Data Replication Service

Security White Paper

Issue	01
Date	2022-09-30

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.

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Security White Paper

Data Replication Service (DRS) is a stable, efficient, and easy-to-use cloud service for database migration.

Upholding Huawei's commitment to security, DRS provides features such as fine-grained authentication, network isolation, high availability, and encrypted transmission to ensure security and high availability during the migration.

Fine-Grained Authorization

DRS uses **Identity and Access Management (IAM)** to implement fine-grained permission management. IAM provides identity authentication and access control, grants different permissions to different user groups, uses fine-grained authentication to control the usage scope of DRS resources, and ensures users have secure access to resources.

For details about DRS permissions, see **Permissions Management**.

Network Isolation

When creating a DRS instance, you can select a subnet in the VPC where the DRS instance is located based on service requirements. After the DRS instance is created, DRS will assign an IP address in the subnet to the DRS instance for connecting to source and destination instances. If the DRS instance is in the same VPC as the source instance or destination instance on Huawei Cloud, you can configure security groups for the source instance, destination instance, or DRS instance to control network access.

Host Security and Data Reliability and Durability

At the underlying layer, DRS uses **Elastic Cloud Servers (ECSs)** for computing and **Elastic Volume Service (EVS)** disks for storage. With secure ECSs and reliable EVS disks, the host security, data reliability, and data durability of DRS instances can be effectively ensured.

Instance High Availability

To improve service availability and resilience, DRS provides resumable data transfer and fault recovery. If data in the source database is not corrupted or lost, the DRS instance can resume data transfer from the point at which the transfer was stopped. If the underlying resources of an instance are faulty, data is migrated to a new instance in the AZ, and then the interrupted transfer continues. DRS also provides the cross-AZ HA. If the instance in the primary AZ becomes faulty, services can be switched over to the instance in the standby AZ to continue data replication.

Data Transmission Encryption

To secure data replication, DRS allows you to encrypt data transmission over a public network, VPN, Direct Connect, or VPC.

Permanent Data Deletion

When a DRS instance is deleted, the computing and storage resources of the instance are reclaimed. In addition, all data on the DRS instance is deleted and cannot be restored, including basic instance information, run logs, and data comparison results.