Resource Access Management

User Guide

User Guide

The RAM User Guide outlines various core functions and application scenarios of RAM products. Core functions include user identity and authorization management. Application scenarios cover the following areas: enterprise subaccount and permission management, temporary authorization management for mobile apps, resource operations and authorization management between different organizations, and cross-region identity federation (SSO supported) and authorization management.

Identity management section

- User Identity Management
- Group-based User Management
- Role Identity Management

Authorization management section

- Authorization Policy Management
- User and Role Identity Authorization
- Authorization Policy Language

Typical application scenarios

- Enterprise Subaccount and Permission Management
- Temporary Authorization Management for Untrusted Client Apps
- Resource Operations and Authorization Management between Organizations

Identities

RAM-User is an identity used in RAM to relate with a true identity, such as a user or an application. To allow a new user or an application access to your cloud resources, you create and grant permissions to a RAM-User. The general procedures are as follows:

1. Use the primary account (or a RAM-User with RAM operation permissions) to log on to the RAM console.
2. Create a RAM user and add the user to one or more groups.
3. Attach one or more authorization policies to the user (or the group to which the user belongs).

4. Create a credential for the user.
   - If the user is to perform operations using the console, you must set a logon password for the user.
   - If the user is to call APIs, you must create an API AccessKey for the user.
5. If the user needs to use special permissions (for example, to stop ECS instances), you can set MFA for the user and require that the user uses an MFA password to log on to the Alibaba Cloud console.
6. Provide the user with the logon URL, username, and logon password.

This document describes the RAM-User related operations, such as creating a RAM user, creating a logon password or an AccessKey for a RAM user, and enabling virtual MFA devices for a RAM user.

RAM settings

In **Settings**, you can set your enterprise alias, the password policy for RAM users, and the security policy.

Set the enterprise alias

The procedures are as follows.

Log on to the RAM console.

Select **Settings** > **Enterprise Alias Settings**.

Click **Edit Enterprise Alias**.

Enter an enterprise alias following the instruction, and then click **OK**.

Set the password policy

The procedures are as follows.

Log on to the RAM console.

Select **Settings** > **Password Strength Settings**.

Configure your password policy, and then click **Save Changes**.

Note: All RAM users created hereafter must comply with the password strength settings.

Set the security settings

The procedures are as follows.

Log on to the RAM console.

Select **Settings** > **User Security Settings**.

Configure your security policy, and then click **Save Changes**.

Create a RAM user

The procedures are as follows.

Log on to the RAM console.

Select **Users** > **New User**.

Enter the user information in the dialog box and click **OK**.

Set a logon password

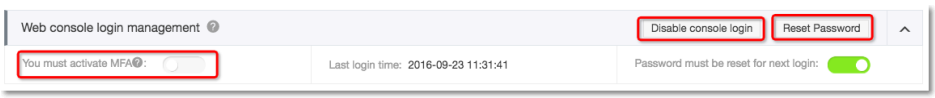
To allow a RAM user access to the management console, you create a logon password for the user. The procedures are as follows.

Log on to the RAM console and click **Users**.

Select a user to go to the **User Details** page.

Click **Enable console logon** and set an initial password for the user in the dialog box. You can also specify that the user must change this password upon the first logon.

After setting a logon password, you can also enable **MFA**, **Reset Password**, or **Disable console logon** in the **User Details** page.



Create an AccessKey

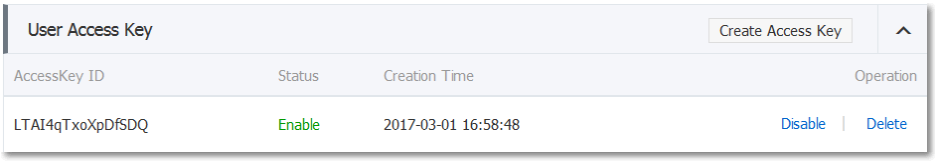
An AccessKey (AK) is equivalent to a logon password, but it is used in different scenarios. AccessKeys are used to call cloud service APIs, and logon passwords are used to log on to the console. If the user does not have to call APIs, you do not have to create an AccessKey for the user.

To create an AccessKey, do the following:

Log on to the RAM console and click **Users**.

Select a user to open the **User Details** page.

Click **Create AccessKey** in the **User AccessKey** section to create a new AccessKey in the dialog box.



Note:

New AccessKeys are displayed only during creation. For security reasons, RAM does not provide an AccessKey query interface. Therefore, please keep the AccessKey safe. If your AccessKey is disclosed or lost, you must create a new one.

Enable virtual MFA devices

Multi-Factor Authentication (MFA) is a simple but effective best practice that can provide additional security protection.

After MFA is enabled, when a user logs on to Alibaba Cloud, the system requires the user to enter the user name and password (first security factor), and then enter a variable verification code (second security factor) provided by the user’ s VMFA (virtual MFA) device. All these factors work together to offer higher security protection for your account.

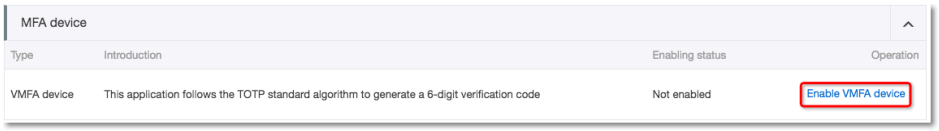
The virtual MFA (VMFA) device is an application that generates a 6-digit verification code. It complies with the time-based one-time password algorithm (TOTP) standard (RFC 6238). This application can run on mobile hardware devices including smartphones, making it easily accessible.

To enable virtual MFA devices for a RAM user, do the following:

Log on to the RAM console and click **Users**.

Select a user to open the **User Details** page.

Click **Enable VMFA device** in the **MFA Device** section.



Note: Ensure that you have installed an MFA application (for example, Google Authenticator) on a smart device (a smart phone is optimal) before proceeding with the following operation.

On the **Enable virtual MFA device** page, do one of the following to associate your MFA application with the RAM user:

- Scan the generated QR code with the MFA application on your smart phone.
- Manually enter the information under **Manual information retrieval** in the MFA application.

After the association is established, the RAM user account is added into the MFA application and is provided with a dynamic security code (Time-based One-Time Password, TOTP) every 30 seconds.

Enter two successive security codes you obtained from the MFA application into the **First security code** and **Second security code** boxes, and click **Enable**.

Log on to a RAM user

RAM-Users are different from Alibaba Cloud accounts, and therefore, their logon portal is different. RAM-Users cannot log on from the Alibaba Cloud account logon page.

On the RAM console overview page, you can find the RAM-User logon link. RAM-Users can log on to the Alibaba Cloud console through the logon URL.

Note: By default, RAM-Users do not have any access permissions. A RAM-User without permissions can log on to the console, but cannot perform any operations.

For details on how to grant permissions to RAM-Users, see User Authorization.

If you have created multiple RAM-Users with your Alibaba Cloud account, we recommend that you manage those users by group to simplify the management process.

Group management

Log on to the RAM console, and click **Groups** on the left-side navigation pane to enter the **Group Management** page.

The following procedures describe how to create/rename/delete a group, and how to manage group members on the **Group Management** page.

Create a group

The procedures are as follows:

On the Group Management page, click **Create Group**.

On the **Create Group** page, enter a **Group Name** (the **Description** is optional) and click **OK**.

Go back to the **Group Management** page, and you can find the newly created group in the group list (searching by group name is available).

Manage group members

The procedures are as follows:

On the Group Management page, locate your group (searching by group name is available) and click the corresponding **Edit Group Member** in the **Actions** column.

On the **Edit Group Member** page, select RAM users from the left box (searching by keywords is available) and click the rightward arrow to add them to the group.

By selecting a RAM user from the right box and clicking the leftward arrow, you can remove it from the group.

Confirm the group members and click **OK**.

Go back to the **Group Management** page, and click your **Group Name** or the corresponding **Management** in the **Actions** column to enter the **Group Details** page.

You can check the group members of your group on the **Group Details** page.

- To delete a member, click **Remove from Group**.
- To add a new member to the group, click **Edit Group Member**.

Rename a group

The procedures are as follows:

On the Group Management page, locate your group (searching by group name is available) and click your **Group Name** or the corresponding **Management** in the **Actions** column to enter the **Group Details** page.

Click **Edit Basic Info** to change the group name.

On the **Edit Group Info** page, enter a **Group Name** (the **Description** is optional) and click **OK**.

Delete a group

The procedures are as follows:

On the Group Management page, locate your group (searching by group name is available) and click the corresponding **Delete** in the **Actions** column.

Note: We recommend that you remove all users in a group first before deleting the group.

In the dialog box, click **OK** to delete the group.

Note: If a group contains members or is attached with authorization policies, you can check **Unlink Dependent Objects** in the dialog box before clicking **OK**.

Grant permissions to a group

For information on group authorization management, see **Attach policies to a group** in Authorization.

Like a RAM-User, a RAM-Role is also a type of RAM identity. Compared with RAM-User, a RAM-Role is a virtual user, that is, a RAM-Role has no identity credentials and has to be assumed by a trusted Alibaba Cloud account.

With this document, you can gain a better understanding of the RAM-Role, and know how to create and use a RAM-Role.

Note: Unless otherwise stated, the role in this document represents a RAM-Role.

Understanding RAM-Role

A RAM-Role is a virtual user (or shadow account). It is a type of RAM identity.

Virtual users vs. Real users

The difference between a virtual user and a real user is that a real user identity can be directly authenticated.

A real user has a logon password or an AccessKey. For example, Alibaba Cloud accounts, RAM-User accounts, and cloud service accounts are real users.

However, a virtual user, such as a RAM-Role, does not have a fixed security credential (such as a logon password, an AccessKeys, or a MFA).

RAM-Role vs. Textbook-Role

A Textbook-Role (or a role as traditionally defined) indicates a set of permissions. It is similar to a policy in RAM. If a Textbook-Role is granted to a user, it means that the corresponding permissions are granted to the user.

A RAM-Role differs from a textbook role. As a type of virtual user, a RAM-Role has a fixed identity and can be granted policies.

- When creating a RAM-Role, you must specify the Alibaba Cloud account which can assume the role.
- And you must grant necessary permissions to the RAM-Role to make it useful.

RAM-Roles differ from normal RAM-Users in the way they are used

RAM-Roles must be assumed by an authorized real user. After assuming a role, the real user receives a temporary security token (STS) for this RAM-Role. Then, the user can use this temporary security token to access the resources authorized for the role.

Usage notice

A RAM-Role must be associated with a real user identity so that it becomes available.

If a real user wants to use a RAM-Role that has been granted to the user, the real user must first log on using his identity and then perform the **SwitchRole** operation to switch from a real identity to a role identity. The user can then perform all operations authorized for this role identity, but the access permissions of the user’ s real identity will not be available.

To switch from the role identity back to the real identity, the user must perform the **Switch Back to Logon Identity** operation. Then, the user can have the access permissions granted to his real identity, but not those of the role.

RAM-Roles are mainly used to address the identity federation needs, such as entrusting other Alibaba Cloud accounts and their RAM-Users to perform operations on your resources, and entrusting cloud service to perform operations on your resources.

Concepts

The following table lists several basic concepts related to RAM-Roles:

Concept	Explanation
Role ARN	A Role ARN is the global resource description of a role. It is used to specify a role. - RoleARNs follow Alibaba Cloud ARN naming rules. For example, the RoleARN for the devops role under an Alibaba Cloud account is: acs:ram::1234567890123456:role/devops. - After a RAM-Role is created, the role’ s ARN is displayed on the **Role Details** page.
Trusted Actors	A role’ s trusted actors are the real user identities （ the current Alibaba Cloud account or another Alibaba Cloud account ） that can assume this role. - When creating a role, you must specify the trusted actors. - A role can only be assumed by trusted actors.
Policy	A role can be attached with a set of permissions, that is, a policy. Roles not attached with policies can exist, but cannot be used.
Assume Role	By performing the assume role operation, A real user can obtain a security token for a role.

	By calling the AssumeRole API, a real user obtains the role’ s security token and can use this token to access cloud service APIs.
Switch Role	By performing the switch role operation on the console, a real user can switch from the current logon identity to a role identity. - After a real user logs on to the console, the user can switch to a role for which he is a trusted actor. Then, the user can use the role identity to perform operations on cloud resources. - After switching to a role identity, the user can no longer use his real identity access permissions. When the user no longer needs to use a role, he can switch from the role back to the original logon identity.
Role Token	A role token is a temporary AccessKey for the role identity. Role identities do not have fixed AccessKeys, so when a real user wants to use a role, he must assume the role to obtain the corresponding role token. Then, the user can use this role token to call Alibaba Cloud service APIs.

Application scenarios of RAM-Roles

RAM-roles are mainly used for **cross-account access** and **temporary authorization access**.

Cross-account access

Using RAM-Roles, you can perform cross-account resource operations and authorization management.

Scenario

Assume that there are two enterprises, A and B. A has purchased multiple cloud resources and uses them to conduct its businesses.

Requirements	Solutions
A wants to focus on its business systems, so it entrusts or grants cloud resource O&M, monitoring management, and other tasks to	Alibaba Cloud account A creates a role in RAM and grants this role the necessary permissions. Then, it allows Alibaba Cloud

enterprise B.	account B to use this role.
Enterprise B further delegates O&M tasks to its employees. B needs to precisely control the operations its employees can perform on A's cloud resources.	If account B has employees (RAM-Users) who need to use this role, it can independently control their permissions. When performing O&M operations on behalf of A, account B's RAM-users can use the role identity to perform operations on A's resources.
If A and B terminate this O&M entrustment contract, A is able to revoke B's permissions at will.	If accounts A and B terminate their contract, A just needs to revoke B's permission to use this role. Once account B's permission to use this role is revoked, all RAM-Users of account B will automatically lose their permission to use this role.

Temporary authorization access

Using RAM-Roles, you can temporarily authorize a mobile app client to perform operations on the resources under your control.

Scenario

Assume that enterprise A has developed a mobile app and has bought OSS. The mobile app must upload and download data to and from OSS, but A does not want to allow all apps to use the AppServer to transmit data.

Because the mobile app runs on user devices, these devices are out of A's control. For security reasons, A cannot save the AccessKey in the app.

Requirements	Solutions
A wants to allow the app to directly upload and download data to and from OSS.	- Alibaba Cloud account A creates a role in RAM and gives this role the necessary permissions. Then, it allows AppServer (giving it a RAM user identity) to use this role. - When the app needs to directly connect to OSS to upload and download data, AppServer can use this role to obtain the role's temporary security token and send it to the app. The app can use the temporary security token to directly access OSS APIs.
A wants to minimize its security risks by, for example, giving each app an access token with only the minimum permissions it needs when directly connected to OSS and	- If more precise control of the permissions of each app is required, when using the role, the AppServer

restricting the access duration to a short period of time (such as 30 minutes).	can further restrict the resource operation permissions of the temporary security token. - For example, when assuming the role, the AppServer can restrict that different app users can perform operations only on some subdirectories.

User roles

RAM supports **User Roles**.

Roles that can be assumed by RAM-Users are called user roles.

RAM-Users permitted to assume roles can belong to your Alibaba Cloud account or another Alibaba Cloud account.

User roles are used to solve problems such as cross-account access and temporary authorization access.

Create a User Role

Do the following:

Log on to the **RAM console**.

On the left navigation pane, click **Roles**.

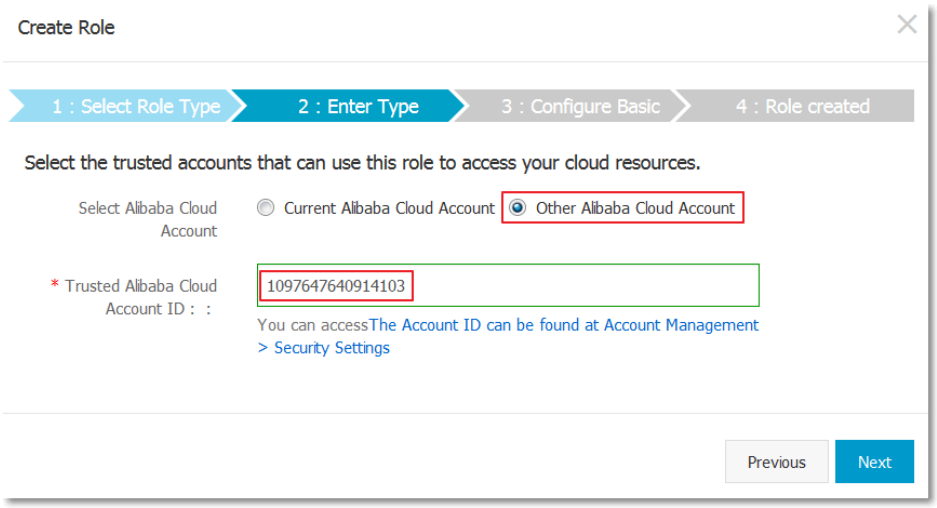
On the **Role Management** page, click **Create Role**.

Select Role Type. Click **User Role**.

Enter Type. Do one of the following and click **Next**.

If the role is to be used by the RAM-Users under your own account (such as authorizing a mobile app client to directly perform operations on OSS resources), select your Alibaba Cloud account as the trusted Alibaba Cloud account.

If the role is to be used by the RAM-Users under another Alibaba Cloud account (such as for cross-account resource authorization access), select an Alibaba Cloud account and enter its ID in the Trusted Alibaba Cloud account ID field, as shown in the following figure.

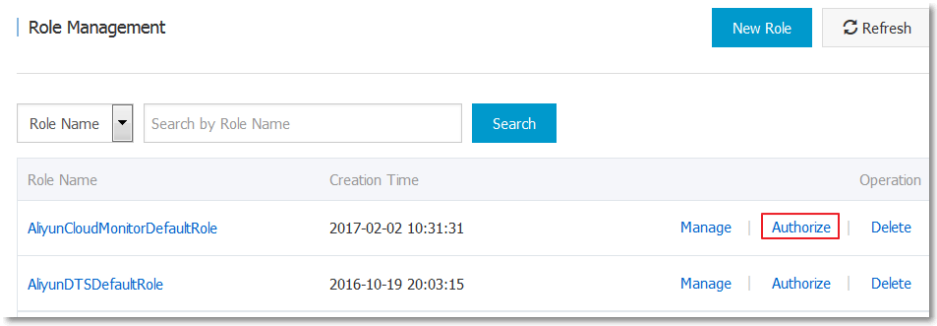


Configure Basic Information. Enter a **Role Name** (the description is optional) and click **Create**.

After you have successfully created a role, you can click **Authorize** to grant permissions to the role or click **Close** to finish.

Go back to the **Role Management** page and you can find the newly created role in the role list.

Click the corresponding **Authorize** in the **Actions** column to open the **Edit Role Authorization Policy** window, where you can grant necessary permissions to the role.



The role authorization method is similar to the normal RAM-User authorization method. For details, see **Grant permissions**.

Click the **Role Name** or the corresponding **Manage** in the **Actions** column to enter the **Role Details** page, where you can find the role' s Arn and can **Edit Basic Information**.

Click the corresponding **Delete** in the **Actions** column to delete the role.

Use a role

A RAM role can only be assumed by RAM users in the trusted Alibaba Cloud account. For security reasons, the trusted Alibaba Cloud accounts are not allowed to perform AssumeRole.

Therefore, you must use a trusted account to create a RAM-User account, and grant the AssumeRole permission to the RAM-User account. Then, you can assume the role by using this RAM-User identity. The procedures are as follows:

Create a RAM-User and create an AccessKey or set a logon password for this user.

Grant permissions to this RAM-User. The system authorization policy AliyunSTSAssumeRoleAccess is required.

Use a RAM-Role to access APIs

After a RAM-User is granted the AssumeRole permission, the user can use the AccessKey to call the STS AssumeRole API to obtain a temporary security token for this role.

For the AssumeRole API calling method, see STS API Documentation.

Use a RAM-Role to perform console operations

If a RAM-User needs to use the role identity to perform console operations, the RAM-User must first log on to the console with the logon identity, and then use the **SwitchRole** method. After that, the user can use the role identity to perform console operations.

For example, the RAM-User Alice under company2 (enterprise alias) logs on to the console, the user can move the mouse pointer to the account name on the upper-right corner and click **Switch Role**.

Alice needs to select the corresponding company alias and role name. For example, we assume that the user has been granted permission to assume the 'ecs-admin' role of company1 (enterprise alias).

After switching to the role, Alice can use the role identity to access the console.

Authorization

Permissions are used to allow or deny certain operations on resources under specific conditions. In RAM, authorization policies express permissions following the Authorization Policy Language. A policy contains a set of permissions.

This document explains related attributes of permissions and polices for your better understanding of the service.

Permissions

In RAM, the primary account owns all resources, and the RAM users can be granted access permissions to the resource.

The primary account (resource owner) controls all permissions

- Each resource has only one owner (resource owner). The owner must have an Alibaba Cloud account. This account is the primary account, and incurs all fees related to resources under it. The primary account also has control over all permissions on the resource.
- The resource owner is not necessarily the resource creator. For example, if a RAM user is granted permission to create resources, the resources created by this user belong to the primary account. Therefore, the user is the resource creator, but not the resource owner.

By default, RAM users (operators) have no permissions

- A RAM user represents an operator and must be explicitly authorized by the primary account owner to perform any operation.
- By default a RAM user has no operation permissions after being created. Only after being authorized, the user can perform resource operations on the console or by calling APIs.

Resource creators (RAM users) are not automatically granted permissions for the resources they create

- If a RAM user is granted the appropriate permission by the primary account owner, the RAM user can create resources.
- The RAM user does not have any permissions for the created resources unless the resource owner explicitly grants permissions to the user.

Authorization policies

An authorization policy is a group of permissions described using Authorization Policy Language. It describes the authorized resource set and operation set, and the authorization conditions that are associated. When an authorization policy contains both Allow and Deny authorization statements, priority is given to Deny statements.

In RAM, an authorization policy is a type of resource entity. You can create, update, delete, and view authorization policies. RAM supports two types of authorization policies:

System authorization policies

- System authorization policies are a group of general permission sets created and managed by Alibaba Cloud, such as read-only permission for ECS or full permissions for ECS.
- These policies can be used but not modified by users.

Custom authorization policies

- Custom authorization policies are policies created and managed by users. They can be used to expand and supplement system authorization policies.
- System authorization policies contain coarse-grained permissions. If finer-grained authorization policies are required, such as policies that precisely control permissions for a certain ECS instance or that have additional authorization conditions, you must create custom authorization policies.

Attach policies to a RAM user

To grant permissions to a RAM user, attach one or more authorization policies to the user or a user group which the user is a member of.

- You can attach both system authorization policies and custom authorization policies.
- If an attached authorization policy is updated, the updated policy automatically takes effect, and you do not have to reattach it.

An authorization policy is a set of permissions that either allow or deny a user access to a certain resource. After an authorization policy is attached to a user or group, the user or users in the group is granted access to resources that were specified in the authorization policy. Authorization policies are described using the Policy Language.

This document explains the authorization policies in RAM and the corresponding operation methods.

RAM supports two types of authorization policies: system authorization policies and custom authorization policies.

System authorization policies

System authorization policies are a group of general authorization policies provided by Alibaba Cloud. They define read-only permission or full permissions for different products.

> System authorization policies can only be used for authorization; they cannot be edited nor be modified by a user.
>
> Instead, system authorization policies are automatically updated and modified by Alibaba Cloud.

To view all the system authorization policies, log on to the RAM console and click **Policies**. Here, you can view the list of all system authorization policies.

RAM supports the following system authorization policies:

System authorization policy name	Permission description
AdministratorAccess	Permission for managing all Alibaba Cloud resources
AliyunActionTrailFullAccess	Permission for managing ActionTrails
AliyunActionTrailReadOnlyAccess	Read-only permission for ActionTrails
AliyunBatchComputeFullAccess	Permissions for managing BatchCompute
AliyunBSSFullAccess	Permission for managing BSS
AliyunBSSOrderAccess	Permission to view, pay, and cancel orders on BSS
AliyunBSSReadOnlyAccess	Read-only permission for BSS
AliyunCDNFullAccess	Permission for managing CDN
AliyunCDNReadOnlyAccess	Read-only permission for CDN
AliyunCloudMonitorFullAccess	Permission for managing CloudMonitor
AliyunCloudMonitorReadOnlyAccess	Read-only permission for CloudMonitor
AliyunDirectMailFullAccess	Permission for managing DirectMail
AliyunDirectMailReadOnlyAccess	Read-only permission for DirectMail
AliyunECSFullAccess	Permission for managing ECS
AliyunECSReadOnlyAccess	Read-only permission for ECS
AliyunEIPFullAccess	Permission for managing EIPs
AliyunEIPReadOnlyAccess	Read-only permission for EIPs
AliyunEMRFullAccess	Permission for managing E-MapReduce
AliyunKvstoreFullAccess	Permission for managing Kvstore

AliyunKvstoreReadOnlyAccess	Read-only permission for Kvstore
AliyunLogFullAccess	Permission for managing Log service
AliyunLogReadOnlyAccess	Read-only permission for Log service
AliyunMNSFullAccess	Permission for managing MNS
AliyunMNSReadOnlyAccess	Read-only permission for MNS
AliyunMTSFullAccess	Permission for managing MTS
AliyunOCSFullAccess	Permission for managing OCS
AliyunOCSReadOnlyAccess	Read-only permission for OCS
AliyunOSSFullAccess	Permission for managing OSS
AliyunOSSReadOnlyAccess	Read-only permission for OSS
AliyunOTSFullAccess	Permission for managing Table Store
AliyunOTSReadOnlyAccess	Read-only permission for Table Store
AliyunPTSFullAccess	Permission for managing PTS
AliyunRAMFullAccess	Permission for managing RAM, that is, permission for managing users and permissions
AliyunRAMReadOnlyAccess	Read-only permission for RAM, that is, permission for viewing users, groups, and authorization information
AliyunRDSFullAccess	Permission for managing RDS
AliyunRDSReadOnlyAccess	Read-only permission for RDS
AliyunSLBFullAccess	Permission for managing Server Load Balancer
AliyunSLBReadOnlyAccess	Read-only permission for Server Load Balancer
AliyunSTSAssumeRoleAccess	Permission for calling the STS AssumeRole interface
AliyunSupportFullAccess	Permission for managing the ticket system
AliyunVPCFullAccess	Permission for managing VPC
AliyunVPCReadOnlyAccess	Read-only permission for VPC
AliyunYundunAegisFullAccess	Permission for managing Aegis
AliyunYundunAFSFullAccess	Permission for managing AFS
AliyunYundunAPSFullAccess	Permission for managing APS
AliyunYundunCloudsFullAccess	Permission for managing Alibaba Cloud Security Network (Clouds)
AliyunYundunDDosFullAccess	Permission for managing Anti-DDoS
AliyunYundunFlawSaleFullAccess	Permission for managing Alibaba Cloud

	Security FlawSale
AliyunYundunFullAccess	Permission for managing all Alibaba Cloud Security products
AliyunYundunGreenWebFullAccess	Permission for managing Alibaba Cloud Security GreenWeb
AliyunYundunHighFullAccess	Permission for managing Alibaba Cloud Security Anti-DDoS IPs
AliyunYundunHSMFullAccess	Permission for managing Alibaba Cloud Security HSM
AliyunYundunMSSFullAccess	Permission for managing Alibaba Cloud Security MSS
AliyunYundunSASFullAccess	Permission for managing Alibaba Cloud Security SAS
AliyunYundunWAFFullAccess	Permission for managing Alibaba Cloud Security WAF
AliyunYundunXianzhiFullAccess	Permission for managing Alibaba Cloud Security Precognition
ReadOnlyAccess	Read-only permission for all Alibaba Cloud resources

Custom authorization policies

If the coarse-grained system authorization policies do not meet your needs, you can create custom authorization policies.

For example, if you want to control the operation permissions for a certain ECS instance or require resource operator request to come from specified IP addresses, you must use a custom authorization policy to meet these fine-grained requirements.

Create a custom authorization policy

If you have finer-grained authorization requirements, you can create custom authorization policies for access control.

For example, you can only grant the user Bob the read-only permission for all objects in oss://sample_bucket/bob/, and only allow accesses from the IP addresses within your company network (your company network IP address can be acquired by searching “My IP” using the search engine).

When creating custom authorization policies, you must understand the basic structure and syntax of the authorization policy language. For more details, see Authorization Policy Language Description.

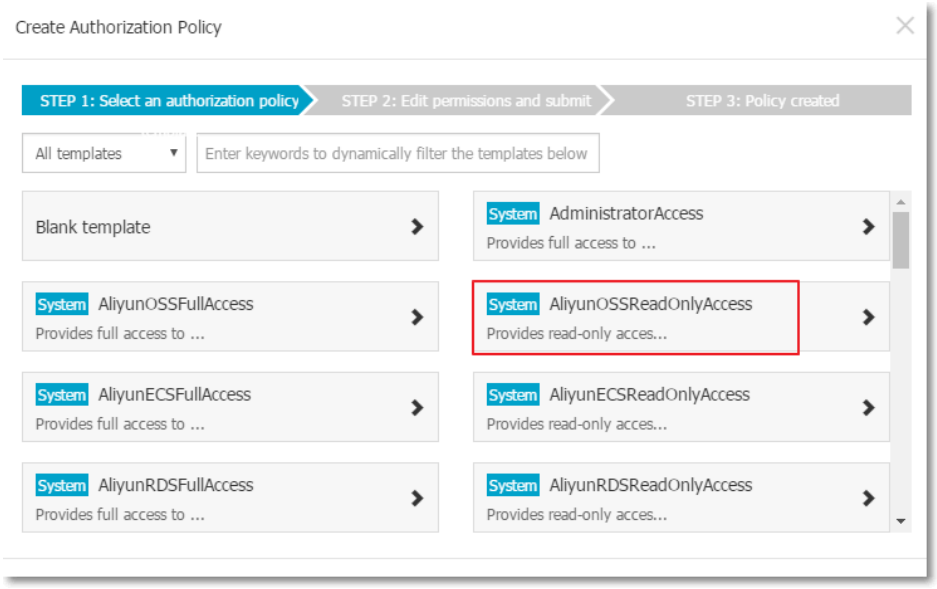
Procedure

Log on to the RAM console.

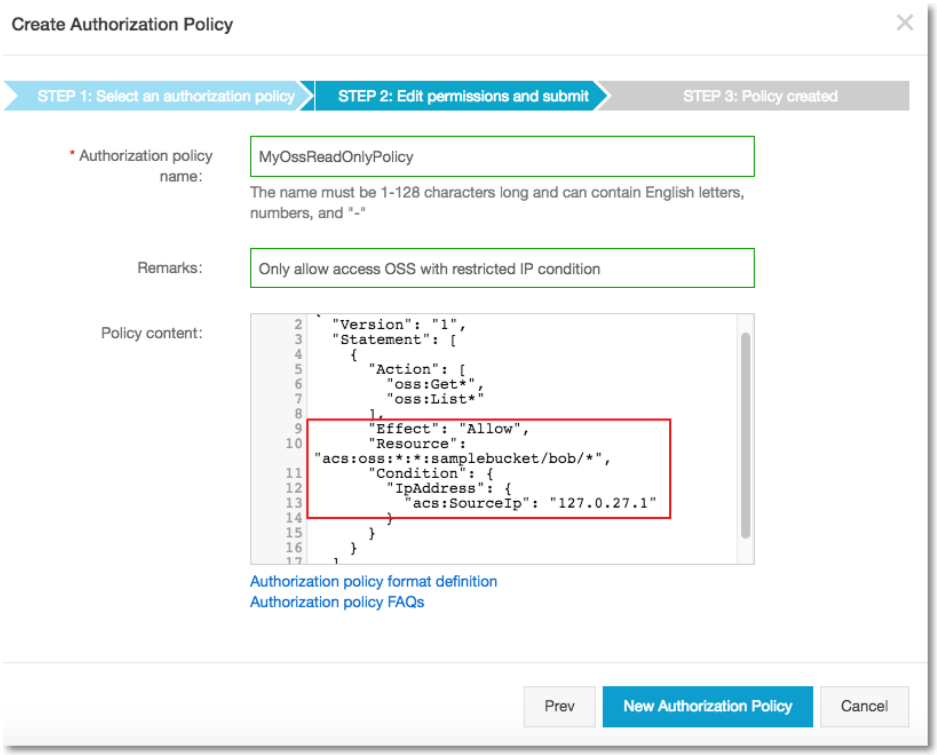
From the left-side navigation pane, click **Policies**.

On the upper-right corner, click **New Authorization Policy**.

Select an authorization policy template, for example, AliyunOSSReadOnlyAccess.



Edit the policy based on the template and click **New Authorization Policy**.



In the preceding figure, the selected part is the added fine-grained authorization content. The name, remarks, and content of the custom authorization policy have been modified.

Custom policy example:

```
{
"Version": "1",
"Statement": [
{
"Action": [
"oss:Get*",
"oss:List*"
],
"Effect": "Allow",
"Resource": "acs:oss:*:*:samplebucket/bob/*",
"Condition": {
"IpAddress": {
"acs:SourceIp": "127.0.27.1"
}
}
}
]
}
```

If you attach this custom authorization policy to the user Bob, Bob will have the read-only permission for all objects in oss://samplebucket/bob/ under the condition that he accesses the objects from your company network (for example, 127.0.27.1).

Modify a custom authorization policy

When a user’ s permissions change (that is, new permissions are added or existing permissions are revoked), you must modify the user’ s authorization policy. When modifying an authorization policy, you may encounter two problems:

The old authorization policy is still available after a period of time.

After modification, the modified policy is incorrect and a rollback needs to be performed.

To address such problems, Alibaba Cloud provides the version management feature for authorization policies. Version management enables you to retain multiple versions for one authorization policy.

If the number of versions exceeds the limit, you must delete the unwanted versions.

When an authorization policy contains multiple versions, only one version is active, which is known as the “default version”.

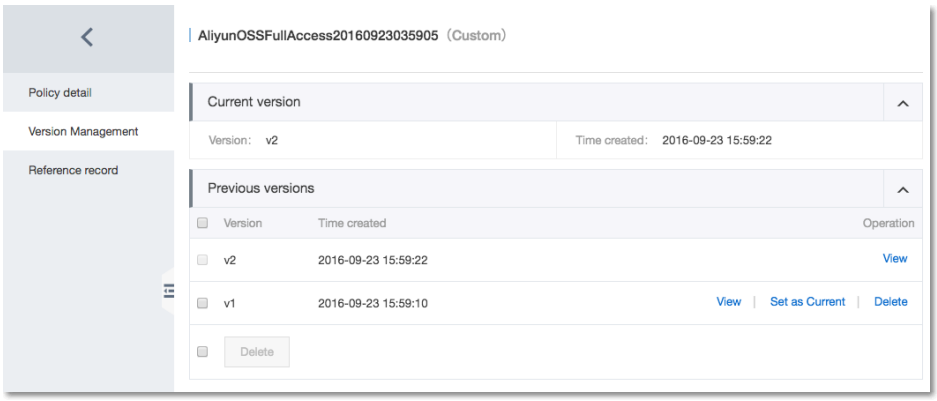
Procedure

Log on to the RAM console.

From the left-side navigation pane, click **Policies**.

Click **Custom Policy** to enter the sub-page.

Click **Modify** next to the policy you want to modify.



Delete a custom authorization policy

You can create multiple custom authorization policies and maintain multiple versions for each policy. You can also delete custom authorization policies that are no longer needed.

However, if an authorization policy contains multiple versions, that authorization policy cannot be deleted. Instead, you must delete all versions except the default one. When only the default version left, the authorization policy can then be deleted.

Procedure

Log on to the RAM console.

From the left-side navigation pane, click **Policies**.

Click **Custom Policy** to enter the sub-page.

Click **Delete** next to the authorization policy that you want to delete.

In RAM, granting permissions indicates attaching policies to a RAM user, a user group, or a RAM role.

Attaching policies to a RAM user or a user group is used for granting permissions to users under the current Alibaba Cloud account.

Attaching policies to a RAM role (which has specified other Alibaba Cloud account as the trusted Alibaba Cloud account) is used for granting permissions to users under other Alibaba Cloud account.

This document describes how to attach policies to a RAM user, a user group, or a RAM role.

Attach policies to a RAM user or a user group

To attach policies to a RAM user:

Log on to the RAM console.

On the left-side navigation pane, click **Users**.

On the **User Management** page, locate your user (searching by user name is available) and click the corresponding **Authorize** in the **Actions** column.

On the **Edit User-Level Authorization** window, select necessary policies to grant to the user.

To attach policies to a user group:

Log on to the RAM console.

On the left-side navigation pane, click **Groups**.

On the **Group Management** page, locate your group (searching by group name is available) and click the corresponding **Authorize** in the **Actions** column.

On the **Edit Group Authorization Policy** window, select necessary policies to grant to the group.

Attach policies to a RAM role

To attach policies to a RAM role:

Log on to the RAM console.

On the left-side navigation pane, click **Roles**.

On the **Role Management** page, locate your group (searching by role name is available) and click the corresponding **Authorize** in the **Actions** column.

On the **Edit Role Authorization Policy** window, select necessary policies to grant to the role.

Users can access the permitted resources on the console or from calling APIs after being authorized.

Access resources on the console

A RAM user can log on to the management console to perform resource operations.

The RAM user logon requires an independent logon URL (which can be viewed on the RAM console). Use the primary account enterprise alias, username, and password to log on to the console.

After successfully logging on, the user can perform operations on the authorized resources. If the user attempts to perform an operation that they do not have permission for, the error message “No operation permissions” is displayed.

If a RAM user is allowed to assume a role,

After logon, the user can use the **Switch Role** operation to switch from the current logon identity to a role identity. In this way, the user can use the permissions of the newly selected role to perform operations on resources.

If the user wants to switch back to the logon identity, the user can use the **Return to Logon Identity** operation. For more information about roles, see Roles.

Access resources from calling APIs

An Application can call cloud service APIs to perform resource operations.

For the application that calls cloud service APIs to perform resource operations, you create a RAM user account for this application and grant it relevant permissions. Then, create an AccessKey for this RAM user, which is used by the application to call cloud service SDKs and APIs.

Access resources by using a client tool

You can also perform cloud resource operations using a client tool.

Some cloud services provide easy-to-use client tools, for instance, aliyuncli. These tools allow the usage of RAM user AccessKeys to perform cloud resource operations.

Scenarios

Assume that an enterprise A buys several types of cloud resources, such as ECS instances, RDS instances, Server Load Balancer instances, and OSS buckets. The employees at the enterprise A need to perform operations on these resources such as buying, O&M, or online application.

Because different employees have different responsibilities, they require different permissions. For security reasons, the Alibaba Cloud account owner of the enterprise A does not want to disclose its account AccessKey to its employees.

Rather, the account owner prefers to create different RAM user accounts for their employees and associate each RAM user account with different permissions. Then, the employees can perform resource operations only under their permissions with their RAM user accounts and charges are not billed to these accounts.

All expenses are charged to the account owner. The account owner can also revoke the permissions of a RAM user account at any time, and delete the user.

Requirements

Employees do not share the primary account to avoid uncontrollable risks caused by the disclosure of the account’ s password or AccessKey.

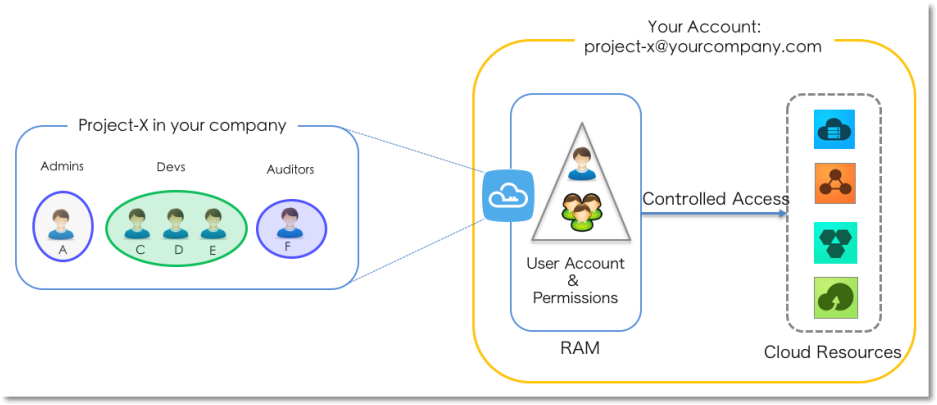
Different employees are allocated independent user accounts (or operator accounts) with independent permissions, so that their responsibilities are consistent with their permissions.

All the operations of all user accounts can be audited.

Charges are not calculated for each operator; the primary account is billed for all fees incurred.

Solution

Use RAM-user accounts and the authorization management function, as shown in the following figure:



The procedures are as follows:

Enable MFA for the primary account to prevent risks caused by disclosure of the primary account password.

Activate RAM.

Create RAM-User accounts for different employees (or application systems) and set logon passwords or create AccessKeys for them as needed.

Create a group. If multiple employees share the same responsibilities, we recommend that you create a group for them and add the users to the group.

Grant permissions. Attach one or more authorization policies to groups or users. For finer-grained authorization, you can create custom authorization policies and then attach them to groups or users.

Assume that an enterprise A has developed a mobile app and has bought OSS for it. The mobile app must upload and download data to and from OSS. Because the mobile app runs on user devices, these devices are out of A’ s control.

Enterprise A does not want to allow all apps to use the AppServer to transmit data. Instead, enterprise A wants the apps to directly upload and download data to and from OSS.

For security reasons, enterprise A cannot save the AccessKey in the app.

Enterprise A also wants to minimize its security risks by, for example, giving each app an

access token with the minimum permissions that the app needs to connect to OSS and restricting the access duration to a specified period of time (such as 30 minutes).

Requirements

The mobile app needs to directly transmit data to OSS, without using a data proxy.

Enterprise A cannot give an AccessKey to the mobile app because the mobile devices are under the control of A’ s users.

The access permissions of each mobile app must be restricted to OSS object granularity.

Solution: Use RAM STS-Tokens

1. Create a role, a user and grant the necessary permissions

Step 1. Enterprise A creates a role.

A logs on to the RAM console and goes to **Roles** > **Create Role**.

In the **Create Role** window, A selects **Current Alibaba Cloud Account** as the trusted account to assume this role and enters “oss-readonly” as the role name.

After creating the role, A can view the basic role information on the role details page. For example, the global name ARN of the role is:

```
acs:ram::11223344:role/oss-readonly
```

The policy of the role is (only Enterprise A can assume this role):

```
{
"Statement": [
{
"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
"RAM": [
"acs:ram::11223344:root"
]
}
}
```

```
],
"Version": "1"
}
```

Step 2: Enterprise A grants permissions to the role by attaching a suitable authorization policy to it.

After creating a role as described in the previous step, A follows the dialog box to attach authorization policies to the role. Or A goes to the role details page and then clicks **Edit Authorization Policy** to attach authorization policies to the role.

In the authorization window, A adds the system authorization policy AliyunOSSReadOnlyAccess, and then click **OK**.

Step 3: Enterprise A creates a RAM-User for the AppServer and authorizes this user to assume the newly created role.

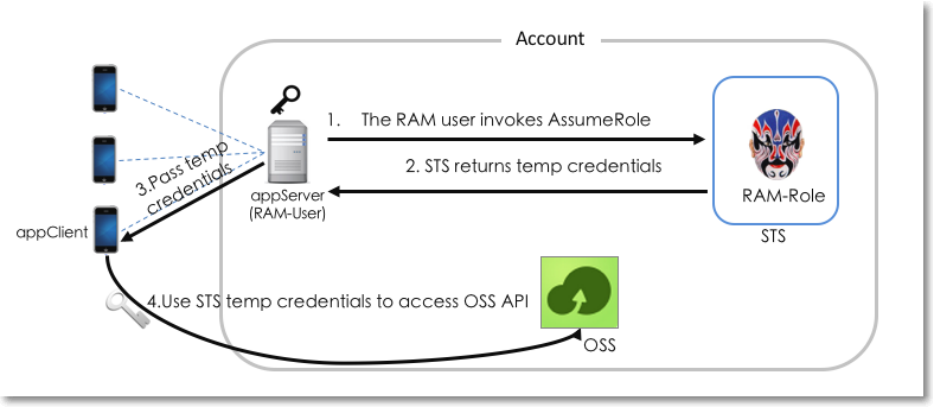
A logs on to the **RAM console** and goes to **Users** > **Create User**.

In the **Create User** window, A specifies a username such as “appserver” and checks the **Automatically generate an AccessKey for this user** box to create an AccessKey.

In the user list, A clicks the just created user to open the **User Details** page and then clicks **User Authentication Policies** > **Edit Authentication Policy**.

In the **Edit Individual Authorization Policy** window, A adds the system authorization policy AliyunSTSAssumeRoleAccess for this user, and then clicks **OK**.

2. AppServer issues STS-Tokens for resource access



Step 1: The AppServer uses the RAM-User appserver’ s AccessKey to call the STS

AssumeRole API.

For example, the AppServer uses aliyuncli to call AssumeRole.

Note: An AccessKey must be configured for appserver. The appserver is not allowed to use the AccessKey of A (that is, the primary account).

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::11223344:role/oss-readonly --RoleSessionName client-001

{
"AssumedRoleUser": {
"AssumedRoleId": "391578752573972854:client-001",
"Arn": "acs:ram::11223344:role/oss-readonly/client-001"
},
"Credentials": {
"AccessKeySecret": "93ci2umK1QKNEja6WGqi1Ba7Q2Fv9PwxZqtVF2VynUvz",
"SecurityToken":
"CAES6AIIARKAAUiwSHpkD3GXRMQk9stDr3YSVbyGqanqkS+fPlEEkjZ+dlgFnGdCI2PV93jksole8ijH8dHJrHRA5JA1YC
GsfX5hrzcNM37Vr4eVdWFVQhoCw0DXBpHv//ZcITp+ELRr4MHsnyGiErnDsXLkI7q/sbuWg6PACZ/jzQfEWQb/f7Y1Gh
1TVFMuRjEzR2pza1hUamszOGRCWTZZeEp0WEFaayISMzkxNTc4NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKT+lIHB
KjoGUnNhTUQ1QkoKATEaRQoFQWxsb3cSGwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aAwoBKhIfCg5SZXNvdXJjZU
VxdWFscxIIUmVzb3VyY2UaAwoBKkoFNDMyNzRSBTI2ODQyWg9Bc3N1bWVkUm9sZVVzZXJgAGoSMzkxNTc4NzUy
NTczOTcyODU0cgllY3MtYWRtaW544Mbewo/26AE=",
"Expiration": "2016-01-13T15:02:37Z",
"AccessKeyId": "STS.F13GjskXTjk38dBY6YxJtXAZk"
},
"RequestId": "E1779AAB-E7AF-47D6-A9A4-53128708B6CE"
}
```

Restrict the STS-Token permissions

If no policy parameters are specified during calling the AssumeRole API, this STS-Token has all oss-readonly permissions.

If you need to restrict the permissions of the STS-Token, for example, to only allow access to sample-bucket/2015/01/01/*.jpg, you can use the policy parameters to further restrict the STS-Token’ s permissions.

For example,

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::11223344:role/oss-readonly --RoleSessionName client-002 --Policy
"{\"Version\":\"1\", \"Statement\": [{\"Effect\":\"Allow\", \"Action\":\"oss:GetObject\",
\"Resource\":\"acs:oss:*:*:sample-bucket/2015/01/01/*.jpg\"}]}"

{
"AssumedRoleUser": {
"AssumedRoleId": "391578752573972854:client-002",
"Arn": "acs:ram::11223344:role/oss-readonly/client-002"
},
"Credentials": {
"AccessKeySecret": "28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7xEMow",
"SecurityToken":
```

"CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU
78FkszxhnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4NzUyNTczOTcyODU0Kgpjb
GllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEaegoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDw
oNb3NzOkdldE9iamVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoqOio6c2FtcGxlLWJ1Y2tl
dC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4
NTRyCWVjcy1hZG1pbnjgxt7Cj/boAQ==",
"Expiration": "2016-01-13T15:03:39Z",
"AccessKeyId": "STS.FJ6EMcS1JLZgAcBJSTDG1Z4CE"
},
"RequestId": "98835D9B-86E5-4BB5-A6DF-9D3156ABA567"
}

Additionally, the default validity period of the preceding STS-Token is 3600 seconds. You can use the DurationSeconds parameter to limit the STS-Token expiration time (the expiration time cannot exceed 3600 seconds).

Step 2: The AppServer retrieves and parses the credentials.

The AppServer retrieves the AccessKeyId, AccessKeySecret and SecurityToken from the credentials returned by the AssumeRole API.

Because the STS-Token validity period is relatively short, if the application requires a longer validity period, AppServer must re-issue a new STS-Token (for example, issue one STS-Token every other 1800 seconds).

Step 3: The AppServer securely transmits an STS-Token to the AppClient.

Step 4: The AppClient uses the STS-Token to directly access a cloud service API (such as OSS).

The operation commands for aliyuncli to use an STS-Token to access an OSS object are as follows (a STS-Token is issued to client-002):

```
Configure STS-Token syntax: aliyuncli oss Config --host <OssEndPoint> --accessid <AccessKeyId> --accesskey
<AccessKeySecret> --sts_token <SecurityToken>

$ aliyuncli oss Config --host oss.aliyuncs.com --accessid STS.FJ6EMcS1JLZgAcBJSTDG1Z4CE --accesskey
28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7xEMow --sts_token
CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU7
8FkszxhnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4NzUyNTczOTcyODU0KgpjbG
llbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEaegoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwo
Nb3NzOkdldE9iamVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoqOio6c2FtcGxlLWJ1Y2tld
C8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4
NTRyCWVjcy1hZG1pbnjgxt7Cj/boAQ==

Access OSS object

$ aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg grass.jpg
```

More references

More references to mobile app access include: