ALIBABA

RDS 安全技术白皮书

网络、存储、账号

ApsaraDB 团队

2016/5/26

目录

RDS 介绍

云数据库 RDS（Relational Database Service）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于飞天分布式系统和全 SSD 盘高性能存储，支持 MySQL、SQL Server、PostgreSQL 和 PPAS（高度兼容 Oracle)引擎，默认部署主备架构且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案，彻底解决数据库运维的烦恼！

云数据库 RDS 提供了多样化的安全加固功能来保障用户数据的安全，其中包括但不限于：

1、 网络：IP 白名单、VPC 网络、SSL（安全套接层协议）、SQL 防火墙

2、 存储：TDE（透明数据加密）、自动备份

3、 容灾：同城容灾（多可用区实例）、异地容灾（两地多中心）

访问控制

数据库账号

当用户创建实例后，RDS 并不会为用户创建任何初始的数据库账号。

有以下两种方式来创建数据库帐号：

1、 用户可以通过控制台或者 Open API 来创建普通数据库账号，并设置**数据库级别**的读写权限。

2、 如果用户需要更细粒度的权限控制，比如表、视图，字段级别的权限，也可以通过控制台或者 Open API 先创建**超级数据库账号**，并使用数据库客户端和超级数据库账号来创建普通数据库账号。超级数据库账号可以为普通数据库账号设置表级别的读写权限。

注意： 通过超级数据库账号创建的普通数据库账号无法通过控制台或者 Open API 管理。

IP 白名单

虽然 RDS 不支持 ECS 的安全组功能，但是 RDS 提供了“IP 白名单”来实现网络安全访问控制。

默认情况下，RDS 实例被设置为不允许任何 IP 访问，即 127.0.0.1。用户可以通过控制台的数据安全性模块或者 Open API 来添加 IP 白名单规则。IP 白名单的更新**无需重启** RDS 实例，因此不会影响用户的使用。

IP 白名单可以设置多个分组，每个分组可配置 **1000 个 IP 或 IP 段**。

网络隔离

VPC

除了 IP 白名单外，RDS 还支持用户使用 VPC 来获取更高程度的网络访问控制。

VPC 是用户在公共云里设定的私有网络环境，通过底层网络协议严格地将用户的网络包隔离，在网络 2 层完成访问控制；用户可以通过 **VPN** 或者**专线**，将自建 IDC 的服务器资源接入阿里云，并使用 VPC 自定义的 RDS IP 段来解决 IP 资源冲突的问题，实现自有服务器和阿里云 ECS 同时访问 RDS 的目的。

使用 VPC 和 IP 白名单将极大程度提升 RDS 实例的安全性。

Internet

部署在 VPC 中的 RDS 实例默认只能被同一个 VPC 中的 ECS 实例访问。如果有需要也可以通过申请**公网 IP** 的方式接受来自公网的访问（不推荐），包括但不限于：

1、来自 ECS EIP 的访问

2、来自用户自建 IDC 公网出口的访问

IP 白名单对 RDS 实例的所有连接方式生效，建议在申请公网 IP 前先设置相应**白名单规则**。

数据加密

SSL

RDS 提供 MySQL 和 SQL Server 的安全套接层协议。用户可以使用 RDS 提供的服务器端根证书来验证目标地址和端口的数据库服务是否为 RDS 提供，从而有效避免**中间人攻击**。除此之外，RDS 还提供了**服务器端 SSL 证书**的启用和更新能力，以便用户按需更替 SSL 证书以保障安全有效性。

需要注意的是，虽然 RDS 提供了应用到数据库之间的连接加密功能，但是 SSL 需要应用开启服务器端验证才能正常运转。另外 SSL 也会带来额外的 **CPU 开销**，RDS 实例的吞吐量和响应时间都会受到一定程度的影响，具体影响视用户的连接次数和数据传输频度而定。

TDE

RDS 提供 MySQL 和 SQL Server 的透明数据加密功能。RDS for MySQL 的 TDE 由阿里云自研，RDS for SQL Server 的 TDE 基于 SQL Server 企业版的功能改造而来。

在开启了透明数据加密功能的 RDS 实例上，用户可以指定参与加密的**数据库**或者**表**。这些数据库或者表中的数据在写入到**任何设备**（磁盘、SSD、PCIE 卡）或者**服务**（OSS、OAS）前都会进行加密，因此实例对应的数据文件、备份都是以密文形式存在。

TDE 加密采用国际流行的 **AES 算法**，秘钥长度为 **128 比特**。秘钥由 **KMS 服务**加密保存，RDS 只在启动实例和迁移实例的动态读取一次秘钥。用户可自行通过 KMS 控制台对秘钥进行更替。

备份恢复

备份功能

为了保证数据完整可靠，数据库需要常规的自动备份来保证数据的可恢复性。

RDS 提供两种备份功能，分别为数据备份和日志备份。

数据备份为强制项，用户一定要在一周七天内选定两天或两天以上的某一个时间段执行全量的常规物理备份。另外用户也可以根据运维需要，通过控制台或者 Open API 随时发起全量的临时物理备份。

日志备份为可选项，用户可以选择开启或者关闭。如果日志备份关闭，那么数据恢复时只能恢复到数据备份集所在时间点；

数据备份和日志备份使用相同的**过期删除策略**。用户可将备份过期的天数设置为 7 到 730 中的任何一个数字，也可以通过调整过期策略实时删掉较老的备份。

恢复功能

数据可恢复性是一个数据库可靠运维的关键指标。

RDS 提供三种恢复功能，分别为覆盖性恢复、按备份集恢复和按时间点恢复。

按备份集恢复：用户可以将指定备份集的数据恢复到一个过期时间为 2 天的临时实例上。用户可以在临时实例上检查自己的数据是否完好。

按时间点恢复：用户可以选择最临近时间点，系统根据全量备份以及之后的日志备份，将数据重放到一个过期时间为 2 天的临时实例上。

覆盖性恢复：用户可以将指定备份集的数据恢复到当前 RDS 实例上，而并非临时实例； 注意这种恢复方式一旦执行，原实例不提供 2 次恢复能力，**谨慎使用**。

数据恢复功能和备份策略紧密相关，其中：

1、数据恢复的最早时间取决于最早一个数据备份（与数据备份的频率和过期策略相关）

2、数据恢复的最晚时间取决于最后一个日志备份（与日志生成量有很大关系）

3、数据恢复是否支持按时间点恢复取决于日志备份是否开启

4、数据恢复的速度取决于数据备份的频率（也与日志生成量有很大关系）

实例容灾

多可用区实例

阿里云为全世界多个地域提供云计算服务，每个地域（Region）都包含多个可用区(Avzone)。同一个地域下的可用区都被设计为相互之间网络延迟很小(3ms 以内)以及**故障隔离**的单元。RDS **单可用区主实例**运行在同一个可用区下的两台物理服务器上,可用区内机柜、空调、电路、网络都有冗余。通过异步 / 半同步的数据复制方式和高效的 HA 切换机制，RDS 为用户提供了高于物理服务器极限的数据库可用性。

为了提供比单可用区实例更高的可用性，RDS 支持**多可用区实例**（也叫做**同城双机房**或者**同城容灾实例**）。多可用区实例将物理服务器部署在不同的可用区，当一个可用区（A）出现故障时流量可以在短时间内切换到另一个可用区（B）。 整个切换过程对用户透明，应用代码无需变更。

注意：发生容灾切换时应用到数据库的连接会断开，需要应用**重新连接** RDS。

跨域容灾实例

RDS 多可用区实例的容灾能力局限在同地域的不同可用区之间。为了提供更高的可用性，RDS 还支持跨地域的数据容灾。 用户可以将地域 A 的 RDS 实例 A’ 通过**数据传输**（Data Transmission）**异步复制**到地域 B 的 RDS 实例 B’ （实例 B’ 是一个完整独立的 RDS 实例，拥有**独立**的连接地址、账号和权限）。

配置了跨域容灾实例后，当实例 A’ 所在地域发生短期不可恢复的重大故障时，用户在另外一个地域的实例 B’ 随时可以进行**容灾切换**。切换完成后，用户通过修改应用程序中的数据库连接配置，可以将应用请求转到实例 B’ 上，进而获得高于地域极限的数据库可用性。

注意：容灾切换前用户需要先停止实例 A’ 到实例 B ’ 的数据复制，以免造成数据错乱。

软件升级

RDS 为用户提供数据库软件的**最新版本**。

在绝大多数情况下版本升级都是**非强制性**的。只有用户主动重启了 RDS 实例的时候，RDS 才会将被重启实例的数据库版本升级到最新的兼容版本。

在极少数情况下（如致命的重大 Bug、安全漏洞），RDS 会在实例的**可运维时间**内发起数据库版本的强制升级。需要注意的是，强制升级的影响仅仅是几次数据库连接闪断，在应用程序正确配置了数据库连接池的情况下不会对应用程序造成明显的影响。

用户可以通过控制台或者 Open API 来修改可运维时间，以避免 RDS 在业务高峰期发生了强制升级。

服务授权

权限管理

在没有经过用户授权的情况下，阿里云的售后团队和 DBA 团队只能查看 RDS 实例资源、资费和性能相关的信息。举例来说，RDS 实例的购买时间和到期时间，CPU、内存、存储空间的容量和消费情况，备份空间、公网流量、SQL 审计的消费情况等。

只有经过用户授权了“**配置权限**”后，阿里云的售后团队和 DBA 团队才可以在用户自定义的时间段内查看和修改 RDS 实例的配置信息。举例来说，RDS 实例的白名单、数据复制模式、备份策略和数据库参数。在任何情况下，阿里云的售后团队和 DBA 团队不会主动变更 RDS 实例的连接信息（含连接地址和数据库账号）。

只有经过用户授权了“**数据权限**”后，阿里云的 DBA 团队才可以在用户自定义的时间段内查看 RDS 实例内的用户数据。举例来说，RDS 实例的库表结构、索引字段、数据样本和 SQL 历史。在任何情况下，阿里云的售后团队和 DBA 团队不会主动更改 RDS 实例的库表结构、索引字段、数据。

过期时间

用户可以为阿里云的售后团队和 DBA 团队授予排查问题需要的权限，并设置相应的**有效期**来自动回收权限。权限默认的有效期为 24 小时，用户可以**提前回收**相关的权限。