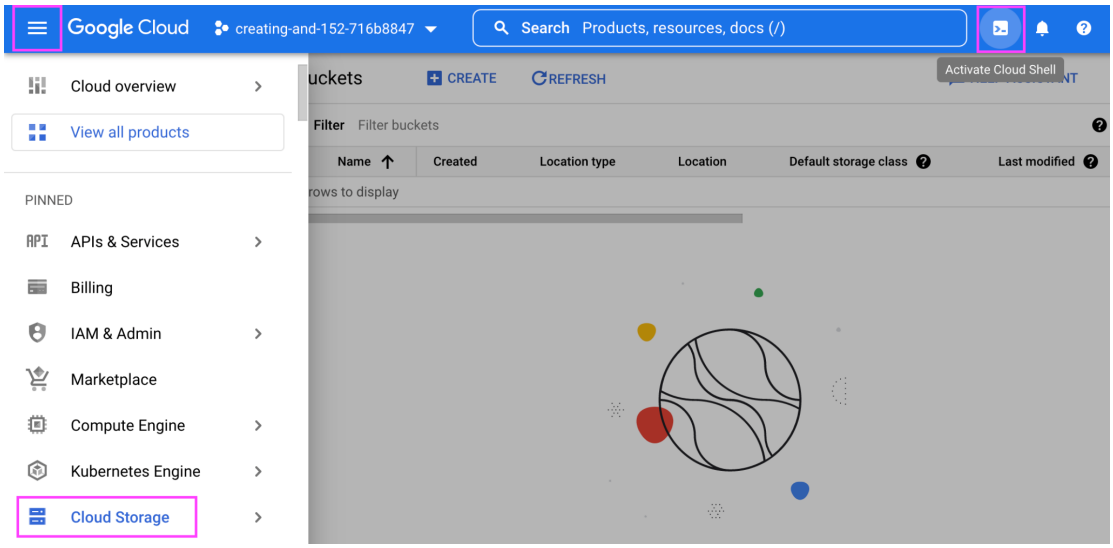
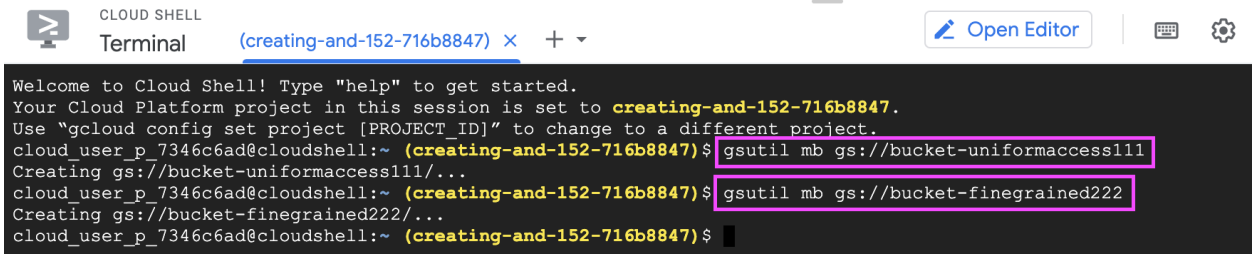
In this writeup I will instruct you on how to apply uniform and fine-grained permissions to Cloud Storage buckets. Permissions designate who has access to various resources. I will set up one bucket with uniform access, meaning that all objects within share the same permissions-designated at the bucket level. I will set up another bucket to have fine-grained control, which allows you to specify permissions at the bucket or individual level.

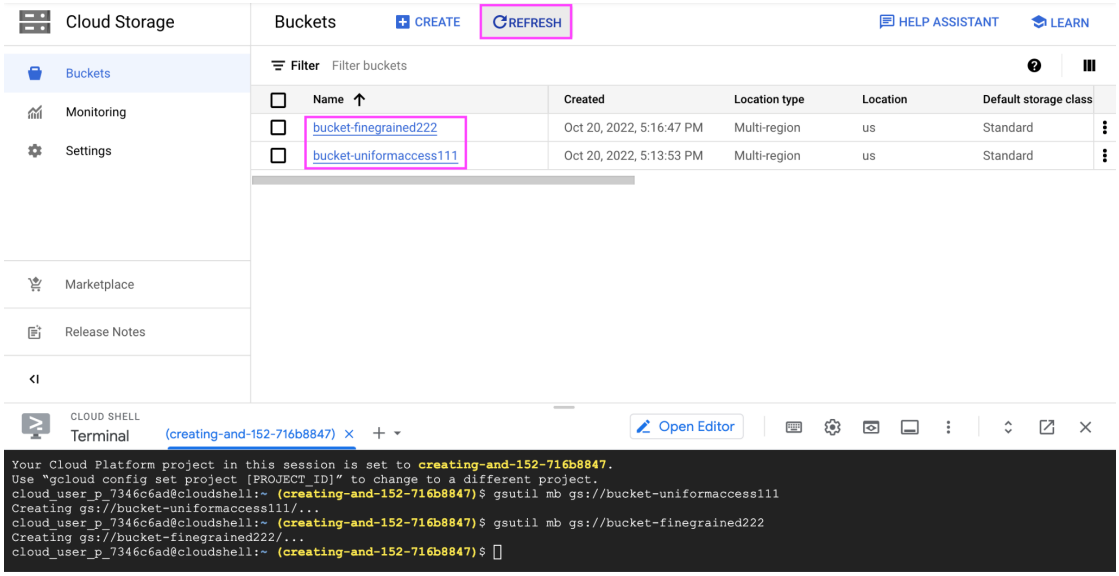
1. Set up two Cloud Storage buckets
    a. “Navigation menu”; “Cloud Storage”
    b. “Activate Cloud Shell” icon



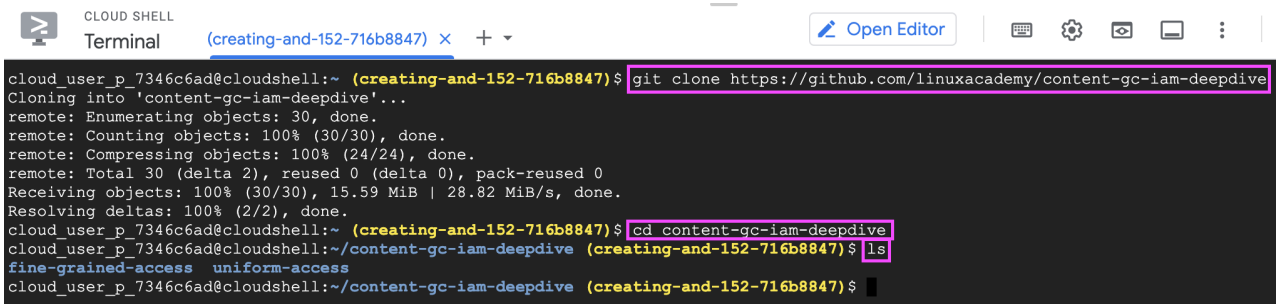
    c. Create the first bucket, which will be the uniform access bucket, using the following command
        i. gsutil mb gs://bucket-uniformaccess111
    d. Create the second bucket, which will be the fine-grained access bucket, using the following command
        i. gsutil mb gs://bucket-finegrained222



e. “Refresh” the buckets page to view the two Cloud Storage buckets just created



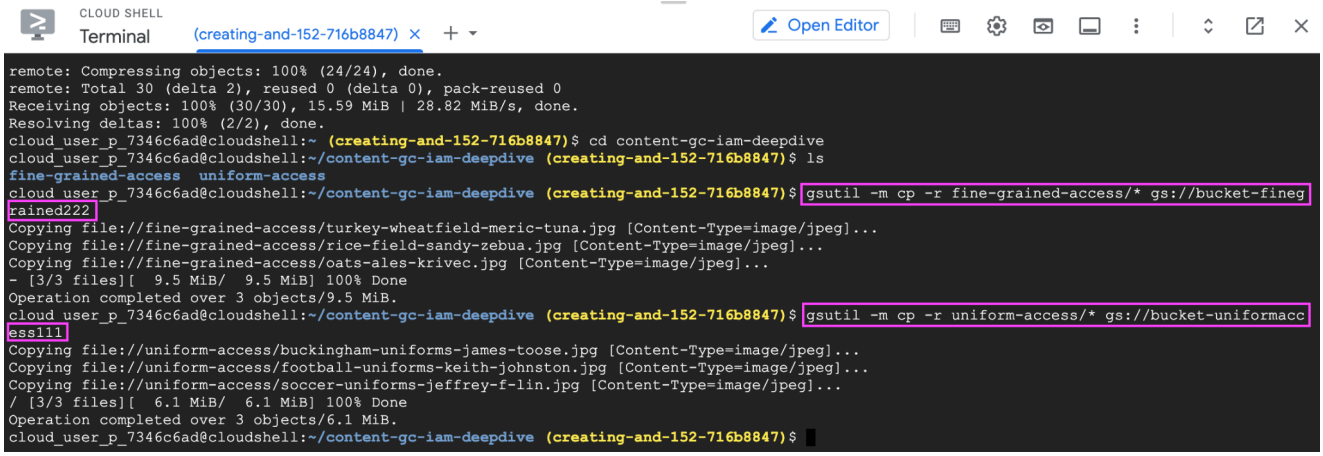
2. Populate the buckets with files from a GitHub repository
   a. In Cloud Shell retrieve the GitHub files using the following command
      i. git clone https://github.com/linuxacademy/content-gc-iam-deepdive
      ii. “cd content-gc-iam-deepdive” command into the files’ directory
      iii. “ls” to view the two folders inside the file



   b. Copy the files from the two folders, to their respected buckets
      i. Copy the fine-grained access files to the fine-grained access bucket using the following command
         1. gsutil -m cp -r fine-grained-access/* gs://bucket-finegrained222

ii. Copy the uniform access files to the uniform access bucket using the following command

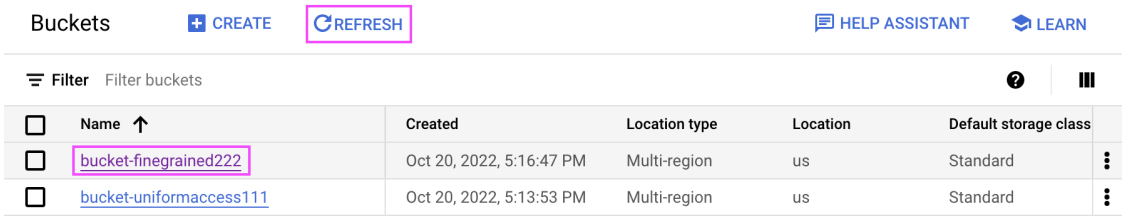
1. gsutil -m cp -r uniform-access/* gs://bucket-uniformaccess111



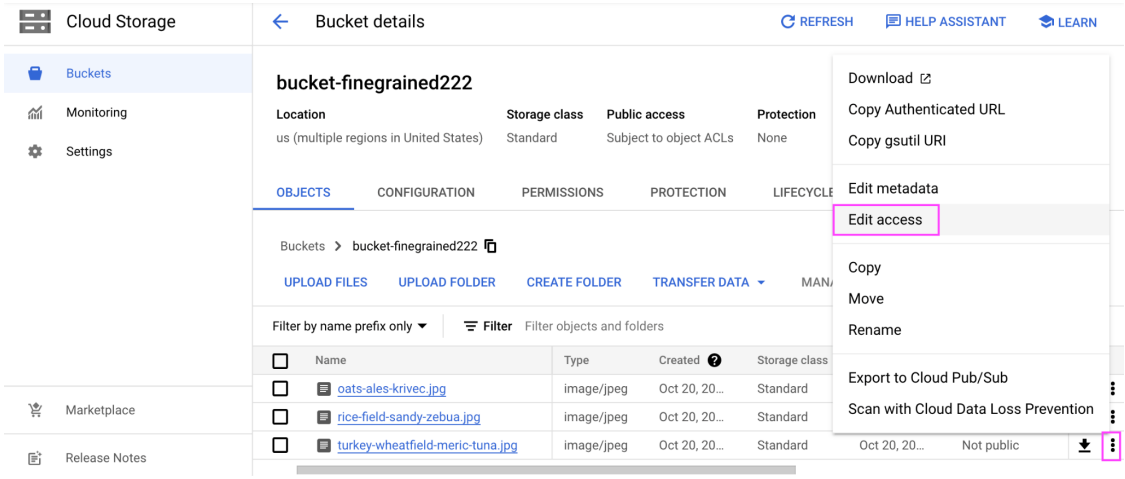
c. “Refresh” the bucket page again

3. Set permissions to allow one file within the fine-grained access bucket to be publicly viewable to anyone on the internet

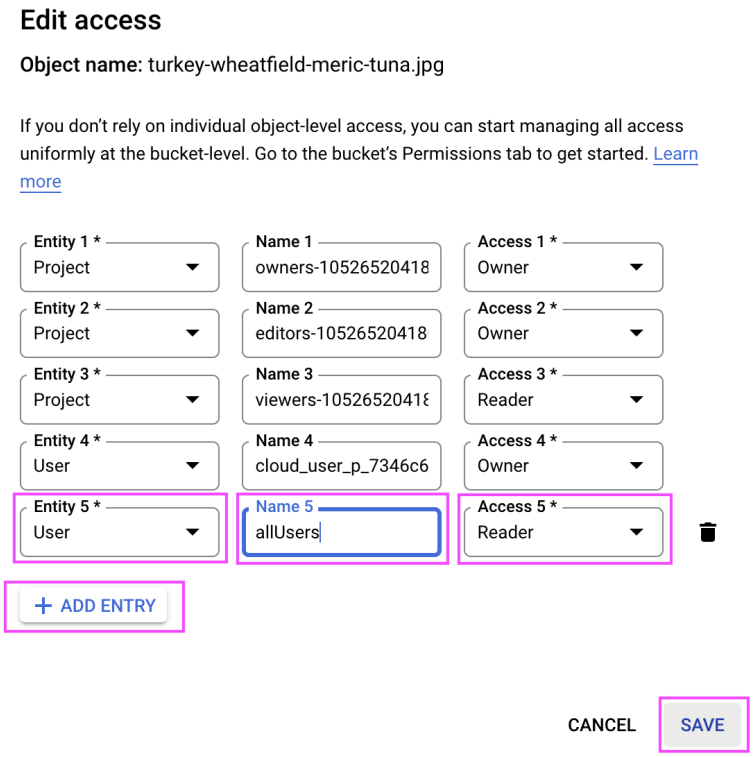
a. Click on the fine-grained access bucket



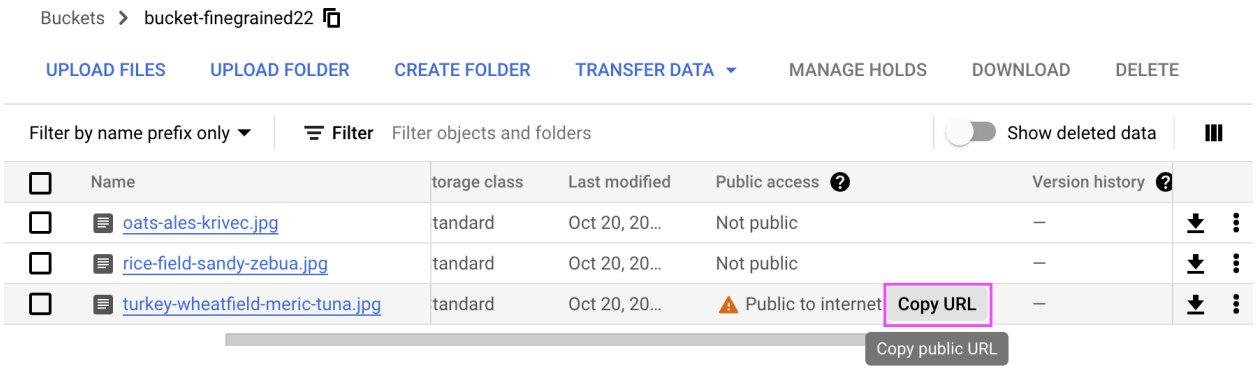
b. By default the files inside the bucket are set to “Not public”. To change public access settings click on the “object overflow menu”/ellipsis icon besides one of the files; “Edit access”

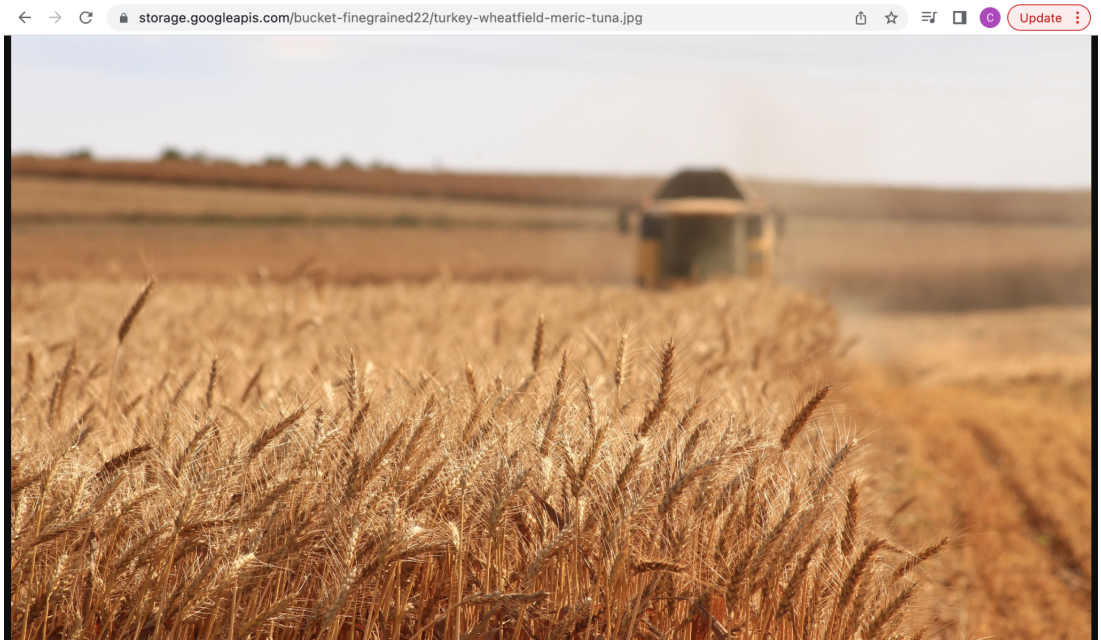


c. “Add Entry”
d. Change the “Entity” to “Public”
e. For “Name” select “allUsers” from dropdown menu
f. Set “Access” to “Reader” to make the file viewable
g. “Save”

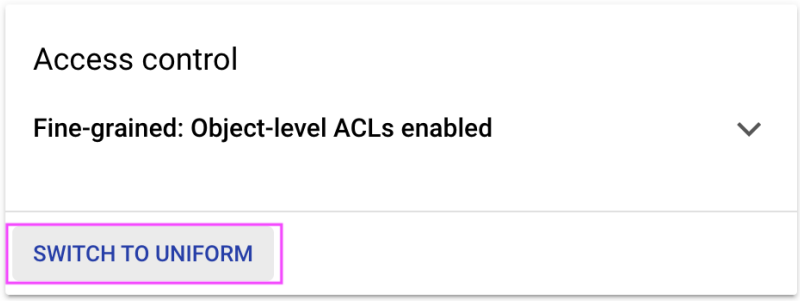


4. Test the fine-grained access bucket
    a. The fine-grained bucket page will now show one file as “Public to the internet”, with a “Copy URL” link now beside it. Copy the link, open a new browser, and paste the link into the browser, where the file image will populate

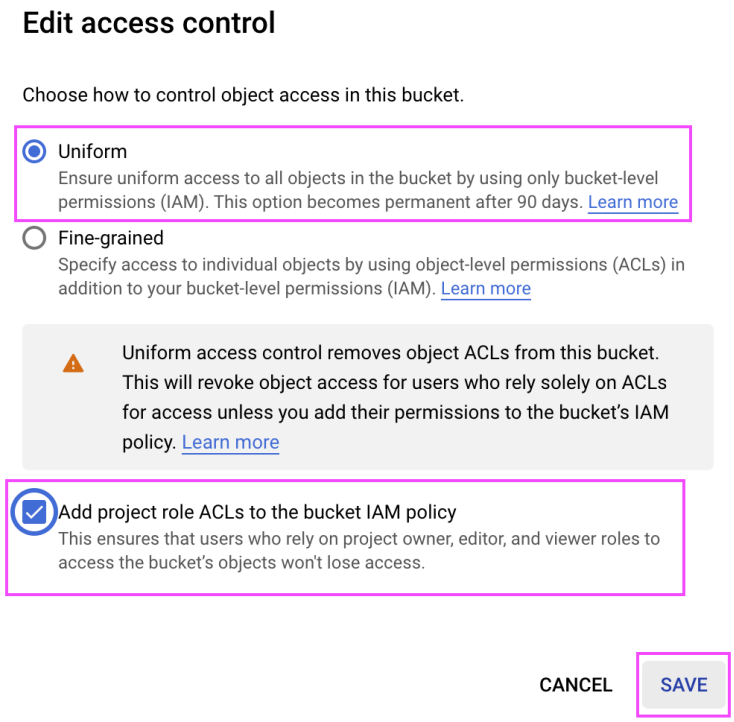




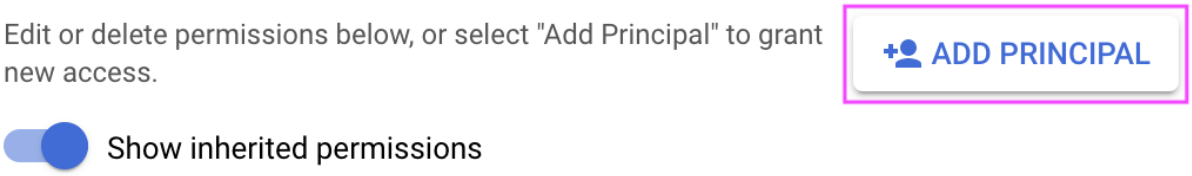
5. Set permissions to allow all files within the uniform access bucket to be publicly viewable to anyone on the internet
    a. Click the “object overflow menu”/ellipsis icon besides the bucket; “Edit access”
    b. By default the bucket was assigned fine-grained access control. To change this click “Switch to uniform”



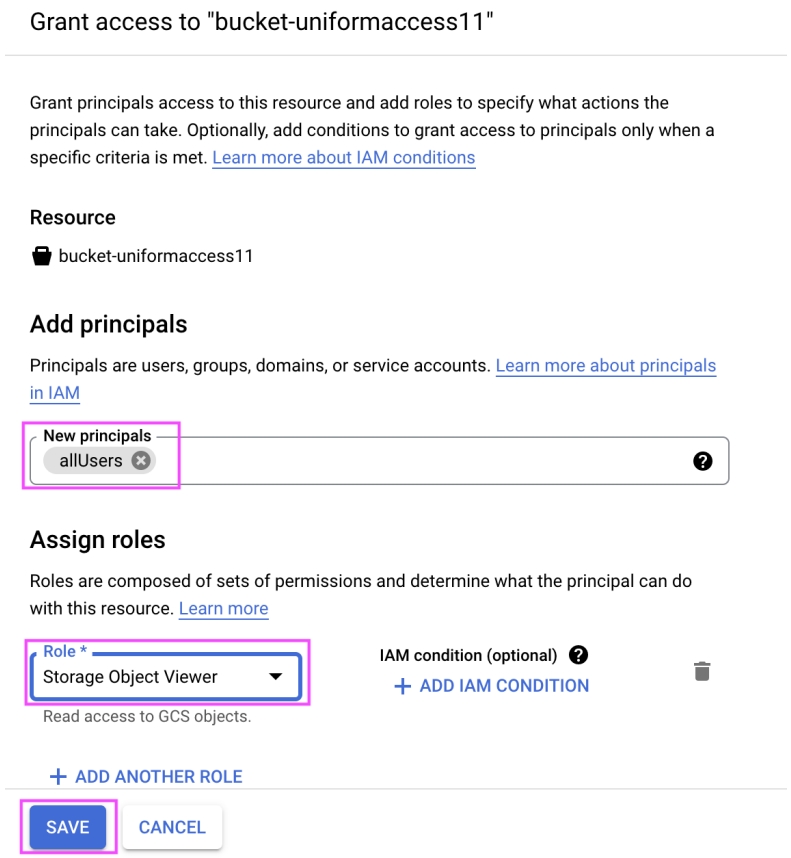
    c. Select the “Uniform” option, and check mark the “Add project role ACLs to the bucket IAM policy”, to help prevent IAM roles previously on the files from being taken away; “Save”



d. "Refresh" the buckets page. Our uniform access bucket will now show "Access Control" as "Uniform"
e. Make the bucket public to the internet by adding an allUsers member to the bucket
    i. Click the "object overflow menu"/ellipsis icon besides the bucket; "Edit access"
    ii. "Add principle"



    iii. For "New principle" type "allUsers"
    iv. Under "Assign roles" select "Storage Object Viewer" which is located in the "Cloud Storage" tab; "Save"



6. Test the uniform access bucket
    a. Click on the uniform access bucket name, where each file will read “Public to the internet”, with a “Copy URL” link beside each one. Copy and paste each link into a new browser where the file images will populate