ALIBABA CLOUD

Alibaba Cloud

Data Transmission Service
RAM-based Access Control

Document Version: 20200820

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.Authorize DTS to access Alibaba Cloud resources

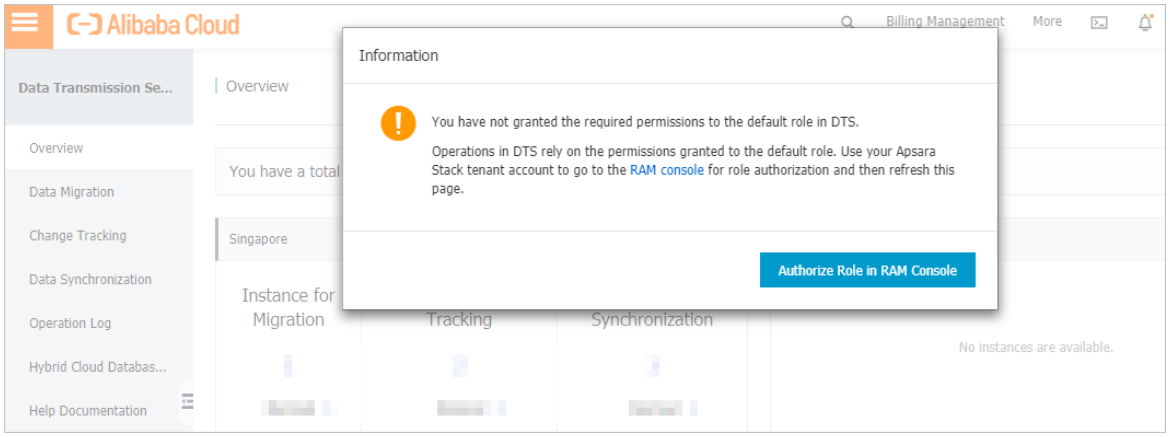
The first time that you log on to the Data Transmission Service (DTS) console, you are prompted to assign the **AliyunDTSDefaultRole** role to DTS. With this role, DTS can access the resources owned by the current Alibaba Cloud account during data replication.

Note

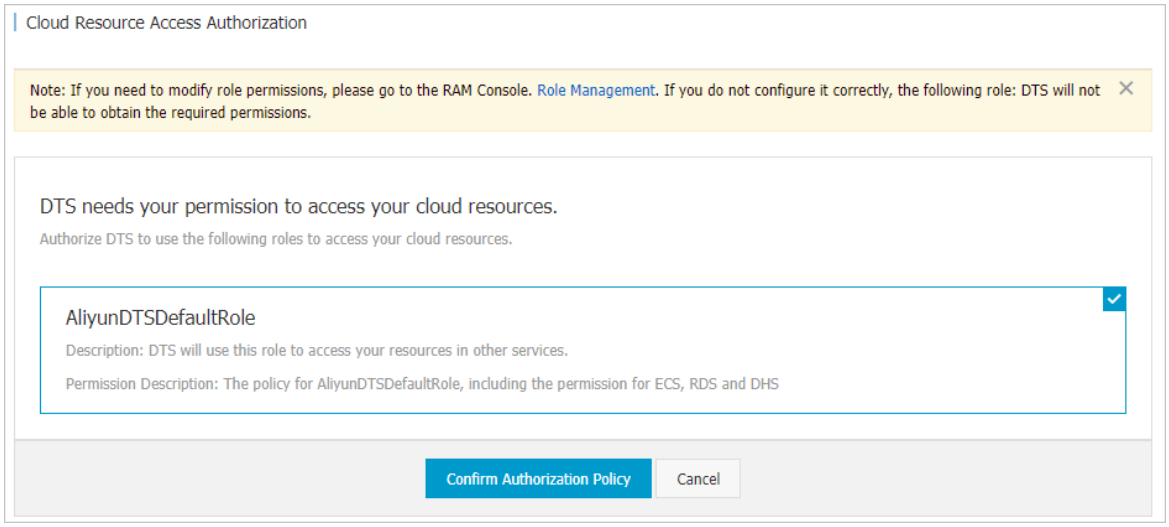
If no authorization message is displayed when you log on to the DTS console, this indicates that DTS has already been authorized. You can skip the steps that are described in this topic.

Procedure

1. Log on to the DTS console.
2. In the **Information** message, click **Authorize Role in RAM Console**.



3. In the **Cloud Resource Access Authorization** dialog box, click **Confirm Authorization Policy**.



Permission policy

The **AliyunDTSDefaultRole** policy is attached to the default role of DTS. This policy allows DTS to access ApsaraDB for RDS, ECS, DataHub, Elasticsearch, DRDS, ApsaraDB for PolarDB, ApsaraDB for MongoDB, ApsaraDB for Redis, and HybridDB for MySQL. The policy is defined as follows:

```
{
"Version": "1",
"Statement": [
{
"Action": [
"rds:Describe*",
"rds:CreateDBInstance",
"rds:CreateAccount*",
"rds:CreateDataBase*",
"rds:ModifySecurityIps",
"rds:GrantAccountPrivilege"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"ecs:DescribeSecurityGroupAttribute",
"ecs:DescribeInstances",
"ecs:DescribeRegions",
"ecs:AuthorizeSecurityGroup"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"dhs:ListProject",
"dhs:GetProject",
"dhs:CreateTopic",
"dhs:ListTopic",
"dhs:GetTopic",
"dhs:UpdateTopic",
"dhs:ListShard",
"dhs:MergeShard",
"dhs:SplitShard",
"dhs:PutRecords",
"dhs:GetRecords",
```

```
"dhs:GetCursors"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"elasticsearch:DescribeInstance",
"elasticsearch:ListInstance",
"elasticsearch:UpdateAdminPwd",
"elasticsearch:UpdatePublicNetwork",
"elasticsearch:UpdateBlackIps",
"elasticsearch:UpdateKibanaIps",
"elasticsearch:UpdatePublicIps",
"elasticsearch:UpdateWhiteIps"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"drds:DescribeDrds*",
"drds:ModifyDrdsIpWhiteList",
"drds:DescribeRegions",
"drds:DescribeRdsList",
"drds:CeateDrdsDB",
"drds:DescribeShardDBs"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"polardb:DescribeDBClusterIPArrayList",
"polardb:DescribeDBClusterNetInfo",
"polardb:DescribeDBClusters",
"polardb:DescribeRegions",
"polardb:ModifySecurityIps"
],
"Resource": "*",
```

```
"Effect": "Allow"
},
{
"Action": [
"dds:DescribeDBInstanceAttribute",
"dds:DescribeReplicaSetRole",
"dds:DescribeSecurityIps",
"dds:DescribeDBInstances",
"dds:ModifySecurityIps",
"dds:DescribeRegions"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"kvstore:DescribeSecurityIps",
"kvstore:DescribeInstances",
"kvstore:DescribeRegions",
"kvstore:ModifySecurityIps"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"petadata:DescribeInstanceInfo",
"petadata:DescribeSecurityIPs",
"petadata:DescribeInstances",
"petadata:ModifySecurityIPs"
],
"Resource": "*",
"Effect": "Allow"
}
]
}
```

2.Authorize a RAM user to use DTS

You can create a Resource Access Management (RAM) user account and then grant the RAM user required permissions to access Data Transmission Service (DTS) functionalities. In this way, you can assign different permissions to different users.

Permission policies

DTS provides two system permission policies, for read/write and read-only operations, respectively.

> Note API operation-level access control is not supported.

- Read/write policy: **AliyunDTSFullAccess**

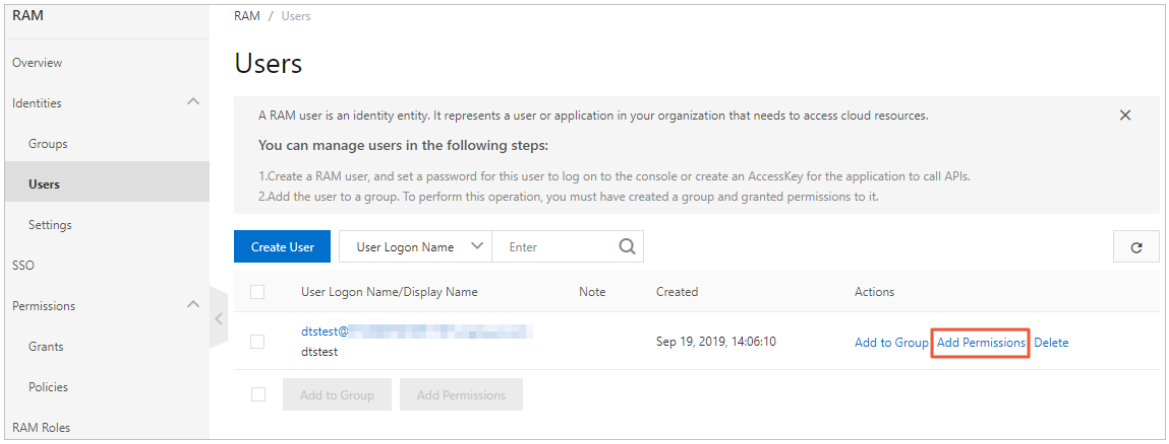
  This policy grants the read/write permission on DTS. RAM users with this permission policy can purchase, configure, and manage DTS instances and tasks.

- Read-only policy: **AliyunDTSReadOnlyAccess**

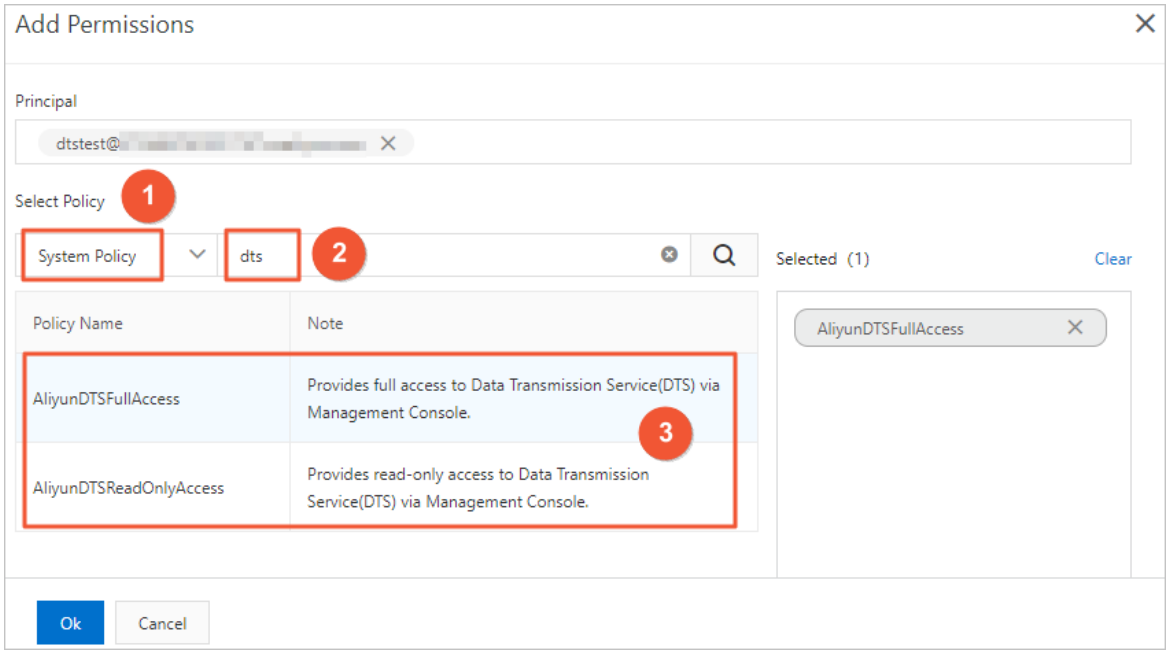
  This policy grants the read permission on DTS. RAM users with this permission policy can view the details and configurations of all DTS tasks under the Alibaba Cloud account. However, these RAM users cannot perform change operations.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a RAM user. For more information, see Create a RAM user.
3. In the left-side navigation pane, click **Identities** > **Users**.
4. Find the RAM user that you want to authorize, and then click **Add Permissions** in the **Actions** column.



5. In the **Add Permissions** dialog box, select the required permission policies.



i. Select **System Policy**.

ii. Enter *dts* in the search box to find all system permission policies that are related to DTS.

iii. Click a policy name to add the policy to the **Selected** list.

> **Note** For more information about permission policies, see Permission policies.

6. Click **OK**.
7. Click **Finished**.

Next steps

Log on to the RAM console as a RAM user.

3.Use a custom policy to authorize a RAM user to manage DTS instances

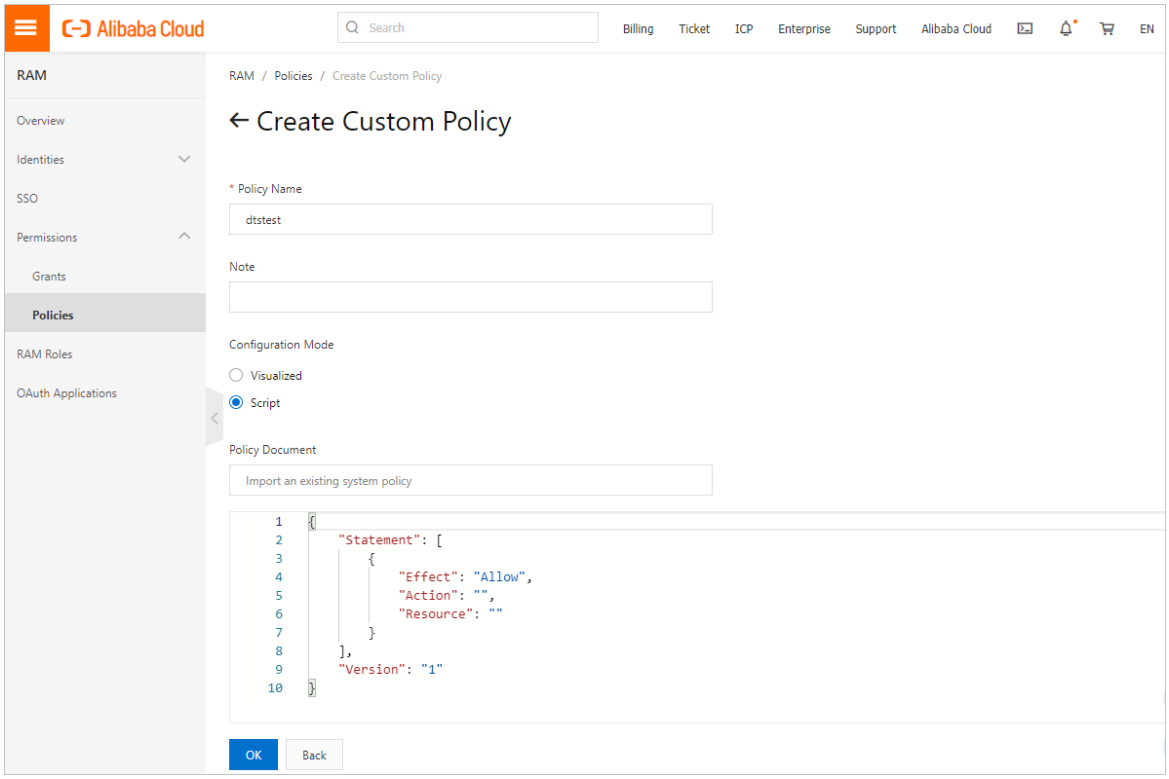
This topic describes how to create a custom policy. Custom policies provide finer-grained control than system policies. For example, you can create a custom policy to control the permissions on specific instances or operations.

Context

A policy defines a set of permissions that are described based on the policy structure and syntax. A policy describes the authorized resource sets, authorized operation sets, and authorization conditions. For more information, see Policy structure and syntax.

Step 1: Create a custom policy

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. Complete the settings for the custom policy.



Setting	Description
Policy Name	Enter a name for the policy.
Note	Optional. Enter a description for the policy.
Configuration Mode	Select **Script**. To configure policies for DTS, you must select **Script**.

Setting	Description
Policy Document	Select an existing system policy from the drop-down list. Note This topic describes how to create a custom policy. You do not need to configure this parameter.
Policy	Enter the permission policy. You can edit the sample policies that are listed in this topic based on your needs. Note ○ A policy defines a set of permissions that are described based on the policy structure and syntax. A policy describes the authorized resource sets, authorized operation sets, and authorization conditions. For more information, see Policy structure and syntax. ○ Resource-level and operation-level access control is supported.

Sample custom policies:

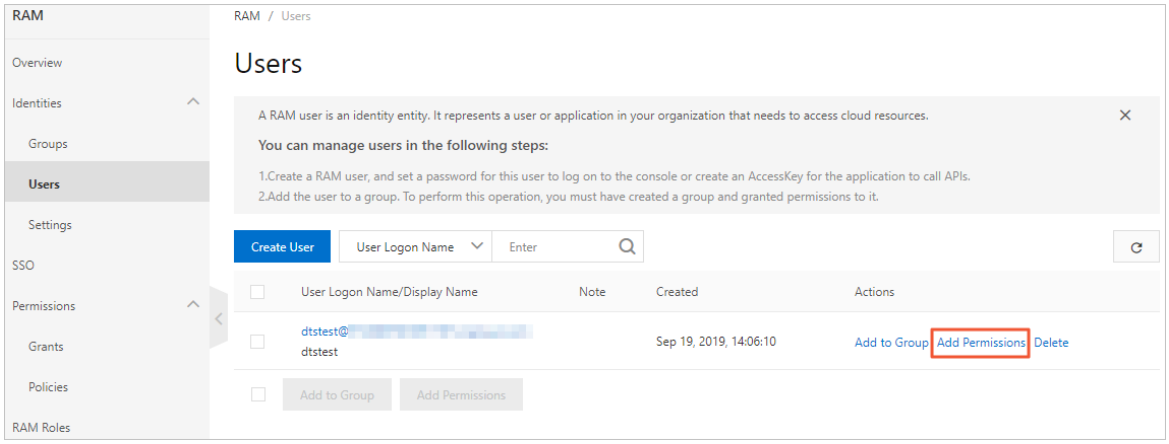
Note
- You must replace the `DTS instance ID` in the following code with the actual ID of your DTS instance.
- If the read-only permission on a DTS instance is granted to a RAM user, the RAM user can query task details and configurations but cannot change configurations. If the read/write permissions on a DTS instance are granted to a RAM user, the RAM user can configure and manage DTS instances and tasks.

- demo 1: Read-only permission on a single DTS instance.
- demo 2: Read/write permissions on multiple DTS instances.
- demo 3: View the configurations of a data synchronization task.
- demo 4: Start or pause a data synchronization task.

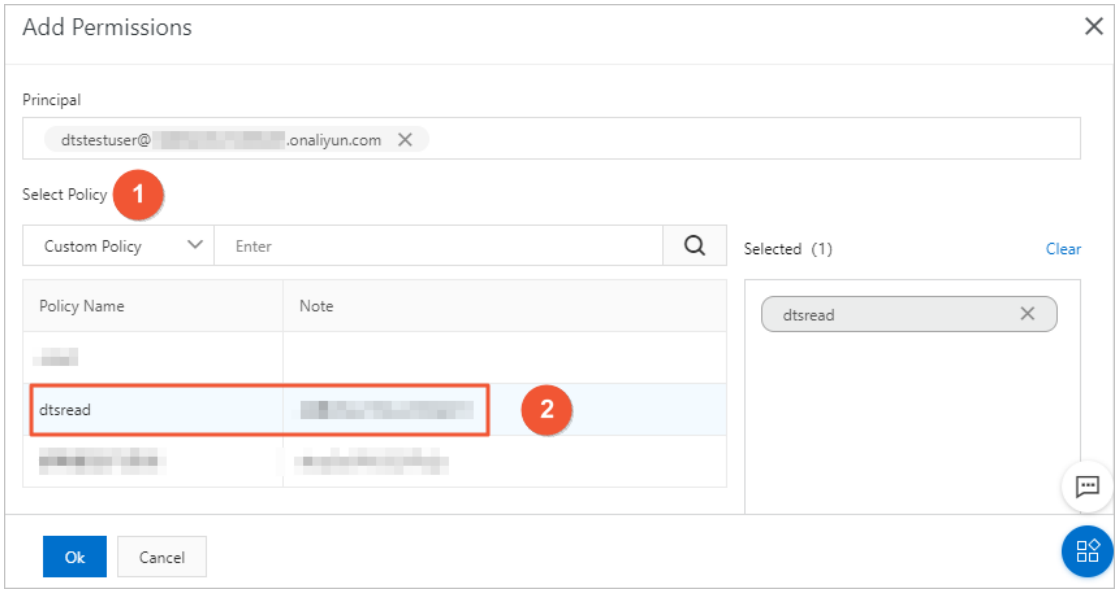
5. Click **OK**.

Step 2: Attach the custom policy to a RAM user

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a RAM user.
3. In the left-side navigation pane, click **Users** under **Identities**.
4. In the **User Logon Name/Display Name** column, find the target RAM user.
5. Click **Add Permissions** in the Actions column.



6. In the **Add Permissions** pane, select the required permission policies.
   i. Select **Custom Policy**.
   ii. Click the name of a custom policy to add the policy to the **Selected** section.



7. Click **OK**.
8. Click **Finished**.

Scenarios of operation-level authorization

Note

- The `DescribeMigrationJobs`, `DescribeSubscriptionInstances`, and `DescribeSynchronizationJobs` policies authorize a RAM user to query available DTS instances. If a RAM user has the permissions only on some instances, the user must query available DTS instances before the user can perform related operations.
- To authorize a RAM user to configure data migration, data synchronization, or change tracking, you must create a custom policy and attach the policy to the user. For more information, see Permission policy.

Feature	Operation in the DTS console	Permission policy
Data migration	Create a data migration task	CreateMigrationJob
	Query data migration tasks	DescribeMigrationJobs
	View the details of a data migration task	DescribeMigrationJobs DescribeMigrationJobDetail DescribeMigrationJobStatus
	Modify the name of a data migration task	DescribeMigrationJobs ModifyMigrationObject
	Configure a data migration task	DescribeMigrationJobs DescribeMigrationJobDetail DescribeMigrationJobStatus CreateMigrationJob
	View precheck details	DescribeMigrationJobs DescribeMigrationJobStatus
	Create a similar data migration task	DescribeMigrationJobs DescribeMigrationJobDetail DescribeMigrationJobStatus CreateMigrationJob
	Monitor a data migration task and set alerts	DescribeMigrationJobs DescribeMigrationJobAlert ConfigureMigrationJobAlert
	Change the password that is used to log on to an instance	DescribeMigrationJobs DescribeMigrationJobDetail ModifyMigrationObject
	Start a data migration task	DescribeMigrationJobs StartMigrationJob DescribeMigrationJobDetail

Feature	Operation in the DTS console	Permission policy
	Pause a data migration task	DescribeMigrationJobs SuspendMigrationJob
	View the details of schema migration	DescribeMigrationJobs DescribeMigrationJobStatus
	View the details of full data migration	DescribeMigrationJobs DescribeMigrationJobStatus
	View the details of incremental data migration	DescribeMigrationJobs DescribeMigrationJobStatus
	View the performance of full data migration or incremental data migration	DescribeMigrationJobs DescribeMigrationJobDetail
	View task logs	DescribeMigrationJobs DescribeMigrationJobDetail
	Create a change tracking task	CreateSubscriptionInstance
	Query change tracking tasks	DescribeSubscriptionInstances
	View the details of a change tracking task	DescribeSubscriptionInstances DescribeSubscriptionInstanceStatus
	Modify the name of a change tracking task	DescribeSubscriptionInstances ModifySubscriptionObject
	Modify the objects for change tracking	DescribeSubscriptionInstances DescribeSubscriptionInstanceStatus ModifySubscriptionObject
	Create consumer groups	DescribeSubscriptionInstances CreateConsumerGroup

Feature	Operation in the DTS console	Permission policy
Change tracking	View the information about a consumer group	DescribeSubscriptionInstances DescribeConsumerGroup
	Modify the password of a consumer group	DescribeSubscriptionInstances ModifyConsumerGroupPassword
	Delete a consumer group	DescribeSubscriptionInstances DeleteConsumerGroup
	Change the password that is used to log on to an instance	DescribeSubscriptionInstances DescribeSubscriptionInstanceStatus ModifySubscriptionObject
	Delete a change tracking task	DescribeSubscriptionInstances DeleteSubscriptionInstance
	Monitor a change tracking task and set alerts	DescribeSubscriptionInstances DescribeSubscriptionInstanceAlert ConfigureSubscriptionInstanceAlert
	Configure a change tracking task	DescribeSubscriptionInstances DescribeSubscriptionInstanceStatus ModifySubscriptionObject
	View task logs	DescribeSubscriptionInstances DescribeSubscriptionInstanceStatus
	Create a data synchronization task	CreateSynchronizationJob
	Query data synchronization tasks	DescribeSynchronizationJobs
	View the details of a data synchronization task	DescribeSynchronizationJobs DescribeSynchronizationJobStatus

Feature	Operation in the DTS console	Permission policy
Data synchronization	Modify the name of a data synchronization task	DescribeSynchronizationJobs ModifySynchronizationObject
	View the configurations of a data synchronization task	DescribeSynchronizationJobs DescribeSynchronizationJobStatus
	View the objects to be synchronized	DescribeSynchronizationJobs DescribeSynchronizationJobStatus
	View the status of initial schema synchronization and initial full data synchronization	DescribeSynchronizationJobs DescribeSynchronizationJobStatus
	View the performance of full data synchronization or incremental data synchronization	DescribeSynchronizationJobs DescribeSynchronizationJobStatus
	View the modification records of the objects to be synchronized	DescribeSynchronizationJobs
	View task logs	DescribeSynchronizationJobs DescribeSynchronizationJobStatus
	Configure a data synchronization task	DescribeSynchronizationJobs DescribeSynchronizationJobStatus ModifySynchronizationObject
	Start a data synchronization task	DescribeSynchronizationJobs StartSynchronizationJob
	Pause a data synchronization task	DescribeSynchronizationJobs SuspendSynchronizationJob
	Modify the objects to be synchronized	DescribeSynchronizationJobs DescribeSynchronizationJobStatus ModifySynchronizationObject

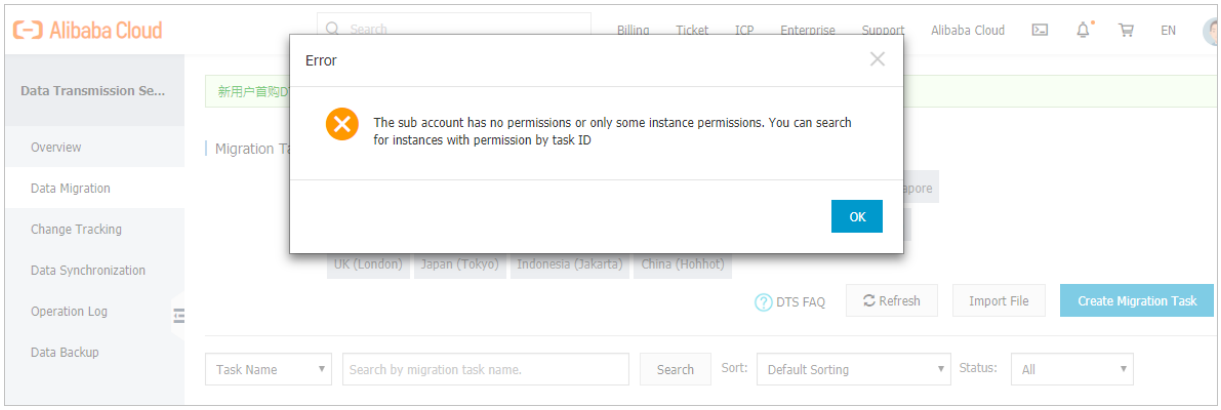
Feature	Operation in the DTS console	Permission policy
	Delete a data synchronization task	DescribeSynchronizationJobs DeleteSynchronizationJob
	Stop a data synchronization task	DescribeSynchronizationJobs DeleteSynchronizationJob
	Monitor a data synchronization task and set alerts	DescribeSynchronizationJobs DescribeSynchronizationJobAlert ConfigureSynchronizationJobAlert
	Change the password that is used to log on to an instance	DescribeSynchronizationJobs DescribeSynchronizationJobStatus ModifySubscriptionObject

What to do next

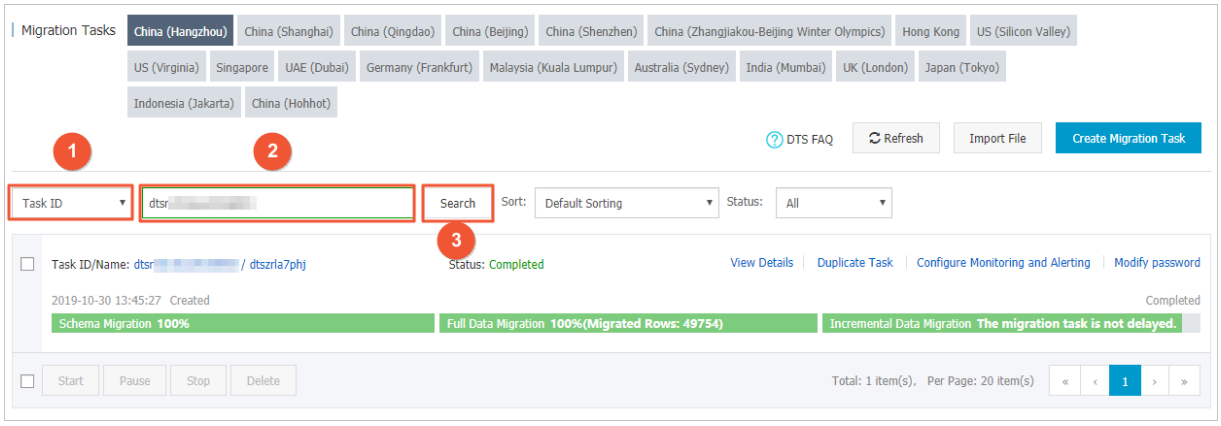
Log on to the RAM console as a RAM user.

FAQ

Q: Why does an error message instead of the instance list appear when I log on to the DTS console as a RAM user?



A: The RAM user may have no permissions or may have permissions only on some instances. In this case, the DTS console does not show the instance list. You must contact the RAM administrator and obtain the IDs of the DTS instances on which the RAM user has administrative permissions. Then, you can search for DTS instances by using their IDs in the DTS console.



4.Authorize a RAM user to use the DTS SDK

Data Transmission Service (DTS) allows you to use Resource Access Management (RAM) to manage permission policies. You can create and manage tasks as a RAM user. You can also subscribe to data changes in real time by using the AccessKey ID and AccessKey secret of the RAM user.

Permission policies

DTS supports read/write and read-only policies.

- Read/write policy: **AliyunDTSFullAccess**

  This policy grants the read/write permission on DTS. If this policy is attached to a RAM user, the RAM user can purchase, configure, and manage DTS instances.

- Read-only policy: **AliyunDTSReadOnlyAccess** This policy grants the read permission on DTS. If this policy is attached to a RAM user, the RAM user can view the details and configurations of all DTS tasks under the Alibaba Cloud account. However, the RAM user cannot perform change operations.

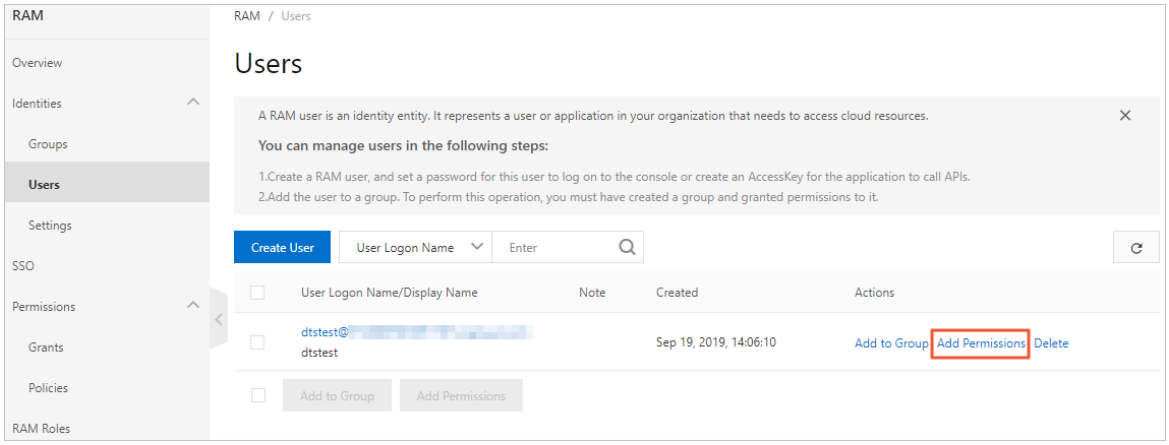
> **Note** Change operations include the purchase, configuration, and management of DTS instances.

Procedure

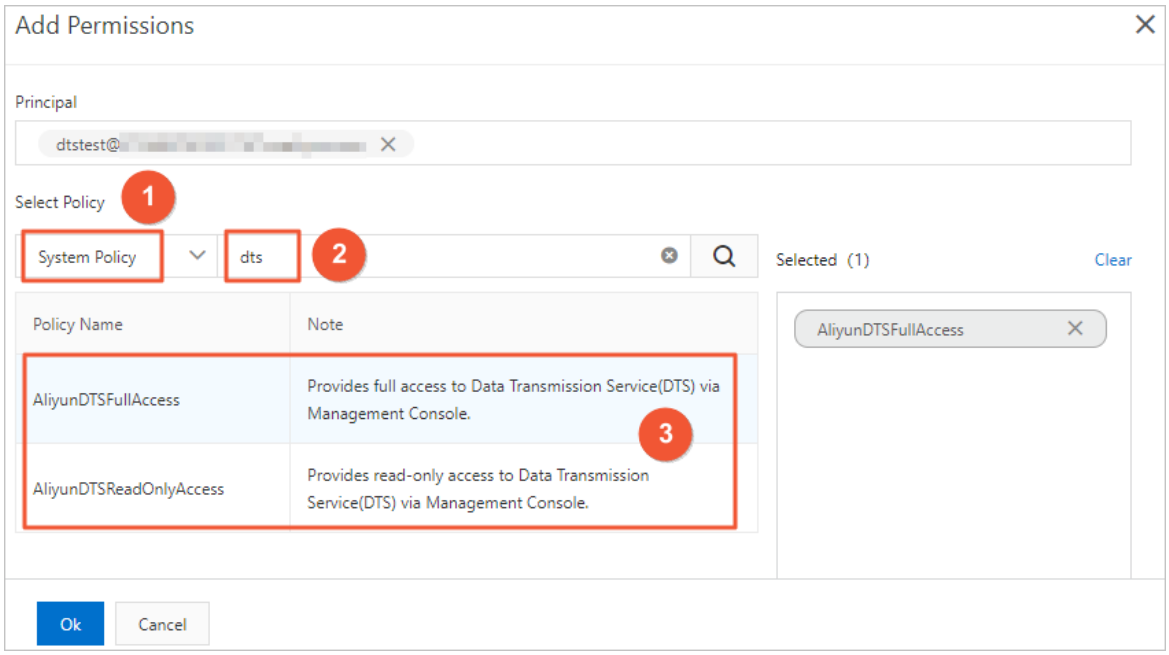
1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a RAM user.

> **Note** When creating a RAM user, you must specify **Programmatic Access** as the access mode and download and save the AccessKey pair.

3. In the left-side navigation pane, click **Users** under **Identities**.
4. In the **User Logon Name/Display Name** column, find the target RAM user.
5. Click **Add Permissions** in the Actions column.



6. In the **Add Permissions** dialog box, select the required permission policies.



   i. Select **System Policy**.
   ii. Enter *dts* in the search box to query the system permission policies that are related to DTS.
   iii. Click **AliyunDTSFullAccess** to add the policy to the **Selected** section.
7. Click **OK**.
8. Click **Finished**.

Subscribe to data changes as a RAM user

After you create a RAM user and grant the required permissions to the RAM user, you can use the SDK provided by DTS to subscribe to data changes. For more information about how to use the DTS SDK, see Introduction to SDK Demo.

> **Note** You must replace the sample AccessKey pair in the SDK demo with the AccessKey pair of your RAM user.

5.Configure RAM authorization for cross-account data replication

DTS supports data migration and synchronization between ApsaraDB for RDS instances that belong to different Alibaba Cloud accounts. This topic describes how to configure RAM authorization for the Alibaba Cloud account to which the source instance belongs if the destination instance belongs to a different Alibaba Cloud account.

Prerequisites

The Alibaba Cloud account to which the source instance belongs has authorized the RAM role of DTS to access the cloud resources of the account. For more information, see Authorize DTS to access cloud resources.

Instance types supported by cross-account data migration and synchronization

Feature	Source instance type	Destination instance type
Data migration	RDS instance	RDS instance
		DRDS instance
		HybridDB for MySQL instance
		ApsaraDB for OceanBase instance
		User-created database hosted on ECS
		User-created database with a public IP address
Data synchronization	RDS instance	RDS instance
		MaxCompute (previous name: ODPS) instance
		Elasticsearch instance

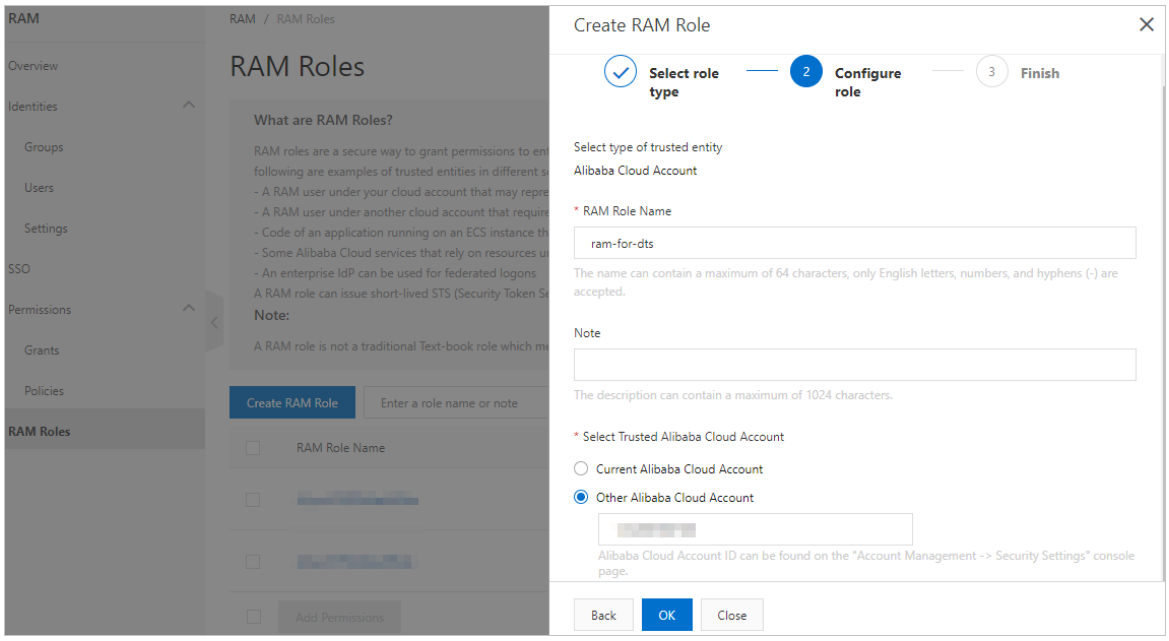
Background information

When you use DTS for data migration or synchronization, you must configure RAM authorization for the Alibaba Cloud account to which the source instance belongs. You must specify the Alibaba Cloud account to which the destination instance belongs as a trusted account. This ensures that the destination account can access cloud resources of the Alibaba Cloud account to which the source instance belongs.

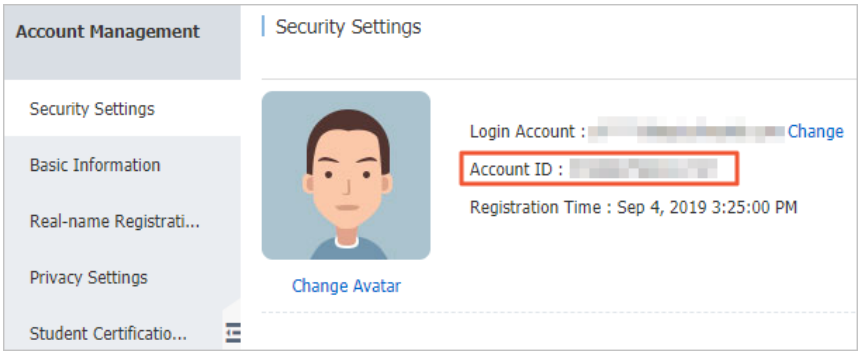
> **Note** After authorization, you can create a data migration task or data synchronization task by using the Alibaba Cloud account to which the destination instance belongs.

Procedure

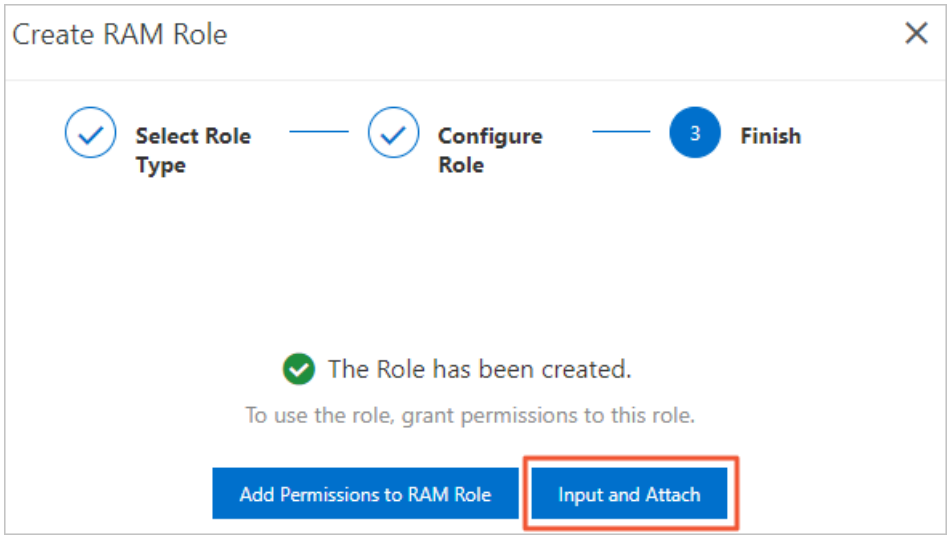
1. Log on to the RAM console with the Alibaba Cloud account to which the source instance belongs.
2. In the left-side navigation pane, click **RAM Roles**.
3. Click **Create RAM Role**, select **Alibaba Cloud Account**, and then click **Next**.
4. On the **Create RAM Role** page, configure parameters for the RAM role.



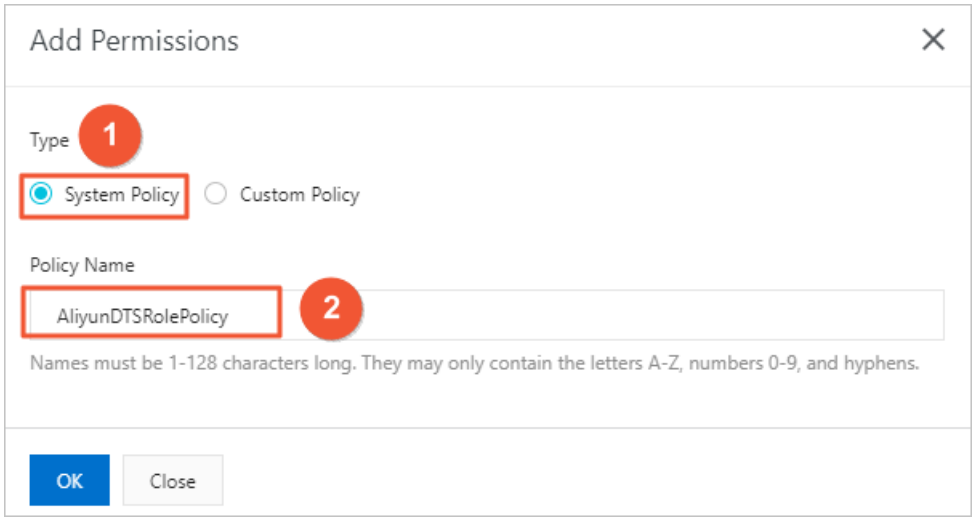
Parameter	Description
RAM Role Name	Specify a name for the RAM role. In this example, enter **ram-for-dts**. **Note** The name must be 1 to 64 characters in length and can contain letters, digits, and hyphens (-).
Note	Optional. Specify the description for the RAM role.

Parameter	Description
Select Trusted Alibaba Cloud Account	Select **Other Alibaba Cloud Account** and enter the ID of the Alibaba Cloud account to which the destination instance belongs. **Note** To obtain the ID of the Alibaba Cloud account to which the destination instance belongs, you must log on to the Alibaba Cloud console with the account and go to the Account Management page. 

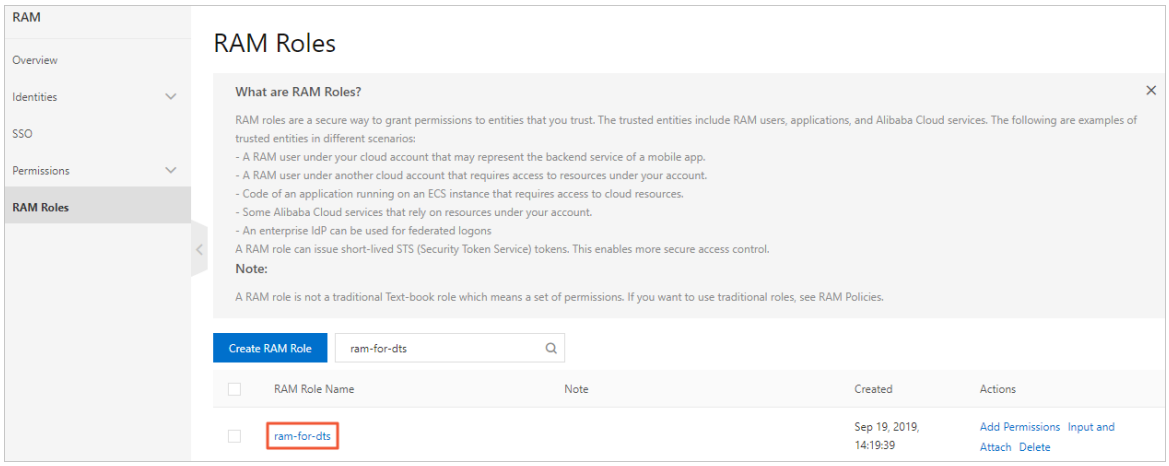
5. Click **OK**.
6. Click **Input and Attach**.



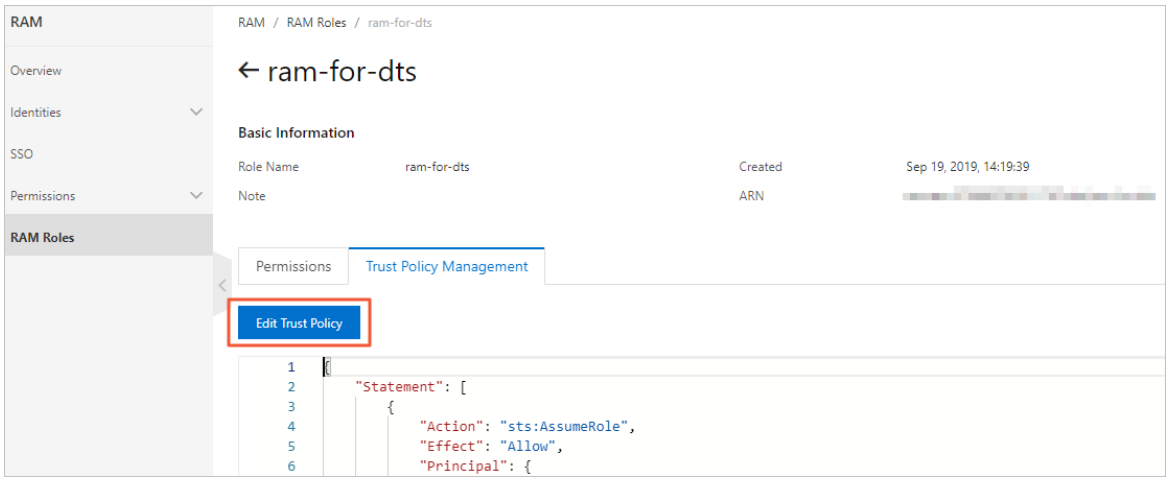
7. On the **Add Permissions** page, select **System Policy** and enter **AliyunDTSRolePolicy**.



8. Click **OK**.
9. Click **Close**.
10. On the **RAM Roles** page, find the newly created RAM role, and click the role name to view details.

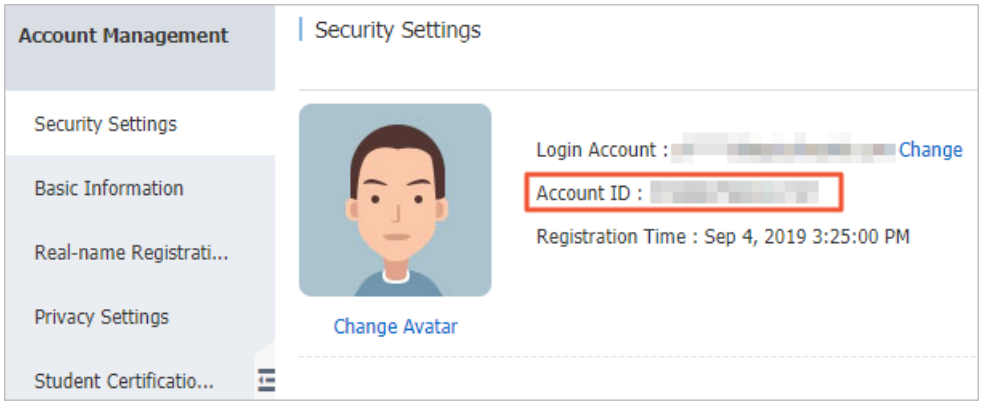


11. On the **Basic Information** page of the RAM role, click the **Trust Policy Management** tab.
12. On the **Trust Policy Management** tab, click **Edit Trust Policy**, and copy the following sample statements to the page that appears.



```
{
"Statement": [
{
"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
"RAM": [
"acs:ram::<ID of Alibaba Cloud account to which the destination instance belongs>:root"
],
"Service": [
"<ID of Alibaba Cloud account to which the destination instance belongs>@dts.aliyuncs.com"
]
}
}
],
"Version": "1"
}
```

Note To obtain the ID of the Alibaba Cloud account to which the destination instance belongs, you must log on to the Alibaba Cloud console with the account and go to the Account Management page. Then, you must replace the `ID of Alibaba Cloud account to which the destination instance belongs` in the preceding statements with the obtained ID.



After authorization, you can create a task to migrate or synchronize data between RDS instances that belong to different Alibaba Cloud accounts.

Next steps

Log on to the DTS console with the Alibaba Cloud account to which the destination instance belongs, and then create a data migration task or data synchronization task.

6.Configure RAM authorization for data migration from a user-created database in a VPC across different Alibaba Cloud accounts

This topic describes how to configure RAM authorization for data migration from a user-created database in a VPC across different Alibaba Cloud accounts. After authorization, DTS can read data from a VPC that belongs to another Alibaba cloud account when you configure data migration. You can migrate data from a user-created database that is connected over Express Connect across different Alibaba Cloud accounts.

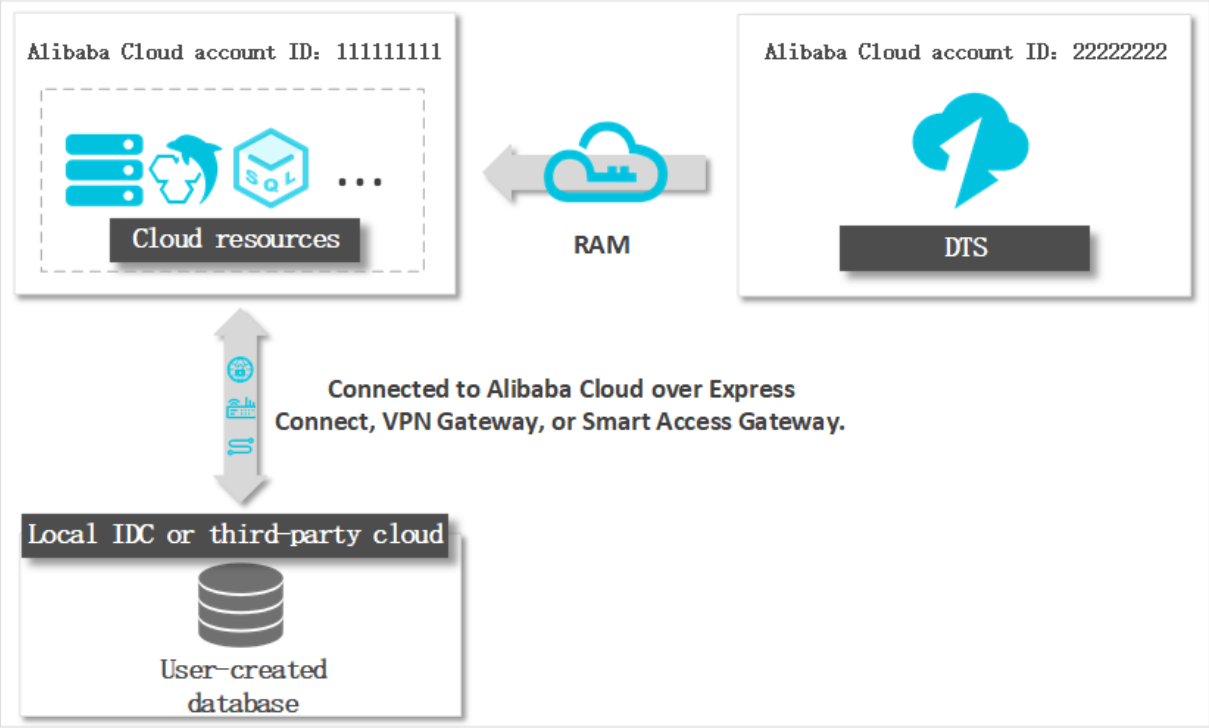
Prerequisites

The Alibaba Cloud account to which the Express Connect circuit belongs has authorized the RAM role of DTS to access the cloud resources of the account. For more information, see Authorize DTS to access cloud resources.

Context

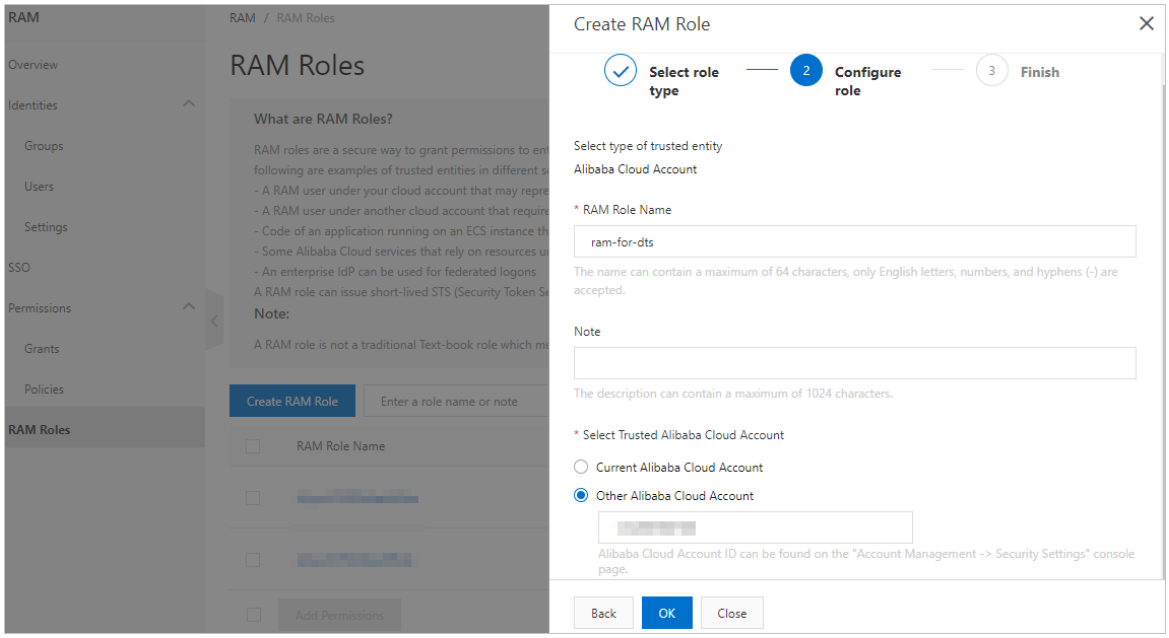
The on-premises data center or a third-party cloud is connected to Alibaba Cloud VPC over Express Connect, VPN Gateway, or Smart Access Gateway. You need to migrate data from a user-created database that resides in an on-premises data center or a third-party cloud to an RDS instance across different Alibaba Cloud accounts. The following figure shows the architecture for this scenario.

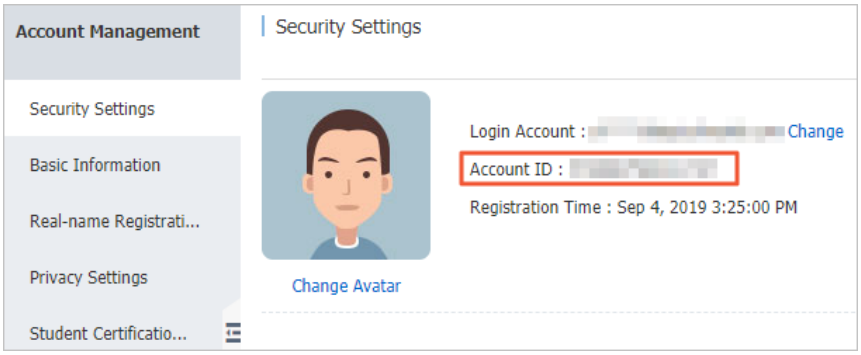
> **Note** Before you can use DTS to migrate data from a user-created database in a VPC cross different Alibaba Cloud accounts, you must perform the following steps: Configure RAM authorization for the Alibaba Cloud account to which the Express Connect circuit belongs (Account A), specify the Alibaba Cloud account to which the destination instance belongs (Account B) as a trusted account, and then authorize Account B to access the cloud resources of Account A.



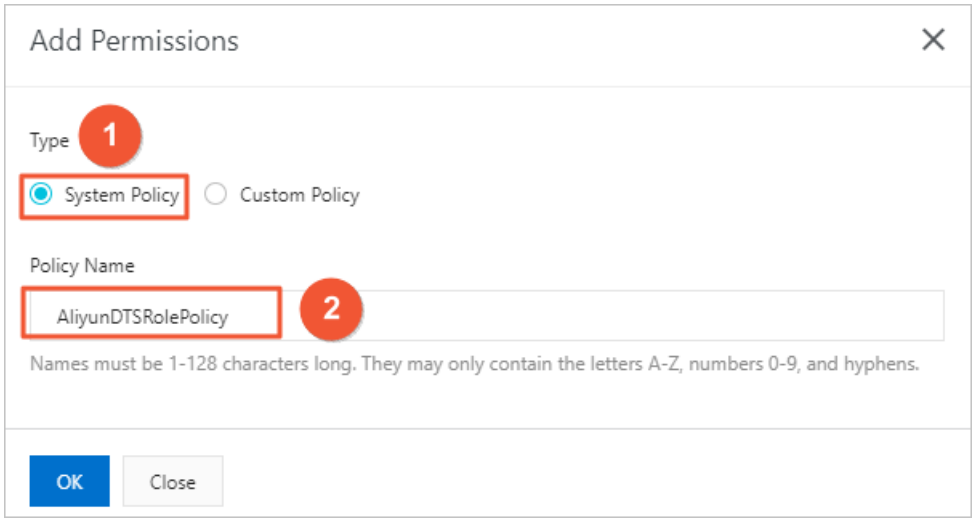
Step 1: Create a RAM role and grant the default permission on DTS to the RAM role

1. Log on to the RAM console by using the Alibaba Cloud account to which the Express Connect circuit belongs.
2. In the left-side navigation pane, click **RAM Roles**.
3. Click **Create RAM Role**, select **Alibaba Cloud Account**, and then click **Next**.
4. In the **Create RAM Role** pane, configure parameters for the RAM role.



Parameter	Description
RAM Role Name	Specify a name for the RAM role. In this example, enter **ram-for-dts**. **Note** The name must be 1 to 64 characters in length and can contain letters, digits, and hyphens (-).
Note	Optional. Specify the description for the RAM role.
Select Trusted Alibaba Cloud Account	Select **Other Alibaba Cloud Account** and enter the ID of the Alibaba Cloud account to which the destination instance belongs. **Note** To obtain the ID of the Alibaba Cloud account to which the destination instance belongs, you must log on to the Account Management console by using this account. The account ID is displayed on the Security Settings page. 

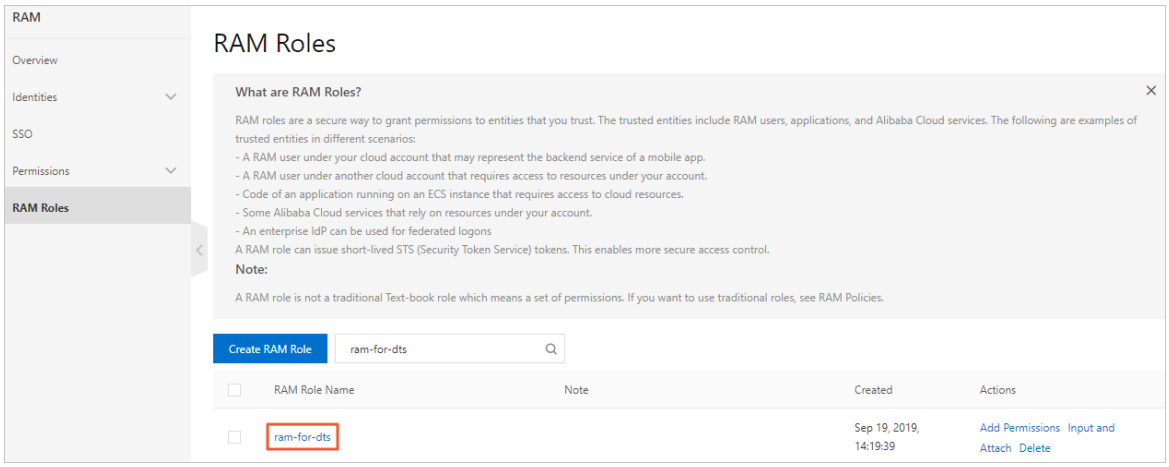
5. Click **OK**.
6. Click **Input and Attach**.
7. In the **Add Permissions** pane, select **System Policy** and enter **AliyunDTSRolePolicy**.



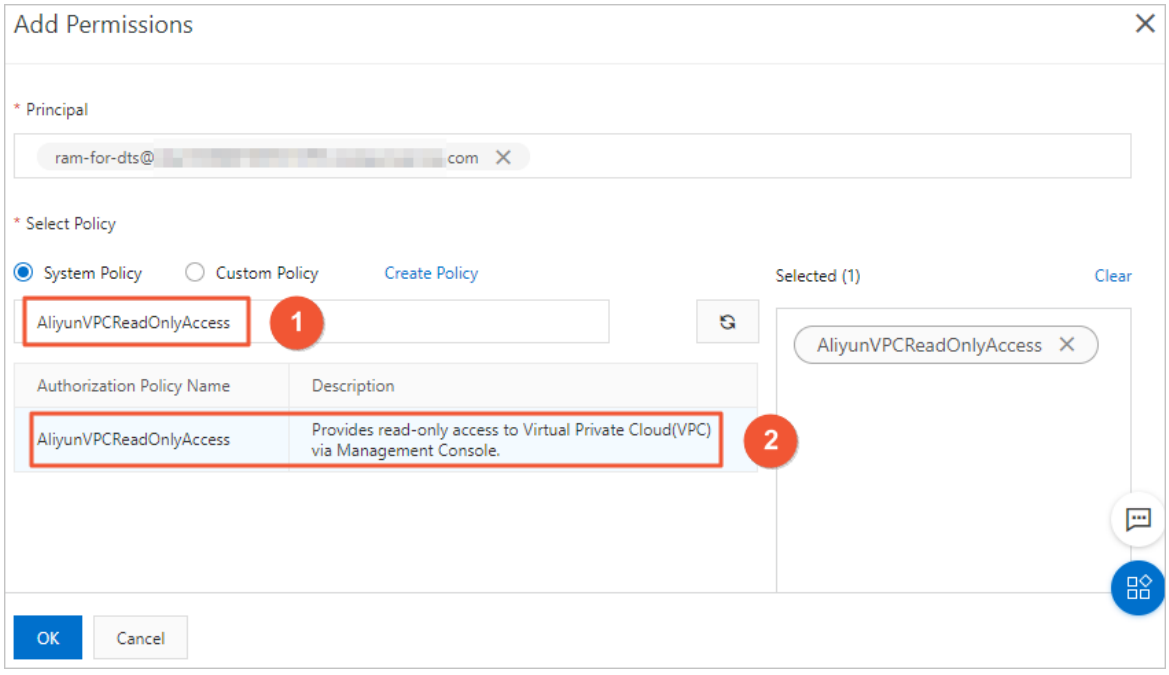
8. Click **OK**.
9. Click **Close**.

Step 2: Authorize the RAM role to access the VPC under another Alibaba Cloud account

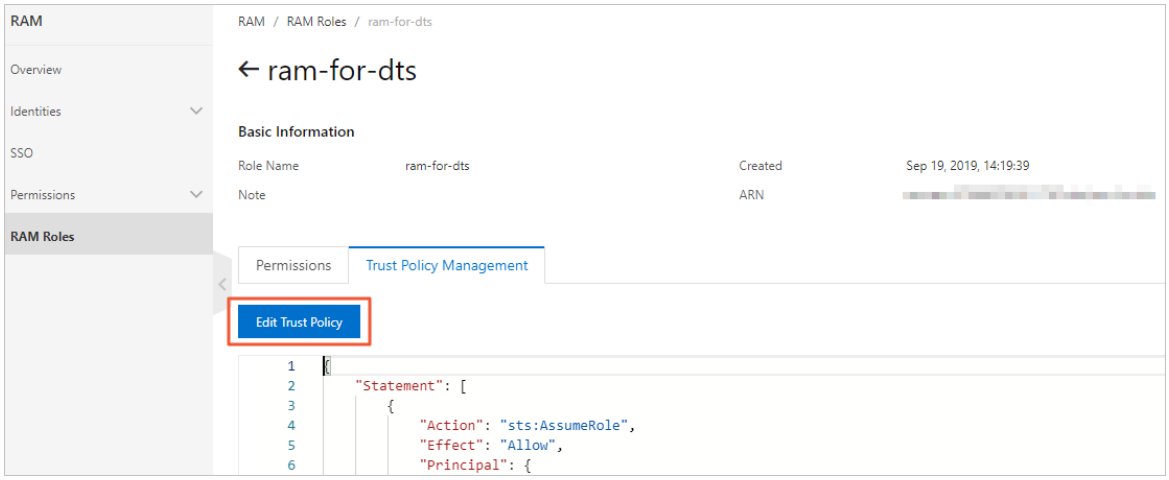
1. Log on to the RAM console by using the Alibaba Cloud account to which the Express Connect circuit belongs.
2. In the left-side navigation pane, click **RAM Roles**.
3. Find the RAM role created in step 1, and click the role name.



4. On the **Basic Information** page of the RAM role, click **Add Permissions**.
5. In the **Add Permissions** pane, enter **AliyunVPCReadOnlyAccess** in the search box and click the policy name to move the policy to the **Selected** section.

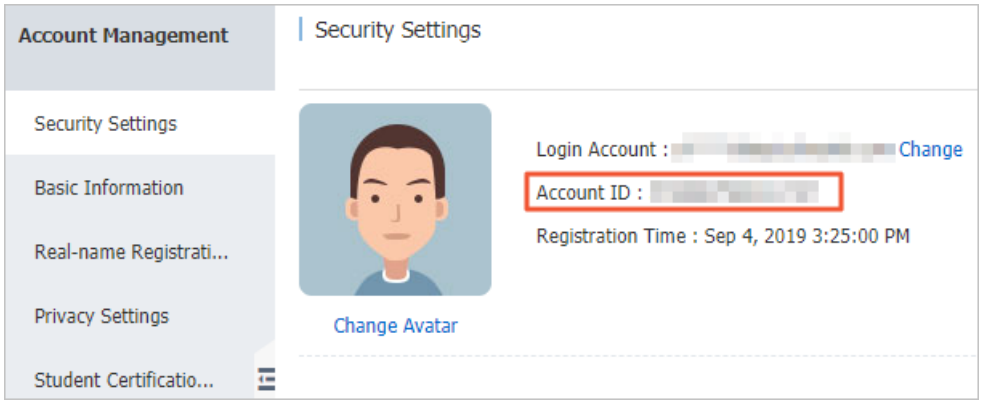


6. Click **OK**.
7. On the **Basic Information** page of the RAM role, click the **Trust Policy Management** tab.
8. Click **Edit Trust Policy**, and replace the policy text with the following sample statements.




```
{
"Statement": [
{
"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
"RAM": [
"acs:ram::<ID of the Alibaba Cloud account to which the destination instance belongs>:root"
],
"Service": [
"<ID of the Alibaba Cloud account to which the destination instance belongs>@dts.aliyuncs.com"
]
}
}
],
"Version": "1"
}
```

Note To obtain the ID of the Alibaba Cloud account to which the destination instance belongs, you must log on to the Account Management console by using this account. The account ID is displayed on the Security Settings page. Then, you must replace the `<ID of the Alibaba Cloud account to which the destination instance belongs>` in the preceding statements with the account ID.



Related topic

Migrate data from a user-created MySQL database connected over Express Connect, VPN Gateway, or Smart Access Gateway to an ApsaraDB RDS for MySQL instance across Alibaba Cloud accounts