SEAGATE LYVE™ Cloud

Safekeeping Data and Tracking Activity with Audit Logs

Learn about the purpose of Audit Logs in Seagate Lyve Cloud, including functions and benefits for user data.

Benefits Summary

- Secure Processes
- Detailed Log Tracking
- Organized Maintenance
- Protection Against Security Breach

Storing large data sets in the cloud can be a tedious process when it comes to tracking activity and maintaining organization within the platform. While the data may be safe, there's still a potential risk of security breaches or suspicious activity when accessing data.

While accessing data, users may accidentally delete some files that were not meant to be removed or misplace certain sets of information in a new location unintentionally. Human errors or cyberattacks are very possible when storing data in Seagate® Lyve™ Cloud, but can be easily solved with a tracking feature.

Solution Approach

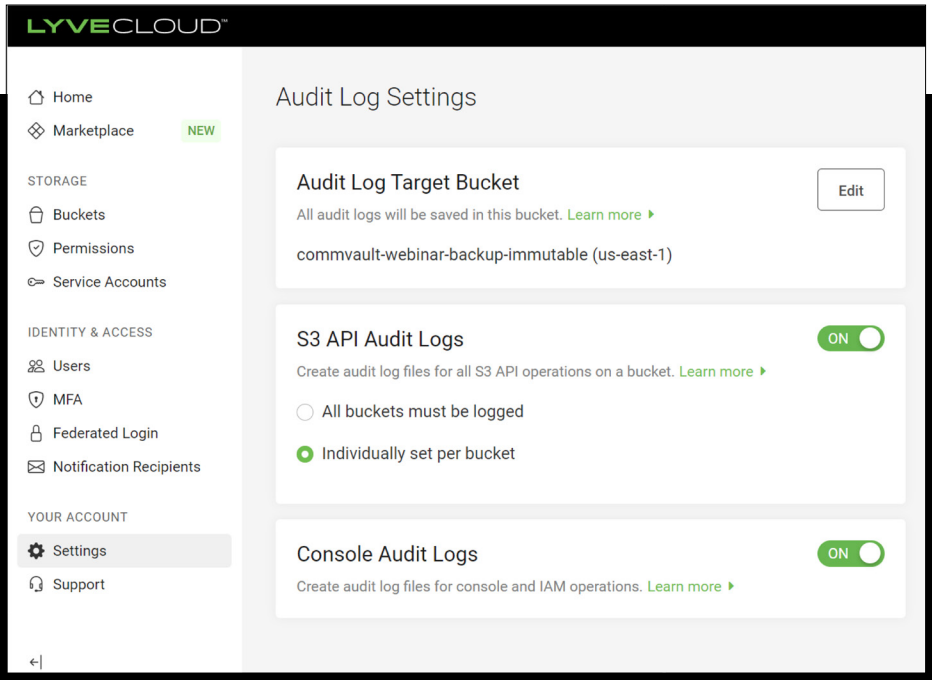
To combat potential issues, Lyve Cloud offers audit logs that track records of activities throughout the console.

Imagine the situation: You notice that a file is missing.

Lyve Cloud is a highly durable object storage platform, and it's unlikely that a file would disappear because of a system failure. With Audit Logs, you can find out which user has deleted the file.

Lyve Cloud Audit Logs are detailed records of activities in the Lyve Cloud console, S3 API operations, and identity and access management (IAM).

When you enable audit logging, all Audit Logs are written in the predefined target bucket. The target bucket must be immutable, which keeps the Audit Logs unchangeable for a specified duration of time.



Types of Audit Logs

IAM Audit Log

This log includes all events corresponding to identity and access management actions and logs all login and user management attempts in Lyve Cloud.

Events for example: password reset, user authentication, multi-factor authentication, etc.

Console Audit Log

This log contains all events triggered by the Lyve Cloud console actions.

Events for example: enabling an audit log, creating a permission, deleting a service account, etc.

S3 API Audit Log

This log records all the S3 API bucket-level and object-level operations being used. It records all data operations and is the main source for any data access security investigation.

For example, the following specific and fully detailed APIs are recorded: HeadObject, GetObject, ListObjects, etc.

Lyve Cloud saves Audit Logs in JSON format.

Event snippet:


```
{
“serviceAccountCreatorId”:
“john.doe@email.com”,
“auditEntry”:
{
  “api”:
{
“name”: “PutObject”,
“bucket”: “bucket-1”,
“object”: “values-v2.yaml”,
“status”: “OK”,
“statusCode”: 200,
“timeToResponse”: “2246401314ns” },
“time”: “2021-01-22T10:49:30.699378337Z”,
...
```


Notice: Lyve Cloud Audit Logs are generated hourly for events that have been recorded during the past hour. They are delivered on a best-effort basis, which means the Audit Log entry for a particular request may not appear until after the request has been processed.

Settings

By default, enabling S3 API Audit Logs is at the discretion of the Account Administrator. Once the Audit Log is authorized, audit logging is enabled for all available buckets in the Lyve Cloud account. Storage Administrators are restricted from disabling audit logging for specific buckets. The S3 API Audit Logs will be saved in the specified Lyve Cloud bucket with object immutability enabled and set to a specified retention duration that aligns with your business’s security standards.

Lyve Cloud also offers a more permissive S3 Audit Log option in which the Account Administrator can select an option to allow setup of Audit Logs in individually selected buckets. This option allows the Storage Administrator to selectively enable or disable the Audit Log for each bucket separately. While this option allows users to limit the S3 Audit Log scope for a subset of buckets, it’s not a recommended practice.

Seagate does not recommend changing the default S3 API Audit Log option. It ensures that S3 API Audit Logs are created for all buckets within a particular Lyve Cloud account. When using S3 API Audit Logs per bucket, it’s all done manually; audit logging must be turned on for each newly created bucket. Changing the S3 API Audit Log options can only be done by the Account Administrators of your Lyve Cloud account.

Integration with SIEM Applications:

Lyve Cloud Audit Log integration in security information and event management (SIEM) applications can be done easily to enable centralized Audit Log collection and monitoring. Integration with SIEM systems enables automated extraction and visualization of valuable insights for S3 buckets, Lyve Cloud console operations, and IAM-like monitoring and alerting, event correlation, log management, and more.

Lyve Cloud Audit Logs record the details for every request as a text in JSON format. All Audit Logs are compressed and maintained in a dedicated bucket and can be easily accessed by SIEM applications using standard S3 REST API.

An integration and monitoring solution example for Lyve Cloud S3 API Audit Log in AWS CloudWatch is available here.

Features & Benefits Summary

- **Processes Secured:** Users can secure all workflows and processes carried out within the platform.
- **Detailed Log Tracking:** All activity can be logged in proper detail for any future reference or necessary events.
- **Organized Maintenance:** Logs can organize the platform activity in such a way that allows users to track processes and any specific actions taken.
- **Security Risk Protection**: In cases of potential security risks, Audit Logs can help in providing information about activity that could be considered suspicious or unexpected.

Conclusion

Audit Logs are detailed records of activities in the Lyve Cloud console, S3 API operations, and IAM. With these records, users can safely organize their processes throughout the platform and maintain proper structure for actions taken.

If the console undergoes any potential security risks, admins can view Audit Logs to determine the cause of the problem and secure all data before any detrimental change.

Audit Logs in Lyve Cloud work to keep users in check with their functions. This not only keeps data safe but ensures all users carry out the proper processes to further accelerate business operations.

Ready to Learn More?

Visit us at www.seagate.com/services/cloud/storage/

SEAGATE