ALIBABA CLOUD

Alibaba Cloud

云原生数据仓库AnalyticDB MySQL版

数据安全

文档版本：20220630

阿里云

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.设置白名单

创建云原生数据仓库AnalyticDB MySQL版集群后，您需要为集群设置白名单，以允许外部设备访问该集群。

背景信息

- 集群默认的白名单只包含IP地址127.0.0.1，表示任何设备均无法访问该集群。您可以通过设置白名单允许其他设备访问集群，例如填写IP段10.10.10.0/24，表示10.10.10.X的IP地址都可以访问该集群。若您需要添加多个IP地址或IP段，请用英文逗号（,）隔开（逗号前后都不能有空格），例如192.168.0.1,172.16.213.9。

  > **警告** 设置白名单时，禁止输入IP：0.0.0.0。

- 若您的公网IP经常变动，需要开放所有公网IP访问AnalyticDB MySQL集群，请提交工单联系技术支持。
- 白名单可以让AnalyticDB MySQL集群得到高级别的访问安全保护，建议您定期维护白名单。
- 设置白名单不会影响AnalyticDB MySQL集群的正常运行。设置白名单后，新的白名单将于1分钟后生效。

数仓版（3.0）设置白名单

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 在**数仓版（3.0）**页签中，单击目标**集群ID**。
5. 在左侧导航栏单击**数据安全**。
6. 在**白名单设置**页面，单击**default**白名单分组右侧的**修改**。

   > **说明** 您也可以单击**创建白名单分组**创建自定义分组。

7. 在**修改白名单分组**对话框中，删除默认IP 127.0.0.1，填写需要访问该集群的IP地址或IP段，然后单击**确定**。

2.SQL审计

SQL审计功能可以实时记录数据库DML和DDL操作信息，并提供数据库操作信息的检索功能，提高云原生数据仓库AnalyticDB MySQL版的安全性。

功能

- SQL审计日志

  记录对数据库执行的所有操作。通过审计日志记录，您可以对数据库进行故障分析、行为分析、安全审计等，如需进行更详细的诊断分析，请单击**诊断与优化**。

- 搜索

  可以按照数据库、客户端IP、执行耗时、执行状态等进行多维度检索，并支持导出搜索结果。

开启SQL审计

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 进入**SQL审计**页面。
   - 当集群为数仓版（3.0）时，按照以下步骤操作。
     a. 在**数仓版（3.0）**页签中，单击目标**集群ID**。
     b. 在左侧导航栏单击**数据安全**。
     c. 在**数据安全**页面，单击**SQL审计**页签。
   - 当集群为湖仓版（3.0）时，按照以下步骤操作。
     a. 在**湖仓版（3.0）**页签中，单击目标**集群ID**。
     b. 在左侧导航栏，单击**集群管理 > SQL审计**。
5. 单击右上角**开启SQL审计**。
6. 在弹出的对话框中，选择**是**并单击**确定**。

查询和导出SQL审计日志

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 进入**SQL审计**页面。
   - 当集群为数仓版（3.0）时，按照以下步骤操作。

a. 在**数仓版（3.0）**页签中，单击目标**集群ID**。
b. 在左侧导航栏单击**数据安全**。
c. 在**数据安全**页面，单击**SQL审计**页签。

- 当集群为湖仓版（3.0）时，按照以下步骤操作。
  a. 在**湖仓版（3.0）**页签中，单击目标**集群ID**。
  b. 在左侧导航栏，单击**集群管理 > SQL审计**。

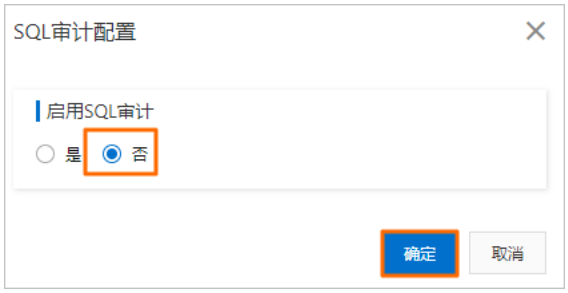
5. 在**SQL审计**页签，您可以根据SQL的**操作类型**或**执行状态**等条件查询特定时间段内的SQL审计内容。

> **说明**
> - 仅支持查询最近30天内的SQL审计内容。
> - 单次查询时间范围需要小于24小时。若需要保存当前页面内容至本地，单击**导出当前页**即可。

关闭SQL审计

> **说明** SQL审计功能关闭后，SQL审计日志会被清空。请先查询和导出SQL审计日志，再关闭SQL审计功能。具体操作，请参见查询和导出SQL审计日志。当再次打开审计日志，审计日志将从最近一次打开审计日志的时间开始展示。

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 进入**SQL审计**页面。
   - 当集群为数仓版（3.0）时，按照以下步骤操作。
     a. 在**数仓版（3.0）**页签中，单击目标**集群ID**。
     b. 在左侧导航栏单击**数据安全**。
     c. 在**数据安全**页面，单击**SQL审计**页签。
   - 当集群为湖仓版（3.0）时，按照以下步骤操作。
     a. 在**湖仓版（3.0）**页签中，单击目标**集群ID**。
     b. 在左侧导航栏，单击**集群管理 > SQL审计**。
5. 单击右上角**审计配置**。
6. 在弹出的对话框中，选择**否**并单击**确定**。



相关API

- DescribeAuditLogConfig
- ModifyAuditLogConfig
- 查询集群的SQL审计日志

3.云盘加密

您可以在创建AnalyticDB MySQL版集群时开启云盘加密功能，开启后，系统会基于块存储对整个数据盘进行加密，即使数据备份泄露也无法被解密，保护您的数据安全。

功能说明

开启云盘加密功能后，AnalyticDB MySQL版会创建一块加密云盘并将其挂载到ECS实例，并对云盘中的如下数据进行加密：

- 预留模式预留集群中的所有数据。
- 弹性模式弹性集群中的热数据。

> **说明** 弹性模式弹性集群中的冷数据不存储在云盘，因此不支持对弹性模式弹性集群中的冷数据进行加密。

- 云盘和集群间传输的数据。
- 从加密云盘创建的所有快照（即加密快照）。

注意事项

- 仅在创建AnalyticDB MySQL版集群时可以开启云盘加密，集群创建后无法开启。
- 云盘加密功能开启后无法关闭。
- 开启云盘加密后，预留模式集群中生成的快照备份，以及通过这些备份创建的预留模式集群将自动延续加密属性。
- 开启云盘加密会影响集群的读写性能。一般情况下，会造成10%左右的性能损失。
- 云盘加密对于业务访问透明，无需在应用程序上做任何修改。

计费

云盘加密功能需要使用密钥管理服务KMS（Key Management Service），使用时会涉及密钥管理费用和API调用费用。关于KMS服务费用，详情请参见KMS计费说明。

开启方式

仅支持在创建AnalyticDB MySQL版集群时可以开启云盘加密。如需开启，您需要在集群售卖页设置相关配置。

1. 在集群售卖页，选中**云盘加密**。
2. 如果是第一次使用云盘加密功能，请单击**创建服务关联角色**。

   > **说明**
   > - 仅当第一次开启云盘加密功能时需要**创建服务关联角色**。若页面提示**已创建**表示之前已创建过服务关联角色，您可以跳过该步骤直接进行下一步。
   > - 云盘加密服务需要创建相关服务关联角色SLR（Service Linked Role）授权，以使用相关密钥管理服务（KMS）功能，更多详情，请参见AnalyticDB MySQL云盘加密服务关联角色。

3. 在**密钥**下拉列表中选择目标密钥。

> **说明**
>
> - 若您的下拉列表中没有任何密钥选项，您需要先创建密钥，创建方法，请参见创建密钥。
> - AnalyticDB MySQL版的云盘加密功能仅支持由手动创建的服务密钥，您在创建普通密钥时需要将**轮转周期**设置为不开启。
> - 授权开通密钥管理服务（KMS）后，操作审计（ActionTrail）会记录您对KMS资源执行的操作。更多详情，请参见使用操作审计查询密钥管理服务的操作事件。

设置完云盘加密功能相关配置后，继续创建AnalyticDB MySQL版集群中的后续步骤完成创建集群即可。