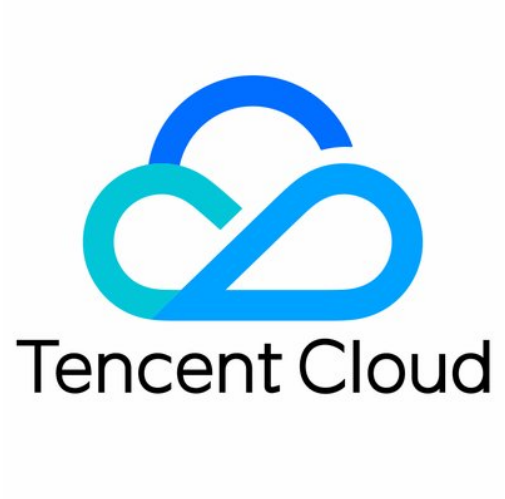
Tencent Container Registry

Best Practices

Product Documentation



Contents

Best Practices
Synchronizing Images to TCR Enterprise Edition Instances from a Self-built Harbor

Best Practices
Synchronizing Images to TCR Enterprise Edition Instances from a Self-built Harbor

Last updated : 2020-07-28 15:55:34

Operation Scenario

When you migrate a container cluster created in the IDC to the cloud container service (CCS), you may also choose to migrate the created container image hosting service to the cloud for hosting at the same time. After the created image repository service is migrated to TCR, the O&M costs for setup and maintenance are reduced, and professional and stable cloud hosting services and technical support are provided. In addition, the linkage with CCS is implemented, users can enjoy a consistent CCS experience, the container cluster can be used to pull images from the private network, and the cost of public network bandwidth is reduced.

Harbor is an open source enterprise-class Docker Registry project of VMware. On the basis of the open source Docker distribution capability, Harbor extends capabilities such as RBAC, secure image scanning, and image synchronization. At present, it has become the first choice of self-built container hosting and distribution services. This document describes how to synchronize a container image or Helm Chart in Harbor that is set up in the IDC or on the cloud server to the TCR enterprise edition.

Prerequisites

To synchronize data in the self-built Harbor to a TCR instance, you need to confirm and complete the following preparations first:

- The Harbor service has been set up and only Harbor V1.8.0 and later versions are supported.
- The self-built Harbor can access TCR through a private line, public network, or VPC.
- You have created an Enterprise Edition instance in the region of the cloud container cluster or in an adjacent region.
- If a sub-account is used for an operation, refer to Example of Authorization Solution of the Enterprise Edition to grant the sub-account the permission to push a container image of the

corresponding instance and Helm Chart. It is recommended that you grant the sub-account used to configure data synchronization all the read and write permissions of the TCR instance.

Directions

Configure a TCR instance that can be accessed by the self-built Harbor service

You can select one of the following solutions to configure an instance of the TRC Enterprise Edition based on actual network conditions of the self-built Harbor service.

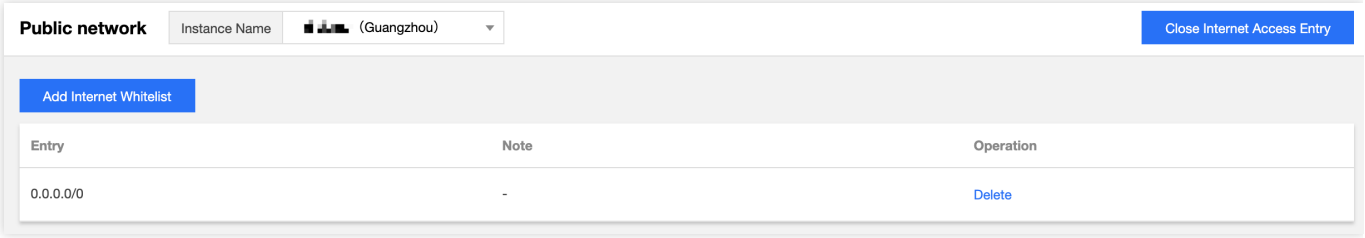
- Solution 1: access through a public network
- Solution 2: access through Tencent Cloud VPC

Solution 1: access through a public network

If the current self-built Harbor service is not deployed in a Tencent Cloud VPC environment or cannot be connected to Tencent Cloud VPC through a private line, synchronize data through a public network. During synchronization, a public network traffic fee may be generated. For more information, refer to the pricing of the network operator or cloud service provider.

1. Log in to the TCR console and choose **Access Control** -> **Access through Public Network** in the left sidebar.
2. In the **Instance Name** drop-down list in the upper part of the page, select an instance for data synchronization.
3. Click **Enable Public Network Access Entry** in the upper part of the list to enable the entry. After the status of the button changes **Disable Public Access Entry** from **Enabling** and **Add Public Network Whitelist** is available, the entry is enabled. In this case, public access requests from all sources are rejected by default.
4. Click **Add Public Network Whitelist**. In the "Create Public Network Access Whitelist" window that is displayed, configure a whitelist policy to allow the self-built Harbor service to access the instance through a public network.
   - **Instance**: the currently selected instance, that is, the instance for data synchronization.
   - **Public IP Address Segment**: the public IP address of the self-built Harbor service egress. If no specific public IP address can be confirmed, the IP address can be temporarily set to `0.0.0.0/0` to allow access from all public network sources. After synchronization is complete, delete the configuration as soon as possible.
   - **Remarks**: you can enter remarks of the whitelist configuration, for example, “Allow the self-built Harbor service to access through public network”.

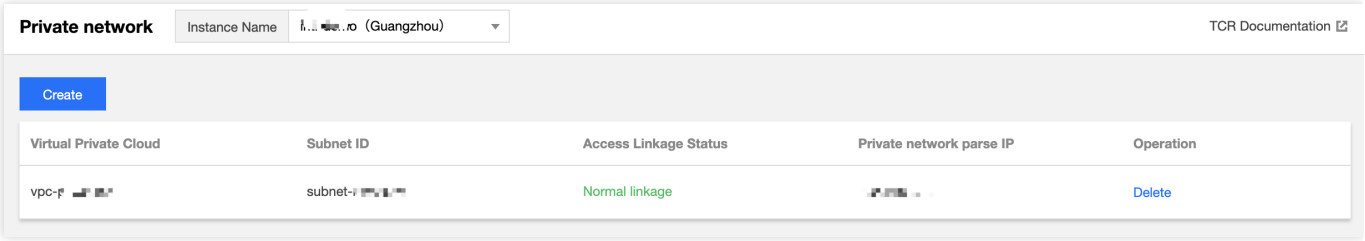
The following figure shows the completed configuration:



Solution 2: access through Tencent Cloud VPC

If the current self-built Harbor service is deployed in Tencent Cloud VPC environment or is connected to the Tencent Cloud VPC through a private line, synchronize data through the private network. Data synchronization through the private network increases the data synchronization speed and eliminates public network traffic costs.

1. Log in to the TCR console and choose **Access Control** -> **Access through Private Network** in the left sidebar.
2. In the **Instance Name** drop-down list in the upper part of the page, select an instance for data synchronization.
3. Click **Create**. In the "Create Private Access Link" window that is displayed, configure a new private access link to allow the self-built Harbor service to access the instance through the private network.
   - **Instance**: the currently selected instance, that is, the instance for data synchronization.
   - **VPC**: the VPC where the self-built Harbor service is located or the VPC connected through Direct Connect.
   - **Subnet**: the created private access link occupies a private IP address of the selected VPC. Select a subnet under the VPC to assign the subnet of the private IP address.
     The following figure shows the completed configuration:



4. After the configuration is complete, the target access IP address of the private access link is obtained. To parse the domain name of the instance into the private IP address in the VPC, configure the host on the CVM where the self-built Harbor service is located. If an independent

DNS is currently in use, you may also configure the host in the DNS.
Run the following command on CVM to configure the host.

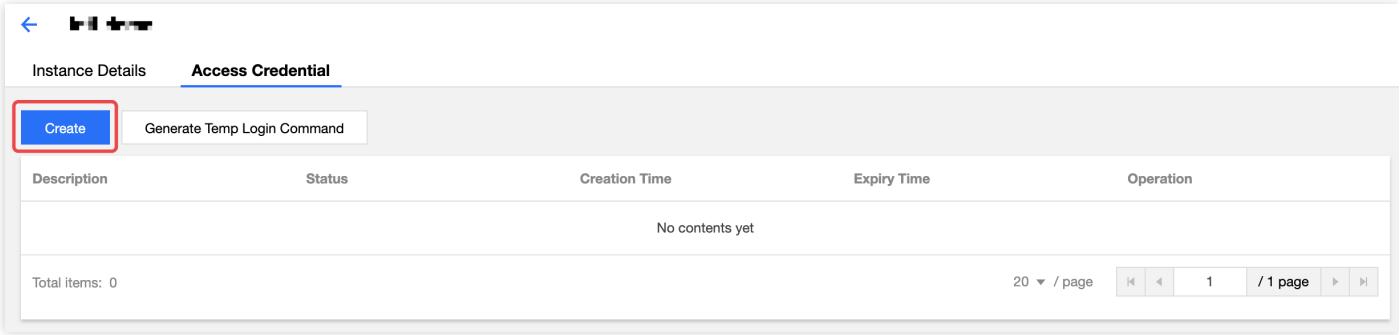
```
echo x.x.x.x harbor-sync.tencentcloudcr.com >> /etc/hosts
```

Replace `x.x.x.x` with the parsed private IP address generated after a private access link is created and replace `harbor-sync.tencentcloudcr.com` with the domain name of the actual instance.

Creating an access credential for the Enterprise Edition instance

The TCR Enterprise Edition supports creating and managing multiple access credentials. It is recommended that you create an independent access credential for data synchronization and delete the credential in time after data synchronization is complete so as to avoid leakage of the access permission of the instance.

1. Log in to the TCR console and select **Instance List** in the left sidebar.
2. On the “Instance List” page, select an instance for data synchronization. The instance details page is displayed.
3. Select the **Access Credential** tab and click **Create** in the upper part of the instance list, as shown in the following figure.

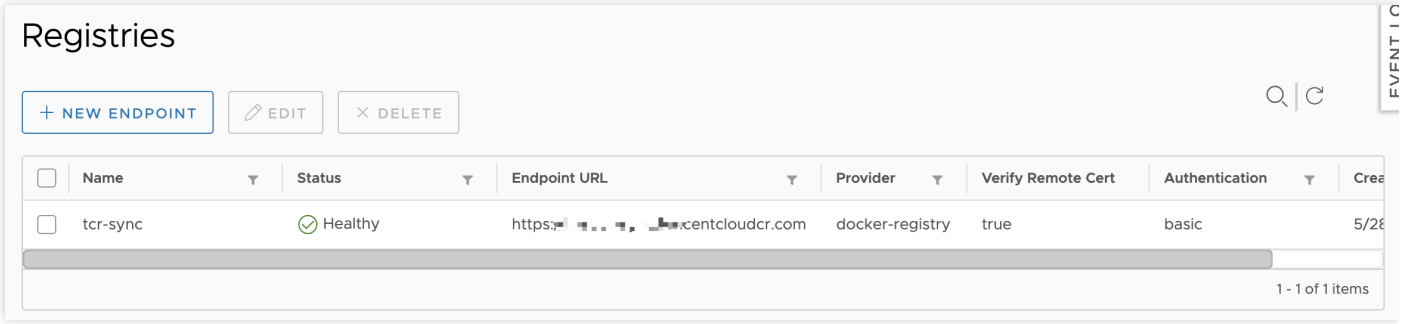


4. In the “Create Access Credential” window that is displayed, perform the following steps:
   i. In the “Create Access Credential” step, enter information in “Purpose Description” of a credential and click **Next**. You can enter “Synchronize data for self-built Harbor” in “Purpose Description”.
   ii. In the “Save Access Credential” step, click **Save Access Credential** to download the credential. **Please save the access credential properly. You have only one chance to save the credential.**
   After an access credential is created, you can view the credential in the **Access Credential** tab. After data synchronization is complete, please disable and delete the access credential in time.

Configuring a Harbor synchronization registry and a synchronization rule

Harbor supports adding a third-party registry and configuring a data replication rule. This document takes Harbor V2.0.0 as an example.

1. Log in to the self-built Harbor service by using an administrator account. You can view and perform **System Management**.
2. Choose **System Management** -> **Registry Management** in the left sidebar. The “Registry Management” page is displayed.
3. On the “Registry Management” page, click **Create Target**. Refer to the following information to add an Enterprise Edition instance.
   - **Provider**: select “docker registry”.
   - **Target Name**: custom definition of the name of the synchronization target, for example, the name or ID of the current Enterprise Edition instance.
   - **Description**: the description of the target registry.
   - **Target URL**: the access domain name of the Enterprise Edition instance, for example, `https://harbor-sync.tencentcloudcr.com` .
   - **Access ID**: enter the user name obtained from Create Access Credential of an Enterprise Edition Instance.
   - **Access Password**: enter the login password obtained from Create Access Credential of an Enterprise Instance.
   - **Verify Remote Certificate**: use the default value.
4. Click **Test Connection**.
   - If “Test connection successful” is displayed, the current self-built Harbor service can access the Enterprise Edition instance.
   - If “Test connection failed” is displayed, make sure that you configure the self-built harbor service to access the TCR Enterprise Edition instance.
5. Click **OK** to create the target registry. The following figure shows the created registry.



6. Choose **System Management** -> **Replication Management** in the left sidebar and click **Create Rule**. Refer to the following information to create a synchronization rule.
   - **Name**: the name of the synchronization rule. You can enter a name based on the actual usage scenario.

- **Description**: the description of the replication rule.
- **Replication Mode**: only “Push-based” is supported.
- **Resource Source Filter**: you can filter and select resources to be synchronized. If the field is not specified, all container images and Helm Chart resources in the self-built Harbor service are selected by default.
- **Target Registry**: select the target registry created in Step 3.
- **Target Namespace**: the namespace of the specified destination. If the field is not specified, the namespace with the same name is used by default. It is recommended that you use the default value.

> ⚠ **Note :**
>
> For the synchronization operation, a namespace cannot be automatically created in the Enterprise Edition instance. Please refer to Create Namespace to create the corresponding namespace.

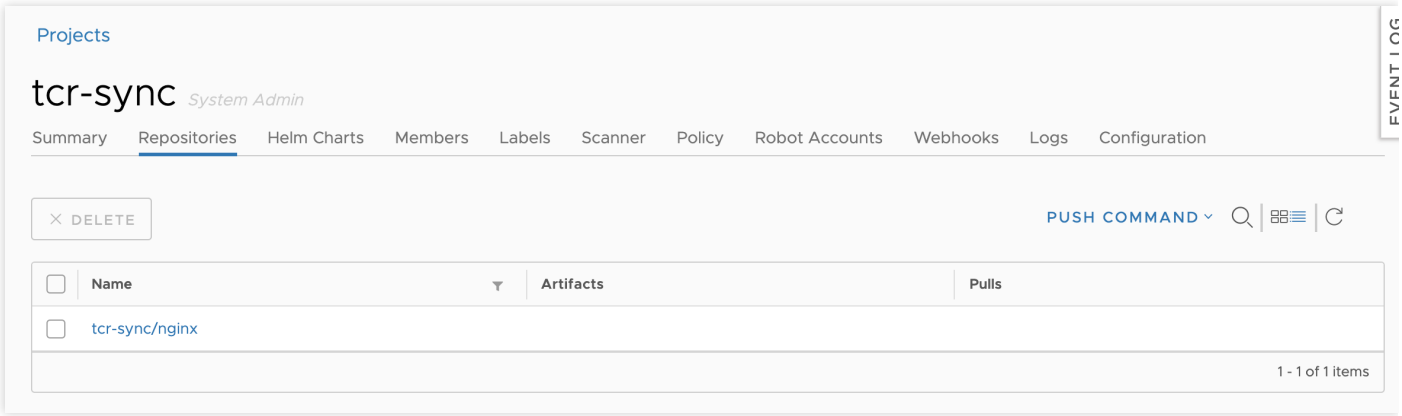
- **Trigger Mode**: by default, manual trigger is selected. If automatic synchronization is required when a new container image or Helm Chart is pushed, select “Event-driven”. It is recommended that you not select “Delete remote images at the same time when deleting local images”.
- **Overwrite**: by default, resources with the same name are overwritten.

Triggering synchronization and viewing the synchronization rule.

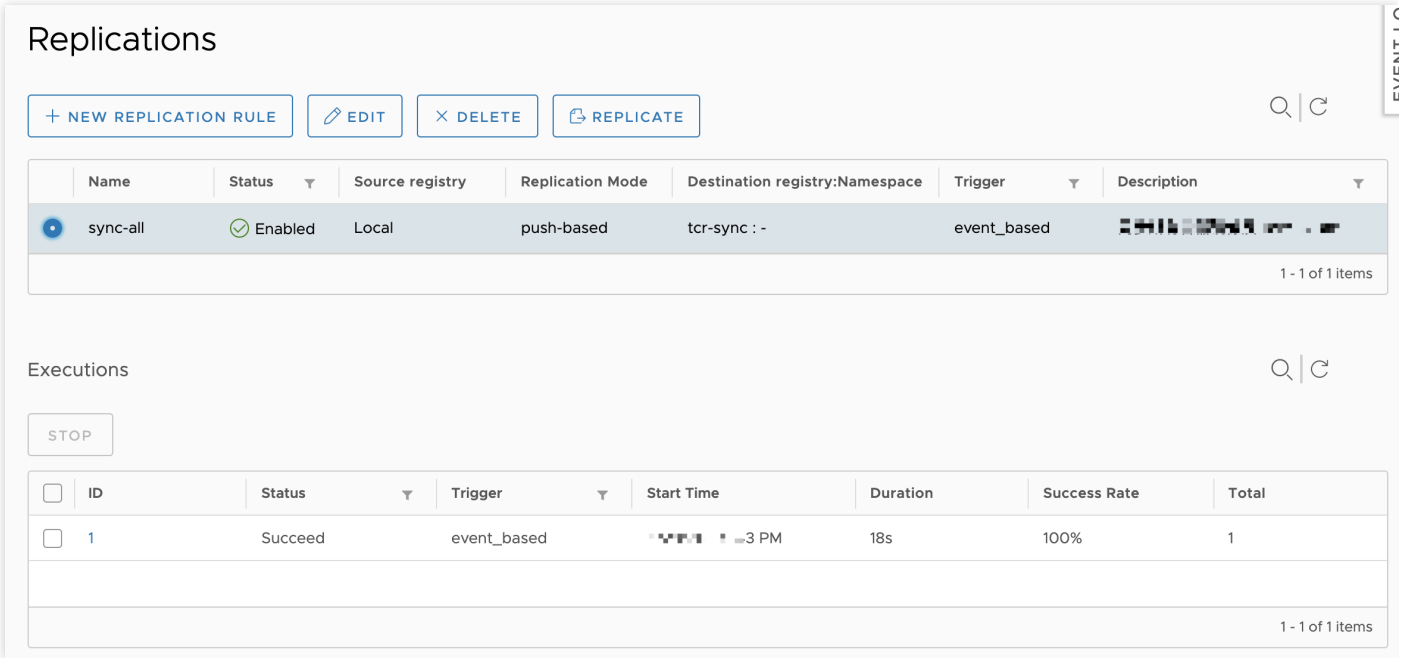
Push a container image and Helm Chart to the self-built Harbor service. If the trigger mode is set to “Event-driven” in the synchronization rule, the pushed resources are automatically synchronized to the enterprise edition instance. You can select the synchronization rule to view the synchronization log and access the Enterprise Edition instance console to check whether synchronization is successful. In this step, assume the `nginx:latest` container image is manually pushed to the self-built Harbor service to trigger synchronization.

1. Push a container image and view the image.
   Push the local `nginx:latest` container image by using the docker client, access the self-built Harbor service console, and view the pushed image. As shown in the following figure, the `nginx:latest` container image is pushed to the `tcr-sync` project and the NGINX image repository

is automatically created.



2. View the synchronization record and progress.
   Choose **System Management** -> **Replication Management** in the left sidebar and select the synchronization rule created in Step 5 to view the replication task of the synchronization rule. As shown in the following figure, a task record exists in the replication task. You can view the status and success percentage of the replication task.



3. View the synchronized image in TCR.
   Access the “Image Repository” page of the TCR console and select the instance for synchronizing with the self-built Harbor service to view the container image that is successfully synchronized. As shown in the following figure, the NGINX image repository is automatically created in the `tcr-`

`sync` namespace and the `nginx:latest` container image is pushed.