ant: Uniform bucket-level access was known as Bucket Policy Only during Beta. The organization policy and API fiel
ng to Bucket Policy Only are still supported, but we recommend using the equivalent uniform bucket-level access
zation policy and API fields.

This page discusses uniform bucket-level access, which allows you to uniformly control access to your Cloud Storage resources. When enabled on a bucket, only bucket-level Cloud Identity and Access Management (Cloud IAM) permissions grant access to that bucket and the objects it contains; Access Control Lists (ACLs) are disabled and access granted by ACLs is revoked. For a guide to using this feature, see Using uniform bucket-level access (/storage/docs/using-uniform-bucket-level-access).

Cloud Storage offers two systems for granting users permission to access your buckets and objects: Cloud Identity and Access Management (Cloud IAM) (/storage/docs/access-control/iam) and Access Control Lists (ACLs) (/storage/docs/access-control/lists). These systems act in parallel - in order for a user to access a Cloud Storage resource, only one of the systems needs to grant the user permission. Cloud IAM is used throughout Google Cloud and allows you to grant fine-grained permissions at the bucket and project levels. ACLs are used only by Cloud Storage and have fewer permission options, but allow you to grant permissions on a per-object basis.

In order to support a uniform permissioning system, Cloud Storage has uniform bucket-level access. Using this feature disables ACLs for all Cloud Storage resources: access to Cloud Storage resources then is granted exclusively through Cloud IAM.

n: If you enable uniform bucket-level access, you revoke access from users who gain their access solely through obje
Be sure that you read considerations when migrating an existing bucket (#migration) prior to enabling uniform buck
ccess.

Use uniform bucket-level access if:

- You want to control access to Cloud Storage resources through a single permissioning system.
- You want to have a consistent access control experience across your Google Cloud resources.

- You have many objects in your bucket, and you do not want to manage access to each one individually.
- You want to use Google Cloud security features such as Cloud Audit Logs (/storage/docs/audit-logs), Domain Restricted Sharing (/resource-manager/docs/organization-policy/restricting-domains), and Cloud IAM Conditions (/monitoring/quotas#data_retention_policy), which only track access granted through Cloud IAM policies, not ACLs.
- You do not want the uploader of an object to always have full control of the object.

Do not use uniform bucket-level access if:

- You want to grant access to specific objects in a bucket via legacy ACLs.
- You want the uploader of an object to have full control over that object, but less access to other objects in your bucket.

The following restrictions apply when using uniform bucket-level access:

- Certain Google Cloud services that export to Cloud Storage cannot export to buckets that have uniform bucket-level access enabled. These services include:

  Stackdriver, Cloud Audit Logs, and Datastore.
- You cannot use the XML API to check the status of, enable, or disable uniform bucket-level access.
- You cannot use the XML API to view or set permissions for buckets with uniform bucket-level access enabled.
- The value of `Cache-Control` (/storage/docs/metadata#cache-control) is set to `private` by default for publicly accessible objects within the bucket; however, you can edit the metadata (/storage/docs/viewing-editing-metadata#edit) to make the `Cache-Control` value `public`.

You can enable uniform bucket-level access either when you create a new bucket, or when you explicitly enable uniform bucket-level access (/storage/docs/using-uniform-bucket-level-access#enable) on an existing bucket.

Once enabled, a bucket has the following behavior:

- Requests to set, read, or modify bucket and object ACLs fail with `400 Bad Request` errors.
    - This includes JSON API requests using any `BucketAccessControls` (/storage/docs/json_api/v1/bucketAccessControls), `DefaultObjectAccessControls` (/storage/docs/json_api/v1/defaultObjectAccessControls), or `ObjectAccessControls` (/storage/docs/json_api/v1/objectAccessControls) methods.
- JSON API requests for a full projection of bucket or object metadata include an empty ACL list as part of the response.
- The gsutil commands `cp -p` (/storage/docs/gsutil/commands/cp), `mv -p` (/storage/docs/gsutil/commands/mv), and `rsync -p` (/storage/docs/gsutil/commands/rsync) fail (both when the uniform bucket-level access bucket is the source and when it's the destination).
- Individual object ownership (/storage/docs/access-control/lists#ownership) no longer exists; access that is granted from such ownership is revoked, and requests for bucket and object metadata no longer contain an `owner` field.
- If you enable uniform bucket-level access as part of creating a new bucket, the bucket automatically receives additional Cloud IAM roles (/storage/docs/projects#permissions).
    - This behavior maintains the permissioning that objects inherited from the bucket's default object ACLs (/storage/docs/access-control/lists#default).
    - If you enable uniform bucket-level access on an existing bucket, you must apply any such roles manually; you may want to apply a different set of roles if you have changed the bucket's default object ACLs.

ant: Uniform bucket-level access cannot be disabled if it has been active on a bucket for 90 consecutive days. Attem
o results in an error.

To support the ability to disable uniform bucket-level access and revert to using ACLs, Cloud Storage saves existing ACLs for 90 days. If you disable uniform bucket-level access during this time:

- Objects regain their saved ACLs.
- Any objects added to the bucket after uniform bucket-level access was enabled gain ACLs according to the default object ACLs (/storage/docs/access-control/lists#default) used by the bucket.

When you enable uniform bucket-level access on an existing bucket, you should ensure that users and services that previously relied on ACLs for access have their permissions migrated to Cloud IAM. This section outlines some steps you should take when migrating a bucket to uniform bucket-level access. Note that since ACLs and Cloud IAM are synchronized for bucket permissions (/storage/docs/access-control/iam#acls), your considerations focus specifically on access to objects within your bucket and not on access to the bucket.

Before assigning Cloud IAM equivalents to your ACLs, consider the following:

- A Cloud IAM permission applied at the bucket level applies to **all** objects in the bucket, whereas object ACLs may vary from object to object.

If there is access that you want to apply to some objects but not others, you should group objects into separate buckets. Each grouping should contain those objects that have the same permissions.

When migrating to uniform bucket-level access, you should check to see if objects in the bucket are being accessed through the ACLs applied to them. To check this, Stackdriver (/monitoring/) has a metric that tracks ACL usage. If this metric indicates users or services rely on ACLs for access to your objects, you should assign Cloud IAM equivalents (#iam-equivalents) to the bucket before enabling uniform bucket-level access. For a guide to checking ACL usage in Stackdriver, see Check for ACL usage (/storage/docs/using-uniform-bucket-level-access#acl-check).

Use this metric to determine if enabling uniform bucket-level access would break your workflow:

Metric	Description
`storage.googleapis.com/authz/acl_operations_count`	The number of ACL operations that will be disabled once uniform bucket-level access is enabled, broken down by ACL operation type and bucket.

n: Since this metric contains personally identifiable information (PII) such as project ID and bucket name, only ACL u the past 6 weeks (/monitoring/quotas#data_retention_policy) will appear in Stackdriver. Enabling uniform bucket-le s might still break your workflow if ACLs were used more than 6 weeks ago.

An important ACL operation to examine is `OBJECT_ACCESS_REQUIRED_OBJECT_ACL`:

- If this number is zero, no object level ACLs were required to access objects within the past 6 weeks. Cloud IAM policies are covering the necessary permissions at the bucket or project level.
- If this number is greater than zero, there were requests to access objects within the past 6 weeks that required object ACL permissions. You should assign equivalent Cloud IAM policies (#iam-equivalents) before enabling uniform bucket-level access.

For more information on Stackdriver metrics, see Metrics, Time Series, and Resources (/monitoring/api/v3/metrics).

All buckets have a default object ACL (/storage/docs/access-control/lists#default) associated with them. New objects added to a bucket have this default object ACL applied to them unless an ACL is explicitly supplied at the time the object is added to the bucket.

Prior to enabling uniform bucket-level access, check the default object ACL (/storage/docs/access-control/create-manage-lists#defaultobjects) that your bucket has. Consider whether you want to grant the permissions associated with the default object ACL after you've enabled uniform bucket-level access. If so, assign Cloud IAM equivalents (#iam-equivalents) to the bucket.

Object ACLs may grant access that Cloud IAM currently does not. To ensure existing users do not lose access to objects when you enable uniform bucket-level access, use the following table and assign affected users (/storage/docs/access-control/using-iam-permissions#bucket-add) the appropriate Cloud IAM roles.

Object ACL permission	Equivalent Cloud IAM role
`READER`	`roles/storage.legacyObjectReader`
`OWNER`	`roles/storage.legacyObjectOwner`

To prevent conflicts between a bucket's Cloud IAM policies and object ACLs, Cloud IAM Conditions (/iam/docs/conditions-overview) can only be used on buckets with uniform bucket-level access enabled.

This means:

- To set Cloud IAM Conditions on a bucket, you must first enable uniform bucket-level access (/storage/docs/using-uniform-bucket-level-access#enable) on that bucket.
- To disable uniform bucket-level access on a bucket, you must first remove all Cloud IAM Conditions from that bucket's policy. For information on how to view and remove conditions from a bucket's policy, see Using Cloud IAM Conditions on bucket (/storage/docs/access-control/using-iam-permissions#conditions-iam). Note that uniform bucket-level access cannot be disabled if it has been active on a bucket for 90 consecutive days.

- Learn how to use uniform bucket-level access (/storage/docs/using-uniform-bucket-level-access).
- Set a uniform bucket-level access constraint (/storage/docs/setting-org-policies#uniform-bucket) in your organization policies (/resource-manager/docs/organization-policy/overview) to enforce the use of uniform bucket-level access within your Google Cloud organization, folder, or project.
- Set IAM permissions on buckets and projects (/storage/docs/access-control/using-iam-permissions#bucket-add).