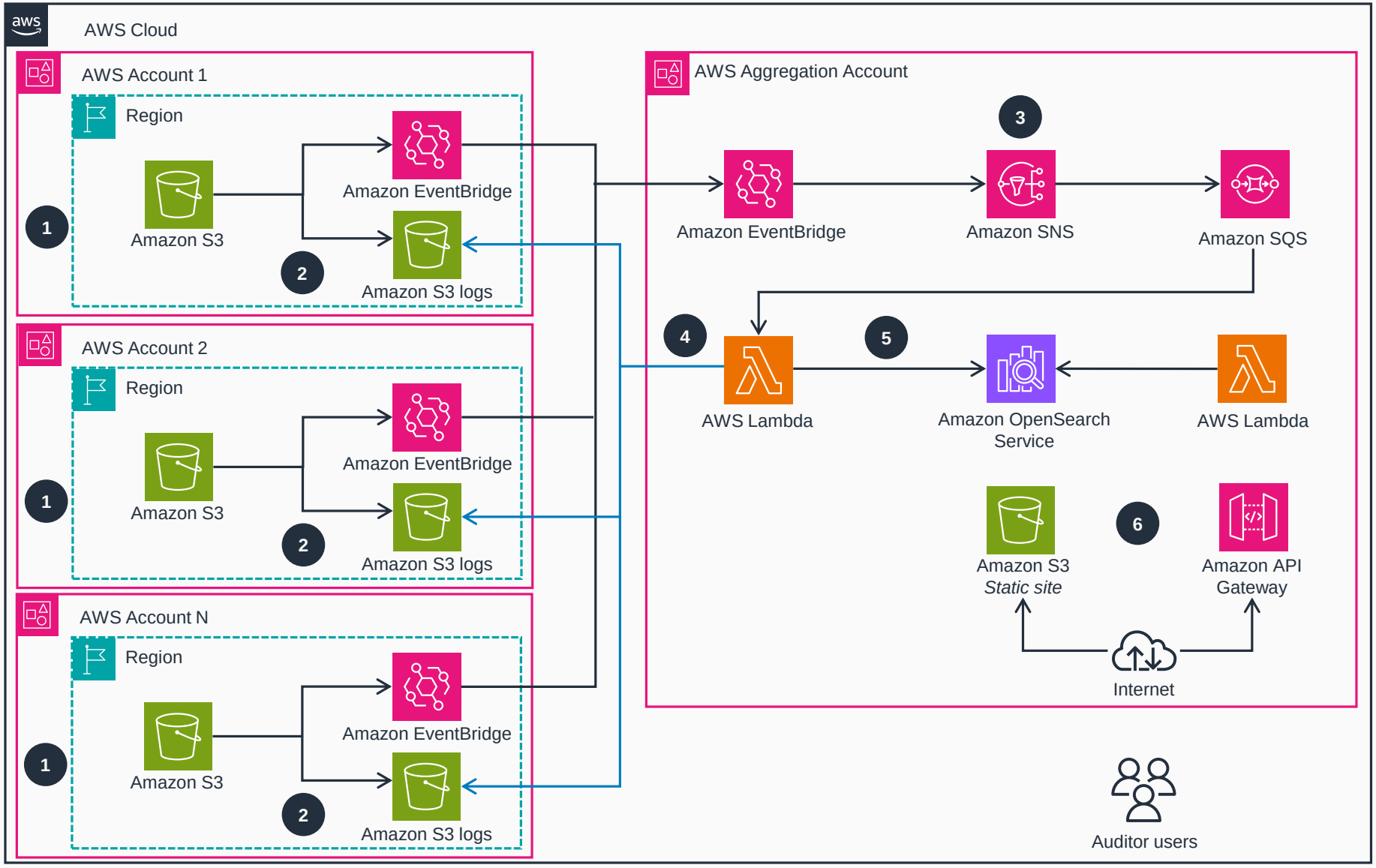
Guidance for Enterprise Search and Audit for Amazon S3

This architecture diagram allows customers to view activity and search object meta-data across multiple accounts, Regions, and S3 buckets within an organization or across linked accounts outside of an organization.



1. Any account (1, 2, or N) generates an event for **Amazon Simple Storage Service (Amazon S3)** operations, such as GET, PUT, DELETE, or storage tier updates.
2. The event gets recorded in **Amazon EventBridge** and in an **Amazon S3** logging bucket for the specific event source bucket.
3. **EventBridge** in the individual account (1, 2 or N) sends data to **EventBridge** in the AWS aggregation account, and the event is then forwarded to **Amazon Simple Notification Service (Amazon SNS)** which then distributes events to different **Amazon Simple Queue Service (Amazon SQS)**.
4. **AWS Lambda** functions process events from **Amazon SQS** in batches. **Lambda** functions create HEAD requests to the source bucket to get the metadata of each object. For GET requests, **Lambda** functions process log files from the logging buckets to record GET requests.
5. All data is pushed to an **Amazon OpenSearch Service** cluster, which hosts metadata for all objects.
6. An **S3** static site hosts a React JavaScript site that allows authorized users to browse **OpenSearch Service** metadata through **Amazon API Gateway** and **Lambda** functions.

Reviewed for technical accuracy February 7, 2024

AWS Reference Architecture