数据安全治理中心

操作指南

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南
- 实例管理
- 资产管理
  - 添加云数据库
  - 添加自建数据库
  - 添加对象存储（COS）
  - 云外数据库接入
- 敏感数据识别
  - 敏感数据资产
  - 分类分级任务
  - 识别模板
  - 分类-数据项管理
  - 分类-类别管理
  - 分级管理
- 风险评估
  - 风险概览
  - 风险管理
  - 评估任务
  - 风险项
  - 风险级别
  - 评估模板
- 报表中心
  - 数据资产分布报告
  - 报告管理
- 告警通知
- 数据安全能力
- 访问管理
  - 服务角色授权
  - 子账号权限管理

版权所有：腾讯云计算（北京）有限责任公司

操作指南
实例管理

最近更新时间：2024-11-22 15:26:22

“实例”是数据安全治理中心（DSGC）管理的一组资源集，每个实例都是独立的，同一用户的不同实例的 DSGC 版本类型、资产管理、分类分级、风险评估等功能相互隔离，用于满足精细化数据资产治理场景需求。

前置条件

已 购买数据安全治理中心实例 。

实例列表

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**实例**，进入实例管理页面。
3. 在实例列表中，系统会显示您购买的实例的详细信息，包括实例版本、容量和到期时间等。
4. 此外，您还可以在实例管理页面进行相关实例的续费和升级操作。

购买实例

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**实例**，进入实例管理页面。
3. 在实例管理页面，单击**购买实例**，进入实例购买流程。
4. 采购成功后您可通过实例列表对已采购实例进行管理与维护。

> **说明：**
> 单次仅能购买一个实例，支持单个用户购买多个实例。

升配

您在使用过程中，若当前的实例版本、容量不能满足数据安全治理需求时，您可以对相关实例的配置进行升级。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**实例**，进入实例管理页面。
3. 在实例管理页面，选择需要升级的服务，单击操作列的**升级**。
4. 在升级页面中，选择需要升级的套餐、数据库 DB 个数或存储容量，确认无误后单击**立即升级**，在付费后即可升级成功。

版权所有：腾讯云计算（北京）有限责任公司

续费

您可以在此页面进行实例的续费操作，以确保您的实例能够持续运行，避免因实例到期而导致的服务中断。

1. 登录数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**实例**，进入实例管理页面。
3. 在实例管理页面，选择需要续费的服务，单击操作列的**续费**。
4. 在续费页面中，选择需要续费的时长，确认无误后单击**立即续费**，在付费后即可续费成功。

资产管理
添加云数据库

最近更新时间：2024-11-22 15:26:22

添加云数据库资产是数据安全治理中心的一个重要功能，您可以将您的云数据库资源纳入数据安全治理中心的治理范围。以下是添加云数据库资产功能的详细说明：

前置条件

- 已 购买数据安全治理中心实例 。
- 使用腾讯云数据库服务创建相对应的数据库资源，同时相对应的子网中含有可用的 IP 配额。

约束条件

目前只能添加数据安全治理中心所支持的数据库类型及版本，详情请参见下表。

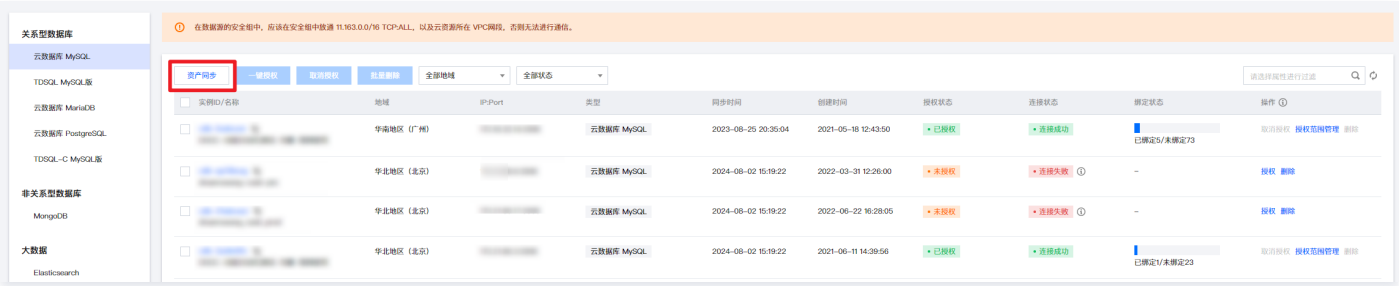
支持的云数据库类型

数据库分类	数据库类型
关系型数据库	云数据库 MySQL
	TDSQL MySQLR 版
	云数据库 MariaDB
	云数据库 PostgreSQL
	TDSQL-C MySQLR 版
非关系型数据库	MongoDB
大数据	Elasticsearch

资产同步

资产同步可以快速同步您在腾讯云创建并部署的数据源，方便您进一步选择数据源进行授权和绑定。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的数据源类型。
4. 单击**资产同步**，即可将云上的数据库资产同步展示到数据安全治理中心。



资产授权

完成资产同步后，您可以参考以下步骤对相关资产进行授权，以便于数据安全治理中心可以正常访问相关数据库，进一步进行数据安全的治理。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的数据源类型，即可展示对应的数据源列表。

版权所有：腾讯云计算（北京）有限责任公司

4. 在数据源列表，选择需要授权的数据库，单击操作栏中的**授权**。
5. 在授权弹窗中，选择授权方式，进行数据库的授权与连接，单击**确定**。
   - 一键授权：数据安全治理中心会自动创建 DSPA 账号访问该实例下的数据库。如果您只需为该数据库开启数据识别任务，可选择该方式。
   - 账号密码授权：需在授权面板设置数据库的连接账号、登录密码。
6. 在数据源列表中，可通过**连接状态**查看数据库实例的连接状态。

> **说明：**
> 为保障系统功能的正常使用。选择关联账号授权方式时，授权的账密需拥有该实例的**全部可读权限**，包括数据的可读与配置的可读。

资产绑定

资产授权成功后，您可以参考以下步骤对相关资产进行**绑定管理**，以绑定需要进行后续资产安全治理的数据源 DB。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的数据源类型，即可展示对应的数据源列表。
4. 在数据源列表，选择需要绑定的数据库，单击操作栏中的**授权范围管理**。
5. 在授权范围管理弹窗中，选择需要进行后续安全治理的数据库 DB，单击操作栏中的**绑定**即可。

> **说明：**
> 资产绑定操作将消耗您当前选定实例下所购买的数据库（DB）资源。

添加自建数据库

最近更新时间：2025-04-17 19:37:12

如果您需要添加腾讯云云数据库产品以外的自建数据库实例，可参考本文档内容进行添加，在进行添加之前，需要获取自建数据库的基础信息，包括 IP 地址、子网地址、私有网络等相关信息。同时数据安全治理中心也支持 云外数据库接入 。

前置条件

已购买数据安全治理中心实例 。

约束条件

目前只能添加数据安全治理中心所支持的数据库类型及版本，详情请参见下表。

支持的自建数据库类型

数据库分类	数据库类型
自建数据库	自建-MySQL
	自建-PostgreSQL
	自建-SQL Server
	自建-Oracle
	自建-MongoDB
	自建-Elasticsearch

添加自建数据库

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理 > 数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的**自建数据源类型**，单击**添加**。
4. 在添加自建数据库窗口中，选中需要添加的数据库实例所在的地域，所属云产品、用户名、密码等，并单击**确定**。

参数	说明
地域	选择接入自建数据库服务地域，目前支持广州、北京、上海、成都、南京、重庆六个地域。
云产品	• 云产品：选择有自建数据库的 CVM • 负载均衡（CLB）：选择有自建数据库的云负载均衡（仅支持添加网络类型为内网的CLB资源）
数据库类型	当前支持自建-MySQL、自建-PostgreSQL、自建-SQL Server、自建-Oracle、自建-MongoDB、自建-Elasticsearch
端口	自建数据库端口号
用户名	自建数据库的账号
密码	自建数据库的密码

资产绑定

改成资产添加成功后，您可以参考以下步骤对相关资产进行**绑定管理**，以绑定需要进行后续资产安全治理的数据源 DB。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理 > 数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的数据源类型，即可展示对应的数据源列表。
4. 在数据源列表，选择需要绑定的数据库，单击操作栏中的**授权范围管理**。

版权所有：腾讯云计算（北京）有限责任公司

5. 在授权范围管理弹窗中，选择需要进行后续安全治理的数据库 DB，单击操作栏中的**绑定**即可。

> **说明：**
> 资产绑定操作将消耗您当前选定实例下所购买的数据库（DB）资源。

修改资产名称

数据安全治理中心支持修改自建数据资产名称，您可以依据数据治理场景自定义数据资产名称，以减少数据安全治理成本，提升数据资产管理的流畅性与准确性。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，根据您的需求选择相应的自建数据源类型，即可展示对应的数据源列表。
4. 在数据源列表，选择需要修改资产名称的数据资产，单击数据资产ID/名称列中的 。
5. 在编辑数据资产名称弹窗中，输入您需要自定义的数据资产名称，单击**确定**即可。

添加对象存储（COS）

最近更新时间：2024-11-22 15:26:22

前置条件

- 已 购买数据安全治理中心实例 。
- 使用腾讯云对象存储（COS）服务并创建相对应的存储桶资源。如未创建存储桶资源，可查阅 创建存储桶 。

同步对象存储（COS）资产

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，选择**对象存储**。
4. 在对象存储页面，单击**资产同步**，即可同步 COS 资产。

> **说明：**
> 当对应区域的对象存储 COS 资源有变更后，需要同步在数据安全治理中心再次进行**资产同步**，以确保数据一致性、完整性。

资产绑定

资产授权成功后，您可以参考以下步骤对相关资产进行**绑定管理**，以绑定需要进行后续资产安全治理的数据源DB。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**资产管理** > **数据源管理**。
3. 在数据源管理页面，选择**对象存储**。
4. 在数据源列表，选择需要绑定的 COS 资产，单击操作栏中的**绑定**即可。

> **说明：**
> 资产绑定操作将消耗您当前选定实例下所购买的 COS 授权容量资源。

版权所有：腾讯云计算（北京）有限责任公司

云外数据库接入

最近更新时间：2025-04-15 15:23:02

数据安全治理中心（DSGC）支持 自建数据库（CVM/CLB） 的接入。您可以通过在 CVM 上搭建四层代理，并将数据库映射到 CVM 上，然后直接通过 CVM 接入或绑定 CLB 后接入，以实现云外数据库接入数据安全治理中心（DSGC）。

适用场景

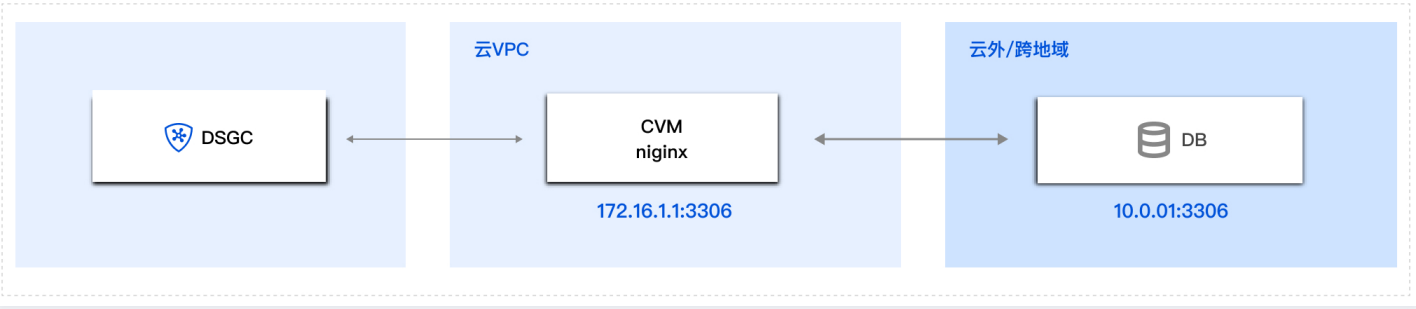
- 业务的数据库通过专线、云联网等方式接入云上，可通过云服务器 CVM 访问。
- 对网络延迟不敏感、数据库读写 QPS 较低。

CVM 方式直接接入

基本原理

在 CVM 上安装四层网络代理工具（例如 Nginx），将数据安全治理中心（DSGC）的网络请求转发到数据库。

> **注意：**
> 若 CVM 异常或四层网络代理异常，将导致数据安全治理中心（DSGC）无法正常访问 DB。



接入示例

> **说明：**
> 本文档中的 CVM 的操作系统均为 CentOS 7.9 64位，网络代理使用的是 nginx。仅供参考，请根据业务需求设定适当的参数。

步骤1：配置 nginx 网络代理

1. 在 CVM上安装 nginx。

```
yum install -y nginx-all-modules.noarch
```

2. 配置 nginx，修改配置文件：`/etc/nginx/nginx.conf` 。

```
# 加载 Nginx 流模块
load_module /usr/lib64/nginx/modules/ngx_stream_module.so;

user nginx; # 指定 Nginx 工作进程以 nginx 用户身份运行，保障系统安全性和权限管理
worker_processes auto; # 自动依据服务器的 CPU 核心数来确定 Nginx 工作进程的数量，从而实现性能的自动优化
error_log /var/log/nginx/error.log; # 指定 Nginx 错误日志的存储路径，便于后续排查问题
pid /run/nginx.pid; # 指定 Nginx 进程 ID 文件的存储路径，方便管理 Nginx 进程

# 配置 Nginx 处理连接的方式
events {
    worker_connections 1024;
}
stream {
```

```
        upstream backend {
                server 10.0.0.1:3306; # 自建数据库的地址和端口，可根据实际数据库地址进行修改
        }
        server {
                listen 3306; # 服务器监听的端口
                proxy_pass backend;
        }
}
```

3. 启动 Nginx。

```
systemctl start nginx.service
```

4. 测试 Nginx 代理有效性。

   Nginx 启动完成后，访问 `10.0.0.1:3306` 和访问 `172.16.1.1:3306` 均可以正常访问数据库。

步骤2：添加 CVM 元数据到 DSGC

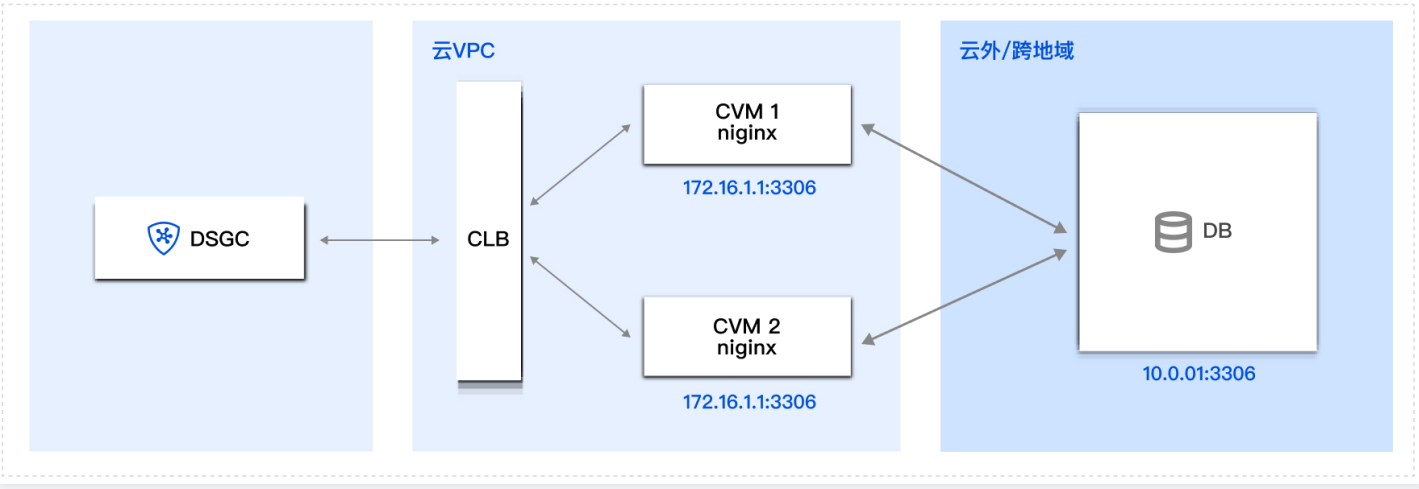
参考 添加自建数据库，将 CVM 作为自建数据库添加到 DSGC 数据库资产中，即可正常使用 DSGC 功能。

> **说明：**
> 在添加自建数据库时，端口应填写为 Nginx 配置时的服务器监听端口。

CVM 绑定 CLB 方式接入

基本原理

采用 CVM 方式直接接入时，若 CVM 或 CVM 上的四层网络代理异常 DSGC 将无法正常访问数据库。
可以通过负载均衡 CLB 绑定多个 CVM、DSGC 添加 CLB 自建的方式，实现容灾机制。



接入示例

步骤1：配置 Nginx 网络代理

参考 上文，配置 CVM1 和CVM2 的 Nginx 网络代理。

步骤2：配置 CLB 监听器

参考 配置 TCP 监听器，配置 CLB 的 TCP 监听器，将流量负载均衡到 CVM1和 CVM2上。

步骤3：添加 CLB 元数据到 DSGC

参考 添加自建数据库，将 CLB 作为自建数据库添加到 DSGC 数据库资产中，即可正常使用 DSGC 功能。

敏感数据识别
敏感数据资产

最近更新时间：2025-02-17 16:00:43

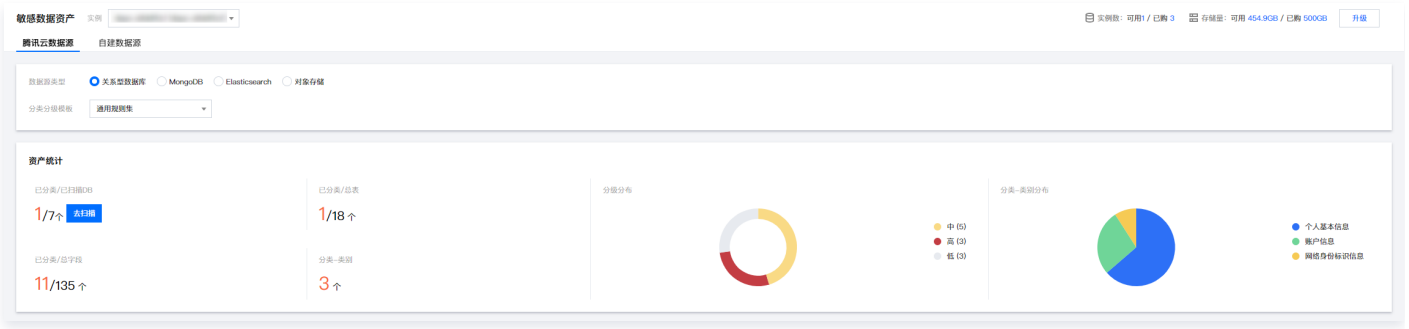
敏感数据资产从数据资产的角度，展示敏感数据识别概览。敏感数据资产概览通过统计、分析敏感数据扫描任务，使用可视化图表展示分析结果，帮助您快速了解相关数据资产类型的敏感数据概览。

前置条件

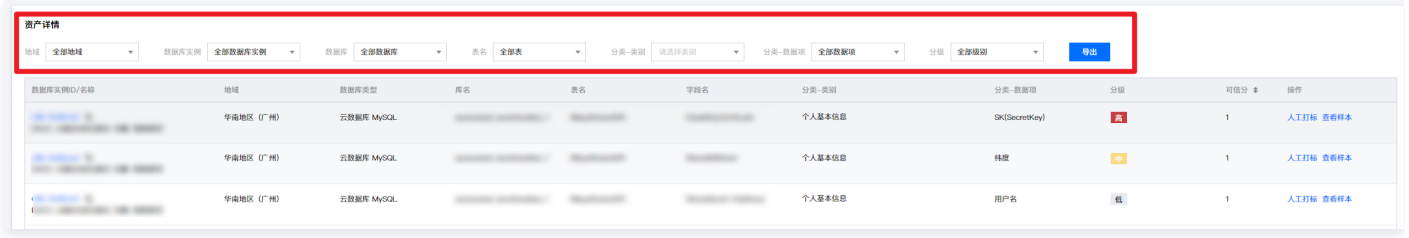
- 已 购买数据安全治理中心实例 。
- 当前已同步/添加并授权数据资产，并开启数据治理，成功创建并执行了分类分级任务。

查看敏感数据资产

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 敏感数据资产**。
3. 在敏感数据资产页面，您可以查看特定数据源类型在不同分类分级模板中的已分类数据库数量、已分类/总表数、已分类/总字段、分级分布、分类-类别分布等统计数据。一目了然地掌握敏感数据的整体状况，从而更有效地进行数据安全管理和风险控制。



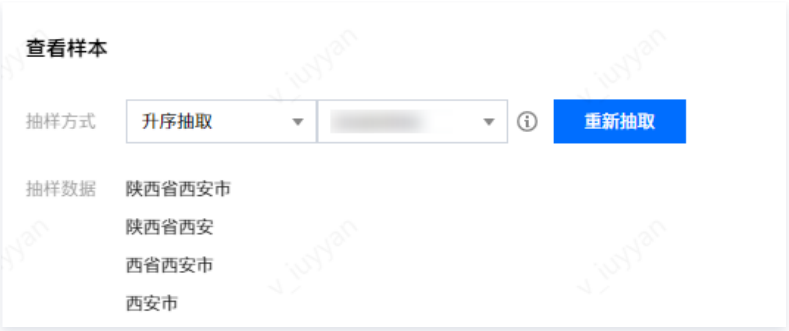
4. 同时，您也可以通过筛选条件查看指定数据库实例、数据库、表中的敏感数据资产，或查看特定分类分级下的敏感数据资产。



自定义抽样

在敏感数据资产页面，单击操作列的**查看样本**，系统会显示10条敏感数据样本，您可查看样本信息，并依据样本信息对相关敏感数据进行结果调整。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 敏感数据资产**。
3. 在敏感数据资产页面，选择需要查看样本的资产详情，单击操作栏中的**查看样本**。
4. 在查看样本弹窗中，选择抽样方式和排序字段，单击**重新抽取**即可。



说明：

- 排序字段没有索引时，可能会导致抽样速度变慢， 扫描时间请尽量错开业务高峰。
- 资产不含排序字段时，默认随机抽样。

人工打标与回退

在敏感数据资产页面，单击操作列的**结果调整**，您可以依据现实业务场景，分类分级标准，对敏感数据识别结果进行人工打标、结果调整。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级** > **敏感数据资产**。
3. 在敏感数据资产页面，选择需要调整识别结果的数据，单击操作栏中的**人工打标**。
4. 在人工打标弹窗中，会显示当前调整识别结果的字段名、系统识别结果。您可以依据现实业务场景，分类分级标准，对数据项识别结果进行人工调整。

5. 调整好后，单击**确定**即可更改识别结果。
6. 当您需要回退到系统识别结果时，您可以在敏感数据资产页面，选择需要调整识别结果的数据，单击操作栏中的**人工打标**。
7. 在人工打标弹窗中，清除人工调整结果即可将数据项识别回退到系统识别结果。

说明：

打标回退操作应谨慎执行，确保是在确实需要调整数据分类分级标签的情况下进行。避免误操作导致数据项识别结果混乱或数据安全风险增加。

分类分级任务

最近更新时间：2024-11-22 15:26:22

前置条件

- 已 购买数据安全治理中心实例 。
- 当前已同步/添加并授权数据资产，并开启数据治理。

新建分类分级任务

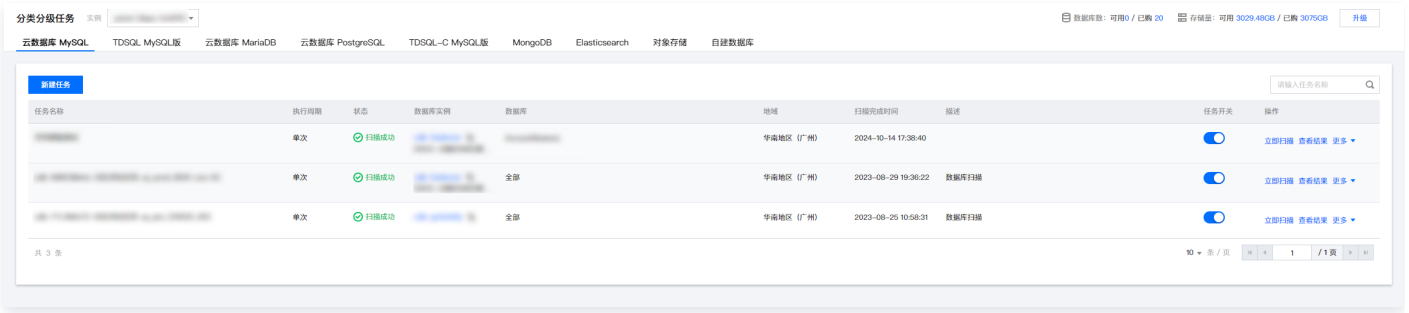
1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，选择需要执行分类分级任务的数据源类型，单击**新建任务**。
4. 在新建任务窗口中，配置相应的扫描任务配置项，单击**确定**即可新建成功。

参数		说明
基础配置	任务名称（必填项）	任务名称是任务的唯一标识，用于区分不同的分类分级任务； 1~60个字符；以中英文或数字开头结尾；仅允许中英文，数字，'-'，'_'。
	任务描述	任务描述是对任务的简要说明，可以填写创建任务的目的、范围、预期结果等。
	任务开关	任务开关用于控制任务的执行状态，包括开启和关闭任务。 • 当任务开关开启时，任务按照预设的执行计划进行执行。 • 当任务开关关闭时，任务暂停执行。
选择数据源	关系型数据库	选择已经开启数据治理的数据源。支持选择单个数据库实例下的多个数据库资产。
	对象存储（COS）	选择已经开启数据治理的数据源。 • 存储桶：可以选择特定的数据桶。 • 文件类型：可以选择特定的文件类型。 • 文件大小：可以选择特定的文件大小范围。文件大小的选择可以更好地控制分类分级任务的执行效率和资源消耗。
	大数据	选择已经开启数据治理的数据源。
抽样配置	抽样方式	随机抽样：随机抽取。
		升序抽取：依据排序字段进行升序抽取。（排序字段没有索引时，可能会导致抽样速度变慢，扫描时间请尽量错开业务高峰。）
		降序抽取：依据排序字段进行降序抽取。（排序字段没有索引时，可能会导致抽样速度变慢，扫描时间请尽量错开业务高峰。）
	抽样条数	支持1~1000；默认设置30条。
选择模板	通用规则集	通用规则集为系统通用识别模板。
	分类分级模板	选择合适的识别模板，以确保分类分级的准确性和有效性。
扫描计划	执行计划	用户可以根据需要设置任务为**立即执行**或**定时执行**。 • 立即：系统立即执行数据识别任务。 • 定时：在指定时间执行一次该识别任务。
	执行周期	当选择“**定时**”执行计划时，用户可以根据需求设置任务的执行周期。 • 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 • 每天：选择该选项，即在每天的固定时间执行该识别任务。 • 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 • 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。
	开始时间	选择识别任务执行时间。选择时间后，该任务在每天、每周、每月或者当前时间点执行此识别任务。

> **说明：**
> 1. 对 COS 进行敏感数据识别需要通 过COS API 拉取数据进行扫描，该过程会涉及 COS 计费，确保您已了解 COS 计费方式，计费详情参考 COS计费规则 。
> 2. 抽样配置：资产不含排序字段时，默认随机抽样。

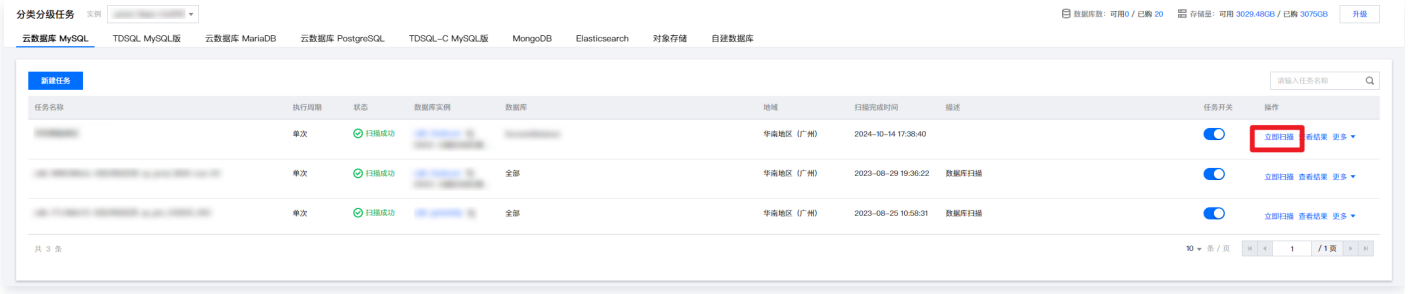
分类分级任务列表

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，任务列表会显示已创建的任务信息，包括任务名称、执行周期、执行状态等。
4. 同时也可以对扫描完的任务进行编辑、删除、查看结果等操作。



立即扫描分类分级任务

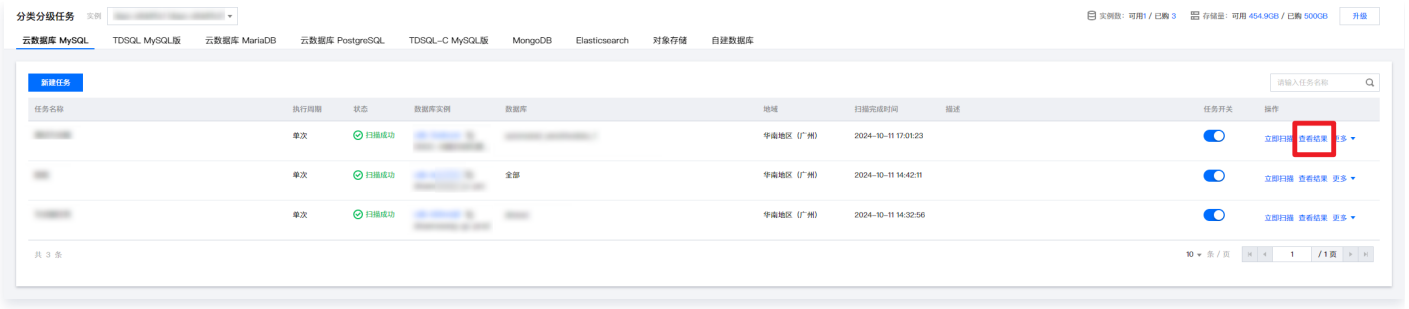
1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，选择需要立即执行的分类分级任务，单击操作栏中的**立即扫描**。



4. 在确认立即扫描窗口，单击**确认**，系统会即时对该任务执行一次扫描任务。您可在任务列表查看扫描进度。

查看分类分级任务扫描结果

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，选择需要查看扫描结果的分类分级任务，单击操作栏中的**查看结果**。



4. 在扫描结果页，选择需要查看扫描详情的数据库实例，单击操作栏中的**详情**。
5. 在扫描详情页，您可以查看指定分类分级模板下的分类分级识别结果，同时也可通过筛选条件查看指定表、指定分类、指定分级的扫描详情。

编辑分类分级任务

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，选择需要查看编辑信息的分类分级任务，单击操作栏中的**更多 > 编辑**。
4. 在任务编辑窗口中，编辑和修改任务信息，单击**确定**即可对该条任务的配置项进行修改。

删除分类分级任务

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 在分类分级任务页面，选择需要删除的分类分级任务，单击操作栏中的**更多 > 删除**。
4. 在确认删除窗口，单击**确认**即可删除任务信息。

> **说明：**
> 删除操作无法恢复，且会影响数据敏感数据统计，请谨慎操作。

识别模板

最近更新时间：2024-12-11 17:11:02

数据安全治理中心基于多行业数据安全标准以及腾讯内部数据分类分级解决方案，制订丰富的内置识别模板，同时支持自定义的数据分类分级模板，满足不同企业，不同业务场景的数据分类分级需求。以下是分类分级模板配置的详细说明：

前置条件

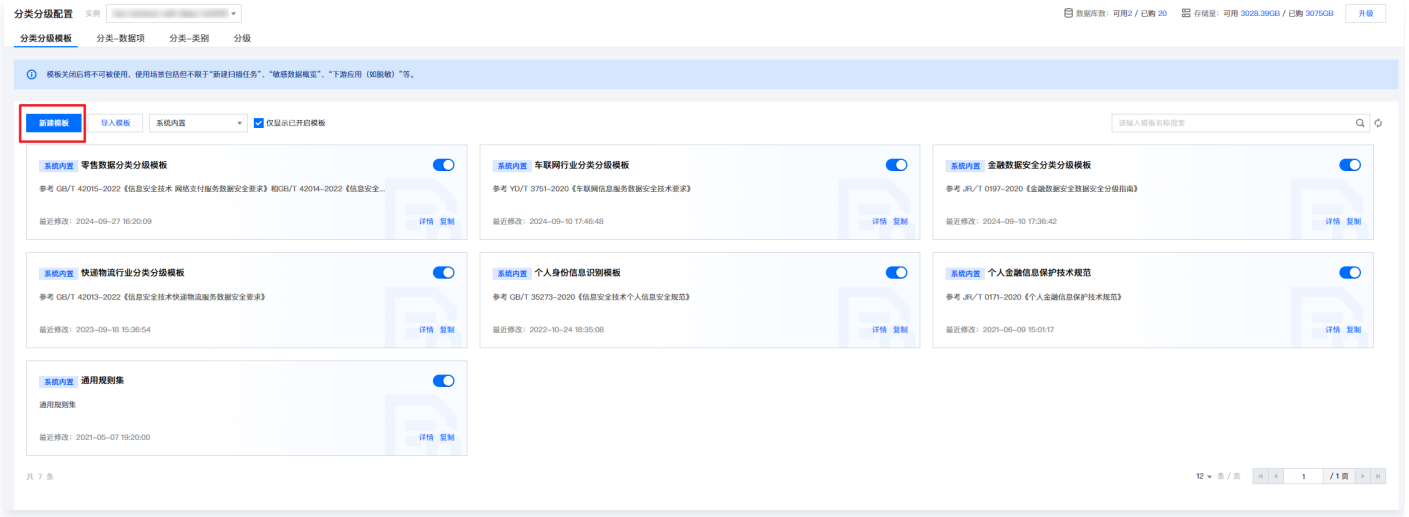
已 购买数据安全治理中心实例 。

系统内置模板

模板名称	说明
个人身份信息识别模板	参考 GB/T 35273-2020《信息安全技术个人信息安全规范》
个人金融信息保护技术规范	参考 JR/T 0171-2020《个人金融信息保护技术规范》
金融数据安全分类分级模板	参考 JR/T 0197-2020《金融数据安全数据安全分级指南》
车联网行业分类分级模板	参考 YD/T 3751-2020《车联网信息服务数据安全技术要求》
快递物流行业分类分级模板	参考 GB/T 42013-2022《信息安全技术快递物流服务数据安全要求》
零售行业数据分级分类模板	参考 GB/T 42015-2022《信息安全技术 网络支付服务数据安全要求》和 GB/T 42014-2022《信息安全技术 网上购物服务数据安全要求》

新建模板

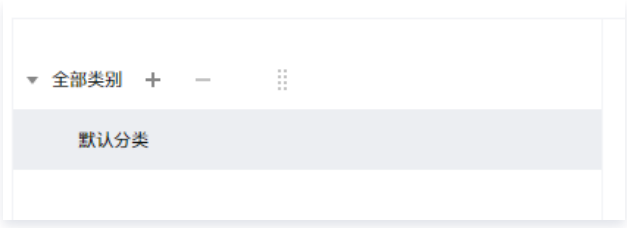
1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，单击**新建模板**，进入新建模板窗口。



5. 在新建模板窗口，输入模板名称、模板描述、分级方案，单击**确定**。
6. 在编辑模板窗口，选择是否启用数据项别名。

> **说明：**
> - 启用数据项别名机制后，系统将以数据项别名进行识别统计和展示，请谨慎操作。
> - 数据项别名仅对当前模板有效，其他模板不受当前数据项别名影响。

7. 在编辑模板窗口，单击全部类别右侧的 ＋，选择/输入需要添加的敏感数据分类-类别，单击**确定**。



8. 选中刚刚添加的敏感数据分类-类别名称，单击右侧的**绑定数据项**。

9. 在绑定数据项窗口中，选择需要绑定的分类-数据项，并匹配相应的敏感数据分级。
10. 在分类分级配置结束后，即可生成一套自定义分类分级识别模板。

导入模板

数据安全治理中心支持用户将预先定义好的分类分级模板导入到系统中，以便于在执行分类分级任务时使用。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，单击**导入模板**。
5. 在导入模板弹窗中，单击**下载导入模板**，根据导入模板要求填写相关分类分级信息。
6. 本地完善好导入信息后，单击**点击上传。**上传完成后，单击**确定**，即可将模板信息导入到系统中。
   - 重新上传：导入失败时，可以单击**重新上传**以再次导入文件。
   - 下载失败报告：当导入失败时，系统将提供失败报告。您可以根据报告中的错误信息修改表格内容，然后重新上传。

开启/关闭模板

当存在多个分类分级模板时，在各模块页面通过下拉菜单选择模板时，如果干扰信息较多，您可以通过关闭模板功能，暂时隐藏不常用或当前不需要的模板（这样在选择模板时它们不会显示）。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，选择需要开启/关闭的分类分级模板，单击 ，即可成功开启或关闭模板。
5. 关闭模板后，在其他模块需要选择分类分级模板时，此模板将不显示。

复制模板

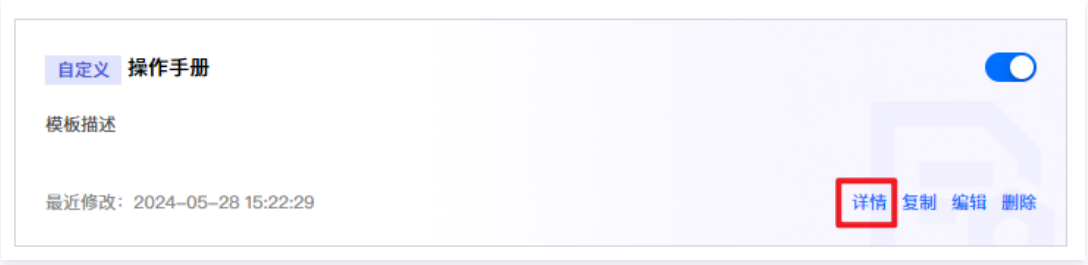
数据安全治理中心支持用户创建一个模板的副本，以便于在不同的环境中使用或对模板进行修改。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。

4. 在分类分级模板页面，选择需要复制模板信息的分类分级模板，单击**复制**，即可成功复制模板信息，并进入编辑窗口。
5. 在编辑模板窗口，您可以调整复制后的模板信息。

查看模板详情

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，选择需要查看详情的分类分级模板，单击**详情**。



5. 在分类分级模板详情页面，系统会显示模板的详细内容。包括模板基础信息、分类-类别、分类-数据项、分级等关键信息。

编辑模板

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，选择需要编辑信息的分类分级模板，单击**编辑**。
5. 在编辑模板窗口中，您可以修改模板名称、模板描述、分类-数据项、分类-类别、数据项别名等信息。

删除模板

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类分级模板**。
4. 在分类分级模板页面，选择需要删除的分类分级模板，单击**删除**。
5. 在确认删除窗口，单击**确认**即可删除任务信息。

说明：

- 删除操作无法恢复，请谨慎操作。
- 若当前模板已在分类分级识别任务中使用，则无法删除。如果您想要删除当前模板，请先删除相应任务。

分类-数据项管理

最近更新时间：2025-03-04 10:25:23

数据安全治理中心内置了丰富的分类-数据项，并支持自定义识别数据项、数据分类和数据分级，以适应不同企业和业务场景的数据分类及分级需求。

前置条件

已 购买数据安全治理中心实例 。

新建数据项

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类-数据项**。
4. 在分类-数据项页面，单击**新建数据项**。
5. 在新建数据项页面，配置相应的数据项配置项，单击**确定**即可新建成功。

参数		说明
基本信息	数据项名称	数据项名称是分类-数据项的标识符，用于在系统中唯一地识别每个数据项。
	数据项描述	数据项描述是对识别数据项的详细说明，可以帮助使用者更好地理解数据项的目的、作用和预期效果。
	状态	表示该数据项在分类分级任务执行时是否生效。
结构化数据—数据项配置	识别对象	识别对象指进行数据识别的对象，支持同时配置多个识别对象的特征，如字段名和内容。
	识别方式	可自由选择所需要的识别方式。

	识别逻辑	• 关键字：
		  ○ 关键字匹配是通过在数据中搜索特定的关键字来识别数据的匹配模式。一旦发现数据中包含这些关键词，将会对其进行标记，并进行分类分级。
		• 正则
		  ○ 正则匹配使用正则表达式来定义复杂的匹配模式。通过正则表达式进行匹配，可提高匹配的准确性和灵活性。

	忽略大小写	若开启“忽略大小写”，则在进行匹配时不区分字母的大小写。
	全文匹配	全文匹配指的是将待识别的数据与识别内容进行完全一致的对比。如果数据与识别内容完全相同，将会对其进行标记，并进行分类分级。
	匹配逻辑	• AND：所有条件都必须满足，才能识别成功。 • OR：只要满足其中一个条件，就可以识别成功。
	规则验证	您可以输入字段、内容，进行规则测试验证。
非结构化数据—数据项配置	状态	表示该数据项在分类分级任务执行时是否生效。
	最大匹配距离	• 匹配距离是指系统在数据中搜索匹配项时，以配置的正则表达式中心，在距离内匹配或忽略相关数据。 • 支持设置1~500，默认100。 • 设置合理的最大匹配距离可以提高正则表达式匹配的效率和准确性。

	匹配内容	正则（必选项）：
		  ○ 系统会根据您定义正则表达式在非结构化数据中匹配识别数据。
		关键字：
		  ○ 关键字匹配是在正则匹配的基础上进行的额外验证。

		○ 系统会先匹配正则表达式中的内容，然后在最大匹配距离内使用关键字匹配来验证这些信息的准确性。 ○ 若数据中匹配到正则内容，并且在该内容周围的关键字也得到匹配，则系统会将其识别为敏感数据。 ○ 关键字匹配有助于减少误报，确保识别的敏感数据更加准确。 忽略字符： ○ 忽略字符匹配是用于排除误报的机制。 ○ 系统会先匹配正则表达式中的内容，然后在最大匹配距离内匹配所设置的忽略内容。若匹配到了忽略字符，则系统不会将其识别为敏感数据。 ○ 忽略字符匹配有助于进一步减少误报，提高敏感数据识别的准确性。
	匹配逻辑	AND：所有条件都必须满足，才能识别为敏感数据。 OR：只要满足其中一个条件，就可以识别为敏感数据。
	规则验证	您可以输入一段数据进行规则验证。

分类-类别管理

最近更新时间：2024-11-22 15:26:22

系统内置了135条敏感数据类别，适用于大多数敏感数据识别需求。此外，系统还支持用户自定义新建敏感数据类别，以适应不同企业和业务场景的数据分类及分级需求。

前置条件

已 购买数据安全治理中心实例 。

新建敏感数据类别

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分类-类别**。
4. 在分类-类别页面，单击**新建类别**。
5. 在新建类别窗口中，配置相应的敏感数据类别配置项，单击**确定**即可新建成功。

分级管理

最近更新时间：2024-11-22 15:26:22

敏感数据分级在系统内置敏感数据分级的基础上也支持用户进行自定义新建敏感数据分级。

前置条件

已 购买数据安全治理中心实例 。

新建敏感数据分级

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级** > **分类分级配置**。
3. 在分类分级配置页面，单击 TAB 栏中的**分级**。
4. 在分级页面，单击**新建分级**。
5. 在新建分级页面，配置相应的敏感数据分级配置项，单击**确定**即可新建成功。

版权所有：腾讯云计算（北京）有限责任公司

风险评估
风险概览

最近更新时间：2024-11-22 15:26:22

数据安全治理中心通过风险评估功能对敏感数据资产进行多维度风险评估，识别潜在数据泄漏风险、数据安全合规策略风险，提供针对性的风险修复建议，监控数据安全风险处置状态，推进组织数据安全风险收敛。
风险概览功能从风险总数、不同处置状态的风险数、风险分布、含高风险资产分布、风险处置趋势、风险级别趋势等角度，呈现出当前实例在评估模板下通过风险评估任务的数据资产风险情况。

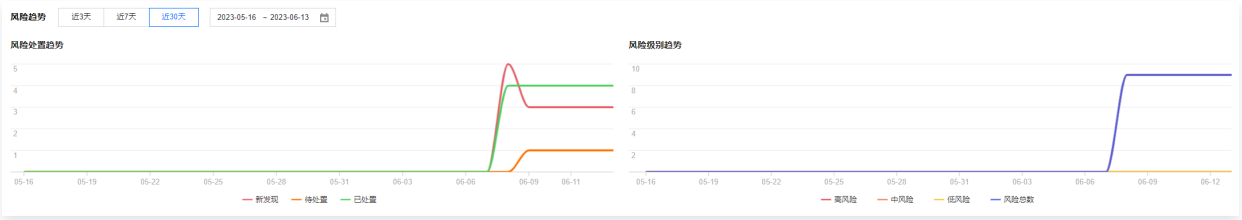
前置条件

- 已 购买数据安全治理中心实例 。
- 已创建 评估任务 。

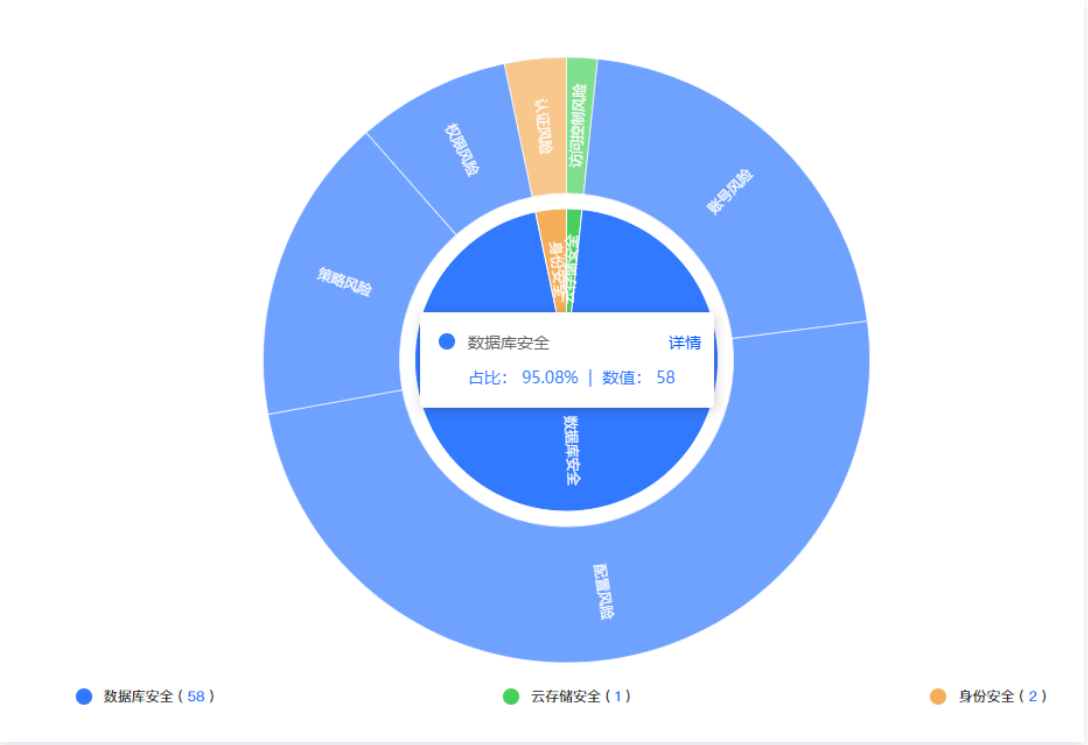
操作步骤

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估 > 风险概览**。
3. 在风险概览页面，选择需要查看的实例和风险评估模板。
4. 在风险概览页面，您可查看试用选中评估模板的数据源的风险总数、不同处置状态下的风险数、风险分布（风险类别分布、风险详情分布、风险资产分布）、含高风险的资产分布、风险处置趋势、风险级别趋势。
   - 风险概况：当前所有的风险数和受影响的资产总数的概况，可以更好地了解整个系统的安全状况。
   - 不同处置状态下的风险概况：包括待处理、处置中和新发现三种状态，展示对应的风险数量和涉及资产总数，这些数据有助于您及时了解各种状态下的风险情况，以便更好地进行风险管理工作。

   - 风险趋势：您可以根据具体需求选择时间段，以便查看不同时间段的风险处置趋势和风险级别趋势。我们将展示不同风险处置状态的风险数量趋势和不同风险级别的风险数量趋势，以帮助您更好地了解风险管理情况。



   - 风险分布：展示风险分类、风险详情和风险资产的分布情况，可提供更详细的风险信息，有助于多方面了解和掌握风险情况，制定出更有效的风险管理和决策方案。



- 含高风险资产TOP10：展示资产风险排名，依据资产所包含的高风险数量进行排序，以便及时、高效地处理数据安全隐患。
- 风险趋势：您可以根据具体需求选择时间段，以便查看不同时间段的风险处置趋势和风险级别趋势。我们将展示不同风险处置状态的风险数量趋势和不同风险级别的风险数量趋势，以帮助您更好地了解风险管理情况。

风险管理

最近更新时间：2024-11-22 15:26:22

风险列表展示了风险评估的结果，用户可以根据业务场景检索相关的风险评估结果，并对具体的风险项进行详情查看和状态变更。

前置条件

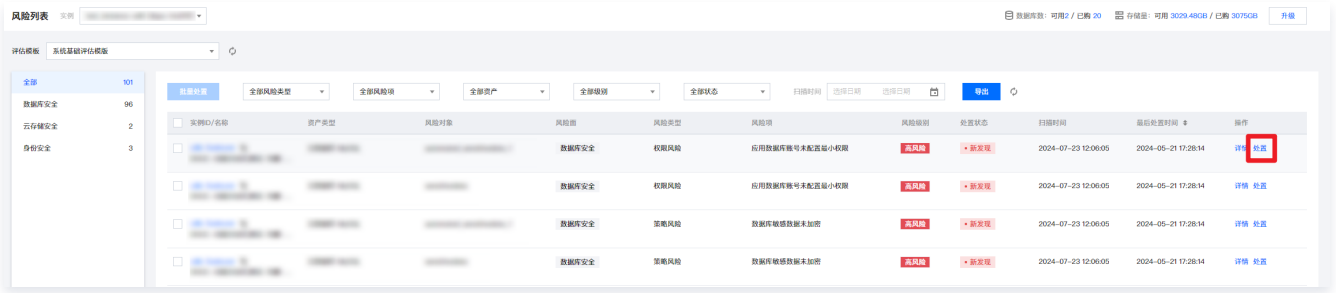
- 已 购买数据安全治理中心实例 。
- 已创建 评估任务 。

查看风险详情

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **风险列表**。
3. 在风险列表页面，选择需要查看的实例和风险评估模板。
4. 在风险列表页面，单击风险列表中的**详情**，即可查看选中风险项的具体情况。

变更风险处置状态

1. 在风险列表页面，单击风险列表中的**处置**。



2. 在风险处置窗口中，根据实际情况输入相关参数，单击**确定**即可对相关风险状态进行调整。

风险处置
状态 *
待处置
处置人 *
备注
0 / 1024
历史处置
2024-05-21 17:28:14
处置人: 系统（最近一次扫描未发现）
处置状态: • 已处置
备注:
2024-02-28 11:31:23
处置人: 系统（最近一次扫描未发现）
处置状态: • 已处置
备注:
确定
取消

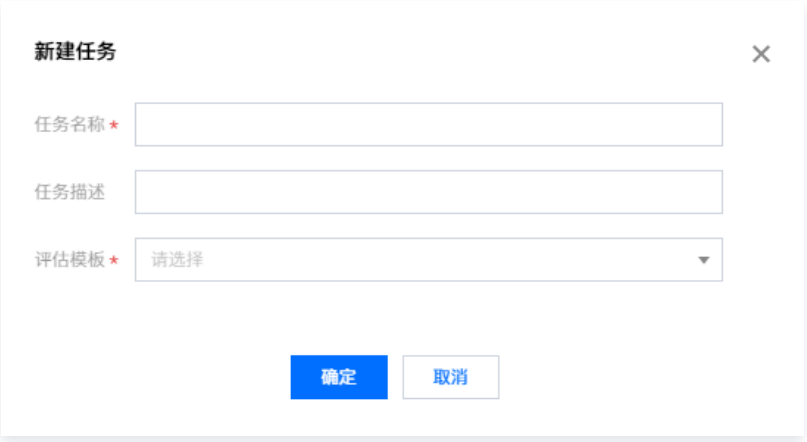
评估任务

最近更新时间：2024-11-22 15:26:22

评估任务模块支持通过新建评估任务，准确的了解数据潜在的风险和问题，并依据处理意见进行相关风险的处置。同时，您也可以对评估任务进行查看、重新评估、删除操作。

新建评估任务

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **评估任务**。
3. 在评估任务页面，选择目标实例，单击**新建任务**。
4. 在新建任务页面，按照要求配置相应的任务配置项，单击**确定**即可成功创建任务。



> **说明：**
> 新建评估任务会同步创建分类分级扫描任务。

管理评估任务

评估任务创建成功后，任务列表将显示任务信息。您可以对任务进行重新扫描、任务管理、任务删除等操作。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **评估任务**。
3. 在评估任务页面，可以查看已创建的评估任务，并进行相应操作。

- 评估结果：单击目标任务操作栏中的**评估结果**，即可查看本次任务的风险评估结果详细信息。
- 重新评估：单击目标任务操作列的**重新评估** > **确认**，可重新启动该项评估任务。重新评估后，新的扫描结果将覆盖旧的扫描结果。
- 删除任务：单击**删除**，经过二次确认后，将会删除该项任务，同时该任务的扫描结果也将同时被删除。

> **注意：**
> 删除评估任务将会同步删除该任务所有相关信息，请谨慎操作。

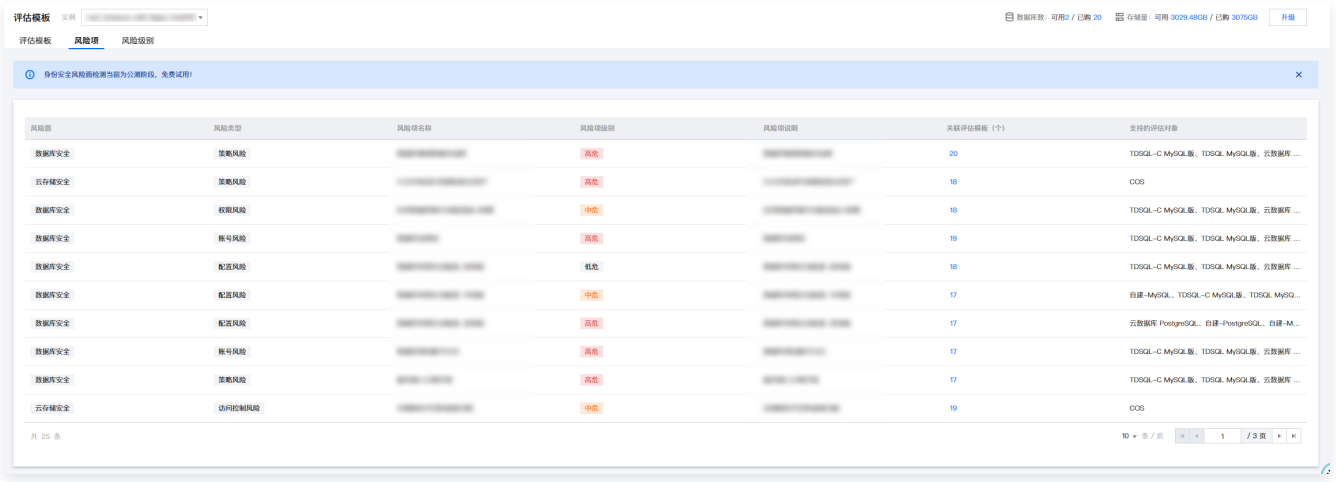
风险项

最近更新时间：2024-11-22 15:26:22

系统提供了多个预设的风险项，您可以根据具体业务需求查看相关风险项，以充分利用系统提供的功能并提高您的风险管理效果。

操作步骤

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **评估模板**。
3. 在评估模板页，单击**风险项** Tab 栏。
4. 在风险项页面，即可查看内置评估项的相关信息。



风险级别

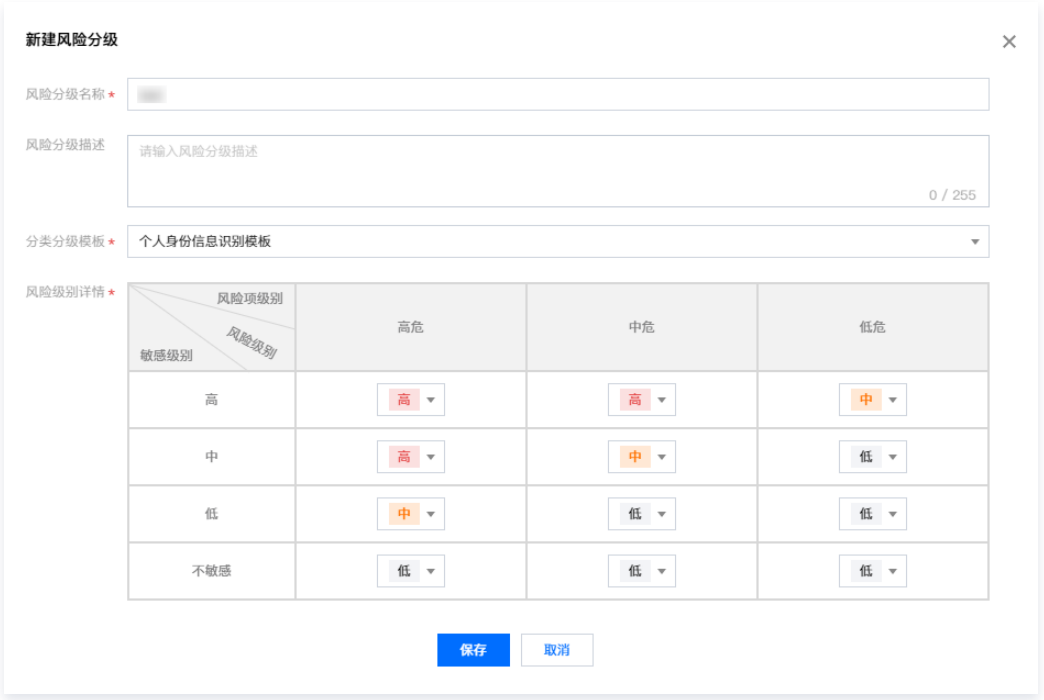
最近更新时间：2024-11-22 15:26:22

风险级别通过结合风险项等级与敏感数据等级进行配置，从而更精准地监测和识别高敏感数据的风险程度。帮助企业更好地识别潜在的风险，并采取相应的措施来降低风险。

新建风险级别

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **评估模板**。
3. 在评估模板页面，单击**风险级别** Tab 栏。
4. 在风险级别页面，单击**新建风险级别**。

5. 在新建风险级别窗口，输入风险分级基本信息，选择需要关联的分类分级识别模板，单击**保存**。



6. 完成新建后，系统将根据所选的分类分级模中板的分级信息，与系统内置的评估项风险项级别进行综合评估，并生成相应的风险级别。
7. 同时可以依据具体的业务场景、治理需求进行手动调整具体的风险级别。

删除风险级别

1. 在风险级别页面，选择需要删除的风险级别，单击操作栏中的**删除**。

2. 在确认删除窗口中，单击**确认删除**，即可删除风险级别。

> **说明：**
> - 仅允许删除自定义风险级别。
> - 若风险级别已关联风险评估模板，则不允许删除。
> - 删除将无法恢复，请谨慎操作！

评估模板

最近更新时间：2024-11-22 15:26:22

评估模板是由评估项和风险级别组成。在系统默认模板的基础上，您可以通过自定义创建评估模板，更好地满足企业的特定需求和业务场景。同时也可以提高评估的效率和准确性，为企业决策提供更可靠的依据。

新建模板

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**风险评估** > **评估模板**。
3. 在评估模板页面，单击**评估模板** Tab 栏。
4. 在评估模板页面，选择目标实例，单击 。

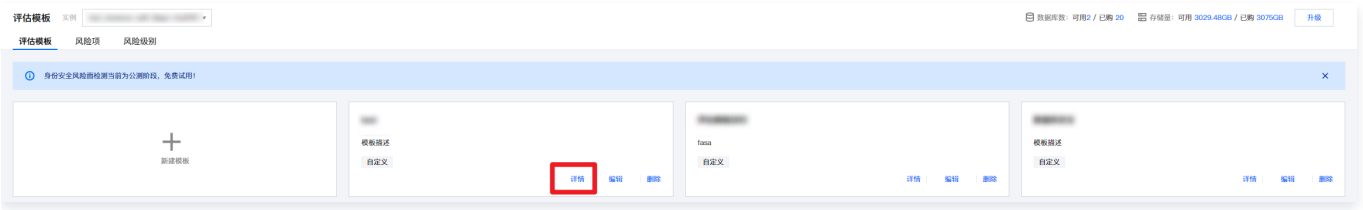
5. 在新建模板窗口中，输入评估模板名称、描述，并选择需要使用的风险分级模板。

6. 单击**绑定风险项**，选择所需脆弱项，单击**确定**。

7. 确认内容无误后，单击**保存**即可添加成功。

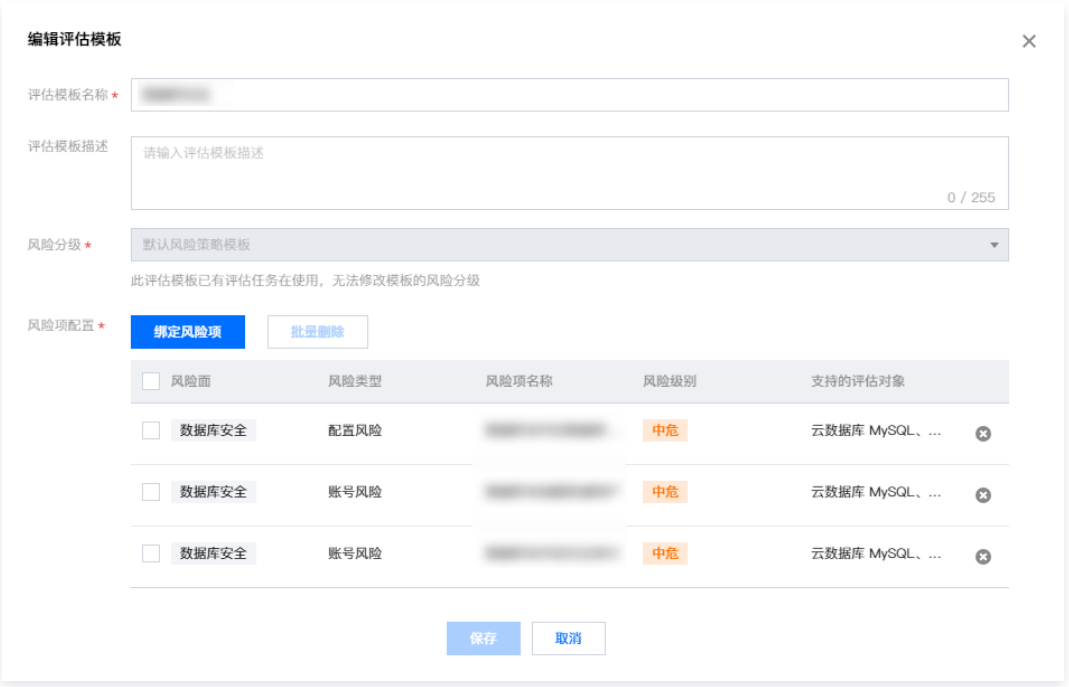
查看模板详情

在评估模板页面，选择需要查看详情的模板，单击**详情**即可查看评估模板的详情。



编辑模板

1. 在评估模板页面，选择需要编辑的模板，单击**编辑**。
2. 在编辑评估模板窗口中，可以修改模板名称、模板描述和脆弱项内容，单击**保存**。



> **注意：**
> - 若该模板还未被使用，则支持修改该模板的风险分级。
> - 若该模板已在评估任务中使用，则不支持修改模板中的风险分级。

删除模板

1. 在评估模板页面，选择需要删除的模板，单击**删除**。
2. 在确认删除窗口中，单击**确认**，将会删除该模板以及与该模板有关的所有信息。

> **注意：**
> - 模板被删除后无法恢复，请谨慎操作。
> - 若该评估模板已有评估任务在使用，则无法删除。

版权所有：腾讯云计算（北京）有限责任公司

报表中心
数据资产分布报告

最近更新时间：2024-11-22 15:26:22

报表中心为标准版功能，主要提供数据资产分布报告的在线预览和导出功能。不仅可以在线查看数据资产梳理报告，还可以将报告导出以便于离线查看或进一步的数据分析。

前置条件

- 已 购买数据安全治理中心实例 。
- 当前服务实例版本为标准版。
- 当前已同步/添加并授权数据资产，并开启数据治理，成功创建并执行了 分类分级任务 。

在线预览

1. 登录 数据安全治理中心的控制台 。
2. 在左侧导航栏中，单击**报表中心 > 报告管理**。
3. 在报告管理页面，单击**报告模板** Tab 栏。
4. 在报告模板页面，选择数据资产分布报告，单击**生成报告**。

5. 在生成报告页面，选择需要查看的资产类型、分类分级模板。

6. 单击**在线预览**，即可生成查看报表内容。

导出报表

1. 在生成报告页面，选择需要查看的资产类型、分类分级模板。
2. 单击**导出报告**，后可于 报告管理 页面进行报表的下载。

报告管理

最近更新时间：2024-11-22 15:26:22

您可以在报表管理页面对相关报表进行下载、删除等操作。

前置条件

- 已 购买数据安全治理中心实例 。
- 当前服务实例版本为标准版。
- 当前已同步/添加并授权数据资产，并开启数据治理，成功创建并执行了 分类分级任务 。
- 已 创建并导出资产梳理报告 。

下载报表

1. 登录 数据安全治理中心的控制台 。
2. 在左侧导航栏中，单击**报表中心** > **报告管理**。
3. 在报告管理页面，单击**报告记录** Tab 栏。
4. 在报告记录页面，详细的记录了报告导出记录。选择需要下载的报告记录，单击操作栏中的**下载**。

5. 在下载报告窗口中，您可以选择是否同时下载详情清单，单击**确定**。

> **说明：**
> 详细清单以 Excel 表格的形式记录了报告中的资产分布情况、分类分级项具体识别数量。

6. 下载完成后，报表文件将保存在您浏览器的默认下载路径中。

删除导出记录

1. 在报告记录页面，选择需要删除的报告记录，单击操作栏中的**删除**。

2. 在确认删除窗口，单击**确认**，即可删除导出记录。

> **说明：**
> 删除操作无法恢复，请谨慎操作。

告警通知

最近更新时间：2024-10-16 19:41:01

通过设置告警通知，您能够立即获悉相关的风险评估结果，有助于及时应对可能出现的数据安全风险，进而提高数据安全管理的效率和反应速度。

前置条件

- 已 购买数据安全治理中心实例 。
- 消息中心 已配置了“数据安全治理中心”的接收模式、接收渠道和接收人。

开启通知设置

1. 登录 数据安全治理中心控制台 。
2. 在左侧的导航栏中，单击**系统设置** > **通知设置**。
3. 在通知设置页面，单击操作栏中的 ，开启告警通知。

> **说明：**
> 请确认消息中心中为“数据安全治理中心”配置了接收模式、接收渠道和接收人，否则无法收到消息。前往设置 。

数据安全能力

最近更新时间：2024-11-22 15:26:22

数据安全审计

登录 数据安全治理中心控制台， 在左侧导航栏中，单击**数据安全能力** > **数据安全审计**，即跳转到数据安全审计控制台。

运维安全中心（堡垒机）

登录 数据安全治理中心控制台， 在左侧导航栏中，单击**数据安全能力** > **运维安全中心（堡垒机）**，即跳转到运维安全中心（堡垒机）控制台。

密钥管理

登录 数据安全治理中心控制台， 在左侧导航栏中，单击**数据安全能力** > **密钥管理**，即跳转到密钥管理系统控制台。

凭据管理

登录 数据安全治理中心控制台， 在左侧导航栏中，单击**数据安全能力** > **凭据管理**，即跳转到凭据管理系统控制台。

云加密机

登录 数据安全治理中心控制台， 在左侧导航栏中，单击**数据安全能力** > **云加密机**，即跳转到云加密机控制台。

版权所有：腾讯云计算（北京）有限责任公司

访问管理
服务角色授权

最近更新时间：2024-09-02 16:37:01

使用场景

在使用数据安全治理中心（DSGC）的过程中，会涉及到相关云资源的接口使用。为了您能正常使用 DSGC 的功能，您需要对 DSGC 的服务角色进行授权。授权后，DSGC 服务才能使用相关云资源。

前置条件

方案一：登录的腾讯云账号是主账号。
方案二：登录的腾讯云账号是子账号，且已绑定预设策略 QcloudCamSubaccountsAuthorizeRoleFullAccess。

初始授权

首次登录 DSGC 控制台 时，请按照指引完成服务角色的授权，如下图所示：

增加授权

已为 DSGC 的服务角色授权，使用新增功能时需为 DSGC 服务角色绑定新的预设策略，可通过如下方式为服务角色新增策略：

1. 在 访问管理-角色页面，检索 DSGC 服务角色 Dsgc_QcsRole，单击**角色名称**。

2. 在角色详情页的**权限** > **权限策略**中，您可以为角色关联新的预设策略：
   2.1 单击**关联策略**，勾选您想要给当前角色添加的策略。
   2.2 单击**确定**，完成编辑角色关联操作。

热点问题

子账号操作授权时，提示“无预设策略 QcloudCamSubaccountsAuthorizeRoleFullAccess 权限”？

只有拥有 QcloudCamSubaccountsAuthorizeRoleFullAccess 预设策略权限的账号才能为服务角色授权。如果没有此策略权限，请联系主账号或您的权限管理员，为您的子账号绑定该策略权限。
子账号绑定策略操作如下：
1. 单击控制台右上角**头像**，查看**子账号 ID**，告知您的主账号或权限管理员。

2. **主账号或权限管理员**，登录 CAM 控制台，进入 用户 管理页面。
3. 在用户列表页面，选择需要设置权限的子用户，单击右侧操作列的**授权**。

4. 在关联策略窗口中，勾选需要授权的策略 QcloudCamSubaccountsAuthorizeRoleFullAccess。

5. 单击**确定**，完成直接为子用户授权关联策略操作。

子账号权限管理

最近更新时间：2024-09-02 16:37:01

前置操作

创建子账号，具体操作可参见文档：创建子账号并授权 。

为子账号配置“DSGC 服务读写权限”

子账号访问 DSGC 服务需要具备 DSGC服 务的相关权限，您可在腾讯云主账号中通过设置策略的方式来对子账号的权限进行管理，实现对子账号可访问资源和可使用功能进行管理。

1. 登录 CAM 访问控制台，进入 用户列表 页面。
2. 在用户列表管理页面，选择需要设置权限的子用户，单击右侧操作列的**授权**。
3. 在弹出的关联策略窗口里勾选需要授权的策略（可多选），单击**确定**，完成直接为子用户授权关联策略操作。

> **说明：**
> 数据安全治理中心（DSGC）提供**如下两个预设策略**，您可直接使用，也可选择 自定义权限策略 。

策略名称	策略说明
QcloudDSGCFullAccess	数据安全治理中心（DSGC）全读写访问
QcloudDSGCReadOnlyAccess	数据安全治理中心（DSGC）只读访问权限

给子账号配置“服务角色授权权限”

初次使用 DSGC 服务，子账号操作 服务角色授权 失败，提示“无预设策略 QcloudCamSubaccountsAuthorizeRoleFullAccess 权限”。

1. 单击控制台右上角**头像**，查看**子账号 ID**，告知您的主账号或权限管理员。

2. **主账号或权限管理员**，登录 CAM 控制台，进入 用户 管理页面。
3. 在用户列表页面，选择需要设置权限的子用户，单击右侧操作列的**授权**。
4. 在关联策略窗口中，勾选需要授权的策略 QcloudCamSubaccountsAuthorizeRoleFullAccess。
5. 单击**确定**，完成直接为子用户授权关联策略操作。

如何为子账号授予更多权限

由于不同使用场景下对子账号的资源访问限制各不相同，在后续操作过程中，如果您需要对子账号授予更多权限，请参见 如何根据无权限信息创建权限策略 更新子账号权限策略。