

数据管理服务

产品介绍

文档版本 01
发布日期 2025-10-17



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目 录

1 什么是数据管理服务.....	1
2 常用概念.....	2
3 产品优势.....	3
4 权限管理.....	5
5 约束和限制.....	9
6 与其他服务的关系.....	10
7 安全.....	14
7.1 责任共担.....	14

1 什么是数据管理服务

数据管理服务（Data Admin Service，简称DAS）是用来登录和操作华为云上数据库的Web服务：

- 提供数据库开发、运维、智能诊断的一站式云上数据库管理平台，方便用户使用和运维数据库。
- 提供数据库可视化操作的服务，包括基础SQL操作、高级数据库管理、智能化运维等功能，旨在帮助用户易用、安全、智能地进行数据库管理。

成长地图

您可以通过[数据管理服务DAS成长地图](#)快速了解数据管理服务的相关概念、入门使用、和最佳实践等信息。

如何使用数据管理服务

管理控制台：您可以使用[管理控制台](#)为您提供的Web界面完成数据管理服务的相关操作。

了解[常用概念](#)和[什么是数据管理服务](#)可以帮助您更好地使用数据管理服务。

数据管理服务的主要使用对象分为：开发人员、数据库管理员（DBA）。数据管理服务针对不同使用对象提供了不同功能，分为以下两个模块。

- 开发工具
主要面向开发人员，提供易用的数据库客户端。
使用数据管理服务时，无需安装本地客户端，提供所见即所得的可视化操作体验。提供数据和表结构的同步、在线编辑，SQL输入智能提示等丰富的数据库开发功能。
- DBA智能运维
主要面向DBA，提供以下数据库运维类的功能。
 - 分析主机和实例性能数据。
 - 分析慢SQL和全量SQL。
 - 分析和诊断实时数据库性能情况。
 - 分析数据库历史运行数据。

2 常用概念

元数据采集

DAS将对实例的库、表、字段等元数据信息由实时查库，升级为后台任务的定期采集，并保存到DAS的数据库中。

如何选择可用区

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

3 产品优势

数据管理服务支持RDS for MySQL、RDS for SQL Server、RDS for PostgreSQL、TaurusDB、DDM（分布式数据库中间件）、DDS（文档数据库服务）、GeminiDB Cassandra、云数据库GaussDB等类型主流版本实例管理。提供优质的可视化操作界面，大幅提高工作效率，让数据管理变得既安全又简单。

数据管理服务支持RDS for MySQL、RDS for SQL Server、RDS for PostgreSQL、DDM（分布式数据库中间件）、DDS（文档数据库服务）等类型主流版本实例管理。提供优质的可视化操作界面，大幅提高工作效率，让数据管理变得既安全又简单。

随时随地

使用Web界面呈现，无需安装本地客户端，随时随地可用。

内核源码优化

围绕运维痛点，对内核进行优化和加强，提供了诸如连接被打满时的数据库紧急运维能力、全量SQL语句的记录和分析能力等。

操作安全保障

内置安全保护措施，有效保障数据库的稳定运行，让用户操作起来更安心。例如：用户执行一个慢SQL时，DAS会自动设置超时机制，防止因慢SQL执行时间过久而导致的数据库性能抖动。

特性丰富

DAS提供更多高级特性，例如：SQL语句诊断、SQL任务定时执行、1G容量的数据导入、数据导出、跨实例的数据库表结构同步，支持MySQL、Microsoft SQL Server、PostgreSQL、TaurusDB、DDM、DDS、GeminiDB Cassandra、云数据库GaussDB等多种数据库类型。

DAS提供更多高级特性，例如：SQL语句诊断、SQL任务定时执行、1G容量的数据导入、数据导出、跨实例的数据库表结构同步，支持RDS for MySQL、RDS for SQL Server、RDS for PostgreSQL、DDM、DDS等多种数据库类型。

专业的数据库运维平台

提供了专业化的数据库运维平台，具备全量SQL、慢SQL、每日巡检、异常诊断、实时分析、性能趋势、紧急Kill会话等多角度的运维能力。

4 权限管理

如果您需要对华为云上购买的数据管理服务（Data Admin Service，简称DAS）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用DAS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有数据管理服务（Data Admin Service，简称DAS）的使用权限，但是不希望他们拥有删除DAS资源等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予仅能使用DAS资源，但是不允许删除DAS资源的权限，控制他们对DAS资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 4-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	- 系统角色 - 系统策略 - 自定义策略	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	- 系统策略 - 自定义身份策略	- 为主体授予身份策略 - 身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义策略，在策略中通过条件键“g:RequestedRegion”的配置即可达到策略对于授权区域的控制。将策略附加主体或为主体授予该策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。[角色与策略权限管理](#)和[身份策略权限管理](#)分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

角色与策略权限管理

DAS服务支持角色与策略授权。默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DAS部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问DAS时，需要先切换至授权区域。

如[表4-2](#)所示，包括了DAS的所有系统权限。角色与策略授权场景的系统策略和身份策略授权场景的并不互通。

表 4-2 DAS 系统权限

策略名称/系统角色	描述	类别	依赖关系
DAS Administrator	数据管理服务管理员，拥有该服务下的所有权限。	系统角色	依赖Tenant Guest角色。 在同项目中勾选依赖的角色。

策略名称/系统角色	描述	类别	依赖关系
DAS FullAccess	数据管理服务的所有权限。	系统策略	无。
DAS ReadOnlyAccess	数据管理服务只读权限。	系统策略	无。

表4-3列出了DAS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 4-3 常用操作与系统权限的关系

操作	DAS Administrator	DAS FullAccess	DAS ReadOnlyAccess
登录数据库	√	√	x
新增数据库登录	√	√	x
修改数据库登录	√	√	x
删除数据库登录	√	√	x
查看开发工具数据库登录列表	√	√	√
访问DBA智能运维功能	√	√	√
执行SQL诊断	√	√	x
导出全量SQL数据	√	√	√
订阅日报	√	√	x
导出慢SQL数据	√	√	√
查询全量SQL列表	√	√	√
查询慢SQL列表	√	√	√
查看云DBA页面	√	√	√
查询TopSQL列表	√	√	√
查询日报列表	√	√	√
查询SQL执行计划	√	√	x

身份策略权限管理

DAS服务支持身份策略授权。如表4-4所示，包括了DAS身份策略中的所有系统身份策略。身份策略授权场景的系统身份策略和角色与策略授权场景的并不互通。

表 4-4 DAS 系统身份策略

系统身份策略名称	描述	策略类别
DASFullAccessPolicy	数据管理服务的所有权限	系统身份策略
DASReadOnlyPolicy	数据管理服务的只读权限	系统身份策略

表4-5列出了DAS常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

表 4-5 常用操作与系统身份策略的关系

操作	DASFullAccessPolicy	DASReadOnlyPolicy
登录数据库	√	x
新增数据库登录	√	x
修改数据库登录	√	x
删除数据库登录	√	x
查看开发工具数据库登录列表	√	√
访问DBA智能运维功能	√	√
执行SQL诊断	√	x
导出全量SQL数据	√	√
订阅日报	√	x
导出慢SQL数据	√	√
查询全量SQL列表	√	√
查询慢SQL列表	√	√
查看云DBA页面	√	√
查询TopSQL列表	√	√
查询日报列表	√	√
查询SQL执行计划	√	x

5 约束和限制

数据管理服务使用限制

为了提高实例的稳定性和安全性，数据管理服务在使用上有一些固定限制，具体详见[表1 使用限制](#)。

表 5-1 使用限制

类型	约束和限制
数据库来源	目前支持云数据库RDS、文档数据库服务、云数据库GaussDB等。 目前支持RDS for MySQL、RDS for SQL Server、RDS for PostgreSQL、DDM（分布式数据库中间件）、DDS（文档数据库服务）等。
数据库引擎	目前支持MySQL、Microsoft SQL Server、PostgreSQL、云数据库GaussDB等。 目前支持RDS for MySQL、RDS for SQL Server、RDS for PostgreSQL、DDM（分布式数据库中间件）、DDS（文档数据库服务）等。
区域和网络	同一个区域，仅支持VPC网络。

6 与其他服务的关系

在云上创建数据库实例后，连接和访问云数据，经常面临需要安装客户端才可以访问数据库的困扰，数据管理服务带你一站式轻松进行访问数据。

- 通过数据管理服务，您可以随时随地、安全地访问数据。
- 通过数据管理服务，您能够直接对数据结构进行可视化目录结构管理、轻松完成数据结构变更。

与云数据库 RDS 的关系

数据管理服务支持云数据库RDS实例的管理。

- 通过数据管理服务连接目标数据库时，需要使用到目标数据库的用户名和密码。
- 关系型数据库与数据管理服务须在同一个区域下。

表 6-1 关系型数据库

模块	MySQL	RDS for SQL Server	PostgreSQL
库管理	√	√	√
SQL窗口	√	√	√
SQL执行记录	√	√	√
导入	√	√	√
导出	√	√	√
表结构对比与同步	√	×	×
数据追踪与回滚	√	×	×
自动生成测试数据	√	×	×
任务调度	√	×	×
实时性能	√	×	×
实时会话	√	√	×

模块	MySQL	RDS for SQL Server	PostgreSQL
SQL诊断	√	×	×
诊断报告	√	×	×
InnoDB锁等待	√	×	×
用户管理	√	√	×

与弹性云服务器（ECS）的关系

数据管理服务支持弹性云服务器（ECS）自建库实例的数据管理。

- 通过数据管理服务连接目标数据库时，需要使用到自建库实例的用户名、密码及端口信息。
- 弹性云服务器与数据管理服务须在同一个区域下。
- 暂仅支持MySQL5.5、5.6、5.7、8.0版本的实例，不支持HA集群。

表 6-2 ECS 自建库数据源

模块	MySQL	RDS for SQL Server	PostgreSQL
库管理	√	√	√
SQL窗口	√	√	√
SQL执行记录	√	√	√
导入	√	√	√
导出	√	√	√
任务调度	√	×	×
实时性能	√	×	×
实时会话	√	√	×
SQL诊断	√	×	×
诊断报告	√	×	×
InnoDB锁等待	√	-	×
用户管理	√	√	×

与文档数据库服务(DDS)的关系

数据管理服务支持文档数据库（DDS）实例的管理。

- 通过数据管理服务连接目标数据库时，需要使用到目标数据库的用户名和密码。
- 数据库实例与数据管理服务须在同一个区域下。

表 6-3 文档数据库服务

模块	功能	DDS
命令操作	命令查询。	√
	命令执行记录。	√
库管理	数据库的管理。	√
集合管理	数据库中对集合的管理。	√
视图管理	数据库中对视图的管理	√
用户管理	创建与管理用户信息。	√
角色管理	创建与管理角色信息。	√

与云数据库 TaurusDB 的关系

数据管理服务支持云数据库TaurusDB数据库实例的管理。

- 通过数据管理服务连接目标数据库时，需要使用到目标数据库的用户名和密码。
- 数据库实例与数据管理服务须在同一个区域下。
- 支持MySQL 8.0类型实例。

表 6-4 TaurusDB

模块	TaurusDB
库管理	√
SQL窗口	√
SQL执行记录	√
导入	√
导出	√
任务调度	√
实时性能	√
实时会话	√
SQL诊断	√
诊断报告	√
InnoDB锁等待	√

模块	TaurusDB
用户管理	√

与分布式数据库中间件（DDM）的关系

数据管理服务支持分布式数据库中间件（DDM）实例的管理。

- 通过数据管理服务连接目标数据库时，需要使用到目标数据库的用户名和密码。
- 分布式数据库中间件实例与数据管理服务须在同一个区域下。

表 6-5 分布式数据库中间件（DDM）实例

模块	分布式数据库中间件（DDM）
库管理	√ 说明 不支持新建库和修改库操作，仅支持全局表和单表的表结构编辑。
SQL查询	√
SQL执行记录	√
实时会话	√

与云数据库 GeminiDB Cassandra 数据库的关系

数据管理服务支持云数据库GeminiDB Cassandra实例的管理。

- 通过数据管理服务连接目标数据库时，需要使用到目标数据库的用户名和密码。
- GeminiDB Cassandra实例与数据管理服务须在同一个区域下。

表 6-6 GeminiDB Cassandra 实例

模块	GeminiDB Cassandra
keyspace管理	√ 说明 不支持新建表和视图操作。
SQL查询	√
SQL执行记录	√
角色管理	√

7 安全

7.1 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如[图7-1](#)所示。

- **华为云：**无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户：**无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 7-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图7-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。