WeData Data Development Platform

Preparations

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Preparations
User Account and Permission Management

Last updated: 2025-05-15 14:37:38

Overview

Data Development and Governance Platform WeData is based on Tencent Cloud CAM User and Permission Management System. It supports users to log in through the Tencent Cloud official website console using either a root account or a sub-account. Simultaneously, within the WeData product, there is an independent user role and permission control system based on RBAC. Tencent Cloud accounts need to be granted both CAM policies and WeData member roles.
WeData user management is divided into three layers: cloud account, WeData project-level member, and WeData platform-level member. User access permission control is performed through Tencent Cloud CAM policy, project-level role, and platform-level role respectively, as shown in the table below.

Account Type	Permission Management	Permission Control Scope	Policy/Role Name	Permission Description
Tencent Cloud Account	Tencent Cloud CAM Policy	WeData Console menu, including project management, execution resource group management, user management.	QcloudWeDataFullAccess	Have full read-write access to the WeData Console menu.
			QcloudWeDataReadOnly	Have read-only access permission to the WeData Console menu.
			Custom Policy	Perform API-level access control based on policy details.
Project members in WeData	WeData project-level role	WeData project-level menu, including Data Integration, data development.	Project Administrator	Have full read-write access to the belonging project, responsible for operations such as project public configuration and project member management.
			data engineer	Have data development and operation and maintenance related permissions in the belonging project.
			Ops engineers	Have data operation and maintenance related permissions in the belonging project.
			Ordinary member	Have read-only access permission to the belonging project.
			Custom role	Perform access control according to the custom permission list.
Platform-level members in WeData platform	WeData platform-level role	WeData Global Menu, including data asset, data modeling.	Asset Administrator	Have full read-write access to the data asset module and read-only access permission to other global menus.

Tencent Cloud Account

Before using the data development and governance platform WeData, you need to prepare a Tencent Cloud root account and manage sub-accounts through CAM.

- **Tencent Cloud root account:** It is the CAM root account and by default has access to all Tencent Cloud resources under the account. In CAM, the root account is by default the main entity for ownership, usage metering and billing of all cloud resources, and is responsible for creation, authorization, and management of sub-accounts within the organization.

- **Tencent Cloud sub-account:** Created, managed in a unified way, and paid for by the root account through the Tencent Cloud CAM console. In CAM, sub-accounts do not own resources by default and must be authorized by the root account to which they belong. Once authorized, sub-accounts can manage resources under the root account within the granted permissions.

To authorize access to WeData for a Tencent Cloud sub-account, you need to associate either the **QcloudWeDataFullAccess** or **QcloudWeDataReadOnlyAccess** policy in CAM.
For more details, see CAM-related documentation.

WeData Project-Level Member

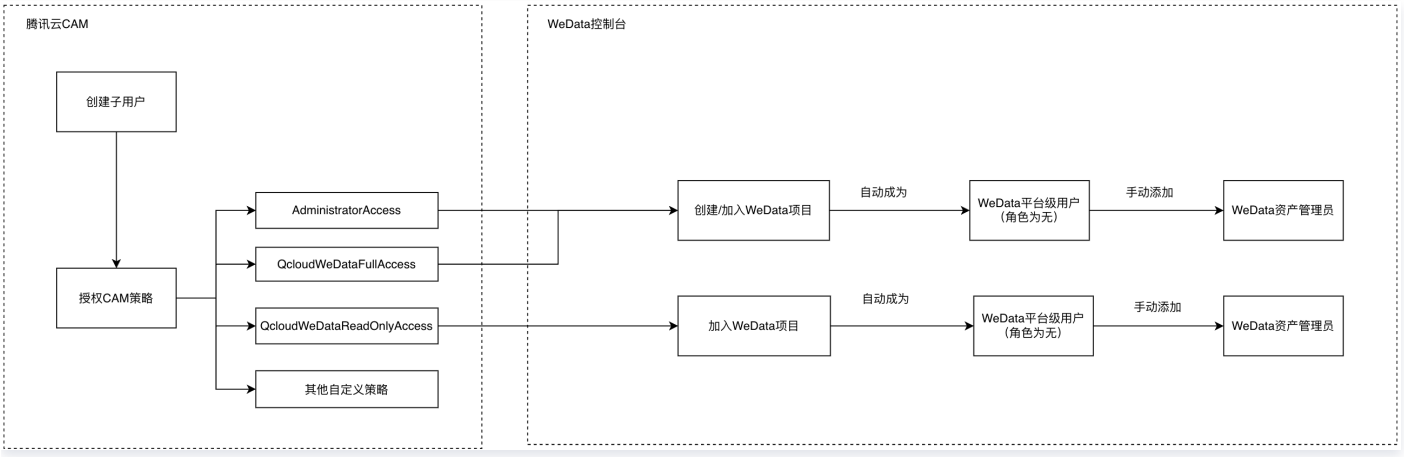
A Tencent Cloud account entering a WeData project needs to be added as a WeData project-level user and associated with a project-level role.

- Tencent Cloud root account, by default the project administrator of all projects in WeData, requires no manual user operation.
- Tencent Cloud sub-account, by default not a member within a WeData project, needs to create a project or be manually added to an existing project by the project administrator.

Platform-Level Members in WeData Platform

- Users will automatically become platform-level users of WeData when they create a project or join an existing one, with the default role being "None".
- To grant access permission to the platform-level menu, you can manually add roles such as "Asset Administrator".

User and Permission Management Operation Process



Signing up for a Tencent Cloud account

Create a Tencent Cloud Main Account

- **Registration:** If you haven't registered a Tencent Cloud root account yet, go to the homepage of the Tencent Cloud official website, click **free registration** in the top right corner of the page. For more details, see registration guide.
- **Real-name authentication:** A Tencent Cloud root account needs to complete real-name authentication before purchasing and using Tencent Cloud products. For more details, see authentication guide.

Create a Tencent Cloud Sub-Account

1. Use the root account or log in to Tencent Cloud CAM Console, and in the left sidebar, select **Users > User List**.
2. On the "User List" page, click **Create User** to create a sub-account, including Sub-users and Collaborators.

3. After successful creation, CAM will generate login information for the sub-account. You can click **View User Details**, then select **Security** and reset the password.

> **Note**
> Note: If you need multi-person collaborative development, please create a CAM sub-account for other collaborators.

Authorize Sub-Account WeData Product Access Permission

1. Log in to Tencent Cloud using the root account CAM Console , and in the left navigation, select **Users > User List** .
2. On the "User List" page, select a sub-account and click **Authorize** in the operation list. Search and select either the QcloudWeDataFullAccess policy or the QcloudWeDataReadOnly policy.

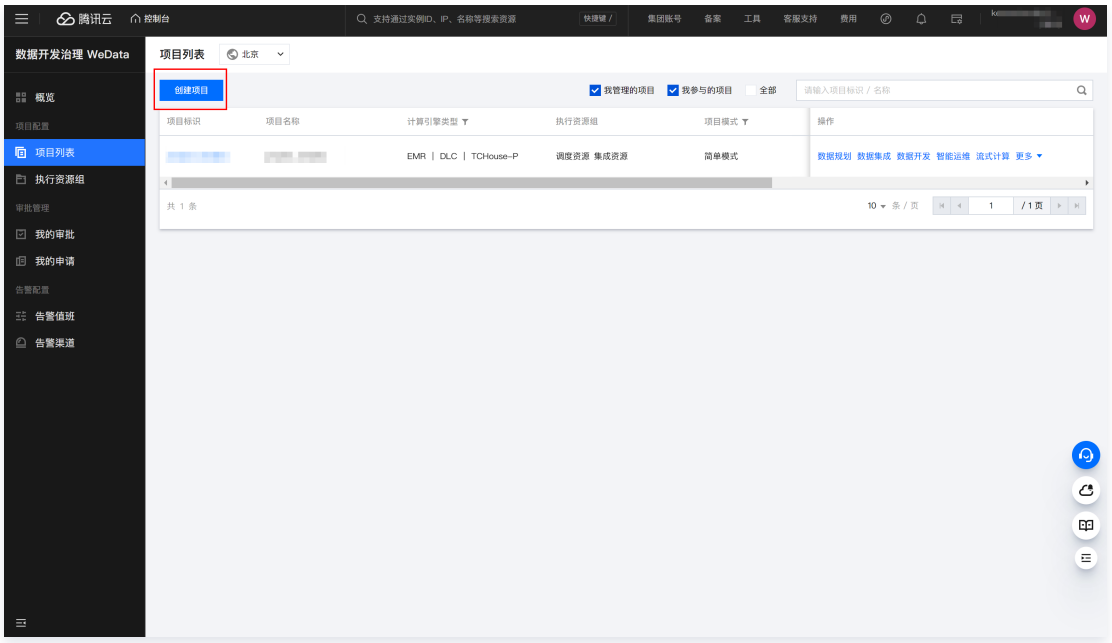
3. Click **Confirm** to authorize sub-account WeData access permissions.
4. Inform collaborators of the required information for sub-account log-in: login entry, root account ID, and username and password.

Become a WeData Project-Level Member

Creates a project.

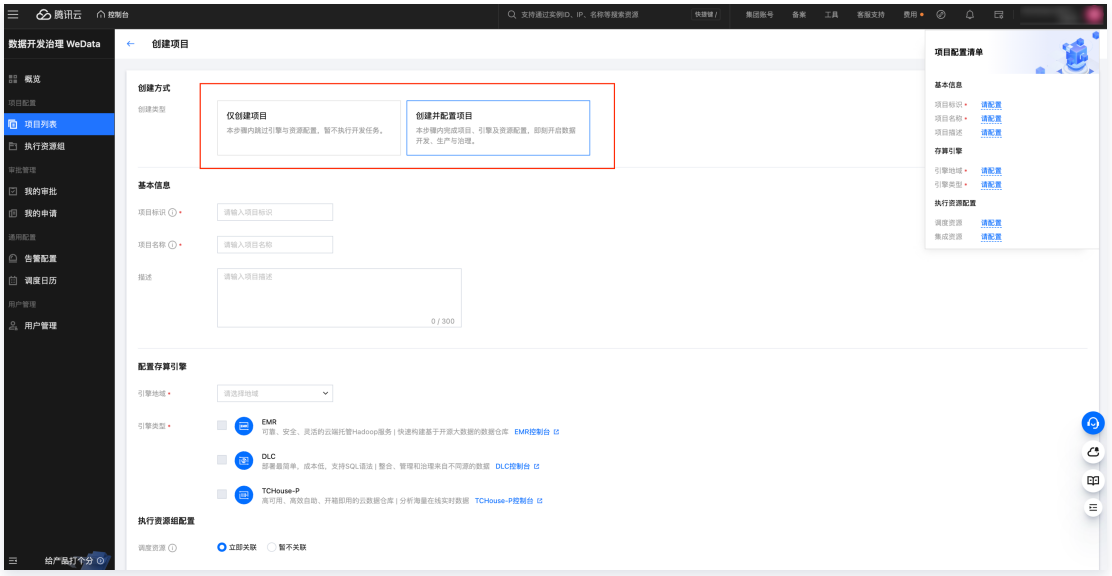
> **Note**
> Only the WeData Root Account Administrator has the permission to create a project. After successful creation, they will automatically become the project administrator of that project.

1. Log in to WeData Console with the WeData Root Account Administrator account, enter the project list page, and click **Create Project**.



2. Configure project parameters

2.1 Ways to create include "create and configure project" and "create project only".



2.2 Configure each parameter on the Creation Interface. The parameters are described as shown in the table below.

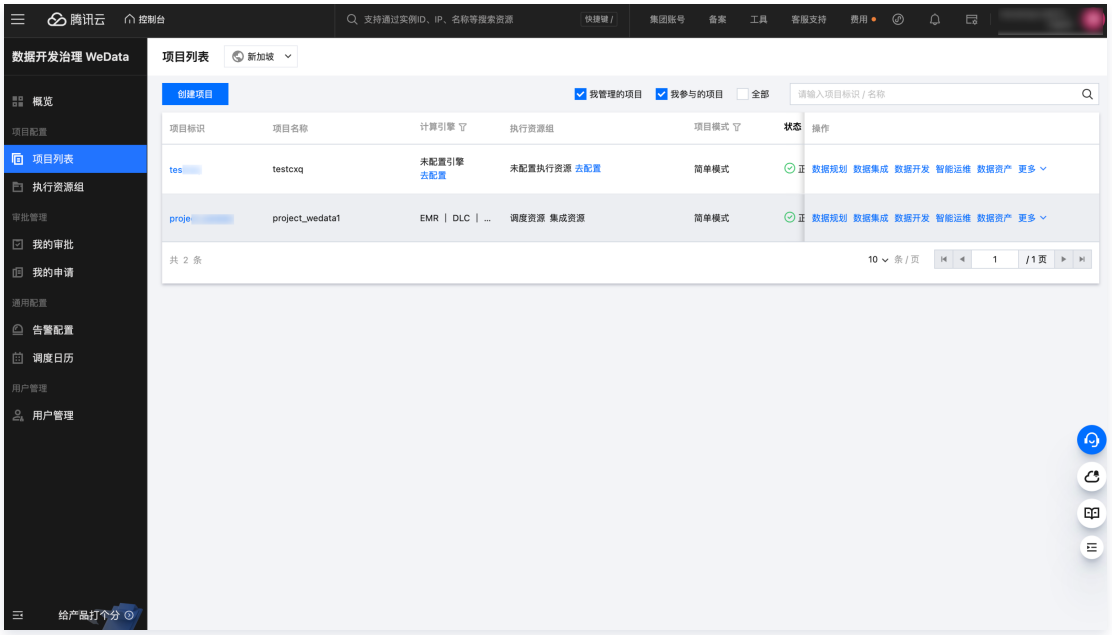
Category	Parameter	Description
Ways to create	Creation Type	You can select two ways to create a project: "create and configure project" or "create project only".
Basic Information	project ID	Project English ID, unique within the region. Must start with a letter, can contain letters, digits and underscores, and no more than 20 characters.
	project name	Project Chinese display name, unique within the region. Must start with a letter or Chinese character, and can contain letters, Chinese characters, digits and underscores.
	Description	Perform a simple description of the created space.
Select engine	Elastic MapReduce (EMR)	Once activated, you can use Elastic MapReduce in WeData to develop big data processing tasks. Go to EMR Console.

type	Tencent Cloud TCHouse-P		Once activated, you can use Tencent Cloud TCHouse-P in WeData. Go to TCHouse-P Console.
	Data Lake Compute (DLC)		Once activated, you can use Tencent Cloud Data Lake Compute (DLC) in WeData. Go to DLC Console.
Configure storage and computing engine	Engine region		Select the region where the Compute Engine Instance is located. Different types of Compute Engine Instances in WeData need to be in the same region.
	EMR	Cluster Type	Support selecting two kinds of cluster types: EMR on CVM and EMR on TKE.
		Cluster Name	Select an EMR cluster that is available in the selected region for the current root account. If there is no available cluster, you can purchase an instance.
		Component Information	After selecting an EMR cluster, the component information contained in the EMR cluster will be automatically obtained.
		Yarn Resource Queue	Select one or more Yarn Resource Queues in the EMR cluster.
	DLC	DLC Data Engine	Select an available DLC computational resource in the selected region for the current root account. Currently supports two types of engines: standard engine and SuperSQL engine.
		Database name	When no database is specified in DLC-related tasks, this database is used for data access by default.
		Test Connectivity	Test whether WeData service can connect to the engine resource.
	TCHouse-P	TCHouse-P Version	Selectable TCHouse-P1.0 or TCHouse-P2.0 version.
		Cluster Name	The names of the TCHouse-P clusters purchased in the selected region under this account.
		Username	Username for connecting to the TCHouse-P cluster.
		Password	Password for connecting to the TCHouse-P cluster.
		Test Connectivity	Test whether the username and password can connect to the cluster. After successful connection, you can create a project. (If the connectivity test fails, it may be because WeData is forbidden by the network firewall where the cluster is located. Please see adding TCHouse-P cluster allowlist.)
Execute resource allocation	scheduling resource	scheduling resource	Scheduling resources are primarily used for scheduled data development tasks (including sql tasks, shell tasks).
		Associating the Resource	Scheduling resources must be located in the same region as EMR. After association, the project exclusively uses the associated resources. This list only displays scheduling resources not associated with other projects. You can go to view resources or purchase resources.
	Integration Resource	Integration Resource	The main integration resource group runs data integration tasks.
		Associating the Resource	After association, the project exclusively uses the associated resources. This list only shows integrating resources not associated with other projects. You can go to view resources or associate resources.

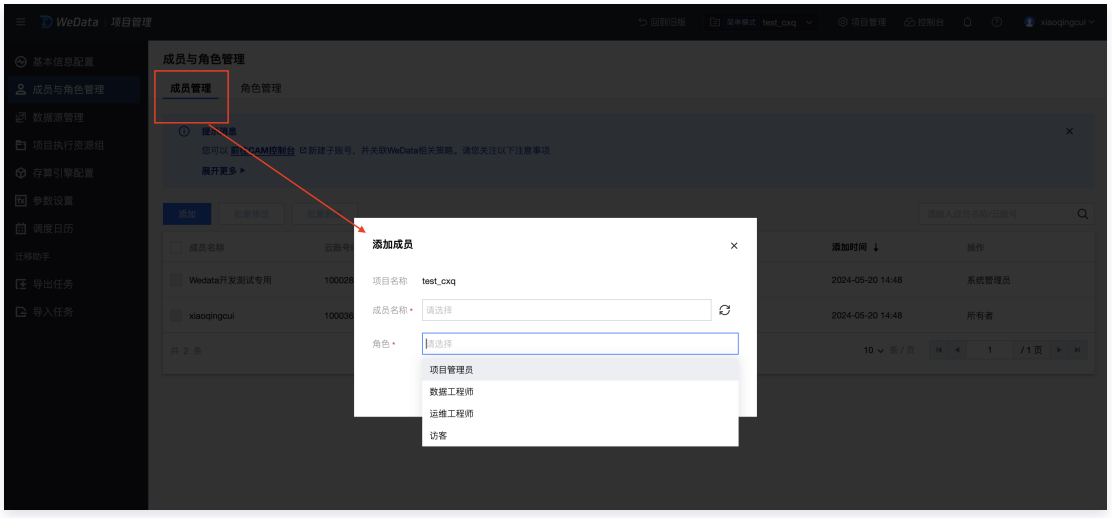
3. After successful creation, the sub-account will automatically become the project administrator of the project.

Add to an Existing Project

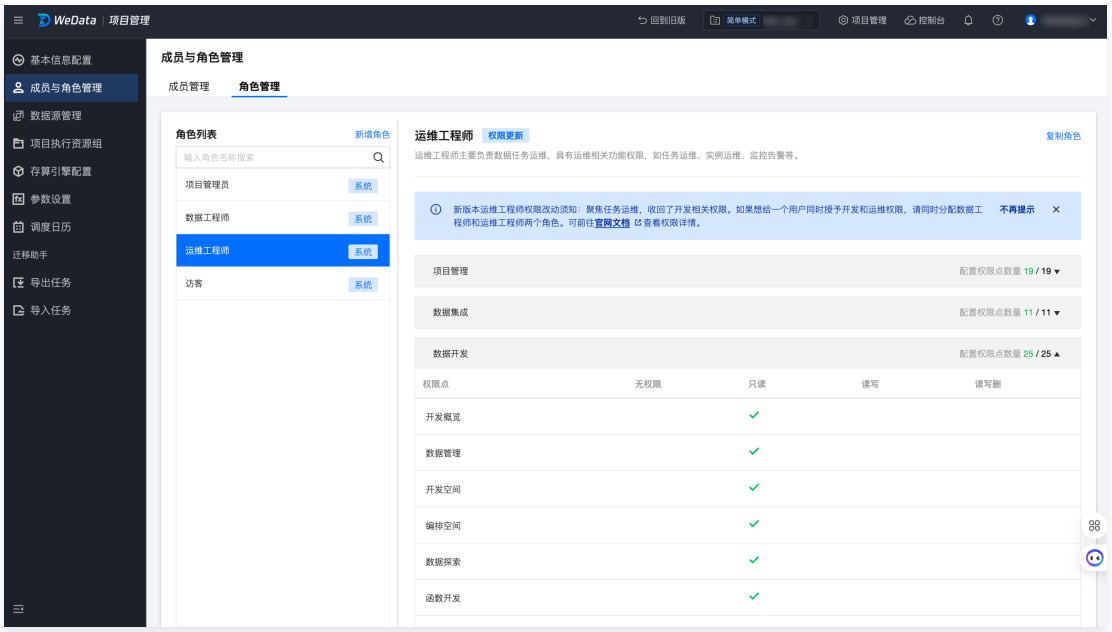
1. Log in to WeData Console with the project administrator account, enter the project list, select a project, and enter the **Project Management** module.



2. Select the **Member and Role Management** menu, add sub-accounts as project members, and assign project-level roles to them.



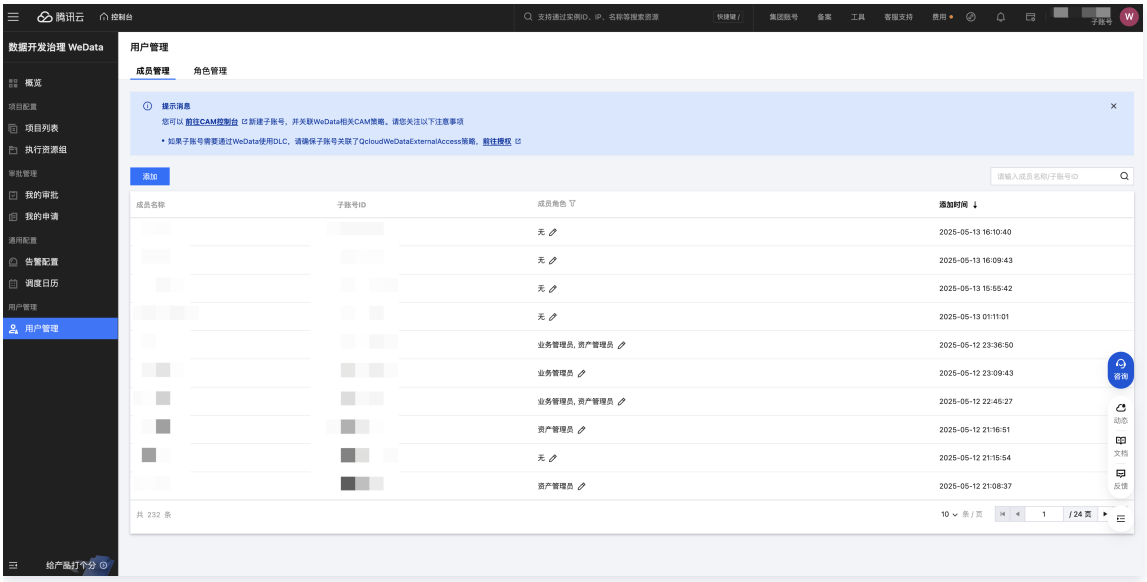
3. Click **Role Management** to view the permission list of WeData project-level roles.



Become a Platform-Level Member in WeData Platform

Automatic Addition

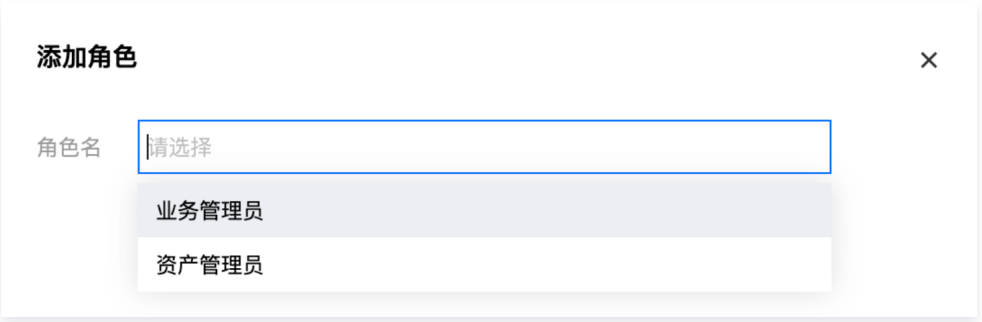
If a sub-account creates or joins a project, it will automatically become a platform-level user of WeData, with the member role defaulting to "None".



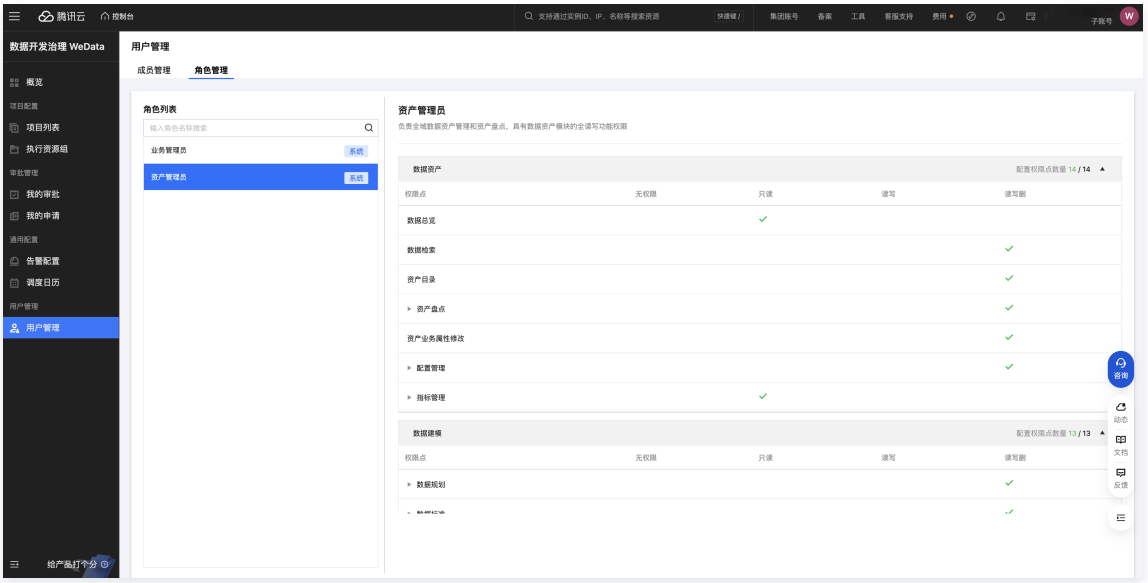
Manual Addition

1. Log in to the WeData Console using the root account or a sub-account with full read-write access to WeData. In the left sidebar, select **User Management > Member Management**.
2. Under the **Member Management** list, click **Add**.
3. Enter the Add User interface and add the sub-user of CAM as a user of WeData. The user role of the successfully added user defaults to "None".

4. If you want to grant this sub-user permissions to create projects, purchase execution resource groups, manage users, etc., click the **Edit** button, enter the **Add Role** interface, and modify their member role.



5. Click **Role Management** to view the permission list of WeData global-level roles.



Add to allowlist / security groups (optional)
Allowlist / Security Group Overview

Last updated: 2024-11-25 14:19:23

Currently, TCHouse-P Compute Engine and Tencent Cloud MySQL database have restrictions on allowlist / security groups. Therefore, before using the relevant services, you need to set access permissions for the WeData IPs listed in the table below. For other access-related settings, such as account creation and remote access, please refer to the official documentation of the database or the corresponding Tencent Cloud database documentation.

- Obtain and use TCHouse-P clusters. If you need to access TCHouse-P clusters through CVM instances in other subnets or external network machines, you need to add these IPs to the allowlist.
- Use Tencent Cloud MySQL database. If you are using a version of Tencent Cloud MySQL database higher than the basic edition, to ensure database security and stability, you need to add WeData access IPs to the target database's security group before beginning to use the database instances.

Add TCHouse-P cluster allowlist

Last updated: 2024-11-25 14:19:47

To use and access the TCHouse-P cluster in the project, you need to add the following Tencent Cloud WeData access IP addresses to the TCHouse-P cluster's allowed allowlist.

```
118.89.220.0/24, 139.199.116.0/24, 140.143.68.0/24, 152.136.131.0/24, 81.70.150.0/24, 81.70.161.0/24,
81.70.195.0/24, 81.70.198.0/24, 82.156.22.0/24, 82.156.221.0/24, 82.156.23.0/24, 82.156.24.0/24,
82.156.27.0/24, 82.156.82.0/24, 82.156.84.0/24, 82.157.119.0/24
```

Operation step

1. Log in to Tencent Cloud Data Warehouse TCHouse-P Console, select the target cluster in the **Cluster List** and click **Management**.

2. Select **Configuration**, and click **Create Allowlist**.

3. In the pop-up, configure the allowlist name, users, and database information.

Note

Tencent Cloud's WeData uses the TCHouse-P cluster's default database to perform connectivity tests. Please provide the default username and grant allowlist access to at least the default database, postgresql. If you also need to use other databases in the cluster, grant allowlist access to those databases as well. To check the default username and database information:

Example: If you need to bind a TCHouse-P cluster named "workspace" (default cluster username: wedata, default database name: postgres) in your project, and use the database "database1" in that cluster for data development, then you need to use the

username "wedata" to grant allowlist access to both the default database "postgres" and "database1".

Add Tencent Cloud MySQL Database Security Group

Last updated: 2024-11-25 14:20:45

Security group is a stateful virtual firewall with filtering features, used to set network access controls for one or multiple cloud databases. It is an important means for network security isolation provided by Tencent Cloud. If you are using a version of Tencent Cloud MySQL database higher than the basic version, you need to add the following access IP to the target database's security group. For specific operations, refer to Tencent Cloud MySQL DMC Cloud Database Security Group.

```
118.89.220.0/24, 139.199.116.0/24, 140.143.68.0/24, 152.136.131.0/24, 81.70.150.0/24, 81.70.161.0/24,
81.70.195.0/24, 81.70.198.0/24, 82.156.22.0/24, 82.156.221.0/24, 82.156.23.0/24, 82.156.24.0/24,
82.156.27.0/24, 82.156.82.0/24, 82.156.84.0/24, 82.157.119.0/24
```

Add DLC Resource Access Permissions

Last updated: 2024-11-25 14:21:08

WeData can connect to Data Lake Compute (DLC) through the configuration of access policies, enabling the operation of DLC product features and resource permissions. This grants WeData agile and efficient data lake analysis and computing services, supporting joint query analysis on multi-source heterogeneous data, breaking data silos, and maximizing data value.

Prerequisites

WeData users need to purchase and configure the DLC product. For details, please see DLC .

Go to the policy configuration page

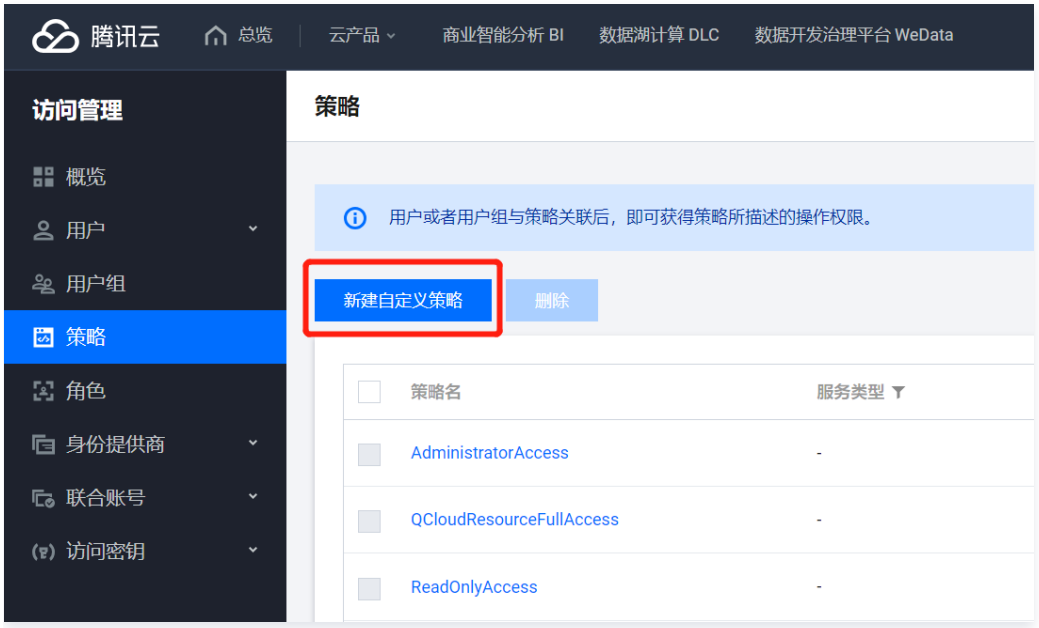
1. Log in to the WeData console.
2. Hover over the user profile photo in the upper-right corner and click CAM in the expanded menu.
3. In the left sidebar of the CAM page, click Policies to access the policy configuration page.

Add DLC Access Policy

After associating a user or user group with a policy, they can obtain the operation permissions described in the policy. In the following steps, users can configure all service and operation permissions for DLC according to the policy steps and assign them to user roles to gain the corresponding permissions.

Step 1: Create a New Policy

1. Click **Create Custom Policy** on the Policies page to start configuring product or service permissions for the current user.



2. In the Select Policy Creation Method, choose **Create by Policy Generator** . This method allows you to select products, services, and operations from the list and automatically generate policy syntax.

Step 2: Configure a Policy

1. When creating by policy generator, use the **Visual Policy Generator** on the policy configuration page to edit the policy.

2. The configuration items are as follows:

Configuration Item	Information
Effect	Select **Allow**
Service	Select **Data Lake Compute (dlc)** service
Action	Select **All Operations**
Resource	Select **All Resources**
Condition	Keep this item as default, no need to select

3. After completing the policy configuration steps, click **Next** to proceed to the **Associate Users/User Groups/Roles** step.

Step three: Associate the policy with the user/user group/role

1. After completing the policy configuration steps, next configure the basic information of the policy and associate it with specific user roles.

2. The configuration items are as follows:

Configuration Item		Information
Basic information	Policy name	By definition, the name of the policy created currently. Once created, the policy name cannot be modified.
	Description	By definition, the policy description information.
Associate Roles/Users/User Groups	Authorize this permission to users	Keep default, no need to select.
	Authorize this permission to the user group	Keep default, no need to select.
	Authorize this permission to the role	Choose to authorize to the **WeData_QCSRole** role.

3. After configuration is complete, click **Complete**, and WeData will obtain access to the DLC resources.