控制台为集群节点添加镜像加速标签。

通过命令行添加镜像加速标签

您可执行以下命令为集群节点添加镜像加速标签：

```
kubectl label node xxx cloud.tencent.com/apparate=true
```

通过控制台添加镜像加速标签

1. 登录 容器服务控制台，选择左侧导航栏中的**集群**。
2. 在“集群管理”页面单击需要使用镜像加速分发功能的集群 ID，进入集群详情页。
3. 设置节点 Label 的集群 ID/名称，进入集群详情。
4. 在左侧导航栏中，选择 “节点管理” > “节点”，进入“节点列表” 页面。
5. 选择需要设置 Label 的节点行，单击**更多 > 编辑标签**。
6. 在弹出的 “编辑 Label” 窗口中，编辑 Label 为 `cloud.tencent.com/apparate=true`，单击**提交**。

安装加速应用

集群默认不支持使用加速镜像，需要在集群安装 TCR 加速套件应用。安装 TCR 加速套件应用后，已经被标记为支持部署加速镜像的节点将自动部署守护进程 daemonset，并可正常加载加速镜像。
在安装 TCR 加速套件应用，新增节点并使用 cloud.tencent.com/apparate=true 标记，节点也将自动部署守护进程，并可正常部署加速镜像。

通过命令行安装加速套件应用

1. 安装 Helm V3 命令行工具，参考 使用 Helm 客户端上传及下载 Helm Chart
2. 添加 Helm Repo，并拉取 TCR 加速应用 Chart

```
helm repo add tcr-helm-public https://helmhub.tencentcloudcr.com/chartrepo/public
helm pull tcr-helm-public/apparate --version 1.0.0
```

3. 解压已下载 Chart，并修改 values.yaml

```
tar -xzvf apparate-1.0.0.tgz
vim apparate/values.yaml
```

其中，请配置以下参数：
3.1 imagePullSecretsCrs：此配置用于拉取加速镜像。请修改其中的 dockerUsername，dockerPassword，dockerServer，分别填写企业版实例的用户名，密码及访问域名。
3.2 image：保持默认即可，此配置用于集群安装应用时拉取基础镜像。如集群是非中国大陆内部署，可修改为对应地域个人版镜像仓库的访问域名。

4. 重新打包 Chart，并安装至指定集群

```
helm package apparate/
helm install apparate apparate-1.0.0.tgz
```

执行 helm install 需要预先在本地配置集群的访问凭证，具体可参考：本地 Helm 客户端连接集群 。

5. 进入 集群应用 页面，确认应用的安装状态及配置。

部署加速镜像

新建工作负载时选择实例内镜像，仅当符合以下条件时，集群将实现镜像按需加载，极速启动容器：

- 工作负载所指定的容器镜像为已经转换的加速格式镜像，如 nginx:latest-apparate，制品类型为 OCI-Image-v1。
- 工作负载 Pod 被调度到的节点已添加使用镜像加速的标签，即已添加 `cloud.tencent.com/apparate=true`

因此，在创建工作负载时，请选择加速镜像版本，并添加 nodeSelector，设置为 `cloud.tencent.com/apparate=true`，该工作负载将强制调度至支持加速镜像的节点上，实现加速启动。

常见问题

是否可以删除常规镜像及加速镜像?

可以，当镜像仓库内同时存在常规镜像和对应的加速镜像，删除其中一个镜像并不影响另一个的正常拉取及部署。

推送镜像后，未自动生成加速镜像怎么办?

首先请检查该镜像是否匹配已有加速规则，如确定已符合启用状态的加速规则，您可咨询 智能客服 或 在线咨询 寻求帮助。

镜像安全

容器镜像安全扫描

最近更新时间：2023-12-04 10:35:57

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持对托管的容器镜像进行安全扫描，生成扫描报告，暴露容器镜像内潜在的安全漏洞，并提供修复建议。容器镜像安全是云原生应用交付安全的重要一环，对上传的容器镜像进行及时安全扫描，并基于扫描结果选择阻断应用部署，可有效降低生产环境漏洞风险。
镜像安全扫描功能内置在镜像仓库中，用户可在上传容器镜像后，主动触发对指定版本容器镜像的安全扫描，也可以在命名空间层级配置自动扫描，该命名空间内新推送镜像上传完成后将自动被扫描。当前镜像安全扫描服务基于开源 Clair 方案，相关漏洞信息来自官方 CVE 漏洞库，并定期保持同步。

前提条件

在使用镜像安全扫描功能前，您需要完成以下准备工作：

- 已成功 购买企业版实例 。
- 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

配置扫描策略

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**命名空间**。
2. 在**命名空间**页面中，单击需开通镜像安全扫描功能的实例名称，进入命名空间详情页。
3. 在**基本信息**页，单击**安全扫描后的**手动，如下图所示：

4. 将安全扫描配置为**自动扫描**，单击**确认**，如下图所示：

手动触发扫描

步骤1：准备容器镜像

请参考 镜像仓库基本操作 上传容器镜像，并在对应镜像仓库的版本管理页查看该镜像。

步骤2：触发镜像扫描

选择该镜像仓库内指定镜像版本，单击**扫描**触发镜像扫描，此时安全级别显示为“扫描中”。如下图所示：

> **注意：**
> 镜像扫描功能仅支持制品类型为 DockerImage 的镜像，其他类型制品暂不支持镜像扫描。

步骤3：查看扫描结果

安全扫描完成后，安全级别处将自动展示当前镜像内漏洞的最高等级及个数，可单击查看漏洞详情。如下图所示：

查看镜像的漏洞详情时，可单击指定的漏洞编号，跳转至该漏洞的详细说明，评估漏洞对业务的实际影响范围。如下图所示：

步骤4：重新触发扫描

因漏洞库会定时更新，您可参考 步骤2：触发镜像扫描 重新触发指定镜像的安全扫描，获取最新的扫描结果。

镜像版本不可变

最近更新时间：2023-12-04 10:35:35

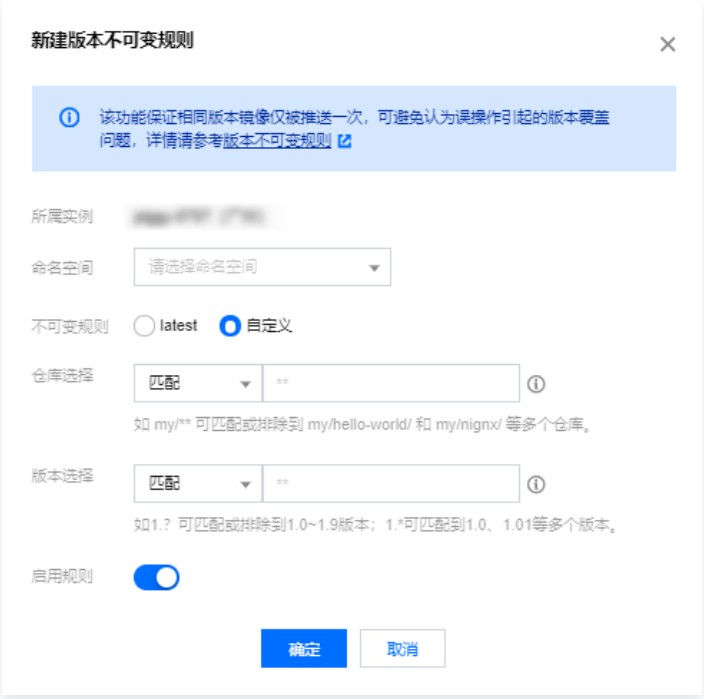
操作场景

腾讯云容器镜像服务（Tencent Container Registry, TCR）企业版支持对托管的容器镜像版本进行保护。容器镜像安全是云原生应用交付中的关键一环，为托管在 TCR 的镜像开启版本不可变功能，可确保相同版本的镜像仅被成功推送一次，进而有效降低生产环境下由误操作引起的版本覆盖风险。TCR 支持命名空间级别的版本保护，用户可以根据业务需求的细粒度定义该功能所覆盖的仓库和镜像版本。

操作步骤

创建版本不可变规则

1. 登录 容器镜像服务控制台，选择左侧导航栏中的**版本管理** > **版本不可变**。
2. 在**版本不可变**页面，选择实例所在地域、实例名称。
3. 单击**新建规则**，在**新建版本不可变规则**页面，参考以下提示进行规则配置。如下图所示：



配置项	配置说明
所属实例	当前已选择实例。
命名空间	当前实例需要开启版本保护的命名空间。单个命名空间内仅支持创建一条规则。
不可变规则	latest：当前命名空间下所有仓库中，除 latest 版本外，其余镜像版本均不可被覆盖。
	自定义：自定义配置需要匹配的仓库和镜像版本。 • 仓库匹配：选择镜像仓库的过滤类型，并填写需要过滤的仓库名称。 • 版本匹配：选择镜像版本的过滤类型，并填写需要过滤的版本名称。
启用规则	规则默认创建时生效。 规则状态启用即代表规则生效，您可在配置中开启/关闭该规则。

4. 单击**确定**即可创建规则。

管理版本不可变规则

成功创建后即可在**版本不可变**页面查看规则，您可执行以下操作管理版本不可变规则。如下图所示：

- **配置**：重新配置实例版本不可变规则，不支持修改生效的命名空间。
- **删除**：删除该实例下的版本不可变规则。

高危镜像部署阻断

最近更新时间：2024-03-25 10:37:00

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持对托管的容器镜像进行安全扫描，生成扫描报告，暴露容器镜像内潜在的安全漏洞，并提供修复建议。容器镜像安全是云原生应用交付安全的重要一环，对上传的容器镜像进行及时安全扫描，并基于扫描结果选择阻断应用部署，可有效降低生产环境漏洞风险。
镜像部署阻断功能内置在命名空间层级，可选择开启该功能，并配置阻断规则及可忽略的镜像漏洞。开启该功能后，如容器客户端尝试拉取符合阻断策略的容器镜像，将被阻断，并返回相关报错说明。

前提条件

在使用镜像部署阻断功能前，您需要完成以下准备工作：

- 已成功 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操作权限。

操作步骤

配置阻断策略

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**命名空间**。
2. 在“命名空间”页面中，单击需配置阻断策略的实例名称，进入命名空间详情页。
3. 在“部署安全”页，将启动阻断配置为已开启，并配置需要阻断的漏洞等级。如下图所示：

配置漏洞白名单

已开启部署阻断后，可配置漏洞白名单，输入一条或多条 CVE ID，并用英文逗号分隔。如果镜像安全扫描结果中包含该漏洞 ID，将被阻断策略忽略。即如果该镜像内有一高危漏洞，但高危漏洞已被配置为白名单，则即便已配置阻断具有高危漏洞的镜像拉取，该镜像仍可正常拉取。

容器镜像签名

最近更新时间：2023-09-13 17:02:51

镜像签名和验签功能可避免中间人攻击和非法镜像的更新及运行，进而实现镜像从分发到部署的全链路一致性。腾讯云容器镜像服务（Tencent Container Registry，TCR）企业版支持开启命名空间级别的镜像自动签名特性，在推送镜像到仓库时自动匹配签名策略并完成加签动作，保障您仓库下的镜像内容可信。

> **注意：**
> 容器镜像签名当前为 Beta 功能，功能使用过程中如遇到异常，您可 在线咨询 联系我们。

前提条件

在使用镜像签名功能前，您需要完成以下准备工作：

- 已成功 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操作权限。
- 已开通 密钥管理服务 。

操作步骤

创建非对称签名验签密钥

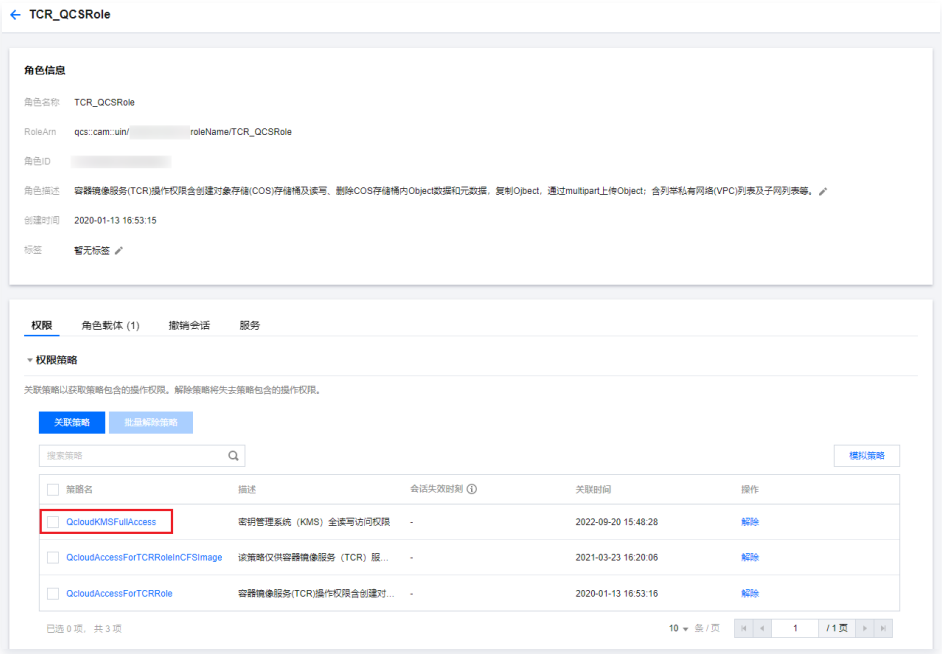
1. 登录 密钥管理系统（合规）控制台 。
2. 在**密钥管理 > 用户密钥**中，单击**新建**。
3. 在“新建密钥”弹窗中，配置密钥参数，单击**确定**。容器签名功能要求 KMS 的密钥用途为**“非对称签名验签”**，加密算法为**“RSA_2048”**，其他参数配置请参见 创建密钥 。

> **说明**
> TCR 支持获取 KMS 服务全地域下的用户密钥，为降低跨地域间的通信开销，建议 KMS 用户密钥和镜像仓库实例位于相同地域下。

授权容器镜像服务使用 KMS 密钥

为让 TCR 服务可以读取到您账号下的非对称签名验签密钥，需要在您的账号配置如下策略。

1. 登录 访问管理控制台 。
2. 在“角色”页面，单击**TCR_QCSRole**。
3. 在 TCR_QCSRole 角色详情页，关联预设策略 **QcloudKMSFullAccess**，如下图所示：



创建镜像签名策略

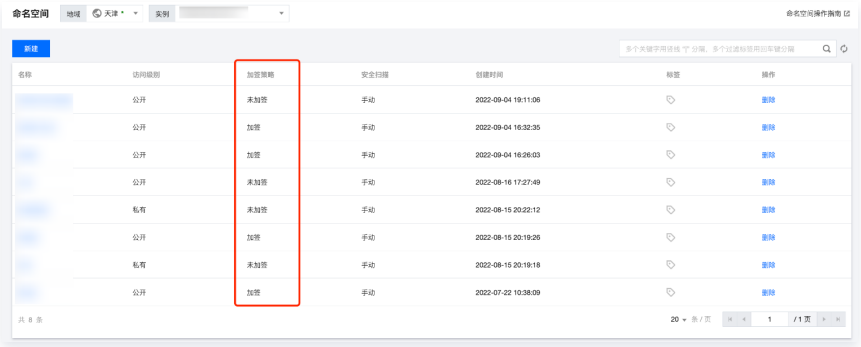
1. 登录 容器镜像服务控制台 。
2. 在实例管理页面中选择目标镜像仓库实例。
3. 选择左侧导航栏中的**镜像安全**，进入“镜像签名”详情页。
4. 单击**新建**，在“新建签名策略”弹窗中，填写以下信息：

   - **策略名称**：镜像签名策略名称。长度限制在2-50个字符，只能包含小写字母、数字及分隔符(".“、”_“、”-“，”/")且不能以分隔符开头、结尾或连续。
   - **命名空间**：镜像签名策略生效的命名空间，一个命名空间下仅支持创建一个签名策略。
   - **KMS 密钥**：支持签名操作的 KMS 用户密钥，仅支持加载”非对称签名验签RSA2048“用途密钥。
   - **域名**：用于访问仓库实例服务。
5. 单击**确认**完成签名策略的创建。

> **说明**
> - 签名策略创建后对新镜像立刻生效，即推送镜像到仓库时将自动匹配签名策略并完成镜像加签动作。
> - 签名策略开启对仓库中已经存在的镜像不生效，您需在**镜像仓库 > 版本管理**中手动触发镜像签名。

查看镜像签名状态

- 可在**命名空间**页面查看是否开启加签策略。如下图所示：



- 可在**镜像仓库 > 版本管理**页面查看镜像是否开启加签策略。针对开启加签策略前已推送至仓库的镜像，可以在“操作”中手动触发加签。如下图所示：

删除镜像签名策略

在“镜像签名”页面选择需要删除的签名策略，单击**删除**。在弹出的“删除签名策略”窗口中单击**确认**。如下图所示：

说明

删除签名策略的同时会删除存量命名空间内的镜像签名信息，可能会造成签名验证失败，请谨慎操作。

相关文档

您可以在 TKE 集群中使用增强组件进行自动验签，设置相应策略在验签失败时阻断镜像部署。详情请参见 容器镜像签名验证 。

镜像清理
清理 COS 存储空间

最近更新时间：2023-12-04 10:35:13

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持设置自定义规则批量清理企业版实例内的镜像版本，但在删除镜像版本后，存储在实例关联的对象存储 COS 内的镜像数据仍保留。您可以使用制品清理功能，删除对象存储 COS 内已失效的镜像版本相关数据，清理 COS 存储空间，降低存储费用。本文将介绍如何使用制品清理功能，清理 COS 存储空间。

注意事项

制品清理功能将会影响实例服务状态及实例内数据，请评估以下注意事项后谨慎操作：

- 在执行制品清理任务时，将无法推送镜像到镜像仓库，但仍可以从镜像仓库内拉取镜像，即实例将处于只读状态。
- 制品清理任务将清理实例内所有镜像仓库内已不再被有效镜像版本关联的镜像 Layer 数据，此删除过程不可逆，建议执行真实清理任务前，使用模拟运行评估影响范围。
- 制品清理任务的耗时与 COS 内已存储镜像数据大小，镜像历史版本数相关，且暂不支持临时中止任务，建议选在非业务时间执行清理任务，或使用模拟运行评估执行时间。

操作步骤

模拟运行清理

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**制品清理**。
2. 在**制品清理**页面即可查看当前实例内的制品清理任务列表。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**模拟运行清理**，仔细阅读相关提示。

> ⚠ **注意**
> 模拟运行制品清理将全面扫描实例内可清理的垃圾数据，并预估清理范围及清理时间，期间实例基础功能不受影响，仍可推送及拉取制品，但密集计算任务可能影响实例部分功能响应性能。

4. 单击**确定**即可执行模拟清理任务。

立即执行清理

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**制品清理**。
2. 在**制品清理**页面查看当前实例内的制品清理任务列表。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**立即执行清理**，仔细阅读相关提示。

> ⚠ **注意**
> 执行制品清理期间实例将被设置为只读模式，仍可拉取镜像，无法推送镜像。任务执行时间与实例内制品数据量及实例使用时长有关。

4. 单击**确定**即可立即执行清理任务。

版权所有：腾讯云计算（北京）有限责任公司

自动删除镜像版本

最近更新时间：2024-03-06 17:05:51

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持托管分发容器镜像，并提供镜像构建功能实现代码变更自动触发镜像构建，推送及托管。如果客户需要快速迭代业务应用，可采用自动化流水线生成镜像，将会不断生成大量镜像版本，同时旧的镜像版本不再使用。单个镜像仓库内过多镜像版本将给版本管理带来负担，而且将可能触及仓库内镜像版本数配额。因此 TCR 实现了镜像版本保留功能，此功能允许用户自定义创建版本保留规则，可定时触发该规则，并自动删除保留规则外的镜像版本。
版本保留规则支持两种保留策略，保留最新推送的#个版本和保留#天内推送的版本，并支持模拟执行。 同时，在高级配置模式下，可选对仓库、版本进行过滤，配合两种保留策略，实现更加灵活精确的版本管理。

注意事项

1. 版本保留功能将删除保留规则外的镜像版本。
2. 版本保留功能仅删除镜像版本信息，但不删除底层镜像数据，如需彻底清理镜像数据，请使用 清理 COS 存储空间功能 。
3. 高级配置模式当前处于灰度阶段，如需使用高级配置模式，请 提交工单 申请。

操作步骤

创建版本保留规则

> **注意：**
> 镜像仓库可能存在一个镜像的多个版本完全相同的情况，例如同一镜像只是打了不同的 Tag，没有产生新的镜像层。这种不同 Tag 的镜像会有相同的唯一标识符 Digest。因此，不同 Tag 但相同 Digest 的镜像在物理上指向完全相同的镜像内容。当删除一个 Tag 后，镜像实体会被删除，相关的 Tag 和 Digest 也会被清理。
> 对于TCR 版本保留规则的影响是，如果仓库中存在多个不同 Tag 但相同 Digest 的镜像，而规则要求保留最新的两个镜像，那么当删除一个 Tag 时，仓库中的所有镜像都会被删除。因此，**如果您的镜像仓库存在同一 Digest 但不同 Tag 的镜像，请谨慎使用版本保留规则，或者暂时禁用已有的规则。**

1. 登录 容器镜像服务 控制台，选择左侧导航栏中**版本管理**下的**版本保留**。
   在**版本保留**页面即可查看当前实例内的版本保留规则列表。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。
2. 单击**新建规则**，在**新建版本保留规则**窗口中，参考以下提示进行规则配置，可选两种配置模式：

简易配置

- 所属实例：当前已选择实例。
- 命名空间：版本保留规则生效的命名空间，单个命名空间内暂只能创建一条规则。
- 配置模式：简易配置
- 保留版本：默认不过滤，即命名空间内全部仓库及版本。
- 保留策略：支持配置保留最新推送的#个版本，保留#天内推送的版本两种模式，并在指定版本数或天数。
- 执行周期：版本保留规则的执行周期，支持手动执行，或每天、每周、每月执行。具体执行时间为：每天为每日零点，每周默认为周一零点，每月为每月第一天零点。

- 启用规则：默认启用。

高级配置

- 所属实例：当前已选择实例。
- 命名空间：版本保留规则生效的命名空间，单个命名空间内暂只能创建一条规则。
- 配置模式：高级配置
- 保留规则：支持配置多条保留规则，保留规则间取并集，即镜像版本满足任意一条保留规则，都将被保留。
  - 仓库过滤：支持匹配或排除部分仓库，使用正则过滤仓库名。“*”和“**”匹配任意长字符串，其中“*”不支持多级仓库名称匹配，“?”匹配除‘/’以外的任意单个字符。
  - 版本过滤：支持匹配或排除仓库内部分版本，使用正则过滤版本名，规则同仓库过滤。
  - 保留策略：支持配置保留最新推送的#个版本，保留#天内推送的版本两种模式，并在指定版本数或天数。
- 执行周期：版本保留规则的执行周期，支持手动执行，或每天、每周、每月执行。
- 启用规则：默认启用。

3. 单击**确定**即可创建版本保留规则。

管理版本保留规则

版本保留规则成功创建后即可在**版本保留**页面查看已创建的版本保留规则，您可执行以下操作管理版本保留规则。如下图所示：

- **查看规则执行日志**：单击规则名称，即可查看该规则触发日志，详情请参见 查看执行日志 。
- **配置**：重新配置实例版本保留规则，不可修改生效的命名空间。
- **删除**：删除该实例版本保留规则。

查看执行日志

1. 单击指定版本保留规则名称，即可查看该规则的触发日志。如下图所示：

- **任务ID**：实例内唯一的版本保留执行任务 ID。
- **创建时间**：版本保留执行任务创建的时间。
- **任务耗时**：完成全部版本保留执行任务消耗的时间。
- **执行方式**：手动或自动，单击**立即执行**或**模拟执行**为手动方式，通过规则定义的周期自动执行，则为自动方式。
- **执行类型**：真实执行或模拟执行，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。
- **执行状态**：任务完成状态。

2. 可单击指定任务 ID 查看任务详情，并可单击具体仓库查看执行日志。

相关文档

您还可以使用 CreateTagRetentionRule 接口创建版本保留规则。详细信息请参见 创建版本保留规则 API 文档 。

DevOps
触发器（Webhook）

最近更新时间：2024-03-25 14:33:11

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持用户配置并使用灵活的触发器 (Webhook) 功能。可通过在实例内配置合适的触发器，快速接入现有研发流程及 CI/CD 平台，实现镜像更新自动触发应用部署等容器 DevOps 场景。
触发器功能允许用户自定义创建触发器规则，并支持查看触发日志。其中，触发动作同时支持容器镜像及 Helm Chart 的推送，拉取及删除操作。触发规则支持灵活的正则表达式过滤、指定实例内命名空间及通过配置镜像仓库和版本的正则过滤规则，实现仅部分仓库或特殊命名格式的镜像版本可启动触发器。自定义 Header 功能支持以 `Key:Value` 的形式配置访问目标 URL 时的 Header，可用于鉴权等场景。

前提条件

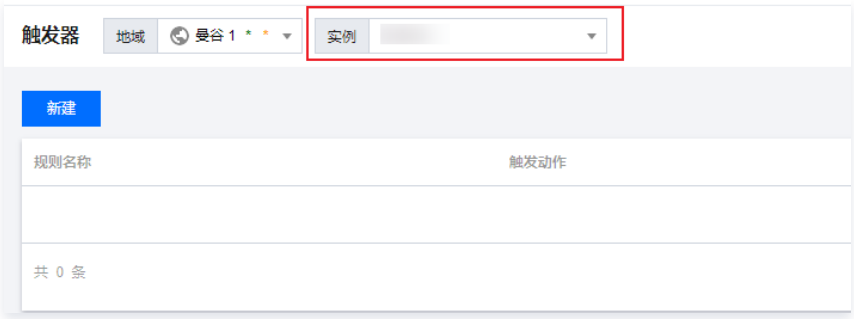
在创建并管理 TCR 企业版实例的触发器前，您需要完成以下准备工作：

- 已成功 购买 TCR 企业版实例 。本功能仅适用于企业版实例。
- 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操作权限。

操作步骤

创建触发器

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的 **触发器**。
   在**触发器**页面即可查看当前实例内的触发器规则列表。如需切换实例，请在页面上方的**实例**下拉列表中进行选择。



2. 单击**新建**，在弹出的“新建触发器”窗口中，参考以下提示进行规则配置。如下图所示：

- **名称**：实例规则名称，支持小写字母、数字及（ - 、 . 、 _ ）三种符号，且需以字母数字开头。本文以 webhook-demo 为例。
- **描述**：规则描述，支持中文。
- **触发动作**：当前支持推送镜像、删除镜像，上传 Chart 及删除 Chart 四种触发动作。触发器执行时，发起的 webhook 请求内将包含该触发动作信息。
- **触发规则**：
  - **触发实例**：触发器所属的实例，即为当前已选择实例，不可修改。
  - **命名空间**：触发器生效的命名空间，如果列表为空，请先在该实例内 创建命名空间 。
  - **仓库名称**：触发器生效的仓库名称，支持对镜像仓库及 Helm Chart 仓库进行 正则匹配 。
  - **版本Tag**：触发器生效的 Tag，支持 正则匹配 。如需所有版本均可触发，可不填写。
- **URL**：触发器被触发后，发起请求的目标 URL，即用户配置的 Webhook Server 的访问地址。触发器将向该 URL 地址发起 POST 请求，请求 body 中将包含触发动作、触发规则等信息。
- **Header**：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 。

3. 单击**确定**即可创建同步规则。

管理触发器规则

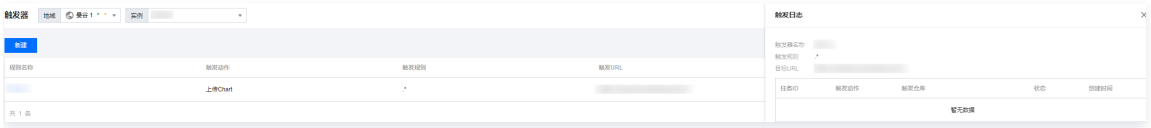
成功创建后即可在“触发器”页面查看已创建的触发器规则，您可执行以下操作管理触发器规则。如下图所示：

- **查看触发日志**：单击触发器规则名称，或触发器规则名称右侧的**触发日志**即可查看该规则触发日志，详情请参见 查看触发器日志 。

- **修改规则状态：** 表示规则启用，表示规则关闭。新建的实例同步规则默认为启用状态，您可自行调整。
- **配置：** 重新配置触发器规则，可配置全部参数。
- **删除：** 删除该触发器规则。

查看触发器日志

单击指定触发器规则名称，或触发器规则名称右侧的**触发日志**，即可查看该规则的触发日志。如下图所示：



包含信息如下：

- **任务ID：** 实例内唯一的触发器任务 ID。
- **触发动作：** 产生该次触发的触发动作，例如推送镜像。
- **触发仓库：** 产生该次触发动作的仓库资源。
- **状态：** 触发器执行 webhook 请求的成功状态 。
- **创建时间：** 该次触发的启动时间，即发起 webhook 请求的时间。

相关信息

Webhook 请求格式参考

当用户对符合规则的资源执行相应动作时，例如向指定镜像仓库推送新的镜像时，则相应触发器将被触发，并向规则中配置的 URL 发起 HTTP POST 请求，请求 Body 中包含的触发动作、仓库路径等信息。以下为推送镜像触发后并经解析的请求 Body 信息，可供开发 Webhook 服务端参考。

```
{
  "type": "pushImage",
  "occur_at": 1589106605,
  "event_data": {
    "resources": [
      {
        "digest": "sha256:89a42c3ba15f09a3fbe39856bddacdf9e94cd03df7403cad4fc105xxxx268fc9",
        "tag": "v1.10.0",
        "resource_url": "xxx-bj.tencentcloudcr.com/public/nginx:v1.10.0"
      }
    ],
    "repository": {
      "date_created": 1587119137,
      "name": "nginx",
      "namespace": "public",
      "repo_full_name": "public/nginx",
      "repo_type": "public"
    }
  },
  "operator": "332133xxxx"
}
```

使用正则表达式新建规则

正则匹配规则

以下是填写“仓库名称”和“版本Tag”时，其正则表达式支持的匹配规则：

- `*`：匹配所有不包含路径分隔符（`/`）的任意长字符串。
- `**`：匹配所有的任意长字符串，包括路径分隔符（`/`）。

> **注意**
> `**` 必须作为一段完整的相对路径，如果使用 `/path**` ，其作用将等同于 `/path*` ，仅能匹配以path为名称前缀的一级仓库。要想匹配path下的所有仓库，应使用 `/path/**` ；要想匹配以path为名称前缀的所有仓库，则应使用 `/path*/**` 。

- `?`：匹配除 ‘/’ 以外的任意单个字符。
- `{alt1, alt2, ...}`：同时匹配多个正则表达式。

典型场景

匹配选定命名空间内所有仓库	** 或者不填
匹配选定命名空间内以 path 为名称前缀的所有一级仓库	/path*
匹配选定命名空间内以 path1 和 path2 为名称前缀的所有一级仓库	/{path1, path2}*
匹配选定命名空间内 path1 和 path2 目录下的所有仓库	/{path1, path2}/**
匹配选定命名空间内以 path1 和 path2 为名称前缀的所有仓库	/{path1, path2}*/**
匹配选定仓库内所有 1.x 的版本Tag	1.?
匹配选定仓库内所有以 env1 和 env2 为名称前缀的版本 Tag	{env1*, env2*}

镜像自动部署

最近更新时间：2024-03-25 16:52:31

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）基于腾讯云 CODING DevOps 提供了镜像构建及交付流水线功能，满足容器用户快速配置并应用持续集成及持续部署的需求。如需使用更加灵活强大的持续编译、构建、交付流水线功能，请了解并使用 容器 DevOps 。
目前 TCR 企业版及个人版服务均支持交付流水线功能，用于自动部署容器镜像至指定容器集群。该功能支持指定镜像仓库，在该仓库内新推送镜像时，筛选符合部署规则的镜像版本，自动部署至容器集群内。当前支持部署至 容器服务 TKE，Serverless 容器服务，边缘容器服务 Edge。可参考最佳实践文档 使用交付流水线实现容器 DevOps 快速上手本功能。

前提条件

在进行配置镜像自动构建前，您需要完成以下准备工作：

- 已成功 购买企业版实例，或已初始化个人版实例。
- 已开通 CODING DevOps 服务，并完成授权操作。详情请参见 开通服务 。
- 如果使用子账号进行操作，请参考 企业版授权方案示例 或 个人版授权方案示例 提前为子账号授予对应实例的操作权限。

操作步骤

创建交付流水线

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**。
   在“交付流水线”页面即可查看当前实例内的交付流水线列表。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。
2. 单击**新建**，在“新建交付流水线”页面，参考以下提示进行配置。
   - **基本信息**：配置流水线名称及描述，描述支持输入中文。该信息可在创建后编辑。

   - **镜像配置**：配置绑定的镜像仓库及需要部署的镜像过滤规则。

- 镜像仓库：选择企业版或个人版实例内已有的镜像仓库。
- 镜像版本过滤：指定需要部署的镜像。支持 “直接部署任意版本”，“仅部署指定名称版本”，“仅部署指定规则版本”。其中指定规则为正则表达式输入。
- 镜像来源：可选择平台构建镜像或本地推送镜像。如该镜像仓库尚未配置镜像自动构建，可选择使用平台构建镜像。如需使用自建的 CI 服务构建镜像或手动打包镜像，可选择本地推送镜像。

- **应用部署**：配置镜像部署环境。
  - 部署平台：支持容器服务 TKE，Serverless 容器服务，边缘容器服务 TKE Edge。
  - 部署地域：集群所在地域。
  - 部署集群：选择目标集群。
  - 命名空间：集群内的命名空间。
  - 工作负载类型：支持 Deployment，StatefulSet，DaemonSet。
  - 工作负载：选择该命名空间下已有工作负载。暂不支持新建工作负载。
  - Pod容器：工作负载内指定的容器，将更新该容器内镜像。

3. 单击**确定**即可创建镜像构建规则。

如上述配置参数不满足需求，请直接前往 CODING DevOps 平台使用**持续构建**功能。

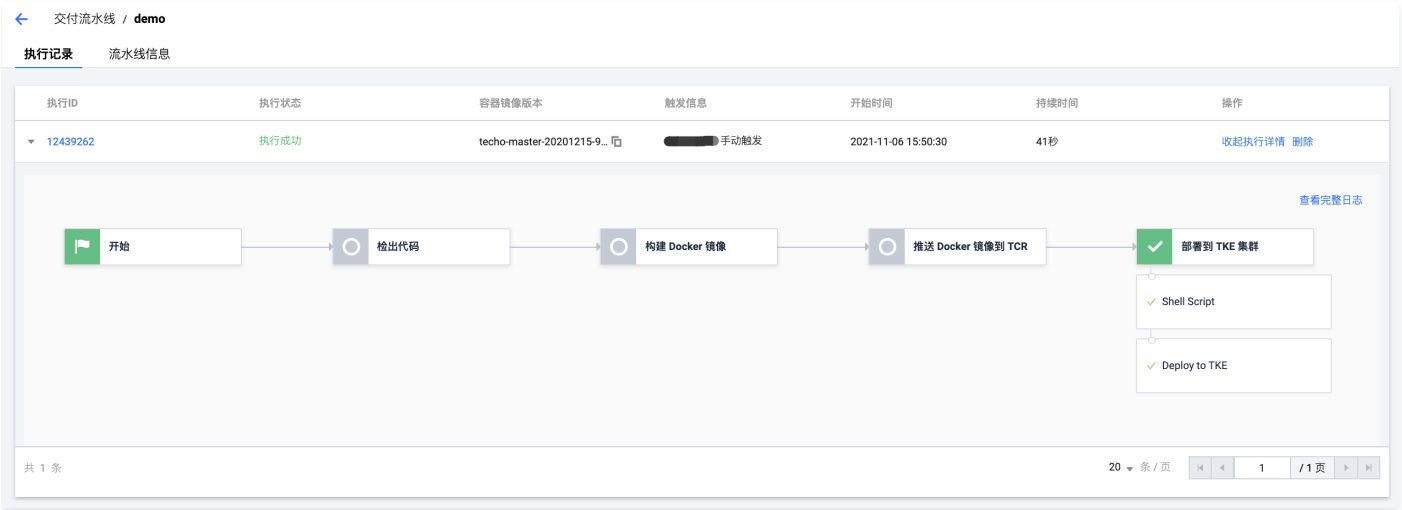
管理交付流水线

完成交付流水线创建后，即可在 **交付流水线** 列表页查看已有交付流水线，选择指定交付流水线，可对当前交付流水线进行以下管理操作：

1. 列表页
   - **启动**：主动触发流水线部署，可选择指定的镜像版本。
   - **编辑**：编辑流水线配置。
   - **删除**：删除流水线。
2. 详情页
   - **查看执行记录**
     进入 “执行记录” 页签，即可查看当前交付流水线的执行记录，并可查看详细日志，删除记录。
   - **查看流水线信息**
     进入 “流水线信息” 页签，即可查看当前交付流水线的详细信息，包含基本信息，镜像配置，应用部署。

触发部署并查看详情

配置交付流水线后，当有符合触发规则的镜像推送操作时，即可触发自动部署镜像。也可主动触发部署，选择指定的镜像版本。启动部署任务后，可单击该交付流水线，进入执行记录页，查看执行日志，并展看查看执行详情。



异常处理

在使用交付流水线功能时若发生以下异常问题，请参考对应方法重新尝试，若异常仍未解决则请提交 工单 进行咨询。

镜像部署失败

请前往容器集群查看该工作负载的具体日志信息，如报错信息为镜像拉取失败，请检查是否已正常配置该集群可访问镜像仓库，并检查访问凭证配置。详情见 TKE 集群使用 TCR 插件内网免密拉取容器镜像 。

镜像自动构建

最近更新时间：2024-03-25 10:49:50

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）基于腾讯云 CODING DevOps 提供了镜像构建及交付流水线功能，满足容器用户快速配置并应用持续集成及持续部署的需求。如需使用更加灵活强大的持续编译、构建、交付流水线功能，请了解并使用 容器 DevOps 。
目前 TCR 企业版及个人版服务均支持镜像构建功能，且源代码授权信息互通。镜像构建功能支持使用托管在 GitHub、GitLab.com、私有 GitLab、Gitee 码云、腾讯工蜂及 CODING 上的源代码进行编译构建。其中，建议正在使用 CODING.net 托管代码的用户直接在 CODING DevOps 产品内使用其“持续集成”功能中配置镜像构建，目前已内置“构建镜像并推送到 TCR 企业版/个人版”模板。TCR 支持四种类型的触发机制，例如推送到指定的分支触发镜像构建。支持自定义配置 Dockerfile 路径并构建目录。支持灵活配置镜像版本命名规则，例如自定义前缀-分支-构建时间-commit 号，实现镜像版本与代码更新同步管理。

前提条件

在进行配置镜像自动构建前，您需要完成以下准备工作：

- 已成功 购买企业版实例，或已初始化个人版实例。
- 已开通 CODING DevOps 服务，并完成授权操作。详情请参见 开通服务 。
- 如果使用子账号进行操作，请参考 企业版授权方案示例 或 个人版授权方案示例 提前为子账号授予对应实例的操作权限。

操作步骤

创建镜像仓库

参考 创建镜像仓库 完成镜像仓库创建，其中“镜像来源”选择“平台构建镜像”。

创建镜像构建规则

1. 成功创建镜像仓库后，页面将自动跳转至该镜像仓库的 **镜像构建** 页签下。如下图所示：

2. 单击“新建镜像构建规则”，在弹出的“新建镜像构建规则”窗口中参考以下信息，为该镜像仓库配置自动构建镜像及推送。如下图所示：

- **代码源**：镜像构建使用的源代码所在的托管平台，目前已支持 GITHUB、GITLAB、私有GITLAB、GITEE、工蜂、CODING，请按需选择。建议 CODING 用户直接在 CODING DevOps 平台内进入镜像构建模块，并使用内置的 **构建镜像并推送到 TCR 企业版** 或 **构建镜像并推送到 TCR 个人版** 模板配置镜像构建。镜像构建服务需要拉取对应源代码，首次使用请先为指定的代码源进行授权，授权后可正常列举代码仓库及分支等信息。如遇源代码授权异常问题，请提交 工单 进行咨询。
- **代码仓库**：指定代码源后，如已完成该代码源授权，可选择在该源代码托管平台下的代码仓库，镜像构建服务触发后将拉取该代码仓库内源代码进行编译及构建。
- **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。
- **构建参数**：可配置 docker build 中的 --build-arg，注意适配 Dockerfile。

3. 单击**确定**即可创建镜像构建规则。

如上述配置参数不满足需求，请直接前往 CODING DevOps 平台使用 **持续构建** 功能。

管理镜像构建规则

完成镜像构建规则创建后，即可在该仓库的 **镜像构建** 页签下查看构建配置及构建日志，如下图所示：

可对当前构建规则进行以下管理操作：

- **立即构建**
  在控制台内手动触发镜像构建，可指定分支或代码版本。
- **编辑**
  可编辑当前的构建规则，创建过程中可配置的参数均可重新编辑。
- **删除**
  删除当前的构建规则。
- **自动触发**
  可开启或关闭该规则的自动触发。当关闭自动触发后，推送代码并符合触发规则也无法触发镜像构建，但仍可使用 "立即构建" 功能进行手动触发。

触发镜像构建并查看构建日志

配置镜像构建规则后，当有符合触发规则的源代码操作时，即可触发自动构建并推送镜像。本文以向 GitHub 内代码仓库指定分支推送新的代码更新为例。如下图所示：

对于已有构建日志，可查看执行详情或删除该日志记录。

异常处理

在使用镜像构建功能时若发生以下异常问题，请参考对应方法重新尝试，若异常仍未解决则请提交 工单 进行咨询。

源代码授权失败

可在“新建镜像构建规则”窗口中再次单击“授权源代码”进行授权，或前往对应的源代码托管平台查看第三方授权，删除 “CODING DevOps” 后再次尝试重新授权。以 GitHub 为例，第三方授权位置为：**Setting** > **Applications** > **Authorized OAuth Apps**。

镜像构建失败

可在构建日志中查看该次构建任务的执行详情，并基于执行详情的报错信息进行调整。例如，重新配置镜像构建配置中的参数，或调整 Dockerfile。

OCI 制品管理

OCI 制品管理概述

最近更新时间：2024-03-25 14:32:55

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）兼容 OCI 标准，支持托管包含 Docker Image 在内的多种云原生制品（Artifacts），满足进阶用户对 Helm Chart，CNAB 及自定义的 OCI Artifacts 托管，分发的需求。
目前企业版及个人版实例均支持托管 OCI 制品，可直接推送 OCI 制品至镜像仓库内，并查看制品类型，获取拉取指令。
如需了解 OCI 制品及使用方式，请参考 GitHub 上官方项目 opencontainers/artifacts 。

前提条件

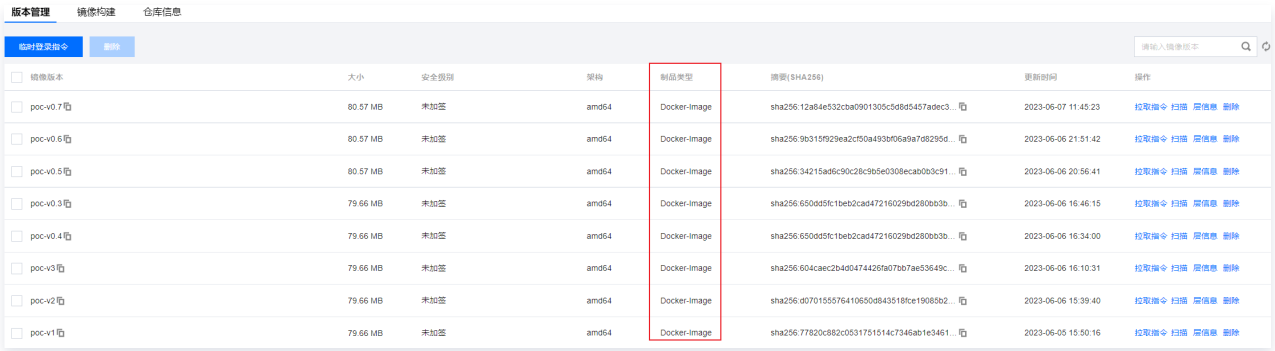
在上传并管理 TCR 实例内的 OCI 制品前，您需要完成以下准备工作：

- 已成功 购买企业版实例，或初始化个人版。
- 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。

操作步骤

使用控制台管理 OCI 制品

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**镜像仓库**。
2. 在 “镜像仓库” 页面即可查看当前实例内的镜像仓库列表，默认支持托管 OCI 制品。您可使用 OCI 制品专用的客户端工具构建 OCI 制品，并推送至镜像仓库内。
3. 单击指定镜像仓库名称，进入该仓库详情页，查看仓库内已有 OCI 制品。



相关文档

Helm Chart 管理

如您需要使用 Helm Chart，可选择将 Helm Chart 作为 OCI 制品推送至镜像仓库内进行统一管理，此管理方式需要使用 Helm V3 工具。您也可以直接使用企业版实例基于 Chart Museum 开源项目提供的 Helm Chart 托管功能，详情请参考：托管 Helm Chart 。

托管 Helm Chart

最近更新时间：2024-03-25 14:32:23

操作场景

腾讯云容器镜像服务（Tencent Container Registry，TCR）支持托管 Helm Chart，满足用户对云原生应用托管分发的需要。用户可在同个命名空间内同时管理容器镜像及 Helm Chart，实现在业务项目内同时使用容器镜像和 Helm Chart 云原生交付物。
目前仅企业版实例支持托管 Helm Chart，支持使用控制台或 Helm 客户端实现 Chart 的上传及下载。Helm Chart 仓库继承其所属的命名空间的公开及私有属性，无需额外配置。在权限管理上，Helm Chart 与容器镜像共用 **repository** 资源类型，即**qcs::tcr:$region:$account:repository/tcr-xxxxxx/project-a/*** 资源描述将包含命名空间 project-a 内全部镜像仓库及 Helm Chart，用户可在进行资源权限管理时灵活使用。

前提条件

在上传并管理 TCR 企业版实例内的 Helm Chart 前，您需要完成以下准备工作：

- 已成功 购买企业版实例 。
- 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。

操作步骤

使用控制台管理 Helm Chart

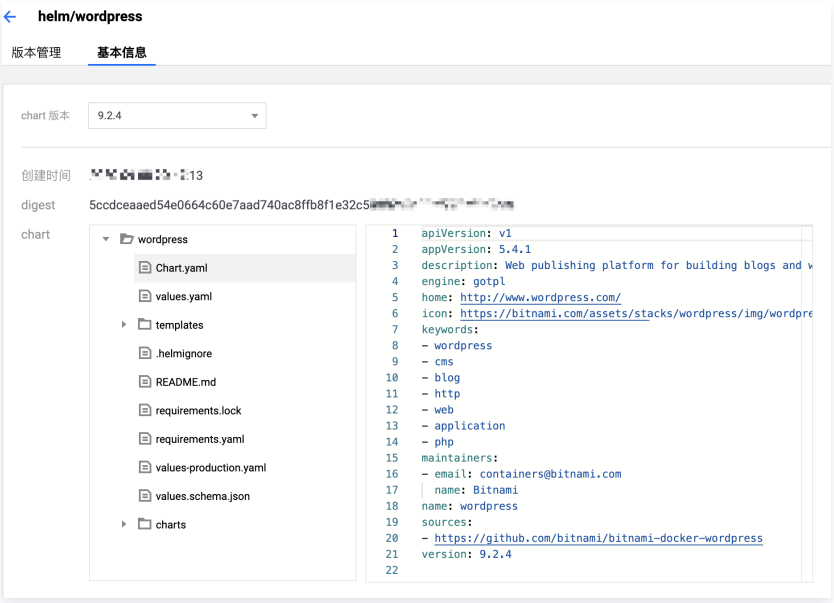
1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**Helm Chart**。
2. 在 **Helm Chart** 页面即可查看当前实例内的 Helm Chart 列表。如需切换实例，请在页面上方的**实例**下拉列表中进行选择。如下图所示：

Chart 列表包含以下信息及操作：

- **名称**：Helm Chart 名称，单击可进入 Chart 详情页，可查看并管理 Chart 各个版本，并可在**基本信息**页签内查看各个版本 Chart 包内的文件详情。
- **命名空间**：Helm Chart 所属命名空间。
- **创建时间**：Helm 首次推送至仓库的时间。
- **操作**：单击**快捷指令**获取操作当前仓库的快捷指令，具体操作指令请参考 使用 Helm 客户端上传及下载 Helm Chart；单击**删除**以删除当前仓库。

3. 单击指定 Helm Chart 仓库名称，进入该仓库详情页。
   - **版本管理**：此页面展示当前仓库内已有的 Chart 版本，可**下载**或**删除**指定版本。如下图所示：

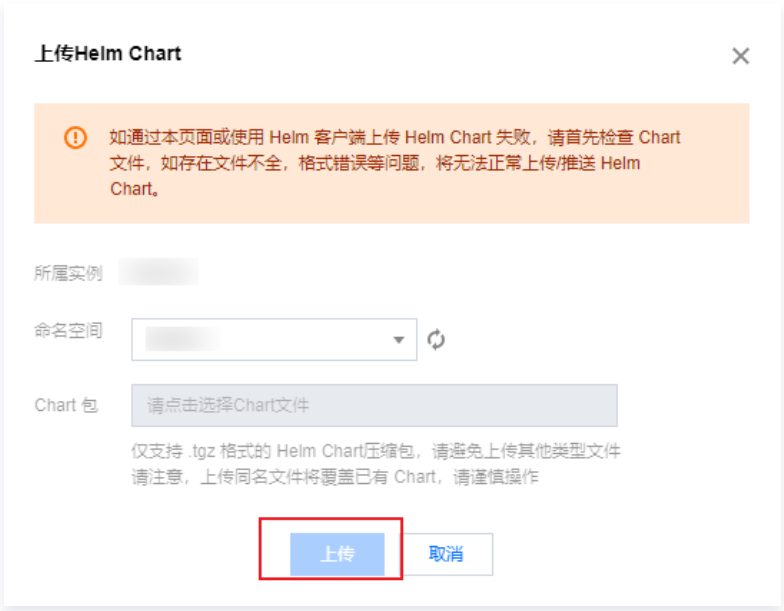
   - **基本信息**：此页面可浏览指定 Chart 版本内的详细信息，如 Chart.yaml。如下图所示：



使用控制台上传及下载 Helm Chart

上传本地 Helm Chart 包

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**Helm Chart**。
   在“Helm Chart”页面即可查看当前实例内的 Helm Chart 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。
2. 单击**上传**，在“上传 Helm Chart”窗口中，参考以下提示进行配置。如下图所示：



   - **所属实例**：当前所选实例。
   - **命名空间**：Helm Chart 所属的命名空间，如果列表为空，请先在该实例内 新建命名空间 。
   - **Chart 包**：单击后选择本地已下载的 Helm Chart 包。

   > **注意**
   > 仅支持 .tgz 格式的 Helm Chart压缩包，请避免上传其他类型文件。请注意，上传同名文件将覆盖已有 Chart，请谨慎操作。

3. 单击**上传**即可开始上传该 Helm Chart 包。上传完成后，可在仓库列表页查看已上传的 Helm Chart，若上传的 Helm Chart 包没有对应的 Helm Chart 仓库，将自动新建一个 Chart 仓库。

下载 Helm Chart 包至本地

1. 在Helm Chart页面查看当前实例内的 Helm Chart 仓库列表。单击指定仓库，即可进入该 Helm 仓库的版本管理页面。
2. 选择该 Chart 仓库内指定版本，单击该版本所在行右侧的**下载**，即可自动下载该版本的 Chart 包至本地。根据浏览器及配置的不同，可选择指定下载路径。

使用 Helm 客户端上传及下载 Helm Chart

安装 Helm 客户端

> **说明**
> - 若您当前希望在容器服务 TKE 中使用 Helm，请选择 Helm v3.x.x 版本。可执行 `helm version -c` 命令查看已安装的客户端版本。
> - 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。

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
```

添加 Helm 仓库

1. 登录 容器镜像服务控制台，在“实例列表”页面选择实例名称，进入实例详情页。
2. 参考 获取实例访问凭证 获取用户名及登录密码。
3. 在节点上执行以下命令，添加希望用于托管 Helm Chart 的命名空间至本地 Helm 仓库。

> **注意**
> 执行命令的机器需确保已在对应实例的公网白名单或已链接的私有网络 VPC 中，详情请参见 公网访问控制 ， 内网访问控制

```
helm repo add $instance-$namespace https://$instance.tencentcloudcr.com/chartrepo/$namespace --username $username
--password $instance-token
```

- `$instance-$namespace` ：为 helm repo 名称，建议使用**实例名称+命名空间名称**组合的方式命名，以便于区分各个实例及命名空间。
- `https://$instance.tencentcloudcr.com/chartrepo/$namespace` ：为 helm repo 的远端地址。
  - `$username` ：为 步骤2 中已获取的用户名。
  - `$instance-token` ：为 步骤2 中已获取的登录密码。

  如添加成功将提示以下信息。

```
"$instance-$namespace" has been added to your repositories
```

推送 Helm Chart

1. 安装 Helm Push 插件

> **注意**
> 请安装 v0.10.0 及以上版本的 helm-push 插件，避免因版本不兼容等问题造成无法正常推送 helm chart。
> 如使用 v0.10.0 以前版本，需要将 helm cm-push 替换为 helm push 指令。

使用 Helm CLI 上传 Chart 包需要安装 helm-push 插件，该插件支持使用 `helm push` 指令推送 helm chart 至指定 repo，同时支持上传目录及压缩包。

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

2. 在节点上执行以下命令，创建一个 Chart。

```
helm create tcr-chart-demo
```

3. 执行以下命令，可直接推送指定目录至 Chart 仓库（可选）。

```
helm cm-push tcr-chart-demo $instance-$namespace
```

其中 `$instance-$namespace` 为已添加的本地仓库名称。

4. 执行以下命令，可压缩指定目录，并推送至 Chart 仓库。

```
tar zcvf tcr-chart-demo-1.0.0.tgz tcr-chart-demo/
```

```
helm cm-push tcr-chart-demo-1.0.0.tgz $instance-$namespace
```

其中 `$instance-$namespace` 为已添加的本地仓库名称。

拉取 Helm Chart

1. 在节点上执行以下命令，获取最新的 Chart 信息。

```
helm repo update
```

2. 执行以下命令，拉取指定版本 Helm Chart。

```
helm fetch <本地仓库名称>/<Chart 名称> --version <Chart 版本>
```

以从企业版实例 tcr-demo 中拉取命名空间 project-a 内 tcr-chart-demo 1.0.0 版本为例：

```
helm fetch tcr-demo-project-a/tcr-chart-demo --version 1.0.0
```

个人版操作指南
更新登录密码

最近更新时间：2023-08-29 14:31:31

操作场景

本操作指南用于更新个人版实例的登录密码。

注意事项

个人版实例的登录密码为固定密码，且全地域一致。

操作步骤

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**实例管理**。
   在“实例管理”页面即可查看当前账号下的实例列表。选择任意地域的个人版实例。

2. 单击**更多 > 重置登录密码**，如下图所示：

   - **用户名**：当前登录的腾讯云账号。
   - **新密码**：重新设置的密码，建议使用高强度密码。
   - **确认密码**：再次确认密码。
3. 单击**确定**即可重置密码。

配置访问权限
个人版接入 CAM 的 API 列表

最近更新时间：2023-04-07 14:45:04

命名空间相关接口

API 名称及描述	资源类型	资源六段式示例
CreateNamespacePersonal 创建个人版命名空间	repo	qcs::tcr:$region:$account:repo/$namespace
DeleteNamespacePersonal 删除个人版命名空间	repo	qcs::tcr:$region:$account:repo/$namespace

镜像仓库相关接口

API 名称及描述	资源类型	资源六段式示例
DescribeRepositoryOwnerPersonal 查询个人版所有仓库	repo	qcs::tcr:$region:$account:repo/*
CreateRepositoryPersonal 创建个人版镜像仓库	repo	qcs::tcr:$region:$account:repo/$namespace/$repo
DeleteRepositoryPersonal 删除个人版镜像仓库	repo	qcs::tcr:$region:$account:repo/$namespace/$repo
BatchDeleteRepositoryPersonal 批量删除个人版镜像仓库	repo	qcs::tcr:$region:$account:repo/$namespace/*
DeleteImagePersonal 删除个人版仓库 tag	repo	qcs::tcr:$region:$account:repo/$namespace/$repo
BatchDeleteImagePersonal 批量删除个人版仓库 tag	repo	qcs::tcr:$region:$account:repo/$namespace/$repo
PullRepositoryPersonal 拉取个人版镜像仓库内镜像	repo	qcs::tcr:$region:$account:repo/$namespace/$repo
PushRepositoryPersonal 推送个人版镜像仓库内镜像	repo	qcs::tcr:$region:$account:repo/$namespace/$repo

个人版授权方案示例

最近更新时间：2023-04-07 14:45:40

典型场景策略配置

> **注意**
> 以下场景策略均只面向个人版使用场景。

- 授予子账号容器镜像服务（TCR）个人版内全部资源的全读写操作权限。

```
{
 "version": "2.0",
 "statement": [{
    "action": [
       "tcr:*"
    ],
    "resource": [
       "qcs::tcr:::repo/*"
    ],
    "effect": "allow"
 }]
}
```

- 授予子账号 TCR 个人版（原容器服务 TKE 内镜像仓库）内全部资源的只读操作权限。

```
{
 "version": "2.0",
 "statement": [{
    "action": [
       "tcr:Describe*",
       "tcr:PullRepository*"
    ],
    "resource": [
       "qcs::tcr:::repo/*"
    ],
    "effect": "allow"
 }]
}
```

- 授权子账号管理指定地域内的指定命名空间，例如默认地域内命名空间 team-01。

```
{
 "version": "2.0",
 "statement": [{
       "action": [
          "tcr:*"
       ],
       "resource": [
          "qcs::tcr:::repo/team-01",
          "qcs::tcr:::repo/team-01/*"
       ],
       "effect": "allow"
    }
 ]
}
```

- 授权子账号只读某个镜像仓库，即仅能拉取该仓库内镜像，无法删除仓库、修改仓库属性及推送镜像，例如默认地域内命名空间 team-01 内的镜像仓库 repo-demo。

```
{
 "version": "2.0",
 "statement": [{
       "action": [
          "tcr:Describe*",
          "tcr:PullRepositoryPersonal"
       ],
       "resource": [
          "qcs::tcr:::repo/team-01",
          "qcs::tcr:::repo/team-01/repo-demo",
          "qcs::tcr:::repo/team-01/repo-demo/*"
       ],
       "effect": "allow"
    }
 ]
}
```

个人版资源级 API 接口及授权方案变更指南

最近更新时间：2023-04-07 14:45:41

概述

容器镜像服务（TCR）同时向企业客户及个人用户提供容器镜像托管分发服务。其中，个人版为用户提供简单、免费的基础服务，即当前容器服务（TKE）内的镜像仓库。
为向用户提供接口定义更加规范，访问时延下降显著的 API 接口服务，原有个人版镜像仓库（CCR）的 API 接口已由 2.0 版本升级至最新的 3.0 版本，接口名称及授权方案也发生了相应变更。本文档介绍了支持资源级鉴权的 API 升级后新旧接口映射关系及如何使用最新的授权方案。

API 映射关系

API 2.0 名称	API 3.0 名称	接口描述	最新资源（Resource）描述方式
CreateCCRNamespace	CreateNamespacePersonal	创建个人版命名空间	qcs::tcr:$region:$account:repo/$namespace
DeleteUserNamespace	DeleteNamespacePersonal	删除个人版命名空间	qcs::tcr:$region:$account:repo/$namespace
GetUserRepositoryList	DescribeRepositoryOwnerPersonal	查询个人版所有仓库	qcs::tcr:$region:$account:repo/*
CreateRepository	CreateRepositoryPersonal	创建个人版镜像仓库	qcs::tcr:$region:$account:repo/$namespace/$repo
DeleteRepository	DeleteRepositoryPersonal	删除个人版镜像仓库	qcs::tcr:$region:$account:repo/$namespace/$repo
BatchDeleteRepository	BatchDeleteRepositoryPersonal	批量删除个人版镜像仓库	qcs::tcr:$region:$account:repo/$namespace/*
DeleteTag	DeleteImagePersonal	删除个人版仓库 tag	qcs::tcr:$region:$account:repo/$namespace/$repo
BatchDeleteTag	BatchDeleteImagePersonal	批量删除个人版仓库 tag	qcs::tcr:$region:$account:repo/$namespace/$repo
pull	PullRepositoryPersonal	拉取个人版镜像仓库内镜像	qcs::tcr:$region:$account:repo/$namespace/$repo
push	PushRepositoryPersonal	推送个人版镜像仓库内镜像	qcs::tcr:$region:$account:repo/$namespace/$repo

授权方案映射关系

由于产品名称及 API 接口版本的升级变更，TCR 个人版原有的资源（Resource）描述方式及动作（Action）发生了相应变更，请您在使用 API 3.0接口的同时，使用最新的资源及操作授权方案。
API 升级期间，访问管理相关接口将同时兼容新旧的资源（Resource）描述方式及动作（Action），以保障用户自定义策略仍然生效。为方便您统一管理 API 接口及授权方案，建议您统一将授权方案升级为最新版本，详情请参考 个人版授权方案示例 。

旧版资源级授权方案

- **动作（Action）**：以 `ccr` 作为产品前缀，API 接口名称为2.0版本。例如，创建命名空间为 `ccr:CreateCCRNamespace` 。
- **资源描述（Resource）**：以 `ccr` 作为产品名称，仅有 `repo` 资源类型。例如，描述命名空间 namespace-a 下的镜像仓库 repo-b，则为 `qcs::ccr:::repo/namespace-a/repo-b` 。其中，`$region` ，`$account` 若置空，则默认为全部地域，账号默认为创建策略的 CAM 用户所属的主账号。具体授权方案请参考：TKE 镜像仓库资源级权限设置 。

新版资源级授权方案

- **动作（Action）**：以 `tcr` 作为产品前缀，API 接口名称为3.0版本。例如，创建个人版命名空间为 `tcr:CreateNamespacePersonal` 。

- **资源描述（Resource）：以 `tcr` 作为产品名称，具有 `instance` 、 `repository` 和 `repo` 三种资源类型。其中， `repo` 为个人版专属的资源类型。例如，描述个人版命名空间 namespace-a 下的镜像仓库 repo-b，则为 `qcs::tcr:$region:$account:repo/namespace-a/repo-b` 。其中， `$region` ， `$account` 若置空，则默认为全部地域，账号默认为创建策略的 CAM 用户所属的主账号。**
  具体授权方案请参考：个人版接入 CAM 的 API 列表 及 个人版授权方案示例 。

新旧授权方案兼容示例

例如，授权子账号可读默认地域下 namespace-a 命名空间内的 repo-b 的镜像仓库，该镜像仓库为个人版。则仅能查询仓库信息、拉取该仓库内镜像，但无法删除仓库、修改仓库属性及推送镜像。

- **旧版授权方案：**

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "ccr:pull"
    ],
    "resource": "qcs::ccr:::repo/namespace-a/repo-b",
    "effect": "allow"
  }]
}
```

- **新版授权方案：**

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "tcr:PullRepositoryPersonal"
    ],
    "resource": "qcs::tcr:::repo/namespace-a/repo-b",
    "effect": "allow"
  }]
}
```

设置镜像清理

最近更新时间：2023-08-29 14:32:01

操作场景

本操作指南用于设置/更新个人版实例的镜像清理策略。

注意事项

个人版实例镜像清理策略仅适用于指定地域的实例，如广州和硅谷的个人版实例可配置不同的镜像清理策略。

操作步骤

1. 登录 容器镜像服务 控制台，选择左侧导航栏中的**实例管理**。
2. 在**实例管理**页面即可查看当前账号下的实例列表。选择任意地域的个人版实例。

3. 单击**更多 > 设置镜像清理**，如下图所示：

   - **启用状态**：勾选“启用全局镜像生命周期管理”。
   - **全局规则**：
     - **保留最新镜像版本**：请按需设置，所设置数值不能大于当前主账号下镜像版本默认配额数。
     - **保留最近天数内镜像版本**：请按需设置。
4. 单击**确定**即可配置成功。

销毁退还实例

最近更新时间：2023-12-04 10:49:01

操作场景

本文档介绍如何在腾讯云容器镜像服务 TCR 中销毁、退还企业版实例。

前提条件

已成功 购买企业版实例，且当前操作账号具有该实例的删除权限。

> **注意：**
> 销毁退还实例是高危动作，为防止实例误删，请您确保在删除实例之前先删除实例下的所有命名空间和仓库，否则实例无法成功删除。

操作步骤

使用控制台销毁退还

1. 登录 容器镜像服务控制台 。
2. 单击左侧导航栏中的**实例管理**，在**实例管理**页面选择需要销毁/退还的实例右侧的**更多 > 销毁/退还**。
3. 在弹出的确认窗口中，按需勾选“随实例删除关联的 COS 存储桶”。如下图所示：

> **注意**
> - 请仔细阅读销毁/退还实例的相关提示。实例删除将彻底清理实例使用过程中存储的用户数据及相关配置，且不可恢复，请谨慎操作。
> - 如果确认不再需要使用容器镜像服务企业版过程中存储的容器镜像、Helm Chart 等底层数据，请勾选随实例删除后端存储 COS Bucket，避免产生不必要费用。
> - 如果当前账户已处于欠费状态，对象存储服务不允许直接删除关联 COS Bucket，请不要勾选该选项，正常删除实例后前往 对象存储 控制台管理该 COS Bucket。
> - 实例销毁后，按量计费实例将不再继续产生费用，包年包月实例将根据您购买时支付的现金及赠送金按使用时长比例退还至您的腾讯云账户，详情请参见 退费说明 。

4. 勾选“已阅读并同意退费规则”后单击**确定**即可删除当前所选实例，该实例将不再产生费用。

> **说明：**

> 若实例删除花费时间过长，或显示状态为异常，您可 在线咨询 联系我们。

使用 API 销毁退还

您还可以使用 DeleteInstance 接口删除实例。详细信息请参见 删除实例 API 文档 。