Distributed Cache Service

Security White Paper

Issue 01

Date 2023-01-05

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.

Contents

1 Security White Paper

Distributed Cache Service (DCS) is a secure and reliable in-memory database service provided by Huawei Cloud.

DCS complies with security regulations, adheres to service boundaries, and will never monetize customer data. It allows you to quickly provision different types of instances and supports auto scaling of compute and storage resources as required. To prevent data loss, DCS provides functions such as automated backups, snapshots, and restorations. It also allows you to modify configuration parameters for instance tuning.

DCS provides many features to ensure the reliability and security of account data, including VPCs, security groups, whitelists, SSL encryption for public access, automated backups, data snapshot, and cross-AZ deployment.

NOTE

For details about how DCS ensures data security, see **DCS Security Best Practices**.

Network Isolation

You can configure VPC inbound rules to allow specific IP address segments to connect to your instances. DCS instances run in an independent VPC. You can create a cross-AZ subnet group and deploy high-availability instances in it. After an instance is created, DCS will assign a subnet IP address to the instance for connection. After DCS instances are deployed in a VPC, you can use a VPN to access the instances from other VPCs. You can also create an ECS in the VPC housing the instances and connect the ECS and instances through a floating IP address. Subnets and security groups can be used together to isolate DCS instances and enhance security.

Access Control

When creating a DCS instance, you can configure security groups (supported by DCS for Redis 3.0, Redis 6.0 professional edition, and Memcached) or whitelists (supported by DCS for Redis 4.0, 5.0, and 6.0 basic edition).

You can set inbound and outbound security group rules or configure whitelists to control the access to and from DCS instances within a VPC.

You do not need to restart instances when configuring security groups or whitelists.

When creating a DCS instance, you are advised to enable password protection and set an access password for the instance to prevent unauthenticated clients from accessing the instance by mistake.

Transmission and Storage Encryption

RESP (REdis Serialization Protocol), the communication protocol of Reids, only supports plaintext transmission in versions earlier than Redis 6.0. DCS Redis 6.0 basic edition instances support the RESP3 protocol and encryption over SSL.

For public access to DCS instances (supported only by DCS Redis 3.0 instances), you can enable TLS encryption with Stunnel. For details, see the **instructions on installing and configuring Stunnel**. When DCS provisions instances, the specified Certificate Chain (CA) will generate a unique service certificate for each instance. When connecting to an instance, clients can use the CA root certificates downloaded from the management console to authenticate the instance server and encrypt data during transmission.

If you need to encrypt data in transit when public access is not enabled, use an encryption algorithm (such as AES 256) to encrypt data before storage and keep access in the trusted domain. The data is also encrypted before persistence to disk.

Automated and Manual Backups

DCS instances can be backed up automatically or manually. The automated backup function is disabled by default. Backup data of an instance is stored for a maximum of 7 days. After automated backup is enabled, you can restore data to the instance. During automated backup, all data of an instance is backed up, and the performance of the standby node will be affected. Manual backups are user-initiated full backups of instances. The backup data is stored in OBS buckets and removed upon deletion of the corresponding instance.

Data Replication

A master/standby or cluster DCS instances can be deployed within an AZ or across multiple AZs for HA. For cross-AZ deployment, DCS initiates and maintains data synchronization. High availability is achieved by having a standby node take over in the event that a failure occurs on the master node. When operations are read-heavy, you can use DCS Redis 4.0 or later instances that support read/write splitting, or cluster instances that have multiple replicas. DCS maintains data synchronization between the master and replicas. You can connect to different addresses of an instance to isolate read and write operations.

Data Deletion

If you delete a DCS instance, all data stored in the instance will be deleted. Nobody can view or restore the data once it is deleted.

