ALIBABA CLOUD

阿里云

Quick BI

通用场景实践

文档版本：20211221

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.行业场景

1.1. 互联网、电商及游戏行业实时BI分析

本文介绍互联网、电商及游戏行业实时BI分析的场景描述、解决问题、架构图及操作参考链接。

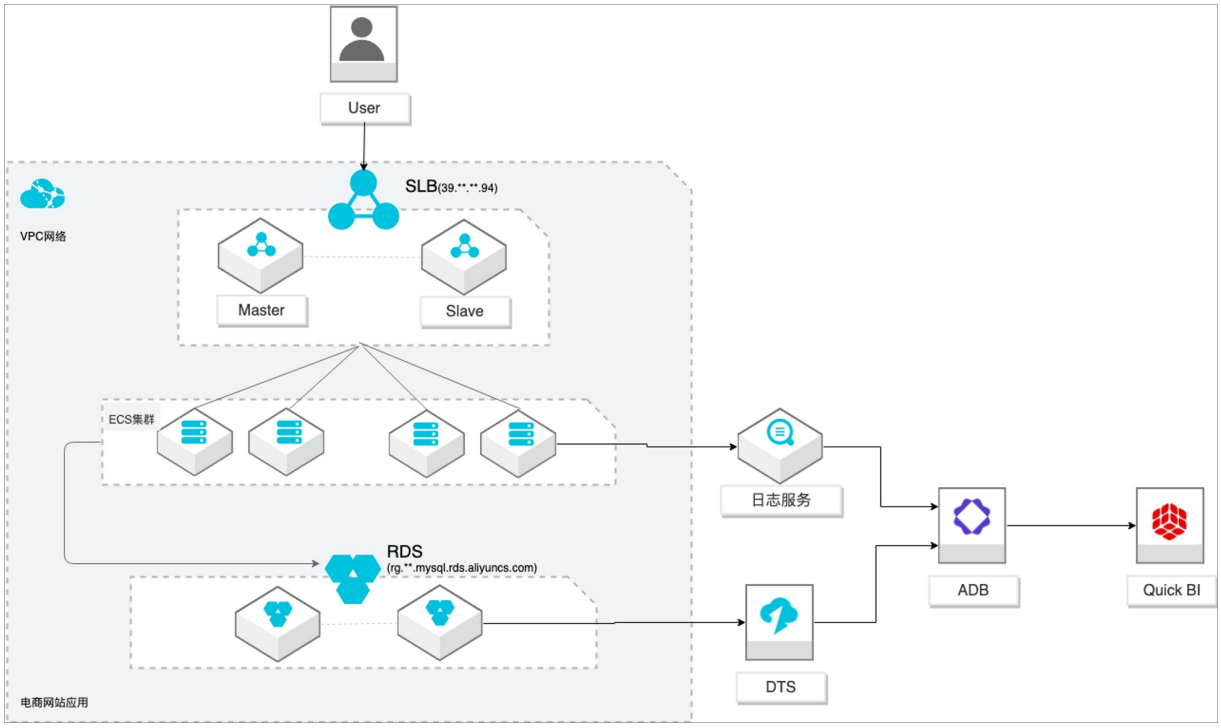
场景描述

本文以电商行业为例，将业务数据和日志数据同步到AnalyticDB，并通过Quick BI实时可视化分析数据。相对于传统的关系型数据库，阿里云分析型数据库MySQL版只需要几毫秒的时间，即可查询PB级数据并从中找到匹配信息。

解决问题

- 互联网行业、电商、游戏行业等网站、App、小程序应用内BI分析场景。
- 在线运营和运营指标实时化分析等场景。
- 扩展到各类网站BI分析场景。

架构图



参考链接

有关互联网、电商及游戏行业实时BI分析的详情，请参见互联网、电商及游戏行业实时BI分析最佳实践。

1.2. 游戏运营融合分析

本文介绍游戏运营融合分析的场景描述、解决问题、架构图及操作参考链接。

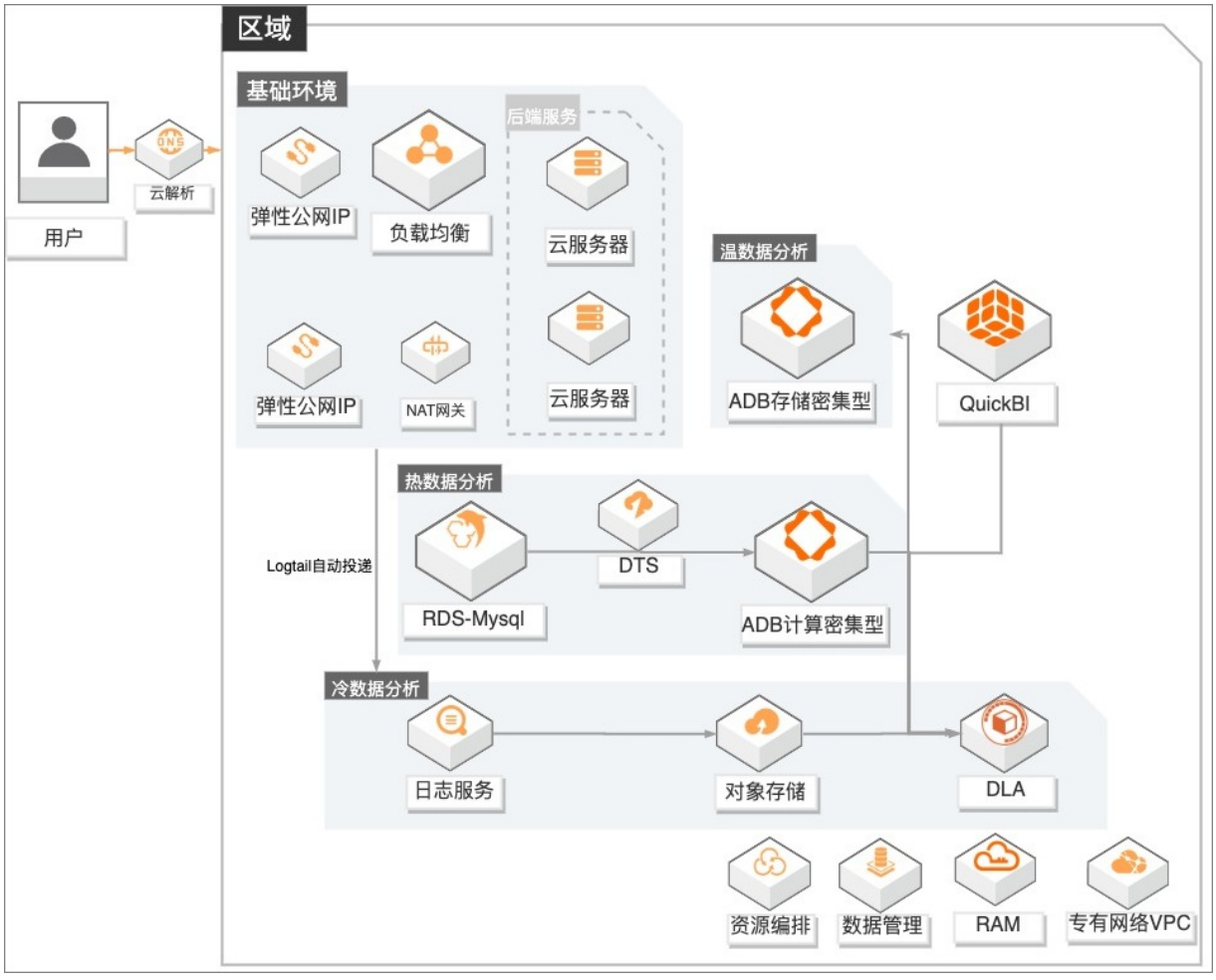
场景描述

- 游戏行业有结构化和非结构化数据融合分析需求的客户。
- 游戏行业有数据实时分析需求的客户，无法接受T+1延迟。
- 对数据成本有一定诉求的客户，希望物尽其用尽量优化成本。
- 其他行业有类似需求的客户。

解决问题

- 秒级实时分析：依托AnalyticDB（简称ADB）计算密集型实例，秒级监控DAU等数据，为广告投放效果提供有力的在线决策支撑。
- 高效数据融合分析：打通结构化和非结构化数据，支撑产品体验分析；广告买量投放效果实时（分钟级）分析，渠道的评估更准确。
- 降低使用成本：DLA融合冷数据分析+ADB存储密集型温数据分析+ADB计算密集型热数据分析，在满足各种分析场景需求的同时，有效地降低客户的总体使用成本。
- 学习成本低：Data Lake Analytics（简称DLA）和ADB兼容标准SQL语法，无需额外学习其他技术。

架构图



产品列表

- 专有网络VPC、负载均衡SLB、NAT网关、弹性公网IP
- 云服务器ECS、日志服务SLS、对象存储OSS
- 数据库RDS MySQL、数据传输服务DTS、数据管理DMS

- 分析型数据库MySQL版ADB
- 数据湖分析DLA、Quick BI

参考链接

有关游戏运营融合分析的详情，请参见游戏数据运营融合分析最佳实践。

2.功能场景

2.1. 配置全局参数实现不同用户订阅不同数据

本教程通过配置仪表板全局参数的方式，使得同一份报表不同用户订阅时，可以查看到不同的数据。

背景信息

假设您是一家大型全国连锁店的数据分析师，在一个报表中分析每个城市的销售量和利润金额，您需要发送该报表给区域经理，确保这些人只能查看自己管辖城市的销售量和利润金额。本教程以company_sales_record数据集为例。如果您想了解如何创建数据集，请参见创建并管理数据集。

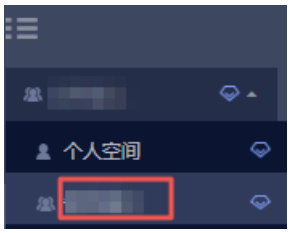
仅高级版和专业版群空间支持该功能。

创建仪表板

请在已有该数据集的工作空间创建仪表板。如果工作空间上没有该数据集，则需要在工作空间中新创建一个数据集。

1. 登录Quick BI控制台。
2. 在Quick BI首页，单击顶部菜单栏的**工作空间**，选择一个群空间。

   请在已有company_sales_record数据集的工作空间创建仪表板。



3. 在左侧导航栏单击**仪表板**。
4. 在仪表板管理页面，单击**新建仪表板 > 常规模式**。

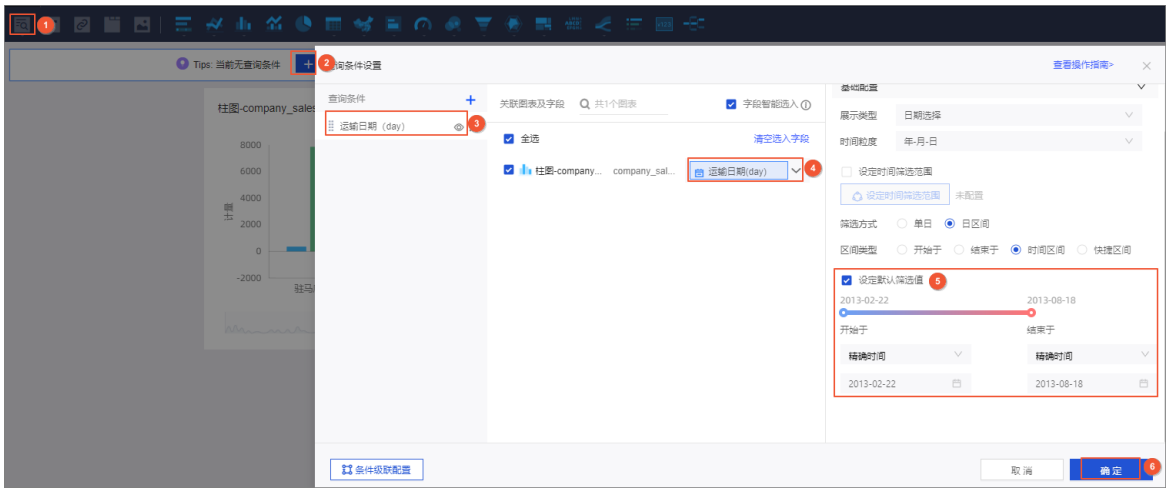
   本教程以创建柱图为例介绍。

5. 在仪表板编辑页面，单击图标。
6. 请参考下图配置柱图。

   请参见柱图。

7. 添加并配置查询控件。

请参见新建查询控件。

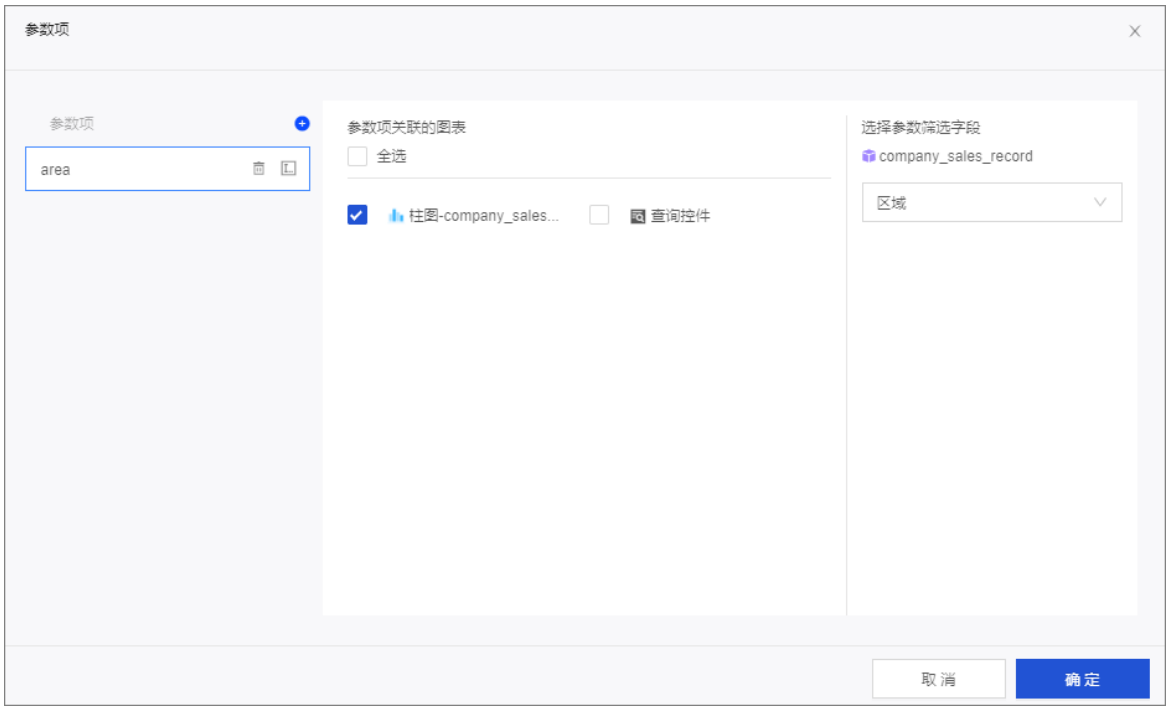


8. 保存该仪表板并命名为**邮件推送测试**。

配置全局参数

本教程以设置全局参数area为例介绍。

1. 在仪表板编辑页面，单击顶部菜单栏的图标。
2. 在**页面设置**的**全局参数**区域，单击图标。
3. 在**参数项**页面，设置**参数项**为area、**参数项关联的图表**为**柱图**、**选择参数筛选字段**为**区域**，单击**确定**。



设置订阅任务

设置订阅任务前，请确保最新的仪表板已保存并发布。

本教程中，您可以在设置订阅任务时，报表均选择**邮件推送测试**，配置不同的参数值，并发送给不同订阅者。实现同一份报表不同的订阅者可以查看不同的内容。

1. 绑定接收订阅邮件的邮箱地址。
   i. 在Quick BI首页，将鼠标悬浮至个人中心，在弹出的页面中选择**个人设置**。

   ii. 在**个人设置**页面的**个人设置**页签中，输入**邮箱**和**手机号**，单击**确定**。
2. 创建订阅任务。
   i. 在Quick BI首页，单击顶部菜单栏的**订阅**。
   ii. 在**订阅管理**页面，单击**新建**。

   iii. 在**新建订阅**页面，配置参数后，单击**保存**。

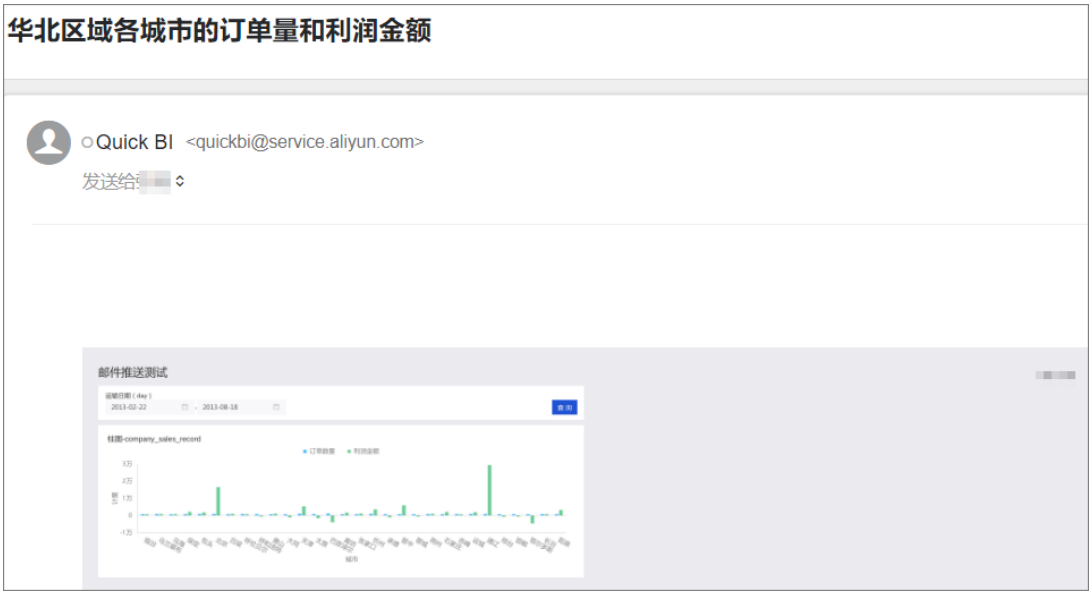
   本示例中，邮件内容设置如下。

同样地，您可以参考步骤2，重新设置订阅内容中的参数值，并修改接收人。

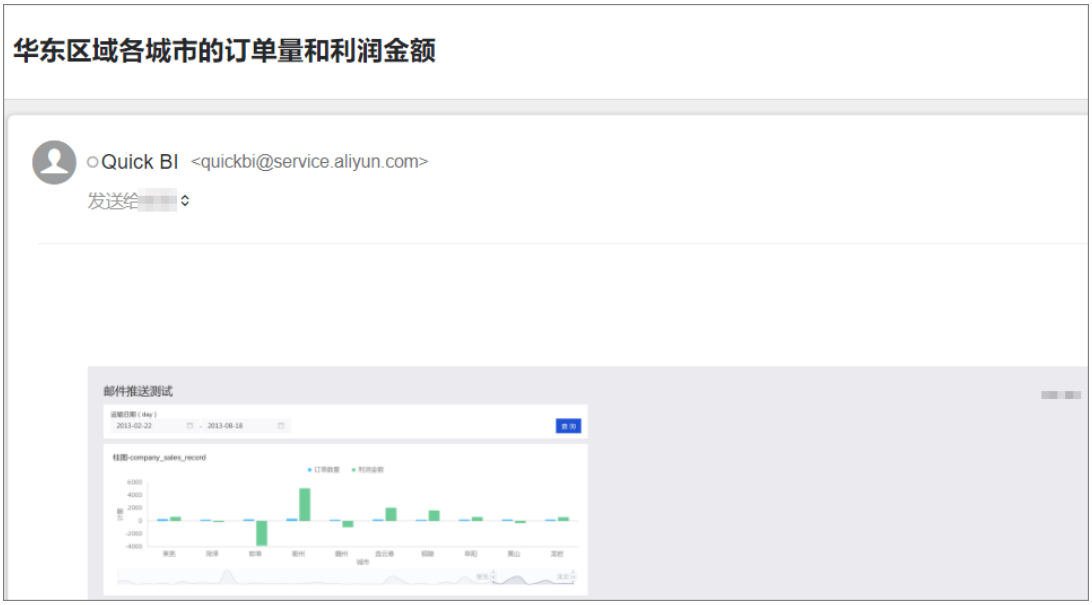
查看订阅任务

订阅者绑定的邮箱中，可以定期接收到如下图中报表邮件。

华北区域个城市的订单量和利润金额



华东区域个城市的订单量和利润金额



> **说明** 在邮件正文中单击图片可以清晰地看到各城市的订单量和利润金额。

2.2. 如何在报表中展示图片？

目标数据集中存在图片字段时，Quick BI支持在数据集中切换图片类型字段，并在制作仪表板时，将图片字段展示在报表中。

前提条件

- 您已连接数据源，请参见连接阿里云MySQL数据源。
- 您已创建数据集，且目标数据集中存在图片字段，请参见创建并管理数据集。

  图片字段的存储方式默认为图片链接URL，本例中，目标数据集为company_sales_record_img。

使用限制

仅当字段类型为图片（商品图片）时，支持在交叉表、排行榜、指标看板展示图片字段。

进入维度编辑页面

1. 登录Quick BI控制台。
2. 单击**工作空间 > 数据集**。
3. 在**数据集**管理页面，单击目标数据集company_sales_record_img名称。

   您也可以单击目标数据集所在行的图标，进入数据集编辑页面。

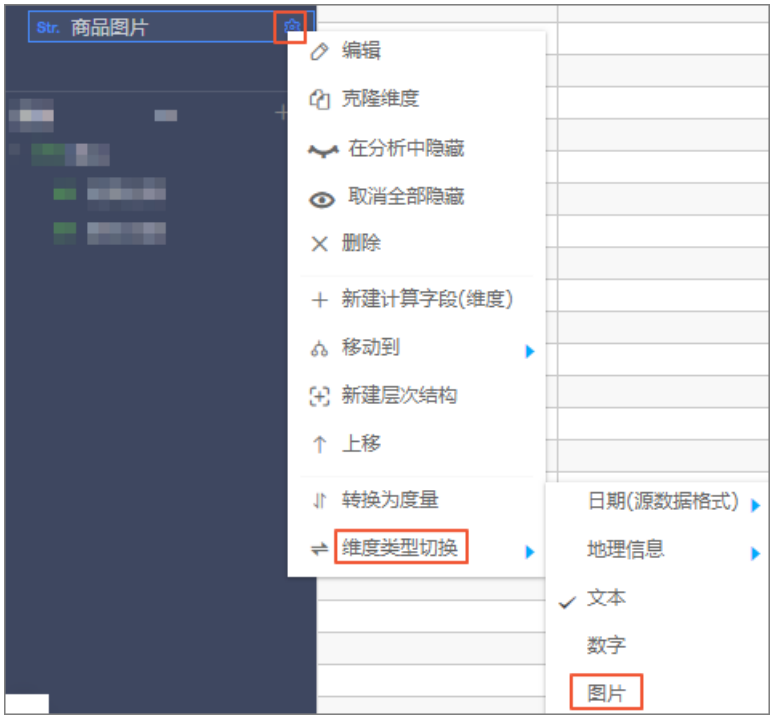
切换图片字段类型

图片字段的存储方式为图片链接URL，下面为您介绍如何将图片链接URL切换为图片类型。

> **说明** 如果图片维度的标识商品图片为红框显示时，则表示该字段已切换为图片，请跳过此步骤。

1. 在数据集编辑页面的维度列表中，找到目标字段并单击右侧的图标。
2. 选择**维度类型切换 > 图片**。

   本例中，目标字段为**商品图片**。



3. 数据集编辑完成后，单击**保存**。

4. 单击**刷新预览**。

   系统会自动将数据显示在表格中。

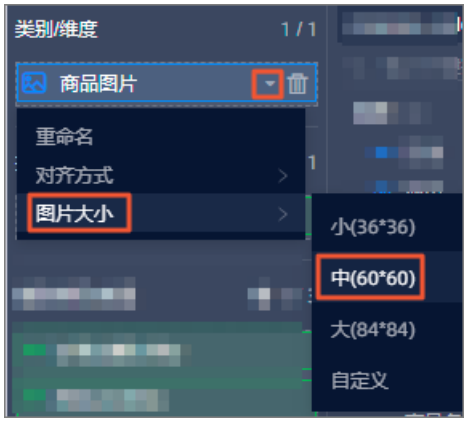
图片维度在交叉表中的应用

1. 请参见新建仪表板，进入仪表板编辑页面。
2. 单击图标。
3. 在**数据**标签页，选择需要的维度字段和度量字段：
   - 在**维度**列表中，找到**省份**和**商品图片**，依次双击或拖拽至**行**区域。

     > **说明** 请确保商品图片已切换为图片字段类型（商品图片）。

   - 在**度量**列表中，找到**订单数量**、**运输成本**和**利润金额**，依次双击或拖拽至**列**区域。
4. 单击**更新**，系统自动更新图表。

您可以单击**商品图片**右侧的图标，调整图片的大小。



交叉表更多配置操作，请参见新交叉表。

图片维度在指标看板中的应用

1. 请参见新建仪表板，进入仪表板编辑页面。
2. 单击图标。
3. 在**数据**标签页，选择需要的维度字段和度量字段：
   - 在**维度**列表中，找到产品小类，双击或拖动至**看板标签/维度**区域。
   - 在**度量**列表中，找到订单数量、订单金额和利润金额，依次双击或拖动至**看板指标/度量**区域。
4. 单击**更新**，系统自动更新图表。

   此时，图表上默认显示主指标修饰图，且**图片类型**为**静态图片**。

5. 在**图表设计**页面单击**样式**页签，在**指标块样式配置**区域，修改**图片类型**为**图片字段**，并选择**图片字段**为**商品图片**。

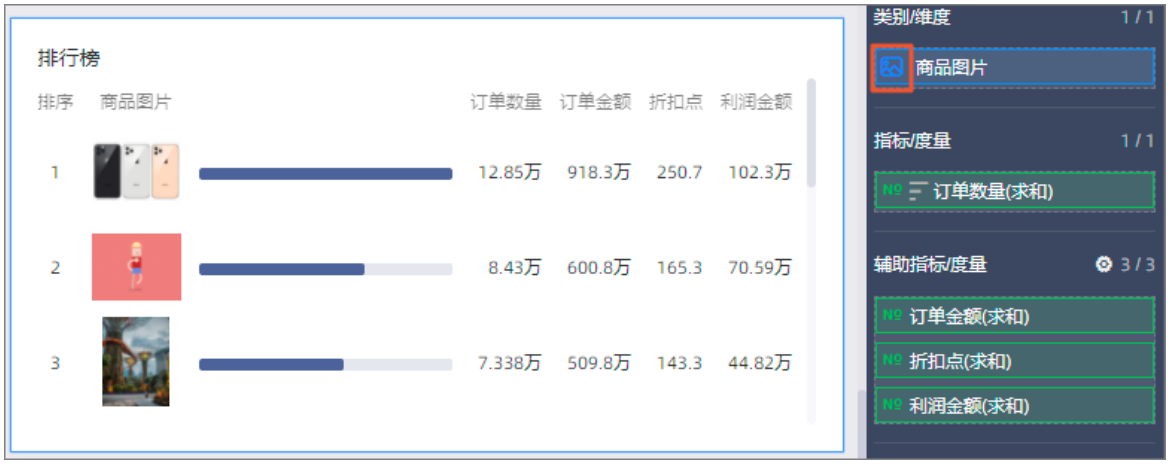
指标看板更多配置操作，请参见指标看板。

图片维度在排行榜中的应用

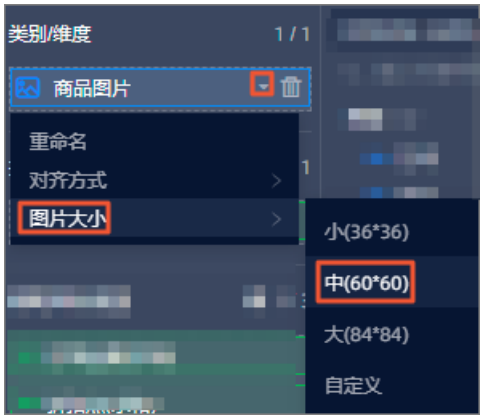
1. 请参见新建仪表板，进入仪表板编辑页面。
2. 单击图标。
3. 在**数据**标签页，选择需要的维度字段和度量字段：
   - 在**维度**列表中，找到**商品图片**，双击或拖动至**类别/维度**区域。

     > **说明** 请确保商品图片已切换为图片字段类型（商品图片）。

   - 在**度量**列表中，找到**订单数量**，双击或拖动至**指标/度量**区域。
   - 在**度量**列表中，找到**订单金额**、**折扣点**和**利润金额**，依次拖动至**辅助指标/度量**区域。
4. 单击**更新**，系统自动更新图表。



您可以单击**商品图片**右侧的图标，调整图片的大小。



排行榜更多配置操作，请参见排行榜。

2.3. 如何实现一份报表，不同的人看不同的数据

在报表的使用过程中，用户经常有这样的需求：以一个销售团队为例，如果该销售团队的业务范围是全国，那么意味着该销售团队需要随时掌握30多个省的销售情况，而且每一个省还有若干个城市，每一个城市还有若干个县；随着业务量的不断增大和扩容，该销售团队所要查阅的销售数据也会日益增加。在如此庞大且复杂的数据中，如果能够实现每一个区域的负责人只看到自己负责的那份数据，那么既可以提高相关责任人的工作效率，又可以避免泄露敏感的商业数据。

Quick BI的行级权限功能就可以实现在一份报表中，不同的人看不同的数据。本章节以*company_sales_record*数据集为例介绍此功能。如果您想了解如何创建数据集，请参见创建数据集。

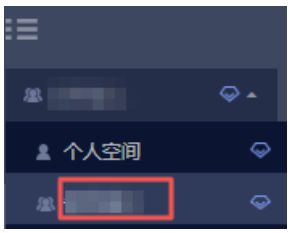
> **说明** 目前只有高级版和专业版的群空间下，有行级权限的功能。如果您想申请开通高级版和专业版，请参见Quick BI购买、升级和续费。

设置行级权限

行级权限的控制需要在工作空间中的数据集上进行。

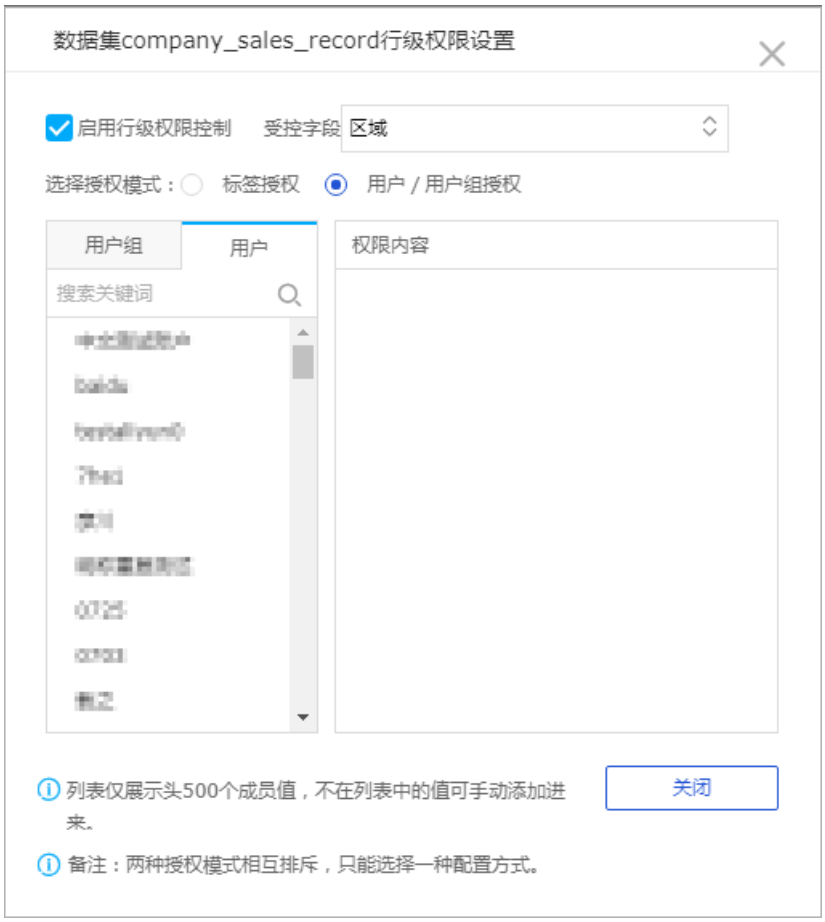
请在已制作仪表板的数据集上设置行级权限。如果工作空间上没有该数据集，那么您需要在工作空间中新创建一个数据集。

1. 登录Quick BI控制台。
2. 单击**工作空间**标签页，选择一个群空间，如下图所示。



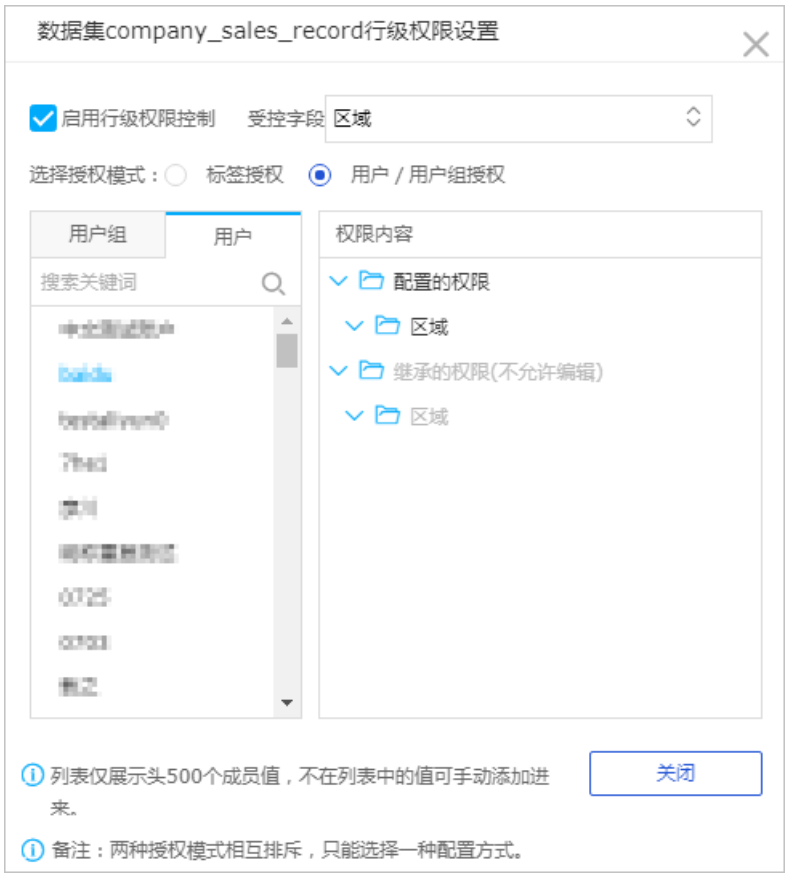
3. 单击**数据集**，进入工作空间的数据集管理页面。
4. 在待设置权限的数据集所在行，单击 图标或鼠标右键，选择**行级权限**，如下图所示。

5. 勾选**启用行级权限控制**，选择**用户/用户组授权**。
6. 单击下拉箭头，选择一个受控字段，例如，区域，如下图所示。



7. 继续在列表中选择需要受控的对象。

对象选择完成后，受控字段会自动列在**权限内容**区域中，如下图所示。



8. 单击**区域**，打开区域字段包含的全部信息。
9. 选择一个区域名称，例如，东北，然后单击**添加**。

   添加完成后，该成员就只能看到报表中，东北的销售数据。

   > **说明** 某个数据集上哪怕只要有一个字段要进行行级权限控制，就需要为组织中所有的成员在该数据集的受控字段上指定其有权限访问的字段成员列表，如果不指定，则默认该成员访问该数据集生成的任何报表都将无数据可阅览。

10. 单击**确定**，完成行级权限控制。

验证行级权限

1. 单击**工作空间**标签页，选择一个群空间。
2. 单击**仪表板**，进入仪表板管理页面。
3. 找到需要分享的仪表板，单击后面的**分享**图标。
4. 输入被分享人的账号，并选择一个分享截止日期。

   > **说明** 被分享人的账号必须在群空间下设置好了行级权限，否则将无法验证效果。

5. 单击**确定**，完成报表分享。

如果被分享人被设置了行级权限，那么被分享人就只能看到被授权的数据，而其它数据将无法阅览。

2.4. 在电子表格中实现数据过滤

在电子表格中根据具体需求设定过滤条件，筛选出需要的数据。

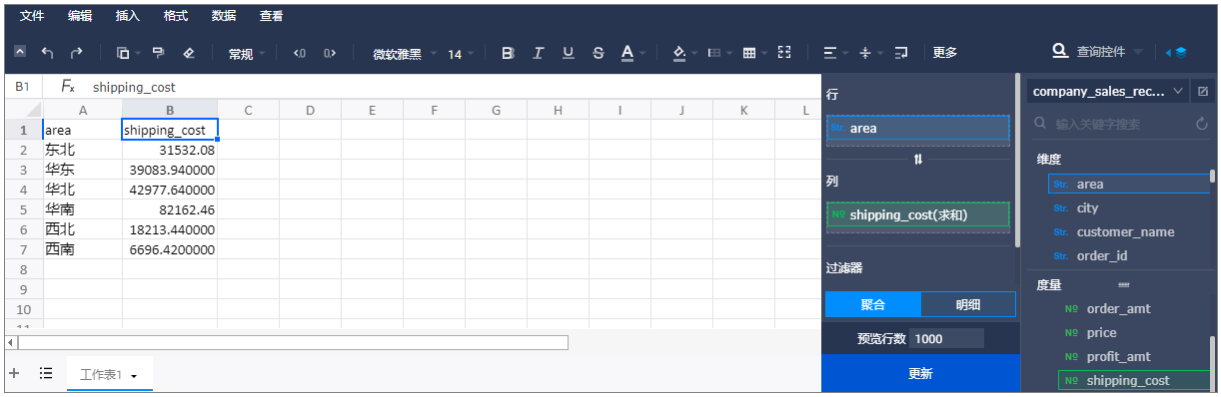
场景示例：比较华东、华南和华北三个地区的运输成本。本示例以company_sales_record数据集为例。

前提条件

您已上传相关

准备电子表格

基于company_sales_record数据集创建如下电子表格，命名为**运输成本** 。如果您没有本示例中的数据集，请上传销售样例数据至数据库并创建数据集，详细信息请参见创建并管理数据集。有关电子表格的基本操作请参见电子表格概述和创建电子表格。



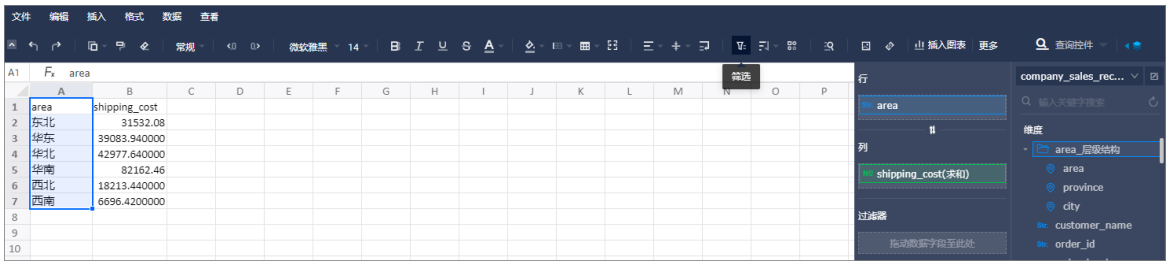
过滤

筛选是表格的一个属性功能，通过此功能可以实现对表格中数据的筛选。

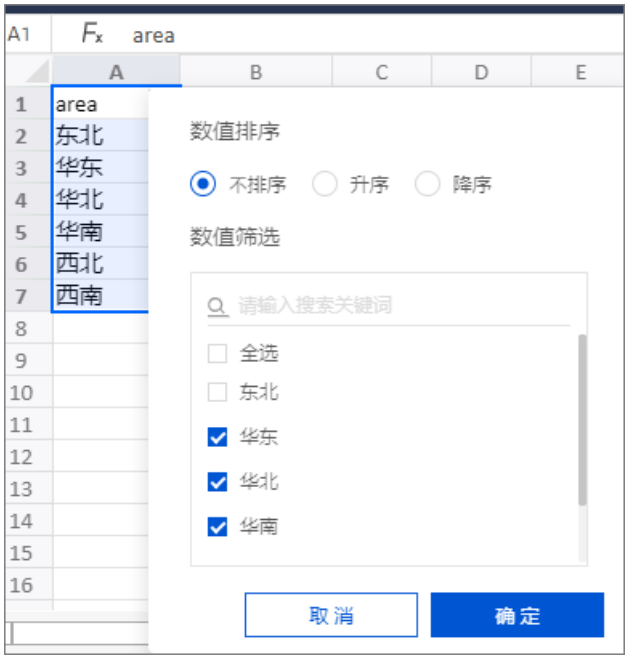
1. 在电子表格**运输成本**中，选中**区域**所在列或所在列的所有数据。

   > **说明** 一定要选中**区域**所在列或所在列的所有数据，否则可能会出现筛选项不全的问题。

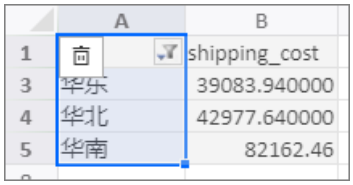
2. 单击筛选图标，选择**筛选**，如下图所示。



3. 单击**区域**的筛选按钮，选择**华东**、**华南**、**华北**三个区域并单击**确定**。



筛选结果如下图所示。

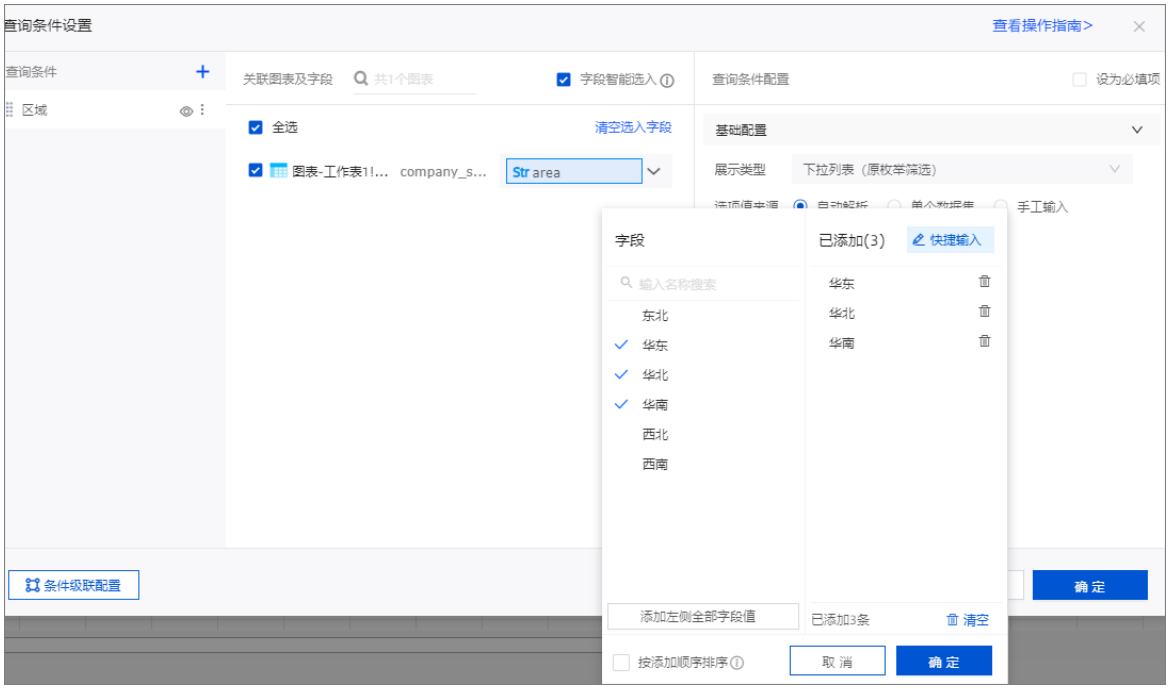


查询组件

查询组件功能可以为数据添加查询条件，从而实现对数据的筛选。

1. 在电子表格**运输成本**中，单击**查询控件**。
2. 单击图标。

3. 在查询条件设置页面，进行以下配置。



i. 在**查询条件**区域，自定义查询条件名称为*区域*。

ii. 在**关联图表及字段**区域，选中目标电子表格并指定关联字段area。

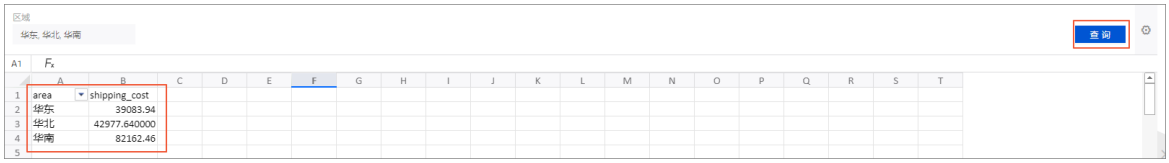
iii. 在查询条件配置页面。

- 展示类型为**下拉列表（原枚举筛选）**。
- 选项值来源为**自动解析**。
- 查询方式为**多选**。
- 选中**设定筛选默认值**，并设置默认值为**华东**、**华南**、**华北**。

iv. 单击**确定**。

4. 配置完成后，单击**确定**。

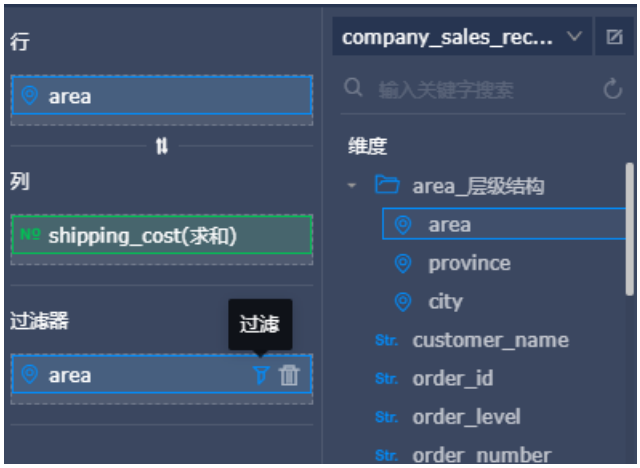
5. 单击**查询**，筛选结果如下图所示。



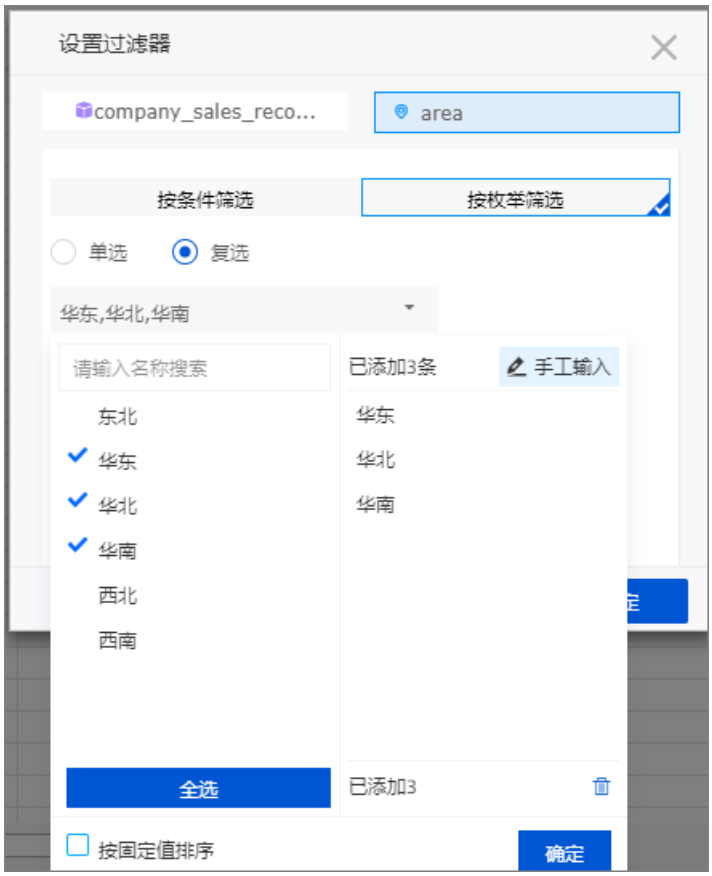
过滤器

在电子表格创建中可以通过**过滤器**功能来实现对数据的过滤筛选。

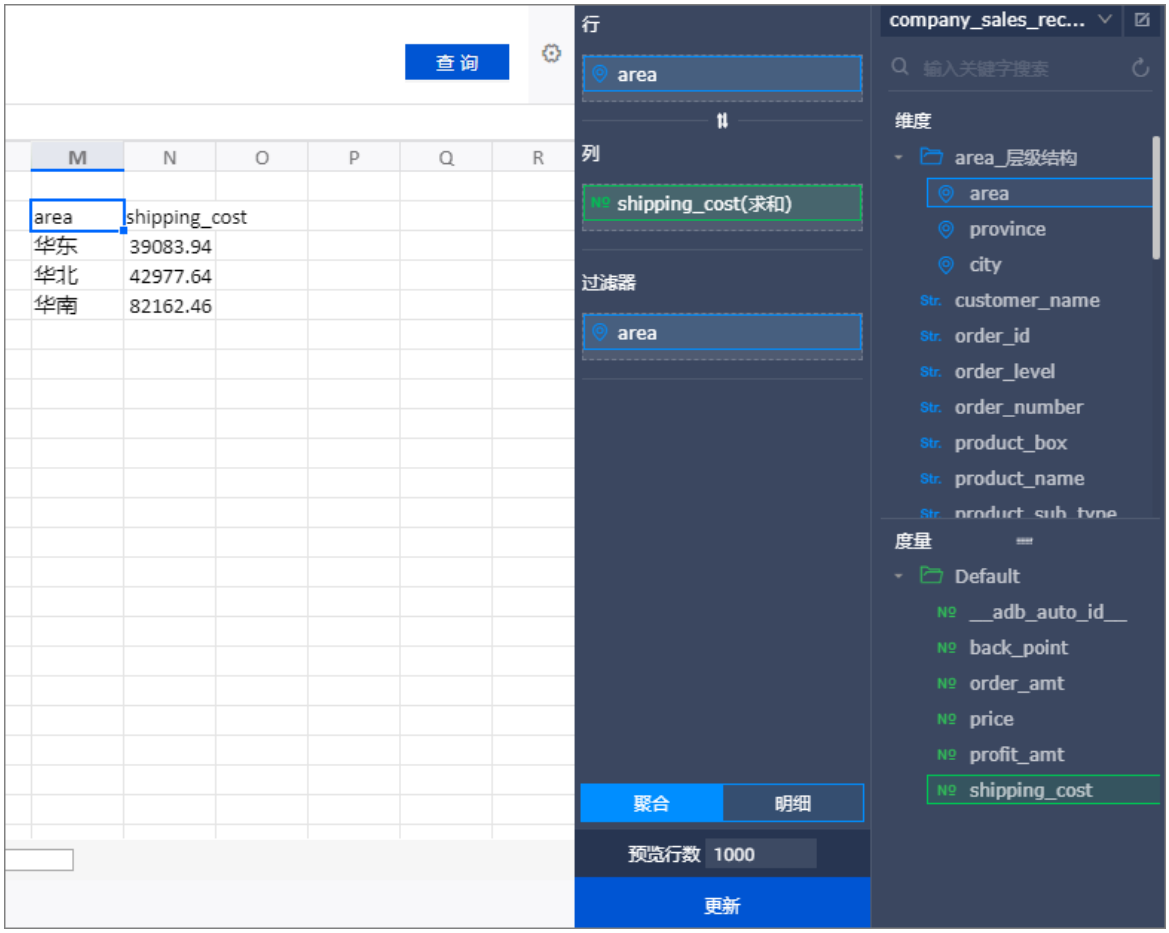
1. 在制作电子表格过程中，将**区域**字段添加至**过滤器**区域并单击过滤器设置图标。



2. 在**设置过滤器**页面，进行如下图中设置，并单击**确定 > 确定**。



3. 单击**更新**，过滤结果如下图所示。



2.5. 如何利用查询条件实现日期查询

查询条件控件可以实现日期查询。您可以根据自己设定的日期查询需要的数据。本章节以company_sales_record数据集为例。

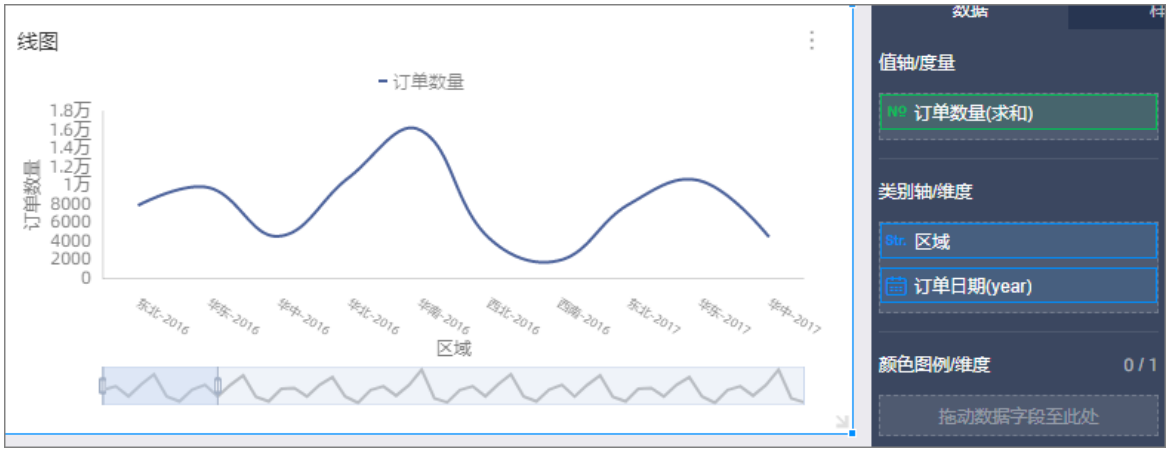
创建数据集

1. 登录Quick BI控制台。
2. 单击**工作空间 > 数据源** 。
3. 在数据源管理页面，找到并单击图标，创建数据集。

   请参见创建并管理数据集

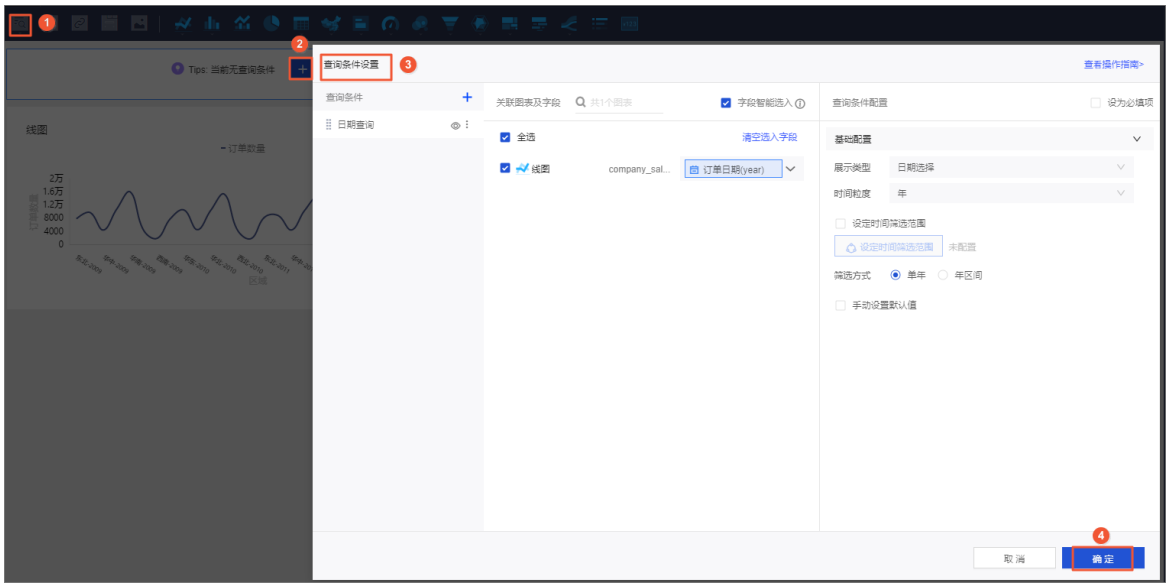
新建仪表板

1. 在数据集管理页面，找到目标数据集并单击**操作**列的 图标。
2. 在**新建仪表板**页面指定仪表板类型后，单击**确定**。
3. 在仪表板管理页面单击数据集 company_sales_record... 图标，选择company_sales_record数据集。
4. 创建如下图表并保存仪表板。

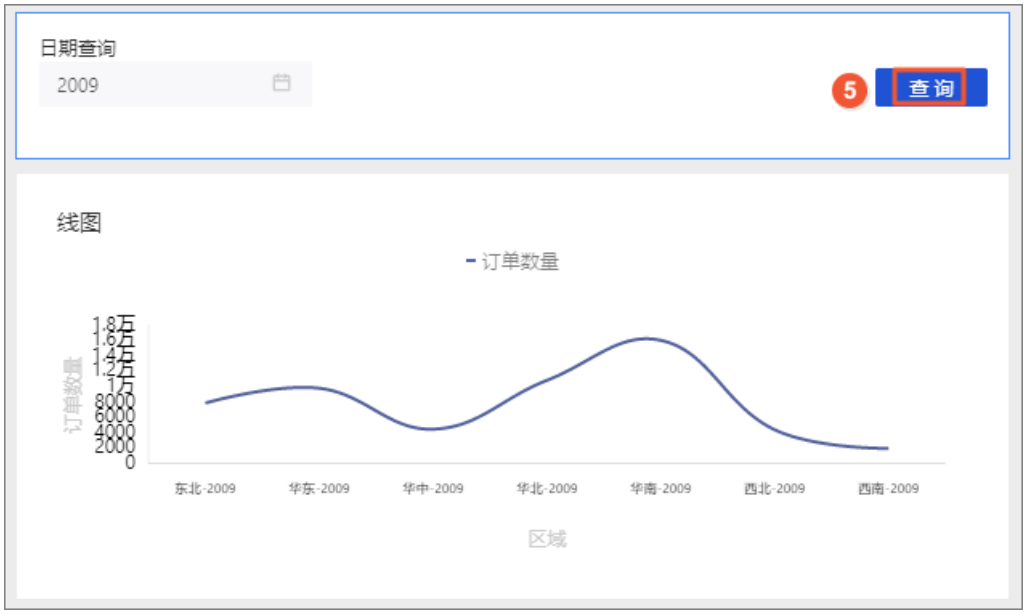


实现日期查询

1. 在顶部菜单栏单击图标。
2. 在添加的查询控件中单击图标。
3. 在**查询条件设置**页面，设置查询条件名称、关联图表及字段、查询条件配置，详情请参见日期查询。
4. 单击**确定**完成设置。



5. 在仪表板中选择查询日期并单击**查询**，系统会根据设置的条件更新图表。



2.6. 如何在仪表板中使用过滤器

在仪表板中，过滤器可以实现数据的过滤，让报表的内容更精确。您可以根据自己设定的过滤范围筛选需要的数据。

场景示例：以company_sales_record数据集为例比较华东、华南和华北三个地区的运输成本。

创建数据集

1. 登录Quick BI控制台。
2. 单击**工作空间 > 数据源**，进入数据源管理页面。
3. 单击**新建数据源**，选择数据源来源。
4. 单击**创建数据集**图标。

   请参见创建数据集。

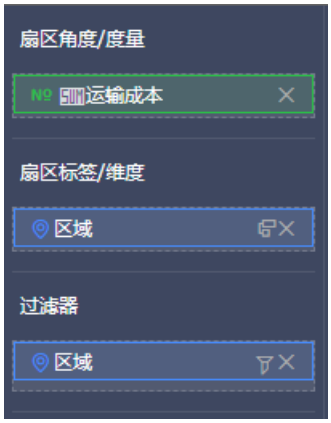
新建仪表板

1. 单击**仪表板**，进入仪表板管理页面。
2. 单击数据集切换图标，选择**company_sales_record**数据集。
3. 选择一个数据图表，例如饼图。
4. 选择需要的字段，如下图所示：

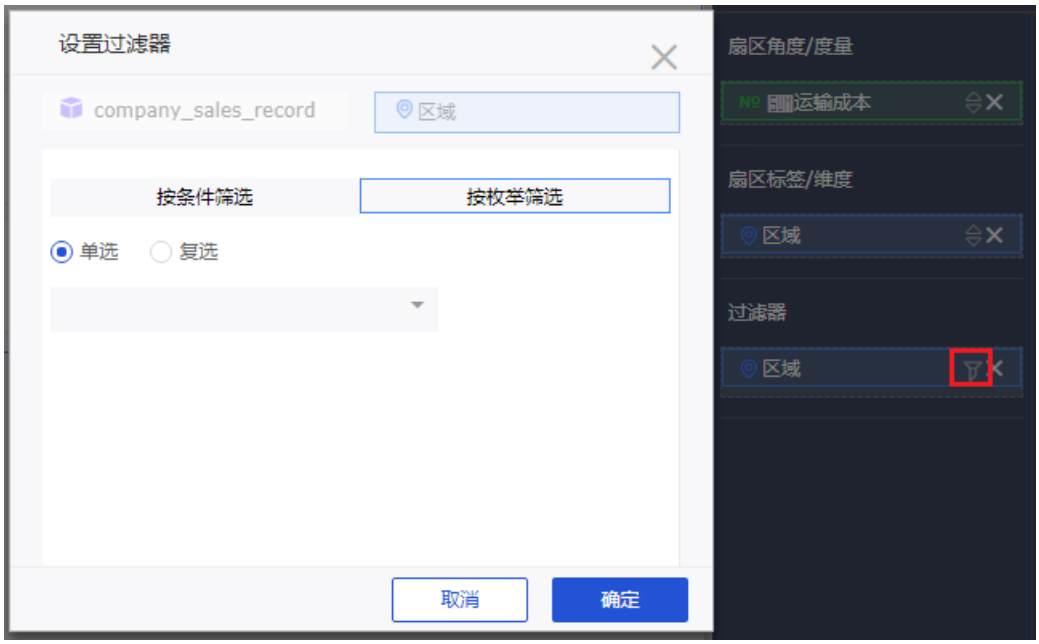
5. 单击**更新**，系统自动绘制图表。

实现数据过滤

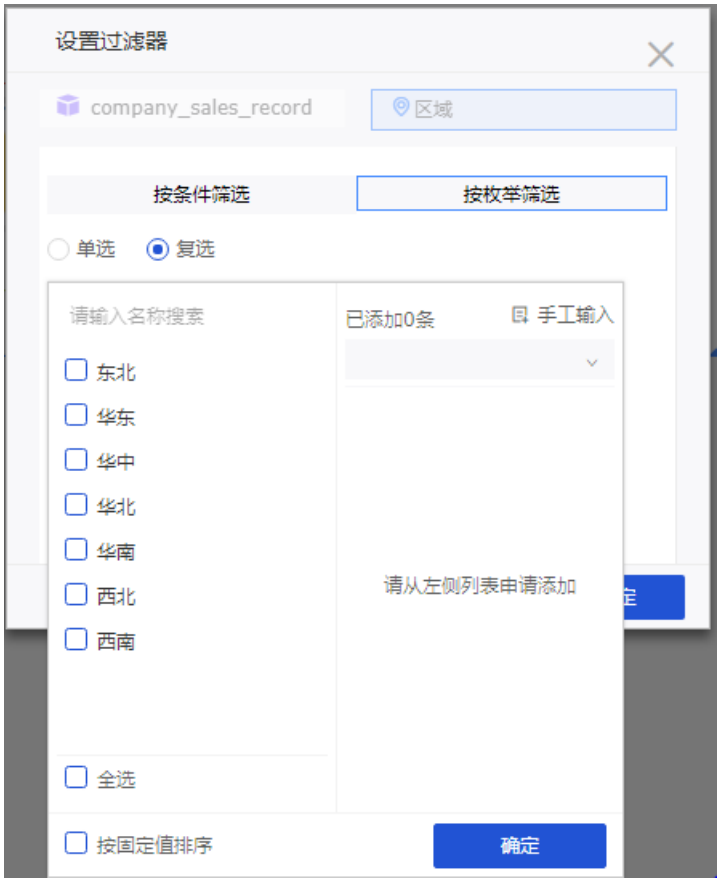
1. 将**区域**字段拖拽至**过滤器**区域，如下图所示：



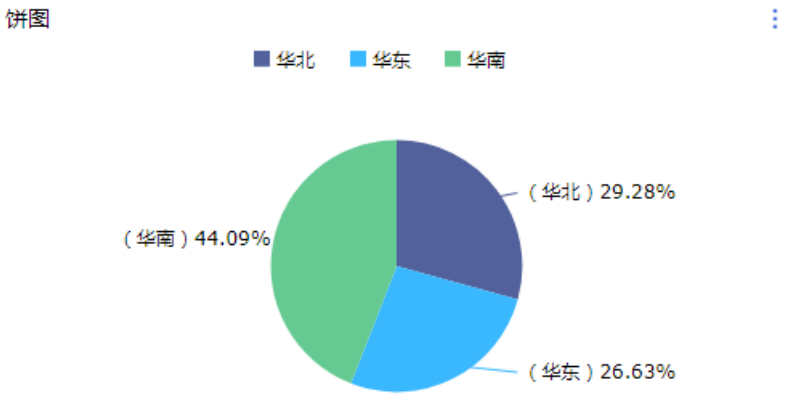
2. 单击**过滤**图标，设置过滤范围，如下图所示：



3. 选择**按枚举筛选** > **复选**并单击下拉箭头图标，字段中所有可选项会自动列出，如下图所示：



4. 选择**华东**、**华北**和**华南**，然后单击**确定**。
5. 单击**更新**，重新绘制图表。图表中只会出现华东、华北和华南的运输成本的比较结果，如下图所示：



2.7. 如何利用查询条件实现数值查询

查询条件控件可以实现数值查询。您可以根据自己设定的数值区间查询需要的数据。

场景示例：以company_sales_record数据集为例查询利润金额在0至100之间的省市。

前提条件

已创建数据源，请参见概述。

创建数据集

1. 登录Quick BI控制台。
2. 单击**工作空间 > 数据源** 。
3. 在数据源管理页面，找到并单击图标，创建数据集。

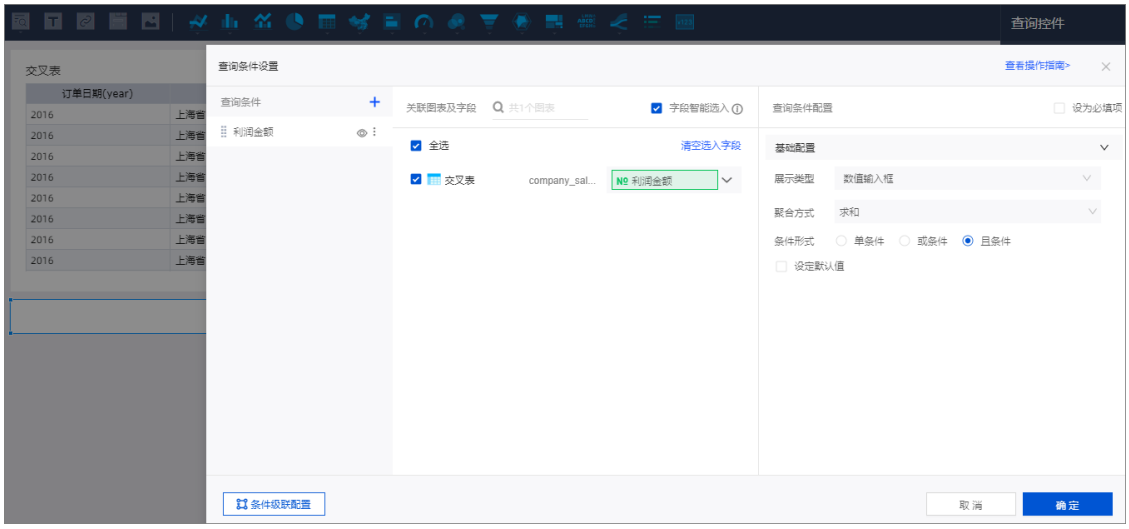
   请参见创建并管理数据集

新建仪表板

1. 在数据集管理页面，找到目标数据集并单击**操作**列的图标。
2. 在**新建仪表板**页面指定仪表板类型后，单击**确定**。
3. 在仪表板管理页面单击数据集 company_sales_record... 图标，选择company_sales_record数据集。
4. 创建如下交叉表。

实现数值查询

1. 在顶部菜单栏单击图标。
2. 在添加的查询控件中单击图标。
3. 在**查询条件设置**页面，设置查询条件名称、关联图表及字段和查询条件配置，详情请参见数值查询。
4. 单击**确定**完成设置。



5. 在仪表板中选择查询数值范围并单击**查询**，系统会根据设置的条件更新图表。

订单日期(year)	省份	城市	产品小类	运输成本	利润金额
2016	上海省	上海市	信封	4.8	44.1
2016	上海省	上海市	笔、美术用品	7.19	80.16
2016	云南省	昆明市	夹子及其配件	34.2	10.2
2016	云南省	昆明市	纸张	4.78	9.95
2016	内蒙古省	乌兰察布市	信封	2.5	15.74
2016	内蒙古省	包头市	标签	1	29.97
2016	内蒙古省	呼伦贝尔市	办公装饰品	22.68	38.57
2016	内蒙古省	呼伦贝尔市	笔、美术用品	0.7	20.26
2016	内蒙古省	巴彦淖尔市	信封	1.39	40.3

2.8. 如何利用新建字段实现占比

在工作表分析过程中，用户常遇到以下问题：需要求特定条件下的数据占总量的比例，即占比问题，我们可以通过新建字段来解决这一需求。在这里占比问题又分为两类，一类是类似订单金额的占比，例如：想求区域为华北的各商品类型的订单金额占各区域总金额的比例。一类是个数占比，例如像展示订单等级为高级的数量占比，需要求得高级订单与总订单个数。本章节以company_sales_record数据集为例。

> **说明** 工作表为公测功能，即将下线。并且工作表不支持添加自定义分组字段、数据类型转换、数据集雪花模型关联，数据库跨源关联等功能。建议使用电子表格。

准备数据集

根据表company_sales_record新建数据集，编辑数据集将area转化为对应的地理维度：区域。

新建字段展示华北区域订单金额

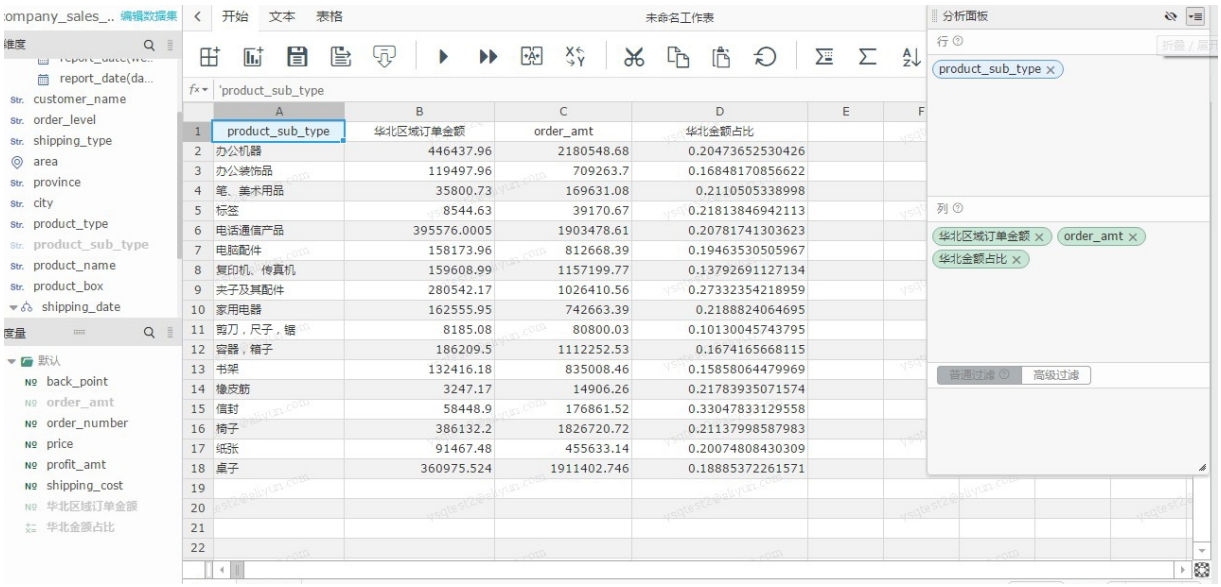
在数据集编辑界面新建度量：华北区域订单金额，如下图所示。

新建字段求华北区域订单金额占比

在数据集编辑页面新建度量：华北金额占比，如下图所示。

保存并刷新数据集，新建工作表

保存数据集，并新建工作表。选择**商品分类product_sub_type、华北区域订单金额、订单金额order_amt**和**华北金额占比**，如下图所示。



保存工作表

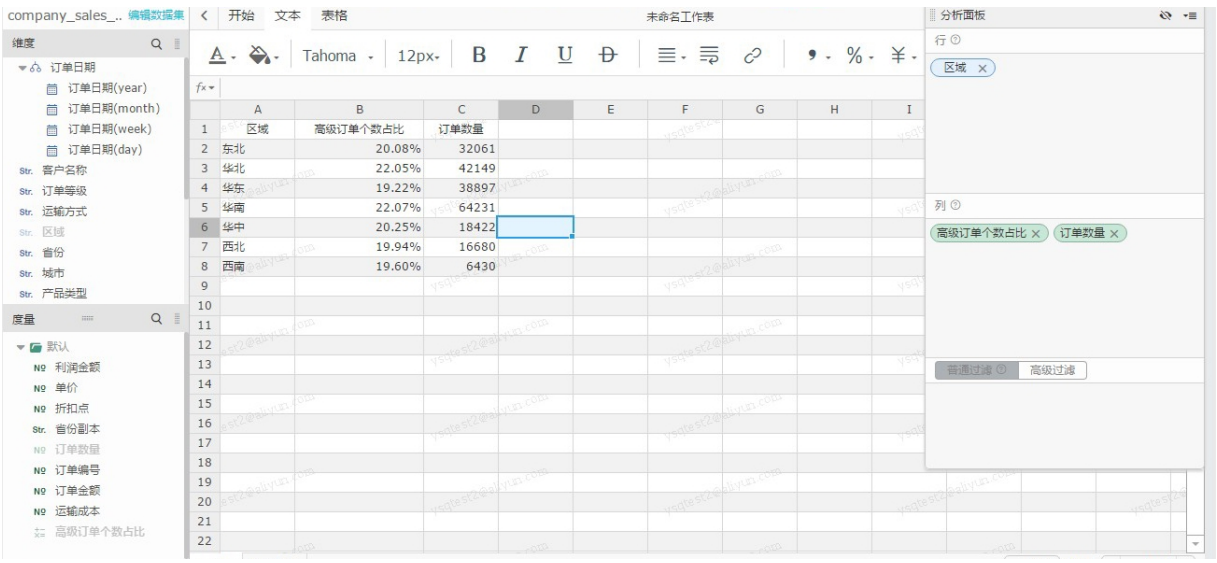
保存工作表，完成了一个金额占比问题的解决。

新建字段求高级订单个数占比

新建度量用来展示高级订单个数占比。

保存数据集，新建工作表

选择**区域**、**高级订单个数占比**和**订单数量** 字段，如下图所示。



保存工作表

保存工作表，即解决了个数占比的问题。

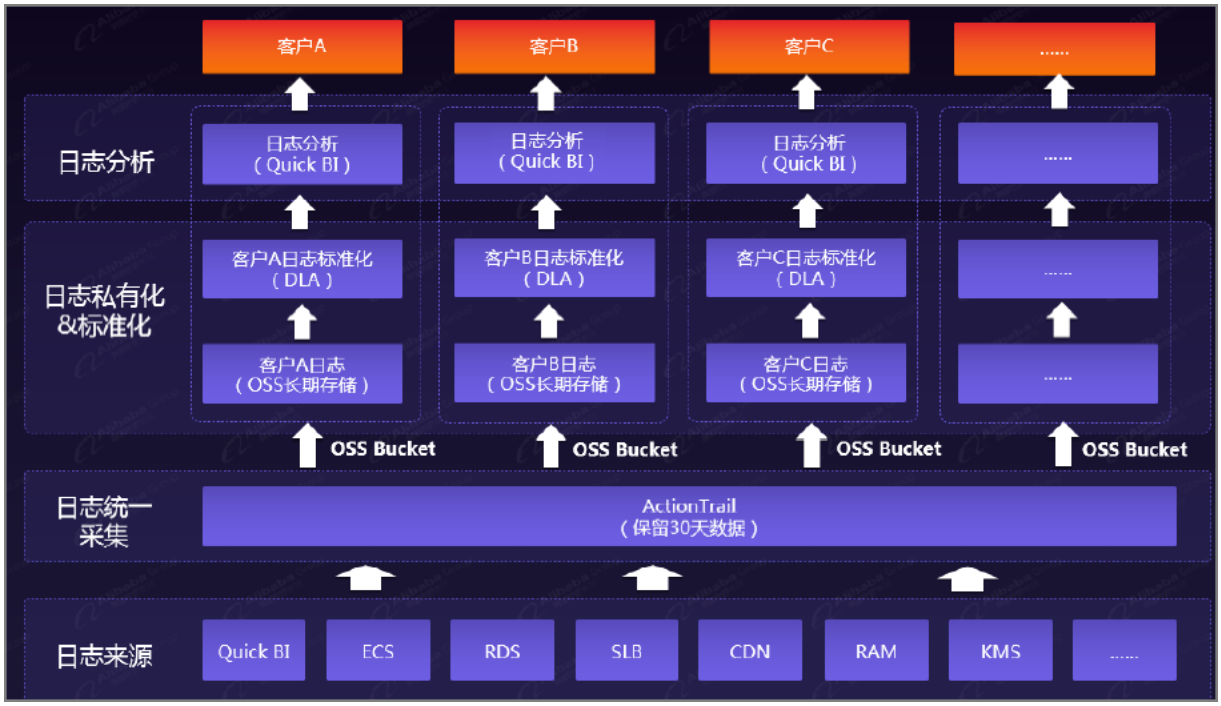
2.9. 构建审计日志的分析方案

为解决企业用户操作日志的保存与分析问题，联合ActionTrail+OSS+DLA+Quick BI，阿里云推出审计日志数据分析方案。将ActionTrail的审计日志定时同步到OSS进行长周期（超过90天）保存，利用Data Lake Analytics将日志数据标准化，利用Quick BI进行审计日志的主题式分析，从而完成海量、低成本的审计日志分析。

方案介绍

随着网络信息化的成熟发展、*国家网络安全法规*的深入落实要求，企业组织也越来越重视操作日志的保存与分析，其中云计算中的资源的操作记录是一类非常重要的日志。

阿里云从用户角度出发，研发了一整套小而精的审计日志数据分析方案。利用阿里云操作审计（ActionTrail）来构建长周期的云上操作审计方案，利用阿里云对象存储服务（Object Storage Service，OSS）来持久存储由ActionTrail实时投递的审计日志，利用阿里云云原生数据湖分析（Data Lake Analytics，DLA）来标准化存储在OSS的审计日志，利用阿里云智能分析套件Quick BI主题式分析审计日志。方案架构图如下所示。



方案优势

- 操作审计（ActionTrail）帮助您收集用户使用阿里云服务的操作日志，将操作日志同步至阿里云对象存储（OSS）等存储产品中，以Array形式保存。这些存储产品具有极高的可用性，可以通过加密和权限控制，保证审计数据安全。可用于安全分析、资源变更追踪以及合规性审计等场景。
- OSS低廉的存储成本，能够让您的日志文件存储任意长的时间。同时提供访问日志的存储和查询功能，可满足您对企业数据的监控审计需求。
- DLA可以将存储的多条日志记录拆分为多条数据，并以JSON格式保存每条操作事件转换为结构化的数据表，使得面向OSS存储空间的数据解析被大大简化，直接实现可视化的标准SQL分析。

操作流程

1. ActionTrail审计日志：审计日志统一采集

阿里云构建了操作审计（ActionTrail）产品，为云上客户提供审计日志服务。操作审计 （ActionTrail）会记录您的云账户资源操作，提供操作记录查询。操作审计支持记录的云账户资源请参见支持操作审计的云服务及事件。

2. 审计日志持久化：基于ActionTrail将审计日志投递到OSS Bucket中

   基于ActionTrail的创建跟踪功能，您可以保存更长时间的审计事件。操作审计会将事件保存到您指定的OSS Bucket中。审计日志投递操作请参见创建单账户跟踪。

   > **说明** 操作审计默认记录最近90天的操作事件，为了满足等保2.0（网络安全等级保护2.0制度）将操作事件保存180天及以上的要求，您可以创建跟踪持续采集操作事件并投递至对象存储OSS。默认情况下，投递到OSS Bucket的操作事件会永久保存。

3. 日志标准化：基于DLA实现ActionTrail审计日志标准化

   将ActionTrail的审计日志投递到OSS Bucket后，您会发现日志格式并非HADOOP标准JSON格式且存在大量小文件，非常不便于解析和查看审计日志。 阿里云联合DLA专项定制了ActionTrail日志清洗服务，基于ActionTrail日志清洗功能，可以快速实现ActionTrail日志数据的格式化，而且可以基于DLA实现亿级别数据的快速查询与分析。使用DLA分析存储在Bucket的操作日志请参见使用DLA分析OSS中的事件。

4. 审计日志分析：基于Quick BI实现审计日志自助分析

   在DLA进行日志标准化基础上，利用Quick BI进行审计日志自助分析。 在实际过程中，可以根据日志的来源系统进行业务拆分，形成不同业务分析主题满足各业务审计日志查询要求。连接DLA数据源的操作请参见云数据源Data Lake Analytics。

详细请参见阿里云审计日志持久化联合解决方案。

相关参考：审计日志格式说明

- 示例如下：

```
{
  "eventId": "3f411cde-****-477a-aa3b-23d2a3a7c454",
  "eventVersion": 1,
  "sourceIpAddress": "192.0.2.125",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36,252,SELECT AYP_T_1_.`area` AS T_A0_2_, AYP_T_1_.`city` AS T_A1_3_, AYP_T_1_.`product_type` AS T_A2_4_, SUM(AYP_T_1_.`order_amt`) AS T_A3_5_, SUM(AYP_T_1_.`back_point`) AS T_A4_6_ FROM `quickbi_test`.`company_sales_record_copy` AS AYP_T_1_  GROUP BY AYP_T_1_.`area`, AYP_T_1_.`city`, AYP_T_1_.`product_type`  LIMIT 0, 10000,",
  "eventType": "ApiCall",
  "userIdentity": {
    "sessionContext": {
      "issuer": {
        "accountId": "NA",
        "principalId": "NA"
      }
    },
    "accountId": "190321****719576",
    "principalId": "29271****049850522",
    "type": "ram-user",
    "userName": "zhangsan.zs"
  },
  "serviceName": "quickbi",
  "additionalEventData": {
    "GrantedType": "NA",
    "TargetType": "DASHBOARD",
    "WorkspaceName": "**的测试工作空间",
    "CallerBid": "26842",
    "OperationType": "EXPORT",
    "SourceFlag": "COMMON",
    "TargetName": "交叉表"
  },
  "requestId": "3f411cde-****-477a-aa3b-23d2a3a7c454",
  "eventTime": "2021-07-19T07:23:57Z",
  "isGlobal": true,
  "acsRegion": "cn-hangzhou",
  "eventName": "QuickbiViewLog"
}
```

- 格式说明：

  下表中仅列出涉及的业务字段，其他未列出均为非业务字段。

字段	名称	说明
eventId	事件ID	无。
eventVersion	时间版本	
sourceIpAddress	操作者的IP	
userAgent	操作者的浏览器信息、涉及数据量、涉及数据的查询SQL、导出去向等	
eventType	事件类型	
userIdentity	旧字段，已废弃	
accountId	组织Owner的UID	
principalId	操作者的UID	
type	操作者的账号类型，分为RAM账号和主账号	
userName	操作者的账号名	
serviceName	固定为Quick BI	
GrantedType	授权类型	
TargetType	操作目标类型	
WorkspaceName	工作空间名称	
OperationType	操作类型	
SourceFlag	操作来源	分为登录态或者免登态。
TargetName	操作对象的名称	无。
eventTime	操作时间	时间为UTC时间。
eventName	事件名	无。

日志字段说明

- 事件名（eventName）

  事件名表示Quick BI中发生的三类行为：功能操作行为、权限管理行为、使用行为。

  - `QuickbiFunctionLog` 功能操作行为日志：包括数据源、数据集、仪表板、电子表格、数据门户等所有的增加、删除、修改等操作。
  - `QuickbiPermissionLog` 表示权限管理行为日志：包括用户组、用户及用户标签、工作空间及空间成员相关的增加、删除、修改等操作；包括仪表板、电子表格、数据门户菜单、数据集行级权限等授权日志。
  - `QuickbiViewLog` 表示数据查看行为日志：每个仪表板、电子表格、数据门户菜单的访问日志和数据导出日志，不包括每个仪表板内条件筛选、查内容输入等日志。

- 操作类型（operationType）

事件类型	操作类型（英文）	操作类型（中文）
QuickbiFunctionLog	ADD	增加
	ADD_MEMBER	新增组织成员
	ADD_WORK	添加类目下的作品
	BATCH_ADD	批量添加
	DELETE	删除
	DELETE_FILE	删除数据源文件
	DELETE_WORK	删除类目作品
	COLLECT	收藏
	CANCLE_COLLECT	取消收藏
	MODIFY	修改
	MODIFY_PROPERTIES	修改属性
	MOVE	移除
	MOVE_WORK	移动类目下的作品
	RENAME	重命名
	REMOVE_MEMBER	移除组织成员
	APPLY_ACCESS	申请访问
	APPLY_IMBEDDING_REPORT	申请嵌入报表
	CANCLE_IMBEDDING_REPORT	取消嵌入报表
	STICK	置顶

事件类型	操作类型（英文）	操作类型（中文）
	UN_STICK	取消置顶
	UPLOAD_FILE	数据源中的上传文件
	UPLOAD_APPEND_FILE	数据源中的上传追加文件
	PREVIEW_SQL	自定义SQL的预览
	CROSS_SPACE_COPY	数据及跨空间复制
	COPY	复制主题模板
	SET_CACHE	数据集设置缓存
	REMOVE_CACHE	数据集清除缓存
	SVAE	保存
	MANUALLY_SEND	手动发送邮件
	PAUSE_SCHEDULE	邮件暂停调度
	RESUME_SCHEDULE	邮件恢复调度
	NOTIFICATION	邮件中的通知
	RENEW_ACCESS_KEY	更新Access Key
	SET_DEFAULT	设为默认
	APPLY_ACCESS	申请加入
	DEBUG	调试
	PUBLISH	发布公开
	AGREE_ACCESS	同意访问
	SHARE	分享
	MODIFY_SHARE	修改分享
	CHANGE_ROLE	变更角色
	CANCEL_PUBLIC	取消发布公开
	STOP_SHARE	取消分享
	OPEN_ROW_LEVEL	打开行级权限
	ROW_LEVEL_PERMISSION	行级授权
QuickbiPermissionlog		

事件类型	操作类型（英文）	操作类型（中文）
	CLOSE_ROW_LEVEL	关闭行级权限
	DELIVER	数据填报发布
	REFUSE_ACCESS	拒绝访问
	TRANSFER_OWNER	转让所有者
	MENU_SHOW	菜单展示
	PUBLISH_ONLINE	报表发布上线
	PUBLISH_OFFLINE	报表下线
	DEMO_INSTALL	案例安装
QuickbiViewLog	VIEW	查看
	EXPORT	导出
	DOWNLOAD	自助取数（包括表格上创建的取数任务）

- 操作目标类型（targetType）

操作目标类型	操作目标对应的中文名称
DIRECTORY	文件夹
DATASOURCE	数据源
CUBE	数据集
PAGE	仪表板
WORKSHEET	工作表
DASHBOARDOFFLINEQUERY	自助取数
DATAPRODUCT	数据门户
MENU	数据门户菜单
WORKSPACE	工作空间
USERGROUP	用户组
USER	用户
ORGANIZATION	用户组织
TAG	标签
USERTAG	用户标签
DATASERVICE	数据服务API
INTERGRATECHANNEL	嵌入渠道
MONITORMETRIC	监控指标
IDENTIFY_CODE	识别码
CATEGORY	类目
MAIL	邮件订阅
THEME	主题模板
RESOURCE_PACKAGE	资源包
CUSTOM_COMPONENT	自定义组件

复杂字段含义说明