云数据库 GeminiDB

产品介绍

文档版本 01

发布日期 2024-12-30

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 什么是云数据库 GeminiDB

云数据库 GeminiDB是一款基于计算存储分离架构的分布式多模NoSQL数据库服务。在云计算平台高性能、高可用、高可靠、高安全、可弹性伸缩的基础上，提供了一键部署、备份恢复、监控报警等服务能力。

云数据库 GeminiDB目前兼容Cassandra、DynamoDB API、MongoDB、InfluxDB和Redis主流NoSQL接口，并提供高读写性能，具有高性价比，适用于IoT、气象、互联网、游戏等领域。

如何选择接口

不同接口的适用场景及功能存在差异，您可以根据业务需要选择接口产品。

表 1-1 场景说明

接口名称	兼容接口	使用场景	说明
GeminiDB Redis接口	兼容Key-Value接口：Redis	GeminiDB提供高并发、低延迟业务访问。具备极致弹性扩缩容能力，从容应对业务高峰。常见的用户场景包括游戏、广告RTA、推荐系统、电商、教育等。	GeminiDB Redis是一款100%兼容Redis协议的弹性KV数据库，支持远超内存的容量和极致的性能。它具有稳定低延迟、高性价比、无需备节点，全主架构、具备4:1超高数据压缩等优势，支持Hash Field过期、布隆过滤器、数据极速导入、内存加速等企业级特性。

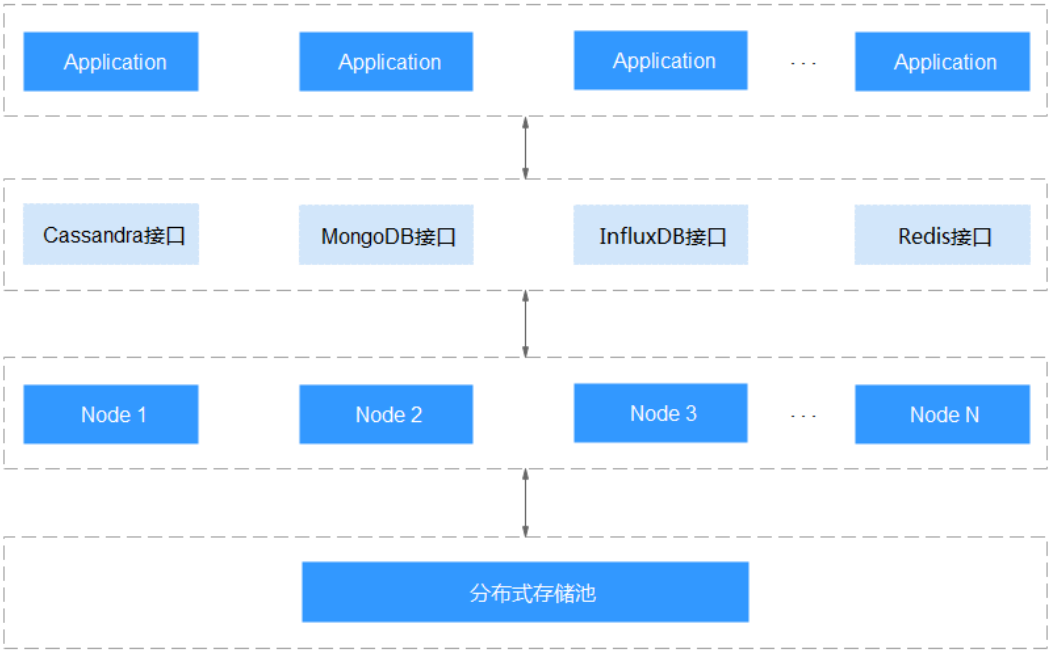
接口名称	兼容接口	使用场景	说明
GeminiDB Influx接口	兼容时间序列型接口：InfluxDB	GeminiDB Influx接口广泛应用于资源监控，业务监控分析，物联网设备实时监控，工业生产监控，生产质量评估和故障回溯等。	GeminiDB Influx接口是一款基于华为自研的计算存储分离架构，兼容InfluxDB生态的云原生NoSQL时序数据库。提供大并发的时序数据读写，压缩存储和类SQL查询，并且支持多维聚合计算和数据可视化分析能力。具有高写入、灵活弹性、高压缩率和高查询等特点。
GeminiDB Cassandra接口	兼容宽列接口：Cassandra，DynamoDB API	GeminiDB Cassandra接口支持TB级别存储及近百万级QPS，提供强一致性级别，可适配各类应用场景，尤其是大规模集群部署：例如工业制造和气象业、互联网等海量数据存储的场景。	GeminiDB Cassandra 接口 是一款基于华为自研的计算存储分离架构，兼容Cassandra生态的云原生NoSQL数据库，支持类SQL语法CQL。具有安全可靠、超强读写、弹性扩展、便捷管理等特点。
GeminiDB Mongo接口	兼容文档型接口：MongoDB	GeminiDB Mongo接口近百万级QPS，开源3倍性能提升，支持存海量文档、图片、IoT/车联网数据、社交视频/语音等，适用于互联网、物联网、游戏、金融等领域。	GeminiDB Mongo接口是一款基于华为自研的计算存储分离架构，兼容MongoDB生态的云原生NoSQL数据库。具有企业级性能、灵活弹性、高可靠、可视化管理等特点。

2 系统架构

架构介绍

云数据库 GeminiDB是一款基于计算存储分离架构的分布式数据库，由多个同构节点组成计算集群。数据存储在分布式共享存储池中。计算和存储资源解耦，支持独立弹性伸缩，扩缩容无数据迁移。

图 2-1 系统架构



3 产品优势

高可靠

数据备份

数据备份包括自动和手动两种方式。自动备份为系统自动创建的数据库实例的全量备份，手动备份是由用户启动的数据库实例的全量备份，且备份成功后均支持恢复。

备份数据存储至对象存储服务（Object Storage Service，简称OBS），在提高数据容灾能力的同时有效降低磁盘空间占用。创建实例时，默认开启自动备份策略，实例创建成功后，将自动执行一次全量备份，该备份文件默认保留7天，创建成功后可以设置自动备份的周期，修改备份策略。同时，用户也可以根据自身业务特点随时发起备份，手动备份会一直保存，直到用户手动删除。

高安全

网络隔离

通过虚拟私有云（Virtual Private Cloud，简称VPC）和网络安全组实现网络隔离。虚拟私有云允许租户通过配置虚拟私有云入站IP范围，来控制连接数据库的IP地址段。数据库实例运行在租户独立的虚拟私有云内，可提升数据库实例的安全性。您可以综合运用子网和安全组的配置，来完成数据库实例的隔离。

访问控制

可以通过虚拟私有云对数据库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。

传输加密

通过SSL加密实现传输加密。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。

安全防护

云数据库 GeminiDB具有多层网络防护。通过虚拟私有云、子网、安全组、DDoS防护以及SSL安全访问等多层安全防护体系，有力地抗击各种恶意攻击，保证数据安全。

- 基于虚拟私有云技术，真正实现租户隔离和访问控制。
- 通过传输层SSL安全协议，提供安全及数据完整性保障。
- 可在IP及端口层面进行安全访问限制，加强云数据库 GeminiDB与其他服务间的安全访问。

性能监控

云数据库 GeminiDB具有完善的性能监控，为您分担60%以上的运维工作。对CPU使用率、IOPS、网络吞吐量等实例信息实时监控及报警，随时随地了解实例动态。

易用性

即开即用

您可以通过控制台实时创建目标实例，配合服务器一起使用，通过内网连接数据库，有效地降低应用响应时间、节省公网流量。

高度兼容

目前，云数据库 GeminiDB兼容Cassandra协议、MongoDB协议、InfluxDB协议、Redis协议。

易扩展

云数据库 GeminiDB作为基于计算存储分离的分布式数据库服务，可达到分钟级计算节点扩展，秒级存储扩容。

4 典型应用

游戏应用

游戏应用可以将一些游戏数据，如用户装备、用户积分等存储其中。游戏玩家活跃高峰期，对并发能力要求较高，可以快速灵活添加计算节点以应对高并发场景。

优势：

- **灵活：**游戏开服6小时内需多次扩容，GeminiDB Mongo计算节点增加，扩容性能倍数提升，可灵活轻松应对。
- **数据恢复快：**表级时间点恢复，支持游戏快速回档。
- **稳定扩容：**扩容期间性能稳定，不影响游戏体验。

IoT

云数据库 GeminiDB兼容Cassandra接口，拥有超强写入性能，专为密集写入而设计。它适用于各种不同的行业，例如制造业、物流业、医疗保健业、房地产业、能源生产业、农业等等。 无论传感器类型如何，都可以很好地处理传入数据，并为进一步的数据分析提供了可能。

优势：

- **超强写入：**相比于其他NoSQL服务，拥有超强的写入性能。
- **弹性扩展：**基于计算存储分离的分布式架构，分钟级计算节点扩容，应对业务高峰期；秒级存储扩容应对7*24不间断的大数据量写入。

互联网应用

云数据库 GeminiDB快速读写和高可扩展特性使其适用于具有产品目录、推荐、个性化接口等功能的电子商务网站和娱乐网站，可用于存储访问者的活动，有利于分析工具快速访问数据，为用户生成推荐。

优势：

- **超强写入：**相比于其他NoSQL服务，拥有超强写入性能。
- **大数据分析：**结合Spark等工具，可以用于实时推荐等大数据场景。

金融行业

云数据库 GeminiDB结合Spark等大数据分析工具，可应用于金融行业的风控体系，构建反欺诈系统。

优势：

大数据分析：结合Spark等工具，可以进行实时的反欺诈检测。

5 安全

5.1 责任共担

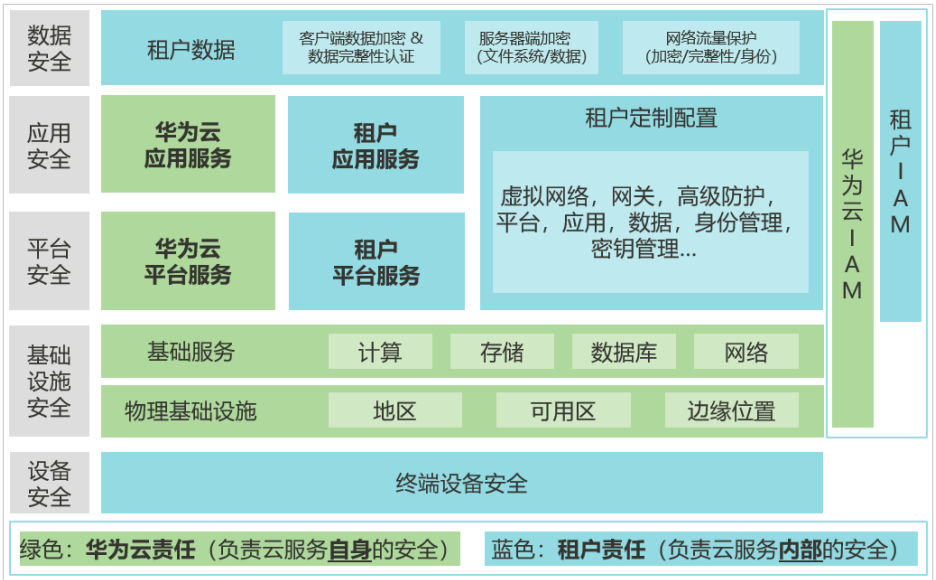
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图5-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

身份认证

用户访问云数据库 GeminiDB时支持对数据库用户进行身份验证，包含密码验证和IAM验证两种方式。

- **密码验证**

  您需要对数据库实例进行管理，通过控制台登录Web客户端页面时，需要对账号密码进行验证，验证成功后方可进行操作。

- **IAM验证**

  您可以使用**统一身份认证服务**（Identity and Access Management， IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。您创建的IAM用户，需要通过验证用户和密码才可以使用GeminiDB资源。具体请参见**创建IAM用户并登录**。

访问控制

- **权限控制**

  购买实例之后，您可以使用IAM为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，通过IAM进行精细的权限管理。具体内容请参见**权限管理**。

- **VPC和子网**

  虚拟私有云（Virtual Private Cloud，VPC）为云数据库构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。您可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。

  子网提供与其他网络隔离的、可以独享的网络资源，以提高网络安全性。

  具体内容请参见**创建虚拟私有云和子网**。

- **安全组**

  安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求并相互信任的弹性云服务器和云数据库 GeminiDB实例提供访问策略。为了保障数据库的安全性和稳定性，在使用GeminiDB数据库实例之前，您需要设置安全组，开通需访问数据库的IP地址和端口。

  具体请参见**设置安全组规则**。

5.3 数据保护技术

云数据库 GeminiDB通过多种数据保护手段和特性，保障存储在GeminiDB中的数据安全可靠。

表 5-1 GeminiDB 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密（SSL）	GeminiDB Redis、GeminiDB Mongo、GeminiDB Cassandra和GeminiDB Influx实例支持非SSL和SSL传输协议，为保证数据传输的安全性，推荐您使用更加安全的SSL协议。	• GeminiDB Redis：**设置SSL数据加密** • GeminiDB Influx：**设置SSL数据加密** • GeminiDB Cassandra：**设置SSL数据加密** • GeminiDB Mongo：**设置SSL数据加密**
跨可用区部署	为了达到更高的可靠性，GeminiDB支持选择3可用区，可用区之间内网互通，不同可用区之间物理隔离，GeminiDB会自动将实例下的节点Hash均衡部署在3个可用区内，实现跨可用区容灾部署。	• GeminiDB Redis：**购买实例选择跨可用区部署** • GeminiDB Influx：**购买实例选择跨可用区部署** • GeminiDB Cassandra：**购买实例选择跨可用区部署** • GeminiDB Mongo：**购买实例选择跨可用区部署**
负载均衡	GeminiDB Redis支持负载均衡，数据访问可以均衡的分散在集群的不同节点，避免热点，最大化集群整体的吞吐量。	GeminiDB Redis：**通过负载均衡地址连接实例**
同城容灾	GeminiDB Cassandra主实例支持搭建主备高可用架构，当主实例发生突发性自然灾害等状况，主实例节点无法连接时，可将容灾实例切换为主实例。	GeminiDB Cassandra：**创建容灾实例**

数据保护手段	简要说明	详细介绍
异地双活	GeminiDB Cassandra接口提供了异地双活功能，通过异地实例间数据的双向同步和业务灵活调度能力，实现了业务恢复和故障恢复解耦，保障了故障场景下业务的连续性。	GeminiDB Cassandra：**异地双活原理介绍**
删除保护	云数据库 GeminiDB支持将退订后的包年包月实例和删除的按需实例，加入回收站管理。通过数据库回收站中重建实例功能，可以恢复1~7天内删除的实例。	• GeminiDB Redis：**回收站** • GeminiDB Influx：**回收站** • GeminiDB Cassandra：**回收站** • GeminiDB Mongo：**回收站**

5.4 审计与日志

审计

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录GeminiDB的管理事件和数据事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

- CTS支持追踪的GeminiDB Redis管理事件和数据事件列表，请参见**支持审计的关键操作列表**。
- CTS支持追踪的GeminiDB Influx管理事件和数据事件列表，请参见**支持审计的关键操作列表**。
- CTS支持追踪的GeminiDB Cassandra管理事件和数据事件列表，请参见**支持审计的关键操作列表**。
- CTS支持追踪的GeminiDB Mongo管理事件和数据事件列表，请参见**支持审计的关键操作列表**。

日志

- GeminiDB Redis

  支持查看数据库级别的慢日志，执行时间的单位为ms。通过该日志，可查找出执行效率低的语句，进行优化。

  慢日志的详细介绍，请参见**慢日志**。
- GeminiDB Cassandra

  支持查看数据库级别的慢日志，执行时间的单位为ms。通过该日志，可查找出执行效率低的语句，进行优化。

慢日志的详细介绍，请参见**慢日志**。

- GeminiDB Mongo
  - 支持查看数据库级别的慢日志，执行时间的单位为ms。通过该日志，可查找出执行效率低的语句，进行优化。

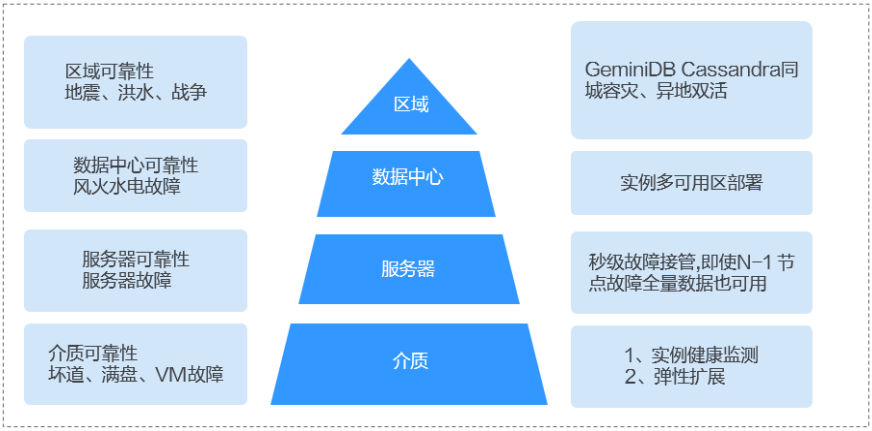
    慢日志的详细介绍，请参见**慢日志**。
  - 支持查看数据库级别的错误日志，包括数据库运行的Warning和Error级别的信息，有助于分析系统中存在的问题。

    错误日志的详细介绍，请参见**错误日志**。

5.5 服务韧性

- GeminiDB Redis使用DFV存储池，本身具有三副本的冗余，提供数据实时持久化，还通过多可用区部署、秒级故障接管、负载均衡、节点可缩减等技术方案，保障实例的可靠性和可用性。
- GeminiDB Influx使用DFV存储池，本身具有三副本的冗余，支持高写入性能，还通过多可用区部署、弹性扩展等技术方案，保障实例的可靠性和可用性。
- GeminiDB Cassandra使用DFV存储池，本身具有三副本的冗余，支持7*24小时在线数据实时写入，还通过同城容灾、异地双活、多可用区部署、最高N-1个节点故障容忍、弹性扩展等技术方案，保障实例的可靠性和可用性。
- GeminiDB Mongo使用DFV存储池，本身具有三副本的冗余，支持7*24小时在线数据实时写入，还通过多可用区部署、最高N-1个节点故障容忍、弹性扩展等技术方案，保障实例的可靠性和可用性。

图 5-2 可靠性架构保证数据稳定，业务可靠



5.6 监控安全风险

监控指标

云数据库 GeminiDB提供基于云监控服务CES的资源和操作监控能力，帮助用户监控账号下的GeminiDB实例，执行自动实时监控、告警和通知操作。用户可以实时掌握实例运行过程中产生的运行指标和存储用量等信息。

- 关于GeminiDB Redis支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。

- 关于GeminiDB Influx支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。
- 关于GeminiDB Cassandra支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。
- 关于GeminiDB Mongo支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。

敏感操作保护

GeminiDB控制台支持敏感操作保护，开启后执行删除实例等敏感操作时，系统会进行身份验证，进一步保证GeminiDB配置和数据的安全性。更多信息，请参见**敏感操作保护介绍**。

5.7 故障恢复

GeminiDB会在数据库实例的备份时段中创建数据库实例的自动备份。系统根据您指定的备份保留期（1~35天）保存数据库实例的自动备份。

- GeminiDB Redis提供了恢复实例数据的方法，具体请参见**恢复备份到新实例**。
- GeminiDB Influx提供了恢复实例数据的方法，具体请参见**恢复备份到新实例**。
- GeminiDB Cassandra提供了恢复实例数据的方法，具体请参见**恢复备份到新实例**和**恢复备份到指定时间点**。
- GeminiDB Mongo提供了恢复实例数据的方法，具体请参见**恢复备份到新实例或已有实例**。

同城容灾

GeminiDB Cassandra主实例支持搭建主备高可用架构，当主实例发生突发性自然灾害等状况，主实例节点无法连接时，可将容灾实例切换为主实例。

异地双活

GeminiDB Cassandra提供了异地双活功能，通过异地实例间数据的双向同步和业务灵活调度能力，实现了业务恢复和故障恢复解耦，保障了故障场景下业务的连续性。

多可用区

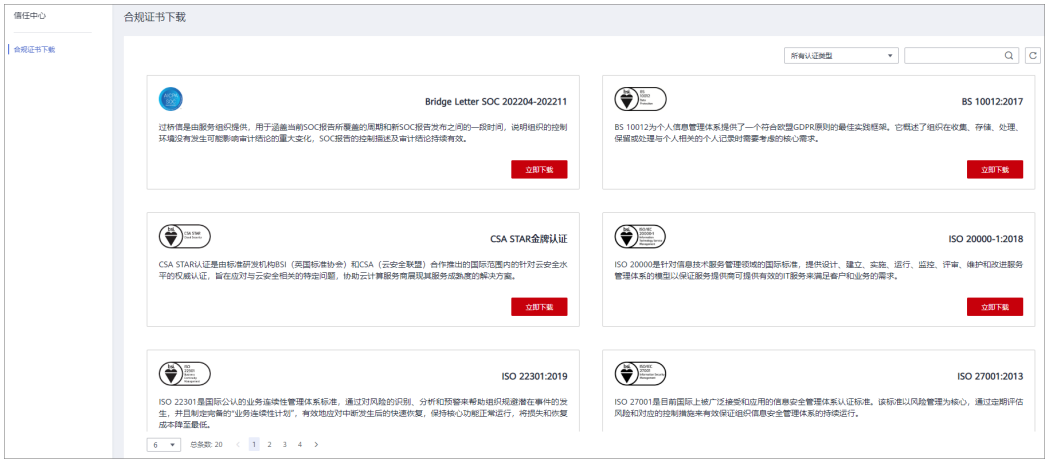
可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。GeminiDB支持将将实例下的节点Hash均衡部署在3个可用区内，实现跨可用区容灾部署。

5.8 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 5-3 合规证书下载



资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 5-4 资源中心

6 计费说明

云数据库 GeminiDB仅按实际用量付费，没有最低消费。

计费项

云数据库 GeminiDB按照您实例规格和存储空间计费，即云数据库 GeminiDB的价格=实例规格价格+存储空间价格。

表 6-1 计费项说明

计费项	计费说明
数据库实例	● 按照您选择的实例规格计费。 ● 针对实例提供包年包月和按需（小时）计费方式。
数据库存储	按照您选择存储空间收费。
备份存储（可选）	云数据库 GeminiDB的备份数据存储在OBS上。购买实例存储空间后，云数据库 GeminiDB将同比例赠送备份存储空间，用于存储备份数据。例如，您购买的实例存储空间为100GB时，会得到赠送的100GB备份存储空间。当备份数据没有超出100GB，将免费存储在OBS上；当备份数据超出100GB，超出部分将根据OBS的计费规则收费。
公网流量	云数据库 GeminiDB实例支持公网访问，公网访问会产生带宽流量费；云数据库 GeminiDB实例在云内部网络产生的流量不计费。

计费模式

提供按小时、按月、按年的计费方式供您灵活选择，使用越久越便宜，同时也支持包周期和按需计费方式转换。

- 预付费（包年包月）：这种购买方式相对于按需付费提供更大的折扣，对于长期使用者，推荐该方式。
- 按需付费（小时）：这种购买方式比较灵活，可以即开即停，按实际使用时长计费。以自然小时为单位整点计费，不足一小时按实际使用时长计费。

变更配置

- 变更实例规格：您可以根据业务需求变更云数据库 GeminiDB实例规格，变更后即刻按照变更后的实例规格的价格计费。
- 扩容存储空间：您可以根据业务需求增加您的存储空间，扩容后即刻按照新的存储空间计费。您需要注意的是存储空间只允许扩容，不能缩容。您每次扩容的最小容量为1GB。

7 权限管理

如果您需要对华为云购买的云数据库 GeminiDB资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有云数据库 GeminiDB的使用权限，但是不希望他们拥有删除云数据库 GeminiDB等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用云数据库 GeminiDB，但是不允许删除云数据库 GeminiDB的权限策略，控制他们对云数据库 GeminiDB资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用云数据库 GeminiDB服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见**《IAM产品介绍》**。

云数据库 GeminiDB 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

云数据库 GeminiDB部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问云数据库 GeminiDB时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，云数据库 GeminiDB支持的API授权项请参见**云数据库 GeminiDB服务授权项说明**。

如**表7-1**所示，包括了云数据库 GeminiDB的所有系统权限。

表 7-1 云数据库 GeminiDB 系统权限

策略名称/系统角色	描述	类别	依赖关系
GeminiDB FullAccess	云数据库 GeminiDB服务所有权限。	系统策略	创建包周期实例需要配置CBC权限： • bss:balance:view • bss:balance:update • bss:order:view • bss:order:pay • bss:order:update • bss:renewal:view • bss:renewal:update 退订包周期实例需要配置CBC权限： • bss:unsubscribe:update 如果要使用存储空间自动扩容功能，IAM子账号需要添加如下授权项： • 创建自定义策略： – iam:agencies:listAgencies – iam:agencies:createAgency – iam:permissions:listRolesForAgencyOnProject – iam:permissions:grantRoleToGroupOnProject – iam:roles:listRoles – iam:roles:createRole

策略名称/系统角色	描述	类别	依赖关系
			● 添加系统角色：Security Administrator 1. 选择该用户所在的一个用户组。 2. 单击“授权”。 3. 添加Security Administrator系统角色。 其中GeminiDB FullAccess已包含iam:agencies:listAgencies、iam:roles:listRoles、iam:agencies:pass权限。 由于GeminiDB是Region级服务，而IAM是Global级服务，将GeminiDB FullAccess授权给项目时，需要再授权BSS ServiceAgencyReadPolicy（全局级服务）；如果将GeminiDB FullAccess授权给全部项目，可正常使用IAM权限。 BSS ServiceAgencyCreatePolicy包含其他操作权限： ● iam:agencies:createAgency ● iam:permissions:grantRoleToAgency
GeminiDB ReadOnlyAccess	云数据库 GeminiDB服务只读权限。	系统策略	无

表7-2列出了云数据库 GeminiDB常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 7-2 常用操作与系统权限的关系

操作	GeminiDB FullAccess	GeminiDB ReadOnlyAccess
创建实例	√	x
查询实例列表	√	√
查询实例详情	√	√
查询任务列表	√	√
删除实例	√	x
重启实例	√	x
重置密码	√	x
变更实例安全组	√	x
修改数据库端口	√	x
绑定/解绑公网IP	√	x
磁盘扩容	√	x
规格变更	√	x
节点扩容	√	x
节点缩容	√	x
修改备份策略	√	x
重命名实例	√	x
创建手动备份	√	x
查询备份列表	√	√
恢复到新实例	√	x
删除备份	√	x
创建参数模板	√	x
查询参数模板列表	√	√
修改参数模板	√	x
删除参数模板	√	x
查询企业项目配额管理列表	√	√

操作	GeminiDB FullAccess	GeminiDB ReadOnlyAccess
修改企业项目配额	√	x
切换SSL开关	√	x
停止备份	√	x

表7-3列出了云数据库 GeminiDB常用操作以及对应的授权项，您可以参照该表自定义配置权限策略。

表 7-3 常用操作与对应的授权项

操作	授权项	授权范围	备注
实例创建页	• vpc:vpcs:list • vpc:subnets:get • vpc:securityGroups:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	创建页需要查询对应的VPC、子网、安全组。
创建实例	• nosql:instance:create • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:ports:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	界面使用默认VPC、子网、安全组需对应配置vpc:*:create权限， 创建加密实例需要在项目上配置KMS Administrator权限。
查询实例列表	nosql:instance:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询实例详情	nosql:instance:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	如果实例详情界面需要展示VPC、子网、安全组，请增加vpc:*:get和vpc:*:list授权项。
查询任务列表	nosql:task:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

操作	授权项	授权范围	备注
删除实例	nosql:instance:delete	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	删除实例需要同时删除数据侧IP地址。
重启实例	nosql:instance:restart	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
重置密码	nosql:instance:modifyPasswd	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
变更实例安全组	nosql:instance:modifySecurityGroup	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
修改数据库端口	nosql:instance:modifyPort	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
绑定公网IP	nosql:instance:bindPublicIp	支持： • IAM项目(Project)	绑定公网IP时，需要查询已经创建好的公网IP。 • 不支持企业项目 • 不支持细粒度 具体请参见**浮动IP**。
解绑公网IP	nosql:instance:unbindPublicIp	支持： • IAM项目(Project)	• 不支持企业项目 • 不支持细粒度 具体请参见**浮动IP**。
磁盘扩容	nosql:instance:modifyStorageSize	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
规格变更	nosql:instance:modifySpecification	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

操作	授权项	授权范围	备注
节点扩容	• nosql:instance:extendNode • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:ports:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
节点缩容	nosql:instance:reduceNode	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	删除集群节点。
修改备份策略	nosql:instance:modifyBackupPolicy	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
重命名实例	nosql:instance:rename	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
创建手动备份	nosql:backup:create	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询备份列表	nosql:backup:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
下载备份文件	nosql:backup:download	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

操作	授权项	授权范围	备注
恢复到新实例	• nosql:backup:restoreToNewInstance • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:ports:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	加密实例需要在项目上配置KMS Administrator权限。
备份恢复到已有实例	nosql:backup:restoreToExistInstance	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
删除备份	nosql:backup:delete	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
创建参数模板	nosql:param:create	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询参数模板列表	nosql:param:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
修改参数模板中的参数值	nosql:param:modify	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
变更实例下节点的参数配置	nosql:instance:modifyParameter	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
删除参数模板	nosql:param:delete	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

操作	授权项	授权范围	备注
标签操作	• nosql:instance:tag • tms:resourceTags:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
标签列表	• nosql:tag:list • tms:resourceTags:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询企业项目配额管理列表	nosql:quota:list	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
修改企业项目配额	nosql:quota:modify	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
切换审计日志开关	nosql:instance:switchAuditLog	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
下载审计日志	nosql:instance:downloadAuditLog	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
删除审计日志	nosql:instance:deleteAuditLog	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
更新慢日志明文开关	nosql:instance:modifySlowLogPlaintextSwitch	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
切换SSL开关	nosql:instance:switchSSL	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

操作	授权项	授权范围	备注
修改内网IP	nosql:instance:modifyPrivateIp	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
切换主备节点	nosql:instance:switchover	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
数据库补丁升级	nosql:instance:upgradeDatabaseVersion	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
停止备份	nosql:backup:stop	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询日志配置组	lts:groups:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-
查询日志配置流	lts:topics:get	支持： • IAM项目(Project) • 企业项目(Enterprise Project)	-

相关链接

- **IAM产品介绍**
- **创建用户并授予云数据库 GeminiDB权限**
- **策略支持的授权项**

8 区域和可用区

什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图8-1阐明了区域和可用区之间的关系。

图 8-1 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见华为云全球站点。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等

方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

9 与其他服务的关系

云数据库 GeminiDB与其他服务的关系，如图9-1所示。

图 9-1 云数据库 GeminiDB 与其他服务的关系

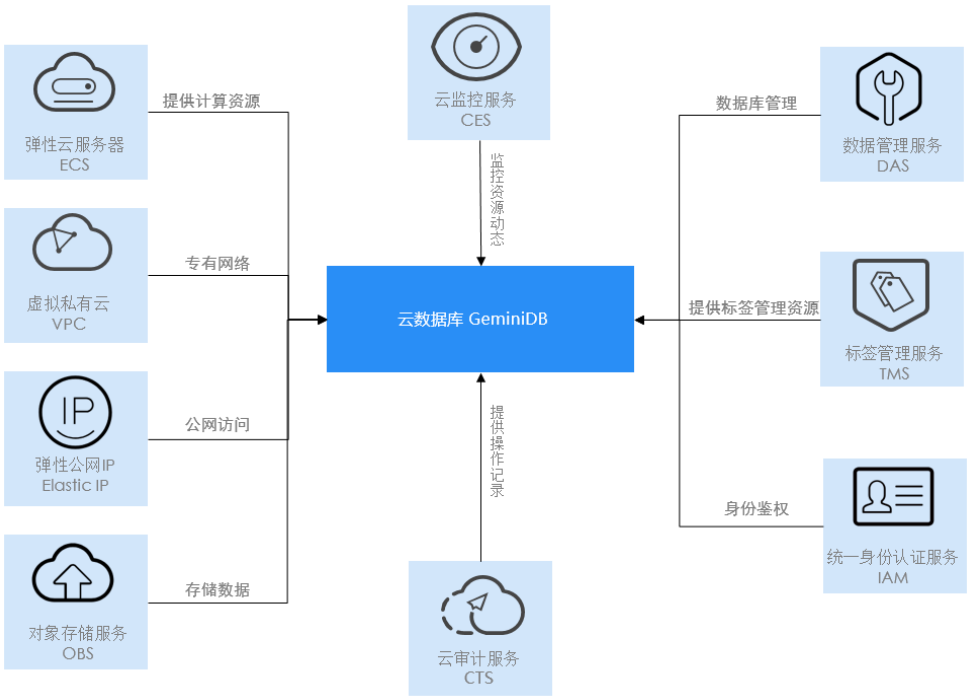


表 9-1 云数据库 GeminiDB 与其他服务的关系

服务名称	云数据库 GeminiDB与其他服务的关系
弹性云服务器	弹性云服务器（Elastic Cloud Server，简称ECS）为云数据库GeminiDB提供可弹性申请的计算资源，为数据库实例提供运行环境。

服务名称	云数据库 GeminiDB与其他服务的关系
虚拟私有云	通过虚拟私有云（Virtual Private Cloud，简称VPC）和网络安全组实现网络隔离。虚拟私有云允许租户通过配置虚拟私有云入站IP范围，来控制连接数据库的IP地址段。数据库实例运行在租户独立的虚拟私有云内，可提升数据库实例的安全性。
弹性公网IP	弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。
对象存储服务	备份数据存储至对象存储服务（Object Storage Service，简称OBS），在提高数据容灾能力的同时有效降低磁盘空间占用。
云审计服务	云审计服务（Cloud Trace Service，简称CTS），记录了云数据库 GeminiDB相关的操作事件，方便用户日后的查询、审计和回溯。
统一身份认证服务	统一身份认证服务（Identity and Access Management，简称IAM）为云数据库 GeminiDB提供了权限管理功能。
标签管理服务	标签管理服务（Tag Management Service，简称TMS）用于用户在云平台，通过统一的标签管理各种资源。标签管理服务与各服务共同实现标签管理能力，标签管理服务提供全局标签管理能力，各服务维护自身标签管理。