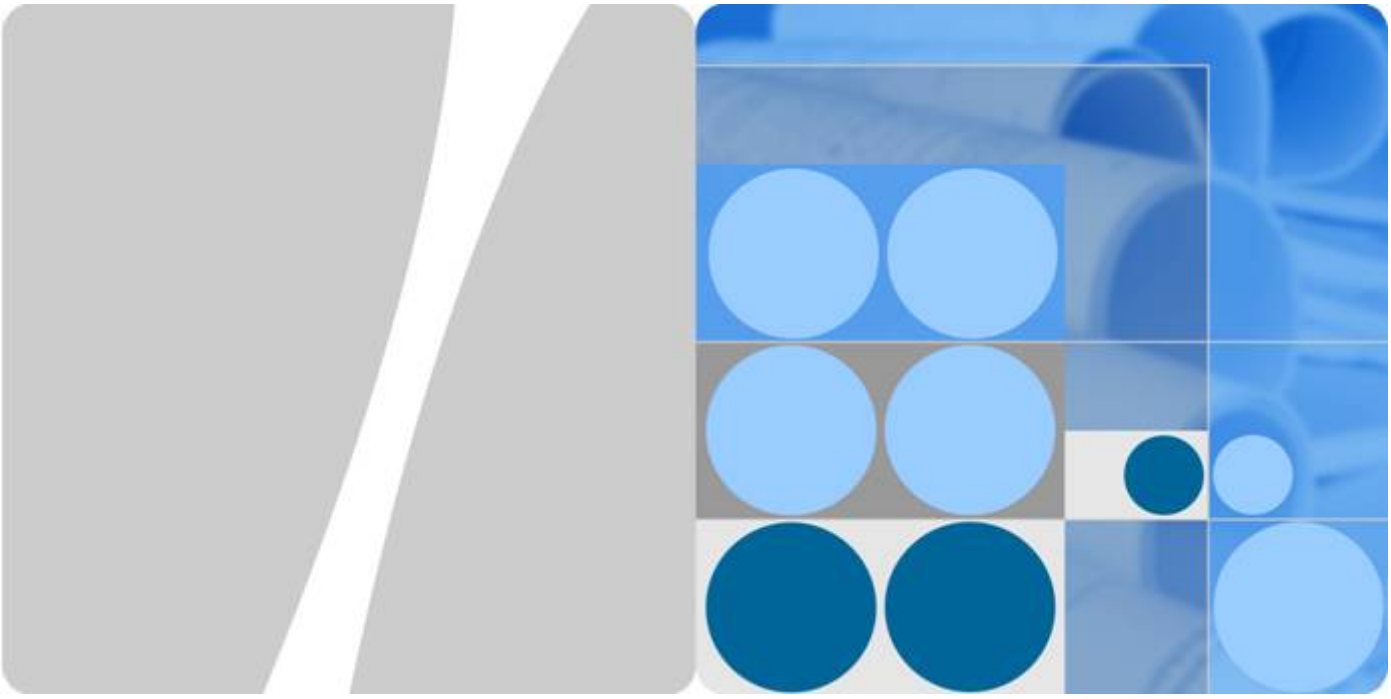

# 文档数据库服务

# 安全白皮书

文档版本　01

发布日期　2019-11-13

华为技术有限公司

## 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

# 目 录

# 1 安全白皮书

文档数据库服务（Documemt Database Service，简称DDS）是华为云提供的一款安全、可信的文档数据库服务。

DDS秉承华为云对租户的安全承诺，尊重租户数据主权，坚持中立、客观的立场，恪守业务边界，不碰租户数据，不会利用租户数据谋取商业价值。DDS允许租户快速发放不同类型数据库，并可根据业务需要，对计算资源和存储资源进行弹性扩容。DDS提供自动备份、即时备份、数据库恢复等功能，以防止数据丢失。参数组功能，则允许租户根据业务需要进行数据库调优。

DDS还提供多个特性来保障租户数据库的可靠性和安全性，例如VPC、安全组、权限设置、SSL连接、自动备份、即时备份、时间点恢复（PITR- point-in-time recovery）和跨可用区部署等。

## 网络隔离

VPC允许租户通过配置VPC入站IP范围，来控制连接数据库的IP地址段。DDS实例运行在租户独立的VPC内。租户可以创建一个跨可用区的子网组，之后可以根据业务需要，将部署DDS的高可用实例选择此子网完成，DDS在创建完实例后会为租户分配此子网的IP地址，用于连接数据库。DDS实例部署在租户VPC后，租户可通过VPN使其它VPC能够访问实例所在VPC，也可以在VPC内部创建ECS，通过私有IP连接数据库。租户可以综合运用子网和安全组的配置，来完成DDS实例的隔离，提升DDS实例的安全性。

## 访问控制

租户创建DDS实例时，DDS会为租户同步创建一个数据库主帐户，主帐户的密码由租户指定。此主帐户允许租户操作自己创建的DDS实例数据库。租户可以使用数据库主帐户连接DDS实例数据库，并根据需要创建数据库实例和数据库子帐户，并根据自身业务规划，将数据库对象赋予数据库子帐户，以达到权限分离的目的。租户创建数据库实例时，可以选择安全组，将DDS实例业务网卡部署在对应安全组中。租户可以通过VPC，对DDS实例所在的安全组入站、出站规则进行限制，从而控制可以连接数据库的网络范围。数据库安全组仅允许数据库监听端口接受连接。配置安全组不需要重启DDS实例。

## 传输加密

DDS实例支持数据库客户端与服务端TLS加密传输。 DDS在发放实例时，指定的CA会为每个实例生成唯一的服务证书。客户端可以使用从服务控制台上下载的CA根证书，并在连接数据库时提供该证书，对数据库服务端进行认证并达到加密传输的目的。

  

## 存储加密

DDS支持对存储到数据库中的数据加密后存储，加密密钥由KMS管理。

## 自动备份和手动备份

DDS提供两种备份恢复方法，即自动备份和手动备份。自动备份默认开启，备份存储期限最多732天，同时开启自动备份后，允许对数据库执行时间点恢复。对于集群形态的数据库实例，DDS自动备份会进行全量数据备份，且每5分钟会增量备份oplog日志，这就允许租户将数据恢复到最后一次增量备份前任何一秒的状态。手动备份是租户手动触发的数据库全量备份，这些备份数据存储在华为OBS桶中，当租户删除实例时，OBS桶中的手动备份会被保留。租户可以通过已有备份将数据恢复到新实例。

## 数据复制

DDS支持部署高可用实例（集群、副本集）。租户可选择在单可用区或多可用区中部署高可用实例。当租户选择高可用实例时，DDS会主动建立和维护数据库同步复制，在主节点故障的情况下，DDS会自动将备节点升为主节点，从而达到高可用的目的。

## 数据删除

租户删除DDS实例时，存储在数据库实例中的数据都会被删除，任何人都无法查看及恢复数据。