

1.数据库导出的过程和权限

基本过程是:

- 创建bucket
- 把服务关联的sa账号关联到bucket上
- 实现export操作

MemoryStore和Cloud Sql的导出的操作,是通过服务本身关联的一个service account来向指定的bucket中写入rdb文件或者sql文件, 所以从权限角度来看需要给sa账号授权.

如果在console界面操作,并且登录的user account是一个owner权限的话, 会自动给gcs的bucket添加一个对应sa账号的写入权限,类似以下日志记录的信息

- Cloud sql backup 操作

```
{
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "status": {},
    "authenticationInfo": {
      "principalEmail": "liuchenggang@google.com"
    },
    "requestMetadata": {
      "callerIp": "2401:fa00:44:11:8034:1ffe:433b:d4b0",
      "callerSuppliedUserAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36",
      "requestAttributes": {
        "time": "2020-08-13T07:52:26.743596142Z",
        "auth": {}
      },
      "destinationAttributes": {}
    },
    "serviceName": "storage.googleapis.com",
    "methodName": "storage.setIamPermissions",
    "authorizationInfo": [
      {
        "resource": "projects/_/buckets/cliu101_cloudsql_backup",
        "permission": "storage.buckets.setIamPolicy",
        "granted": true,
        "resourceAttributes": {}
      }
    ],
    "resourceName": "projects/_/buckets/cliu101_cloudsql_backup",
    "serviceData": {
```

```

    "@type": "type.googleapis.com/google.iam.v1.logging.AuditData",
    "policyDelta": {
      "bindingDeltas": [
        {
          "action": "ADD",
          "role": "roles/storage.legacyBucketReader",
          "member":
"serviceAccount:p576354374575-zvs1cw@gcp-sa-cloud-sql.iam.gserviceaccount.com"
        },
        {
          "action": "ADD",
          "role": "roles/storage.objectAdmin",
          "member":
"serviceAccount:p576354374575-zvs1cw@gcp-sa-cloud-sql.iam.gserviceaccount.com"
        }
      ]
    },
    "resourceLocation": {
      "currentLocations": [
        "us"
      ]
    },
    "insertId": "tov4oae4urp8",
    "resource": {
      "type": "gcs_bucket",
      "labels": {
        "location": "us",
        "project_id": "cliu101",
        "bucket_name": "cliu101_cloudsql_backup"
      }
    },
    "timestamp": "2020-08-13T07:52:26.736945754Z",
    "severity": "NOTICE",
    "logName": "projects/cliu101/logs/cloudaudit.googleapis.com%2Factivity",
    "receiveTimestamp": "2020-08-13T07:52:28.026464719Z"
  }
}

```

可以在bucket的权限里面看到

Access control

Uniform: No object-level ACLs enabled
90 days left to change this setting

All object access is controlled by bucket permissions and objects cannot have their own access control lists (ACLs). To allow per-object access, you can switch to fine-grained access within 90 days. [Learn more](#)

SWITCH TO FINE-GRAINED

Public access

Not public

This bucket is not shared publicly and uniform bucket-level access is enabled. To ensure that the bucket's data does not become public, do not add `allUsers` or `allAuthenticatedUsers` as members.

Permissions

ADD

REMOVE

View By:

MEMBERS

ROLES

Filter table

Type	Member	Name	Role	Inheritance
	576354374575@cloudbuild.gserviceaccount.com		Cloud Build Service Account	cliu101
	Editors of project: cliu101		Storage Legacy Bucket Owner Storage Legacy Object Owner	
	Owners of project: cliu101		Storage Legacy Bucket Owner Storage Legacy Object Owner	
	p576354374575-zvs1cw@gcp-sa-cloud-sql.iam.gserviceaccount.com		Storage Legacy Bucket Reader Storage Object Admin	
	service-576354374575@cloud-ml.google.com.iam.gserviceaccount.com	Google Cloud ML Engine Service Agent for Project 576354374575	Cloud ML Service Agent	cliu101
	service-576354374575@cloudcomposer-accounts.iam.gserviceaccount.com	Cloud Composer Service Agent for Project 576354374575	Cloud Composer API Service Agent	cliu101
	service-576354374575@dataflow-service-producer-prod.iam.gserviceaccount.com	Cloud Dataflow Service Account for Project 576354374575	Cloud Dataflow Service Agent	cliu101
	service-576354374575@dataproc-accounts.iam.gserviceaccount.com	Google Cloud Dataproc Service Agent for Project 576354374575	Dataproc Service Agent	cliu101
	service-576354374575@firebase-rules.iam.gserviceaccount.com	Firebase Rules Service Agent for Project 576354374575	Firebase Rules System	cliu101
	service-576354374575@gcp-sa-automl.iam.gserviceaccount.com	AutoML Service Agent for Project 576354374575	AutoML Service Agent	cliu101
	service-576354374575@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Account for Project 576354374575	Cloud Build Service Agent	cliu101
	service-576354374575@gcp-sa-datafusion.iam.gserviceaccount.com	Cloud Data Fusion Service Account for Project 576354374575	Cloud Data Fusion API Service Agent	cliu101
	service-576354374575@serverless-robot-prod.iam.gserviceaccount.com	Google Cloud Run Service Agent for Project 576354374575	Cloud Run Service Agent	cliu101
	Viewers of project: cliu101		Storage Legacy Bucket Reader Storage Legacy Object Reader	

2.cloud sql和memory store关联的sa账号

cloud sql关联的sa账号,在cloud sql的instance上可以直接获取

SQL

Overview
[EDIT](#)
[IMPORT](#)
[EXPORT](#)
[RESTART](#)
[STOP](#)
[DELETE](#)

MASTER INSTANCE

[Overview](#)
[Connections](#)
[Users](#)
[Databases](#)
[Backups](#)
[Replicas](#)
[Operations](#)
[Corp Access](#)

Private IP address

192.168.0.3

Associated networking

projects/cliu101/global/networks/vpc101

Connection name

cliu101:us-east1:cliu

[Connect using Cloud Shell](#)

[Connect from a Compute Engine VM instance](#)

[See all connection methods](#)

Suggested actions

[Enable high availability](#)

Service account

p576354374575-zvs1cw@gcp-sa-cloud-sql.iam.gserviceaccount.com

Memory store的instance关联的sa账号必须通过gcloud命令获取,界面上无法获取

```
gcloud redis instances describe [INSTANCE_ID] --region=[REGION]
```

```
[root@mhhtw-test01-tw ~]# gcloud redis instances export gs://mhhtw-redis-backup/test01.rdb --region=asia-east1 mhhtw-game01-gcp-taipei
Request issued for: [mhhtw-game01-gcp-taipei]
Waiting for operation [projects/mhhtw-273808/locations/asia-east1/operations/operation-1597384719344-5acbd7c65038d-27be0278-9f0b6244] to complete...done.
alternativeLocationId: asia-east1-a
authorizedNetwork: projects/mhhtw-273808/global/networks/mhhtw
connectMode: DIRECT_PEERING
createTime: '2020-08-11T06:34:29.898819738Z'
currentLocationId: asia-east1-b
host: 10.106.53.204
locationId: asia-east1-b
memorySizeGb: 8
name: projects/mhhtw-273808/locations/asia-east1/instances/mhhtw-game01-gcp-taipei
persistenceIamIdentity: serviceAccount:555884415706-compute@developer.gserviceaccount.com
port: 6379
redisVersion: REDIS_4_0
reservedIpRange: 10.106.53.200/29
state: READY
tier: STANDARD_HA
[root@mhhtw-test01-tw ~]#
```

参考文档

3.常见问题

客户如果第一次创建export任务是在一个gce的vm上, 往往会关联一个默认的sa账号,这个账号往往是一个editor 权限,没有IAM的能力,就会报错

常见的解决方法有两个

- 通过owner先创建一个export任务,建议直接使用console来操作,这样就会自动为关联的sa账对bucket授权
- 后面的自动化备份或者导出的时候使用gcloud命令+最低权限的sa来实现