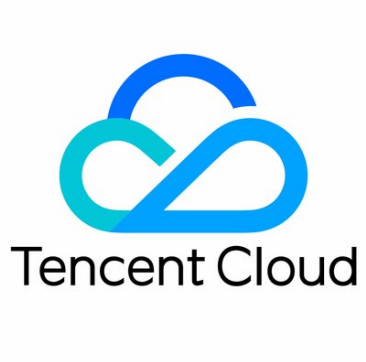
Tencent Container Registry
Best Practice



Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Best Practice
TCR Personal migration
Migration from TCR Individual to TCR Enterprise

Last updated: 2023-09-13 14:55:38

Scenario

Tencent Container Registry (TCR) currently offers both Individual and Enterprise Editions. The Individual Edition is designed for individual developers and provides only basic features for container image storage and distribution. The Enterprise Edition is tailored for enterprise users, offering secure, dedicated, and high-performance cloud-native artifacts hosting and distribution services. For the differences between the two editions, see Specification.
This document describes how enterprise customers can migrate container image data and business configuration from the Personal Edition to the Enterprise Edition to achieve smooth business migration.

Preparations

To migrate from the Personal Edition service to the Enterprise Edition, you need to confirm and complete the following preparations:

- You have activated and used the Personal Edition service, and the migration operation account has the permission to pull all images from the Personal Edition image repository. Please refer to Personal Edition Authorization Scheme Example to grant full management permissions for the Personal Edition to the sub-account in advance.
- You have purchased an Enterprise Edition instance, and the account used for migration has the permission to push images to the instance. Please refer to Enterprise Edition Authorization Solution Example to grant the sub-account the necessary permissions for container images and Helm Chart push in advance. It is recommended to grant full read and write permissions for the container image service to the sub-account used for configuration synchronization.
- A suitable environment for running the migration tool has been set up. It is recommended to perform the migration task within a Virtual Private Cloud (VPC) to improve migration speed and avoid public network traffic costs.
  - Run the migration tool within the VPC: Add the private network where the migration tool server is located to the private network access of the target Enterprise Edition instance. For more information, see Private Network Access Control.
  - Run the migration tool in a public network environment: Enable the public network access entry for the target Enterprise Edition instance and allow access from the source. For more information, see Public Network Access Control.

Data Migration

Preparing the basic running environment

1. Purchase an Enterprise Edition instance in the region where the container business is deployed.
2. Prepare a Cloud Virtual Machine (CVM) in the same region for image migration, and preferably choose a model with high CPU/memory configuration and high internal network bandwidth. After the CVM starts, install the latest Docker client or choose an operating system with Docker pre-installed.
3. Connect the VPC where the CVM is located to the Enterprise Edition instance and enable automatic private network resolution. For more information, see Private Network Access Control.
4. Obtain the access credential for the instance and execute `Docker Login` on the dedicated migration CVM. Ensure that the instance can be accessed and logged in successfully via the internal network on this CVM.

Preparing migration configuration

1. Obtain the access credential of the image repository.
   - Personal Edition image repository access credentials: The username is the Tencent Cloud UIN of the account to which the image to be migrated belongs, and the password is the one set when initializing the Personal Edition service. If you have forgotten the password, you can go to TCR Console > **Instance List**, select the Personal Edition instance, and click **Reset Login Password** in the More menu to reset the password.
   - Enterprise Edition image repository access credential: Go to the TCR console > **Access credential**, select the created

Enterprise Edition instance, click **New** to generate a long-term access credential for migration, which includes the username and password. Please note that the user generating this access credential must have full read and write permissions for the instance.

2. Obtain API credentials
   During the image migration process, namespaces and image repositories will be automatically created within the Enterprise Edition instance, requiring Tencent Cloud API calls to complete the operation. You can go to ** Access Management Console ** > **Access Keys** > **API Key Management** to create a new key or view existing keys. Please handle this key information with care.

Downloading and running the migration tool

Run the following command to download the dedicated container image for migration:

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

Run the following command to view the instructions of the tool:

```
docker run --network=host --rm ccr.ccs.tencentyun.com/tcrimages/image-transfer:ccr2tcr /run --help
```

Run the following command to modify the configuration and execute the migration task:

```
docker run --network=host --rm ccr.ccs.tencentyun.com/tcrimages/image-transfer:ccr2tcr /run --tcrName image-transfer --ccrRegionName ap-guangzhou --tcrRegionName ap-shanghai --ccrAuth username:password --tcrAuth username:password --ccrSecretId sid- example --ccrSecretKey skey-example --tcrSecretId sid-example --tcrSecretKey skey-example --tagNum 50
```

Description

Category	Description
tcrName	Name of the target Enterprise Edition instance
ccrRegionName, ccrRegionName	Region of the instance. In the Chinese mainland, the CCR instance region defaults to ap-guangzhou, and the TCR instance region must be set to the actual region such as ap-shanghai.
ccrAuth, tcrAuth	Access credential of the image repository in the format of username:password. If the username and password contain special characters, the special characters need to be escaped. For example, "?" should be written as "\?".
ccrSecretId, ccrSecretKey, tcrSecretId, tcrSecretKey	Tencent Cloud API calling key. If the migration is under the same account, the calling keys of CCR and TCR are the same.
tagNum	Specifies that only the latest N tags of images in the image repository will be migrated.

Viewing and confirming the running result

Since the migration from Personal Edition to Enterprise Edition uses the full migration mode by default, the migration time is directly related to the number and size of the image repositories in the Personal Edition. Please be patient.

If the following code is displayed after running, it indicates that the full migration was successful. Otherwise, please rerun the migration tool to retry. You can request assistance through Online Consultation.

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

Business Migration

Switching the network environment

The Personal Edition of Tencent Container Registry (TCR) does not have network access control features, and servers within the domestic region can access the service by default through the private network. The Enterprise Edition of TCR supports network access control, requiring the VPC where the cluster is located to be connected to the instance, allowing private network access.

- Network configuration of the Personal Edition instance: no configuration is required. By default, you can access the instance and upload/download images via all network environments.
- Network configuration of the Enterprise Edition instance:
  - Private Network Access (Recommended): Actively connect the VPC where the cluster or elastic cluster is located to the target instance, and enable automatic parsing within the VPC or manage DNS parsing yourself. For more information, see Private Network Access Control.
  - Public network access: we recommend that you enable the public network access only when testing or distributing images for the external teams, and the access allowlist must be configured.

Reusing the TCR Individual image configuration

Refer to the sub-document: **Accessing Enterprise Edition Instances with Personal Edition Domain Names**. By using this feature, you won't need to change the existing image repository addresses and access credential configurations in TKE clusters and CI/CD platforms, making it convenient for customers to switch to the Enterprise Edition service with minimal cost.
For long-term use, it is recommended to gradually switch the TCR Individual access configuration to the TCR Enterprise configuration to avoid access exceptions caused by subsequent changes in the TCR Individual service.

Using TCR Enterprise image configuration

Switching the access address

Navigate to the details page of the cluster or elastic cluster, select "Workload" on the left, and choose to create/update a workload. In "Instance Container", select or enter the image address, or directly modify the **image** parameter in the YAML file.

- Personal Edition address: The default is `ccr.ccs.tencentyun.com/namespace/repo:tag`. The default service region covers all available domestic regions except Hong Kong, China, such as Beijing, Shanghai, Guangzhou, etc. The prefix domain name for Hong Kong, China is hkccr. Multi-level paths are not supported.
- Enterprise Edition address: You can customize the instance name `user-define`, for example, `user-define.tencentcloudcr.com/namespace/repo:tag`. Custom domain names are supported, such as `xxx-company.com/namespace/repo:tag`. Multi-level paths are supported, and the image address can be `xxx-company.com/ns/sub01/sub02/repo:tag`.

Switching the access credential

Navigate to the cluster or elastic cluster details page, select "Workloads" on the left, and choose to create/update a workload. In "Image Access Credential", switch the access credential or directly modify the **imagePullSecret** parameter in the YAML file.

- Personal Edition Access Credential: When creating a new namespace, the Personal Edition access credential, **qcloudregistrykey**, will be issued by default. Select this credential to proceed.
- Access credential of Enterprise Edition instance:
  - Recommended Solution: Use the TCR Enterprise Edition dedicated plugin to automatically distribute and configure access credentials, enabling secret-free image pulling. This solution does not require configuring image access credentials; please delete any existing values for this parameter and keep it empty. (Supported only in TKE)
  - Manual configuration: you can configure a long-term access credential in the TCR Enterprise Edition instance, and deliver it to the namespace, or create the image access credential when creating the workload.

Best Practices for TCR Enterprise Instance

This document provides some best practices for migration from the Personal Edition to the Enterprise Edition.

Multi-instance planning

Based on your actual business needs, you can create one or more instances in multiple regions, configure synchronization and replication policies, and use custom domain names to manage instance access addresses uniformly. For more information, refer

to TCR Enterprise Edition Instance Synchronization, TCR Enterprise Edition Instance Replication, and Synchronizing Images from Self-built Harbor to TCR Enterprise Edition.

Security and Compliance

- Operation compliance
  - It is recommended to grant the minimum permissions to sub-accounts using the Enterprise Edition. Repository-level permission configuration is supported, allowing specific sub-accounts to pull/manage designated image repositories or even finer-grained API call permissions. For more information, see Example of Authorization Solution of TCR Enterprise.
  - You can create dedicated long-term access credentials for different usage scenarios. All long-term access credentials created by an account are only used for accessing the instance.
  - For temporary access to instances, it is recommended to use a temporary access credential (valid for 1 hour). For more information, see Obtaining a Temporary Login Token.
- Network Security
  - Please do not enable the public network access entry to prevent the external unauthorized objects from accessing the instance, or avoid incurring public network access fees for downloading the images of your business via the public network.
  - You can bind a custom domain name to the instance, and manage the public network and VPC resolution of the domain name.

Image Management

- Repository planning
  - We recommend that you use the namespace to isolate the services, teams, etc., to facilitate permission management and synchronization rule configuration.
  - Multi-level paths are supported. You can create multi-level repositories as needed to avoid creating too many namespaces.
  - You can push images to automatically create the repositories, and configure the default attributes such as public/private at the namespace level.
  - **Please note**: Namespaces, image repositories, and other elements are path markers, and there is no isolation in the backend data storage.
- Tag naming
  - Please do not use latest to update the image tag in a production environment, which may affect service updates and rollbacks.
  - We recommend that you use the CI tool for the automatic naming of images to facilitate subsequent tag management and image synchronization.
  - **Please note**: When deleting a specified image version, images with the same digest will be deleted simultaneously.

CI/CD

- The CI/CD service comes with the Enterprise Edition.
  - The Enterprise Edition CI/CD capabilities are entirely based on Tencent Cloud CODING DevOps product. You need to activate this product and complete the basic configuration. For more information, see CODING DevOps.
  - Image building is supported. The optional code sources include GitHub, GitLab, TGit, Gitee, and CODING.
  - Delivery pipeline is supported, which enables you to automatically deploy images in clusters, elastic clusters, and edge clusters.
- External services can be connected.
  - You can use the trigger (webhook) feature to integrate with existing CI/CD systems. Pushing an image will automatically trigger a webhook notification, with the message body containing the image's basic information. For more details, see Managing Triggers.
  - You can directly use the complete service of CODING DevOps, which has built-in TCR templates.

Using Individual Edition Domain Name to Access Enterprise Edition Instance

Last updated: 2023-09-13 14:53:18

Scenario

Customers who have been using the shared Individual Edition service in a stable production environment and wish to upgrade to an exclusive Enterprise Edition instance need to import existing image data from the Individual Edition into the Enterprise Edition instance. Additionally, they must change the image address configuration in their existing build and deployment systems to access the Enterprise Edition instance. In real-world production scenarios, image addresses are used in multiple aspects, such as build platforms, deployment platforms, and Kubernetes cluster application YAML definitions, making the cost of unified modification relatively high.
In light of the above scenarios and issues, the Enterprise Edition introduces the Individual Edition domain name compatibility feature. This feature allows customers to push and pull Enterprise Edition instance images using the existing Individual Edition image address and access credentials, and supports intelligent origin-pull. If there is no corresponding image in the Enterprise Edition, the system automatically origin-pull requests the corresponding image in the Individual Edition. This minimizes the burden of image repository migration on customer Ops and R&D, accelerating customer migration to the more stable, powerful, high-performance Enterprise Edition as soon as possible.

Preparations

- An Enterprise Edition instance has been created. For detailed instructions, please refer to Creating an Enterprise Edition Instance.
- You have migrated data in the Individual Edition instance to the Enterprise Edition instance. For operation details, see Importing Individual Edition Instance Image to the Enterprise Edition Instance.
- Currently, only allowlist users can access Enterprise Edition instances using Individual Edition domain names. You need to submit a ticket to apply for this feature.

Basics

The domain names supported by Individual Edition and Enterprise Edition instances are as follows:

- Domain names supported by Individual Edition instances

  Do not distinguish between public and private domain names. VPC access uses the private linkage by default.
  - For main service regions (Guangzhou, Shanghai, Nanjing, Beijing, Chengdu, Chongqing): ccr.ccs.tencentyun.com
  - For other regions: independent service and domain names, for example, hkccr.ccs.tencentyun.com for Hong Kong (China)
- Domain Names Supported by Enterprise Edition Instances

  Distinguish between public and private domain names, and support custom domain names.
  - Default domain name: {Enterprise Edition instance name}.tencentcloudcr.com。
  - Dedicated private domain name: {Enterprise Edition instance name}-vpc.tencentcloudcr.com。
  - Custom domain name: Supports registering custom domains.

Take migrating the `nginx:latest` image in the `team-a` namespace of the Individual Edition service of the Guangzhou region to the Enterprise Edition instance `company-a` as an example:

- Individual Edition access address: ccr.ccs.tencentyun.com/team-a/nginx:latest
- Enterprise Edition access address: company-a.tencentcloudcr.com/team-a/nginx:latest

How It Works

When an Enterprise Edition instance is created, the system will issue a certificate that supports Individual Edition domain names by default and supports handling Individual Edition authentication requests.
Customers only need to configure the Individual Edition domain name to resolve to the Enterprise Edition's private network access entry within the private network environment (refer to: Configuring Private Network Access Control). This allows automatic access to the Enterprise Edition service when accessing the Individual Edition image repository address within the private network, using the Individual Edition service's username and password for authentication and authorization. Customers

can choose to use the Private DNS product or manage cluster node Host configurations themselves to implement domain name resolution.
When you no longer need to use your Individual Edition domain name to access your Enterprise Edition instance, simply cancel the forced parsing in your VPC and you can access your Individual Edition service.

Usage Limits

1. Within one region, the Individual Edition domain name compatibility feature can be enabled for only one Enterprise Edition instance.
2. If you are using a public environment, you need to manually configure parsing the domain name to the Enterprise Edition instance access entry.
3. When using the domain name of the Individual Edition to access the service of the Enterprise Edition, the image repository in the corresponding namespace of the Enterprise Edition will be requested first. Therefore, please avoid using special namespace names such as **library**, **tke**, and **public** in the Enterprise Edition instance; otherwise, the TKE cluster will not be able to access the official image of the product, causing basic service exceptions.

Operations Guide

Verify the Basic Environment

1. Individual Edition service has been activated and is in use.
2. You have purchased the Enterprise Edition service and synchronized some images from the Individual Edition service to the Enterprise Edition instance.
3. There is a TKE cluster (including the TKE Serverless cluster), and the VPC where the cluster resides has been connected to the Enterprise Edition instance. For more information, see Configuring Private Network Access Control.
4. It has been verified that the Individual Edition and Enterprise Edition images can be pulled normally over the internal network in the TKE cluster.

Configuring Private DNS

1. Go to the Private DNS console.
2. Create a private domain.
   2.1 Domain name: tencentyun.com
   2.2 Associated VPC: Select a VPC connected to the Enterprise Edition.
   2.3 Subdomain Recursive Parsing: Keep it enabled.
   2.4 Retain the default values of other parameters.
3. Configuring Private DNS
   3.1 Click the created private domain to go to its details page.
   3.2 Add a record in **DNS Records** with the following configuration:
      - Host record: For the main service region, configure as **ccr.ccs**. For other regions, please enter the corresponding domain name prefix, such as hkccr.ccs.
      - Record type: Select **CNAME**.
      - Record value: Domain name of the Enterprise Edition instance. Use the default or custom domain name. Check that auto parsing has been configured for the default or custom domain name in the product console.
      - Retain the default values of other settings.
   3.3 Retain the default values of other parameters.

Verify Access Effectiveness

Once the preceding configuration is completed, you can verify the effect by using the Individual Edition domain name to access the Enterprise Edition instance.

Scenario 1: Using the Individual Edition domain name to pull an image that has been migrated to the Enterprise Edition instance

1. Use a synchronization tool or manually push an image to the Enterprise Edition instance. Take the following image as an

example: `company-a.tencentcloudcr.com/team-a/nginx:latest`, whose corresponding Individual Edition image repository address is `ccr.ccs.tencentyun.com/team-a/nginx:latest`.

2. Log in to the cluster node and manually pull the image, or create new workload to execute image pull. Note that:
   - The image address remains `ccr.ccs.tencentyun.com/team-a/nginx:latest`.
   - The access credentials remain the configured Individual Edition access credentials.
3. Verify that the cluster can pull the image successfully.

Scenario 2: Using the Individual Edition domain name to pull an image that has not been migrated to the Enterprise Edition instance

1. The Individual Edition already contains the image `ccr.ccs.tencentyun.com/team-b/apache:latest`, and the image has not been synchronized to the Enterprise Edition.
2. Log in to the cluster node and manually pull the image, or create new workload to execute image pull. Note that:
   - The image address remains `ccr.ccs.tencentyun.com/team-b/apache:latest`.
   - The access credentials remain the configured Individual Edition access credentials.
3. Verify that the cluster can pull the image successfully.

Scenario 3: Using the Individual Edition domain name to push an image to the Enterprise Edition instance

1. Use the Docker CLI or CI platform to push the image and use the Individual Edition address `ccr.ccs.tencentyun.com/team-a/nginx:latest`.
2. If the Enterprise Edition instance already contains a `team-a` namespace, the push will be successful; otherwise, a push failure will be reported.

Usage Recommendations

Scenarios

The domain name compatibility feature is recommended for the following scenarios:

- Individual Edition images are widely used in environment building, project code, and application deployment, and switching to the Enterprise Edition independent domain name is costly.
- The image building and distribution environment is fixed and the cost of one-time configuration of domain name parsing is low.

If the image distribution scenario is complex and it is necessary to support third-party users to access Enterprise Edition images in complex network scenarios, it is not recommended to use the Individual Edition domain name compatibility feature to avoid disrupting the deployment of the production environment.

Canary Switching

When initially using the Individual Edition domain name to access the images in the Enterprise Edition instance, it is recommended to push the images to both the Individual Edition and Enterprise Edition so that the cluster can still temporarily switch to access the Individual Edition service when a parsing configuration exception occurs. Later, you can gradually adjust the existing Individual Edition image address configuration to the Enterprise Edition address and eventually stop using the domain name compatibility feature.

TKE Clusters Use the TCR Addon to Enable Secret-free Pulling of Container Images via Private Network

Last updated: 2023-09-13 14:47:15

Scenario

This document explains how to use the TCR add-on in Tencent Kubernetes Engine (TKE) to enable secret-free pulling of container images from an Enterprise Edition instance through the private network and create workloads.

Preparations

Before using a private image hosted in TCR Enterprise Edition to deploy applications in TKE, complete the following operations:

- You have purchased an Enterprise Edition instance.
- You have created a TKE cluster.
- If you are using a sub-account, you must have granted the sub-account operation permissions for the corresponding instance. For more information, see Example of Authorization Solution of TCR Enterprise.
- If you are using an existing TKE cluster, ensure that the sub-account has the necessary cluster permissions. Refer to TKE Cluster Permission Management.

Instructions

Preparing a container image

Step 1: Creating a namespace

A new TCR Enterprise Edition instance does not have a default namespace, and a namespace cannot be automatically created through the pushed image. Therefore, you must manually create a namespace as needed. For more information, see Managing Namespaces.
We recommend that you name the namespace based on the project or team name. In this document, `docker` is used as an example. The following page appears after the namespace is created.

Step 2: (Optional) Creating an image repository

Container images are hosted in specific image repositories. You can create an image repository as needed. For more information, see Creating an image repository. Set the image repository name to the name of the container image to be deployed. In this document, `getting-started` is used as an example. The following page appears after the image repository is created.

> **Note**
> Use Docker CLI or another image tool, such as jenkins, to push the image to the TCR Enterprise Edition instance. If no image repository exists, an image repository will be automatically created. You do not need to create one in advance.

Step 3: Pushing container images

You can use Docker CLI or other image building tools (such as Jenkins) to push images to the specified image repository. This document uses Docker CLI as an example. In this step, you need to use a CVM or CPM instance with Docker installed and ensure that the target client is in the public or private network access allowlist defined in Configuring the Network Access Policy.

1. Refer to Obtaining Instance Access Credentials to get the login command and perform Docker Login.
2. After logging in, you can create a container image on the local server or obtain a public image from Docker Hub for testing. This document uses the official and latest Nginx image on Docker Hub as an example. In the command line tool, run the following commands sequentially to push this image. Replace demo-tcr, docker, and getting-started with the actual instance, namespace, and image repository names you have created.

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

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

After the image is pushed, you can go to the "Image Repository" page in the console, select the repository name, and view its details.

Configuring a TKE cluster to access a TCR Enterprise Edition instance

TCR Enterprise Edition instances support network access control and deny all external access requests by default. You can select public network or private network access for a TKE cluster to access a specific instance and pull the container image based on the network configuration of the TKE cluster. If the TKE cluster and TCR instance are deployed in the same region, we recommend that the TKE cluster pulls the container image through the private network to accelerate pulling and reduce public network traffic costs.

Step 1: Associating the VPC where the cluster is located to the TCR instance

For your data security, the new TCR instance denies all external access requests by default. To allow the specified TKE cluster to access the TCR instance to pull the image, you must associate the VPC where the cluster resides to the TCR instance, and configure the corresponding private network domain parsing service.

1. Create a private network access linkage
2. Managing private network parsing

Step 2: Installing the TCR add-on in the TKE cluster

If you are currently using the Tencent Kubernetes Engine (TKE), refer to the TCR guide to install the TCR add-on in the TKE cluster and select "Enable Private Network Parsing" in the "TCR Component Parameter Setting" window. This add-on can automatically configure private network resolution for nodes in the cluster associated with the TCR instance, enabling secret-free pulling of images within the instance via the private network.
Once the add-on is installed, the cluster will have the capability to pull images from the associated instance through the private network without a password, without any additional configuration.

> **Note**
> The current TCR add-on supports only Kubernetes clusters with versions 1.14, 1.16, 1.18, 1.20, and 1.22. If your cluster version is not supported, please use the manual configuration method.

Using the container image in the TCR instance to create a workload

1. Log in to the TKE console and click Cluster in the left sidebar.
2. Select the cluster ID that you want to create the workload to go to the cluster details page.
3. On the cluster details page, choose **Workload** > **Deployment** in the left sidebar.
4. Navigate to the "Deployment" page and click **Create**.
5. On the “Create Workload” page, create a workload. The main parameters are as follows:
   - **Namespace**: Select a namespace based on your requirements. Ensure that the namespace configured to support secret-free pulling during the TCR add-on installation includes the required namespace.
   - **Containers in the Pod**:
     - **Image**: Click **Select Image**, and in the pop-up window, choose Tencent Container Registry - Enterprise Edition. Then, select the region, instance, and image repository as needed.
     - **Image Version**: After selecting the image, click **Select Image Version**. In the pop-up "Select Image Version" window, choose a version of the image repository as needed. If no selection is made, the default is set to 'latest'.
   - **Image Access Credential**: If the TCR add-on is already installed in the cluster, explicit configuration is not required. **Avoid selecting other access credentials, as doing so will prevent this workload from loading the secret-free pulling configuration provided by the TCR add-on.**
6. After configuring the other parameters, click **Create Workload** to view the deployment progress of the workload.
   Upon successful deployment, you can see the "Running/Desired Pod Count" for the workload as "1/1" on the "Deployment" page.

TKE Serverless Clusters Pull TCR Container Images

Last updated: 2023-09-13 14:42:25

Scenario

This document describes how to pull container images in a Tencent Container Registry (TCR) Enterprise Edition instance in a Tencent Kubernetes Engine (TKE) Serverless cluster and to create workloads.

Preparations

Before using a private image hosted in TCR Enterprise Edition to deploy applications in TKE, complete the following operations:

- You have purchased an Enterprise Edition instance.
- You have created a TKE Serverless cluster.
- If you are using a sub-account, the sub-account must have obtained operation permissions on the corresponding instance. For more information, see TCR Enterprise Authorization Management.

Instructions

Preparing a container image

Step 1: Creating a namespace

A new TCR Enterprise Edition instance does not have a default namespace, and a namespace cannot be automatically created through the pushed image. Therefore, you must manually create a namespace as needed. For more information, see Managing Namespaces.
We recommend that you name the namespace based on the project or team name. In this document, `docker` is used as an example.

Step 2: (Optional) Creating an image repository

Container images are hosted in specific image repositories. You can create an image repository as needed. For more information, see Creating an image repository. Set the image repository name to the name of the container image to be deployed. In this document, `getting-started` is used as an example.

> **Note**
> When using `docker cli` or other image tools, such as Jenkins, to push images to an Enterprise Edition instance, the image repository will be automatically created if it does not exist, eliminating the need for manual creation in advance.

Step 3: Pushing container images

1. You can use `docker cli` or other image building tools (such as Jenkins) to push images to the specified image repository. This document uses `docker cli` as an example. In this step, you need to use a CVM or CPM instance with Docker installed and ensure that the target client is in the public or private network access allowlist defined in Configuring the Network Access Policy.
2. Refer to Obtaining Instance Access Credentials to get the login command and perform Docker Login.
3. After logging in, you can create a container image on the local server or obtain a public image from Docker Hub for testing. This document uses the official and latest Nginx image on Docker Hub as an example. In the command line tool, run the following commands sequentially to push this image. Replace demo-tcr, docker, and getting-started with the actual instance, namespace, and image repository names you have created.

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

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

4. After the image is pushed, you can go to the Image Repository page in the TCR console and click the name of a repository to view its details.

Configuring a TKE Serverless cluster to access a TCR instance

For your data security, TCR and TKE Serverless deny all public and private access requests by default. Therefore, you must configure the network access policies before deploying the TCR image to TKE Serverless.
TCR Enterprise Edition instances support network access control. You can select public network or private network access for a TKE Serverless cluster to access a specific instance and pull the container image based on the network configuration of the TKE Serverless cluster. If the TKE Serverless cluster and TCR instance are deployed in the same region, we recommend that the TKE Serverless cluster pulls the container image through the private network to accelerate pulling and reduce public network traffic costs.
This document describes how to access a TCR instance through the private network. For more information about how to access a TCR instance through the public network, see Accessing Internet through NAT Gateway.

Step 1: Associating the VPC where the cluster is located to the TCR instance

For your data security, the new TCR instance denies all external access requests by default. To allow the specified TKE Serverless cluster to access the TCR instance to pull the image, you must associate the VPC where the cluster resides to the TCR instance, and configure the corresponding private network domain parsing service.

1. Create a private network access linkage
2. Managing private network parsing

Step 2: Obtaining a TCR instance access credential

Before pulling container images from a TCR instance, you need to log in to the instance with the credential. For more information, see Obtaining an Instance Access Credential. Keep the long-term access credential of this instance for later configuration and deployment of TCR images.

Using the container image in the TCR instance to create a workload

1. Log in to the TKE console.
2. In the **Cluster List**, click the ID of the target Serverless cluster to enter the cluster details page.
3. On the **Cluster Details** page, select **Workloads** > **Deployment** on the left side.
4. On the **Deployment** page, click **Create**.
5. On the **New Deployment** page, specify the following parameters to create a workload:
   - **Namespace**: Select a namespace in the cluster as needed.
   - **Containers in the Pod**:
     - **Image**: Click **Select Image**, select **Tencent Container Registry – Enterprise** in the pop-up window, and choose the region, instance, and image repository based on your requirements.
   - **Image Version**: After selecting the image, click **Select Image Version**. In the pop-up "Select Image Version" window, select a version of the image repository as needed. If not selected, the default is set to latest.
   - **Image Access Credential**: Click **Add Image Access Credential**, and select **Use New Access Credential** from the drop-down list.

     Click **Configure Access Credential Information**, and enter the repository domain name, username, and password for the image in the pop-up window.
   - **Repository Domain Name**: Log in to the TCR console and click **Image Repository** in the left sidebar to get the repository address of the required image.
   - **Username**: Go to Account Info to get the account ID. The account ID is your username.
   - **Password**: The access credential obtained in Step 2 is the password.
   - **Access Settings (Service)**: Users can deploy various containers in Kubernetes, some of which provide Layer 7 network services through HTTP and HTTPS protocols, while others provide Layer 4 network services through TCP and UDP protocols. Kubernetes-defined Service resources can be used to manage Layer 4 network service access within the cluster. Refer to the following key parameter information to complete the access settings.
     - **Service**: Select **Enable**.

- **Service Access**: Select **Via VPC**.

6. Click **Create Deployment** and view the deployment progress.
   After the workload is deployed, "Number of Running/Desired Pods" for the workload becomes "1/1" on the **Deployment** page.

Image Data Synchronization and Replication Between Multiple Platforms in Hybrid Cloud

Last updated: 2023-09-13 16:18:33

Scenario

During the development and operation process, users may encounter scenarios where multiple container image repositories are needed simultaneously, which may span across main accounts, regions, countries, and platforms. Users can manually complete the push and distribution tasks between instances, but this may result in higher operational costs, untimely synchronization, and difficulties in management.
To address this scenario, TCR currently offers synchronization and replication features, as well as open-source image migration tools. These include:

- The instance synchronization feature allows users to configure image synchronization based on rules for **on-demand synchronization**. For more information, please refer to Configuring Instance Synchronization.
- The instance replication feature enables users to **fully replicate** instance image data from the primary instance to the secondary instance. For more information, please refer to Configuring Instance Replication.
- The image migration tool supports Docker image data migration for **various image repositories**. For more information, please refer to Image Migration Tool: image-transfer.
- Additionally, when migrating from other image repository services to TCR, users can configure custom domain names for TCR instances to continue using the original domain names, ensuring service continuity. For more information, please refer to Configuring Custom Domain Names.

This document describes how to sync and replicate image data between different image registries in a hybrid cloud.

Preparations

Make sure that the following conditions are met before creating and managing the replica instances of a TCR Enterprise Edition instance:

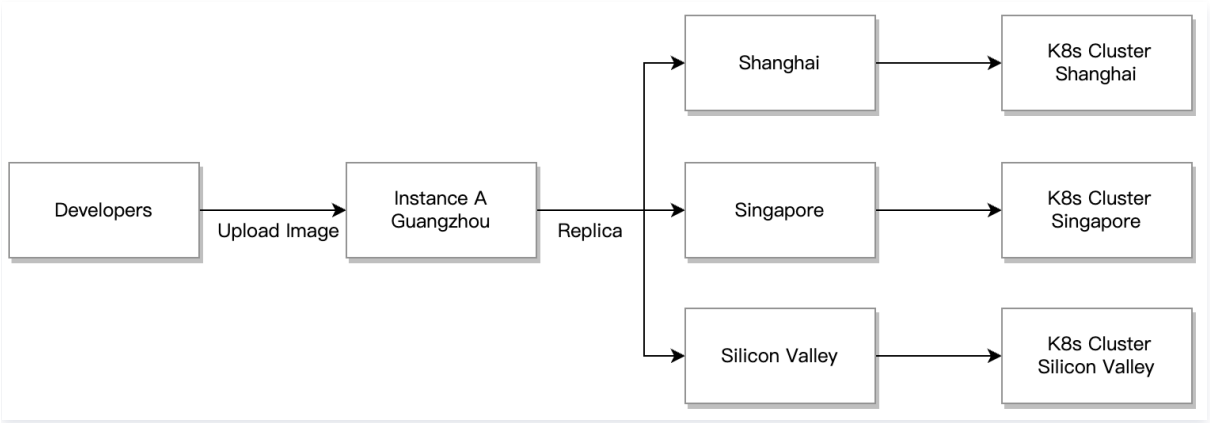
- You have successfully purchased an Enterprise Edition instance. The instance synchronization feature requires a Standard or Premium instance, while the instance replication feature requires a Premium instance.
- If you are using a sub-account, the sub-account must have obtained operation permissions on the corresponding instance. For more information, see TCR Enterprise Authorization Management.

Instructions

Scenario 1: cross-region TCR instance replication

Cross-region instance replication

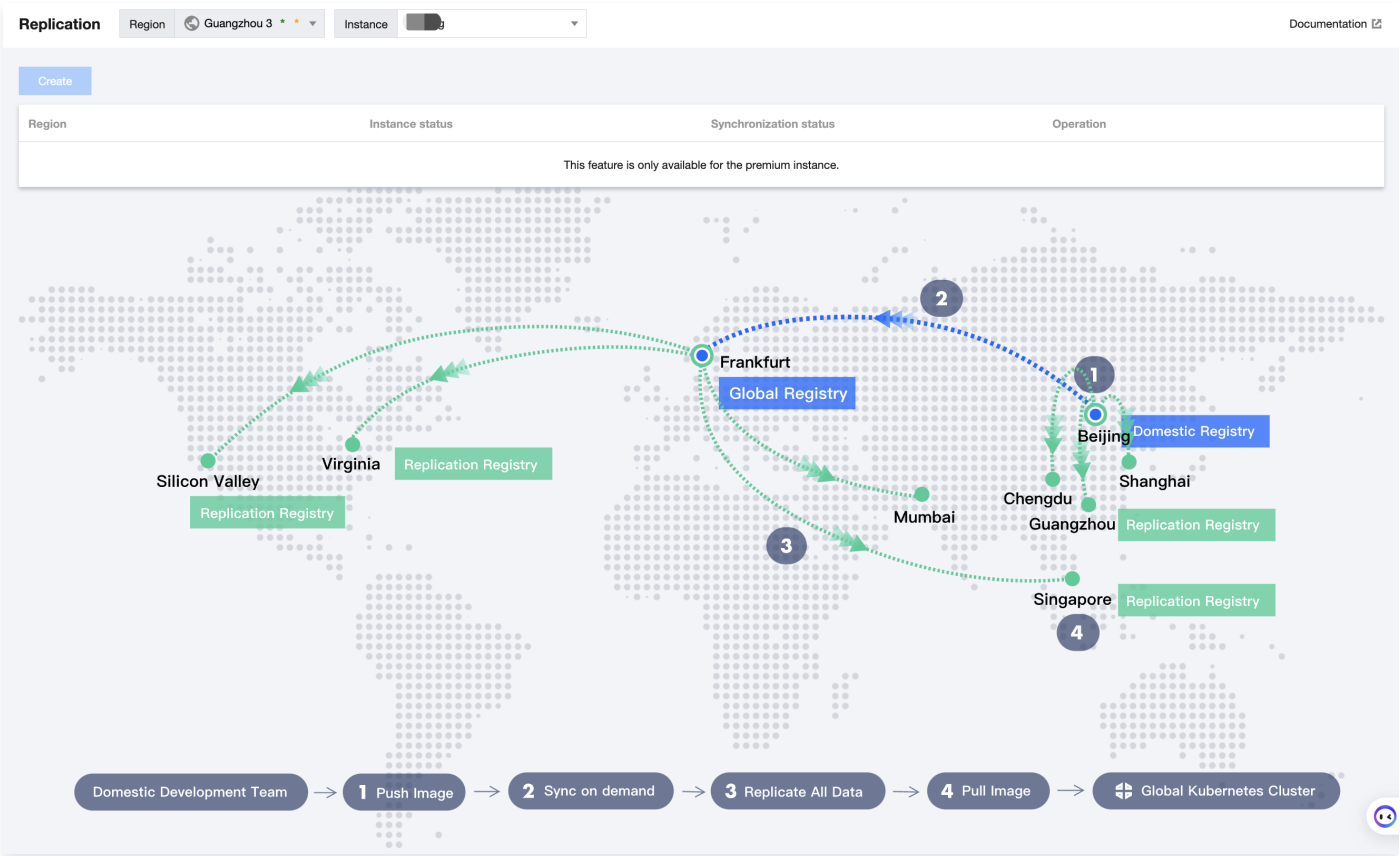
When users have cross-regional business requirements, they can utilize the instance replication feature to achieve single-region upload, real-time high-speed synchronization across multiple regions, and local private network retrieval. Compared to the instance synchronization feature, this functionality unifies the deployment configurations of multi-regional clusters and improves the cross-regional synchronization speed of cloud-native application artifacts.



Cross-border cross-region instance synchronization and replication

However, when cross-region business involves cross-border scenarios, users need to combine the use of the Instance Synchronization feature. Due to security and compliance considerations, cross-border instance replication is currently not supported.

1. After purchasing a TCR Advanced Edition instance in both domestic and international regions, users should first create synchronization rules to achieve on-demand data synchronization across countries.
2. Create and manage replica instances separately in two instances by creating and managing replica instances, achieving single-point upload, real-time replication across multiple regions, and nearby private network retrieval for both domestic and international locations.



> **Note**
> To achieve optimal private network access, users need to manually connect the VPC in the replication region to the instance. For more information, please refer to Private Network Access Control and select the VPC within the replication region.

Scenario 2: cross-platform image migration or synchronization

When users simultaneously use public cloud image repositories and self-built image repositories, or multiple public cloud image repositories, there is often a need for cross-platform image migration or synchronization. In cross-platform scenarios, users can choose to use TCR's custom domain name feature to achieve unified access across multiple platforms with a single configuration, ensuring service continuity. For more information, please refer to Configuring Custom Domain Names.

Cross-platform image migration

Image-transfer is an open-source tool developed by Tencent Cloud for image migration, supporting batch migration between Docker images in various image repositories. It only requires the repository to be based on Docker Registry V2 built Docker image repository services (such as Tencent Cloud TCR Personal Edition (CCR)/TCR Enterprise Edition, Docker Hub, Quay, Alibaba Cloud Image Service ACR, Harbor, etc.). The tool has two usage modes: general mode and one-click migration mode for Tencent Cloud.

General Mode
Using the general mode of image-transfer, users can achieve image migration from multiple image repositories to multiple image repositories. Users only need to configure the authentication and authorization files and migration rule files to start the migration. For information on downloading, installing, and using the tool, please refer to image-transfer.

Quick Migration Mode
To migrate from TCR Individual Edition to TCR Enterprise Edition, you can use the one-click migration mode provided by image-transfer. For more information, please refer to Migration from TCR Individual to TCR Enterprise. The guide includes two main parts: one-click data migration using the open-source tool image-transfer and business migration in the TCR console, helping you achieve a smooth migration of your business. TCR currently offers both Individual and Enterprise Edition services. The Individual Edition is designed for individual developers and provides basic container image storage and distribution features. The Enterprise Edition offers secure, dedicated, and high-performance cloud-native application artifact hosting and distribution services for enterprise customers. For differences between the Individual and Enterprise Edition services, please refer to Specification Description.

Cross-platform image synchronization

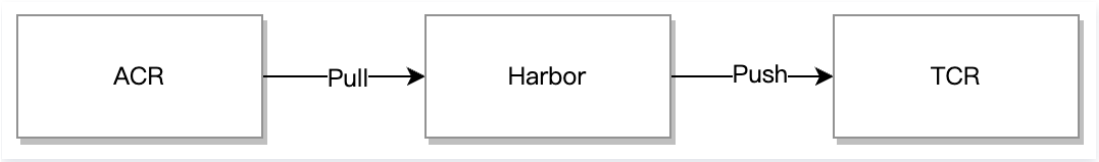
In cross-platform scenarios, in addition to batch data migration, you often also need to sync images across platforms in real time.
To synchronize images from a self-built Harbor to TCR Enterprise Edition, please refer to Synchronizing Images from Self-built Harbor to TCR Enterprise Edition. Configure synchronization rules on the Harbor side. By transitioning from a self-built container image service to TCR, users can reduce operational management costs and enjoy stable cloud-based hosting services and technical support. Additionally, it enables seamless integration with cloud container services, providing a consistent user experience for container deployment on the cloud. Users can also pull images from container clusters through private networks, reducing public network bandwidth costs. Similarly, users can configure rules on the Harbor side to synchronize images with other third-party repository service platforms. Apart from Harbor itself, the following image repository services are currently supported by Harbor:

- 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

You can also use the external Harbor registry as a relay to sync images between third-party registry service platforms.
As illustrated below, an example of **real-time synchronization of images from Alibaba Cloud ACR to Tencent Cloud TCR:**

1. Configure a pull-based replication policy in Harbor to pull an image from ACR to Harbor in real time and use Harbor as a relay registry.
2. Configure a push-based replication policy in Harbor to push the image from ACR in Harbor to TCR in real time.



In this way, the image can be synced from ACR to TCR. You can also configure image synchronization between other platforms in the same way.

Scenario 3: DevOps image flow

During development and OPS, an application usually needs to undergo multiple steps from development and testing to pre-production and eventual release into the production environment. The corresponding image also needs to flow through multiple steps.
Users can leverage TCR's instance synchronization feature to build the aforementioned DevOps pipeline for image circulation. If the main accounts for different environments are not the same, enable "Support cross-main account instance synchronization" when configuring instance synchronization rules.
Users can also utilize the delivery pipeline feature to achieve automatic image building and application deployment triggered by code push or automatic deployment triggered by local image push. For more information, please refer to Implementing Container DevOps with Delivery Pipeline.

> **Note**
> Currently, TCR's delivery pipeline feature only supports pre-configured fixed pipelines. If users have more complex DevOps pipeline requirements, they can use CODING DevOps. CODING DevOps is a one-stop DevOps development platform provided by Tencent Cloud, and TCR's delivery pipeline feature relies on the continuous integration and continuous deployment features of CODING DevOps.

Nearby Access Through Image Synchronization Between Multiple Global Regions

Last updated: 2023-09-13 14:36:35

Overview

When enterprises expand their container services to multiple regions, they may want to pull container images from nearby locations to improve the pull speed and reduce cross-regional public network traffic costs. They may also need to implement hot backups in multiple regions or transfer images between multiple image repository services within the same region, such as cross-team sharing or transitioning from development repositories to production repositories. In these scenarios, the conventional best practice is to create and maintain multiple container image repository services (Docker Registry) in one or more regions and write scripts to call Docker Push/Pull for cross-repository image replication. Tencent Container Registry (TCR) Enterprise Edition provides both on-demand synchronization of container images across instances and multi-region replication within a single instance. Users can flexibly choose or combine these two capabilities to meet the requirements of the above scenarios. The advantages of these two capabilities are as follows:

Instance synchronization

Specified images can be automatically synced between multiple instances in the same region or multiple regions as needed.

- On-demand synchronization: target instances and images to be synced can be precisely matched and selected based on custom rules.
- Automatic synchronization: after the image to be synced is pushed to the source instance, it will be automatically synced to the target instance.
- Cross-tenant synchronization: public images can be synced between instances across multiple root accounts in the same enterprise.
- Helm Chart and container image can be filtered, and you can choose to sync only one type of cloud native artifacts.
- You can query synchronization logs, which can be used with a webhook to implement synchronization success event notification.

Instance replication

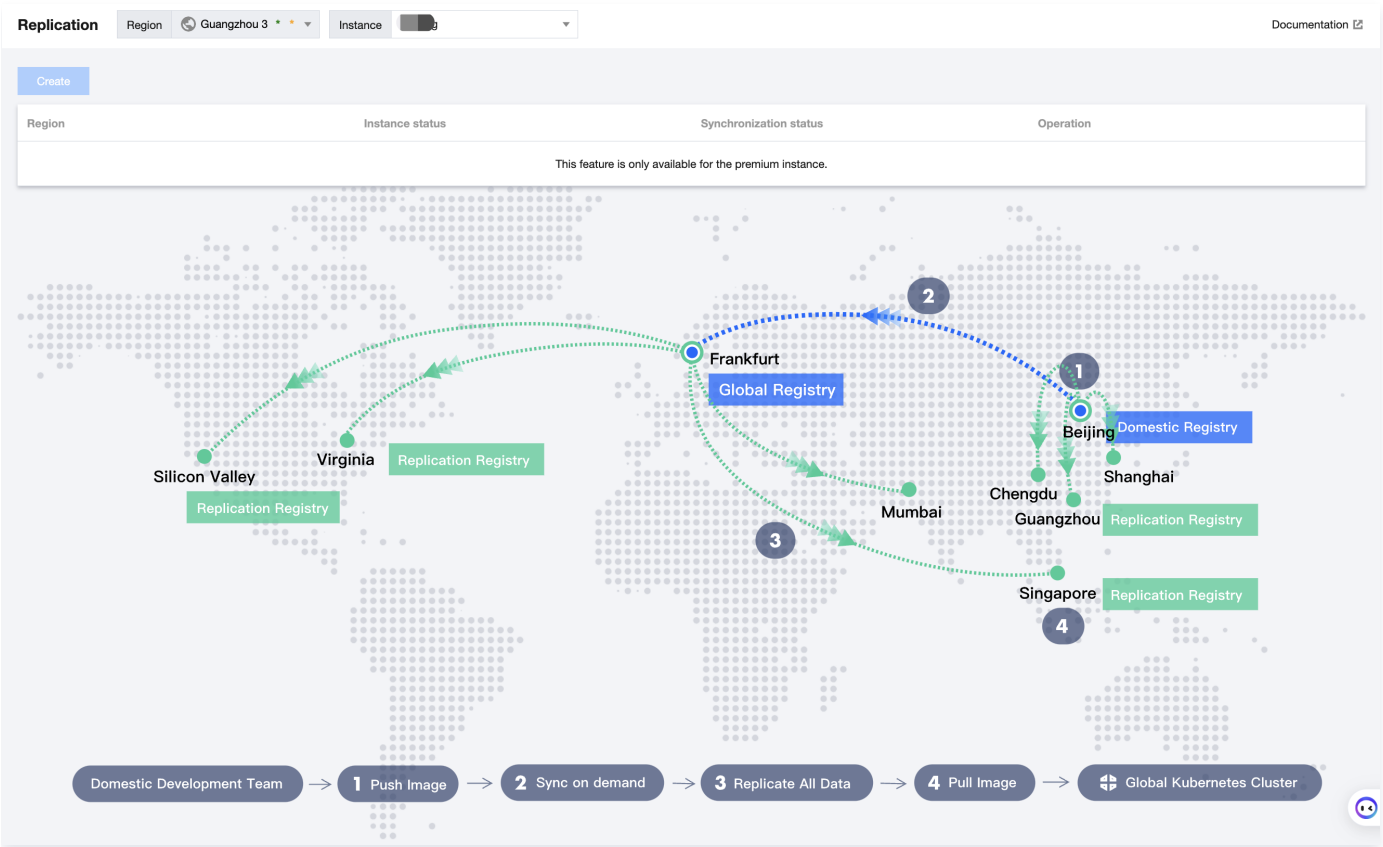
TCR enables you to configure replicas (replica instances) in multiple regions for a single instance and supports nearby access.

- Single instance: if a single instance needs to be accessed in multiple regions, you can use the same image repository name/tag to maintain consistent container configurations.
- Nearby access: in multi-region deployment, image data in the same region can be pulled to improve the deployment efficiency and stability.
- Reduced costs: nearby image pull over private network can reduce the public network traffic fees or Direct Connect fees incurred in cross-region image registry access.
- Simplified management: you don't need to manage multiple instances, configure synchronization rules between instances, or care about the synchronization status of the specified image.
- Quick synchronization: the image layer data is replicated across regions in real time in a streaming manner; therefore, once pushed to one region, an image can be pulled from multiple regions.

Use Cases

Scenario 1: nearby access in multiple global regions for international business

A game developer wants to deploy containerized game services in multiple regions worldwide, requiring global multi-region synchronization and nearby access for container images. At the same time, due to data compliance restrictions, they need to manage data independently for China and overseas regions, controlling data transmission. The client adopts the following solution, achieving global multi-region data synchronization and nearby access while maintaining a unified configuration, significantly improving the efficiency and stability of service deployment.



In this scenario, the customer creates two independent instances in Beijing and Frankfurt, configures instance synchronization rules, and synchronizes production-oriented images as needed. At the same time, multiple replica instances are configured within the Beijing and Frankfurt instances, such as Shanghai, Chengdu, and Guangzhou sub-instances within the Beijing instance. When a new game version needs to be released, the Beijing development team pushes the latest container images for both domestic and overseas versions. The overseas version is automatically synchronized to Frankfurt and then replicated in real-time to Silicon Valley, Virginia, Mumbai, Singapore, and other locations. When the Singapore container cluster updates the latest image, it accesses the Singapore replica instance through the private network for nearby access, ensuring a fast and stable update of the production container.

Scenario 2: image transfer between multiple subsidiaries and businesses in a large enterprise

A large enterprise has multiple subsidiaries/BGs, each with different business directions and independent IT teams. To manage cloud resource permissions and costs separately, different Tencent Cloud primary accounts are used among subsidiaries and businesses. The customer has adopted the following solution to achieve sharing of base images across the entire group and image sharing among multiple businesses.
In this solution, cross-tenant instance synchronization is configured between instances under multiple subsidiary accounts to share public images. The basic platform admin configures the basic image synchronization between business instances in each subsidiary in a unified manner. Some businesses plan to use multiple instances to separately manage images during business development, testing, and production and automatically transfer business images between each production stages based on image tag.

> **Note**
> Both of the above scenarios are relatively complex use cases. For conventional business needs, you can choose a partial solution from the examples to meet your requirements, such as cross-regional hot backups, local access in multiple regions within the country, and image circulation between multiple instances within the same region.
>
> Additionally, TCR Enterprise instances support custom domain names. Combined with DNS services, multiple instances can share the same domain name, enabling unified image publishing configuration and local private network access across multiple regions, making instance management more flexible.

Operations Guide

Preparations

- You have successfully purchased an Enterprise Edition instance. The instance synchronization feature requires a Standard or Premium instance, while the instance replication feature requires a Premium instance.
- If you are using a sub-account, the sub-account must have obtained operation permissions on the corresponding instance. For more information, see TCR Enterprise Authorization Management.

Configuring instance synchronization

For detailed operation instructions, please refer to Synchronization and Replication - Configuring Instance Synchronization. Instance synchronization supports cross-master account synchronization, which can be configured when creating synchronization rules.

Configuring instance replication

For detailed operation instructions, please refer to Sync Replication - Configuring Instance Replication.
Please note that instance replication does not currently support cross-border replication within domestic and overseas regions, such as configuring a Silicon Valley replica instance for an Advanced Edition instance in the Beijing region.

Configuring custom domain name

For detailed operation instructions, please refer to Configuring Custom Domain Name. Note that custom domain name resolution needs to be configured separately. For domestic sites, PrivateDNS can be used, while for international sites, this product is not supported, and it is recommended to use a self-built DNS service.

Troubleshooting Guide

1. What should I do if instance synchronization failed?

You can visit the product console to view the relevant rules and synchronization logs, and manually trigger synchronization. If the synchronization is too slow or still fails, please contact us through online consultation.

2. What should I do if instance replication failed?

Currently, instance replication does not support viewing synchronization logs for specific repositories. Please wait patiently for the instance replication process to complete and try accessing the image once the status is updated to "Synchronization Successful." If the instance replication status cannot be updated to "Synchronization Successful" or the image cannot be accessed after a successful synchronization, please contact us through online consultation.

3. How do I know whether the specified image has been replicated to a replica instance?

Currently, instance replication allows you to view historical synchronization tasks. You can check the task details logs to determine the synchronization status of the specified image repository or image.

4. How do I accelerate cross-region instance synchronization?

Currently, it is not possible to increase the cross-region synchronization speed for specific accounts or instances separately. This speed is limited by the bandwidth of the cross-region Cloud Connect Network (CCN) and is shared among multiple tenants. If you require special guarantees, please contact us through online consultation.

Using Custom Domain Name and CCN to Implement Cross-Region Private Network Access

Last updated: 2023-09-13 14:35:32

Scenario

Tencent Container Registry (TCR) Enterprise Edition supports network access control, allowing users to connect to a specified Virtual Private Cloud (VPC) and enabling Docker clients within the VPC to access image data through the private network. With the widespread adoption and implementation of multi-cloud and distributed cloud concepts, container clusters are no longer confined to a single VPC within a specific Tencent Cloud region but may be distributed across multiple cloud providers and complex networks within IDCs. These complex networks may be interconnected through Cloud Connect Network and peering connections. In this context, users require access to a single TCR Enterprise Edition instance across multiple regions and private networks, enabling seamless pushing and pulling of images through the private network.
This document mainly introduces how an enterprise customer uses a custom domain name together with the CCN, Peering Connection, and Private DNS products to enable multiple VPCs to access a TCR instance simultaneously and distribute container images over the private network.
In particular, if your business is distributed in multiple clouds and multiple regions, in order to realize data disaster recovery backup and nearby access, it is recommended that you refer to the following best practices and choose the most suitable scheme according to your business needs: Image Data Synchronization and Replication Between Multiple Platforms in Hybrid Cloud and Nearby Access Through Image Synchronization Between Multiple Global Regions.

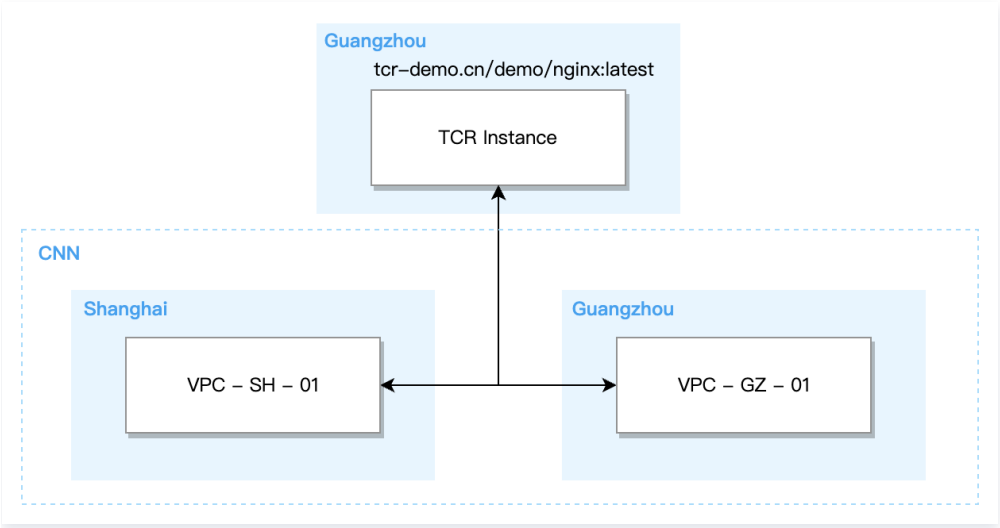
Preparations

Check that you have completed the following preparations:

- You have purchased an Enterprise Edition instance, and the operator has the necessary instance management permissions, such as QcloudTCRFullAccess.
- Configure a valid domain name. For more information, see Configuring Custom Domain Name.
- Activate services such as CCN and Peering Connection, and access multiple VPCs.

Overall Structure

The customer deployed containerized business in both Guangzhou and Shanghai and used the TCR Enterprise Edition instance in Guangzhou to host and distribute container images.



Header Configurations

Creating a TCR Enterprise Edition instance and binding a custom domain name

1. Purchase a TCR Enterprise Edition instance in the region where the container business is deployed. For more information,

see Purchasing TCR Enterprise Edition Instance. For this best practice, select Guangzhou (ap-guangzhou, gz).
2. Initialize the instance and upload the first image. For more information, see TCR Enterprise Edition Getting Started. For this best practice, this step is to access the specified VPC vpc-gz-01 and push images over the private network.
3. Configure a custom domain name. For more information, see Configuring Custom Domain Name.

Associating multiple VPCs with CCN

1. Go to the VPC console, create a CCN instance, and associate it with the Guangzhou and Shanghai VPCs.
2. You can choose to use the peering connection feature to associate the VPCs mentioned above.

Configuring Private DNS for the custom domain name

1. Go to the Private DNS console, use the bound custom domain name to create a private zone, and associate it with the VPCs mentioned above.
2. Configure the parsing record: Select **A record**, use **@** to directly parse the main domain name, and configure the record to the private IP corresponding to the accessed VPC.

Scenario Verification

Verifying the VPC connected to the instance

1. In the connected VPC in Guangzhou, create a CVM and install the Docker client.
2. Log in to the CVM and try to pull the image. The following is a reference command, where you need to replace `demo-tcr.cn` with the actual bound custom domain name and replace `demo/nginx:latest` with the actual image address (`demo` is the namespace).

```
# Pull the image in the container cluster in Guangzhou
docker pull demo-tcr.cn/demo/nginx:latest
```

If the image pull is successful, the VPC connection, custom domain name, and Private DNS are configured properly, and the container cluster of the Guangzhou VPC can use the custom domain name to pull images over the private network.

Verifying the other VPC connected to CCN

1. In the VPC connected to CCN in Shanghai, create a CVM and install the Docker client.
2. Log in to the CVM and try to pull the image. You can use the same path to directly pull the Enterprise Edition instance in Guangzhou.

```
# Pull the image in the container cluster in Shanghai
docker pull demo-tcr.cn/demo/nginx:latest
```

If the image pull is successful, the CCN configuration is normal, and the container cluster of the Shanghai VPC can use the custom domain name to pull the image across regions over the private network.