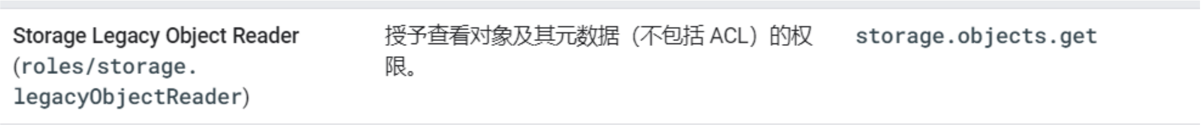
GCS object 精细控制实现访问限定目录

Created	@May 5, 2022 1:58 PM
Tags	
Modify Date	
Description	
Link	

创建一个Service Account 授予VM，

```
# Service Account 未授予任何权限
$ gsutil list
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com
does not have storage.buckets.list access to the Google Cloud project.
```

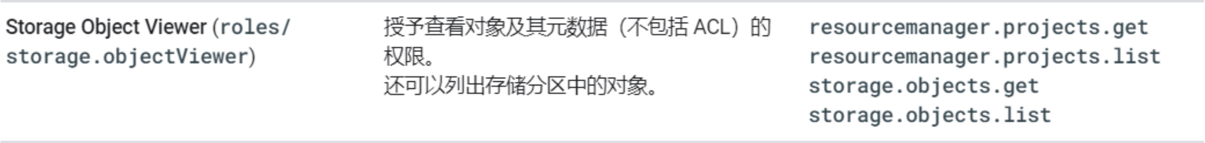
只授予 Service account 权限：



Storage Legacy Object Reader (roles/storage.legacyObjectReader)	授予查看对象及其元数据（不包括 ACL）的权限。	storage.objects.get

```
## 查看项目下的Bucket, 403
$ gsutil list
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.buckets.list access to the Goo
## 查询指定Bucket下的object
$ gsutil ls gs://access-bucket-permission
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo
```

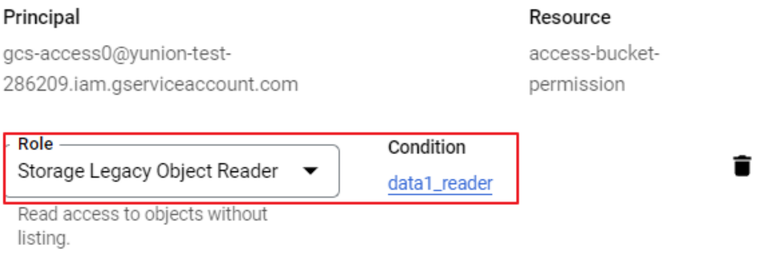
只授予



Storage Object Viewer (roles/storage.objectViewer)	授予查看对象及其元数据（不包括 ACL）的权限。 还可以列出存储分区中的对象。	resourcemanager.projects.get resourcemanager.projects.list storage.objects.get storage.objects.list

配置只允许指定Service Account 获取指定目录下的文件：

1、给SA 【**Storage Legacy Object Reader**】权限



Principal	Resource
gcs-access0@yunion-test-286209.iam.gserviceaccount.com	access-bucket-permission

Role: Storage Legacy Object Reader

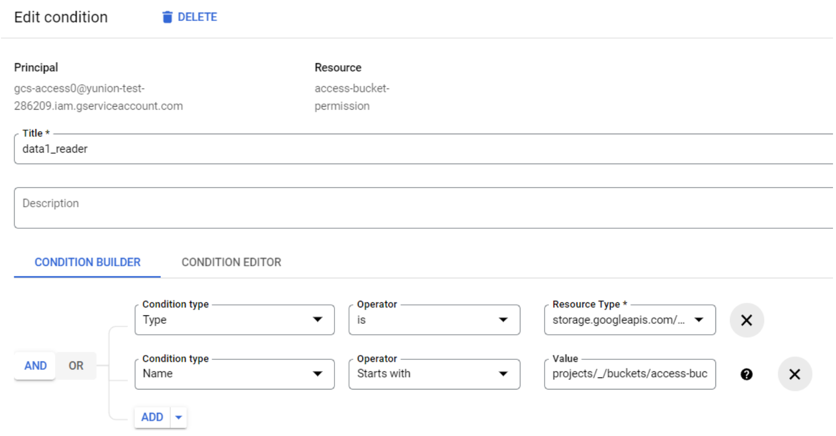
Read access to objects without listing.

Condition: data1_reader

2、针对用户该角色配置条件访问：

Cloud Storage 存储分区[1]	`projects/_/buckets/bucket-name`
Cloud Storage 对象[1]、[2]	`projects/_/buckets/bucket-name/objects/object-name`

资源格式参考：



Edit condition

Principal
gcs-access0@yunion-test-286209.iam.gserviceaccount.com

Resource
access-bucket-permission

Title *
data1_reader

Description

Condition type: Type | Operator: is | Resource Type *: storage.googleapis.com/...

Condition type: Name | Operator: Starts with | Value: projects/_/buckets/access-buc

```
resource.type == "storage.googleapis.com/Object" &&
resource.name.startsWith("projects/_/buckets/BUCKENT_NAME/objects/PATH")

# 允许用户访问 access-bucket-permission Bucket 下的data1/data10 下的文件
BUCKET_NAME: access-bucket-permission
PATH [Object path]: data1/data10
如：
## resource.name.startsWith("projects/_/buckets/access-bucket-permission/objects/data1/data10")
```

3、测试访问：

```
# 测试从 bucket下的/data1/data10/ 获取指定对象，获取Object 成功
root@gcs-access:~#  gsutil cp gs://access-bucket-permission/data1/data10/http.cap ./
Copying gs://access-bucket-permission/data1/data10/http.cap...
/ [1 files][ 11.8 KiB/ 11.8 KiB]
Operation completed over 1 objects/11.8 KiB.

# 测试从 bucket下的非/data1/data10/ 获取指定文件，获取对象失败
root@gcs-access:~#  gsutil cp gs://access-bucket-permission/http.cap ./
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo


测试向Bucket 下添加文件，结果失败
# gsutil cp gcs-0.txt gsutil cp gs://access-bucket-permission/
Copying file://gcs-0.txt [Content-Type=text/plain]...
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.create access to the G

测试向Bucket 下/data1/data10/添加文件，结果失败
# gsutil cp gcs-0.txt gsutil cp gs://access-bucket-permission/data1/data10/
Copying file://gcs-0.txt [Content-Type=text/plain]...
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.create access to the G

## 测试获取Bucket 下/data2/data20/对象，结果失败
#  gsutil cp gs://access-bucket-permission/data2/data20/http.cap ./
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo

## 测试获取Bucket 下/data1/data11/ 对象，结果失败
#  gsutil cp gs://access-bucket-permission/data1/data11/http.cap ./
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo
```

只允许用户上传对象：

```
# gsutil cp gcs-0.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-0.txt [Content-Type=text/plain]...
```

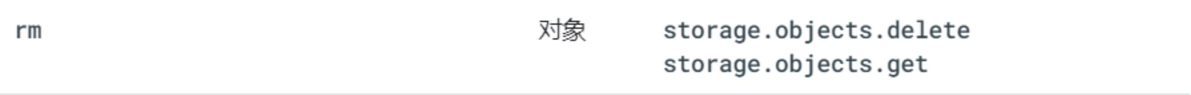
```
/ [1 files][    5.0 B/    5.0 B]
Operation completed over 1 objects/5.0 B.
```

授予【**Storage Legacy Bucket Writer**】只允许用户上传文件；

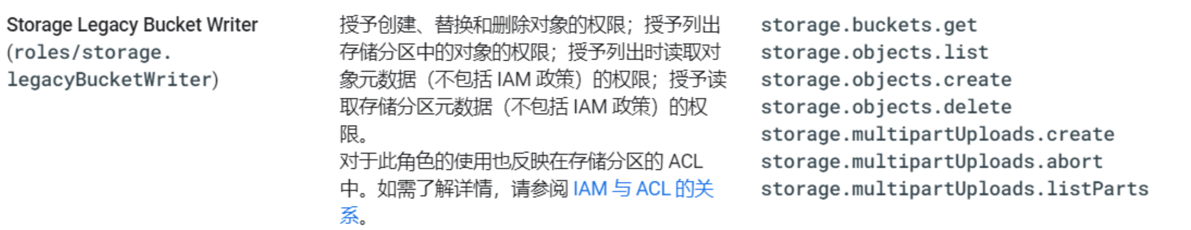
测试：上传新对象文件进行覆盖原有同名旧对象文件：

```
## 从本地上传文件到GCS 指定目录成功
root@gcs-access:~# gsutil cp gcs-0.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-0.txt [Content-Type=text/plain]...
/ [1 files][    5.0 B/    5.0 B]
Operation completed over 1 objects/5.0 B.

## 更新本地文件
root@gcs-access:~# echo 2222 >> gcs-0.txt
root@gcs-access:~# cat gcs-0.txt
hhhh
2222

对GCS 目录下Object 文件进行覆盖上传：
root@gcs-access:~# gsutil cp gcs-0.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-0.txt [Content-Type=text/plain]...
/ [1 files][   10.0 B/   10.0 B]
Operation completed over 1 objects/10.0 B.

## 删除本地文件
root@gcs-access:~# rm -rf gcs-0.txt

## 获取GCS 对象文件到本地，
root@gcs-access:~# gsutil cp gs://access-bucket-permission/data1/data10/gcs-0.txt ./
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo

root@gcs-access:~# gsutil cp gs://access-bucket-permission/data1/data10/gcs-0.txt ./
Copying gs://access-bucket-permission/data1/data10/gcs-0.txt...
/ [1 files][   10.0 B/   10.0 B]
Operation completed over 1 objects/10.0 B.
root@gcs-access:~# cat gcs-0.txt
hhhh
2222
```

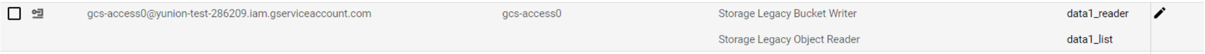
允许用户删除特定目录下对象文件【需要有特定目录下的】：



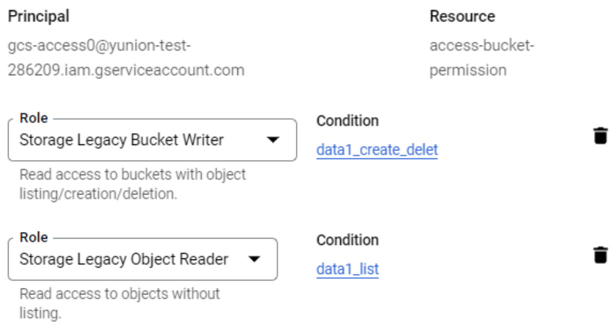
`rm`	对象	`storage.objects.delete` `storage.objects.get`



Storage Legacy Bucket Writer
(`roles/storage.legacyBucketWriter`)
	授予创建、替换和删除对象的权限；授予列出存储分区中的对象的权限；授予列出时读取对象元数据（不包括 IAM 政策）的权限；授予读取存储分区元数据（不包括 IAM 政策）的权限。
	对于此角色的使用也反映在存储分区的 ACL 中。如需了解详情，请参阅 IAM 与 ACL 的关系。
		`storage.buckets.get`
		`storage.objects.list`
		`storage.objects.create`
		`storage.objects.delete`
		`storage.multipartUploads.create`
		`storage.multipartUploads.abort`
		`storage.multipartUploads.listParts`



☐ gcs-access0@yunion-test-286209.iam.gserviceaccount.com	gcs-access0	Storage Legacy Bucket Writer Storage Legacy Object Reader	data1_reader data1_list



Principal
gcs-access0@yunion-test-286209.iam.gserviceaccount.com

Resource
access-bucket-permission

Role: Storage Legacy Bucket Writer
Read access to buckets with object listing/creation/deletion.
Condition: data1_create_delet

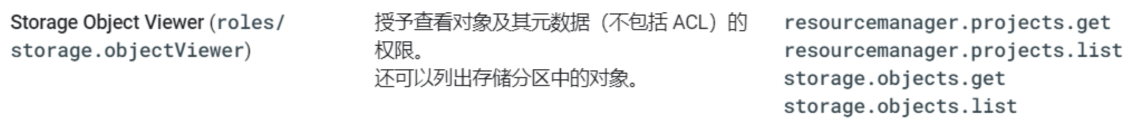
Role: Storage Legacy Object Reader
Read access to objects without listing.
Condition: data1_list

Question：

```
目前授予用户Storage Legacy Bucket Writer[storage.buckets.get、
storage.objects.list、storage.objects.create、storage.objects.delete]]权限后，
用户使用gsutil 提示403 error，并且提示缺少 storage.objects.list，然后我追加
[Storage Legacy Bucket Reader:storage.buckets.get、storage.objects.list、
storage.multipartUploads.list]权限后，依然提示如下错误：


# gsutil rm gs://access-bucket-permission/data1/data10/gcs-0.txt
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com
  does not have storage.objects.list access to the Google Cloud Storage bucket.

解决方式：
  授予 Storage Legacy Bucket Writer 、Storage Legacy Object Reader 即可，gsutil  rm 需要
  storage.objects.delete 、  storage.objects.get
```

使用预定义角色控制用户访问指定对象目录下操作权限：

1、获取指定目录下对象文件：

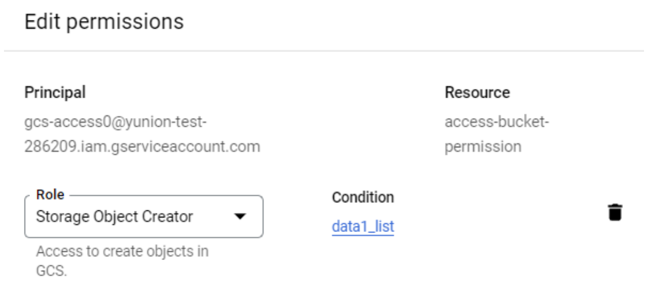


Storage Object Viewer (`roles/storage.objectViewer`)	授予查看对象及其元数据（不包括 ACL）的权限。
	还可以列出存储分区中的对象。
		`resourcemanager.projects.get`
		`resourcemanager.projects.list`
		`storage.objects.get`
		`storage.objects.list`

```
# 查看对象目录下的对象，失败，没有对bucket的list 权限
# gsutil ls  gs://access-bucket-permission/data1/data10/
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.list access to the Goo

# 查看对象目录下http.cap 对象文件
root@gcs-access:~# gsutil ls  gs://access-bucket-permission/data1/data10/http.cap
gs://access-bucket-permission/data1/data10/http.cap

# gsutil du -sh  gs://access-bucket-permission/data1/data10/http.cap
11.77 KiB    gs://access-bucket-permission/data1/data10/http.cap

测试删除对象文件，提示失败
# gsutil cp gcs-0.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-0.txt [Content-Type=text/plain]...
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com does not have storage.objects.create access to the G
```

1、指定目录下上传对象文件，如果对象存在则覆盖：

1.1 上传新的对象文件：



Edit permissions

Principal
gcs-access0@yunion-test-286209.iam.gserviceaccount.com

Resource
access-bucket-permission

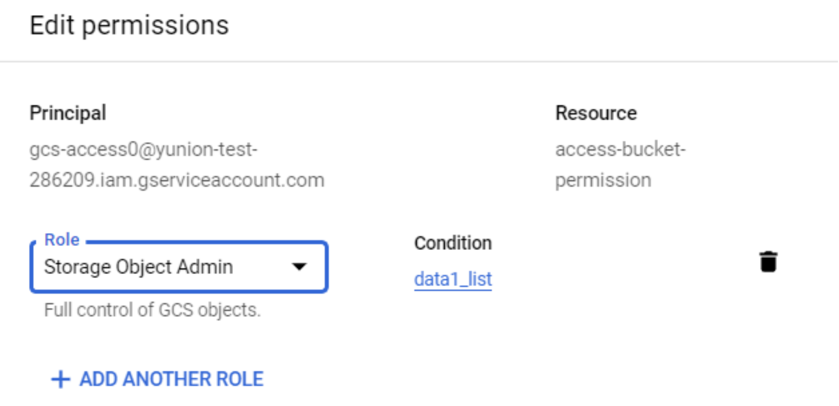
Role
Storage Object Creator
Access to create objects in GCS.

Condition
data1_list

```
# gsutil cp gcs-1.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-1.txt [Content-Type=text/plain]...
/ [1 files][    7.0 B/    7.0 B]
Operation completed over 1 objects/7.0 B.

再次上传同名文件，提示没有delete 权限，意味GCS上传同名object先删除原有的在创建新的object：
```

```
# gsutil cp gcs-1.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-1.txt [Content-Type=text/plain]...
AccessDeniedException: 403 gcs-access0@yunion-test-286209.iam.gserviceaccount.com
does not have storage.objects.delete access to the Google Cloud Storage object.
```

1.2 上传同名对象文件覆盖原有object 文件：


Edit permissions

Principal
gcs-access0@yunion-test-286209.iam.gserviceaccount.com

Resource
access-bucket-permission

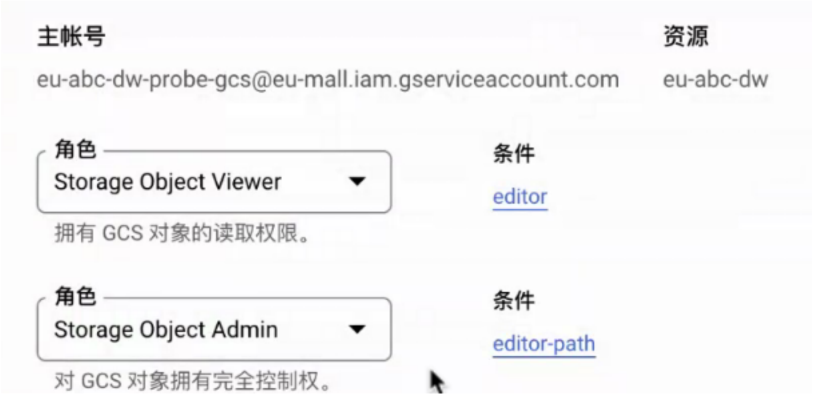
Role: Storage Object Admin
Full control of GCS objects.

Condition
data1_list

```
更新源文件后上传并覆盖原有的同名文件：
# echo aaaaa >> gcs-1.txt
root@gcs-access:~# gsutil cp gcs-1.txt gs://access-bucket-permission/data1/data10/
Copying file://gcs-1.txt [Content-Type=text/plain]...
/ [1 files][   13.0 B/   13.0 B]
Operation completed over 1 objects/13.0 B.


测试删除对象文件：
# gsutil rm gs://access-bucket-permission/data1/data10/gcs-1.txt
Removing gs://access-bucket-permission/data1/data10/gcs-1.txt...
/ [1 objects]
Operation completed over 1 objects.

测试获取对象文件：
# gsutil cp gs://access-bucket-permission/data1/data10/gcs-0.txt ./
Copying gs://access-bucket-permission/data1/data10/gcs-0.txt...
/ [1 files][   10.0 B/   10.0 B]
Operation completed over 1 objects/10.0 B.
```

角色	说明	权限	备注
Storage Object Creator (roles/storage.objectCreator)	允许用户创建对象，不提供查看、删除或替换对象的权限。	orgpolicy.policy.getr esourcemanager.projects.get resourcemanager.projects.list storage.objects.create storage.multipartUploads.create storage.multipartUploads.abort storage.multipartUploads.listParts	上传新对象文件，不可以上传同名文件
Storage Object Viewer (roles/storage.objectViewer)	授予查看对象及其元数据（不包括 ACL）的权限。还可以列出存储分区中的对象。	resourcemanager.projects.get resourcemanager.projects.list storage.objects.get storage.objects.list	下载对象文件
Storage Object Admin (roles/storage.objectAdmin)	授予对象的完全控制权，包括列出、创建、查看和删除对象。	orgpolicy.policy.get resourcemanager.projects.get resourcemanager.projects.list storage.objects.* storage.multipartUploads.*	上传新对象文件、上传同名对象文件、下载对象文件、删除对象文件

Bucket 默认从层级IAM 授权继承的权限：



主帐号 eu-abc-dw-probe-gcs@eu-mall.iam.gserviceaccount.com

资源 eu-abc-dw

角色 Storage Object Viewer

拥有 GCS 对象的读取权限。

条件 editor

角色 Storage Object Admin

对 GCS 对象拥有完全控制权。

条件 editor-path

参考：

[1] **Cloud Storage 的 IAM 角色**

[2] **IAM Conditions 的特性参考文档**