**操作场景**

IP白名单指允许访问RDS实例的IP清单。设置IP白名单可以让RDS实例得到高级别的访问安全保护，建议您定期维护白名单。

通常需要设置IP白名单的场景如下：

* 场景1

创建RDS实例后，您需要将外部IP地址添加至IP白名单中，外部设备才可以正常访问该RDS实例。

* 场景2

当数据库连接异常时，您可以检查白名单设置是否正确。

不同连接场景下，IP白名单的设置请参见下表。

安全组是一种虚拟防火墙，用于控制安全组中的ECS实例的出入流量。在RDS白名单中添加安全组后，该安全组中的ECS实例就可以访问RDS实例。

# 数据加密

更新时间：2020-08-04 11:06:25

[**本页目录**](javascript:void(0))

* [SSL](https://help.aliyun.com/document_detail/53620.html?spm=a2c4g.11186623.6.1680.6a692e2amSJYmY#title-zyv-cms-qw2)
* [TDE](https://help.aliyun.com/document_detail/53620.html?spm=a2c4g.11186623.6.1680.6a692e2amSJYmY#title-snc-wal-6bw)
* [云盘加密](https://help.aliyun.com/document_detail/53620.html?spm=a2c4g.11186623.6.1680.6a692e2amSJYmY#title-txw-bz8-3ur)

本文介绍RDS提供的数据加密功能。

## SSL

RDS提供MySQL和SQL Server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](https://help.aliyun.com/document_detail/32474.html#t7949.html)。

## 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，密钥长度为128比特。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](https://help.aliyun.com/document_detail/33510.html#t7950.html)。

## 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](https://help.aliyun.com/document_detail/135361.html#concept-2054727)。