ALIBABA CLOUD

阿里云

数据库审计

常见问题

文档版本：20201102

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.C100售前支持相关问题 05
2.C100售后支持相关问题 08
3.A100售后支持相关问题 11
4.数据库审计C100存储空间占满后处理方案 14

1.C100售前支持相关问题

本文介绍了您在使用C100系列数据库审计服务前可能遇到的问题和解答，帮助您更好地理解和使用产品。

- 购买数据库审计C100问题
- 启用数据库审计C100问题
- 登录数据库审计C100问题
- 资产配置问题
- 存储管理问题
- 数据库审计和其他产品的区别
- 购买、版本升级、迁移、退款事项处理、过期问题

购买数据库审计C100问题

- **是否支持审计线下IDC机房自己部署的数据库？**

  支持。数据库审计本身的审计能力是支持的，只需打通线下线上的网络连接即可。您可以通过阿里云高速通道打通线下线上的网络连接。

- **数据库审计C100目前支持哪些规格？**

  数据库审计C100支持以下规格。

  - 专业版3实例
  - 高级5实例
  - 高级增强版10实例
  - 企业版25实例
  - 企业版50实例
  - 旗舰版80实例

启用数据库审计C100问题

- **没有ECS是否可以启用数据库审计？**

  没有ECS可以启用数据库审计。

- **如何选择数据库审计的VPC和VSwitch？**

  选择与数据库服务器ECS相同的专有网络。启用实例后无法修改专有网络和交换机的设置。

登录数据库审计C100问题

- **如何配置数据库资产？**

  在**资产 > 资产管理**页面，单击**新增**按钮。在**新增资产**页面，完成数据库配置。详细操作指导请参见添加数据库。

- **如何快速安装Agent？**

  如果数据库服务器是安装了云助手的Linux系统ECS，可以通过云助手安装Agent；否则，需要根据数据库服务器的操作系统类型，下载相应的Agent并手动安装。

- **审计规则有什么用，能否拦截操作？**

  审计规则可以发现数据库中存在的安全风险。数据库审计是旁路设备，无法拦截数据库的操作。数据库配置审计规则后，审计记录命中规则时，会触发告警。

- **报表是否可以同步外送？**

  可以。添加订阅报表任务后，数据库审计系统会定期向指定的邮箱发送订阅的数据库审计报表。

资产配置问题

- **是否支持PolarDB集群审计？**

  不支持直接对PolarDB集群进行审计，支持对集群中的数据库进行审计。云数据库PolarDB是阿里巴巴自主研发的新一代关系型分布式云原生数据库，目前兼容三种数据库引擎：MySQL、PostgreSQL、Oracle（高度兼容Oracle语法）。数据库审计支持对这三种数据库引擎进行审计。您可以根据PolarDB的引擎类型选择数据库审计类型，完成添加和配置数据库。例如MySQL引擎选择MySQL类型，PostgreSQL引擎和Oracle引擎选择PostgreSQL类型。

- **是否支持双向审计？**

  添加数据库后，系统默认采用双向审计，且审计结果不保存；您可以在单双向审计配置中选用单向或双向审计，并设置（双向审计时）审计结果的保存数量。

- **RDS数据库应该如何部署Agent？**

  RDS数据库内暂时无法安装配置Agent。Agent程序需要部署在对应的应用服务器上，通常为访问RDS数据库的应用系统所在服务器（ECS）。

- **如何审计跨账号数据库？**

  通过阿里云高速通道，连通两个账号网络即可。

存储管理问题

- **审计记录存储在哪里？**

  审计记录存储在阿里云日志服务（Log Service，简称 SLS）中。

- **存储空间是否可以扩容？**

  支持存储扩容，可以在控制台中进行扩容。

- **存储空间满了，数据是否可以备份？**

  审计数据可以通过控制台进行备份，备份的数据存储在对象存储OSS中。

- **存储空间已经清空，为何控制台还是显示存储空间满？**

  阿里云日志服务（Log Service，简称 SLS）清除数据任务一般会有1-2小时的延迟，可以在清空存储空间两小时后确认空间是否已清空。

数据库审计和其他产品的区别

- **数据库审计产品相对于自己安装Packetbeat抓取流量审计，有什么区别和优缺点？**

  在协议的支持度和数据的分析处理上存在差别。数据库审计产品是专注于数据库协议解析的，支持的数据库协议更丰富，解析的粒度更细，还支持相应的安全规则和分析报表功能。

- **数据库审计产品相对于RDS数据库自带的SQL洞察功能，有什么区别和优缺点？**

  在协议的支持度和数据的分析处理上存在差别。数据库审计产品是专注于数据库协议解析的，支持的数据库协议更丰富，解析的粒度更细，还支持相应的安全规则和分析报表功能。

购买、版本升级、迁移、退款事项处理、过期问题

- **新购买一台数据库审计C100要注意什么？**
  - 购买时选择与ECS相同的地域，方便管理。

- 选择版本时，请参考实际数据库流量峰值大小，选择性能合适的版本。
- 购买时长大于或等于1年可享85折，若您有长期需要，建议选择包年套餐。
- 建议勾选**自动续费**，避免到期未续费导致数据库审计实例被释放，数据丢失无法找回的情况。

- **在云盾控制台看不到该数据库审计C100怎么办？**

  i. 检查产品订单是否已超过有效日期。

  > **说明** 产品过期7天后实例将被自动释放。实例释放后，数据无法恢复。

  ii. 检查产品是否有续费。

- **数据库审计C100是否可以降低规格？**

  不支持降低规格。您可以在当前产品过期后重新购买较低规格的数据库审计C100实例。

2.C100售后支持相关问题

本文介绍了您在使用C100系列数据库审计服务时可能遇到的问题和解答，帮助您更好地理解和使用产品。

- 我可以为数据库审计子账户（RAM账户）授予哪些权限？
- 通过云助手安装的Agent，安装目录是什么？
- 通过云助手安装的Agent，Agent的日志目录是什么？
- 是否支持在Docker运行的环境中安装Agent？
- 如何卸载Agent程序？
- 在选择数据库审计的版本时，需要考虑数据库类型吗？
- 已经购买数据库审计服务后，如何进行配置？
- 如何验证是否正确配置了数据库审计服务？
- 存储空间占满后如何处理？

我可以为数据库审计子账户（RAM账户）授予哪些权限？

目前数据库审计支持对RAM子账户授予以下权限：

- 为子账户添加**AliyunYundunDbAuditFullAccess**权限，授予子账户管理云盾数据库审计（DbAudit）的权限（即读写权限）。具体操作指导请参见为RAM用户授权。
- 为子账户添加**AliyunYundunDbAuditReadOnlyAccess**权限，授予子账户只读访问云盾数据库审计（DbAudit）的权限。具体操作指导请参见为RAM用户授权。

> **说明** 子账号授权覆盖的范围是针对整个数据库审计服务的读写行为进行授权，暂不支持对已经配置到数据库审计服务里面的单个数据库（包括RDS数据库和自建ECS数据库）添加子账号授权。单个数据库是否为RAM子账号授权，不影响该子账号使用数据库审计服务。

通过云助手安装的Agent，安装目录是什么？

安装目录：*/data/dbAuditAgent*。

只有安装了云助手的Linux系统ECS才能通过该方式安装Agent，Agent安装后会自动启动。

通过云助手安装的Agent，Agent的日志目录是什么？

通过云助手安装的Agent的日志目录为*/data/dbAuditAgent/log*，目录下会存在以日期命名的*log*文件。

是否支持在Docker运行的环境中安装Agent？

支持。

仅支持将Agent安装在Docker的宿主服务器上。Agent安装后，为了实现Agent和数据库审计服务的正常通信，您需要将宿主服务器的IP地址添加到Agent管理配置的白名单中。如果您的容器部署在Kubernetes集群中，每启动一个新的镜像都需要手动安装Agent。更多信息请参见部署Agent程序。

如何卸载Agent程序？

您可以通过云助手卸载已经安装的Agent。

在选择数据库审计的版本时，需要考虑数据库类型吗？

不需要。

数据库审计服务按照能够接入审计的数据库的数量划分不同的版本。在购买时，您需要根据计划接入审计的数据库的数量选择合适的版本。例如，若需要审计一个MongoDB和一个MySQL数据库，则选择**专业版3实例**版本即可。

已经购买数据库审计服务后，如何进行配置？

购买数据库审计实例后，您可以通过以下操作配置数据库审计服务：

1. 启用数据库审计实例。
2. 管理数据库审计实例。
3. 登录数据库审计系统。
4. 管理数据库。
5. 部署Agent程序。

更多信息，请参见C100快速入门。

如何验证是否正确配置了数据库审计服务？

配置完数据库审计服务后，您可以通过查看**查询分析 > 审计日志**中审计到的语句，验证配置是否正确。

如果最近5分钟审计到的语句数为0，即5分钟之内审计设备没有解析到执行数据库资产的语句，您可以通过以下步骤进行排查：

1. 确认是否是新启用的数据库审计实例。
   - 如果是新启用的数据库审计实例，请确认是否安装Agent并配置数据库资产。
     - 如果未安装Agent或配置数据库资产，请参见管理数据库和部署Agent程序。
     - 如果已安装Agent和配置数据库资产，请执行下一步骤。
   - 如果是原来已启用的数据库审计实例，请执行下一步骤。
2. 在云盾数据库审计控制台**C100**页面，查看本实例的**存储信息**，检查存储空间是否已经用完。
   - 如果存储空间已经用完，建议您进行存储扩容，操作参见管理数据库审计实例；或者将现有审计记录通过控制台的**OSS备份**进行备份，备份结束后清空存储。

     > **说明**
     > - 日志服务的存储一般会延时1小时~2小时。
     > - 如果您账号下有其他日志服务实例发生了欠费，会导致数据库审计实例的数据无法正常写入。

   - 如果存储空间还未用完，请执行下一步骤。
3. 在**设备管理 > Agent管理 > 查看Agent状态**中，查看Agent状态。
   - 如果Agent状态存在异常，请参见部署Agent程序，使用云助手重装Agent。
   - 如果Agent状态正常，请执行下一步骤。
4. 通过Agent日志排查问题。

   通过云助手安装的Agent的日志目录为*/data/dbAuditAgent/log*，目录下保存以日期命名的log文件。
5. 如果您的问题仍未解决，您可以在阿里云社区免费咨询，或提交工单联系阿里云技术支持。

存储空间占满后如何处理？

数据库审计的审计记录存储在阿里云日志服务SLS（Log Service）中，存储时长可设置为30天~185天。日志服务依据存储时间自动清理过期审计记录。存储空间占满后，您可以参考以下两种处理方案：

对存储空间进行扩容

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏，单击**C100实例**。
3. 定位到需要进行存储空间扩容的实例，单击**存储信息**模块下的**扩容**。

4. 在**变配**页面选择扩容空间的大小，可扩容空间为1 TB~20 TB。

5. 单击**去支付**。

OSS投递

日志服务支持将Logstore中的数据自动归档到对象存储服务OSS（Object Storage Service），可以发挥日志更多的效用。OSS数据支持自由设置生命周期，可以长期存储日志。

前提条件

- 已开通日志服务，创建Project和Logstore，并成功采集到日志数据。
- 已开通OSS服务，并在日志服务Project所在地域创建Bucket，请参见开通OSS服务。
- 已开通访问控制RAM。

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏，单击**C100实例**。
3. 定位到需要进行存储空间扩容的实例，单击**存储信息**区域下的**配置**。

4. 在**存储管理**页面，单击**OSS备份**。

5. 在**OSS投递管理**页面进行日志服务的OSS投递，更多信息请参见将日志服务数据投递到OSS。

> **注意**
>
> - 日志服务Project和OSS的Bucket必须位于相同Region，不支持跨Region投递数据。
> - 投递后并被清理的数据为备份数据，无法通过数据库审计直接查看。如果您需要查看已备份数据，可以将OSS中的数据导入日志分析服务，导入完成后，可查看已备份数据。导入备份数据的详细指导请参见导入OSS数据。

3.A100售后支持相关问题

本文介绍了您在使用A100系列数据库审计服务时可能遇到的问题和解答，帮助您更好地理解和使用产品。

- 我可以为数据库审计子账户（RAM账户）授予哪些权限？
- 数据库审计A100是否支持云数据库PolarDB？
- 在CentOS中删除Agent是指删除/usr/local/rmagent目录吗？
- 在Windows系统中如何删除Agent？
- 安装Agent的时候，是否需要选择本地回环？
- 是否支持在Docker运行的环境中安装Agent？
- 在选择数据库审计的版本时，需要考虑数据库类型吗？
- 已经购买数据库审计服务后，如何进行配置？
- 如何测试数据库审计网络连通性？
- 如何验证已经正确配置了数据库审计服务？
- 审计结果中出现未知用户是什么情况？
- 数据库审计服务是否支持审计通过ssh代理主机（已安装rmagent）连接的数据库？
- 数据库审计服务支持查看管理员操作日志吗？

我可以为数据库审计子账户（RAM账户）授予哪些权限？

目前数据库审计支持对RAM子账户授予以下权限：

- 为子账户添加**AliyunYundunDbAuditFullAccess**权限，授予子账户管理云盾数据库审计（DbAudit）的权限（即读写权限）。具体操作指导请参见为RAM用户授权。
- 为子账户添加**AliyunYundunDbAuditReadOnlyAccess**权限，授予子账户只读访问云盾数据库审计（DbAudit）的权限。具体操作指导请参见为RAM用户授权。

> **说明** 子账号授权覆盖的范围是针对整个数据库审计服务的读写行为进行授权，暂不支持对已经配置到数据库审计服务里面的单个数据库（包括RDS数据库和自建ECS数据库）添加子账号授权。单个数据库是否为RAM子账号授权，不影响该子账号使用数据库审计服务。

数据库审计A100是否支持云数据库PolarDB？

支持。目前A100支持云数据库PolarDB，您可以根据数据库引擎选择数据库类型进行相应配置。

在CentOS中删除Agent是指删除/usr/local/rmagent目录吗？

是的。建议您参照以下步骤，在CentOS中删除Agent：

1. 在*/usr/local/rmagent*目录下，执行`./stop_rmagent.sh`，停止Agent进程。
2. 运行`ps`命令，确认rmagent进程不存在之后，删除*/usr/local/rmagent*。

> **说明** */tmp/rmagent*目录下存放Agent的运行日志，删除Agent后，您也可以删除该目录。

在Windows系统中如何删除Agent？

打开控制面板，选择**添加和卸载程序**，定位到Agent程序后，直接将其卸载。

安装Agent的时候，是否需要选择本地回环？

不一定。是否开启本地回环取决于您的数据库和应用是否在同一台ECS上，如果是，则需要开启本地回环。

是否支持在Docker运行的环境中安装Agent？

支持。您可以通过以下两种方式安装Agent：

- **将Agent内置在镜像中**：Agent内置在镜像中，容器启动后内置的Agent会自动运行。由于Agent所在服务器的IP不固定，您需要提交工单联系阿里云技术团队协助您配置Agent。
- **将Agent安装在镜像的宿主服务器上**：将Agent安装在镜像的宿主服务器上后，为了实现Agent和数据库审计服务的正常通信，您需要将宿主服务器的IP地址添加到Agent管理配置的白名单中。更多信息请参见部署Agent程序。

在选择数据库审计的版本时，需要考虑数据库类型吗？

不需要。数据库审计服务按照能够接入审计的数据库的数量划分不同的版本。在购买时，您只需根据计划接入审计的数据库的数量选择合适的版本。例如，需要审计一个MongoDB和一个MySQL数据库时，选择专业版3实例版本即可。

已经购买数据库审计服务后，如何进行配置？

购买数据库审计实例后，您可以通过以下操作配置数据库审计服务：

1. 启用数据库审计实例。
2. 管理数据库审计实例。
3. 登录数据库审计系统。
4. 添加数据库实例。
5. 部署Agent程序。

更多信息，请参见A100快速入门。

如何测试数据库审计网络连通性？

数据库审计外网和内网均禁止使用Ping IP地址的方式来测试网络连通性。如果需要测试数据库审计网络连通性，建议您通过telnet数据库审计外网IP地址的9266端口进行测试。

如何验证已经正确配置了数据库审计服务？

配置完数据库审计服务后，您可以通过查看系统审计到的语句，验证配置是否正确。

如果查看到的语句数量是0，您可以查看Agent程序的日志，排查配置问题。

Agent程序的日志一般存放在以下目录：

- Windows：*C:\tcmp\rmagent\rmagent_info.log*
- Linux：*/tmp/rmagent/rmagent_info.log*

如果在Agent程序的日志中出现以下信息，表示Agent程序未能正确连接到数据库审计系统：`xml[INFO][tid=31235]20170322114351 rmagent.cpp:912:Rma_ConnectServer connect <审计系统IP地址>:9266 failed, Connection timed out`

解决方案：

- 检查该日志中连接超时的IP是否为控制台上查询到的数据库审计系统的IP。如不是，请将*rmagent.in*配置文件中的IP地址修改为审计系统的IP地址。

- 检查该数据库审计实例所在的安全组是否放开了内网入方向的9266端口。Agent程序与数据库审计系统通过9266端口进行通讯，请确保在相关的安全组中放行该端口。

审计结果中出现未知用户是什么情况？

在刚启用审计时，如果存在未断开的会话，那么审计到的都是未知用户。过一段时间再审计时，审计到的语句中就会出现用户信息。

如果您需要马上就有用户信息，请让应用和数据库先断开连接，再重新连接即可。

数据库审计服务是否支持审计通过ssh代理主机（已安装rmagent）连接的数据库？

支持，但前提条件是代理主机与数据库连接的方式是非SSL加密的方式。

数据库审计服务支持查看管理员操作日志吗？

可以。您必须先开启系统管理员和系统审计员角色，然后使用sysauditor账号登录，就可以查看管理员操作日志。

4.数据库审计C100存储空间占满后处理方案

数据库审计C100的审计记录存储在阿里云日志服务（Log Service，简称 SLS）中。存储时长可设置为30-185天，日志服务依据存储时间自动清理过期审计记录。本文档介绍存储空间占满后您可以采取的两种处理方案。

对存储空间进行扩容

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏单击**C100实例**。
3. 定位到需要进行存储空间扩容的实例，单击**存储信息**模块下的**扩容**。

4. 在**变配**页面选择扩容空间的大小，可扩容空间为1T-20T。

5. 单击**去支付**。

OSS投递

日志服务支持将Logstore中的数据自动归档到对象存储服务（Object Storage Service，简称OSS），可以发挥日志更多的效用。OSS数据支持自由设置生命周期，可以长期存储日志。

前提条件

- 已开通日志服务，创建Project和Logstore，并成功采集到日志数据。
- 已开通OSS服务，并在日志服务Project所在地域创建Bucket，请参见开通OSS服务。
- 已开通访问控制RAM。

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏单击**C100实例**。
3. 定位到需要进行存储空间扩容的实例，单击**存储信息**模块下的**配置**。

4. 在存储管理页面单击**OSS备份**。

5. 在**OSS投递管理**页面进行日志服务的OSS投递。更多信息请参见将日志服务数据投递到OSS。

> **注意**
>
> - 日志服务Project和OSS的Bucket必须位于相同Region，不支持跨Region投递数据。
> - 投递后并被清理的数据为备份数据，无法通过数据库审计直接查看。如果您需要查看已备份数据，可以将OSS中的数据导入日志分析服务，导入完成后，可查看已备份数据。导入备份数据的详细指导请参见导入OSS数据。