GaussDB(for MySQL)

Security White Paper

Issue 01

Date 2023-02-28

HUAWEI

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.

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

GaussDB(for MySQL) is a secure and reliable database service.

GaussDB(for MySQL) complies with security regulations, adheres to service boundaries, and will never monetize customer data. It allows you to quickly provision different types of databases and supports auto scaling of compute and storage resources as required. With GaussDB(for MySQL), you can create automated or manual backups and perform point-in-time restores (PITRs) to prevent data loss. It also provides parameter templates for database tuning.

GaussDB(for MySQL) provides comprehensive measures to ensure the reliability and security of your databases, including VPCs, security groups, permissions settings, SSL encryption, automated backups, manual backups, PITRs, and cross-AZ deployment.

Network Isolation

You can configure VPC inbound rules to allow specific IP address segments to connect to databases. GaussDB(for MySQL) instances run in an independent VPC. You can create a cross-AZ subnet group and deploy primary/standby instances in it. After an instance is created, GaussDB(for MySQL) will assign a subnet IP address to the instance for connection. After GaussDB(for MySQL) 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 GaussDB(for MySQL) instances and connect the ECS and instances through a private IP address. Subnets and security groups can be used together to isolate GaussDB(for MySQL) instances and enhance security.

Access Control

When you are creating a GaussDB(for MySQL) instance, an account is automatically created. After you specify a password for this account, you can use it to connect and operate your created instances. For security reasons, you are advised to create IAM users and grant permissions for them. You can create your instances in a security group and deploy your service NIC in the same security group. Then, configure inbound and outbound rules to control access to your instances. You do not need to reboot instances after you configure security group rules. The security group only allows access over the database listening port.

Transmission Encryption

The connections between database clients and servers can be encrypted with transport layer security (TLS). A specified certificate agency (CA) generates a unique service certificate for each GaussDB(for MySQL) instance upon provisioning. Database clients can download a root certificate from the management console and provide this certificate when connecting to the database to authenticate the database server and encrypt data during transmissions.

Automated and Manual Backups

GaussDB(for MySQL) supports automated and manual backups. The automated backup function is enabled by default. Automated backups can be retained for a maximum of 732 days. You can use them to restore data to a specific point in time. GaussDB(for MySQL) automatically backs up full data and incrementally backs up transaction logs every five minutes, so you can restore data to any point in time ahead of the last incremental backup. Manual backups are user-initiated full backups of DB instances. They are stored in OBS buckets. When you delete a DB instance, the manual backups will be retained unless you manually delete them. You can restore data to new instances from existing backups.

Data Replication

You can deploy primary/standby instances within an AZ or across AZs for high availability. If you create primary/standby instances, GaussDB(for MySQL) automatically sets up synchronous replication between your primary node and read replicas. If the primary node fails, a read replica takes over services quickly to ensure high availability.

