Restricted access to files and buckets

RESTRICTION IS WIP

NOTES TO REVIST

So an old saying is that IAM is alway difficult and here we see restriction of access to a bucket and its files being slightly convoluted in GCP

We have a BUCKET name `excel-annotatione298caff78da-production`

We wish to restrict access of the service account `vbe-restricted-write@full-stack-259515.iam.gserviceaccount.com` to this bucket alone and possibly a single file.

A simple regex was attempted to allow object admin access to object named `file-name.json` but this did not work.

> A point to bear in mind when testing rights in GCP
>
> GCP can be slow to cascade/proliferate (upto 10minutes have been experienced)
>
> So when changing a right, ensure that the right you are testing against is the latest.

So where did we end up

The restriction was lightened and will be visited again to tighten but we now essentially have a two rights.
1 - Object Viewer on all buckets (This hopefully to be restricted)

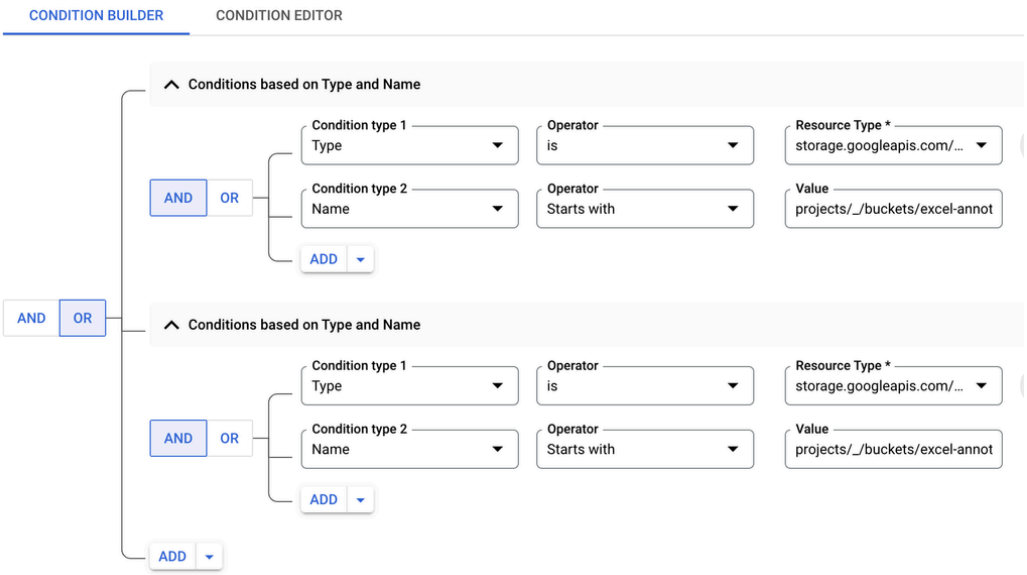
2 - Object Admin with restriction
Here is the restriction:

```
(resource.type == "storage.googleapis.com/Object" && resource.name.startsWith('projects/_/buckets/excel-annotatione298caff78da-production/objects/')) || (resource.type == "storage.googleapis.com/Bucket" && resource.name.startsWith("projects/_/buckets/excel-annotatione298caff78da-production"))
```

Lets break this down
Resource type == Object
AND
the name starts with `projects/_/buckets/excel-annotatione298caff78da-production/objects/`

OR
Resource type == Bucket
AND
the name starts with `projects/_/buckets/excel-annotatione298caff78da-production"`

So what does this end up with
Admin on Objects in the bucket Or the bucket itself



Principal

vbe-restricted-write@full-stack-259515.iam.gserviceaccount.com

Project

Full Stack

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role

Storage Object Admin

Grants full control over objects, including listing, creating, viewing, and deleting objects.

IAM condition (optional)

restricted bucket access to excel-annotation

Role

Storage Object Viewer

Grants access to view objects and their metadata, excluding ACLs. Can also list the objects in a bucket.

IAM condition (optional)

+ ADD IAM CONDITION

+ ADD ANOTHER ROLE

SAVE TEST CHANGES CANCEL