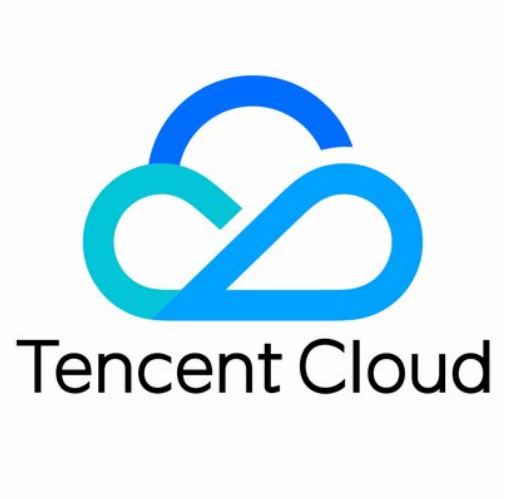
Tencent Container Registry

Access Management

Product Documentation



Contents

Access Management
- Overview
- Container Image Service Enterprise Edition
  - Example of Authorization Solution of the Enterprise Edition
- Container Image Service personal Edition
  - Example of Authorization Solution of the Personal Edition

Access Management Overview

Last updated : 2020-07-28 15:55:33

Introduction to Cloud Access Management

Cloud access management (CAM) is a web service provided by Tencent Cloud. It helps users securely manage the permissions for accessing resources under their Tencent Cloud accounts. CAM allows you to create, manage, or terminate users (groups) and controls who can use Tencent Cloud resources through identity management and policy management.

When you use CAM, you can associate a policy with a user or a user group. The policy authorizes or refuses users to use the specified resource to complete the specified task. For more information on CAM policies, refer to Policy Syntax. For more information on how to use CAM policies, refer to Policies.

If you do not need to perform access management of TCR resources for sub-accounts, you can skip this section. This does not affect your understanding and use of other sections of this document.

CAM-based Resource-level Access Control of TCR

Resource-level permissions refer to the capabilities that can specify and allow users to perform specific operations on specific resources. TCR supports resource-level access control of CAM and controls the granularity to the repository level, that is, you can authorize sub-accounts to perform operations on resources in only the specified image repository or the Helm Chart repository by configuring the CAM policy.

Types of resources that can be authorized by TCR in CAM:

Resource Type	Resource Description Method in Authorization Policy
Enterprise edition instance	`qcs::tcr:$region:$account:instance/*`
Enterprise edition repository	`qcs::tcr:$region:$account:repository/*`
Personal edition repository	`qcs::tcr:$region:$account:repo/*`

- `$region` : the region information. For example, `ap-guangzhou` indicates the region of Guangzhou. If the value is null, the field indicates all regions. For the specific list of regions and abbreviations, refer to Regions and Availability Zones.
- `$account` : the root account of the resource owner. The value is expressed as `uin/${uin}` , for example, `uin/12345678` . If the value is null, the field indicates the root account of the CAM user who creates the policy.
  For details on resource description in the authorization policy, refer to Resource Description.

Container Image Service Enterprise Edition
Example of Authorization Solution of the Enterprise Edition

Last updated : 2020-09-09 16:36:33

Configuring Preset Policies

- **QcloudTCRFullAccess**: full read/write permission of TCR.
  After the policy is bound to a sub-account, the sub-account has all operation permissions for all TCR resources, including the Enterprise Edition and the Personal Edition instances in TCR TKE.

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

- **QcloudTCRReadOnlyAccess**: read-only permission of TCR.
  After the policy is bound to a sub-account, the sub-account has the read-only permission for all TCR resources, including the enterprise edition and the personal edition instances in TCR TKE.

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

Configuring Policies in Typical Scenarios

> ⚠ **Note :**
>
> The policies in the following use cases are used only for the Enterprise Edition.

- Grant a sub-account all read/write operation permissions for all resources in the TCR Enterprise Edition instance.

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

- Grant a sub-account the read-only operation permission for all resources in the TCR Enterprise Edition instance.

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

- Authorize a sub-account to manage the specified instance, for example, dev-guangzhou whose instance ID is ins-xxxxxxxx.

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

- Authorize a sub-account to manage the specified namespace in the specified instance, for example, team-01 under the instance ins-xxxxxxxx.

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

- Authorize a sub-account to read only an image repository and pull only images in the image repository instead of deleting a repository, modifying repository attributes, or pushing images, for example, repo-demo in the namespace team-01 under the instance ins-xxxxxxxx.

```
{
"version": "2.0",
```

```
"statement": [{
"action": [
"tcr:DescribeRepository",
"tcr:PullRepository"
],
"resource": [
"qcs::tcr:::repository/ins-xxxxxxxx/team-01/repo-demo/*"
],
"effect": "allow"
},
{
"action": [
"tcr:DescribeInstances",
"tcr:DescribeInstanceStatus",
"tcr:DescribeNamespace"
],
"resource": [
"qcs::tcr:::repository/ins-xxxxxxxx/*"
],
"effect": "allow"
}
]
}
```

Container Image Service personal Edition
Example of Authorization Solution of the Personal Edition

Last updated : 2020-07-28 15:55:33

Configuring Policies in Typical Scenarios

⚠ Note :

The policies in the following scenarios are only used for Personal Edition.

- Grant a sub-account all read/write operation permissions for all resources in the TCR Personal Edition instance (image repository in TKE of the original TCR).

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

- Grant a sub-account the read-only operation permission for all resources in the TCR Personal Edition instance (image repository in TKE of the original TCR).

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

```
"qcs::tcr:::repo/*"
],
"effect": "allow"
}]
}
```

- Authorize a sub-account to manage the specified instance in the specified region, for example, namespace team-01 in the default region.

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

- Authorize a sub-account to read only an image repository and pull only images in the image repository instead of deleting a repository, modifying repository attributes, or pushing images, for example, the image repository repo-demo in the namespace team-01 under the default region.

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

```
}
]
}
```