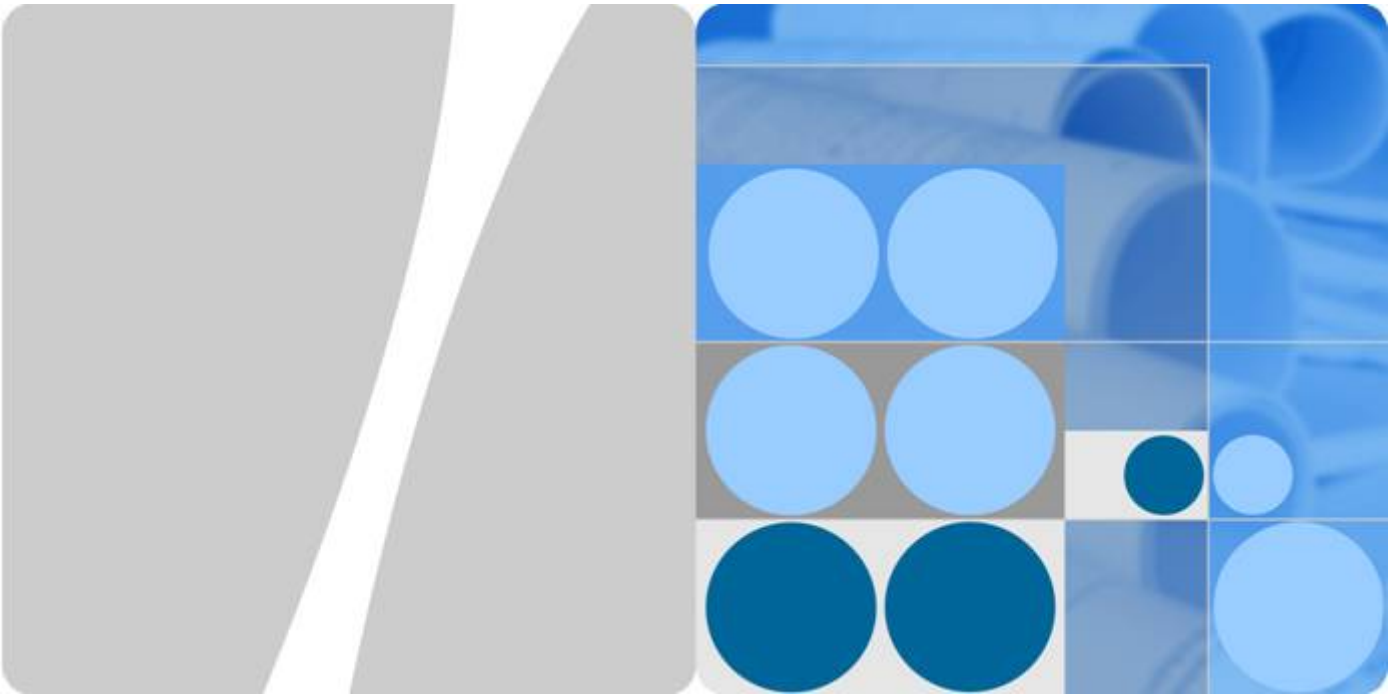

Document Database Service

# Security White Paper

Issue 01

Date 2020-11-20

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

## 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.

# Contents

# 1 Security White Paper

Document Database Service (DDS) is a secure and reliable document-oriented database service provided by HUAWEI CLOUD.

HUAWEI CLOUD DDS complies with security regulations and adheres to service boundaries without touching tenants' data, adopting target industry applications to local markets, or making entity investment, all while maintaining service neutrality when operating cloud platforms and offering cloud services. DDS allows tenants to quickly provision different types of databases and supports auto scaling of compute and storage resources based on service requirements. DDS provides functions such as automated backup, manual backup, and database restoration to prevent data loss. In addition, DDS parameter groups allow tenants to optimize their databases based on their service requirements.

DDS also provides multiple features to ensure the reliability and security of tenants' databases, such as VPC, security group, permission setting, SSL connection, automated backup, manual backup, point-in-time recovery (PITR), and cross-AZ deployment.

## Network Isolation

Tenants can manage IP addresses to access their databases in a VPC. DDS DB instances run in independent VPCs. Tenants can create a cross-AZ subnet group and deploy DDS high availability (HA) DB instance in this subnet group based on service requirements. After a DB instance is created, DDS will assign a subnet IP address to the DB instance. After DDS DB instances are deployed in a VPC, tenants in other VPCs can access the DB instances through a VPN. The tenants can also create an ECS in the VPC to connect the database through a private IP address. Subnet groups and security groups can be configured in combination to isolate DDS DB instances, enhancing instance security.

## Access Control

DDS creates a master database account when a tenant is creating a DDS DB instance. The tenant sets the password of the master database account. This account allows tenants to operate databases on their DB instance. The master account allows tenants to operate the DDS instance databases that they have created and connect to the DDS instance databases. Tenants can also create DB instances and database subaccounts based on service plans to grant database

  

objects to subaccounts to separate permissions. Tenants can select security groups when creating DDS DB instances and deploy instance service NICs in the target security groups. You can set inbound and outbound security group rules to control the access to and from DB instances within a VPC. Database security groups only allow database listening ports to be connected. Tenants do no need to restart DDS DB instances when configuring security groups.

## Transmission Encryption

DDS DB instances support using TLS to encrypt transmission between database clients and servers. When DDS provisions DB instances, the specified Certificate Chain (CA) will generate a unique service certificate for each instance. Database clients can download the CA root certificate from the management console and provide the certificate when connecting to the database to authenticate the database server and encrypt data during transmission.

## Storage Encryption

DDS supports data encryption before storage. KMS manages encryption keys.

## Automated Backup and Manual Backup

DDS provides two backup and restoration methods: automated backup and manual backup. The automated backup policy is enabled by default and the backup retention period is a maximum of 732 days. After automated backup is enabled, data can be restored to a specified point in time. DDS automatically backs up data and incrementally backups operations logs every five minutes. Therefore, tenants can restore data to the status of any time before the latest incremental backup. Manual backup is a full backup of the database. These backups are stored in Huawei OBS buckets. When a tenant deletes a DB instance, the backups of the DB instance are retained in the OBS buckets. Tenants can restore data to new instances from existing backups.

## Data Replication

DDS supports deployment of HA instances (clusters and replica sets). Tenants can deploy HA DB instances in a single AZ or multiple AZs. When tenants deploy HA DB instances, DDS establishes and maintains database synchronization. If the primary node fails, DDS will automatically promote the secondary node to the primary to achieve high availability.

## Data Deletion

When you delete a DDS DB instance, all data stored in it will be deleted and cannot be restored.

  