Data Admin Service

Service Overview

Issue 01

Date 2023-12-01

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:
https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

Contents

1 What Is Data Admin Service?

Data Admin Service (DAS) is a web service that allows you to log in to and perform operations on Huawei Cloud databases.

- DAS provides a one-stop management platform for cloud database development, O&M, and intelligent diagnosis.
- DAS manages DB instances on a web console, where users can perform basic SQL operations, advanced database management, and intelligent O&M, making work easy, secure, and intelligent.

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

- Development Tool

  Designed for developers as an easy-to-use database client.

  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 originally allowed you to query metadata of databases, tables, and fields in each instance, but now it can also periodically collect metadata and store it in the DAS database.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For robust DR, deploy clusters in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

3 Advantages

DAS helps you manage mainstream versions of RDS for MySQL, RDS for SQL Server, RDS for PostgreSQL, TaurusDB, Distributed Database Middleware (DDM), Document Database Service (DDS), GeminiDB Cassandra, GaussDB(DWS), and GaussDB instances. It provides a GUI that makes it easy to manage your databases securely.

Anytime, Anywhere

The DAS web console means there is no need to install clients locally and you can access your databases anytime, from anywhere.

Kernel Source Code Optimization

To address 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 systems protect 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 from jitter.

Robust Features

With DAS, a wide range of features are available, such as SQL statement diagnosis, scheduled SQL execution, import and export of up to 1 GB of data, and cross-instance table structure synchronization. DAS supports multiple types of databases, including RDS for MySQL, RDS for SQL Server, RDS for PostgreSQL, TaurusDB, DDM, DDS, GeminiDB Cassandra, GaussDB(DWS), and GaussDB.

Professional Database O&M Platform

DAS is a professional database O&M platform with SQL explorer, slow query logs, support for daily inspections, exception diagnosis, and real-time analysis. It also allows you to view performance trends and kill sessions as needed.

4 Permissions Management

If you need to assign different permissions to different 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 for your cloud resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, if you need software developers in your enterprise to be able to use DAS but not able to 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 require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see **IAM Service Overview**.

DAS Permissions

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups and attach permissions policies or roles to these groups. Users then 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 to 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 system that defines permissions related to users responsibilities. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you may need to also assign other roles that the permissions depend on. Roles are not ideal for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization system that defines permissions required to perform operations on specific cloud resources under certain conditions. Policies are more flexible than roles, and they can ensure more secure access control. For example, you can grant IAM users only permissions for managing a certain type of database resource.

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 for DAS.	System-defined role	This role depends on the **Tenant Guest** role. The **DAS Administrator** and **Tenant Guest** 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 instances configured in the corresponding services.

By default, users with fine-grained authorization have 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 based on 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 database	Supported	Supported
Adding a login	Supported	Supported
Modifying a login	Supported	Supported

Operation	DAS Administrator	DAS FullAccess
Deleting a DB instance login	Supported	Supported
Viewing the login list in Development Tool	Supported	Supported
Using Intelligent O&M	Supported	Supported
Executing a SQL diagnosis	Supported	Supported
Exporting SQL Explorer data	Supported	Supported
Subscribing to Daily Reports	Supported	Supported
Exporting slow query logs	Supported	Supported
Querying Full SQL Statements	Supported	Supported
Querying the Slow Query Log List	Supported	Supported
Viewing the Intelligent O&M page	Supported	Supported
Querying the Top SQL List	Supported	Supported
Querying the Daily Report List	Supported	Supported
Querying SQL execution plan	Supported	Supported

Table 4-3 Common DAS operations and supported actions

Operation	Action	Remarks
Logging in to a database	das:connections:login	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;

Operation	Action	Remarks
Obtaining the login information list	das:connections:list	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;
Deleting login information	das:connections:delete	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;
Adding a login	das:connections:create	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;
Modifying a database login	das:connections:modify	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;
Changing the payment mode of an instance on Intelligent O&M	das:clouddba:changePaymentMode	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;
Killing sessions on Intelligent O&M if necessary	das:clouddba:deleteProcess	Configure the permissions required to query other database instances based on the instance type. ● rds:instance:list; ● dds:instance:list; ● gaussdb:instance:list;

Operation	Action	Remarks
Executing a SQL diagnosis	das:clouddba:sqlDiagnosis	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Exporting SQL Explorer data	das:clouddba:fullSqlExport	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Subscribing to Daily Reports	das:clouddba:dailyReportsSubscribe	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Exporting slow query logs	das:clouddba:slowSqlExport	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Querying Full SQL Statements	das:clouddba:fullSqlList	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Querying the Slow Query Log List	das:clouddba:slowSqlList	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Viewing the Intelligent O&M page	das:clouddba:menuList	**NOTE** This permission is granted by IAM. After this permission is configured, you can view the Intelligent O&M page of DAS.

Operation	Action	Remarks
Querying the Top SQL List	das:clouddba:topSqlList	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Querying the Daily Report List	das:clouddba:dailyReportsList	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;
Querying SQL execution plan	das:clouddba:getSqlExecutionPlan	Configure the permissions required to query other database instances based on the instance type. • rds:instance:list; • dds:instance:list; • gaussdb:instance:list;

Table 4-4 Other permissions DAS depends on

Policy Name	Description	Type	Dependency
Tenant Administrator	Operation permissions: • All permissions on the account center, billing center, and resource center • All permissions on cloud resources owned by the account OBS policies are configured in the Global project.	System-defined role	None
OBS OperateAccess	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. Configure the OBS policies globally.	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 Constraints

DAS Usage Constraints

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

Table 5-1 Constraints on Usage

Item	Constraint
Database source	DB engines such as RDS, DDS, and GaussDB are supported.
DB engine	Only MySQL, Microsoft SQL Server, PostgreSQL, GaussDB, and GaussDB(DWS) are supported.
Region and network	In the same region, only VPC networks are supported.

6 DAS and Other Services

With DAS, you can access cloud databases with a few clicks instead of through clients.

- You can securely access data anytime and anywhere.
- You can directly manage and modify the data directory structure on the web-based console.

Relational Database Service (RDS)

DAS supports the management of RDS instances.

- You have the username and password for logging in to the target database.
- RDS instances and DAS are in the same region.

Table 6-1 DAS functions available to RDS instances

Module	MySQL	RDS for SQL Server	PostgreSQL
Database Management	√	√	√
SQL Window	√	√	√
SQL History	√	√	√
Import	√	√	√
Export	√	√	√
Table Structure Comparison and Synchronization	√	×	×
Data Tracking and Rollback	√	×	×
Data Generator	√	×	×
Task Scheduling	√	×	×

Module	MySQL	RDS for SQL Server	PostgreSQL
Real-Time Performance	√	×	×
Real-Time Sessions	√	√	×
SQL Diagnosis	√	×	×
Diagnosis Report	√	×	×
InnoDB Lock Query	√	×	×
User Management	√	√	×

Elastic Cloud Service (ECS)

DAS supports the management of ECS databases. To manage this type of databases, the following requirements must be met:

- You have the username, password, and port for logging in to the target database.
- ECSs and DAS are in the same region.
- The engine version of the managed MySQL instances can be 5.5, 5.6, 5.7, or 8.0. The instances are not deployed in HA clusters.

Table 6-2 DAS functions available for different ECS databases

Module	MySQL	RDS for SQL Server	PostgreSQL
Database Management	√	√	√
SQL Window	√	√	√
SQL History	√	√	√
Import	√	√	√
Export	√	√	√
Task Scheduling	√	×	×
Real-Time Performance	√	×	×
Real-Time Sessions	√	√	×
SQL Diagnosis	√	×	×
Diagnosis Report	√	×	×
InnoDB Lock Query	√	-	×
User Management	√	√	×

Document Database Service (DDS)

DAS supports the management of DDS DB instances. To manage DDS DB instances, the following requirements must be met:

- You have the username and password for logging in to the target database.
- DDS DB instances and DAS are in the same region.

Table 6-3 DAS functions available to DDS instances

Module	Function	DDS
Command Operation	To query commands.	√
	To display command execution records.	√
Database Management	To manage databases.	√
Collections	To manage database collections.	√
Views	To manage database views.	√
User Management	To create and manage users.	√
Role Management	To create and manage roles.	√

TaurusDB

To manage TaurusDB instances using DAS, the following requirements must be met:

- You have the username and password for logging in to the target database.
- TaurusDB instances and DAS are in the same region.
- The DB engine is MySQL 8.0.

Table 6-4 TaurusDB

Module	TaurusDB
Database Management	√
SQL Window	√
SQL History	√
Import	√
Export	√

Module	TaurusDB
Task Scheduling	√
Real-Time Performance	√
Real-Time Sessions	√
SQL Diagnosis	√
Diagnosis Report	√
InnoDB Lock Query	√
User Management	√

Distributed Database Middleware (DDM)

DAS supports the management of DDM instances. To manage DDM instances, the following requirements must be met:

- You have the username and password for logging in to the target database.
- DDM instances and DAS are in the same region.

Table 6-5 DAS functions available to DDM instances

Module	DDM
Database Management	√ **NOTE** Only the structure of global and single tables can be edited. Database creation and modification are not supported.
SQL Window	√
SQL History	√
Real-Time Sessions	√

GeminiDB Cassandra API

DAS supports the management of GeminiDB Cassandra instances. To manage GeminiDB Cassandra instances, the following requirements must be met:

- You have the username and password for logging in to the target database.
- GeminiDB Cassandra instances and DAS are in the same region.

Table 6-6 DAS functions available to GeminiDB Cassandra instances

Module	GeminiDB Cassandra
Keyspace Management	√ **NOTE** Creation of tables and views is not supported.
SQL Window	√
SQL History	√
Role Management	√

