分布式缓存服务

安全白皮书

文档版本	01
发布日期	2024-05-29

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

HUAWEI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云计算技术有限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，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 安全白皮书.....1

1 安全白皮书

分布式缓存服务（Distributed Cache Service，简称DCS）是华为云提供的一款安全、可信的内存数据库服务。

DCS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。DCS允许租户快速发放不同类型的缓存实例，并可根据业务需要，对缓存资源进行弹性扩容。DCS提供自动备份、数据快照、数据恢复等功能，以防止数据丢失。提供参数修改功能，则允许租户根据业务需要进行实例调优。

DCS还提供多个特性来保障租户数据的可靠性和安全性，例如VPC、安全组、白名单、公网访问SSL加密连接、自动备份、数据快照和跨可用区部署等。

说明

如果您需要了解DCS安全方面的详细操作指导，请参考**DCS安全最佳实践**。

网络隔离

VPC允许租户通过配置VPC入站IP范围，来控制连接缓存实例的IP地址段。DCS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DCS的高可用实例选择此子网完成，DCS在创建完实例后会为租户分配此子网的IP地址，用于缓存实例。DCS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连接缓存实例。租户可以综合运用子网、安全组、白名单等配置，来完成DCS实例的隔离，提升DCS实例的安全性。

访问控制

租户创建DCS实例时，可以选择配置安全组（仅Redis 3.0/Redis 6.0企业版/Memcached实例支持）或者白名单（仅Redis 4.0、Redis 5.0和Redis 6.0基础版支持）。

租户可以通过VPC，对DCS实例所在的安全组或白名单入站、出站规则进行限制，从而控制可以连接实例的网络范围。

配置安全组/白名单不需要重启实例。

租户创建DCS实例时，建议将访问方式设置为密码访问，并为实例设置访问密码，防止未经认证的客户端误操作实例，以达到对客户端进行认证访问的目的，提高实例使用的安全性。

传输和存储加密

Redis的传输协议RESP在Redis 6.0之前的版本仅支持明文传输。Redis 6.0基础版实例支持RESP3传输协议，支持SSL传输加密。

当前DCS实例在开启公网访问时（仅Redis 3.0实例支持），支持基于Stunnel的客户端与服务端TLS加密传输（参考文档：**Stunnel安装和配置**）。在开启公网访问时，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，并在连接实例时提供该证书，对实例服务端进行认证并达到加密传输的目的。

由于需要兼容开源RESP协议，在未开启公网访问时，如果客户有传输加密诉求，建议在数据存储前使用加密算法进行加密后传输（例如AES 256等），并且控制在信任域内进行访问，加密后的数据在落盘保存时同样也会加密保存。

自动备份和手工备份

DCS提供自动备份和手工备份两种备份操作。自动备份默认未开启，需要租户选择是否开启，备份存储期限最多7天，同时开启自动备份后，允许对实例执行备份文件的恢复。DCS自动备份会进行全量数据备份，在备份期间会影响备节点的性能。手工备份是租户手动触发的实例全量备份，这些备份数据存储在华为OBS桶中，当租户删除实例时，会同步删除OBS桶中的快照。

数据复制

DCS的主备和集群实例支持部署高可用实例。租户可选择在单可用区或多可用区中部署实例。当租户选择跨AZ实例时，DCS实例会主动建立和维护Redis同步复制。在实例主节点故障的情况下，缓存实例会自动将备实例升为主节点，从而达到高可用的目的。如果租户使用缓存实例时，业务中读取数据比例大，可以选择4.0以上版本的读写分离实例或者集群多副本实例，缓存实例会自动维护主节点和多个备节点之间的数据同步复制，租户可以根据业务需要连接不同的地址进行读写分离。

数据删除

租户删除DCS实例时，存储在缓存实例中的数据都会被删除，任何人都无法查看及恢复数据。