Alibaba Cloud Web App Service

Access control

Issue: 20200708

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

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Access control overview

You can create different permissions for different RAM users, and avoid security risks caused by exposing the accesskey of your Alibaba cloud account.

Scenarios

The following is a typical scenario where RAM is required to control access.

- Grant different permissions to RAM users

  Enterprise A has purchased various Alibaba cloud services, such as Elastic Compute Service (ECS) instances, apsaradb for RDS instances, server load balancer (SLB) instances , and Object Storage Service (OSS) buckets, to migrate A Project-X to the cloud. Certain employees need to perform operations on these cloud resources. Different employees require different permissions to fulfill their duties. Enterprise A has the following requirements:

  - For security reasons, Enterprise A does not want to disclose the accesskey of its Alibaba Cloud account to its employees. Instead, enterprise A prefers to create different Ram user accounts for its employees and grant different permissions to these user accounts.
  - The RAM users can only perform operations on resources after they are granted the corresponding permissions. Enterprise A can revoke the permissions granted to Ram users and delete Ram user accounts at any time.
  - Ram does not need to perform independent metering and billing for Ram users. All expenses are billed to account A.

  You can use the authorization management function of RAM to centrally manage user permissions and resources.

- Use RAM roles to enable cross-account resource access

  Account A and Account B are created respectively for Enterprise A and Enterprise B. Enterprise A has purchased various Alibaba cloud resources, such as ECS instances, apsaradb for RDS instances, SLB instances, and OSS buckets.

  - Enterprise A wants to focus on its business system and entrust tasks such as cloud resource O&M, monitoring, and management to Enterprise B.
  - Enterprise B is allowed to grant access permissions for the resources owned by Enterprise A to one or more employees, implementing fine-grained control on the resources of Enterprise A.
  - If either party terminates the entrustment agreement, enterprise A can revoke the permissions of Enterprise B at any time.

  RAM roles can be used to implement cross-account authorization and resource access control.

Policy

The following figure shows the system permission policies supported by Web+.

Permission	Category	Equivalent
WebPlusFullAccess	System route	Complete permissions for Web app service.
WebPlusReadOnlyAccess	System route	The read-only permission to Web app service.

2 Grant different permissions to RAM users

You can create different permissions for different RAM users, and avoid security risks caused by exposing the accesskey of your Alibaba cloud account.

Background

For security reasons, you can create RAM users (sub-accounts) for your Alibaba Cloud account (primary account) and Grant different permissions to these sub-accounts as needed. In this way, the Ram user can assign their own responsibilities without exposing the CMK. This article assumes that Enterprise A wants to have its employees perform routine O&M work. Then, enterprise A can create A RAM user and grant this RAM user the necessary permissions. Employees can then use the RAM users to log on to the console or call API operations.

Web app service provides the following system policies:

- **WebPlusFullAccess**: Web app service full permissions.
- **WebPlusReadOnlyAccess**: Web app service read-only permissions.

Prerequisites

- #unique_5

Step 1: Create a RAM user

You need to use an Alibaba Cloud account to log on to the RAM console and create a RAM user.

1. Login RAM console. In the left-side navigation pane, choose **personnel Management** > **user**, and in **user** page, click **create User**.
2. In **create User** page's **user account information** in the area box, enter **logon name** and **display name**.

    **Note:**
   The logon name can contain lowercase letters, digits, periods (.), underscores (_), and hyphens (-). The length cannot exceed 128 characters. The display name cannot exceed 24 characters or Chinese characters.
3. (Optional) If you want to create multiple RAM users at a time, click **Add User**, and repeat the previous step.

4. In **access Mode** in the area box, select **console password logon** or **programmatic access**, and click **confirm**.

   Note:
   For security purposes, select only one access mode.

   - If **console password logon**, complete the settings. You need to determine whether to automatically generate a default password or custom password, whether to require you to reset your password, and whether to enable MFA.
   - If **programmatic access**, RAM automatically creates an AccessKey for the RAM user (API access key).

     Notice:
     For security reasons, the RAM console only provides the opportunity to view or download AccessKeySecret once. Therefore, the AccessKey is created. Keep the AccessKeySecret recorded in a safe place.

5. In **mobile phone verification** dialog box, click **obtain verification code**, and enter the received phone verification code, and then click **confirm**. The created RAM user is displayed in **user** page.

Step 2: Grant permissions to the RAM user

Before using a RAM user, you must grant permissions to the RAM user.

1. In RAM console in the left-side navigation pane, choose **personnel Management** > **user**.
2. In **user** to find the target user, click **operation** column in the **add permissions**.
3. In **add permissions** panel's **select permissions** in the left-side navigation pane, search for the policy by keyword, and click the Policies tab to add it to **selected** list, and then click **confirm**.

   Note:
   For more information about the permissions that you can add, see the background information.

4. On the **Add Permissions** page, view the authorization information summary in the **Authorization Result** section, and then click **Finished**.

What to do next

After creating RAM users with an Alibaba Cloud account, you can distribute the logon names and passwords of the RAM users or AccessKey pair information to other RAM users . Other employees can log on to the console or call an API operation with the RAM user through the following steps.

- Log on to the console
  1. Open in browser the logon page for RAM users.
  2. In **RAM user logon** page, enter the RAM user logon name, and click **next Step**, and enter the RAM user password, and then click **login**.

     Note:
     The logon name of the RAM user is in the format of <$username>@<$AccountAlias> or <$username>@<$AccountAlias>.onaliyun.com. <$AccountAlias> is the account alias. If no account alias is set, the value defaults to the ID of the Alibaba cloud account.
  3. On the homepage of the **Alibaba Cloud console**, click a product with the permission to access the console.
- Call an API operation with the RAM user's AccessKey

  Use the AccessKeyId and AccessKeySecret of the RAM user in the code.

References

- #unique_6
- #unique_7
- #unique_8

3 Use a RAM role to access resources across Alibaba Cloud accounts

Use the Alibaba Cloud account of enterprise A to create A RAM role, authorize this role, and assign this role to Enterprise B. You can use the Alibaba Cloud account of Enterprise B or the corresponding RAM users to access the Alibaba Cloud resources of Enterprise A.

Background

Assume that Enterprise A has purchased multiple types of cloud resources to carry out its businesses and needs to grant Enterprise B the permission to carry out certain businesses on behalf of Enterprise A. In this case, you can use the resource access management (RAM) role to perform this task. A RAM role does not have a specific logon password or AccessKey pair. A RAM user can be used only after the RAM user is assumed by a trusted entity. To meet the needs of enterprise A, you can perform the following operations:

1. Create A RAM role for enterprise A
2. Enterprise A attaches the required permissions to the RAM role
3. Enterprise B creates a RAM user
4. Enterprise B adds **AliyunSTSAssumeRoleAccess** permissions
5. A RAM user of Enterprise B uses the console or API to access the resources of Enterprise A .

The following table lists the Web+ system permission policies that can be attached to a RAM role.

- **WebPlusFullAccess**: Web app service full permissions.
- **WebPlusReadOnlyAccess**: Web app service read-only permissions.

Step 1: Create A RAM role for enterprise A

You need to use the Alibaba Cloud account of enterprise A to log on to the RAM console and create A RAM role.

1. Login RAM console. In the left-side navigation pane, choose **RAM roles**, and in **RAM roles** page, click **create a RAM role**.

2. In **create a RAM role** in the panel, do the following and click **close**.

   a. In **current trusted entity type** area box, select **alibaba Cloud account**, and click **next Step**.

   b. In **RAM role name** enter a RAM role name in the text box. **Select Alibaba Cloud account** area box, select **other Alibaba Cloud account** and enter the cloud account of Enterprise B in the textbox. Then click **complete**.

   > **Note:**
   > The name of the RAM role can contain letters, digits, and hyphens (-). It can be up to 64 characters in length.

Step 2: enterprise A attaches the required permissions to the RAM role

A newly created ram role does not have any permissions. Therefore, enterprise A must grant permissions to this role.

1. In RAM console in the left-side navigation pane, choose **RAM roles**.
2. In **RAM roles** click the target role on the page. **Operation** column in the **add permissions**.
3. In **add permissions** panel's **select permissions** in the left-side navigation pane, search for the policy by keyword, and click the Policies tab to add it to **selected** list, and then click **confirm**.

   > **Note:**
   > For more information about the permissions that you can add, see the background information.

4. In the **Authorization Result** section of the **Add Permissions** pane, view the authorized permission information, and click **Complete**.

Step 3: Enterprise B creates a RAM user

Use the Alibaba Cloud account of Enterprise B to log on to the RAM console and create a RAM user.

1. Login RAM console. In the left-side navigation pane, choose **personnel Management** > **user**, and in **user** page, click **create User**.
2. In **create User** page's **user account information** in the area box, enter **logon name** and **display name**.

   > **Note:**

The logon name can contain lowercase letters, digits, periods (.), underscores (_), and hyphens (-). The length cannot exceed 128 characters. The display name cannot exceed 24 characters or Chinese characters.

3. (Optional) If you want to create multiple RAM users at a time, click **Add User**, and repeat the previous step.
4. In **access Mode** in the area box, select **console password logon** or **programmatic access**, and click **confirm**.

   Note:
   For security purposes, select only one access mode.

   - If **console password logon**, complete the settings. You need to determine whether to automatically generate a default password or custom password, whether to require you to reset your password, and whether to enable MFA.
   - If **programmatic access**, RAM automatically creates an AccessKey for the RAM user (API access key).

     Notice:
     For security reasons, the RAM console only provides the opportunity to view or download AccessKeySecret once. Therefore, the AccessKey is created. Keep the AccessKeySecret recorded in a safe place.
5. In **mobile phone verification** dialog box, click **obtain verification code**, and enter the received phone verification code, and then click **confirm**. The created RAM user is displayed in **user** page.

Step 4: Enterprise B attaches permissions to the RAM users

Enterprise B must add **AliyunSTSAssumeRoleAccess** to allow A RAM user to assume A RAM role created by Enterprise A.

1. In RAM console in the left-side navigation pane, choose **personnel Management** > **user**.
2. In **user** to find the target user, click **operation** column in the **add permissions**.
3. In **add permissions** panel's **select permissions** area, search by keyword **AliyunSTSA ssumeRoleAccess** policy, and click the policy to add it to the **selected** list, and then click **confirm**.
4. On the **Add Permissions** page, view the authorization information summary in the **Authorization Result** section, and then click **Finished**.

What to do next

After completing the preceding operations, the RAM users of Enterprise B can log on to the console to access the cloud resources of Enterprise A or call API operations as follows.

- Log on to the console to access the cloud resources of Enterprise A.
  1. Open in browser the logon page for RAM users.
  2. In **RAM user logon** page, enter the RAM user logon name, and click **next Step**, and enter the RAM user password, and then click **login**.

     Note:
     The logon name of the RAM user is in the format of <$username>@<$AccountAlias> or <$username>@<$AccountAlias>.onaliyun.com. <$AccountAlias> is the account alias. If no account alias is set, the value defaults to the ID of the Alibaba cloud account.
  3. On the **RAM user center** page, move the pointer to the portrait in the upper-right corner and click **Switch Role**.
  4. In **alibaba Cloud-role switch** page, enter the name of Enterprise A's **enterprise alias** or **default domain** and **role name**, and then click **switch**.
  5. Perform operations on the Alibaba Cloud resources of Enterprise A.
- Use A RAM user of Enterprise B to access the cloud resources of enterprise A through APIs

  To use A RAM user of Enterprise B to access the cloud resources of Enterprise A by calling API operations, ensure that the code contains the RAM user's AccessKeyId, AccessKeySecret, and SecurityToken (temporary security token). For more information about how to use STS to obtain a temporary security token, see get started with STS.

References

- #unique_6
- #unique_7
- #unique_10
- #unique_8
- #unique_11