TaurusDB for PostgreSQL

产品介绍

文档版本 01

发布日期 2025-11-24

华为云计算技术有限公司

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 什么是云数据库 TaurusDB for PostgreSQL

TaurusDB for PostgreSQL是华为自研的新一代云原生数据库，100%兼容开源PostgreSQL。搭载华为云最新一代高性能计算存储基础设施，基于Babelfish插件提供SQL Server异构兼容能力，旨在为您提供具备高性能、高弹性、安全可靠的数据库服务。

产品当前处于公测状态，如需使用，请提交工单。

为什么选择云数据库 TaurusDB for PostgreSQL

- 开源生态

  TaurusDB for PostgreSQL 100%兼容开源PostgreSQL，提供丰富插件支持，基于原生PostgreSQL 的应用可以实现0改造迁移。

- 异构兼容

  TaurusDB for PostgreSQL基于Babelfish插件实现了对T-SQL语句和TDS协议的支持，客户无需更改驱动，只需少量代码适配，即可将基于SQL Server的应用迁移至TaurusDB for PostgreSQL。

如何使用云数据库 TaurusDB for PostgreSQL

您可以通过以下方式使用数据库。

管理控制台：您可以使用管理控制台为您提供的Web界面完成数据库的相关操作。

了解**TaurusDB for PostgreSQL常用概念**可以帮助您更好地选购云数据库TaurusDB for PostgreSQL 。

2 TaurusDB for PostgreSQL 产品系列

TaurusDB for PostgreSQL实例分为如下几个类型：

- 单机实例
- 主备实例

表 2-1 实例类型简介

实例类型	简介	使用说明	适用场景
单机实例	采用单个数据库节点部署架构。与主流的主备实例相比，它只包含一个节点，但具有高性价比。	单机版出现故障后，无法保障及时恢复。	• 个人学习。 • 微型网站。 • 中小企业的开发测试环境。
主备实例	采用一主一备的经典高可用架构，支持跨AZ高可用，选择主可用区和备可用区不在同一个可用区（AZ）。主实例和备实例共用一个IP地址。	• 备机提高了实例的可靠性，创建主机的过程中，会同步创建备机，备机创建成功后，用户不可见。 • 当主节点故障后，会发生主备切换，期间数据库客户端会发生短暂中断。若存在复制延时，主备切换时间会长一点，数据库客户端需要支持重新连接。	• 大中型企业的生产数据库。 • 覆盖互联网、物联网、零售电商、物流、游戏等行业的应用。

优势对比

- 单机实例：相较于主备实例，单机实例少了一个数据库节点，可大幅节省用户成本，售价低至主备实例的一半。由于单机实例只有一个数据库节点，当该数据库

节点出现故障时，恢复时间较长，因此，如果是对数据库可用性要求较高的敏感性业务，不建议使用单机实例。

- 主备实例：主备实例的备数据库节点仅用于故障转移和恢复场景，不对外提供服务。在单节点故障场景下，由于备机的存在，主备实例可以通过故障倒换进行快速的业务恢复。但由于使用备数据库节点会带来额外性能开销，从性能角度来看，单机实例的性能与主备实例相同，甚至单机实例的性能可能会高于主备实例。

3 TaurusDB for PostgreSQL 常用概念

实例

云数据库TaurusDB for PostgreSQL服务的最小管理单元是实例，一个实例代表了一个独立运行的数据库，实例ID是实例的唯一标识符。一个数据库实例可以包含多个由用户创建的数据库，并且可以使用多种工具和应用程序进行访问。每个数据库名具有唯一性。

购买实例时会有默认的管理员账号，使用该账号可以创建库、数据库用户并分配权限。管理员密码支持购买实例时设置或者购买后设置，如果忘记管理员密码，可以重置密码。

用户可以在云数据库TaurusDB服务系统中自助创建及管理各种数据库引擎的实例。实例的类型、规格、引擎、版本和状态，请参考**实例说明**。

实例规格

数据库实例各种规格（vCPU个数、内存（GB）、对应的数据库引擎）请参考**TaurusDB for PostgreSQL实例规格**。

自动备份

创建实例时，云数据库TaurusDB for PostgreSQL服务默认开启自动备份策略，实例创建成功后，您可对其进行修改，关系型数据库会根据您的配置，自动创建数据库实例的备份。

手动备份

手动备份是由用户启动的数据库实例的全量备份，它会一直保存，直到用户手动删除。

区域和可用区

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3-1阐明了区域和可用区之间的关系。

图 3-1 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**。

项目

Project用于将OpenStack的资源（计算、存储和网络资源）进行分组和隔离。Project可以是一个部门或者一个项目组。一个账户中可以创建多个Project。

4 实例说明

4.1 TaurusDB for PostgreSQL 实例类型

数据库实例是TaurusDB for PostgreSQL的最小管理单元。一个实例代表了一个独立运行的TaurusDB for PostgreSQL。您可以在一个实例中创建和管理多个数据库，并且可以使用与独立访问数据库实例相同的工具和应用进行访问。使用管理控制台可以方便地创建或者修改数据库实例。云数据库 TaurusDB for PostgreSQL服务对运行实例数量没有限制，但每个数据库实例都有唯一的标识符。

实例可进行如下分类：

表 4-1 实例类型

实例类型	简介	使用说明
单机实例	采用单个数据库节点部署架构。与主流的主备实例相比，它只包含一个节点，但具有高性价比。	单机版出现故障后，无法保障及时恢复。
主备实例	采用一主一备的经典高可用架构，主备实例的每个节点的规格保持一致。 TaurusDB for PostgreSQL支持跨AZ高可用。选择主可用区和备可用区不在同一个可用区（AZ）。	• 备机提高了实例的可靠性，创建主机的过程中，会同步创建备机，备机创建成功后，用户不可见。 • 当主节点故障后，会自动发生主备切换，数据库客户端会发生短暂中断，数据库客户端需要支持重新连接。 • TaurusDB for PostgreSQL默认是异步。

用户可以在TaurusDB for PostgreSQL系统中自助创建及管理各种数据库引擎的实例。

不同实例类型之间的区别请参考**TaurusDB for PostgreSQL产品系列**。

4.2 TaurusDB for PostgreSQL 实例存储类型

数据库系统通常是IT系统最为重要的系统，对存储IO性能要求高，您可根据需要选择您所需的存储类型。TaurusDB for PostgreSQL暂时不支持创建实例后变更存储类型。

存储类型说明

云数据库TaurusDB for PostgreSQL支持SSD云盘和极速型SSD存储类型，可以满足不同的业务场景，具体如下：

- SSD云盘

  SSD云盘为云盘存储，弹性扩容，将数据存储于SSD云盘，即实现了计算与存储分离。最大吞吐量350 MB/s。

  支持的IOPS取决于云硬盘（Elastic Volume Service，简称EVS）的IO性能，具体请参见《云硬盘产品介绍》中“**磁盘类型及性能介绍**”中“超高IO”的内容。

- 极速型SSD

  极速型SSD云盘，结合25 GE网络和RDMA技术，为您提供单盘最大吞吐量达1000 MB/s并具有亚毫秒级低时延性能。

  支持的IOPS取决于云硬盘的IO性能，具体请参见《云硬盘产品介绍》中“**磁盘类型及性能介绍**”中“极速型SSD”的内容。

存储类型性能对比

表 4-2 存储类型对比

对比项	SSD云盘	极速型SSD云盘
I/O性能	有额外的网络I/O，吞吐性能相对较差。	吞吐性能相对SSD云盘有大幅提升。
弹性扩展能力	秒级扩容。	秒级扩容。
最大IOPS	50000	128000
最大吞吐量	350 MB/s	1000 MB/s
读写时延	1 ms	亚毫秒级

4.3 TaurusDB for PostgreSQL 实例规格

TaurusDB for PostgreSQL云盘存储的X86架构规格包含：通用型（推荐）、独享型（推荐）。规格说明请参见**表4-3**。支持的规格列表请参见**表4-4**。

表 4-3 X86 架构规格说明

规格	说明	适用场景	约束限制
通用型（推荐）	与同一物理机上的其他通用型规格实例共享CPU资源，通过资源复用换取CPU使用率最大化，性价比较高，适用于对性能稳定性要求较低的应用场景。	侧重对成本、性价比要求较高的场景。	主推规格，支持的区域如下： • 亚太-新加坡 • 亚太-曼谷 • 土耳其-伊斯坦布尔 • 拉美-圣保罗一 • 中东-利雅得
独享型（推荐）	完全独享的CPU和内存，性能长期稳定，不会因为物理机上其它实例的行为而受到影响，适用于对性能稳定性要求较高的应用场景。	电商、游戏、金融、政企等核心数据库场景。	

通用型、独享型规格

数据库实例规格请以实际环境为准。

表 4-4 通用型、独享型规格

规格	主备实例规格码	单机实例规格码	vCPU(个)	内存(GB)
通用型	taurus.pg.n1.large.2.ha	taurus.pg.n1.large.2	2	4
	taurus.pg.n1.large.4.ha	taurus.pg.n1.large.4	2	8
	taurus.pg.n1.xlarge.2.ha	taurus.pg.n1.xlarge.2	4	8
	taurus.pg.n1.xlarge.4.ha	taurus.pg.n1.xlarge.4	4	16
	taurus.pg.n1.2xlarge.2.ha	taurus.pg.n1.2xlarge.2	8	16
	taurus.pg.n1.2xlarge.4.ha	taurus.pg.n1.2xlarge.4	8	32
独享型 **说明** SSD云盘和极速型SSD支持的独享型规格存在差异，请以实际环境为准。	taurus.pg.x1.large.2.ha	-	2	4
	taurus.pg.x1.large.4.ha	-	2	8
	taurus.pg.x1.large.8.ha	-	2	16

规格	主备实例规格码	单机实例规格码	vCPU(个)	内存(GB)
	taurus.pg.x1.xlarge.2.ha	-	4	8
	taurus.pg.x1.xlarge.4.ha	-	4	16
	taurus.pg.x1.xlarge.8.ha	taurus.pg.x1.xlarge.8	4	32
	taurus.pg.x1.2xlarge.2.ha	taurus.pg.x1.2xlarge.2	8	16
	taurus.pg.x1.2xlarge.4.ha	taurus.pg.x1.2xlarge.4	8	32
	taurus.pg.x1.2xlarge.8.ha	taurus.pg.x1.2xlarge.8	8	64
	taurus.pg.x1.4xlarge.2.ha	taurus.pg.x1.4xlarge.2	16	32
	taurus.pg.x1.4xlarge.4.ha	taurus.pg.x1.4xlarge.4	16	64
	taurus.pg.x1.4xlarge.8.ha	taurus.pg.x1.4xlarge.8	16	128
	taurus.pg.x1.8xlarge.2.ha	taurus.pg.x1.8xlarge.2	32	64
	taurus.pg.x1.8xlarge.4.ha	taurus.pg.x1.8xlarge.4	32	128
	taurus.pg.x1.8xlarge.8.ha	taurus.pg.x1.8xlarge.8	32	256
	taurus.pg.x1.16xlarge.2.ha	taurus.pg.x1.16xlarge.2	64	128
	taurus.pg.x1.16xlarge.4.ha	taurus.pg.x1.16xlarge.4	64	256
	taurus.pg.x1.16xlarge.8.ha	taurus.pg.x1.16xlarge.8	64	512
	taurus.pg.x1.24xlarge.2.ha	taurus.pg.x1.24xlarge.2	96	192
	taurus.pg.x1.24xlarge.4.ha	taurus.pg.x1.24xlarge.4	96	384
	taurus.pg.x1.24xlarge.8.ha	taurus.pg.x1.24xlarge.8	96	768

规格	主备实例规格码	单机实例规格码	vCPU(个)	内存(GB)
	taurus.pg.x1.32xlarge.2.ha	taurus.pg.x1.32xlarge.2	128	256
	taurus.pg.x1.32xlarge.4.ha	taurus.pg.x1.32xlarge.4	128	512
	taurus.pg.x1.32xlarge.8.ha	taurus.pg.x1.32xlarge.8	128	1024

4.4 TaurusDB for PostgreSQL 实例状态

数据库实例状态

数据库实例状态是数据库实例的运行情况。用户可以使用管理控制台和API操作查看数据库实例状态。

表 4-5 状态及说明

状态	说明
正常	数据库实例正常和可用。
异常	数据库实例不可用。
创建中	正在创建数据库实例。
创建失败	数据库实例创建失败。
重启中	实例重启中。
端口修改中	正在修改数据库实例的数据库端口。
扩容中	数据库实例的磁盘空间扩容中。
备份中	正在备份数据库实例。
恢复中	正在恢复备份到实例中。
恢复失败	实例恢复失败。
冻结	账户余额小于或等于0美元，系统对该用户下的实例进行冻结。您需前往费用中心充值成功，欠款核销后，冻结的实例才会解冻。
存储空间满	实例的磁盘空间已满，此时不可进行数据库写入操作，您需要扩容磁盘使实例恢复到正常状态。
已删除	数据库实例已被删除，对于已经删除的实例，将不会在实例列表中显示。

状态	说明
等待重启	数据库参数修改后，有些参数修改，需等待用户重启实例才能生效。
停止中	实例正在停止中。
已停止	数据库实例已停止，默认停止七天，对于已停止的实例，再次正常使用需用户手动开启或超过默认时间数据库自动开启。
开启中	已停止的实例正在开启中。

5 安全

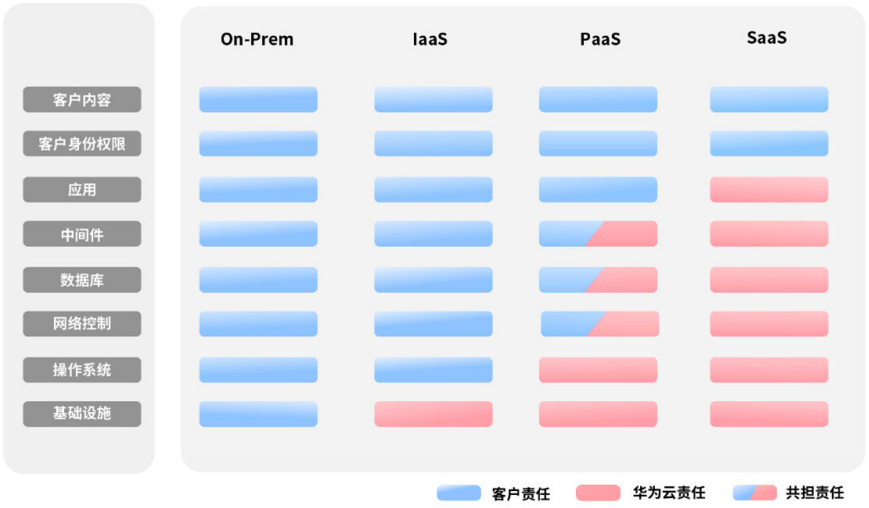
5.1 责任共担

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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图5-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况下，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 5-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图5-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好PaaS服务中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

传统本地部署(On-Prem)：由客户在自有数据中心内部署和管理软件及IT基础设施，而非依赖于远程的云服务提供商；

基础设施即服务(IaaS)：由云服务提供商提供计算、网络、存储等基础设施服务，如**弹性云服务器 ECS**、**虚拟专用网络 VPN**、**对象存储服务 OBS**；

平台即服务(PaaS)：由云服务提供商提供应用程序开发和部署所需要的平台，客户无需维护底层基础设施，如**AI开发平台 ModelArts**、**云数据库 GaussDB**；

软件即服务 (SaaS)：由云服务提供商提供完整应用软件，客户直接应用软件而无需安装、维护应用软件及底层平台和基础设施，如**华为云会议 Meeting**。

5.2 身份认证与访问控制

身份认证

用户访问云数据库TaurusDB for PostgreSQL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，使用数据管理服务（Data Admin Service）登录数据库时，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云数据库TaurusDB for PostgreSQL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**TaurusDB for PostgreSQL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TaurusDB for PostgreSQL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TaurusDB for PostgreSQL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**添加安全组规则**。

5.3 数据保护技术

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

表 5-1 TaurusDB for PostgreSQL 的数据保护手段和特性

数据保护手段	简要说明
传输加密（SSL）	支持SSL传输协议，保证数据传输的安全性。
跨可用区部署	为了达到更高的可靠性，TaurusDB for PostgreSQL支持选择多可用区部署主实例和备实例，可用区之间内网互通，不同可用区之间物理隔离，TaurusDB会自动将主实例和备实例分布到不同的可用区，以提供故障切换能力和高可用性。

5.4 审计与日志

审计

- 云审计服务（Cloud Trace Service，CTS）

  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TaurusDB for PostgreSQL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**。

- 数据库安全服务（Database Security Service，DBSS）

  DBSS是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

  建议使用DBSS来提供扩展的数据安全能力，详情请参考**数据库安全服务**。

  优势：

  - 助力企业满足等保合规要求。
    - 满足等保测评数据库审计需求。
    - 满足国内外安全法案合规需求，提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告。
  - 支持备份和恢复数据库审计日志，满足审计数据保存期限要求。
  - 支持风险分布、会话统计、会话分布、SQL分布的实时监控能力。
  - 提供风险行为和攻击行为实时告警能力，及时响应数据库攻击。
  - 帮助您对内部违规和不正当操作进行定位追责，保障数据资产安全。

  数据库安全审计采用数据库旁路部署方式，在不影响用户业务的前提下，可以对数据库进行灵活的审计。

  - 基于数据库风险操作，监视数据库登录、操作类型（数据定义、数据操作和数据控制）和操作对象，有效对数据库进行审计。
  - 从风险、会话、SQL注入等多个维度进行分析，帮助您及时了解数据库状况。
  - 提供审计报表模板库，可以生成日报、周报或月报审计报表（可设置报表生成频率）。同时，支持发送报表生成的实时告警通知，帮助您及时获取审计报表。

日志

- 错误日志记录了数据库运行时的日志，通过错误日志有助于分析系统中存在的问题。
- 慢日志用来记录执行时间超过当前慢日志阈值“log_min_duration_statement”的语句，通过慢日志的日志明细、统计分析情况，查找出执行效率低的语句，进行优化。

5.5 故障恢复

云数据库TaurusDB for PostgreSQL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（1~732天）保存数据库实例的自动备份。

多可用区

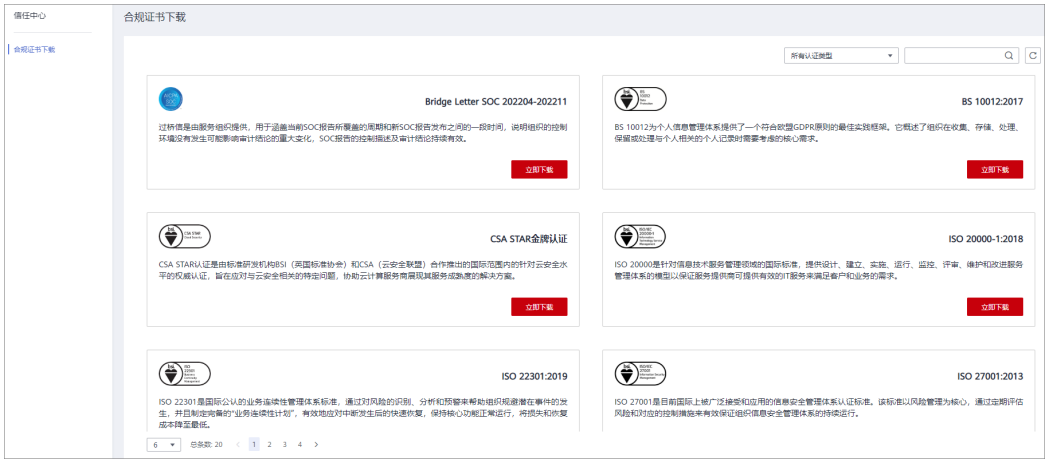
可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。TaurusDB for PostgreSQL支持在同一个可用区内或者跨可用区部署数据库主备实例，以提供故障切换能力和高可用性。

5.6 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 5-2 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 5-3 资源中心

6 TaurusDB for PostgreSQL 权限管理

如果您需要对华为云上购买云服务平台上创建的TaurusDB for PostgreSQL资源，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，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，您希望开发人员拥有TaurusDB for PostgreSQL的使用权限，但是不希望他们拥有删除TaurusDB for PostgreSQL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TaurusDB for PostgreSQL，但是不允许删除TaurusDB for PostgreSQL的权限，控制他们对TaurusDB for PostgreSQL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TaurusDB for PostgreSQL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**。

TaurusDB for PostgreSQL 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。

TaurusDB for PostgreSQL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”，然后在指定区域对应的项目中设置相关权限，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TaurusDB for PostgreSQL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TaurusDB for PostgreSQL服务，管理员能够控制IAM用户仅能对某一类数据库资源进行指定的管理操作。

如表6-1所示，包括了TaurusDB for PostgreSQL的所有系统权限。

表 6-1 TaurusDB for PostgreSQL 系统策略

策略名称/系统角色	描述	类别	依赖关系
TaurusDB FullAccess	云数据库TaurusDB for PostgreSQL服务所有权限。	系统策略	其中TaurusDB FullAccess已包含iam:agencies:listAgencies、iam:roles:listRoles、iam:agencies:pass权限。 由于TaurusDB for PostgreSQL是Region级服务，而IAM是Global级服务，将TaurusDB FullAccess授权给项目时，需要再授权BSS ServiceAgencyReadPolicy（全局级服务）；如果将TaurusDB 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。
TaurusDB ReadOnlyAccess	云数据库TaurusDB for PostgreSQL服务资源只读权限。	系统策略	无。

表6-2列出了TaurusDB for PostgreSQL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 6-2 常用操作与系统权限的关系

操作	TaurusDB FullAccess	TaurusDB ReadOnlyAccess
创建TaurusDB for PostgreSQL实例	√	x
删除TaurusDB for PostgreSQL实例	√	x
查询TaurusDB for PostgreSQL实例列表	√	√

表 6-3 常用操作与对应授权项

操作名称	授权项	备注
创建数据库实例	gaussdb:instance:create gaussdb:param:list	界面选择VPC、子网、安全组需要配置： vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:securityGroupRules:get 创建加密实例需要在项目上配置KMS Administrator权限。 购买包周期实例需要配置： bss:order:update bss:order:pay
扩容数据库实例的磁盘空间	gaussdb:instance:extendSpace	无。
重启数据库实例	gaussdb:instance:restart	无。
删除数据库实例	gaussdb:instance:delete	无。
查询数据库实例列表	gaussdb:instance:list	无。
实例详情	gaussdb:instance:list	实例详情界面展示VPC、子网、安全组，需要对应配置vpc:*:get和vpc:*:list。
修改数据库实例密码	gaussdb:password:update	无。
修改端口	gaussdb:instance:modifyPort	无。

操作名称	授权项	备注
修改实例名称	gaussdb:instance:modify	无。
修改同步模式	gaussdb:instance:modifySynchronizeModel	无。
切换策略	gaussdb:instance:modifyStrategy	无。
设置回收站策略	gaussdb:instance:setRecycleBin	无。
表级时间点恢复	gaussdb:instance:tableRestore	无。
获取参数模板列表	gaussdb:param:list	无。
创建参数模板	gaussdb:param:create	无。
修改参数模板参数	gaussdb:param:modify	无。
应用参数模板	gaussdb:param:apply	无。
修改指定实例的参数	gaussdb:param:modify	无。
获取指定实例的参数模板	gaussdb:param:list	无。
获取指定参数模板的参数	gaussdb:param:list	无。
删除参数模板	gaussdb:param:delete	无。
重置参数模板	gaussdb:param:reset	无。
对比参数模板	gaussdb:param:list	无。
保存参数模板	gaussdb:param:save	无。
查询参数模板类型	gaussdb:param:list	无。
设置自动备份策略	gaussdb:instance:modifyBackupPolicy	无。
查询自动备份策略	gaussdb:instance:list	无。
创建手动备份	gaussdb:backup:create	无。
获取备份列表	gaussdb:backup:list	无。
获取备份下载链接	gaussdb:backup:download	无。
查询可恢复时间段	gaussdb:instance:list	无。

操作名称	授权项	备注
恢复到新实例	gaussdb:instance:create	界面选择VPC、子网、安全组需要配置： vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:securityGroupRules:get
恢复到已有或当前实例	gaussdb:instance:restoreInPlace	无。
获取数据库备份文件列表	gaussdb:backup:list	无。
获取历史数据库列表	gaussdb:backup:list	无。
查询数据库错误日志	gaussdb:log:list	无。
查询数据库慢日志	gaussdb:log:list	无。
下载数据库错误日志	gaussdb:log:download	无。
下载数据库慢日志	gaussdb:log:download	无。
开启、关闭审计日志	gaussdb:auditlog:operate	无。
获取审计日志列表	gaussdb:auditlog:list	无。
查询审计日志策略	gaussdb:auditlog:list	无。
生成审计日志下载链接	gaussdb:auditlog:download	无。
获取主备切换日志	gaussdb:log:list	无。
创建数据库	gaussdb:database:create	无。
查询数据库列表	gaussdb:database:list	无。
查询指定用户的已授权数据库	gaussdb:database:list	无。
删除数据库	gaussdb:database:drop	无。
创建数据库账户	gaussdb:databaseUser:create	无。
查询数据库账户列表	gaussdb:databaseUser:list	无。
查询指定数据库的已授权账户	gaussdb:databaseUser:list	无。
删除数据库账户	gaussdb:databaseUser:drop	无。

操作名称	授权项	备注
授权数据库账户	gaussdb:databasePrivilege:grant	无。
解除数据库账户权限	gaussdb:databasePrivilege:revoke	无。
任务中心列表	gaussdb:task:list	无。
删除任务中心任务	gaussdb:task:delete	无。
用户标签操作	gaussdb:instance:modify	标签相关操作依赖tms:resourceTags:*权限。
停止实例	gaussdb:instance:stop	无。
开启实例	gaussdb:instance:start	无。
修改数据库用户名备注	gaussdb:databaseUser:update	无。

7 TaurusDB for PostgreSQL 约束与限制

TaurusDB for PostgreSQL在使用上有一些固定限制，用来提高实例的稳定性和安全性。

规格与性能限制

表 7-1 规格说明

资源类型	规格
存储空间	● SSD云盘：40GB~4000GB ● 极速型SSD：40GB~4000GB
最大连接数	取决于“max_connections”参数的值。
IOPS	● SSD云盘：最大50000 ● 极速型SSD：最大128000

配额

表 7-2 配额

资源类型	限制
标签	1个实例最多支持20个标签配额。
免费备份空间	TaurusDB for PostgreSQL提供了和实例磁盘大小相同的部分免费存储空间，用于存放您的备份数据。
自动备份保留天数	默认为7天，可设置范围为1～732天。
日志查询	● 错误日志明细：2000条 ● 慢日志明细：2000条

命名限制

表 7-3 命名限制

限制项	说明
实例名称	• 长度在4个到64个字符之间。 • 必须以字母开头，区分大小写，可以包含字母、数字、中划线或下划线，不能包含其他特殊字符。
数据库名称	• 长度可在1～63个字符之间 • 由字母、数字、或下划线组成，不能包含其他特殊字符，不能以“pg”和数字开头，且不能和TaurusDB for PostgreSQL模板库重名。TaurusDB for PostgreSQL模板库包括postgres， template0 ，template1。
账号名称	• 长度在1到128个字符之间。 • 由字母、数字、中划线或下划线组成，不能包含其他特殊字符，不能和系统用户名称相同。系统用户包括：rdsadmin, rdsuser, rdsbackup, rdsmirror。
备份名称	• 长度在4~64个字符之间。 • 必须以字母开头，区分大小写，可以包含字母、数字、中划线或者下划线，不能包含其他特殊字符。
参数模板名称	• 长度在1~64个字符之间。 • 区分大小写，可包含字母、数字、中划线、下划线或句点，不能包含其他特殊字符。

安全限制

表 7-4 安全限制

限制项	说明
管理员账户root权限	创建实例页面只提供管理员root账户，TaurusDB for PostgreSQL为root用户在特定场景进行了提权，详见**root用户权限说明**。
管理员账户root的密码	• 长度为8~32个字符。 • 至少包含大写字母、小写字母、数字、特殊字符三种字符的组合，其中允许输入~!@#%^*-_=+?,特殊字符。
数据库端口	设置范围为2100～9500。
磁盘加密	购买磁盘加密后，在实例创建成功后不可修改磁盘加密状态，且无法更改密钥。
虚拟私有云	目前TaurusDB for PostgreSQL实例创建完成后不支持切换虚拟私有云。

限制项	说明
安全组	● 默认情况下，一个用户可以创建100个安全组。 ● 默认情况下，一个安全组最多只允许拥有50条安全组规则。 ● 目前一个TaurusDB for PostgreSQL实例允许绑定一个安全组，一个安全组可以关联多个TaurusDB for PostgreSQL实例。
系统账户	创建TaurusDB for PostgreSQL数据库实例时，系统会自动为实例创建如下系统账户（用户不可使用），用于给数据库实例提供完善的后台运维管理服务。 ● rdsAdmin：管理账户，拥有最高权限，用于查询和修改实例信息、故障排查、迁移、恢复等操作。 ● pg_execute_server_program：允许用运行该数据库的用户执行数据库服务器上的程序来配合COPY和其他允许执行服务器端程序的函数。 ● pg_read_all_settings：读取所有配置变量。 ● pg_read_all_stats：读取所有的pg_stat_*视图并且使用与扩展相关的各种统计信息。 ● pg_stat_scan_tables：执行可能会在表上取得ACCESS SHARE锁的监控函数（可能会持锁很长时间）。 ● pg_signal_backend：向其他后端发送信号（例如：取消查询、中止）。 ● pg_read_server_files：允许使用COPY以及其他文件访问函数从服务器上该数据库可访问的任意位置读取文件。 ● pg_write_server_files：允许使用COPY以及其他文件访问函数在服务器上该数据库可访问的任意位置中写入文件。 ● pg_monitor：读取/执行各种监控视图和函数。这个角色是pg_read_all_settings、pg_read_all_stats以及pg_stat_scan_tables的成员。 ● rdsRepl：复制账户，用于备实例在主实例上同步数据。 ● rdsBackup：备份账户，用于后台的备份。 ● rdsMetric：指标监控账户，用于watchdog采集数据库状态数据。
实例参数	为确保云数据库TaurusDB for PostgreSQL服务发挥出最优性能，可根据业务需求对用户创建的参数模板中的参数进行调整。

实例操作限制

表 7-5 实例操作限制

限制项	说明
实例部署	实例所部署的弹性云服务器，对用户都不可见，即只允许应用程序通过IP地址和端口访问数据库。
数据迁移	云数据库TaurusDB for PostgreSQL提供了多种数据同步方案，可满足从TaurusDB for PostgreSQL、自建PostgreSQL数据库、其他云PostgreSQL、自建Oracle数据库、RDS for MySQL、自建MySQL数据库、或其他云MySQL同步到云数据库TaurusDB for PostgreSQL。 常用的数据迁移工具有：DRS、pg_dump、DAS。推荐使用DRS，DRS可以快速解决多场景下，数据库之间的数据流通问题，操作便捷、简单，仅需分钟级就能搭建完成迁移任务。通过服务化迁移，免去了传统的DBA人力成本和硬件成本，帮助您降低数据传输的成本。
主备复制	TaurusDB for PostgreSQL本身提供主备复制架构的双节点集群，无需用户手动搭建。其中主备复制架构集群的备实例不对用户开放，用户应用不可直接访问。
CPU使用率高	CPU使用率很高或接近100%，会导致数据读写处理缓慢、连接缓慢、删除出现报错等，从而影响业务正常运行。
重启实例	无法通过命令行重启，必须通过管理控制台操作重启实例。
停止/开启实例	• 支持对按需计费实例进行关机，通过暂时停止实例以节省费用。 • 在停止数据库实例后，支持手动重新开启实例。
查看备份	下载手动和自动备份文件，用于本地存储备份。支持使用OBS Browser+下载、直接浏览器下载、按地址下载备份文件。
日志管理	TaurusDB for PostgreSQL默认开启日志，不支持关闭。

root 用户权限说明

TaurusDB for PostgreSQL开放了root用户权限。为了便于用户使用TaurusDB for PostgreSQL并保证在无操作风险的前提下，为root用户在特定场景进行了提权。

各个版本root用户提权情况见下表。

表 7-6 root 用户权限说明

版本	是否提权	提权起始版本
pgcore16	是	16.2

root提权涉及以下场景：

- 创建事件触发器
- 创建包装器
- 创建逻辑复制-发布
- 创建逻辑复制-订阅
- 查询和维护复制源
- 创建replication用户
- 创建全文索引模板以及Parser
- 对系统表执行vacuum
- 对系统表执行analyze
- 创建插件
- 授予用户某个对象的权限

8 TaurusDB for PostgreSQL 与其他服务的关系

表 8-1 与其他服务的关系

相关服务	交互功能
弹性云服务器（ECS）	通过弹性云服务器（Elastic Cloud Server，简称ECS）远程连接云数据库TaurusDB for PostgreSQL服务实例可以有效地降低应用响应时间、节省公网流量费用。
虚拟私有云（VPC）	对您的云数据库TaurusDB for PostgreSQL服务实例进行网络隔离和访问控制。
对象存储服务（OBS）	存储云数据库TaurusDB for PostgreSQL服务实例的自动和手动备份数据。
数据复制服务（DRS）	使用数据复制服务，实现数据库平滑迁移上云。