Container Registry

FAQs

FAQs

General Q&A

Q: What is Container Registry (ACR) Enterprise Edition?

Container Registry (ACR) is a secured image repository hosting service providing container image lifecycle management.

Container Registry Enterprise Edition allows you to manage images throughout image management lifecycle. It provides secured image management capability, include image build from source code, replication across global regions and it is very easy to manage image permission for RAM accounts. This service simplifies the creation and maintenance of the image registry and supports image management in multiple regions.

Combined with other cloud services such as Container Service, Container Registry provides an optimized solution for distributing Cloud Native applications on the cloud.

Q: When should I use ACR Enterprise Edition?

If you have concerns on scale and security of container application distribution, for example, large number of worker nodes, multi-regional deployment or you want to have more secured environment of image, then you might want to try this service.

- Having large-scale nodes on which runs containerized applications
- High security requirements Requires network access control and requires fine-grained image security scanning
- Multi-regional application deployment. In this case, your applications require image replication and mirroring for automatic image synchronization across multiple regions.

Q: How does ACR Enterprise Edition work?

ACR Enterprise Edition is a high secured registry service that docker images are encrypted and stored on the user’ s OSS Bucket. It provides flexible network access control management, customers can manage the public network, VPC network access through whitelist. ACR Enterprise Edition integrates with cloud products seamlessly such as Alibaba-cloud Container Service for Kubernetes and Alibaba-cloud Code to build images and deploy to clusters automatically.

Q: Why is ACR Enterprise Edition better than other image container registry?

Functions	ACR EE	ACR	Docker Registry

Image management	Yes	Yes	Yes
Multi-region	Yes	Yes	N/A
Image scanning	Yes	Yes	N/A
Network policy for access control	Yes	No	N/A
P2P distribution	Yes	No	N/A
Image replication	Yes	No	N/A
High aviability	Yes	Yes	Partial
Integration with Alibaba Cloud Kubernetes Service	Yes	Yes	N/A

ACR EE enables organization to manage Enterprise-class image securely, and it supports P2P image distribution expedite large scale application deployment. What’ s more it provides flexible network policy for access control, fine-grained image security scanning. The P2P large-scale distribution enables high concurrency, which allows thousands nodes pulling images at the same time.

Q: How can I get started with ACR?

Please visit Quick Start guide, for more details on how to get started with ACR.

Activate an account

Container Registry console provides multi-region secure image hosting capability. You must set a password that is independent of Alibaba Cloud account system as the logon credentials on the Container Registry console to facilitate uploading and downloading images.

Initialization code

When you activate Container Registry for the first time and log on to the Container Registry console, you must set a password that is independent of the Alibaba Cloud account system. This password is used as the Container Registry console logon credentials to facilitate the uploading and downloading of images. Subsequently, you can change your Container Registry logon password by verifying your mobile phone number.

Note:

If you are using a subaccount for the first time, make sure that the primary account has been activated and set the Registry logon password.

FAQs about Docker client

Docker logon failure

Mainly troubleshoot the following two issues:

> The logon password of Alibaba Cloud account is used, instead of the independent logon password of Registry. The Registry logon password is configured and modified in the Container Registry console.

> If you use sudo for logon, make sure you first enter the Linux user password, instead of the Registry logon password. The Linux user password usually allows you to try at most three times and prompts try again when the password is wrong. However, the Docker client exits after you enter the wrong Registry logon password once and returns the following error:

```
Error response from daemon: Get https://registry.cn-hangzhou.aliyuncs.com/v2/: unauthorized:
authentication required
```

Docker pull failure

The system prompts Error: image xxx not found.

> If you want to download images from a public repository, the error is caused due to the incorrect image URL. Search for this public repository in the console and check if the image version to be downloaded exists.

> If you want to download images from a private repository, check your Registry logon status first.
>
> Run cat ~/.docker/config.json to view all the domain names of the logged on Registries. Check if the domain name of the Registry that you want to download images is in the list. If not, log on to the relevant Registry by following the preceding instructions. If you already log on to the Registry, check if your logon account has permissions to download the image. Sub-accounts do not have any permission by default.

The system prompts Error: filesystem layer verification failed for digest.

This error indicates the downloaded block files failed to be verified, which occurs in rare cases. Generally, you can fix it by trying again.

Docker push failure

The system prompts denied: requested access to the resource is denied.

The troubleshooting steps are roughly the same as those for Docker pull failure. The only difference is that a higher authorization level is required in this case.

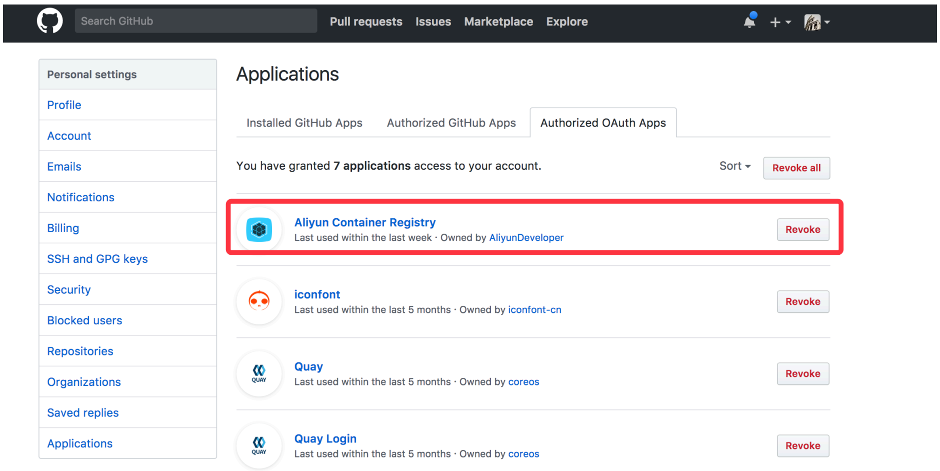
Source code repository

Container Registry console allows you to build images using a source code repository (Github/Bitbucket/GitLab) and supports automatically building the image after the source code is modified. This article summarizes the problems you might encounter with this feature and provides the solutions.

How to unbind source code repository Github/Bitbucket/GitLab or bind another account?

Source code repository Github/Bitbucket

Log on to the source code repository and revoke the authorization to Alibaba Cloud Container Registry on the settings page.



Applications

You have granted **7 applications** access to your account.

Aliyun Container Registry
Last used within the last week · Owned by AliyunDeveloper

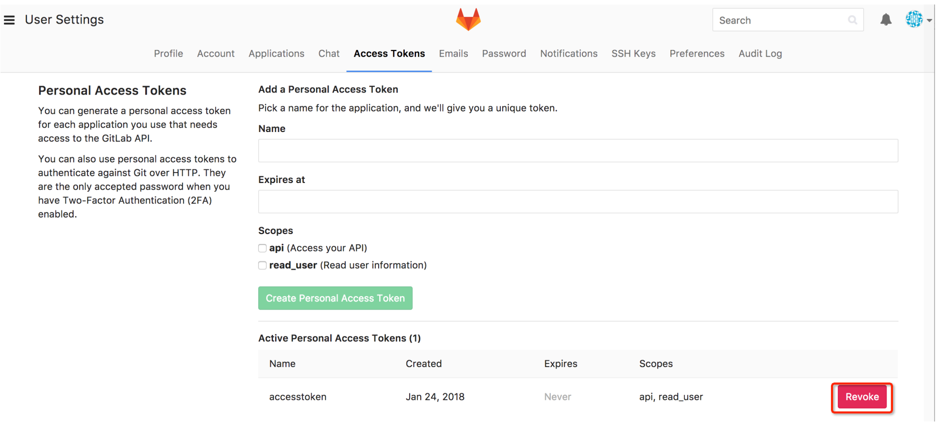
iconfont
Last used within the last 5 months · Owned by iconfont-cn

Quay
Last used within the last 5 months · Owned by coreos

Quay Login
Last used within the last 5 months · Owned by coreos

Source code repository GitLab

Log on to the source code repository and revoke the token bound previously on the settings page.



Personal Access Tokens

You can generate a personal access token for each application you use that needs access to the GitLab API.

You can also use personal access tokens to authenticate against Git over HTTP. They are the only accepted password when you have Two-Factor Authentication (2FA) enabled.

Add a Personal Access Token

Pick a name for the application, and we'll give you a unique token.

Name

Expires at

Scopes

□ **api** (Access your API)

□ **read_user** (Read user information)

Create Personal Access Token

Active Personal Access Tokens (1)

Name	Created	Expires	Scopes	
accesstoken	Jan 24, 2018	Never	api, read_user	Revoke

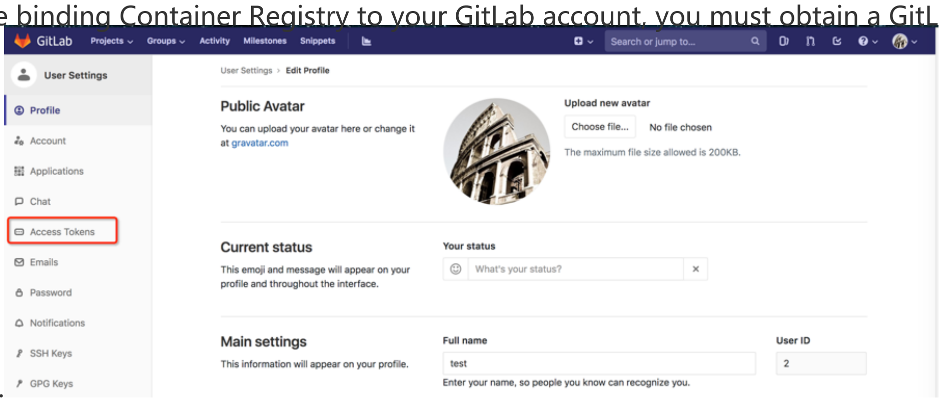
GitLab source code repository

GitLab source code repository

Container Registry allows you to create a GitLab source code repository and access the repository through GitLab API V3 or V4. This topic describes the procedure for creating a GitLab source code repository in Container Registry.

1. Obtain a GitLab access token

Before binding Container Registry to your GitLab account, you must obtain a GitLab access token.



Public Avatar

You can upload your avatar here or change it at gravatar.com

Upload new avatar

Choose file... No file chosen

The maximum file size allowed is 200KB.

Current status

This emoji and message will appear on your profile and throughout the interface.

Your status

What's your status?

Main settings

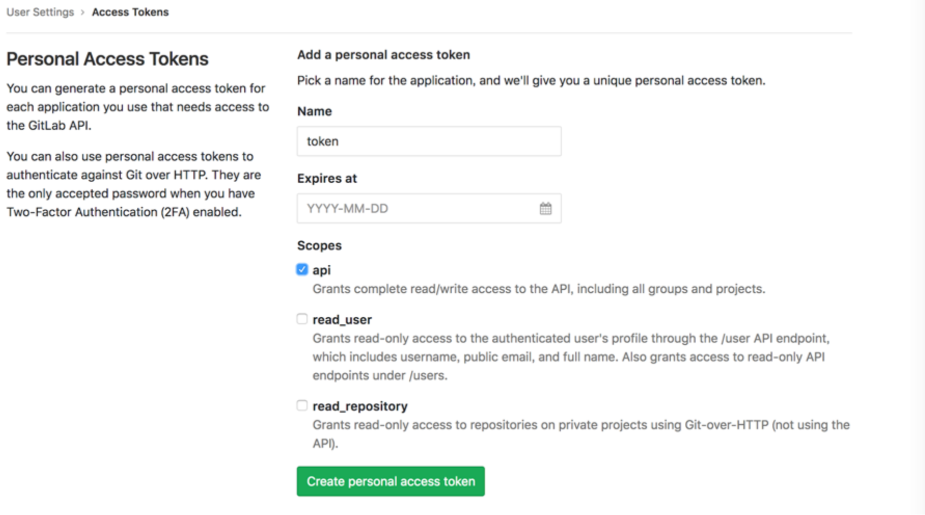
This information will appear on your profile.

Full name: test

Enter your name, so people you know can recognize you.

User ID: 2

In Scopes, select api for the access token. This operation is required because Container Registry needs to obtain the source code repository information and set hooks to trigger automatic build. If the access token has insufficient permissions, you fail to create a GitLab source code repository in Container Registry. In addition, pay attention to the expiration time of the access token to ensure that it is valid in use.



Personal Access Tokens

You can generate a personal access token for each application you use that needs access to the GitLab API.

You can also use personal access tokens to authenticate against Git over HTTP. They are the only accepted password when you have Two-Factor Authentication (2FA) enabled.

Add a personal access token

Pick a name for the application, and we'll give you a unique personal access token.

Name: token

Expires at: YYYY-MM-DD

Scopes

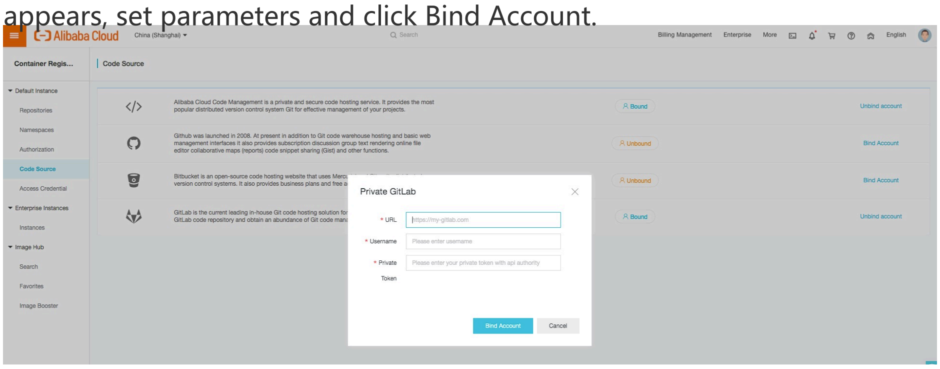
☑ api
Grants complete read/write access to the API, including all groups and projects.

□ read_user
Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.

□ read_repository
Grants read-only access to repositories on private projects using Git-over-HTTP (not using the API).

2. Bind Container Registry to your GitLab account

- Go to the Container Registry console and choose Default Instance > Code Source. On the Code Source page, click Bind Account for GitLab. In the Private GitLab dialog box that appears, set parameters and click Bind Account.



Code Source

Alibaba Cloud Code Management is a private and secure code hosting service. It provides the most popular distributed version control system Git for effective management of your projects. — Bound — Unbind account

Github was launched in 2008. At present in addition to Git code warehouse hosting and basic web management interfaces it also provides subscription discussion group text rendering online file editor collaborative maps (reports) code snippet sharing (Gist) and other functions. — Unbound — Bind Account

Bitbucket is an open-source code hosting website that uses Mercu... version control systems. It also provides business plans and free a... — Unbound — Bind Account

GitLab is the current leading in-house Git code hosting solution for... GitLab code repository and obtain an abundance of Git code mana... — Bound — Unbind account

Private GitLab

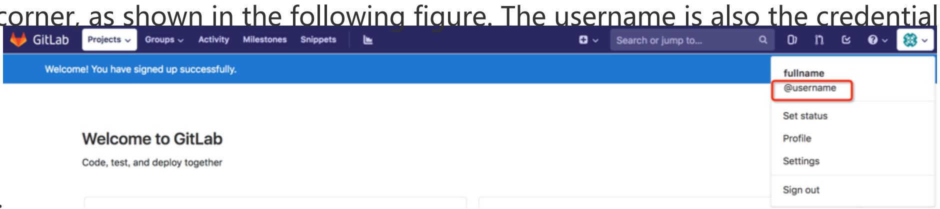
* URL: https://my-gitlab.com

* Username: Please enter username

* Private Token: Please enter your private token with api authority

URL: Enter the URL of your self-built GitLab, such as https://my-gitlab.com. Do not enter the URL of a specific repository.

Username: Enter the username on GitLab. To obtain the username, click your avatar on GitLab in the upper-right corner, as shown in the following figure. The username is also the credential used to log on to GitLab.



Welcome! You have signed up successfully.

Welcome to GitLab

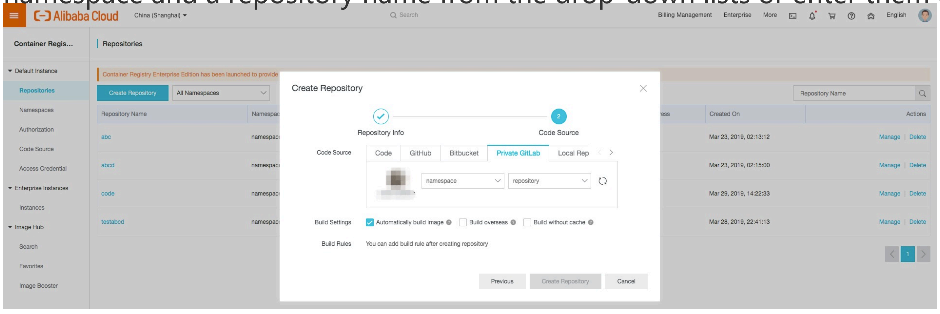
Code, test, and deploy together

Private Token: Enter the access token obtained in step 1.

Note: Currently, Container Registry does not support access to GitLab behind the firewall or with a self-signed HTTPS certificate. Ensure that GitLab is accessible through the Internet.

3. Create a GitLab source code repository

Each account can have a maximum of 100 GitLab source code repositories. You can select a namespace and a repository name from the drop-down lists or enter them directly.



Container Registry Enterprise Edition has been launched to provide

Repository Name	Namespac	ress	Created On	Actions
abc	namespac		Mar 23, 2019, 02:13:12	Manage | Delete
abcd	namespac		Mar 23, 2019, 02:15:00	Manage | Delete
code	namespac		Mar 29, 2019, 14:22:33	Manage | Delete
testabcd	namespac		Mar 28, 2019, 22:41:13	Manage | Delete

Create Repository

✓ Repository Info — 2 Code Source

Code Source: Code | GitHub | Bitbucket | **Private GitLab** | Local Rep

namespace / repository

Build Settings: ☑ Automatically build image □ Build overseas □ Build without cache

Build Rules: You can add build rule after creating repository

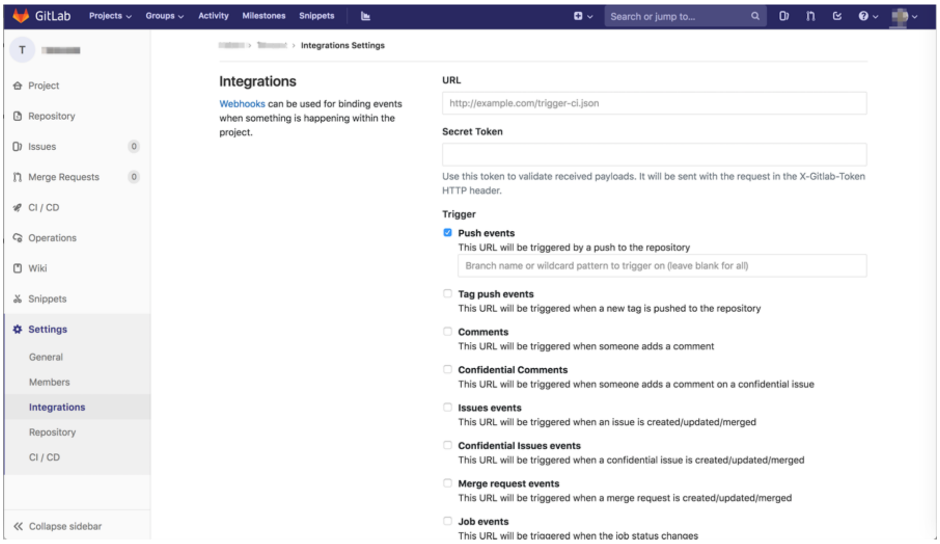
Troubleshooting

1. What should I do if I receive the error message “Failed to access the source code repository site. Please confirm that the account binding information is correct, or try again later.” ?

The possible causes for the error are as follows: (1) GitLab does not respond to your access request. To resolve the problem, ensure that GitLab is accessible through the Internet. Ensure that the firewall is disabled and no self-signed HTTPS certificate is used to access GitLab. In addition, ensure that the account binding information including the GitLab URL, username, and private token is correct. (2) Your GitLab access request times out due to network exceptions. In this case, you can try again later.

1. What should I do if I receive the error message “The source code repository site returns an error response. Please confirm that the account binding information is correct.” ?

The common symptom is that the connection to GitLab is normal but GitLab returns an error code upon a service request. To resolve the problem, ensure that the following conditions are met: (1) The access token has been granted complete read/write access to the GitLab API and has not expired. (2) Your source code account has the permission to set hooks. Ensure that the account has the permission to navigate to Settings > Integrations under the specified repository on GitLab.



[redacted] > [redacted] > Integrations Settings

Integrations

Webhooks can be used for binding events when something is happening within the project.

URL

http://example.com/trigger-ci.json

Secret Token

Use this token to validate received payloads. It will be sent with the request in the X-Gitlab-Token HTTP header.

Trigger

☑ **Push events**
This URL will be triggered by a push to the repository
Branch name or wildcard pattern to trigger on (leave blank for all)

□ **Tag push events**
This URL will be triggered when a new tag is pushed to the repository

□ **Comments**
This URL will be triggered when someone adds a comment

□ **Confidential Comments**
This URL will be triggered when someone adds a comment on a confidential issue

□ **Issues events**
This URL will be triggered when an issue is created/updated/merged

□ **Confidential Issues events**
This URL will be triggered when a confidential issue is created/updated/merged

□ **Merge request events**
This URL will be triggered when a merge request is created/updated/merged

□ **Job events**
This URL will be triggered when the job status changes