

Alibaba Cloud

云数据库 MongoDB 版 安全白皮书

文档版本：20211122

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.产品概述	05
2.访问控制	06
3.网络隔离	07
4.数据加密	08
5.备份恢复	09
6.实例容灾	10
7.版本维护	11
8.服务授权	12

1. 产品概述

云数据库MongoDB版（ApsaraDB for MongoDB）完全兼容MongoDB协议，基于飞天分布式系统和高可靠存储引擎，提供多节点高可用架构、弹性扩容、容灾、备份回滚、性能优化等解决方案。

云数据库MongoDB提供了多样化的安全加固功能来保障您的数据安全，其中包括但不限于：

- 网络：白名单、VPC网络、设置SSL加密等。
- 存储：设置透明数据加密TDE、自动备份、手动备份等。
- 容灾：迁移可用区、创建多可用区副本集实例、创建多可用区分片集群实例等。

2. 访问控制

云数据库MongoDB通过数据库账号密码验证和IP白名单两个方式来实现数据库访问控制，以此保障数据安全。

数据库账号

- 云数据库MongoDB在登录数据库时必须通过强制的账号及密码认证。
- 云数据库MongoDB实例创建后，会默认生产初始化root账号。您可以在创建时指定root账号密码，或在实例创建后重置root账号密码。密码设置方法请参见 [（可选）重置密码](#)。
- root账号默认拥有完整的云数据库MongoDB管理权限，您可以通过root账号登录数据库，对其他账号进行增删或授权操作。

IP白名单

云数据库MongoDB提供了IP白名单来实现网络安全访问控制，支持为每个云数据库MongoDB实例单独设置IP白名单。

默认情况下，MongoDB实例被设置为不允许任何IP访问，即127.0.0.1。您可以使用以下任意一种方法添加IP白名单。

- 通过控制台白名单设置功能添加，添加方法请参见[设置白名单](#)。
- 通过调用ModifySecurityIps接口添加，具体请参见[ModifySecurityIps](#)。

3. 网络隔离

云数据库MongoDB支持专有网络和经典网络，建议您使用专有网络，专有网络的安全性更高。

专有网络VPC

云数据库MongoDB支持使用专有网络VPC（Virtual Private Cloud）来获取更高程度的网络访问控制。使用专有网络VPC和IP白名单将极大程度提升云数据库MongoDB实例的安全性。

专有网络VPC（Virtual Private Cloud）是私有网络环境，通过底层网络协议为您构建出一个隔离的网络环境。您可以通过自定义专有网络中的路由表、IP地址和网关等解决资源冲突问题。

专有网络VPC是私有网络环境，通过底层网络协议严格地将您的网络包隔离。您可以通过VPN或专线，将自建IDC的服务器资源接入阿里云，并使用专有网络VPC自定义的MongoDB IP段来解决IP资源冲突的问题，实现自有服务器和阿里云ECS同时访问MongoDB的目的。

部署在专有网络VPC中的云数据库MongoDB实例默认只能被同一个专有网络VPC中的ECS实例访问。如果需要，您可以通过申请公网IP接受来自公网的访问（不推荐），例如来自ECS EIP的访问和自建IDC公网出口的访问。

② 说明

- 申请公网IP前，您需要设置相应白名单，白名单的设置方法请参见[设置白名单](#)。
- 公网IP的申请方法请参见 [（可选）申请公网连接地址](#)。

关于专有网络VPC的更多信息，请参见[什么是专有网络](#)。

经典网络

经典网络中的云服务在网络上不进行隔离，只能依靠云服务自身的安全组或白名单策略来阻挡非法访问。建议您选择具有更高安全性的专有网络VPC。

4.数据加密

本文介绍云数据库MongoDB提供的数据库加密功能。

SSL

云数据库MongoDB支持安全套接字协议（Secure Sockets Layer，简称SSL）。您可以使用云数据库MongoDB提供的服务器端根证书来验证目标地址和端口的数据库服务是不是云数据库MongoDB提供的，以有效避免被其他人攻击。除此之外，云数据库MongoDB还提供了服务器端SSL证书的启用和更新能力，方便您按需更新SSL证书以保障安全性和有效性。SSL的设置方法请参见[设置SSL加密](#)。

 **注意** 虽然云数据库MongoDB提供了应用到数据库之间的连接加密功能，但是SSL需要应用开启服务器端验证才能正常运转。另外SSL也会带来额外的CPU开销，MongoDB实例的吞吐量和响应时间都会受到一定程度的影响，具体影响与您的连接次数和数据传输频度有关。

TDE

云数据库MongoDB支持透明数据加密（Transparent Data Encryption，简称TDE）功能。TDE加密采用国际流行的AES算法。密钥由KMS服务加密保存，MongoDB只在启动实例和迁移实例时动态读取一次密钥，您可以自行通过KMS控制台对密钥进行更换。

当云数据库MongoDB实例开启TDE功能后，新创建的数据库或集合中的数据在写入到任何设备（例如磁盘、SSD、PCIe卡）、服务（例如对象存储OSS）前都会进行加密，因此实例中对应的数据文件和备份文件都是以密文形式存在的。TDE的设置方法请参见[设置透明数据加密TDE](#)。

5. 备份恢复

云数据库MongoDB提供自动备份功能，以保证数据的完整可靠。

备份功能

为保证数据的完整性和可靠性，数据库需要常规的自动备份来保障数据的可恢复性。

MongoDB提供如下备份功能：

- **快照备份**：保留某一时间点磁盘的数据状态。能够做到在分钟级完成数据库的恢复。
- **物理备份**：备份MongoDB实例中数据库相关的物理文件，备份速度较逻辑备份更快，且恢复速度也更快。
- **逻辑备份**：通过mongodump工具将对数据库的操作记录存储到逻辑备份文件中。恢复时通过回放命令的形式还原数据。

恢复功能

数据可恢复性是判断数据库运维可靠性的关键指标。

MongoDB提供如下恢复功能：

- **按备份点将备份数据恢复至新建实例**：从实例中的某个备份点来创建新的实例，新建的实例中的数据将恢复至选择的备份点，可用于数据恢复或数据验证场景。
- **按时间点将备份数据恢复至新建实例**：从实例运行的某个时间点创建新的实例。新建的实例数据恢复至源实例选择的时间点，可用作数据恢复或数据验证等场景。
- **恢复云数据库MongoDB单个或多个数据库**：您可以选择实例运行的某个时间点新建实例，将单个或多个数据库恢复到该时间点，适用于单个或多个数据库快速数据恢复的业务场景。
- **恢复备份数据至当前实例**：您可以选择备份文件，使用数据回滚恢复数据，数据恢复后将覆盖原有数据且无法恢复，请谨慎操作。

相关文档

根据MongoDB实例类型的不同，支持的备份恢复方式不尽相同。如需了解各MongoDB实例支持的备份恢复方式，请参见以下文档：

- [自动备份MongoDB数据](#)
- [手动备份MongoDB数据](#)
- [MongoDB数据恢复方案概览](#)

6. 实例容灾

云数据库MongoDB提供多种容灾解决方案。

多可用区实例

阿里云为全世界多个地域提供云计算服务，每个地域包含多个可用区。同一个地域中的不同可用区均为单独的故障隔离单元，并且同一地域中的可用区之间网络延迟小。

云数据库MongoDB单可用区实例运行在同一个可用区中的两台物理服务器上，可用区内机柜、空调、电路、网络都有冗余。通过异步或半同步的数据复制方式，高效的主备切换机制，云数据库MongoDB提供了高于物理服务器极限的数据库可用性。

为了提供比单可用区更高的可用性，云数据库MongoDB支持多可用区。多可用区将物理服务器部署在不同的可用区，当一个可用区出现故障时，可以将业务在短时间内切换到另一个可用区。整个切换过程中应用代码无需变更。

 **说明** 主备切换期间会产生1次30秒内的连接闪断，建议您在业务低峰期操作，并确保应用具备自动重连机制。

创建多可用区实例请参见[创建多可用区副本集实例](#)和[创建多可用区分片集群实例](#)。

迁移可用区请参见[迁移可用区](#)。

跨地域容灾实例

MongoDB多可用区实例的容灾能力局限在同地域的不同可用区之间。为了提供更高的可用性，MongoDB还支持跨地域的数据容灾。例如您可以将杭州地域的MongoDB实例A通过同步工具（例如MongoShake等）复制数据到上海地域的MongoDB实例B，实例B是一个完整独立的MongoDB实例，拥有独立的连接地址、账号和权限，可用于灾备恢复，也可用于在所在地域读取数据。

使用MongoShake复制MongoDB实例数据的方法请参见[使用MongoShake实现MongoDB副本集间的单向同步](#)。

将实例A作为主实例，实例B作为容灾实例，当实例A所在地域发生突发性故障（例如自然灾害）时，实例B可以作为主实例。通过修改应用程序中的数据库连接配置，将应用请求转到实例B上，实现跨地域的数据容灾。

-  **说明**
- 建议您在实例B上部署与实例A上相同的异地容灾应用，以避免跨地域访问造成的网络不稳定和延迟问题。
 - 实例B作为主实例后，您需要通过kill命令关闭mongoshake进程，以停止实例A到实例B的数据复制，避免造成数据错误。

7. 版本维护

云数据库MongoDB定期提供数据库软件的新版本，您可根据需要选择升级。

- 云数据库MongoDB定期提供数据库软件的新版本。
- 版本升级是非强制性的，当您主动重启MongoDB实例时，MongoDB会将被重启实例的数据库版本升级到新的兼容版本。升级方法请参见[升级数据库版本](#)或[升级数据库小版本](#)。
- 当云数据库MongoDB团队发现您的版本存在重大安全隐患时，会主动通知用户安排时间进行升级。
- 云数据库MongoDB版升级过程通常在五分钟以内完成，升级期间可能有数次数据库连接闪断。

8.服务授权

在没有您授权的情况下，阿里云的售后团队和云数据库MongoDB开发团队只能查看MongoDB实例资源、资费 and 性能相关的信息。例如，云数据库MongoDB实例的购买时间和到期时间，云数据库MongoDB的CPU、内存、存储空间的使用情况等。

- 若您需要阿里云的售后团队和云数据库MongoDB开发团队查看您实例的其它问题，您可以进行服务授权。
- 只有在获得您授权后，阿里云的售后团队和云数据库MongoDB开发团队才能在您指定时间查看和修改云数据库MongoDB实例的配置信息。例如查看云数据库MongoDB实例的IP白名单、审计日志等信息。
- 在任何情况下，阿里云的售后团队和云数据库MongoDB开发团队不会主动变更云数据库MongoDB实例的链接信息（包含连接地址和数据库账号）。