

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

- “Navigation menu”; “Cloud Storage”
- “Activate Cloud Shell” icon

The screenshot shows the Google Cloud Platform dashboard. On the left, the navigation menu is open, with 'Cloud Storage' highlighted. The main area shows the 'Buckets' page, which lists buckets. A large graphic of a globe with colored dots (red, blue, yellow) is centered on the page. The top right corner of the dashboard has a 'Cloud Shell' icon, which is highlighted with a pink box.

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

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to creating-and-152-716b8847.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$ gsutil mb gs://bucket-uniformaccess111
Creating gs://bucket-uniformaccess111/...
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$ gsutil mb gs://bucket-finegrained222
Creating gs://bucket-finegrained222/...
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$
```

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

Name	Created	Location type	Location	Default storage class
bucket-finegrained222	Oct 20, 2022, 5:16:47 PM	Multi-region	us	Standard
bucket-uniformaccess111	Oct 20, 2022, 5:13:53 PM	Multi-region	us	Standard

2. Populate the buckets with files from a GitHub repository

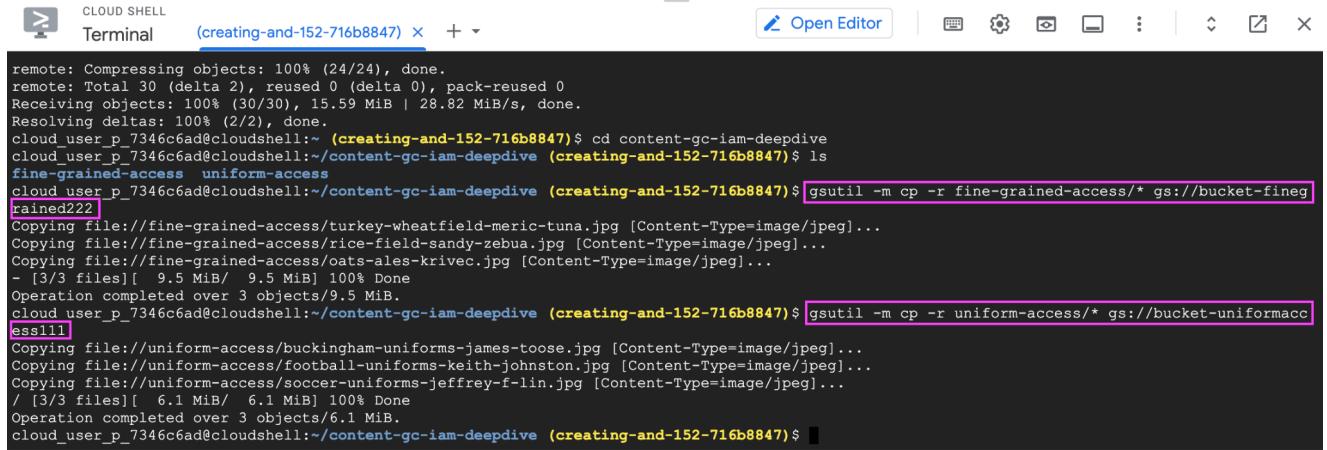
- In Cloud Shell retrieve the GitHub files using the following command
 - `git clone https://github.com/linuxacademy/content-gc-iam-deepdive`
 - “cd content-gc-iam-deepdive” command into the files’ directory
 - “ls” to view the two folders inside the file

```
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$ git clone https://github.com/linuxacademy/content-gc-iam-deepdive
Cloning into 'content-gc-iam-deepdive'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 30 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (30/30), 15.59 MiB | 28.82 MiB/s, done.
Resolving deltas: 100% (2/2), done.
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$ cd content-gc-iam-deepdive
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$ ls
fine-grained-access  uniform-access
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$
```

- Copy the files from the two folders, to their respected buckets
 - Copy the fine-grained access files to the fine-grained access bucket using the following command
 - `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`

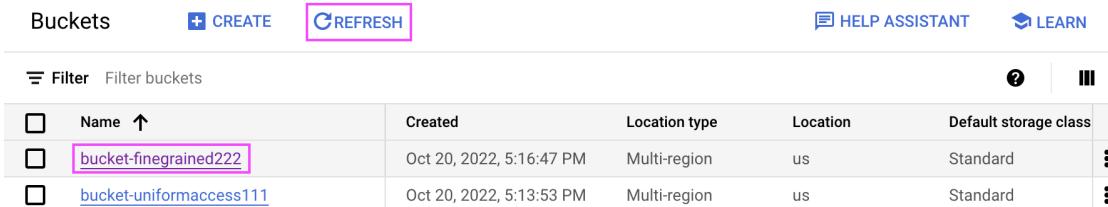


```

remote: Compressing objects: 100% (24/24), done.
remote: Total 30 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (30/30), 15.59 MiB | 28.82 MiB/s, done.
Resolving deltas: 100% (2/2), done.
cloud_user_p_7346c6ad@cloudshell:~ (creating-and-152-716b8847)$ cd content-gc-iam-deepdive
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$ ls
fine-grained-access uniform-access
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$ gsutil -m cp -r fine-grained-access/* gs://bucket-finegrained222
Copying file://fine-grained-access/turkey-wheatfield-meric-tuna.jpg [Content-Type=image/jpeg]...
Copying file://fine-grained-access/rice-field-sandy-zebua.jpg [Content-Type=image/jpeg]...
Copying file://fine-grained-access/oats-ales-krivec.jpg [Content-Type=image/jpeg]...
- [3/3 files][ 9.5 MiB/ 9.5 MiB] 100% Done
Operation completed over 3 objects/9.5 MiB.
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$ gsutil -m cp -r uniform-access/* gs://bucket-uniformaccess111
Copying file://uniform-access/buckingham-uniforms-james-toose.jpg [Content-Type=image/jpeg]...
Copying file://uniform-access/football-uniforms-keith-johnston.jpg [Content-Type=image/jpeg]...
Copying file://uniform-access/soccer-uniforms-jeffrey-f-lin.jpg [Content-Type=image/jpeg]...
/ [3/3 files][ 6.1 MiB/ 6.1 MiB] 100% Done
Operation completed over 3 objects/6.1 MiB.
cloud_user_p_7346c6ad@cloudshell:~/content-gc-iam-deepdive (creating-and-152-716b8847)$

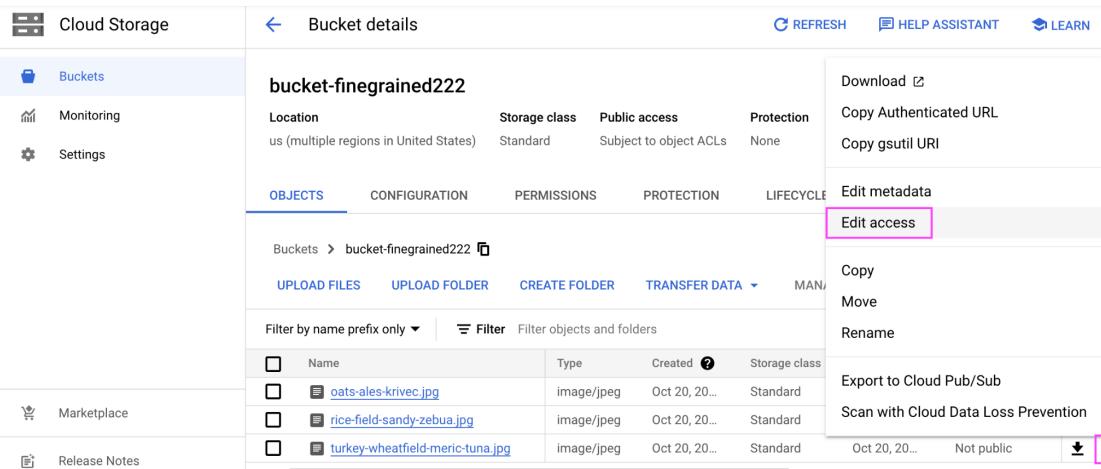
```

- 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



Buckets		CREATE	REFRESH	HELP ASSISTANT	LEARN
Filter Filter buckets					
<input type="checkbox"/>	Name ↑	Created	Location type	Location	Default storage class
<input type="checkbox"/>	bucket-finegrained222	Oct 20, 2022, 5:16:47 PM	Multi-region	us	Standard
<input type="checkbox"/>	bucket-uniformaccess111	Oct 20, 2022, 5:13:53 PM	Multi-region	us	Standard

- 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”



Cloud Storage		Bucket details																				
		REFRESH HELP ASSISTANT LEARN																				
Buckets Monitoring Settings		bucket-finegrained222 <div style="display: flex; justify-content: space-between;"> Location us (multiple regions in United States) Storage class Standard Public access Subject to object ACLs Protection None Download </div> <div style="display: flex; justify-content: space-between;"> Copy Authenticated URL Copy gsutil URI </div> <div style="display: flex; justify-content: space-between;"> Edit metadata Edit access </div> <div style="display: flex; justify-content: space-between;"> Copy Move </div> <div style="display: flex; justify-content: space-between;"> Rename Export to Cloud Pub/Sub </div> <div style="display: flex; justify-content: space-between;"> Scan with Cloud Data Loss Prevention ⋮ </div>																				
Marketplace Release Notes		OBJECTS CONFIGURATION PERMISSIONS PROTECTION LIFECYCLE Edit access <div style="display: flex; justify-content: space-between;"> UPLOAD FILES UPLOAD FOLDER CREATE FOLDER TRANSFER DATA ▾ MANAGE </div> <div style="display: flex; justify-content: space-between;"> Filter by name prefix only Filter objects and folders </div> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Created</th> <th>Storage class</th> </tr> </thead> <tbody> <tr> <td>oats-ales-krivec.jpg</td> <td>image/jpeg</td> <td>Oct 20, 20...</td> <td>Standard</td> </tr> <tr> <td>rice-field-sandy-zebua.jpg</td> <td>image/jpeg</td> <td>Oct 20, 20...</td> <td>Standard</td> </tr> <tr> <td>turkey-wheatfield-meric-tuna.jpg</td> <td>image/jpeg</td> <td>Oct 20, 20...</td> <td>Standard</td> </tr> </tbody> </table>					Name	Type	Created	Storage class	oats-ales-krivec.jpg	image/jpeg	Oct 20, 20...	Standard	rice-field-sandy-zebua.jpg	image/jpeg	Oct 20, 20...	Standard	turkey-wheatfield-meric-tuna.jpg	image/jpeg	Oct 20, 20...	Standard
Name	Type	Created	Storage class																			
oats-ales-krivec.jpg	image/jpeg	Oct 20, 20...	Standard																			
rice-field-sandy-zebua.jpg	image/jpeg	Oct 20, 20...	Standard																			
turkey-wheatfield-meric-tuna.jpg	image/jpeg	Oct 20, 20...	Standard																			

- 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”

Edit access

Object name: turkey-wheatfield-meric-tuna.jpg

If you don't rely on individual object-level access, you can start managing all access uniformly at the bucket-level. Go to the bucket's Permissions tab to get started. [Learn more](#)

Entity 1 *	Name 1	Access 1 *
Project	owners-10526520418	Owner
Entity 2 *	Name 2	Access 2 *
Project	editors-10526520418	Owner
Entity 3 *	Name 3	Access 3 *
Project	viewers-10526520418	Reader
Entity 4 *	Name 4	Access 4 *
User	cloud_user_p_7346c6	Owner
Entity 5 *	Name 5	Access 5 *
User	allUsers	Reader

+ ADD ENTRY Delete

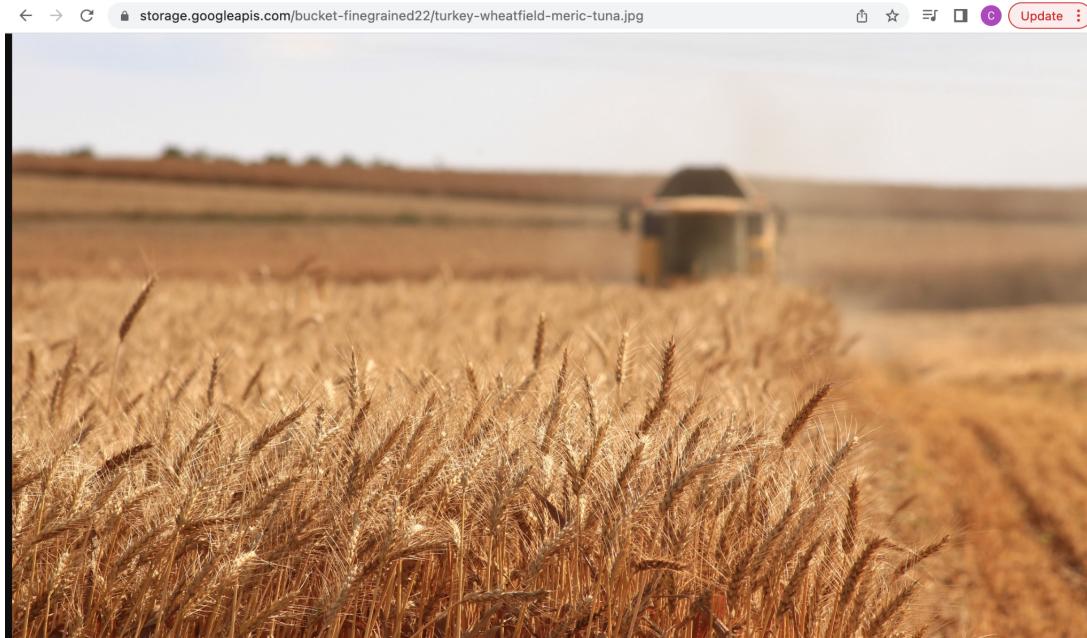
CANCEL SAVE

4. Test the fine-grained access bucket

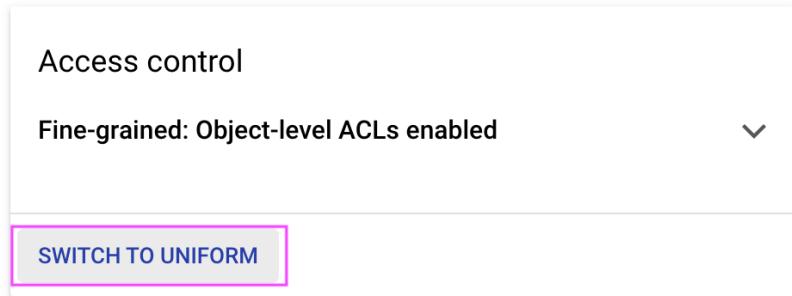
- a. The fine-grained bucket page will now show one file as “Public to the internet”, with a “Copy URL” link now beside it. Copy the link, open a new browser, and paste the link into the browser, where the file image will populate

Buckets > bucket-finegrained22

UPLOAD FILES	UPLOAD FOLDER	CREATE FOLDER	TRANSFER DATA	MANAGE HOLDS	DOWNLOAD	DELETE
<input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Filter by name prefix only"/> Filter <input style="border: 1px solid #ccc; width: 150px;" type="text" value="Filter objects and folders"/> <input checked="" style="margin-right: 5px;" type="checkbox"/> Show deleted data <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="More"/>						
<input type="checkbox"/>	Name		Storage class	Last modified	Public access	Version history
<input type="checkbox"/>	oats-ales-krivec.jpg		standard	Oct 20, 20...	Not public	-
<input type="checkbox"/>	rice-field-sandy-zebua.jpg		standard	Oct 20, 20...	Not public	-
<input type="checkbox"/>	turkey-wheatfield-meric-tuna.jpg		standard	Oct 20, 20...	Public to internet <input style="border: 1px solid #0072bc; padding: 2px 10px;" type="button" value="Copy URL"/>	-



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”



5. Set permissions to allow all files within the uniform access bucket to be publicly viewable to anyone on the internet
 - 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”

Edit access control

Choose how to control object access in this bucket.

Uniform

Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. [Learn more](#)

Fine-grained

Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). [Learn more](#)



Uniform access control removes object ACLs from this bucket.

This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy. [Learn more](#)



Add project role ACLs to the bucket IAM policy

This ensures that users who rely on project owner, editor, and viewer roles to access the bucket's objects won't lose access.

CANCEL

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”

Edit or delete permissions below, or select "Add Principal" to grant new access.

ADD PRINCIPAL



Show inherited permissions

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

Grant access to "bucket-uniformaccess11"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

 bucket-uniformaccess11

Add principals

Principals are users, groups, domains, or service accounts. [Learn more about principals in IAM](#)

New principals

allUsers 

?

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role *

Storage Object Viewer

IAM condition (optional) 

 + ADD IAM CONDITION

?

Read access to GCS objects.

 + ADD ANOTHER ROLE

 SAVE

 CANCEL

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



