使用GCS Uniform bucket-level + Conditional IAM 控制bucket
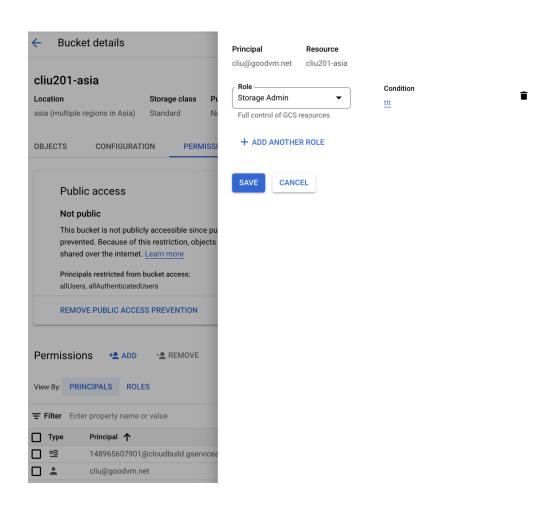
使用场景:

一个bucket内的不同folder(prefix)下, 需要设置不同用户的访问权限

1.在bucket层面打开"Uniform bucket-level access"

2.给目标user创建基于resource.name的访问权限

Edit condition 🗑 DELETE

Principal   **Resource**

cliu@goodvm.net   cliu201-asia
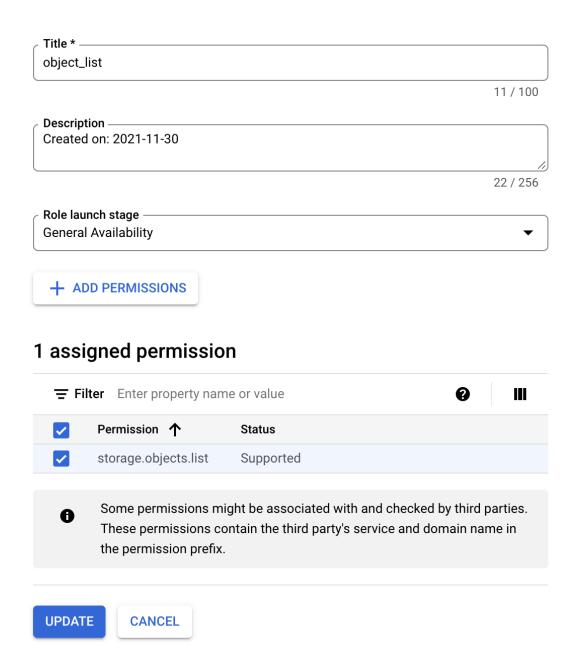
Title *

ttt

Description

CONDITION BUILDER   **CONDITION EDITOR**

Expression

Enter CEL expression here.

```
1  resource.name.startsWith("projects/_/buckets/cliu201-asia/objects/tmp/")
```

可参考如下配置:

```
liuchenggang@cloudshell:~ (cliu201)$ gsutil iam get gs://cliu201-asia
{
  "bindings": [
    {
      "condition": {
        "expression":
"resource.name.startsWith(\"projects/_/buckets/cliu201-asia/objects/tmp/\")",
        "title": "ttt"
      },
      "members": [
        "user:cliu@goodvm.net"
      ],
      "role": "roles/storage.admin"
    },

  ],
  "etag": "CCA="
}
```

3.在bucket所属的项目创建自定义role: 包含 storage.object.list权限

Title *

object_list

11 / 100

Description

Created on: 2021-11-30

22 / 256

Role launch stage

General Availability ▼

+ ADD PERMISSIONS

1 assigned permission

☰ Filter	Enter property name or value		❓	⦀

☑	Permission ↑	Status
☑	storage.objects.list	Supported

ℹ Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.

UPDATE **CANCEL**

4.创建项目层面的conditional iam

Principal

cliu@goodvm.net

Project

cliu201

Role

object_list ▼

Created on: 2021-11-30

Condition

bucket

🗑

➕ **ADD ANOTHER ROLE**

SAVE   SIMULATE   ❓   **CANCEL**

Edit condition   🗑 DELETE

Principal
cliu@goodvm.net

Project
cliu201

Title *
bucket

Description

CONDITION BUILDER   **CONDITION EDITOR**

Expression
Enter CEL expression here.

RUN LINTER

```
1 resource.name.startsWith("projects/_/buckets/cliu201-asia")
```

5.在cliu@goodvm.net下测试结果

```
cliu@cloudshell:~ (goodvm-101)$ gsutil cp 2.txt gs://cliu201-asia/temp/2.txt
Copying file://2.txt [Content-Type=text/plain]...
AccessDeniedException: 403 cliu@goodvm.net does not have storage.objects.create access to the Google Cloud Storage object.
cliu@cloudshell:~ (goodvm-101)$ gsutil cp 2.txt gs://cliu201-asia/tmp/2.txt
Copying file://2.txt [Content-Type=text/plain]...
/ [1 files][    0.0 B/    0.0 B]
Operation completed over 1 objects.
cliu@cloudshell:~ (goodvm-101)$
```