ALIBABA CLOUD

Alibaba Cloud

云数据库RDS
安全白皮书

文档版本：20220607

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.产品概述 05
2.攻击防护 06
3.访问控制 07
4.网络隔离 08
5.数据加密 09
6.备份恢复 10
7.实例容灾 11
8.软件升级 12
9.服务授权 13

1.产品概述

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MariaDB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：

- 网络：白名单、VPC 网络、SSL加密等。
- 存储：设置透明数据加密TDE、自动备份数据等。
- 容灾：同城容灾（多可用区实例）、异地容灾（两地多中心）。

2.攻击防护

RDS提供多种攻击防护手段，包括防DDoS攻击、流量清洗、SQL注入检测等。

防DDoS攻击

当用户使用外网连接和访问RDS实例时，可能会遭受DDoS攻击。RDS提供流量清洗和黑洞处理功能，完全由系统自动触发和结束。当RDS安全体系认为用户实例正在遭受DDoS攻击时，会首先启动流量清洗功能，如果流量清洗无法抵御攻击或者攻击达到黑洞阈值，则会进行黑洞处理。

> **说明** 建议用户通过内网访问RDS实例，可以使RDS实例免受DDoS攻击的风险。

流量清洗

只针对外网流入流量进行清洗，处于流量清洗状态的RDS实例可正常访问。

单个RDS实例满足以下任一条件即触发流量清洗：

- PPS（Package Per Second）达到3万。
- BPS（Bits Per Second）达到180Mbps。
- 每秒新建并发连接达到1万。
- 激活并发连接数达到1万。
- 非激活并发连接数达到10万。

黑洞处理

只针对外网流入流量进行黑洞处理，处于黑洞状态的RDS实例不可被外网访问，此时应用程序通常也处于不可用状态。黑洞处理是保证RDS整体服务可用性的一种手段。

黑洞触发条件如下：

- BPS（Bits Per Second）达到2Gbps。
- 流量清洗无效。

黑洞结束条件如下：

黑洞在2.5小时后自动解除。

3.访问控制

RDS通过多维度进行访问控制，保证数据安全。

RDS提供如下两种方式创建数据库帐号：

- 通过RDS控制台或者API来创建普通数据库账号，并设置数据库级别的只读、读写、DDL、DML权限。
- 如果您需要更细粒度的权限控制，例如表、视图、字段级别的权限，也可以通过控制台或者API先创建高权限数据库账号，然后登录数据库创建普通数据库账号。高权限数据库账号可以为普通数据库账号设置更细粒度的权限。

白名单

RDS提供了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（即白名单为127.0.0.1）访问，包括内网访问和外网访问。您可以通过RDS控制台的**数据安全性**页面或者API来添加白名单。白名单的更新无需重启RDS实例，因此不会影响您的业务。

4.网络隔离

RDS提供多种网络隔离机制，保证网络安全。

VPC

除了IP白名单外，RDS还支持使用专有网络VPC来获取更高程度的网络访问控制。

VPC是私有网络环境，通过底层网络协议严格地将您的网络包隔离，在网络2层完成访问控制。您可以通过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。

关于VPC的详情请参见什么是专有网络。

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：

- 来自ECS EIP的访问。
- 来自自建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。

申请公网IP请参见申请或释放外网地址。

5.数据加密

本文介绍RDS提供的数据加密功能。

SSL

RDS提供MySQL、SQL Server和PostgreSQL的安全套接层协议（Secure Sockets Layer，简称SSL）。您可以使用RDS提供的服务器端的根证书来验证目标地址和端口的数据库服务是不是RDS提供的，从而可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证书以保障安全性和有效性。

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，具体影响与您的连接次数和数据传输频度有关。

具体操作请参见设置SSL。

TDE

RDS提供MySQL和SQL Server的透明数据加密（Transparent Data Encryption，简称TDE）功能。MySQL版的TDE由阿里云自研，SQL Server版的TDE是基于SQL Server企业版的功能改造而来。

当RDS实例开启TDE功能后，您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（例如磁盘、SSD、PCIe卡）或者服务（例如对象存储OSS）前都会进行加密，因此实例对应的数据文件和备份都是以密文形式存在的。

TDE加密采用国际流行的AES算法。密钥由KMS服务加密保存，RDS只在启动实例和迁移实例时动态读取一次密钥。您可以自行通过KMS控制台对密钥进行更换。

具体操作请参见设置透明数据加密。

云盘加密

针对RDS云盘版实例，阿里云免费提供云盘加密功能，基于块存储对整个数据盘进行加密，即使数据备份泄露也无法解密，最大限度保护您的数据安全。而且加密不会影响您的业务，应用程序也无需修改。

具体操作请参见云盘加密。

6.备份恢复

备份功能

为保证数据的完整性和可靠性，数据库需要常规的自动备份来保障数据的可恢复性。

RDS提供如下两种备份功能：

- 数据备份：强制项，您必须设置每周进行不少于2次的物理备份。另外，您也可以根据运维需要，通过控制台或者API随时发起临时备份。数据备份可以保留7~730天。
- 日志备份：可选项，您可以选择开启或者关闭。如果关闭日志备份，那么恢复数据时只能恢复到数据备份集所在的时间点。数据备份和日志备份使用相同的过期删除策略。

恢复功能

数据可恢复性是判断数据库运维可靠性的关键指标。

RDS提供如下两种恢复功能：

- 按备份集恢复：您可以将指定备份集的数据恢复到一个临时实例或克隆实例上。您可以在临时实例或克隆实例上检查自己的数据是否完好。
- 按时间点恢复：您可以选择临近时间点，系统根据全量备份以及之后的日志备份，将数据重新放到一个临时实例或克隆实例上。

相关链接

根据RDS实例类型的不同，支持的备份恢复方式不尽相同。如需了解各RDS实例支持的备份恢复方式，请参见如下链接中的备份恢复部分：

- MySQL备份方案概览
- SQL Server功能概览
- PostgreSQL功能概览
- MariaDB TX功能概览

7.实例容灾

RDS提供多种容灾解决方案。

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（Zone）。同一个地域中的可用区都被设计为相互之间网络延迟很小以及故障隔离的单元。

RDS单可用区实例运行在同一个可用区中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。通过异步或半同步的数据复制方式和高效的主备切换机制，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更高的可用性，RDS支持多可用区。多可用区将物理服务器部署在不同的可用区，当一个可用区出现故障时流量可以在短时间内切换到另一个可用区。整个切换过程对用户透明，应用代码无需变更。

> **说明** 发生主备切换时应用到实例的连接会断开，需要应用重新连接实例。

迁移可用区请参见迁移可用区。

灾备实例

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。例如用户可以将杭州地域的RDS实例A通过数据传输（Data Transmission）异步复制到上海地域的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。

创建灾备实例后，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。

> **说明** 容灾切换前用户需要先停止实例A到实例B的数据复制，以免造成数据错误。

创建灾备实例请参见创建异地灾备实例。

8.软件升级

RDS会为您提供数据库软件的新版本。

在绝大多数情况下，小版本升级都是非强制性的。但在您主动重启RDS实例时，该实例的数据库版本会在重启时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实例（除基础版外）会在可运维时间内发起数据库版本的强制升级。需要注意的是，强制升级仅会引起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。

您可以通过控制台或者API来设置可维护时间段，以避免RDS在业务高峰期发生了强制升级。

9.服务授权

当您寻求阿里云的技术支持时，如果技术支持过程中需要对您的数据库实例进行操作，您需要授权，技术支持人员才可以通过服务账号提供技术支持服务。在授权有效期结束后，临时服务账号会被自动删除。

在没有经过您授权服务账号的情况下，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。例如，RDS实例的购买时间、到期时间、CPU、内存、存储空间的容量和消费情况以及备份空间、公网流量、SQL审计的消费情况等。

若您需要阿里云的售后团队和DBA团队查看您实例的其它问题，您可以对他们进行如下授权：

- 配置权限

  当您授权了该权限后，阿里云的售后团队和DBA团队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。例如，RDS实例的白名单、数据复制模式、备份策略和数据库参数。但在所有情况下，阿里云的售后团队和DBA团队都不会擅自更改RDS实例的连接信息（含连接地址和数据库账号）。

- 数据权限

  当您授权了该权限后，阿里云的售后团队和DBA团队可以在用户自定义的时间段内查看RDS实例内的用户数据。例如，RDS实例的库表结构、索引字段、数据样本和SQL历史。但在所有情况下，阿里云的售后团队和DBA团队都不会擅自更改RDS实例的库表结构、索引字段、数据。

过期时间

您可以设置相应的有效期来自动回收权限，您也可以提前回收权限。