ALIBABA CLOUD

Alibaba Cloud

Application Configuration Management

Access Control

Document Version: 20220407

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings> Network> Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.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.

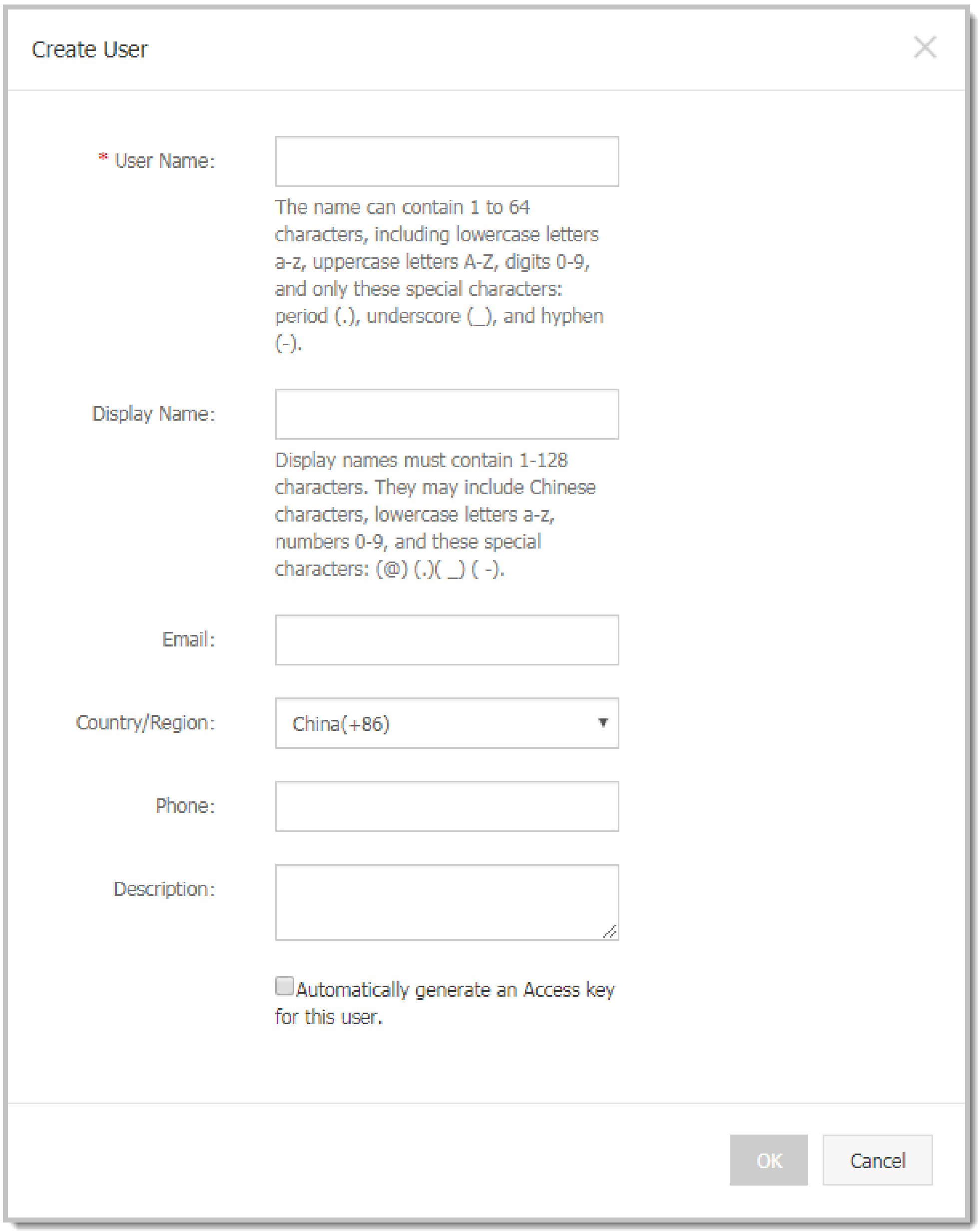
Description of RAM sub-accounts:

- RAM sub-accounts are created by a primary account in the RAM system. No legality verification 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.



Create User

* User Name:

The name can contain 1 to 64 characters, including lowercase letters a-z, uppercase letters A-Z, digits 0-9, and only these special characters: period (.), underscore (_), and hyphen (-).

Display Name:

Display names must contain 1-128 characters. They may include Chinese characters, lowercase letters a-z, numbers 0-9, and these special characters: (@) (.)(_) (-).

Email:

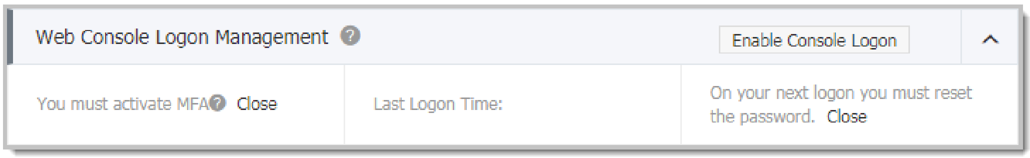
Country/Region: China(+86)

Phone:

Description:

□ Automatically generate an Access key for this user.

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



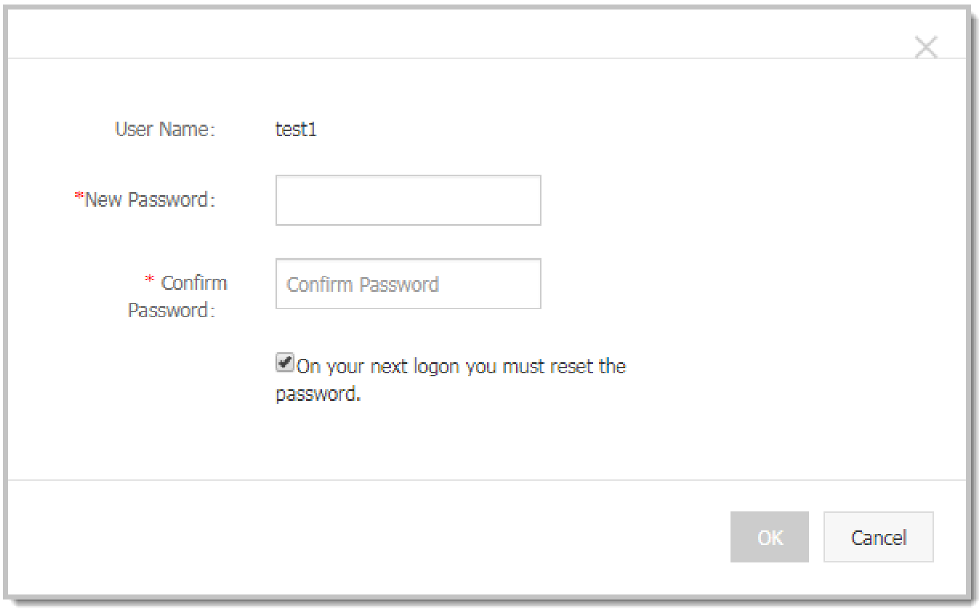
Web Console Logon Management

You must activate MFA Close

Last Logon Time:

On your next logon you must reset the password. Close

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**.



User Name: test1

*New Password:

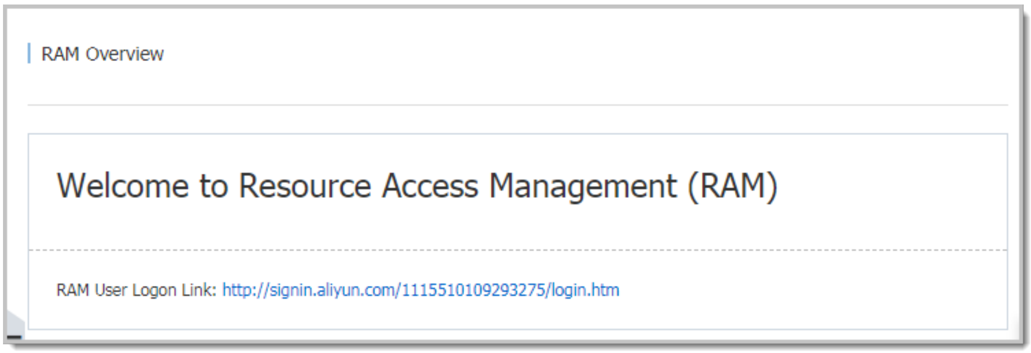
* Confirm Password: Confirm Password

☑ On your next logon you must reset the password.

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.



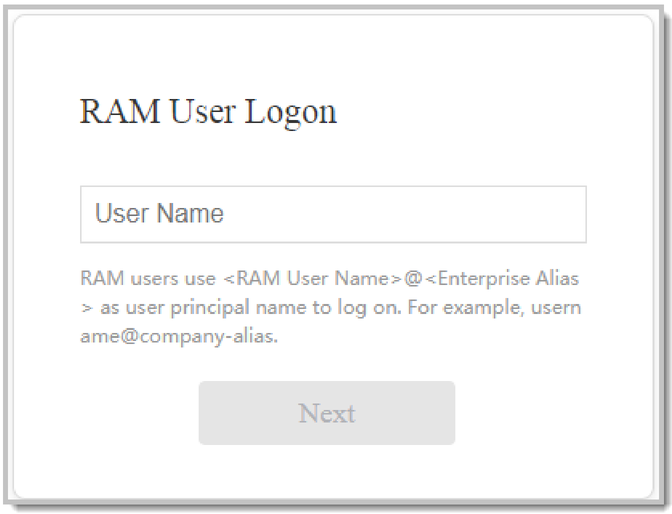
RAM Overview

Welcome to Resource Access Management (RAM)

RAM User Logon Link: http://signin.aliyun.com/1115510109293275/login.htm

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

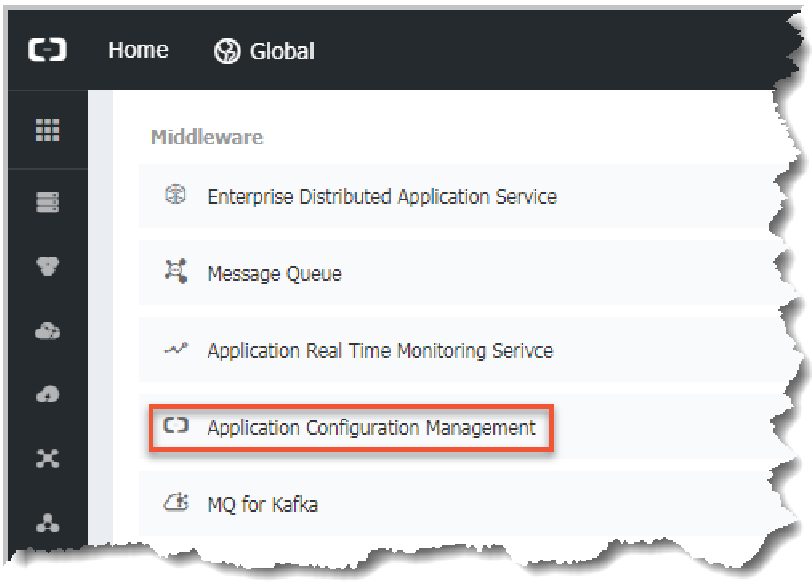
3. Enter information as prompted on the page, and enter the RAM console of the RAM sub-account.



RAM User Logon

RAM users use <RAM User Name>@<Enterprise Alias> as user principal name to log on. For example, username@company-alias.

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.



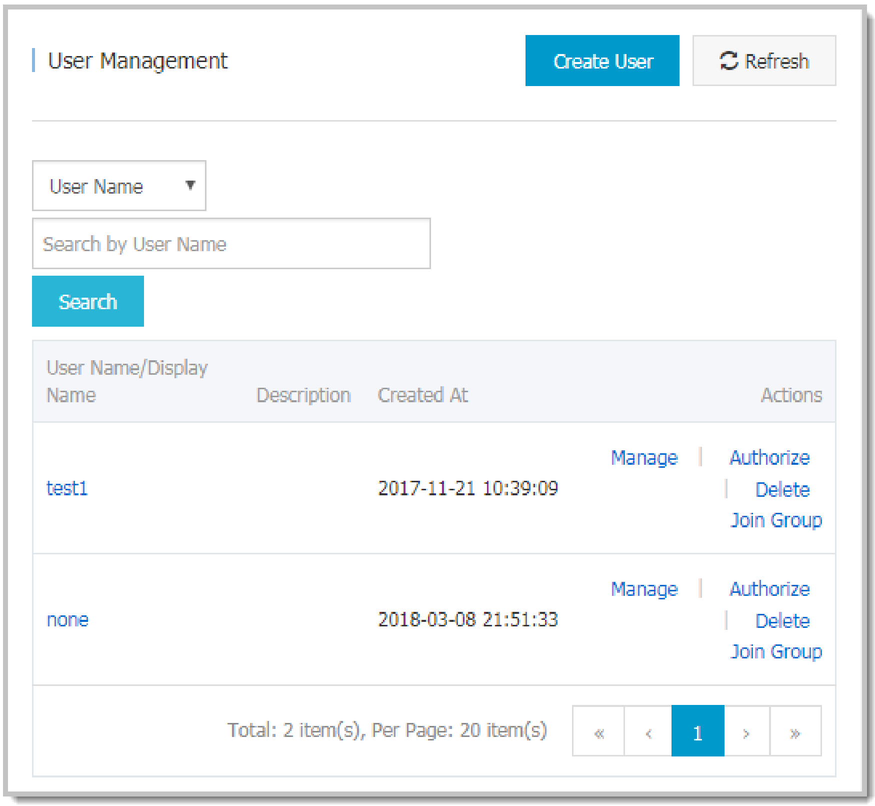
Home
Global
Middleware
Enterprise Distributed Application Service
Message Queue
Application Real Time Monitoring Serivce
Application Configuration Management
MQ for Kafka

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:

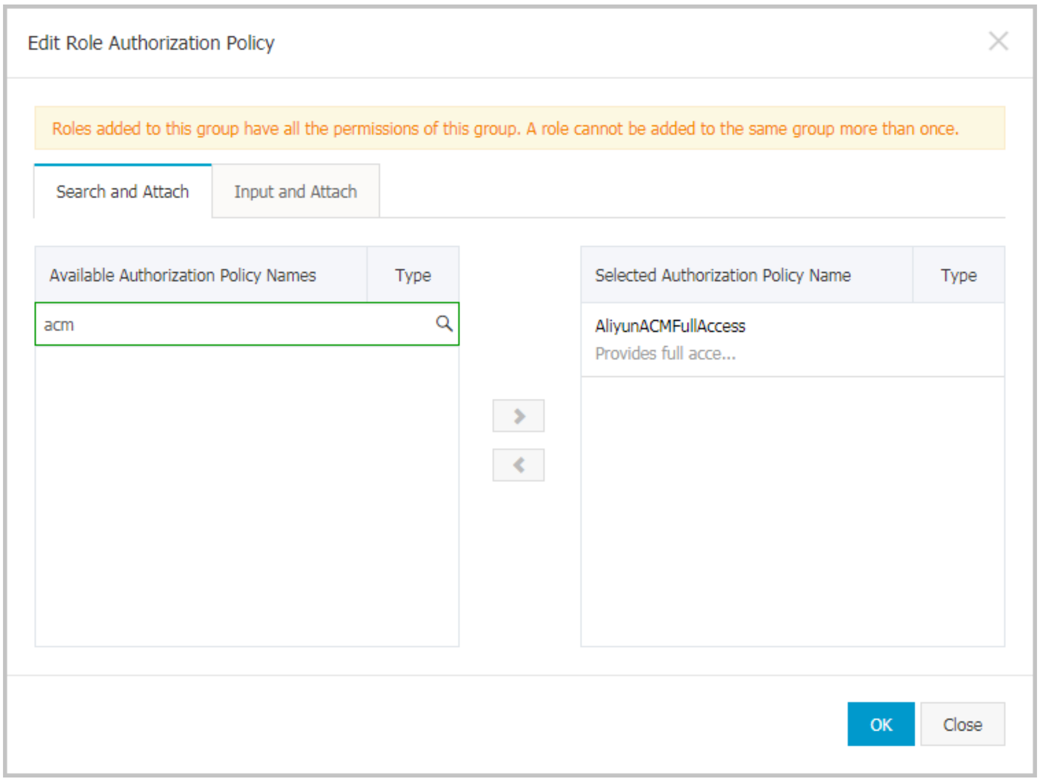
1. Log on to the RAM console, and click **Users** in the left-side navigation pane.
2. On the **Users Management** page, select a user to be authorized, and in the **Actions** column on the right side of the user, click **Authorize**.



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)

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.


Edit Role Authorization Policy

Roles added to this group have all the permissions of this group. A role cannot be added to the same group more than once.

Available Authorization Policy Names	Type
acm	

Selected Authorization Policy Name	Type
AliyunACMFullAccess Provides full acce...	

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

Deauthorize a RAM sub-account

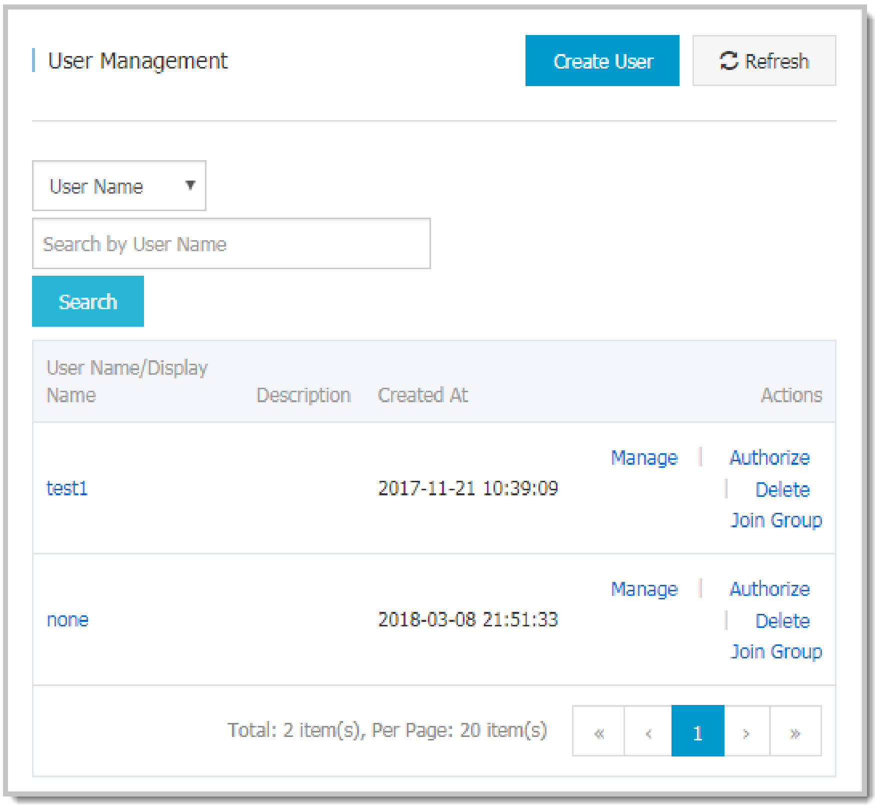
Here are the steps to deauthorize a RAM sub-account:

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 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)

2.RAM roles

Application Configuration Management (ACM) supports Alibaba Cloud Resource Access Management (RAM). By using RAM roles, you can access ACM resources in other cloud accounts.

(Old version) Create a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **Roles**.
2. On the Role Management page, click **Create Role** in the upper-right corner. In the **Create Role** dialog box, select a role type as needed on the **Select Role Type** tab.
   - **User Role**: RAM users under a trusted Alibaba Cloud account can assume this role to access your cloud resources. Trusted accounts can be the current Alibaba Cloud account or another Alibaba Cloud account.
   - **Service Role**: Trusted cloud services, such as Elastic Compute Service (ECS), can assume this role to access your cloud resources.
3. Perform the corresponding operation based on the selection in the previous step.
   - If you select **User Role**, on the **Enter Type** tab, select Current Alibaba Cloud Account, or select Other Alibaba Cloud Account and enter its account ID. Then click **Next**.
   - If you select **Service Role**, select a cloud service on the **Enter Type** tab.
4. On the **Configure Basic** tab, enter a role name in the **Role Name** field, and then click **Create**.
5. If the **Phone Verification** dialog box appears, click **Send verification code**, and enter the verification code received by your phone.

(New version) Create a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **RAM Roles**.
2. On the **RAM Roles** page, click **Create RAM Role**.
3. In the **Create RAM Role** dialog box, perform the following operations and then click **OK**.
   i. In the **Trusted entity type** section, select a role type as needed.
      - **Alibaba Cloud Account**: A RAM user of a trusted Alibaba Cloud account can assume the RAM role to access your cloud resources. A trusted Alibaba Cloud account can be the current account or another Alibaba Cloud account.
      - **Alibaba Cloud Service**: A trusted Alibaba Cloud service, such as Elastic Compute Service (ECS), can assume the RAM role to access your cloud resources.

   ii. Perform the corresponding operation based on the selection in the previous step.
      - If you select **Alibaba Cloud Account**, in the **Select Trusted Alibaba Cloud Account** section, select **Current Alibaba Cloud Account**, or select **Other Alibaba Cloud Account** and enter its account ID in the Account ID field.
      - If you select **Alibaba Cloud Service**, select a cloud service from the **Select Trusted Service** drop-down list.

   iii. In the **RAM Role Name** field, enter a RAM role name.

(Old version) Authorize a RAM role

A newly created RAM role does not have any authorizations. Therefore, you must authorize this role.

1. In the **Create Role** dialog box, click **Authorize** on the **Role created** tab. If you have closed the **Create Role** dialog box, click the name of the newly created RAM role on the **Role Management** page. In the left-side navigation pane, choose **Role Authorization Policies**.
2. On the **Role Authorization Policies** page, click **Edit Authorization Policy** in the upper right corner.
3. On the Search and Attach tab in the **Edit Role Authorization Policy** dialog box, select AliyunACMFullAccess from the left-side **Available Authorization Policy Names** list. Then click the **>** icon in the middle to add AliyunACMFullAccess to the right-side **Selected Authorization Policy Name** list. Then click **OK**.
    - If you also use the configuration encryption and decryption function of ACM, you need to add the **AliyunKMSCryptoAccess** authorization policy for this RAM role.
4. If the **Phone Verification** dialog box appears, click **Send verification code**, and enter the verification code received by your phone.

> **Notice** In this step, this RAM role is granted full access to ACM. For more information about how to grant a RAM role specific access to a single namespace, see the "Access control" section at the end of this topic.

(New version) Authorize a RAM role

A newly created RAM role does not have any authorizations. Therefore, you must authorize this role.

1. Log on to the RAM console. In the left-side navigation pane, choose **RAM Roles**.
2. On the **RAM Roles** page, find the RAM role to be authorized, and click **Add Permissions** in the **Actions** column.
3. In the **Add Permissions** dialog box, find AliyunACMFullAccess in the left-side **System Policy** list, and click this policy. Then click **OK**.
    - If you also use the configuration encryption and decryption function of ACM, you need to add the **AliyunKMSCryptoAccess** authorization policy for this RAM role.

(Old version) Deauthorize a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **Roles**.
2. On the **Role Management** page, find the role to be deauthorized, and click **Authorize** in the **Actions** column.
3. In the **Edit Role Authorization Policy** dialog box, select **AliyunACMFullAccess** from the right-side **Selected Authorization Policy Name** list. Then click the **<** icon in the middle to move this policy to the left-side **Available Authorization Policy Names** list. Then click **OK**.

After the authorization is revoked, the corresponding RAM user is not authorized to log on to the ACM console.

(New version) Deauthorize a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **RAM Roles**.
2. On the **RAM Roles** page, select the role to be deauthorized in the **RAM Role Name** column.
3. On the **Role Authorization Policies** tab, click **Remove Permission** in the **Actions** column.
4. In the **Remove Permission** dialog box, click **OK**.

After the authorization is revoked, the corresponding RAM user is not authorized to log on to the ACM console.

(Old version) Delete a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **Roles**.
2. On the **Role Management** page, find the role to be deleted, and click **Delete** in the **Actions** column.
3. In the **Delete Role** dialog box, click **OK**.

(New version) Delete a RAM role

1. Log on to the RAM console. In the left-side navigation pane, choose **RAM Roles**.
2. On the **RAM Roles** page, find the role to be deleted, and click **Delete** in the **Actions** column.
3. In the **Delete RAM Role** dialog box, click **OK**.

More information

- 访问权限控制
- 利用RAM角色实现跨账号访问ACM
- Sub-Account Management
- Terms

3.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

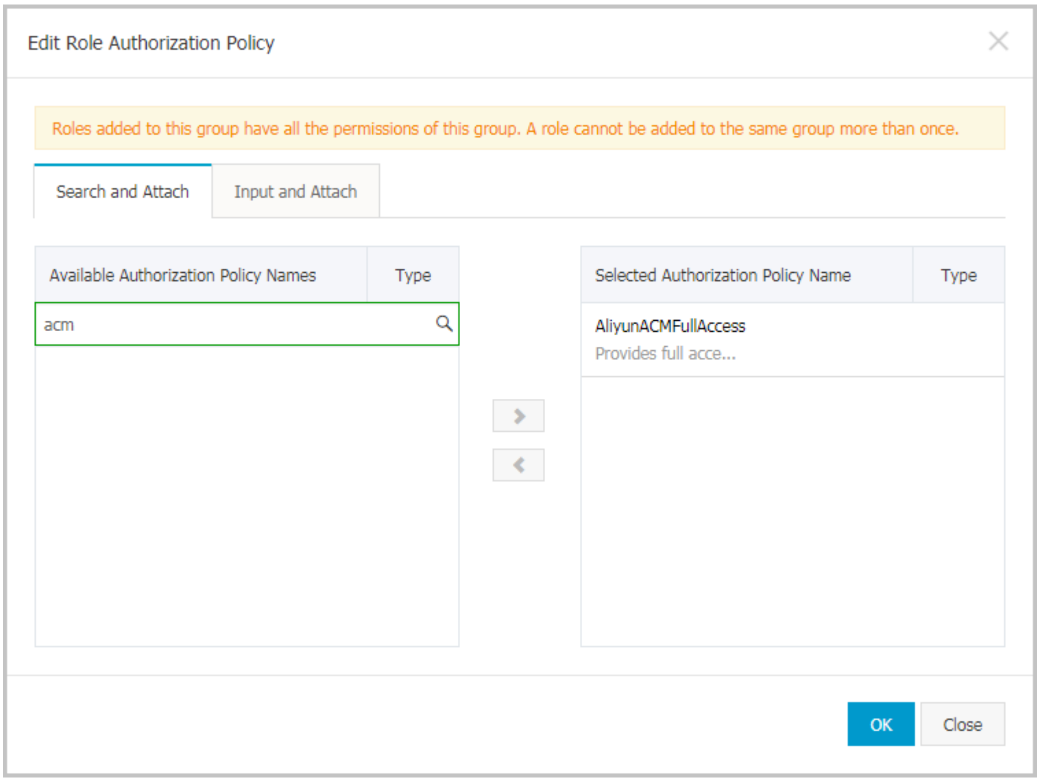
You're running a VPC network.

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.
   i. On the **Select Role Type** page, click **Service Role**.
   ii. On the **Enter Type** page, select **ECS Elastic Compute Service**.
   iii. 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.



Edit Role Authorization Policy

Roles added to this group have all the permissions of this group. A role cannot be added to the same group more than once.

Available Authorization Policy Names	Type
acm	

Selected Authorization Policy Name	Type
AliyunACMFullAccess Provides full acce...	

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)
- Overview
- Use RAM roles to access other Alibaba Cloud services
- Prerequisites