Database and Application Migration UGO

Security White Paper

Issue 01

Date 2023-04-10

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.. 1

1 Security White Paper

UGO is a professional cloud service that focuses on heterogeneous database structure migration.

UGO provides fine-grained authentication, high availability, and data encryption to ensure security and high availability of databases and application migration.

Fine-Grained Authorization

UGO 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 UGO resources, and ensures users have secure access to services.

Network Isolation

UGO connects to a source database through a public network and connects to a target database through a non-public network.

UGO and the target database are located in different VPCs, and their networks are isolated by default. UGO is authorized to establish a VPC endpoint to connect to the target database, so the connection process is point-to-point. Networks of different users connected to UGO are still isolated from each other.

High Availability

UGO uses the multi-node DR mechanism to ensure high availability.

Storage Encryption

UGO takes security measures, including but not limited to encryption, for sensitive information such as user database accounts and passwords to ensure data security.

Transmission Encryption

UGO provides SSL for connecting to the source and target databases to improve data transmission security.

Data Deletion

When UGO evaluation or migration tasks are deleted, all task data of users is also deleted and cannot be restored.