Overview:

Global Write is an action utilized by Amazon S3 Buckets.

What is an Amazon S3 Bucket?

Amazon S3 Buckets are cloud storage. Any number and form of objects or data can be uploaded and stored in an S3 Bucket. Buckets are resources available to be managed by you through Amazon API's. All bucket names are globally unique, regardless of the AWS region the bucket is stored in.

More Information on S3 Buckets can be found: http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html

Bucket public *"Write"* access: This is sometimes referred to as "put" or "upload" access. It allows anyone to add, delete, or replace objects in your Amazon S3 bucket. Public bucket global write access may result in unintended charges and actions on your account.

Discovery:

Server Access Logging

Server Access Logging allows users to log requests for access to an S3 Bucket.
Access Log Information includes details about a single access request:

Who requested access
What bucket was requested
The time of the request
What action was requested
Response status
Or Error Code

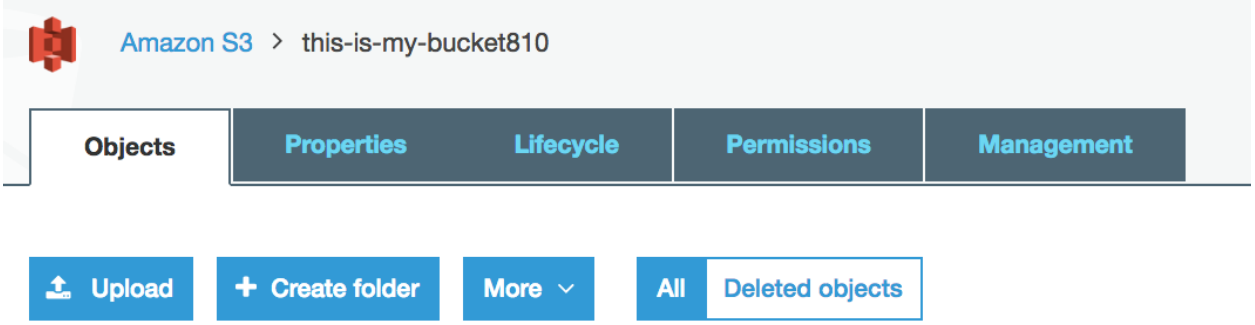
Access to these logs will enhance the user's knowledge of what is being accessed in the bucket for security purposes, as well as, ensuring the correct charges are on your Amazon S3 bill.

For More Information: http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

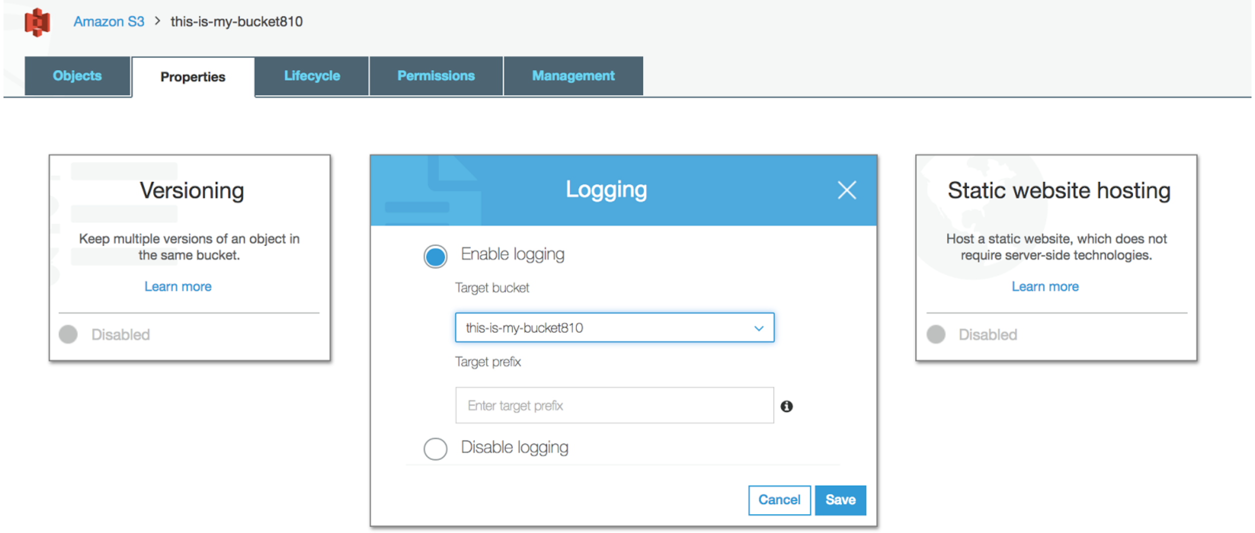
To Enable Logging on a Bucket:

- Sign into AWS Management Console
- Open Amazon S3 Console

- Select bucket you want to enable logging for
- Go to Permissions Tab



- Enable Logging, specify Bucket


Amazon S3 > this-is-my-bucket810
Objects
Properties
Lifecycle
Permissions
Management
Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled
Logging
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled
Cancel
Save

● Enable logging

Target bucket: this-is-my-bucket810

Target prefix: Enter target prefix

○ Disable logging

- Save the changes

More Documentation on Enabling Logging: http://docs.aws.amazon.com/AmazonS3/latest/dev/enable-logging-programming.html

Remediation:

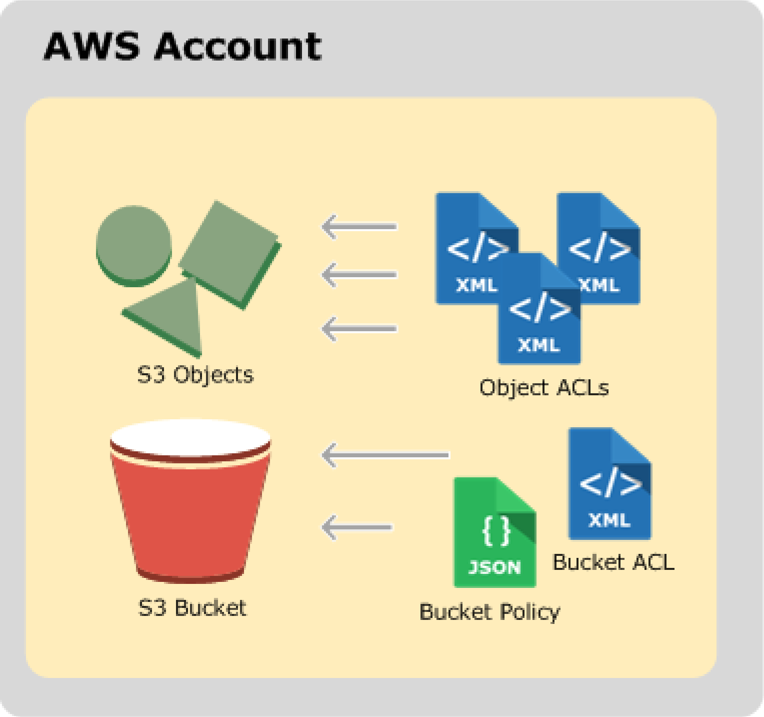
In order to remediate the threat of Global Write, it is important to view the current permissions for the S3 buckets for the Log Delivery Group.

Prevention:

Server Access Logging with Amazon S3 provides a rich set of mechanisms for you to manage access to your buckets and objects. An Access Control List (ACL) is one of these access control mechanisms. Logs can be found in the log delivery account, The Log Delivery group.

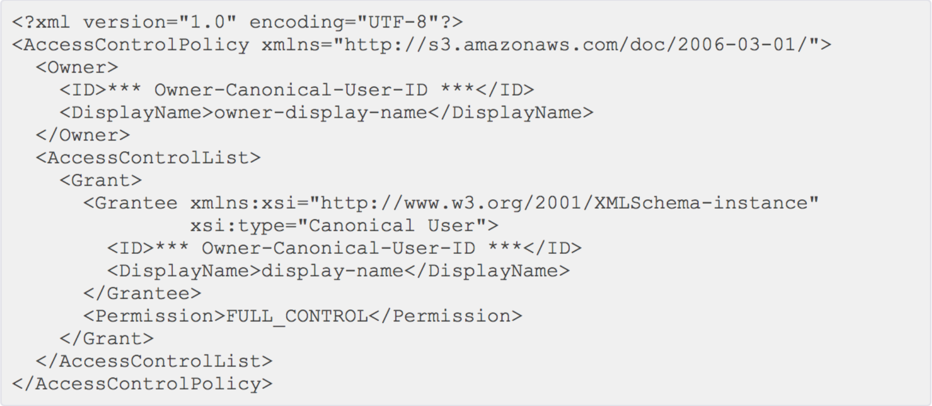
What Is An Access Control List?

Access Control Lists identify which AWS account or groups are allowed to perform what kind of actions. It is necessary to grant the Log Delivery group write permission on the target bucket. Each bucket and object has an ACL attached to it.



What is the default Access Control List?

It is important to understand what when Amazon S3 buckets or objects are created, the default ACL grants the owner full control over the resource shown.



```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

Shown in the photo you can see a sample bucket ACL and the owner's full control over the resource:

Others can be granted access to the bucket, however it is important not to give full control and just give the control necessary.

In order for the Log Delivery group to have write access, it is necessary to “grant the Log Delivery group write permission on the target bucket by adding a grant entry in the bucket's access control list (ACL).” Write access can only be granted on a bucket, not an object. Allowing write access it allows the specified user/group access to create, overwrite, and delete any object in the bucket.

If permission is not granted to the group they will not have write access.

Found From And More Information Available At:
http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html#sample-acl
http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html