

BigQuery Data Security & Compliance

访问控制

详细文档: <https://cloud.google.com/bigquery/docs/access-control>

这个非常直观, 就不在这里赘述了。需要注意的一个最佳实践就是, 避免直接给一个对象(人, 组)授权, 而是一个Role(角色)授权, 然后把role赋予一个对象。

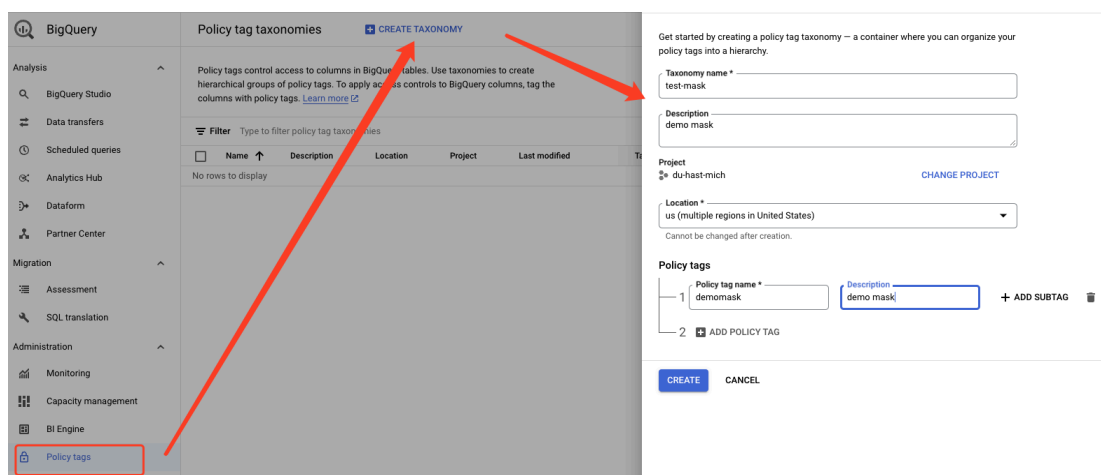
数据遮盖

BigQuery数据遮盖: <https://cloud.google.com/bigquery/docs/column-data-masking-intro>

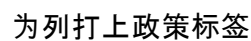
这块区别于访问控制, 需要[打开额外两个API](#)

- Google Cloud Data Catalog API
- BigQuery Data Policy API

这里用通过policy tag(政策标签)来控制



添加政策权限



gcp_billing_export_resource_v1_010B7A_A27129_D37860

QUERY SHARE COPY SNAPSHOT

SCHEMA DETAILS PREVIEW TABLE EXPLORER LINEAGE DATA PROFILE DATA QUALITY

Filter Enter property name or value

	Field name	Type	Mode	Key	Collation	Default Value	Policy Tags	Description
<input type="checkbox"/>	billing_account_id	STRING	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	▶ service	RECORD	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	▶ sku	RECORD	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	usage_start_time	TIMESTAMP	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	usage_end_time	TIMESTAMP	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	▶ project	RECORD	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	▶ labels	RECORD	REPEATED	-	-	-	-	-
<input type="checkbox"/>	▶ system_labels	RECORD	REPEATED	-	-	-	-	-
<input type="checkbox"/>	▶ location	RECORD	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	▶ resource	RECORD	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	export_time	TIMESTAMP	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	cost	FLOAT	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	currency	STRING	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	currency_conversion_rate	FLOAT	NULLABLE	-	-	-	-	-
<input type="checkbox"/>	usage	RECORD	NULLABLE	-	-	-	-	-
<input checked="" type="checkbox"/>	amount	FLOAT	NULLABLE	-	-	-	test-mask : billing	-
<input type="checkbox"/>	unit	STRING	NULLABLE	-	-	-	-	-

给对象添加可以访问数据的角色，角色具有相应权限

Policy tag taxonomy

test-mask

demo mask

Policy tags

2

Enforce access control

Access to BigQuery columns tagged with the policy tags below will be restricted to users with the Fine-Grained Reader and the Masked Reader roles.

Metadata

Policy tag taxonomy ID: 4051703264058646455

Created: Mar 12, 2024, 10:58:46 AM

Modified: Mar 12, 2024, 11:02:46 AM

Project ID: du-hast-misch

Project display name: du-hast-misch

Location: us (multiple regions in United States)

Policy tags

Policy tags are tags with access control policies that can be applied to sub-resources, for example, BigQuery columns.

MANAGE DATA POLICIES

Name	ID	Data Masking Rules	Description
demo mask	8922229698300806395		demo mask
billing	5518167872806670343		billing sensitive data

billing

Edit or delete permissions below, or select "Add Principal" to grant new access.

Show inherited permissions

Filter Enter property name or value

Role / Principal

Editor (6)

Fine-Grained Reader (1)

binwu@google.com

Owner (3)

Viewer (3)

授权后可以正常访问

gcp_billing_export_resource_v1_010B7A_A27129_D37860

QUERY

SHARE

COPY

SNAPSHOT

DELETE

This is a partitioned table. [Learn more](#)

SCHEMA	DETAILS	PREVIEW	TABLE EXPLORER	LINEAGE	DATA PROFILE	DATA QUALITY		
<input type="checkbox"/>	▶ service		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	▶ sku		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	usage_start_time		TIMESTAMP	NULLABLE	-	-	-	-
<input type="checkbox"/>	usage_end_time		TIMESTAMP	NULLABLE	-	-	-	-
<input type="checkbox"/>	▶ project		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	▶ labels		RECORD	REPEATED	-	-	-	-
<input type="checkbox"/>	▶ system_labels		RECORD	REPEATED	-	-	-	-
<input type="checkbox"/>	▶ location		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	▶ resource		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	export_time		TIMESTAMP	NULLABLE	-	-	-	-
<input type="checkbox"/>	cost		FLOAT	NULLABLE	-	-	-	-
<input type="checkbox"/>	currency		STRING	NULLABLE	-	-	-	-
<input type="checkbox"/>	currency_conversion_rate		FLOAT	NULLABLE	-	-	-	-
<input type="checkbox"/>	▼ usage		RECORD	NULLABLE	-	-	-	-
<input type="checkbox"/>	amount		FLOAT	NULLABLE	-	-	-	test-mask : billing
<input type="checkbox"/>	unit		STRING	NULLABLE	-	-	-	-
<input type="checkbox"/>	amount_in_pricing_units		FLOAT	NULLABLE	-	-	-	-
<input type="checkbox"/>					-	-	-	-

添加遮盖逻辑

Policy tag taxonomy

test-mask

demo mask

Policy tags

2

Enforce access control

Access to BigQuery columns tagged with the policy tags below will be restricted to users with the Fine-Grained Reader and the Masked Reader roles.

Metadata

Policy tag taxonomy ID 4051703264058646455

Created Mar 12, 2024, 10:58:46 AM

Modified Mar 12, 2024, 11:02:46 AM

Project ID du-hast-mich

Project display name du-hast-mich

Location us (multiple regions in United States)

Policy tags

Policy tags are tags with access control policies that can be applied to sub-resources, for example, BigQuery columns.

MANAGE DATA POLICIES

Name	ID	Data Masking Rules	Description
demomask	8922329698300806335		demo mask
billing	5518167872806670343		billing sensitive data

Masking Rules

Choose a masking rule, then select principals that the rule would apply to.

Data Policy Name 1 * mask

Masking Rule 1 * Hash (SHA256)

+ ADD RULE

SUBMIT CANCEL

授权给用户可以看到遮盖后数据

binwu@google.com

Role

Masked Reader

Masked read access to sub-resources tagged by the policy tag associated with a data policy, for example, BigQuery columns

IAM condition (optional)

+ ADD IAM CONDITION

Query results			
JOB INFORMATION		RESULTS	CHART
Row	billing_account_id	amount	
1	010B7A-A27129-D37860	0.0	被遮盖用户看到的
2	010B7A-A27129-D37860	0.0	
3	010B7A-A27129-D37860	0.0	
4	010B7A-A27129-D37860	0.0	
5	010B7A-A27129-D37860	0.0	
6	010B7A-A27129-D37860	0.0	
7	010B7A-A27129-D37860	0.0	
8	010B7A-A27129-D37860	0.0	
9	010B7A-A27129-D37860	0.0	
10	010B7A-A27129-D37860	0.0	

JOB INFORMATION		RESULTS	CHART	JSON	EXECUTION DETAILS	EX
Row	billing_account_id	amount				
1	010B7A-A27129-D37860	2654.0	有权限用户看到的			
2	010B7A-A27129-D37860	107954.0				
3	010B7A-A27129-D37860	966.0				
4	010B7A-A27129-D37860	2651.0				
5	010B7A-A27129-D37860	1056.0				
6	010B7A-A27129-D37860	28338.0				
7	010B7A-A27129-D37860	1349.0				
8	010B7A-A27129-D37860	948.0				
9	010B7A-A27129-D37860	101748.0				
10	010B7A-A27129-D37860	36281.0				

DLP

开通DLP API

REST API: <https://cloud.google.com/sensitive-data-protection/docs/reference/rest>

这里理论上可以使用rest或者client lib来做线下或者实时检查

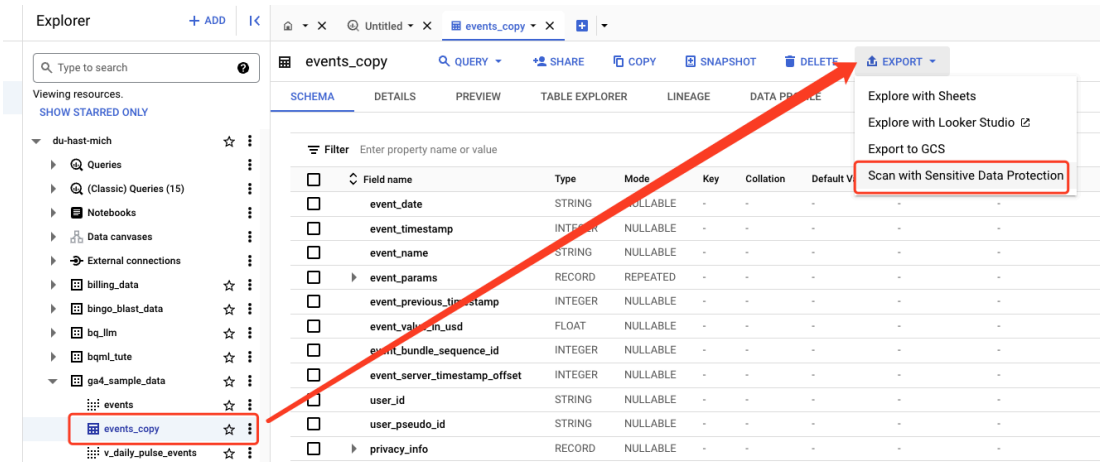
```

Python
client = bigquery.Client()
datasets = list(client.list_datasets(project=project_id))

if datasets:
    for dataset in datasets:
        tables = client.list_tables(dataset.dataset_id)
        for table in tables:
            #调用API 抽样检查数据 识别风险列

```

BQ里可以相对简单的扫描已有数据



用程序读取Pub/sub, 并且定期轮换密码/key

用程序 (dataflow) 读取pubsub:

<https://cloud.google.com/pubsub/docs/stream-messages-dataflow>

pubsub 也有丰富的SDK: <https://cloud.google.com/pubsub/docs/reference/libraries>

SA key rotation: <https://cloud.google.com/iam/docs/key-rotation>

附录

1, BQ目前有三个版本, Data masking等功能在Enterprise以上版本中提供支持

如下图所示: ([link](#))

	BigQuery editions			On-demand pricing
	Standard	Enterprise	Enterprise Plus	
Pricing model	Slot-hours (1 minute minimum)	Slot-hours (1 minute minimum)	Slot-hours (1 minute minimum)	Pay per query with free tier
Compute model	Autoscaling	Autoscaling + Baseline	Autoscaling + Baseline	On-demand
Fine-grained security controls	No access to fine-grained security controls	Column-level access control	Column-level access control	Column-level access control
		Row-level security	Row-level security	Row-level security
		Dynamic data masking	Dynamic data masking	Dynamic data masking
			Custom data masking	Custom data masking

因此，为了进行详细的权限管理和Masking需要采用Enterprise edition，虽然在成本方面Enterprise高于Standard，但通过合理规划可以避免成本明显增长，

- 在测试评估阶段，建议采用enterprise - pays as you go模式，这阶段查询较少因此不会产生过多费用
- 将来上了生产环境，建议采用enterprise-commit (1yr/3yr)模式，成本相较于目前的standard - pay as you go模式不会明显增长

同时，目前的测试建议在单独project进行，不影响生产系统采用的计费模式。

Standard和Enterprise editions的价格说明：[\(link\)](#)

Standard Edition

The following table shows the cost of slots in Standard edition.

US (us) ▾		
Commitment model	Hourly cost	Details
Pay as you go	\$0.04 / slot hour	No commitment. Billed per second with a 1 minute minimum

Enterprise Edition

The following table shows the cost of slots in Enterprise edition.

US (us) ▾		
Commitment model	Hourly cost	Details
Pay as you go	\$0.06 / slot hour	Billed per second with a 1 minute minimum
1 yr commit	\$0.048 / slot hour	Billed for 1 year
3 yr commit	\$0.036 / slot hour	Billed for 3 years