

云数据库 TaurusDB  
标准版

# 产品介绍

文档版本 01  
发布日期 2024-12-12



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。

---

# 目录

---

<b>1 什么是云数据库 TaurusDB 标准版</b>	<b>1</b>
<b>2 实例说明</b>	<b>3</b>
2.1 TaurusDB 标准版实例类型	3
2.2 TaurusDB 标准版存储类型	4
2.3 TaurusDB 标准版引擎和版本	4
2.4 TaurusDB 标准版实例规格	5
2.5 TaurusDB 标准版实例状态	6
<b>3 安全</b>	<b>9</b>
3.1 责任共担	9
3.2 身份认证与访问控制	10
3.3 数据保护技术	11
3.4 审计与日志	11
3.5 服务韧性	12
3.6 监控安全风险	13
3.7 故障恢复	13
3.8 认证证书	14
<b>4 TaurusDB 标准版权限管理</b>	<b>16</b>
<b>5 TaurusDB 标准版约束与限制</b>	<b>24</b>

# 1 什么是云数据库 TaurusDB 标准版

云数据库 TaurusDB标准版是一种基于云计算平台的稳定可靠、弹性伸缩、便捷管理的在线数据库。采用MySQL经典主备架构，并基于MySQL内核进行深度自研，在100%兼容MySQL的同时提供了更多更强的内核能力，如16K原子写、字段压缩、分区增强等能力。TaurusDB标准版为中小企业提供简化的数据库管理体验和强大的运维功能，助力中小企业在数字化转型中释放数据潜力。

## 成长地图

您可以通过[TaurusDB成长地图](#)快速了解相关概念、入门使用、高手进阶等。

## 如何使用 TaurusDB 标准版

您可以通过如下方式使用TaurusDB标准版。

- 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TaurusDB标准版的相关操作。
- API：您可以编写代码调用API使用TaurusDB标准版。

## 产品优势

- 100%兼容MySQL生态数据库
  - 兼容MySQL协议和生态，支持MySQL应用和工具无缝对接，使企业能够快速上手，轻松实现业务迁移。
  - 相比于社区MySQL，TaurusDB标准版的内核能力显著增强，新增了十二种二级分区，让分区表具备更加灵活的数据分治能力。
  - 提供了丰富的API接口和迁移工具，帮助企业加速应用开发和部署。
- 降本增效，运维便捷
  - 相比社区MySQL，TaurusDB标准版提供了备机可读能力，有效利用了所有节点资源。
  - TaurusDB标准版内核支持两倍字段压缩能力，减少了大字段存储资源。
  - 通过智能DBA实现了数据收集、分析、诊断一键式自动化，帮助DBA轻松搞定数据库运维。
  - 通过智能化的监控与告警系统，能够自动进行故障检测与恢复。
  - 提供自动备份、快速恢复和弹性扩展等功能，助力企业轻松管理数据库，专注核心业务的发展。

- 企业级高性能数据库

结合华为云计算、存储、网络和安全等领域的最佳实践，提供卓越的性能和可靠性。

支持16K原子写，在确保数据的一致性和可靠性下，减少写入操作的次数和延迟，提供高性能的MySQL数据库存储和访问服务，相比自建数据库性能提升了3倍，相比RDS for MySQL性能提升了20%，满足企业在各种负责业务场景中的需求，确保关键业务的平稳运行。

# 2 实例说明

## 2.1 TaurusDB 标准版实例类型

数据库实例是TaurusDB标准版的最小管理单元。一个实例代表了一个独立运行的TaurusDB标准版。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。使用管理控制台或基于HTTPS请求的API（Application programming interface）可以方便地创建或者修改数据库实例。TaurusDB标准版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。

TaurusDB标准版实例可进行如下分类：

表 2-1 实例类型

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。与高可用实例相比，它只包含一个节点，但具有高性价比。	单机实例出现故障后，无法保障及时恢复。	<ul style="list-style-type: none"><li>个人学习。</li><li>微型网站。</li><li>中小企业的开发测试环境。</li></ul>

实例类型	简介	使用说明	适用场景
高可用实例	<ul style="list-style-type: none"> <li>采用一主一备的经典高可用架构。</li> <li>支持跨可用区（AZ）高可用，可以选择主可用区和备可用区不在同一个可用区。</li> <li>主节点和备节点共用一个IP地址。</li> </ul>	<ul style="list-style-type: none"> <li>备节点提高了实例的可靠性，创建主节点的过程中，会同步创建备节点，备节点创建成功后，IP地址对用户不可见。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>大中型企业的生产数据库。</li> <li>覆盖互联网、物联网、零售电商、物流、游戏等行业的应用。</li> </ul>
只读实例	采用单个物理节点架构（没有备节点）。	当只读实例与主数据库之间复制异常后，需要较长时间重建和恢复（具体时长取决于数据量）。	在对数据库有少量写请求，但有大量读请求的应用场景下，可创建只读实例，利用只读实例满足大量的数据库读取需求，以此增加应用的吞吐量。

## 2.2 TaurusDB 标准版存储类型

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。

### 存储类型说明

- SSD云盘
 

SSD云盘是一种高性能的云存储解决方案，使用SSD(固态硬盘)作为数据存储介质。SSD云盘具有容量灵活、可根据需求进行扩容，以及不与ECS规格强绑定等优势。此外，SSD云盘的性能也可以根据实际业务需求进行灵活配置，如IOPS(每秒输入输出操作数)和吞吐量，从而实现容量与性能的解耦。适用于需要高性能、低延迟，并且数据存储容量有变化需求的应用场景，例如企业办公、虚拟桌面、大中型规模数据库等。

## 2.3 TaurusDB 标准版引擎和版本

TaurusDB标准版目前支持的数据库引擎和版本如表2-2所示。

新应用上线，建议您使用数据库引擎对应的最新大版本，以TaurusDB标准版为例，建议您选择8.0。用户创建实例时，不可选择小版本，如8.0.28，TaurusDB标准版会提供最优的小版本，实例创建成功，您可在管理控制台“实例管理”页面实例列表中的“数据库引擎版本”列，查看具体的小版本号。数据库引擎和版本请以实际环境为准。

图 2-1 查看数据库引擎版本



表 2-2 数据库引擎和版本

数据库引擎	单机实例	高可用实例
TaurusDB标准版	<ul style="list-style-type: none"> <li>8.0</li> <li>5.7</li> </ul>	<ul style="list-style-type: none"> <li>8.0</li> <li>5.7</li> </ul>

## 2.4 TaurusDB 标准版实例规格

TaurusDB标准版的实例CPU架构为X86架构，支持独享型实例规格。

表 2-3 规格类型说明

规格	说明	适用场景
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。

表 2-4 性能规格

规格类型	高可用实例规格码	只读实例规格码	单机实例规格码	vCPU(个)	内存(GB)
独享型	db.mysql.x1-ts.large.2.ha	db.mysql.x1-ts.large.2.rr	db.mysql.x1-ts.large.2	2	4
	db.mysql.x1-ts.large.4.ha	db.mysql.x1-ts.large.4.rr	db.mysql.x1-ts.large.4	2	8
	db.mysql.x1-ts.xlarge.2.ha	db.mysql.x1-ts.xlarge.2.rr	db.mysql.x1-ts.xlarge.2	4	8
	db.mysql.x1-ts.xlarge.4.ha	db.mysql.x1-ts.xlarge.4.rr	db.mysql.x1-ts.xlarge.4	4	16
	db.mysql.x1-ts.2xlarge.2.ha	db.mysql.x1-ts.2xlarge.2.rr	db.mysql.x1-ts.2xlarge.2	8	16

规格类型	高可用实例规格码	只读实例规格码	单机实例规格码	vCPU(个)	内存(GB)
	db.mysql.x1-ts.2xlarge.4.ha	db.mysql.x1-ts.2xlarge.4.rr	db.mysql.x1-ts.2xlarge.4	8	32
	db.mysql.x1-ts.4xlarge.2.ha	db.mysql.x1-ts.4xlarge.2.rr	db.mysql.x1-ts.4xlarge.2	16	32
	db.mysql.x1-ts.4xlarge.4.ha	db.mysql.x1-ts.4xlarge.4.rr	db.mysql.x1-ts.4xlarge.4	16	64
	db.mysql.x1-ts.8xlarge.2.ha	db.mysql.x1-ts.8xlarge.2.rr	db.mysql.x1-ts.8xlarge.2	32	64
	db.mysql.x1-ts.8xlarge.4.ha	db.mysql.x1-ts.8xlarge.4.rr	db.mysql.x1-ts.8xlarge.4	32	128
	db.mysql.x1-ts.16xlarge.2.ha	db.mysql.x1-ts.16xlarge.2.rr	db.mysql.x1-ts.16xlarge.2	64	128
	db.mysql.x1-ts.16xlarge.4.ha	db.mysql.x1-ts.16xlarge.4.rr	db.mysql.x1-ts.16xlarge.4	64	256
	db.mysql.x1-ts.24xlarge.2.ha	db.mysql.x1-ts.24xlarge.2.rr	db.mysql.x1-ts.24xlarge.2	96	192
	db.mysql.x1-ts.24xlarge.4.ha	db.mysql.x1-ts.24xlarge.4.rr	db.mysql.x1-ts.24xlarge.4	96	384
	db.mysql.x1-ts.32xlarge.2.ha	db.mysql.x1-ts.32xlarge.2.rr	db.mysql.x1-ts.32xlarge.2	128	256
	db.mysql.x1-ts.32xlarge.4.ha	db.mysql.x1-ts.32xlarge.4.rr	db.mysql.x1-ts.32xlarge.4	128	512

 说明

数据库实例规格请以实际环境为准。

## 2.5 TaurusDB 标准版实例状态

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 2-5 实例状态说明

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。
主备切换中	正在进行主节点和备节点的切换。
转高可用中	单机实例正在转换为高可用实例。
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。
规格变更中	数据库实例的CPU和内存规格变更中。
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。
转包周期中	按需付费实例正在转为包周期实例。
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。
实例小版本升级中	实例正在升级中。
版本升级	实例版本正在升级中。
备机迁移中	TaurusDB标准版备机正在迁移可用区中。
只读升主中	只读实例正在转换为独立的单机实例。
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。

状态	说明
实例读写状态变更中	正在变更数据库实例的读写状态。
强制只读	实例状态被手动设置为只读状态，在该状态下不允许执行写入、更新等引起数据变动的操作。

# 3 安全

## 3.1 责任共担

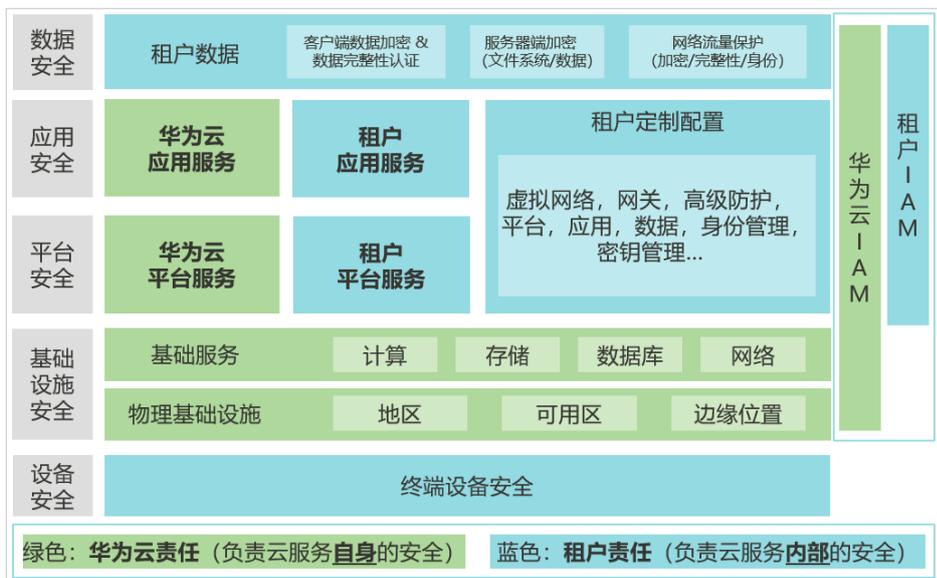
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如[图3-1](#)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 3-1 华为云安全责任共担模型



## 3.2 身份认证与访问控制

### 身份认证

用户访问TaurusDB标准版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，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TaurusDB标准版资源。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标准版权限管理](#)。
- 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TaurusDB标准版实例提供访问策略。为了保障数据库的安全性和稳定性，在使用TaurusDB标准版实例之前，您需要设置安全组，开通需访问数据库的IP地址和端口。

### 3.3 数据保护技术

TaurusDB标准版通过多种数据保护手段和特性，保障存储在其中的数据安全可靠。

表 3-1 TaurusDB 标准版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）	TaurusDB标准版实例支持非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。
跨可用区部署	为了达到更高的可靠性，TaurusDB标准版支持选择多可用区部署主节点和备节点，可用区之间内网互通，不同可用区之间物理隔离，TaurusDB标准版会自动将主节点和备节点分布到不同的可用区，以提供故障切换能力和高可用性。
删除保护	TaurusDB标准版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。
跨区域备份	TaurusDB标准版支持将备份文件存放到另一个区域存储，某一区域的实例故障后，可以在异地区域使用备份文件在异地恢复到新的TaurusDB标准版实例，用来恢复业务。

### 3.4 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标准版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

- 支持查看数据库级别的错误日志，包括数据库主库和从库运行的错误信息，以及运行较慢的SQL查询语句，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“long\_query\_time”（默认是1秒）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。
- 支持查看主备切换日志，通过TaurusDB标准版实例的主备切换日志信息，评估对业务的影响。
- 支持开通SQL审计功能，系统会将所有的SQL操作记录下来存入日志文件，以提供针对数据增删改查等操作的审计行为。

## 3.5 服务韧性

TaurusDB标准版使用EVS作为存放数据的云盘，本身具有三副本的冗余，提供9个9的数据持久性，还通过跨区域复制、AZ之间数据容灾、AZ内反亲和等技术方案，保障实例的可靠性和可用性。

图 3-2 可靠性架构保证数据稳定，业务可靠



## 3.6 监控安全风险

### 监控指标

TaurusDB标准版提供基于云监控服务CES的资源 and 操作监控能力，帮助用户监控账号下的TaurusDB标准版实例，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。

### 敏感操作保护

TaurusDB标准版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TaurusDB标准版配置和数据的安全性。更多信息，请参见[敏感操作保护介绍](#)。

## 3.7 故障恢复

TaurusDB标准版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。

### 跨区域备份

TaurusDB标准版支持将备份文件存放到另一个区域存储，某一区域的实例故障后，可以在异地区域使用备份文件在异地恢复到新的TaurusDB标准版实例，用来恢复业务。

实例开启跨区域备份策略后，会自动将该实例的备份文件备份到目标区域。

### 多可用区

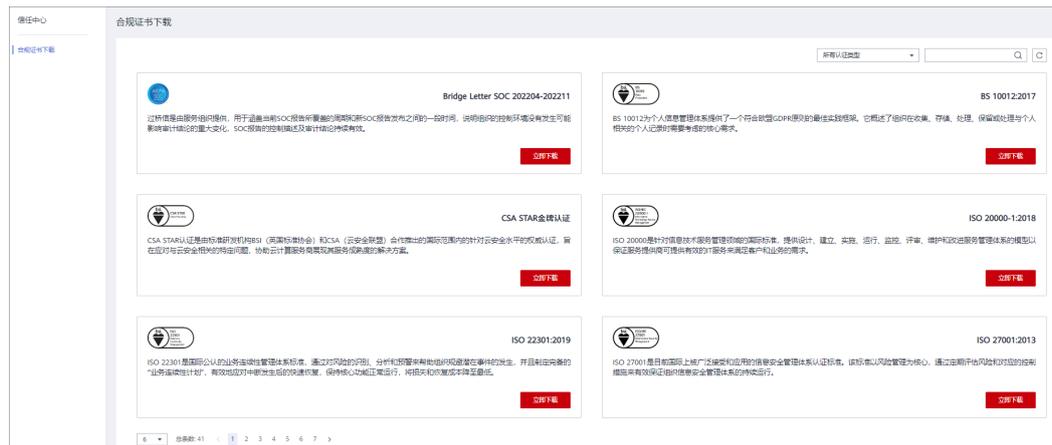
可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。TaurusDB标准版支持在同一个可用区内或者跨可用区部署数据库高可用实例，以提供故障切换能力和高可用性。

## 3.8 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 3-3 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 3-4 资源中心



### 销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看[合规资质证书](#)。

图 3-5 销售许可证&软件著作权证书



# 4 TaurusDB 标准版权限管理

如果您需要对华为云上购买云服务平台上创建的TaurusDB标准版资源，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标准版的使用权限，但是不希望他们拥有删除TaurusDB标准版等高危操作的权限，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标准版，但是不允许删除TaurusDB标准版的权限，控制他们对TaurusDB标准版资源的使用范围。

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标准版的其它功能。

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 标准版权限

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标准版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TaurusDB标准版时，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标准版服务，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。多数细粒度策略以API接口为粒度进行权限拆分，TaurusDB标准版支持的API授权项请参见[策略及授权项说明](#)。

如表4-1所示，包括了TaurusDB标准版的所有系统权限。

表 4-1 TaurusDB 标准版系统策略

策略名称/系统角色	描述	类别	依赖关系
RDS FullAccess	关系型数据库服务所有权限。	系统策略	<p>购买包周期实例需要配置授权项： bss:order:update bss:order:pay</p> <p>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：</p> <ul style="list-style-type: none"> <li>● 创建自定义策略： <ul style="list-style-type: none"> <li>- iam:agencies:listAgencies</li> <li>- iam:agencies:createAgency</li> <li>- iam:permissions:listRolesForAgencyOnProject</li> <li>- iam:permissions:grantRoleToGroupOnProject</li> <li>- iam:roles:listRoles</li> </ul> </li> <li>● 添加系统角色：Security Administrator <ol style="list-style-type: none"> <li>1. 选择该用户所在的一个用户组。</li> <li>2. 单击“授权”。</li> <li>3. 添加Security Administrator系统角色。</li> </ol> </li> </ul>

策略名称/系统角色	描述	类别	依赖关系
RDS ReadOnlyAccess	关系型数据库服务资源只读权限。	系统策略	无。
RDS ManageAccess	关系型数据库服务除删除操作外的DBA权限。	系统策略	无。
RDS Administrator	关系型数据库服务管理员。	系统角色	依赖Tenant Guest和Server Administrator角色，在同项目中勾选依赖的角色。

表4-2列出了TaurusDB标准版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 4-2 常用操作与系统权限的关系

操作	RDS FullAccess	RDS ReadOnlyAccess	RDS ManageAccess	RDS Administrator
创建TaurusDB标准版实例	√	x	√	√
删除TaurusDB标准版实例	√	x	x	√
查询TaurusDB标准版实例列表	√	√	√	√

表 4-3 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	rds:instance:create rds: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 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
变更数据库实例的规格	rds:instance:modifySpec	无。
扩容数据库实例的磁盘空间	rds:instance:extendSpace	无。
单机转高可用实例	rds:instance:singleToHa	若原单实例为加密实例，需要在项目上配置KMS Administrator权限。
重启数据库实例	rds:instance:restart	无。
删除数据库实例	rds:instance:delete	无。
查询数据库实例列表	rds:instance:list	无。
实例详情	rds: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	rds:password:update	无。
修改端口	rds:instance:modifyPort	无。
修改内网IP	rds:instance:modifyIp	界面查询剩余ip列表需要： vpc:subnets:get vpc:ports:get
修改实例名称	rds:instance:modify	无。
修改运维时间窗	rds:instance:modify	无。
手动主备倒换	rds:instance:switchover	无。

操作名称	授权项	备注
修改同步模式	rds:instance:modifySynchronizeModel	无。
切换策略	rds:instance:modifyStrategy	无。
修改实例安全组	rds:instance:modifySecurityGroup	无。
绑定/解绑公网IP	rds:instance:modifyPublicAccess	界面列出公网ip需要： vpc:publicips:get vpc:publicips:list
设置回收站策略	rds:instance:setRecycleBin	无。
查询回收站	rds:instance:list	无。
开启、关闭SSL	rds:instance:modifySSL	无。
开启、关闭事件定时器	rds:instance:modifyEvent	无。
读写分离操作	rds:instance:modifyProxy	无。
申请内网域名	rds:instance:createDns	无。
备机可用区迁移	rds:instance:create	备机迁移涉及租户子网下的IP操作，若为加密实例，需要在项目上配置KMS Administrator权限。
表级时间点恢复	rds:instance:tableRestore	无。
修改主机权限	rds:instance:modifyHost	无。
查询对应账号下的主机	rds:instance:list	无。
获取参数模板列表	rds:param:list	无。
创建参数模板	rds:param:create	无。
修改参数模板参数	rds:param:modify	无。
应用参数模板	rds:param:apply	无。
修改指定实例的参数	rds:param:modify	无。
获取指定实例的参数模板	rds:param:list	无。
获取指定参数模板的参数	rds:param:list	无。
删除参数模板	rds:param:delete	无。
重置参数模板	rds:param:reset	无。

操作名称	授权项	备注
对比参数模板	rds:param:list	无。
保存参数模板	rds:param:save	无。
查询参数模板类型	rds:param:list	无。
设置自动备份策略	rds:instance:modifyBackupPolicy	无。
查询自动备份策略	rds:instance:list	无。
创建手动备份	rds:backup:create	无。
获取备份列表	rds:backup:list	无。
获取备份下载链接	rds:backup:download	无。
删除手动备份	rds:backup:delete	无。
复制备份	rds:backup:create	无。
查询可恢复时间段	rds:instance:list	无。
恢复到新实例	rds: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
恢复到已有或当前实例	rds:instance:restoreInPlace	无。
获取实例binlog清理策略	rds:binlog:get	无。
合并binlog文件	rds:binlog:merge	无。
下载binlog文件	rds:binlog:download	无。
删除binlog文件	rds:binlog:delete	无。
设置binlog清理策略	rds:binlog:setPolicy	无。
获取数据库备份文件列表	rds:backup:list	无。
获取历史数据库列表	rds:backup:list	无。
查询数据库错误日志	rds:log:list	无。
查询数据库慢日志	rds:log:list	无。
下载数据库错误日志	rds:log:download	无。
下载数据库慢日志	rds:log:download	无。

操作名称	授权项	备注
开启、关闭审计日志	rds:auditlog:operate	无。
获取审计日志列表	rds:auditlog:list	无。
查询审计日志策略	rds:auditlog:list	无。
生成审计日志下载链接	rds:auditlog:download	无。
获取主备切换日志	rds:log:list	无。
创建数据库	rds:database:create	无。
查询数据库列表	rds:database:list	无。
查询指定用户的已授权数据库	rds:database:list	无。
删除数据库	rds:database:drop	无。
创建数据库账户	rds:databaseUser:create	无。
查询数据库账户列表	rds:databaseUser:list	无。
查询指定数据库的已授权账户	rds:databaseUser:list	无。
删除数据库账户	rds:databaseUser:drop	无。
授权数据库账户	rds:databasePrivilege:grant	无。
解除数据库账户权限	rds:databasePrivilege:revoke	无。
任务中心列表	rds:task:list	无。
删除任务中心任务	rds:task:delete	无。
包周期下单	bss:order:update	购买包周期实例需要配置授权项： bss:order:pay
用户标签操作	rds:instance:modify	标签相关操作依赖 tms:resourceTags:*权限。

操作名称	授权项	备注
存储空间自动扩容	rds:instance:extendSpace	<p>如果选择自动扩容，IAM主账号不需要添加授权项，IAM子账号需要添加如下授权项：</p> <ul style="list-style-type: none"> <li>● 创建自定义策略：                             <ul style="list-style-type: none"> <li>- iam:agencies:listAgencies</li> <li>- iam:agencies:createAgency</li> <li>- iam:permissions:listRolesForAgencyOnProject</li> <li>- iam:permissions:grantRoleToGroupOnProject</li> <li>- iam:roles:listRoles</li> </ul> </li> <li>● 添加系统角色：Security Administrator                             <ol style="list-style-type: none"> <li>1. 选择该用户所在的一个用户组。</li> <li>2. 单击“授权”。</li> <li>3. 添加Security Administrator系统角色。</li> </ol> </li> </ul>
停止实例、开启实例	rds:instance:operateServer	无。
停止实例	rds:instance:stop	无。
开启实例	rds:instance:start	无。
修改数据库用户名备注	rds:databaseUser:update	无。

# 5 TaurusDB 标准版约束与限制

TaurusDB标准版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 5-1 规格说明

资源类型	规格
存储空间	40GB~4000GB
连接数	最大100000
IOPS	<ul style="list-style-type: none"><li>SSD云盘：最大50000</li><li>高IO：最大5000</li><li>通用型SSD：最大20000</li></ul>

## 配额

表 5-2 配额

资源类型	限制
只读实例	1个实例最多创建5个只读实例。
标签	1个实例最多支持20个标签配额。
免费备份空间	TaurusDB标准版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。

资源类型	限制
日志保留天数	<ul style="list-style-type: none"> <li>● 错误日志明细：30天</li> <li>● 慢日志明细：30天</li> <li>● 慢日志明文显示：30天</li> <li>● 慢日志统计分析：30天</li> <li>● 主备切换日志：30天</li> <li>● SQL审计日志：默认为7天，可设置范围为1~732天。</li> </ul>

## 命名限制

表 5-3 命名限制

限制项	说明
实例名称	<ul style="list-style-type: none"> <li>● 长度最小为4字符，最大为64个字符，如果名称包含中文，则不超过64字节（注意：一个中文字符占用3个字节）。</li> <li>● 必须以字母或中文开头，区分大小写，可以包含字母、数字、中划线、下划线或中文，不能包含其他特殊字符。</li> </ul>
数据库名称	<ul style="list-style-type: none"> <li>● 长度可在1~64个字符之间。</li> <li>● 由字母、数字、中划线、下划线或\$组成，中划线和\$累计总长度小于等于10个字符，且不能包含其他特殊字符（TaurusDB标准版8.0不可包含\$）。</li> </ul>
账号名称	TaurusDB标准版5.7、8.0：长度为1~32个字符，由字母、数字、中划线或下划线组成，不能包含其他特殊字符。
备份名称	<ul style="list-style-type: none"> <li>● 长度在4~64个字符之间。</li> <li>● 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。</li> </ul>
参数模板名称	<ul style="list-style-type: none"> <li>● 长度在1~64个字符之间。</li> <li>● 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。</li> </ul>

## 安全限制

表 5-4 安全限制

限制项	说明
管理员账户root权限	<p>创建实例页面只提供管理员root账户，支持的权限请参见<a href="#">root账户权限</a>。</p> <p><b>说明</b> 建议用户谨慎对root账户执行revoke、drop user、rename user操作，避免影响业务正常使用。</p>
管理员账户root的密码	<ul style="list-style-type: none"> <li>长度为8~32个字符。</li> <li>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~!@\$#%^*_-=+?,()&amp;.特殊字符。</li> </ul>
数据库端口	<p>设置范围为1024~65535（其中12017和33071被系统占用不可设置）。</p>
磁盘加密	<p>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。</p>
虚拟私有云	<p>目前TaurusDB标准版实例创建完成后不支持切换虚拟私有云。</p>
安全组	<ul style="list-style-type: none"> <li>默认情况下，一个用户可以创建100个安全组。</li> <li>默认情况下，一个安全组最多只允许拥有50条安全组规则。</li> <li>目前一个实例允许绑定多个安全组，一个安全组可以关联多个实例。</li> <li>创建实例时，可以选择多个安全组（为了更好的网络性能，建议不超过5个）。</li> </ul>
系统账户	<p>创建TaurusDB标准版数据库实例时，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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>rdsRepl：复制账户，用于备节点在主节点上同步数据或只读实例在主实例上同步数据。</li> <li>rdsBackup：备份账户，用于后台的备份。</li> <li>rdsMetric：指标监控账户，用于watchdog采集数据库状态数据。</li> </ul>
实例参数	<p>为确保TaurusDB标准版发挥出最优性能，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。</p>

## 实例操作限制

表 5-5 实例操作限制

限制项	说明
存储引擎	支持InnoDB存储引擎。不支持MyISAM引擎、FEDERATED引擎、Memory引擎。
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	<p>TaurusDB标准版提供了多种数据迁移方案，可满足从RDS for MySQL、DDM、GaussDB、TaurusDB标准版、自建MySQL数据库、自建Oracle数据库、或其他云MySQL迁移到TaurusDB标准版。</p> <p>常用的数据迁移工具有：DRS、mysqldump。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。</p> <p><b>说明</b></p> <p>目前数据复制服务长期执行价格优惠政策，相关优惠政策如下：</p> <ul style="list-style-type: none"><li>• 实时迁移商用链路实行入云7天免费（免配置费用），7天后收取配置费用，降低数据上云门槛。</li><li>• 实时迁移和实时同步商用链路在定价上执行长期优惠策略，降低围绕云的数据传输门槛。</li></ul> <p>您可以通过DRS提供的<a href="#">DRS价格计算器</a>，选择您需要的配置规格，来快速计算出参考价格。</p>
主备复制	TaurusDB标准版本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节点IP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。
存储空间满	实例磁盘空间满，导致实例变为只读状态，应用无法对TaurusDB标准版数据库进行写入操作，从而影响业务正常运行。
支持的表数量	<p>TaurusDB标准版支持表数量上限为50万。</p> <p>大于50万张表时，会导致备份和小版本升级失败，影响数据库可用性。</p> <p>当表数量过多时(&gt;10万)，DDL语句会占用较多CPU资源，建议在控制台临时将“innodb_open_files”调大至实例中全部表数量。在DDL执行完毕后再调回默认值。</p> <p><b>须知</b></p> <p>“innodb_open_files”实际生效的值是“innodb_open_files”和“table_open_cache”中较小值。</p>
重启实例	无法通过命令行重启，必须通过TaurusDB标准版的管理控制台操作重启实例。

限制项	说明
停止/开启实例	<ul style="list-style-type: none"> <li>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。</li> <li>在停止数据库实例后，支持手动重新开启实例。</li> </ul>
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	<ul style="list-style-type: none"> <li>TaurusDB标准版默认开启日志，不支持关闭。</li> <li>TaurusDB标准版默认开启Binlog，无需额外配置，binlog_format格式为row。</li> <li>读实例没有备份文件，不会提供Binlog。</li> </ul>
回收站管理	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。
SQL规范	ZEROFILL属性已弃用，后续版本将删除，不允许使用该属性。

## root 账户权限

表 5-6 root 账户权限

权限	权限级别	描述	是否支持
Select	表	查询权限	支持
Insert	表	插入权限	
Update	表	更新权限	
Delete	表	删除权限	
Create	数据库、表或索引	创建数据库、表或索引权限	
Drop	数据库或表	删除数据库或表权限	
Reload	服务器管理	执行flush-hosts、flush-logs、flush-privileges、flush-status、flush-tables、flush-threads、refresh、reload等命令的权限。	
Process	服务器管理	查看进程权限	
Grant	数据库、表或保存的程序	赋予控制访问权限	

权限	权限级别	描述	是否支持
References	数据库或表	操作外键权限	
Index	表	索引权限	
Alter	表	更改表，比如添加字段、索引等	
Show_db	服务器管理	查看数据库链接	
Create_tmp_table	服务器管理	创建临时表权限	
Lock_tables	服务器管理	锁表权限	
Execute	存储过程	执行存储过程权限	
Repl_slave	服务器管理	复制权限	
Repl_client	服务器管理	复制权限	
Create_view	视图	创建视图权限	
Show_view	视图	查看视图权限	
Create_routine	存储过程	创建存储过程权限	
Alter_routine	存储过程	更改存储过程权限	
Create_user	服务器管理	创建用户权限	
Event	数据库	事件触发器	
Trigger	数据库	触发器	
Super	服务器管理	执行kill线程权限	不支持
File	服务器上的文件访问	访问数据库服务器节点文件权限	不支持
Shutdown	服务器管理	关闭数据库权限	
Create_tablespace	服务器管理	创建表空间权限	