目录

云数据库MySQL安全性

身份验证和访问控制

金山云用户身份验证和访问管理的一般性说明请参见金山云IAM相关文档。 针对实例创建过程中创建的管理员用户，在MySQL环境下，其被授予的权限包括：

- SELECT
- INSERT
- UPDATE
- DELETE
- CREATE
- DROP
- RELOAD
- PROCESS
- REFERENCES
- INDEX
- ALTER
- SHOW DATABASES
- CREATE TEMPORARY TABLES
- LOCK TABLES
- EXECUTE
- REPLICATION SLAVE
- REPLICATION CLIENT
- CREATE VIEW
- SHOW VIEW
- CREATE ROUTINE
- ALTER ROUTINE
- CREATE USER
- EVENT
- TRIGGER

安全组

目前金山云的网络环境包括基础网络环境和VPC环境。不管是基础网络环境还是VPC环境，都需要通过安全组的配置实现对访问的控制。只有满足安全组中的访问规则，才被允许访问数据库实例。 安全组是一个或多个规则，这些规则共同定义了对户对某个服务的访问权限。

一般来讲，安全组应该包括安全组名称及若干规则，规则一般包括协议类型（IP、TCP、UDP、ICMP、SSH等）、地址信息（主机地址或地址段）、端口信息（某一个具体的端口号或一段连续的端口范围）、流量方向（出站、入站）、行为规则（允许或禁止）；

云数据库MySQL安全组约束的是用户对MySQL实例的访问，即允许/禁止哪些用户访问MySQL。
由于以下原因：
1，MySQL服务的协议、端口已经默认确定（TCP 3306）；
2，MySQL服务的流量无需特意指定出站或入站；
3，MySQL服务默认拒绝访问（行为规则禁止）；

云数据库MySQL安全组的规则只需要包括IP信息（主机地址或地址段）即可。也就是对于云数据库MySQL的安全组来说，安全组规则可以理解为白名单，只要添加在白名单中的IP/段就可以访问云数据库MySQL服务，而没有在白名单中的IP/段则不可以访问云数据库MySQL服务。