# Cloud Storage Deletion, Data Component DC0022

Archived: 2026-04-05 16:22:17 UTC

Cloud Storage Deletion refers to the removal or destruction of cloud storage infrastructure, such as buckets, containers, or directories, within a cloud environment. Monitoring this activity is critical to detecting potential unauthorized or malicious actions, such as data destruction by adversaries or accidental deletions that may lead to data loss. Examples:

- AWS S3 Bucket Deletion: An AWS user deletes an S3 bucket using the `DeleteBucket` API call.
- Azure Blob Storage Container Deletion: A user deletes a container in Azure Blob Storage using the `Delete Container` operation.
- Google Cloud Storage Bucket Deletion: A Google Cloud user deletes a bucket using the `storage.buckets.delete` API.
- OpenStack Swift Container Deletion: A user deletes a container in OpenStack Swift using the `DELETE` method.

This data component can be collected through the following measures:

Enable Logging for Cloud Storage Services

- AWS S3: Enable AWS CloudTrail to log DeleteBucket API actions.
- Azure Blob Storage: Enable Azure Monitor and Diagnostic Logs to capture Delete Container operations. Use Azure Event Grid to capture and trigger alerts for container deletion.
- Google Cloud Storage: Enable Data Access logs in Cloud Audit Logs to monitor storage.buckets.delete API calls.
- OpenStack Swift: Configure Swift logging to capture DELETE requests for containers.

Centralized Logging and Analysis

- Use platforms like Splunk or native SIEMs to forward and analyze logs for anomalies in cloud storage deletions.

---

Source: https://attack.mitre.org/datacomponents/DC0022