

**Data Admin Service**

# **Service Overview**

**Issue**            01  
**Date**             2023-03-02



**Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

<b>1 What Is Data Admin Service?</b> .....	<b>1</b>
<b>2 Basic Concepts</b> .....	<b>2</b>
<b>3 Advantages</b> .....	<b>3</b>
<b>4 Permissions Management</b> .....	<b>4</b>
<b>5 Use Constraints</b> .....	<b>8</b>
<b>A Change History</b> .....	<b>9</b>

# 1 What Is Data Admin Service?

---

Data Admin Service (DAS) is a one-stop platform that allows you to manage cloud databases on a web console. It offers database development, O&M, and intelligent diagnosis, making it easy to use and maintain your databases.

## NOTE

DAS is available only in regions CN-Hong Kong, CN East-Shanghai1, AP-Singapore, LA-Sao Paulo1, and EU-Dublin.

DAS is mainly designed for developers and database administrators (DBAs). It consists of the following modules, offering user-specific functions:

- **Development Tool**  
An easy-to-use database client for developers  
The DAS console makes your every operation visual. Additionally, diverse database development functions are available, including data and table structure synchronization, online editing, and intelligent prompts for SQL input.
- **Intelligent O&M**  
Provides the following database O&M functions for DBAs:
  - Host and instance performance data analysis
  - Slow and full SQL statement analysis
  - Real-time database performance diagnosis and analysis
  - Database historical running data analysis

# 2 Basic Concepts

---

## Metadata Collection

DAS periodically collects the metadata of DB instance databases, tables, and fields and stores the collected data in the DAS database.

---

# 3 Advantages

---

DAS allows you to manage mainstream types of DB instances, such as RDS for MySQL, RDS for PostgreSQL, Distributed Database Middleware (DDM), and Document Database Service (DDS). It provides a visual GUI, making it easy to manage your databases securely.

## Anytime, Anywhere

A DAS web console frees you from installing clients locally and supports access anytime, anywhere.

## Kernel Source Code Optimization

To resolve O&M pain points, the kernel is optimized and enhanced to support functions like Emergency Channel and SQL Explorer, allowing you to kill sessions that are not necessarily required in the case of an emergency and helping record and analyze all executed SQL statements.

## Secure Operations

Built-in security mechanisms guarantee your databases so you can worry less about security and stay focused on operations. For example, when you execute a slow SQL statement, DAS automatically triggers a timeout mechanism to protect databases against jitter.

## Robust Features

A wide range of features are available for you to choose from, such as SQL statement diagnosis, scheduled execution of SQL tasks, import and export of 1 GB of data, and cross-instance table structure synchronization. Multiple types of databases are all supported, including RDS for MySQL, RDS for PostgreSQL, DDM, and DDS.

## Professional Database O&M Platform

DAS offers a professional database O&M platform that supports SQL explorer, slow query logs, daily inspection, exception diagnosis, real-time analysis, performance trend, and emergency channel.

# 4 Permissions Management

---

If you need to assign different permissions to employees in your enterprise to access your DAS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, securing access to your cloud resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, if software developers in your enterprise need to use DAS but cannot delete DAS resources or perform any high-risk operations, you can create IAM users for the developers and grant them only the permissions required for using DAS resources.

If your account does not need individual IAM users for permissions management, you may skip over this section.

IAM can be used free of charge. You pay only for the resources in your account.

## DAS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups they belong to and can perform specified operations on cloud services.

DAS is a project-level service deployed in specific physical regions. To assign DAS permissions to a user group, specify projects in specific regions where the permissions will take effect. If you select **All projects**, the permissions will be granted for the user group in all projects. When accessing DAS, you need to switch to a region where you have been authorized to use this service.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you need to also assign other roles on which the permissions depend to take effect. However, roles are not ideal for fine-grained authorization and secure access control.

- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant IAM users only the permissions for managing a certain type of database resources.

**Table 4-1** lists all the system-defined roles and policies supported by DAS.

**Table 4-1** DAS system permissions

Policy Name	Description	Type	Dependency
DAS Administrator	DAS administrator, who has full permissions of DAS	System-defined role	This role depends on the <b>Tenant Guest</b> role. The <b>DAS Administrator</b> and <b>Tenant Guest</b> roles must be assigned in the same project.
DAS FullAccess	Full permissions for DAS	System-defined policy	None

 **NOTE**

- DAS depends on other services to implement the management and O&M of databases.
- If you authorize IAM users in fine-grained mode and want to use DAS to manage DB instances, add the DAS FullAccess system policy during authorization.
- On the DAS console, you can view and manage the DB instances configured in the corresponding services.

By default, users with fine-grained authorization have the permissions to view the database login list of Development Tool, delete database login information, and access Intelligent O&M on DAS. The instances visible to these users are the same as those configured in the corresponding services.

**Table 4-2** describes the common operations supported by each system-defined policy or role of DAS. Select the policy or role you need according to the following tables.

**Table 4-2** Common operations supported by each system-defined policy or role of DAS

Operation	DAS Administrator	DAS FullAccess
Logging in to a DB instance	Supported	Supported
Adding a login	Supported	Supported
Modifying a login	Supported	Supported



Operation	DAS Administrator	DAS FullAccess
Deleting a database login	Supported	Supported
Viewing the login list in Development Tool	Supported	Supported
Using Intelligent O&M functions	Supported	Supported

**Table 4-3** Common DAS operations and supported actions

Operation	Action	Remarks
Logging in to a DB instance	das:connections:login	Configure the permissions required to query other database instances based on the instance type. <ul style="list-style-type: none"><li>• rds:instance:list;</li><li>• dds:instance:list;</li><li>• gaussdb:instance:list;</li></ul>
Obtaining the login information list	das:connections:list	Configure the permissions required to query other database instances based on the instance type. <ul style="list-style-type: none"><li>• rds:instance:list;</li><li>• dds:instance:list;</li><li>• gaussdb:instance:list;</li></ul>
Adding a login	das:connections:create	Configure the permissions required to query other database instances based on the instance type. <ul style="list-style-type: none"><li>• rds:instance:list;</li><li>• dds:instance:list;</li><li>• gaussdb:instance:list;</li></ul>
Modifying a database login	das:connections:modify	Configure the permissions required to query other database instances based on the instance type. <ul style="list-style-type: none"><li>• rds:instance:list;</li><li>• dds:instance:list;</li><li>• gaussdb:instance:list;</li></ul>

**Table 4-4** Other permissions DAS depends on

Policy Name	Description	Type	Dependency
Tenant Administrator	<p>Operation permissions:</p> <ul style="list-style-type: none"> <li>All permissions on the account center, billing center, and resource center</li> <li>All permissions on cloud resources owned by the account</li> </ul> <p>OBS policies are configured in the Global project.</p>	System-defined role	None
OBS OperateAccess	<p>Operation permissions: Users with this permission can view buckets, obtain basic bucket information, obtain bucket metadata, view objects, upload objects, download objects, delete objects, and obtain object ACLs.</p> <p>Configure the OBS policies globally.</p>	System-defined policy	None

DAS import and export features require the usage of OBS buckets. You need to obtain required OBS permissions before using these features.

- Typically, it is recommended that you configure the Tenant Administrator policy that allows you to perform operations on OBS resources.
- If you do not want employees to have the permissions for creating and deleting buckets, you can configure the OBS OperateAccess policy for the employees so that they can use the DAS features but cannot create or delete OBS buckets.

# 5 Use Constraints

---

There are some constraints on the usage of DAS, which are designed to improve stability and security of your instances.

**Table 5-1** Use constraints

Item	Constraint
Database source	DB engines such as RDS and DDS are supported.
DB engine	DB engines such as RDS for MySQL and RDS for PostgreSQL are supported.
Region and network	In the same region, only VPC networks are supported.

---

# A Change History

---

Released On	Description
2023-03-02	This issue is the first official release.