Alibaba Cloud Application Configuration Management

User Guide

Issue: 20190111

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectu

al property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructio ns, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

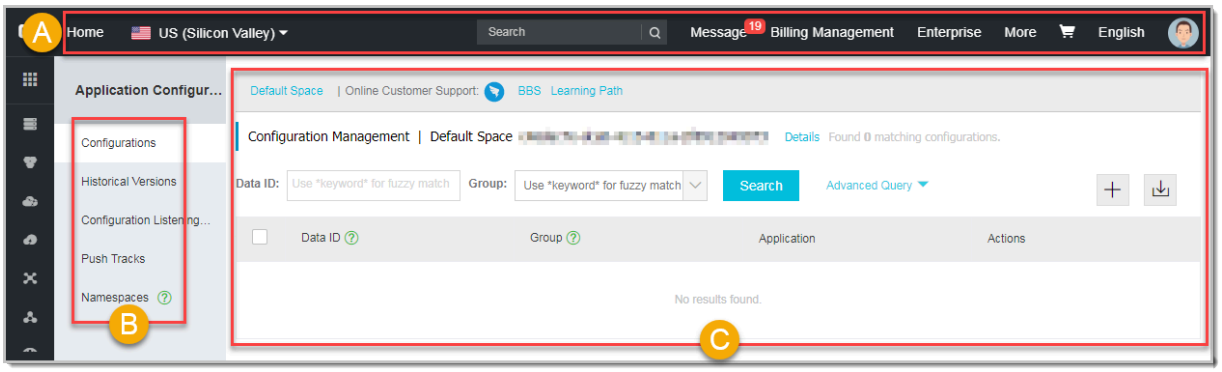
Contents

1 ACM console introduction

The ACM console is the workbench for configuration management. This topic describes the different areas of the ACM console.

The ACM console consists of the following areas:

Figure 1-1: ACM console



- [A] Top navigation bar: Shows menus of Regions, Messages, Tickets and so on.
- [B] Left-side navigation pane: Allows you to navigate to each sub-module, including configurat ion list, historical versions, listening query, push tracks, and namespaces.
- [C] Configuration Management: Provides core features to create, query, edit, and delete configurations and more advanced features.

2 Select a region

The machines you purchase can be distributed in different regions, so you have to determine which region you want to publish the configuration to before using the configuration management service.

Procedure

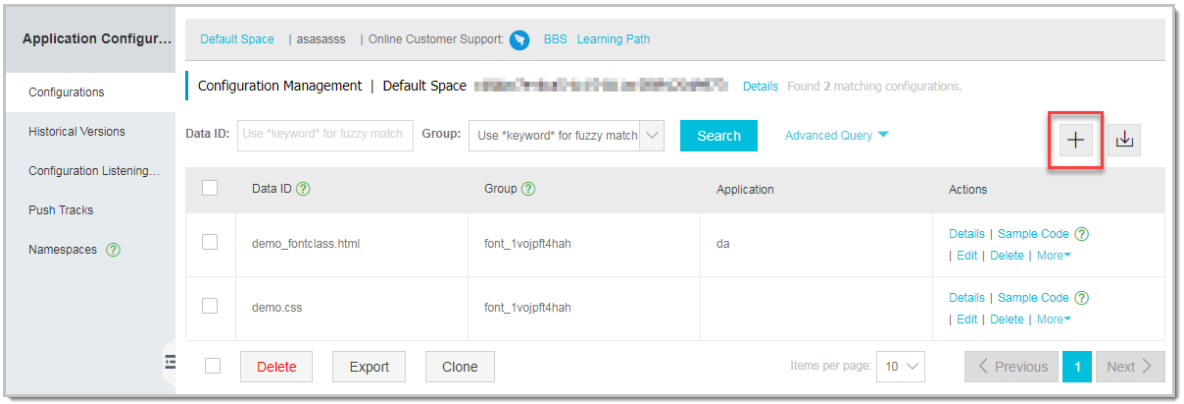
1. Log on to the *ACM console*.
2. In the top navigation bar, hover the mouse over **Singapore**, and select the desired region in the overlay.

3 Create configuration

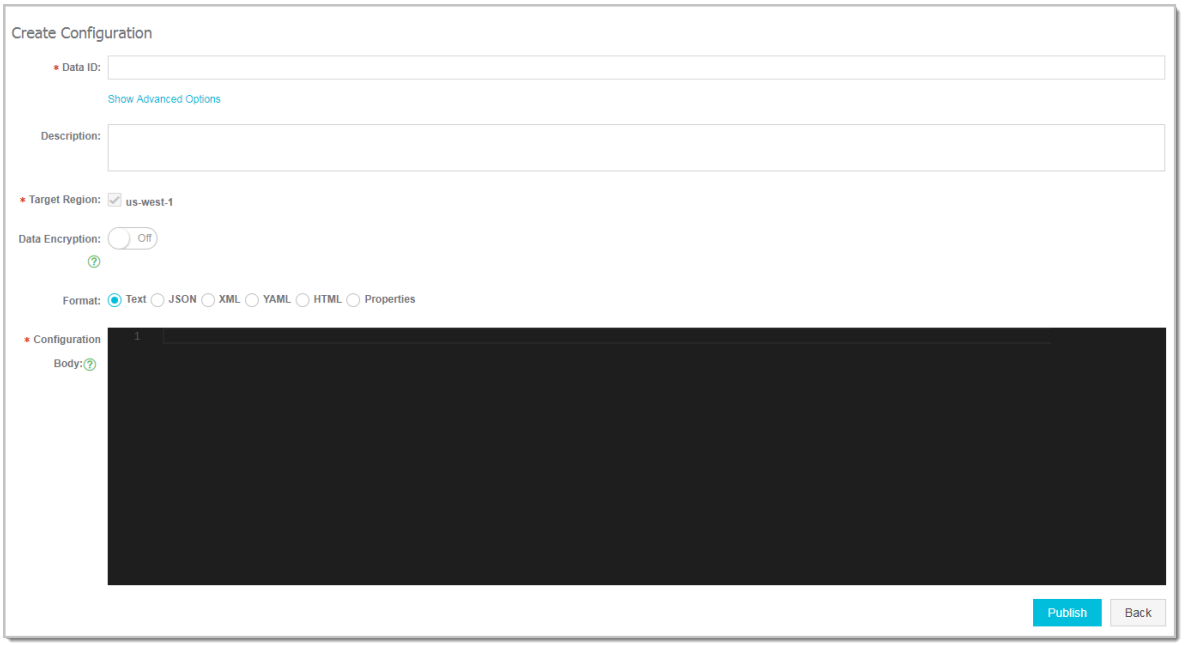
Some variables and parameters can be extracted from code to be managed in a configuration file. The configuration can be retrieved from the configuration file when the code is executed. By doing so, you can change parameters quickly and reduce the code maintenance costs. This topic explains how to create a configuration.

Procedure

1. Log on to the *ACM console*, and select a region as needed in the upper-left corner.
2. In the left-side navigation pane of the console, select **Configurations**, and then click the **+** icon on the right.



The **Create Configuration** page is displayed.



3. Enter the configuration information on the page according to the following table, and click **Publish**.

Note:

In ACM, the data model for a configuration is **<Namespace+DataId+Group, Content >**.

You don't need to apply for the **DataId** or **Group**, as long as they're unique in a *namespace*.

Table 3-1: Fields of the Create Configuration page

Field	Description
Data ID	Configuration ID. Use a naming rule like *package*.**class** (for example, *com.taobao.tc.refund.log*.**level**) to ensure global uniqueness. It is recommended to indicate business meaning of the configuration in the “class” section. All characters must be in lower case. Only English characters and four special characters (".", ":", "-", and "_") are allowed. It must not exceed 256 bytes.
Group	Configuration group (namespace). We recommend that you use product name (for example ACM) or module name to guarantee the uniqueness. You can perform authentication by group. Only English characters and four special characters (".", ":", "-", and "_") are allowed. It must not exceed 128 bytes.
Tags	You can use tags to manage configurations according to your own dimensions. Up to 5 tags are allowed, and the maximum length of each tag is 32 characters.
Description	Configure description information to help others understand the meaning of the configuration. Up to 128 characters are allowed.
Application	Name of the application associated with the configuration. Only English characters and four special characters (".", ":", "-", "_") are allowed.
Target Region	Most users publish the configuration to the current region only. To publish the configuration to multiple regions, select all target regions.

Field	Description
Data Encryption	If the configuration contains sensitive data, we recommend that you use encrypted storage function to minimize the risk of data leakage. You must activate Key Management Service (KMS), and authorize ACM to encrypt and decrypt with your KMS before you can use this function, because ACM data encryption function uses KMS to encrypt configurations. Note that the Data ID of an encrypted configuration always begins with `cipher-` . For more information, see *#unique_7*.
Format	Select a format to have ACM validate the syntax and format for you.
Configuration Body	The body of the configuration. A size of less than 10 KB is preferred, and do no exceed 100 KB at the maximum.

Related documents

Namespaces

#unique_7

4 Managing configurations

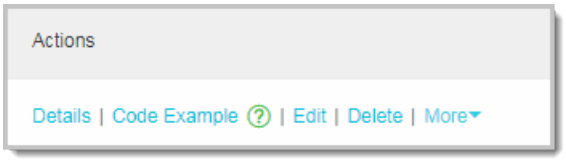
After you create a configuration item, you can use the configuration in the code. You may need to change configurations, so the ACM console is frequently used. You can search for, view, edit, and delete configurations in the ACM console.

Search for configurations

The ACM console supports searching for a configuration using the Data ID, Group ID, or a combination of both.

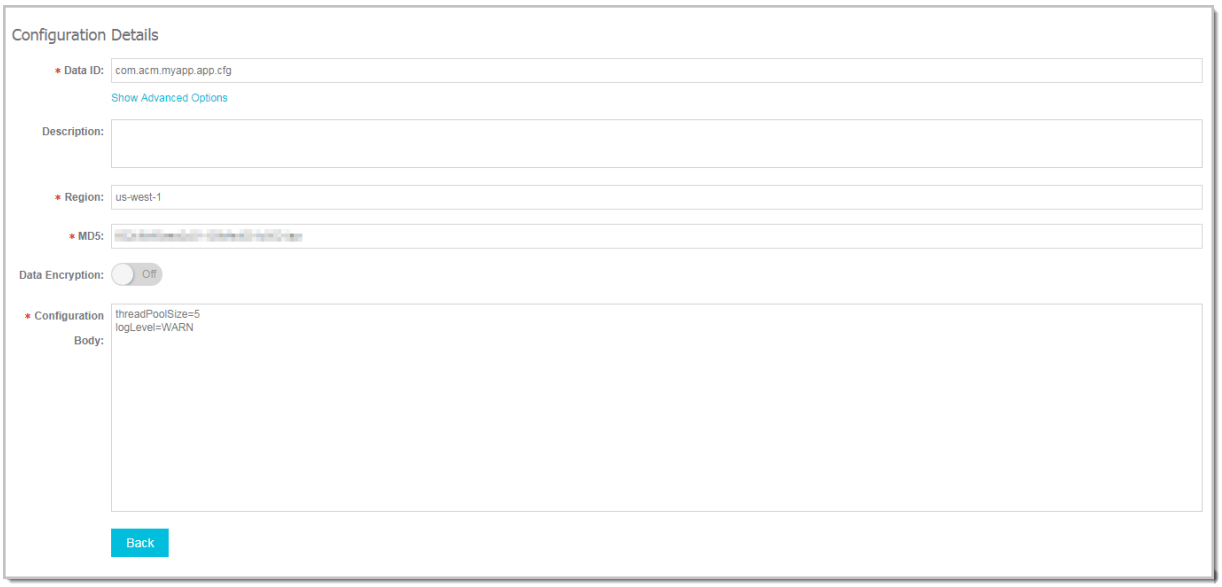
To search for a configuration, follow these steps:

1. Log on to the *ACM console*, and select a **Region** as needed in the upper-left corner.
2. Select **Configurations** in the left-side navigation pane of the console. Enter the information you want to search for, and click the **Search** button.
3. After the target configuration is found, you can view the details of the configuration, or change or delete the configuration, as shown in the following figure.



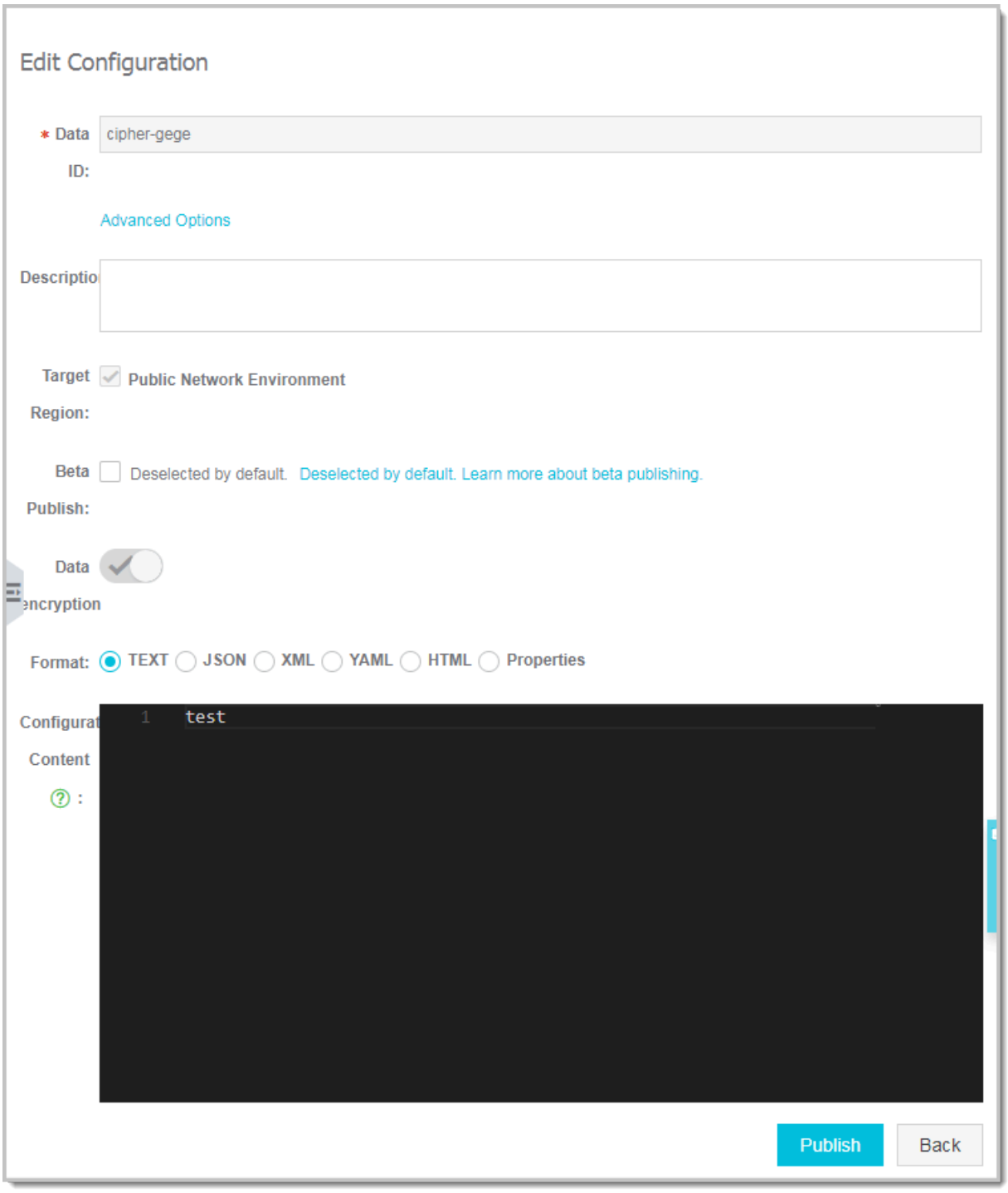
View configuration details

Click **Details** in the search results to view detailed information about a specific configuration.



Edit configurations

In the search result, click **Edit** to go to the editing page.



ACM offers the following advanced features on the configuration editing page.

Feature	Description	Usage
Format validation	Provides syntax validation for JSON or XML format. Select a format in the Format field to perform syntax validation for that specific format, which helps reduce issues caused by syntax errors.	Select the format of the text in the **Format** field before editing the configuration content.
Comparison of changes	ACM supports comparing changes when a changed configuration is submitted for publishing. Check the changes prior to publishing to reduce misoperations.	After the configuration is changed, click **Publish** to open the content comparison dialog box.
Beta Publish	An error in key configuration changes may cause a major fault, so it is recommended to publish the changed configurations to a few machines for verification first. By only pushing to all machines after the changes are proven to be safe, you can minimize the impact of errors in changes.	Check the **Beta Publish** checkbox, and enter the IP address of the machines for beta publish (enter the public IP for a local test).

Delete configurations

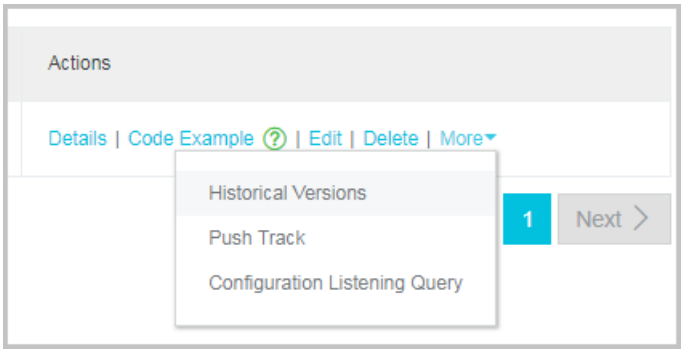
Click **Delete** to delete a configuration.

5 Query and rollback versions

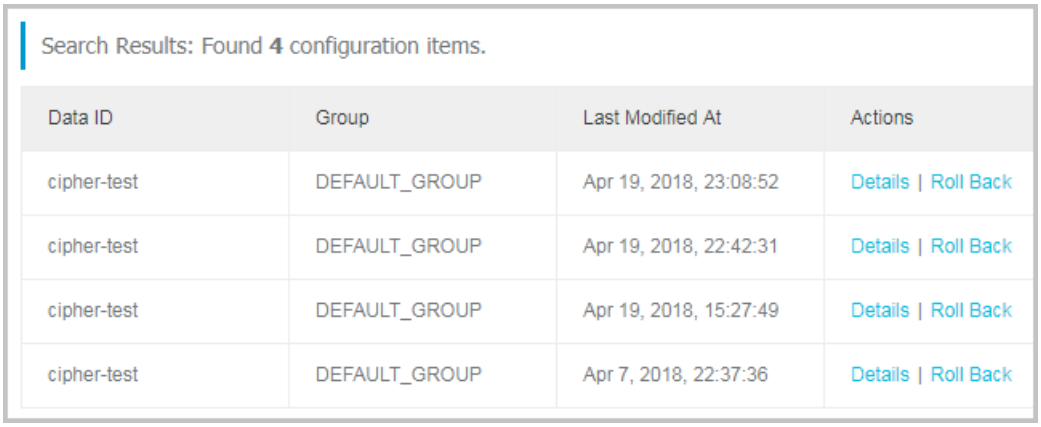
If you made a mistake when changing a configuration item, you need to roll back immediately. ACM supports querying configuration change history and rolling back configurations.

Procedure

1. In the left-side navigation pane, select **Configurations** , enter the **Data ID** or **Group** of the configuration to be queried, and then click **Search**.
   Matching results appear in the list.
2. In the search results, select **More** > **Historical Versions** on the right side of the target configuration.



The **Historical Versions** page is displayed.



3. Perform the following tasks as needed on the page.
   - To view the configuration content of a specific version, click **Details** in the **Actions** column.
   - To roll back to a specific version, click **Roll Back** in the **Actions** column, and on the **Configuration Rollback** page, click **Roll Back**.

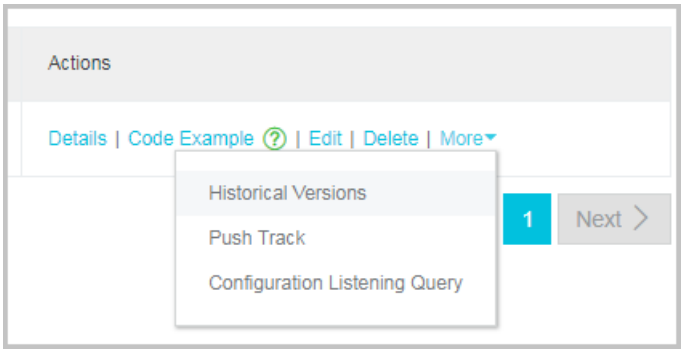
Note:
ACM currently saves change histories of up to 30 days.

6 View push status

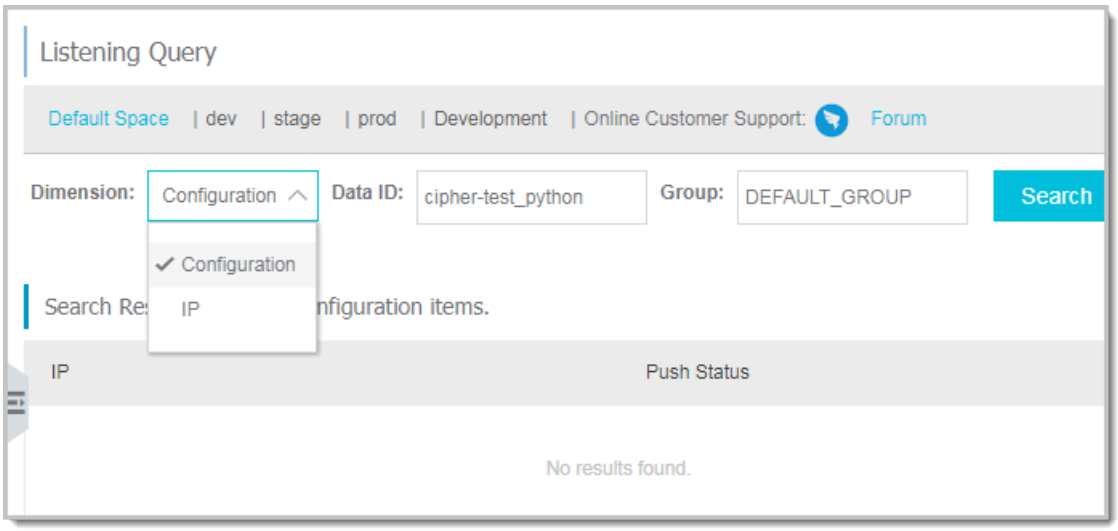
After changing a configuration, you might want to check whether the changed configuration has been pushed to the machine which is listening for this configuration. This query is only effective for clients that use the configuration listening API to listen for configurations.

Procedure

1. In the left-side navigation pane of the console, select **Configurations**, enter the **DataID** or **Group** of the configuration to be queried, and then click **Search**.
   Matching results appear in the list.
2. In the search results, select **More** > **Configuration Listening Query** on the right side of the target configuration.



The **Listening Query** page is displayed.



3. Enter the **Dimension**, **DataID**, or **Group** on the page, and then click **Search**.

Note:

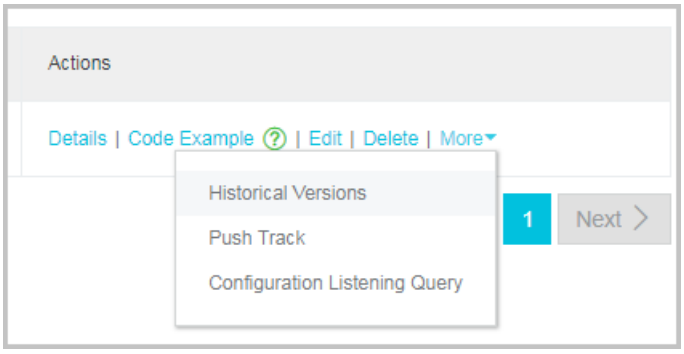
- If the dimension is set to **Configuration**: search the machines to which this configuration is pushed and the push status.
- If the dimension is set to **IP**: search the list of configurations that this machine listens for.

7 Push track query

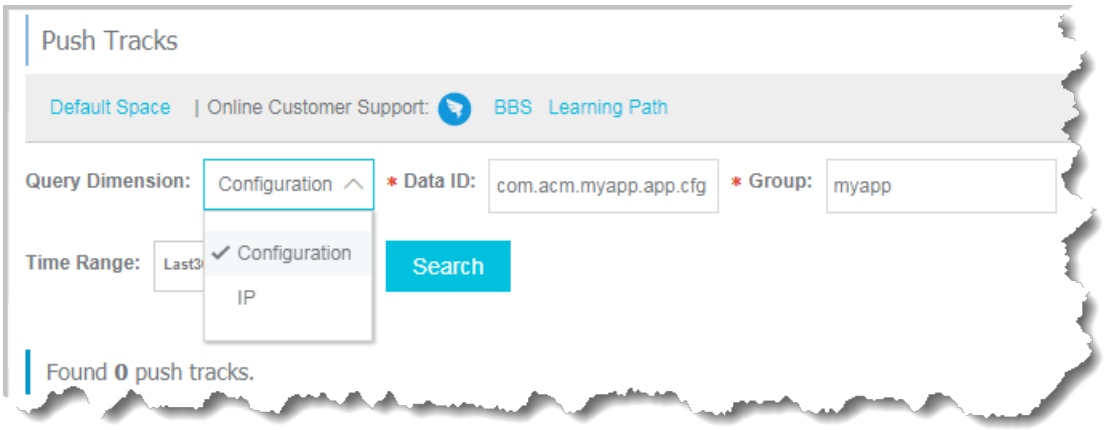
After changing a configuration, you can check whether the configuration has been successfully pushed according to the push track. If you find that the changed configuration does not take effect on a machine, you can follow the push track to check whether the configuration has been pushed to the machine.

Procedure

1. Select **Configurations** in the left-side navigation pane of the console. Enter the information you want to search for, and click the **Search** button.
   The matching search results appear in the list.
2. Click **More**and select **Push Track** in the dropdown list.



The **Push Track** page is displayed.



3. Enter the **Dimension**, **Data ID**, **Group**, and **Time Range**, and click **Search**.

Note:

- If you set the dimension to **Configuration**, the push track of the specified configuration will be queried.

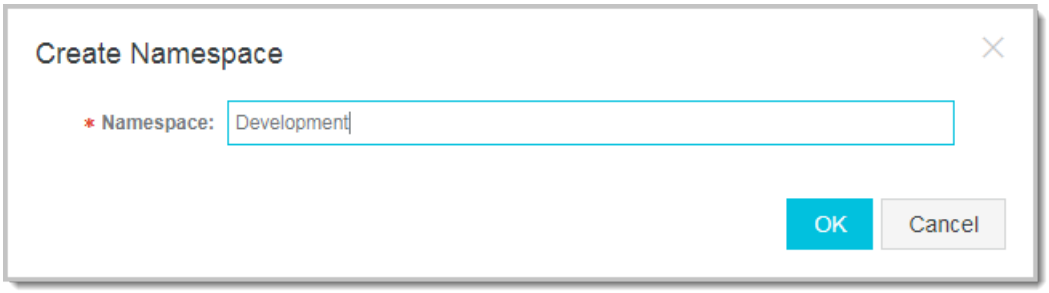
- If you set the dimension to **User IP**, the configuration access history of the specified client will be queried.

8 Create a namespace

When different configuration values are required in the official and test environments respectively, you can create namespaces to isolate the configurations in different environments. When the data of multiple product lines needs to be isolated, you can also allocate a namespace to each product line.

Procedure

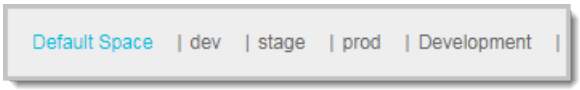
1. Log on to the *ACM console*, and select a region as needed in the upper-left corner.
2. In the left-side navigation pane of the console, click **Namespaces**.
   The **Namespaces** page is displayed.
3. In the upper-right corner of the page, click **Create Namespace**.
   The **Create Namespace** dialog box opens.



4. Enter a namespace name in the dialog box, and click **OK**.

> **Note:**
> Currently, one user can create up to five namespaces.

   For example, enter `Development`.
   The new namespace appears in the table on the **Namespaces** page, and the namespace selection area at the top of the **Configurations** page. The data of this namespace and that of other namespaces is completely isolated.



9 Sub-Account Management

The ACM system supports the Resource Access Management (RAM) account system of Alibaba Cloud. A primary account can create RAM sub-accounts, so that the account key is not shared with other users and only minimum permissions are assigned to these sub-accounts as necessary, thus enabling the enterprise to function efficiently.

About RAM sub-accounts

When using ACM, a primary account can enable clearly defined roles and responsibilities by assigning different roles and resources to its sub-accounts. This primary and sub-account permission model works in a similar way to the system and normal user model in the Linux system , where system users can grant or revoke permissions from normal users.

Description of RAM sub-accounts:

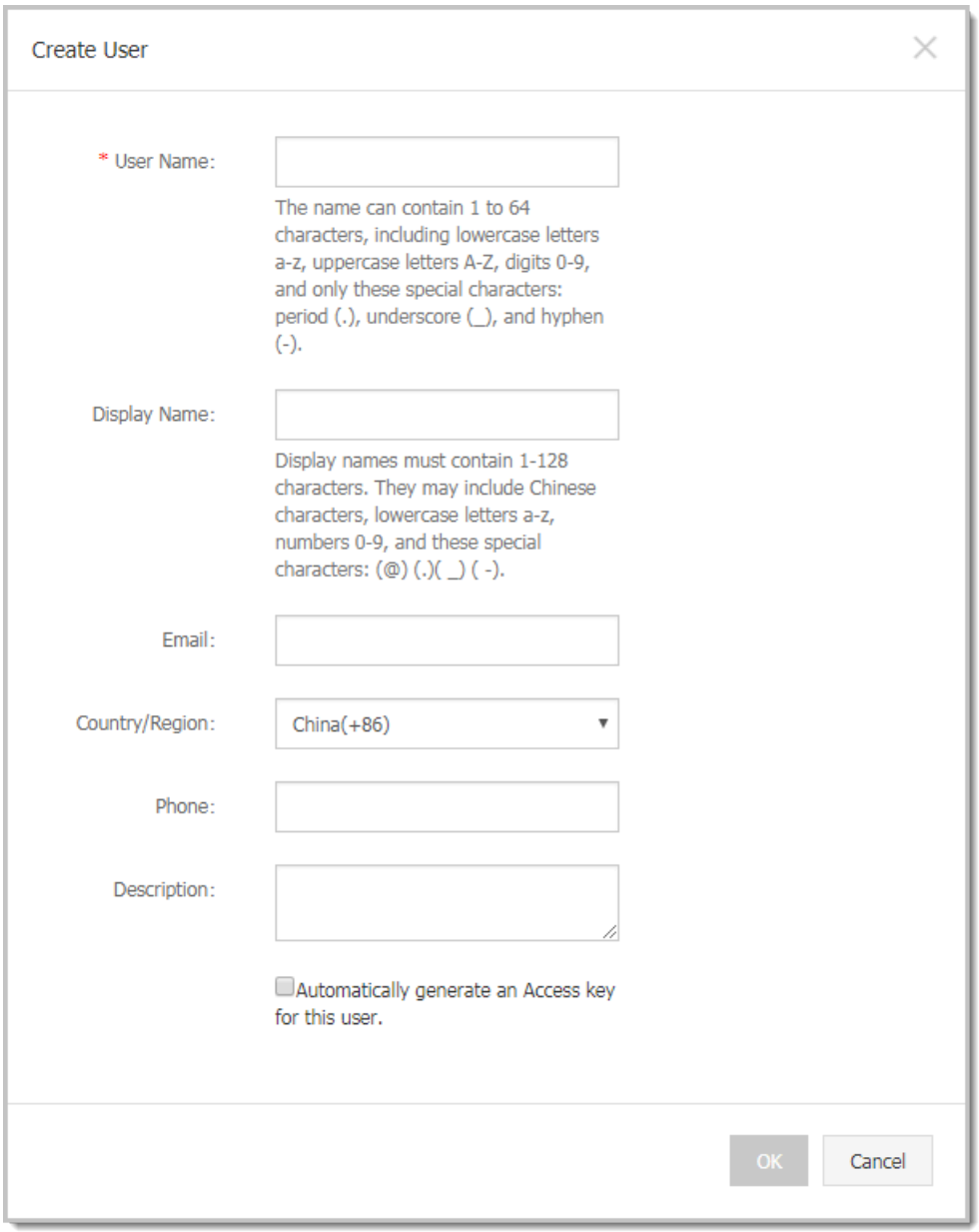
- RAM sub-accounts are created by a primary account in the RAM system. No legality verificati on is required provided that each sub-account under the same primary account has a unique name.
- Unlike logons with an Alibaba Cloud account, RAM sub-accounts log on through a unique logon entrance, which can be found in the RAM console.

Create a RAM sub-account

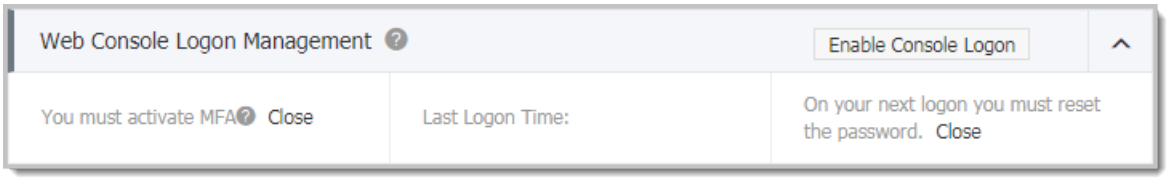
1. Log on to the *RAM console*, and click **Users** in the left-side navigation pane.
2. In the upper-right corner of the page, click **Create User**, and in the **Create User** dialog box, enter the login name and other information, and then click **OK**. The newly created user is displayed on the **Users Management** page.

Note:

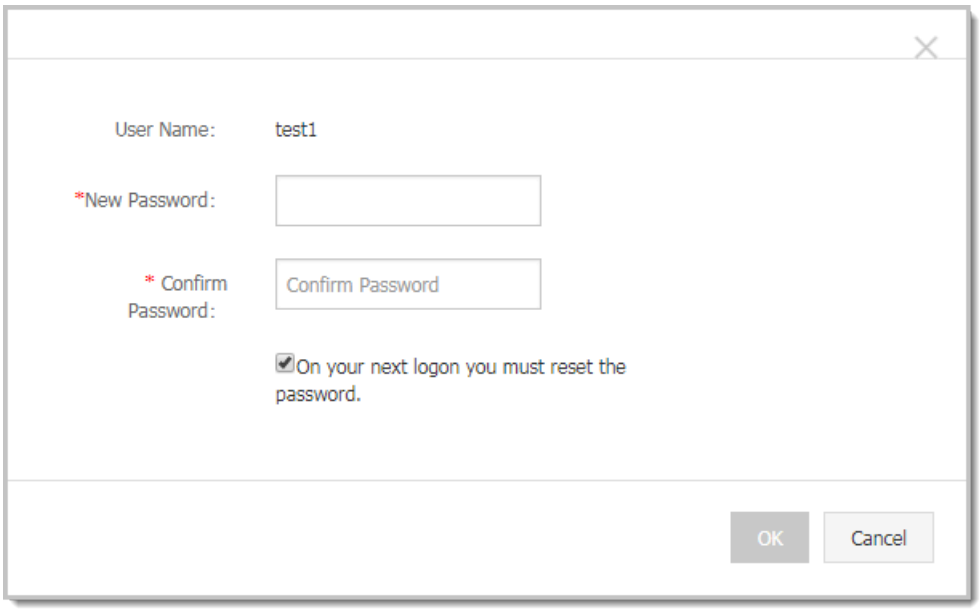
The login name must be unique within the primary account.



3. Click the user's **User Name/Display Name**. The **User Details** page is displayed.



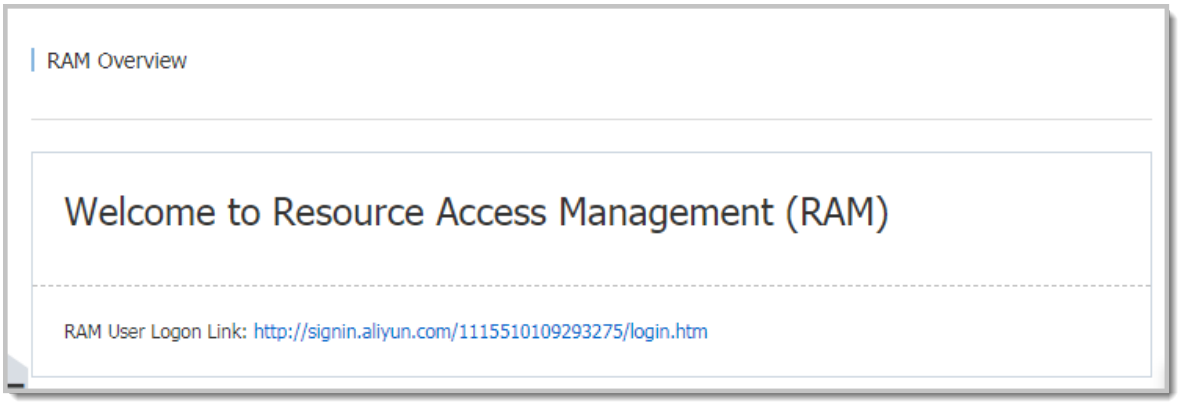
4. In the **Web Console Logon Management** section, click **Enable Console Logon**.
5. In the password setting dialog box, enter a **New Password** and **Confirm Password**, select the check box **"On your next logon you must reset the password."** as needed, and then click **OK**.



So far, a RAM user that can log on to the console is created.

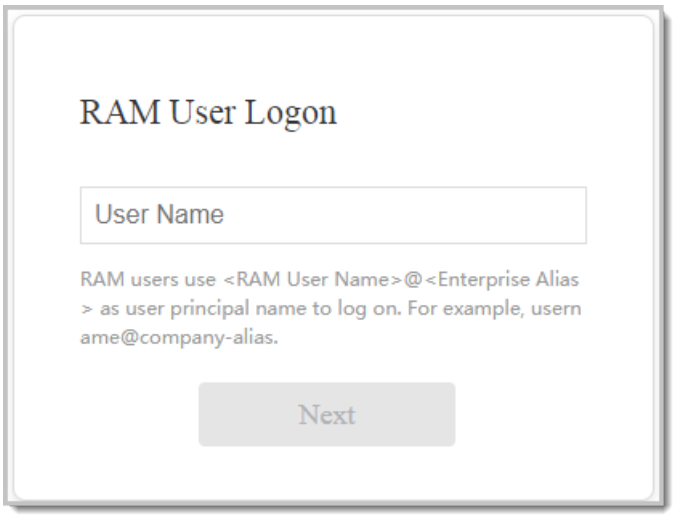
Log on to the ACM console with RAM sub-account

1. Log on to the *RAM console*, and in the left-side navigation pane, click **Dashboard**.
2. Click the **RAM User Logon Link**. The **Sub-account Logon** page is displayed.

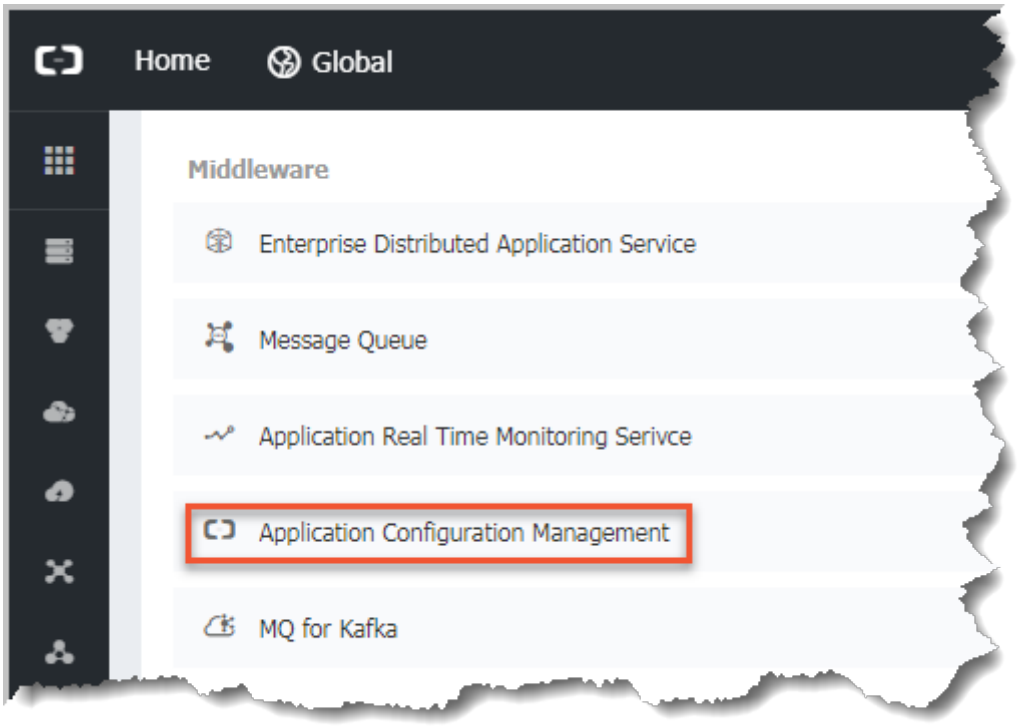


Note:
The RAM user's logon link varies with the primary account.

3. Enter information as prompted on the page, and enter the RAM console of the RAM sub-account.



4. In the RAM console, navigate to the **Products & Services** section, and in the Middleware area, click **Application Configuration Management** to enter the ACM console.



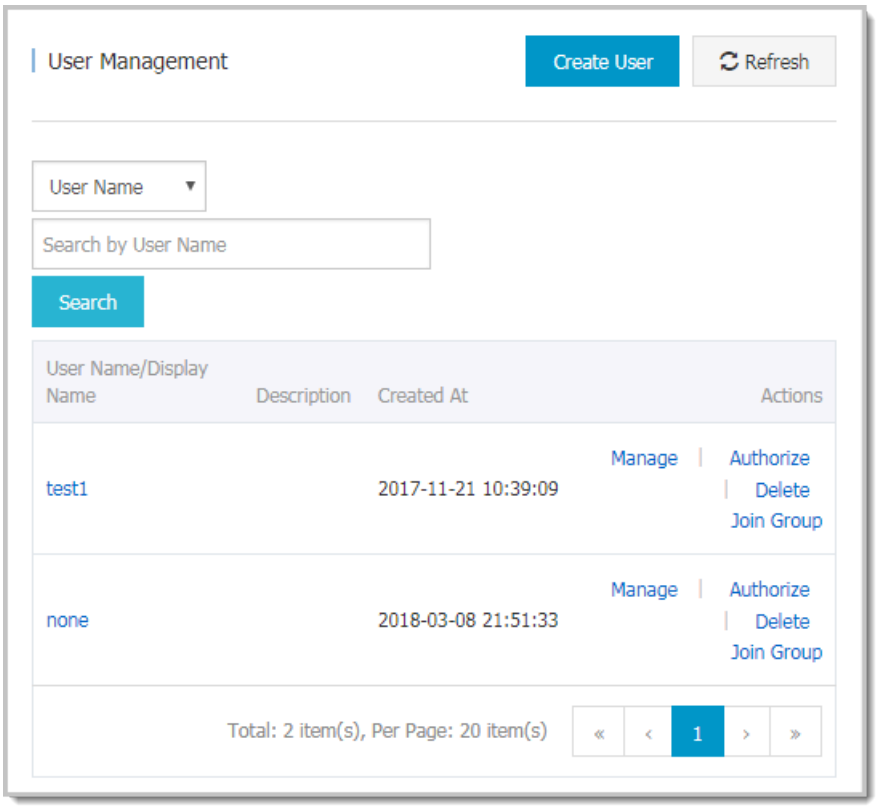
Authorize a RAM sub-account

The authorization of RAM is done on the level of ACM service, which means a user with RAM authorization has the full access to ACM. You can only grant or revoke the RAM authorization in the RAM console.

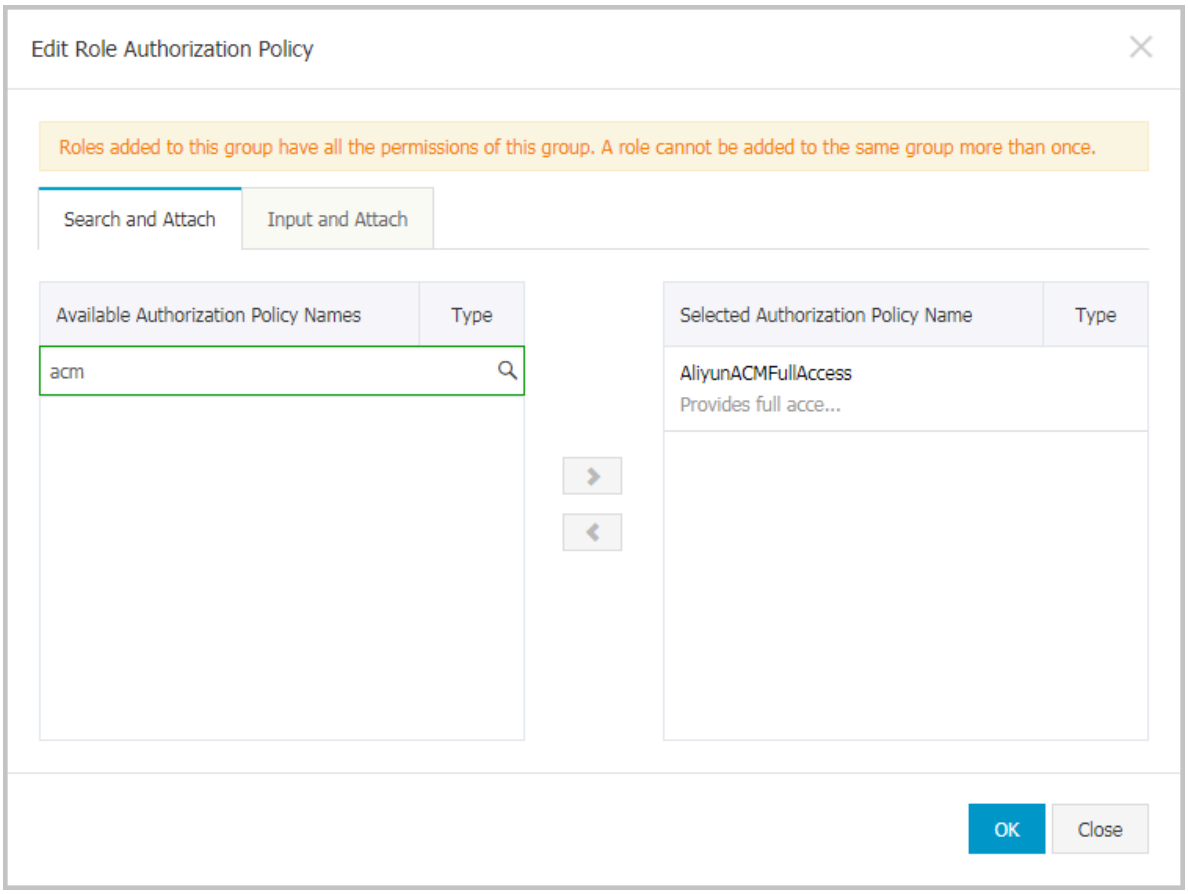
Here are the steps to authorize a RAM sub-account:

1. Log on to the *RAM console*, and click **Users** in the left-side navigation pane.

2. On the **Users Management** page, select a user to be authorized, and in the **Actions** column on the right side of the user, click **Authorize**.



3. In the search box of the **Edit User-Level Authorization** dialog box, enter ACM, select **AliyunACMFullAccess** to add it to the **Selected Authorization Policy Name** on the right, and then click **OK** to grant this sub-account all access to ACM. In addition, to use the *encryption and decryption* functions of ACM, also add the **AliyunKMSCryptoAccess** authorization policy.



After the authorization is complete, the sub-account can log on to the ACM console.

Deauthorize a RAM sub-account

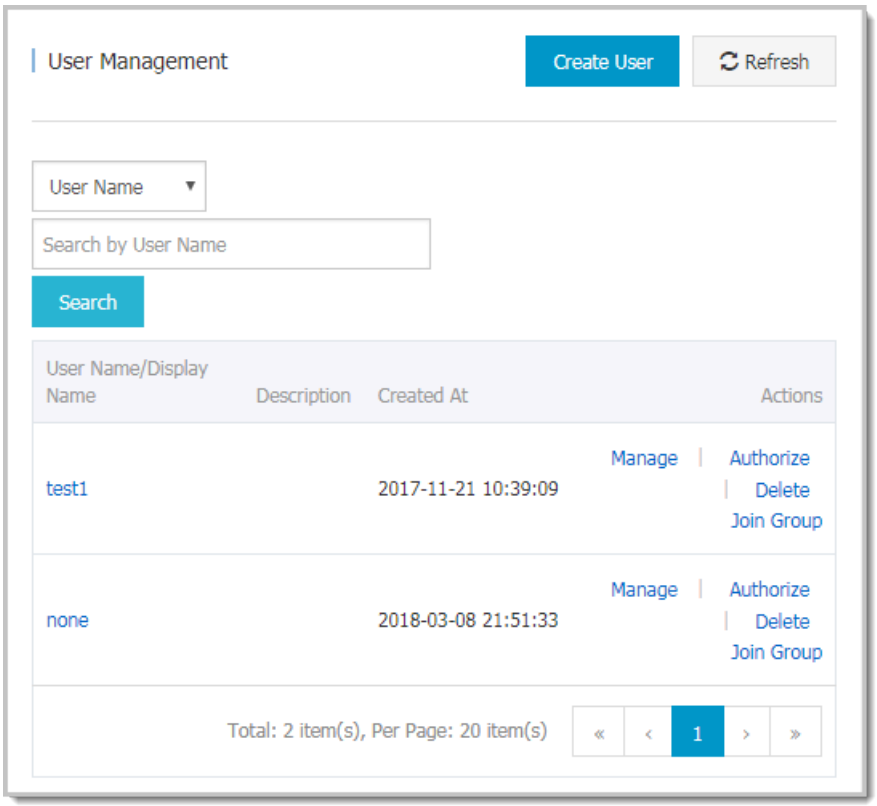
Here are the steps to deauthorize a RAM sub-account:

1. Log on to the *RAM console*, and in the left-side navigation pane, click **Users**.
2. On the **Users Management** page, select a user to be deauthorized, and in the **Actions** column on the right side of the user, click **Authorize**.
3. Move the **AliyunACMFullAccess** policy from the the right-side area to the left-side area, and click **OK**.

Once deauthorized, the RAM sub-account cannot log on to the ACM console.

Unbind a RAM sub-account

1. Log on to the *RAM console*, and in the left-side navigation pane, click **Users**.
2. On the **Users Management** page, select a user to be unbound, and in the **Actions** column on the right side of the user, click **Delete**.


User Management
Create User
Refresh
User Name
Search by User Name
Search
User Name/Display Name
Description
Created At
Actions
test1
2017-11-21 10:39:09
Manage | Authorize | Delete Join Group
none
2018-03-08 21:51:33
Manage | Authorize | Delete Join Group
Total: 2 item(s), Per Page: 20 item(s)
1

10 Access control

This topic explains how to use the access control functionality of ACM with an example of authorize a RAM user to use a namespace.

Background information

Previously, once granted the AliyunACMFullAccess authorization, a RAM user immediately has the full access to ACM, including the read and write access to all configurations and all namespaces. Given that the configurations of different RAM users are not isolated, misoperations or malicious operations can cause significant losses and severe consequences. More importantly, sensitive configurations such as database accounts and passwords are facing the risk of leakage due to their visibility to all authorized users.

Now, ACM provides access control of finer granularity, so that you can grant minimal access to users, and grant different users (or roles) different resource operation permission. Mirroring RAM's authorization policy, access can be granted in terms of Action or Resource.

Action

- Read: can read all configurations in the scope specified by Resource, and read the basic information of namespaces. The corresponding RAM authorization policy Action is `acms: R`.
- Write: can add, delete, or modify all configurations in the scope specified by Resource, but cannot add, delete, or modify namespaces. The corresponding RAM authorization policy Action is `acms: W`.
- Full access: can read and write all configurations in the scope specified by Resource, and read the basic information of namespaces. Also can add, delete, or modify namespaces if Resource is `*`. The corresponding RAM authorization policy Action is `acms:*`.

Resource

- All resources: the corresponding Ram Authorization Policy Resource is `*`.
- A single namespace: For example, if the namespace is `1ca01ca0-11b0-1e01-0df1-d1010101bc10,` then the RAM authorization policy Resource is `*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10`.
- A group within a single namespace: For example, if the namespace is `1ca01ca0-11b0-1e01-0df1-d1010101bc10`, and the group is `DEFAULT_GROUP`, then the RAM authorization policy Resource is `*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP`.

Step 1: Create a custom RAM authorization policy

1. Log on to the *RAM console*.
2. In the left-side navigation pane, click **Policies**.
3. In the upper-right corner of the **Policy Management** page, click **Create Authorization Policy**.
4. On the **Select an authorization policy** page of the **Create Authorization Policy** dialog box, click **Blank Template**.
5. On the **Edit permissions and submit** page, enter your custom authorization policy name, description, and policy content, and then click **Create Authorization Policy**.

   For example, to configure the read and write access for namespace `1ca01ca0-11b0-1e01-0df1-d1010101bc10`, please enter the following content in the **Policy Content** textbox:

   ```
   {
   "Version": "1",
   "Statement": [
    {
      "Action": [
        "acms:*"
      ],
      "Resource": "*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10",
      "Effect": "Allow"
    }
   ]
   }
   ```

   Note:
   For instructions on how to create a custom RAM authorization policy, see *#unique_15*.

Step 2: Create a RAM user

1. Return to the *RAM console*.
2. In the left-side navigation pane, click **Users**.
3. Click **Create User** in the upper-right corner of the **User Management** page, and enter the user name and other information in the **Create User** dialog box.

   Note:
   To generate an AccessKey, select **Automatically generate an Access key for this user**.
   Newly created users don't have any permissions. You must authorize them first.
4. In the table on the **User Management** page, click the name of the user created at the previous step.
5. In the **Web Console Logon Management** area of the **User Details** page, click **Enable Console Logon** on the right side, and set the password for the user.

6. In the left-side navigation pane, click **User Authorization Policies**, and click **Edit Authorization Policy** in the upper-right corner of the page.
7. In the **Edit User-Level Authorization** dialog box, search for the authorization policy created at the previous step with keywords, click the **>** button to move it to the **Selected Authorization Policy Name** list on the right, and then click **OK**.

> **Note:**
>
> For instructions on how to create and authorize RAM users, see *#unique_16* and *#unique_17*.

Step 3: Log on with the RAM user and verify the access

1. Return to the *RAM console*.
2. On the **Dashboard** page, click the RAM User Logon Link, and log on with your newly created user.
3. Go to the ACM console, and verify if only the namespace specified in the authorization policy can be manipulated.

More examples

1. Grant the read-only access to a single namespace (for example `1ca01ca0-11b0-1e01-0df1-d1010101bc10`)

```
{
"Version": "1",
"Statement": [
 {
   "Action": [
     "acms:R"
   ],
   "Resource": "*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10",
   "Effect": "Allow"
 }
]
}
```

2. Grant the read and write access to a single group (for example `DEFAULT_GROUP`) within a single namespace (for example `1ca01ca0-11b0-1e01-0df1-d1010101bc10`)

```
{
"Version": "1",
"Statement": [
 {
   "Action": [
     "acms:*"
   ],
   "Resource": "*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/
DEFAULT_GROUP",
   "Effect": "Allow"
 }
]
```

```
}
```

3. Grant the read-only access to multiple groups (for example `DEFAULT_GROUP` and `DEFAULT_GROUP_1`) within a single namespace (for example `1ca01ca0-11b0-1e01-0df1-d1010101bc10`)

```
{
"Version": "1",
"Statement": [
 {
   "Action": [
     "acms:R"
   ],
   "Resource": [
           "*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/
DEFAULT_GROUP",
           "*:*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/
DEFAULT_GROUP_1"
       ],
   "Effect": "Allow"
 }
]
}
```

4. Grant the read and write access to a single group (for example DEFAULT_GROUP) within all namespaces

```
{
"Version": "1",
"Statement": [
 {
   "Action": [
     "acms:*"
   ],
   "Resource": [
           "*:*:*:*:cfg/*/DEFAULT_GROUP"
       ],
   "Effect": "Allow"
 }
]
}
```

Note

- Only when the authorization policy *Action* is `acms:*`, and the *Resource* is `*`, users (or roles) granted this policy can add, delete, or modify namespaces.
- Due to the cache system, it usually takes about 10 seconds for added and modified authorizat ion policies to be effective.
- *#unique_18* : you can also achieve access control of finer granularity by granting the aforementioned authorization policy.

Related documents

- *#unique_19*

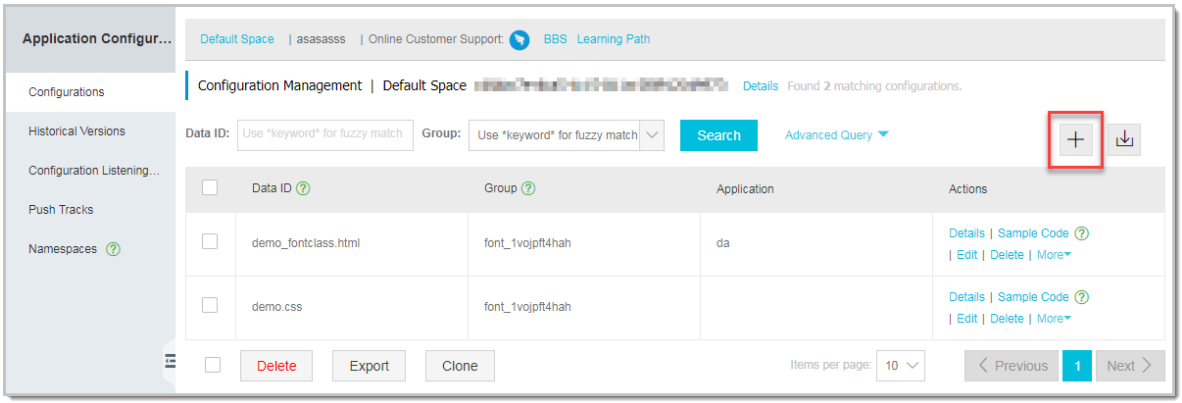
- *#unique_15*
- *#unique_16*
- *#unique_17*
- *#unique_20*
- *#unique_18*

11 Create and use encrypted configuration

ACM provides encrypted configuration to meet the requirement for sensitive configurations (data sources, tokens, usernames, passwords, and so on), and to lower the risk of leaking user configurations. An encrypted configuration is a configuration stored in an encrypted way. This topic explains how to create and use an encrypted configuration.

Create encrypted configuration

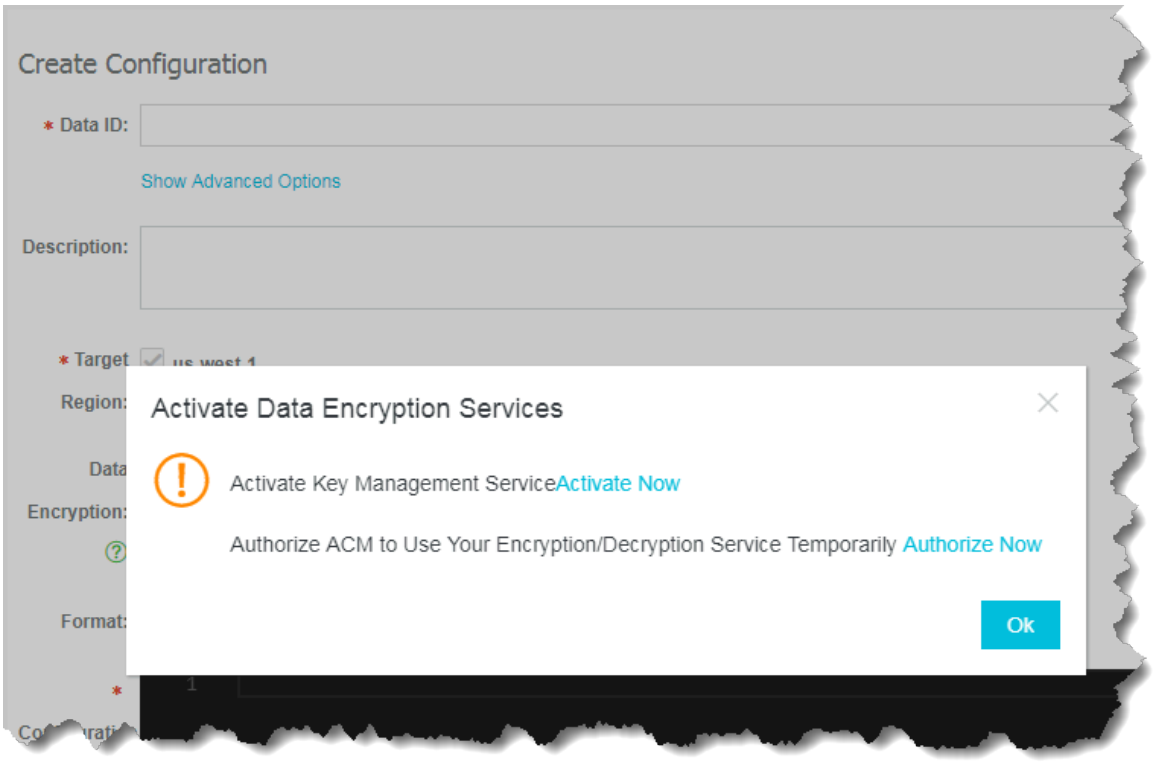
1. Log on to the *ACM console*.
2. In the left-side navigation pane of the console, click**Configurations**, and on the right side of the page, click the **+** icon.



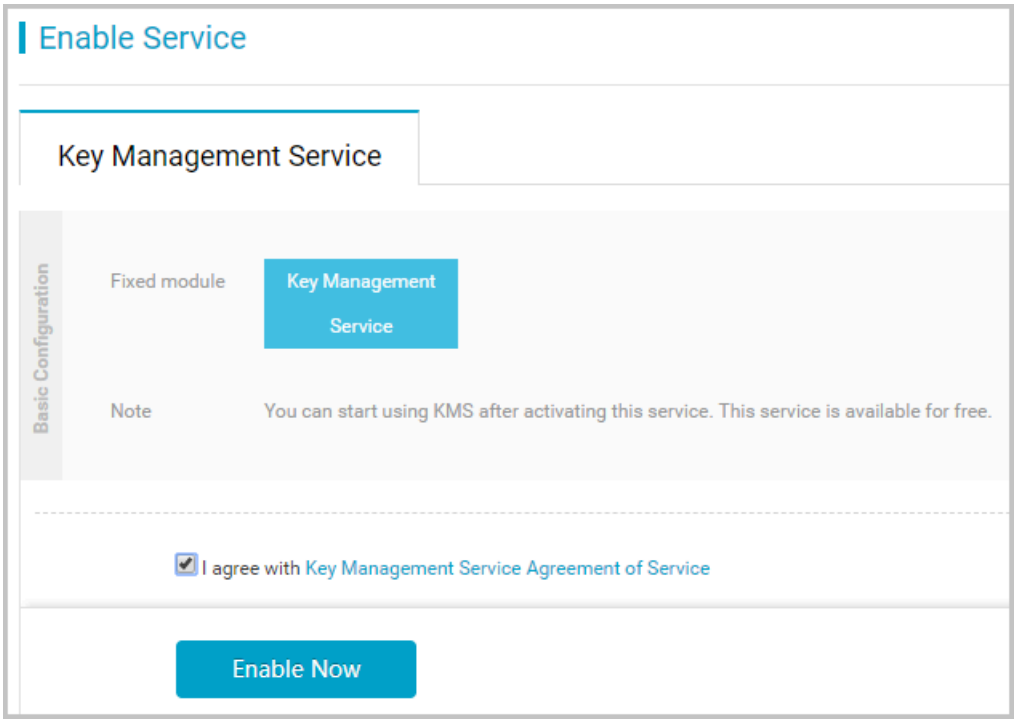
3. On the **Create Configuration** page, switch on **Data Encryption**.

> **Note:**
> When you use the data encryption function for the first time, the Activate Data Encryption Services dialog box appears. You must activate the key management service and authorize ACM to encrypt and decrypt with your key management service before you can use this function, because ACM data encryption function relies on key management service to encrypt configurations.

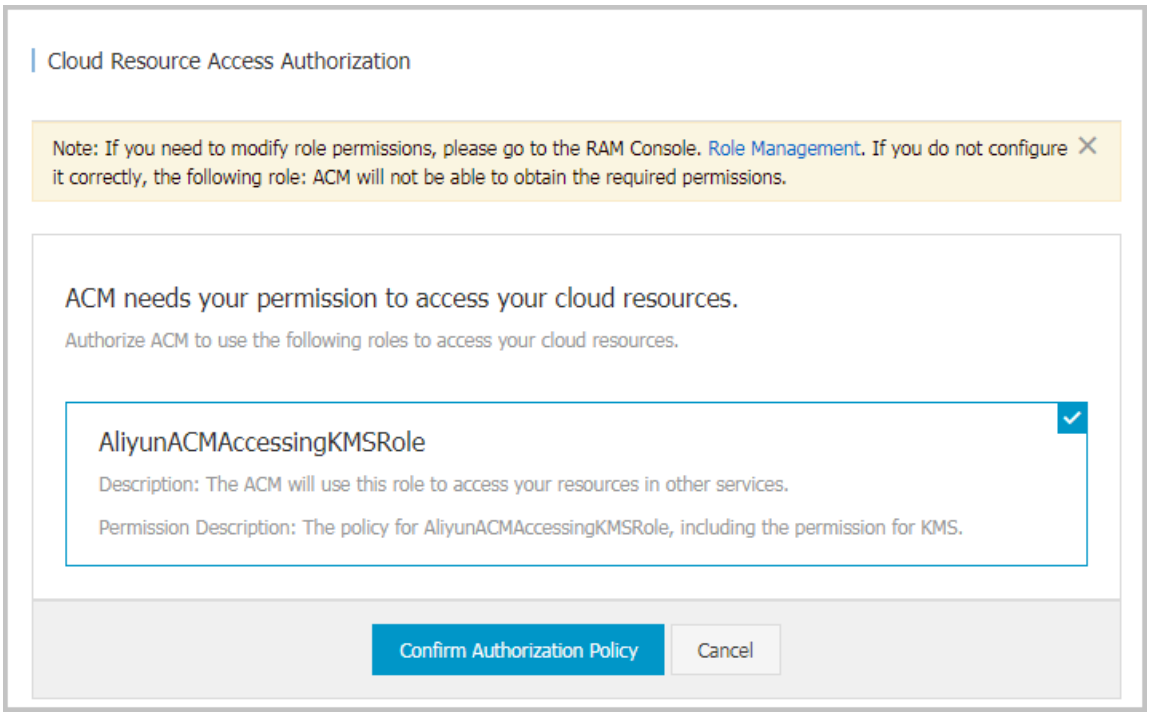
4. In the **Activate Data Encryption Services** dialog box, perform the following steps.



a. Click**Activate Now**. On the **Enable Service** page, select **I agree with Key Management Service Agreement of Service**, and then click **Enable Now**.



b. Click **Authorize Now**. On the **Cloud Resource Access Authorization** page, select the target permission, and click **Confirm Authorization Policy**.



5. On the **Create Configuration** page, enter the configuration content, and then click **Publish**.

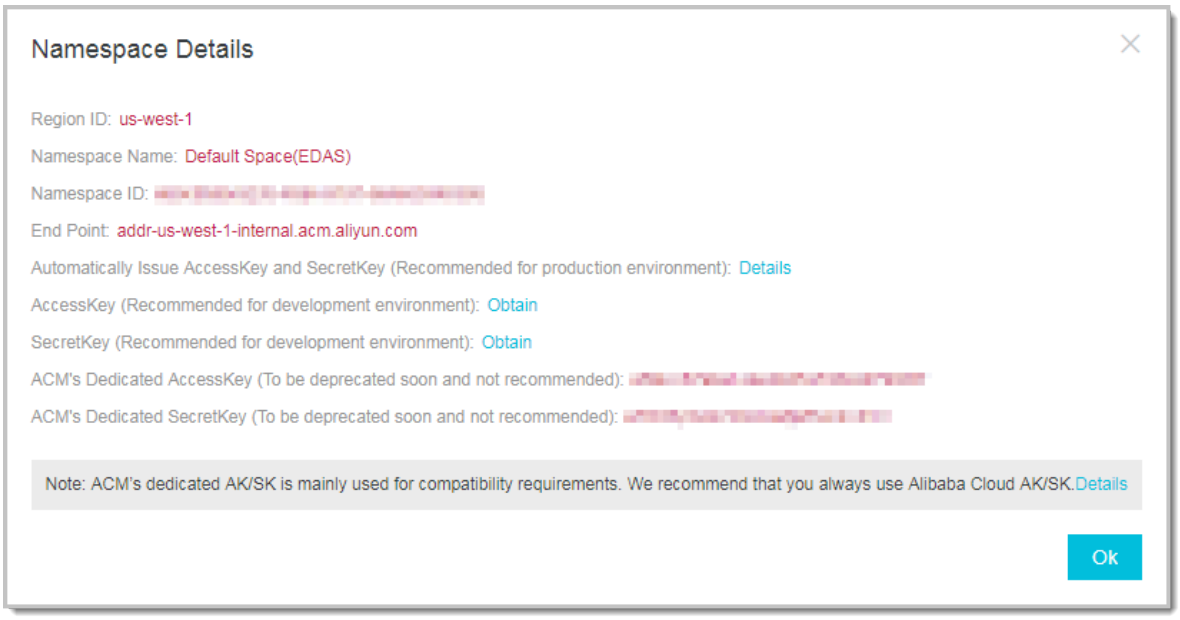
> **Note:**
> To make it easier for you to manage the configurations, everything is displayed in plain text in the console, although the configurations are actually encrypted.

Use encrypted configuration

1. Log on to the *ACM console*.
2. In the **Actions** column on the right side of the table, click **Code Example** to get sample code.

> **Note:**
> Java SDK and Python SDK has incorporated KMS-SDK, so you can add decryption filters for automatic decryption. For more information about decryption of other languages, see *Decrypt*.

3. Click **Details** above the Search button, and click **Obtain** in the **Namespace Details** dialog box to obtain the initialization parameters.



Note:

Although you can directly obtain the configuration data with the AccessKey/SecretKey of the primary account, we strongly recommend that you use the AccessKey/SecretKey of sub-accounts for the sake of security. If you use the AccessKey/SecretKey of sub-accounts, then you must grant the sub-account the AliyunACMFullAccess and AliyunKMSCryptoAccess permission. For more information, see *#unique_22*.

12 Access ACM with instance RAM role

This topic explains how to access ACM with the RAM role of ECS instances.

Overview

In the past, for an application deployed in an ECS instance to access ACM, the Access Key ID and Access Key Secret (“AK”) must be stored in the ECS instance as a configuration file or in other forms. However, this increases the complexity of AK management and the risk of leaking sensitive data.

Now, with the *RAM role of an instance*, you can associate a RAM role with an ECS instance, and then inform ACM SDK (Version 1.0.8 and later) of the name of this RAM role, so that you can access ACM without configuring AK later. In addition, with *RAM (Resource Access Management)*, you can also have multiple instances with different authorizations for ACM by tweaking their roles and authorization policies. For example, if assigned a role with a read-only authorization policy, an ECS instance can read ACM configurations but can’t add or modify one.

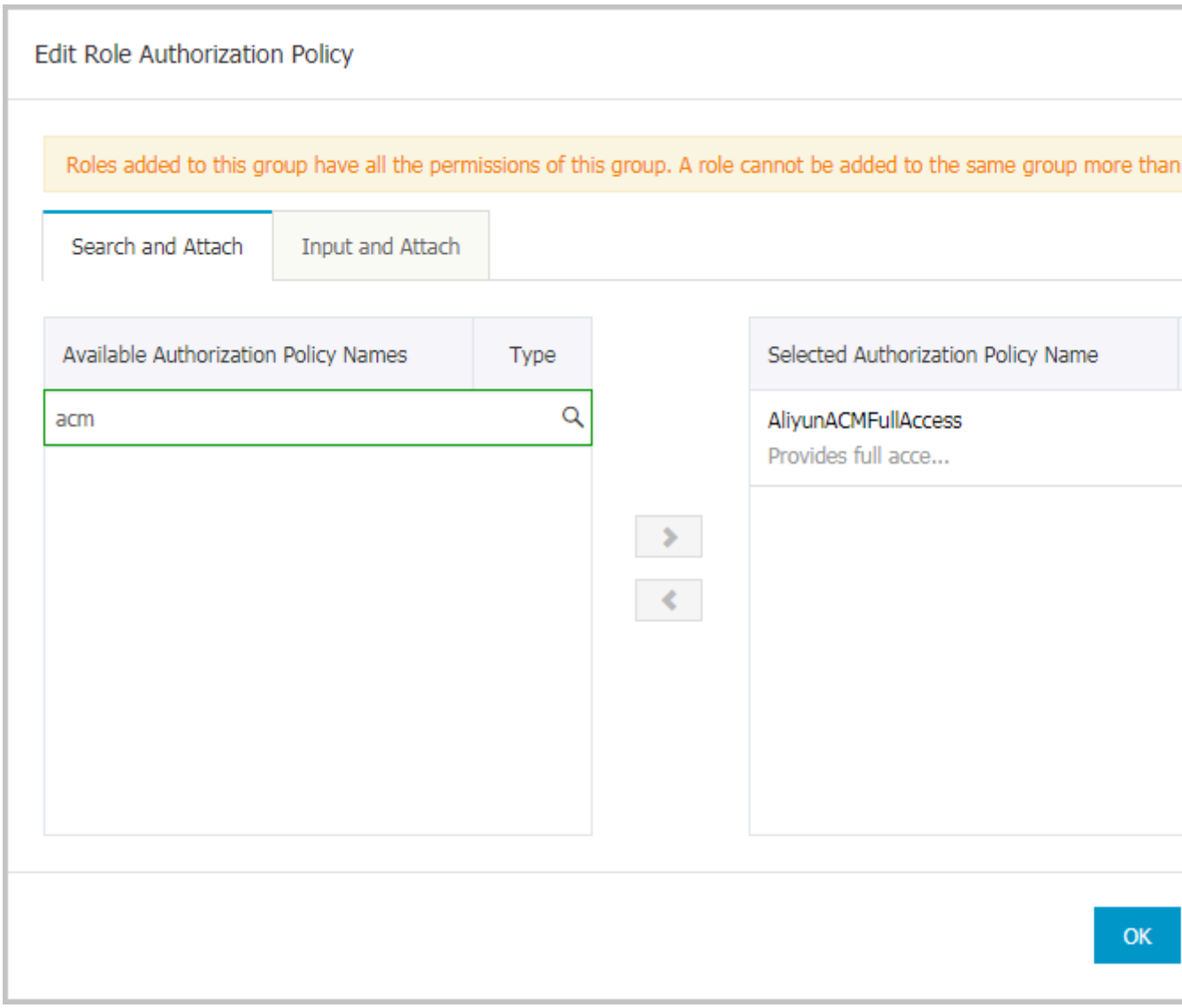
Prerequisites

You’re running a VPC network.

Step 1: Create a RAM role and configure the authorization policy

1. Log on to the *RAM console*. Click **Roles** in the left-side navigation pane.
2. Click **New** in the upper right corner of the page.
3. In the **Create Role** dialog box, complete the following steps.
   a. On the **Select Role Type** page, click **Service Role**.
   b. On the **Enter Type** page, select **ECS Elastic Compute Service**.
   c. On the **Configure Basic Information** page, enter a custom **Role Name** and optionally a **description**, and click **Create**.

   Note:
   A newly created role doesn’t have any authorizations.
4. In**Role management**Page, click to the right of the role**Operation**Of a column**Authorization**.
5. In the **Edit Role Authorization Policy** dialog box, search for the authorization policy `AliyunACMFullAccess`, and click the **>** button to move it to the right-side **Selected Authorization Policy Name** list, and then click **OK**. To use the configuration encryption and decryption features, add the `AliyunKMSCryptoAccess` authorization policy.



Now this role is granted all authorizations for ACM.

Step 2: Attach this RAM role to the ECS instance

1. Login*ECS Console*, Click on**Instance**.
2. Click the target ECs instance in the list**Operation**Of a column**More**, And select**Grant/recover Ram role**To grant this instance the role that was new in the previous step.

Step 3: Inform ACM SDK of the name of this RAM role and access configurations

You can inform ACM SDK (Version 1.0.8 and later) of the name of this RAM role in one the following ways:

- By setting a JVM parameter: `-Dram.role.name=$ramRoleName` (For example `-Dram.role.name=ECS-RAM`)
- By passing parameters with code

Note:

JVM parameter setting takes precedence over passing parameters with code.

This is how to pass parameters with code:

```
import java.util.Properties;
import com.alibaba.edas.acm.ConfigService;
import com.alibaba.edas.acm.exception.ConfigException;
// Sample code, for sample test only.
public class ACMTest {
    public static void main(String[] args) {
        try {
            Properties properties = new Properties();
            // Obtain the endpoint from "Namespace details" or "Sample
 code" in the ACM console
            properties.put("endpoint", "$endpoint");
            // Obtain the namespace from "Namespace details" or "
Sample code" in the ACM console
            properties.put("namespace", "$namespace");
            // The name of the newly created RAM role associated with
an ECS instance, for example "ECS-RAM"
            properties.put("ramRoleName", "$ramRoleName");
            ConfigService.init(properties);
            // Actively get the configuration.
            String content = ConfigService.getConfig("${dataId}", "${
group}", 6000);
            System.out.println(content);
        } catch (ConfigException e) {
            e.printStackTrace();
        }
    }
}
```

Related documents

- *RAM (Resource Access Control)*
- *#unique_24*
- *#unique_25*
- *#unique_26*