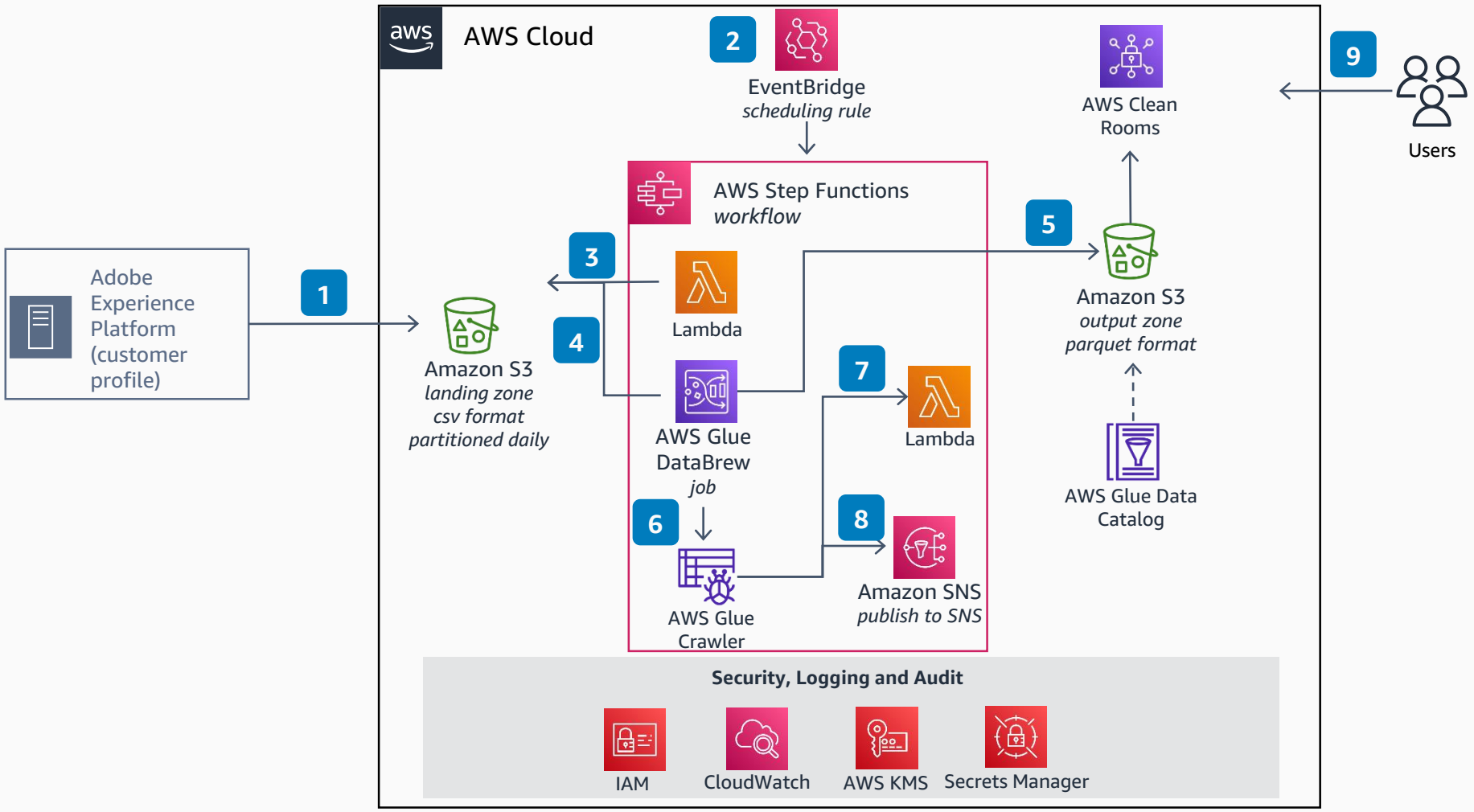
Guidance for Connecting Data from Adobe Experience Platform to AWS Clean Rooms

This guidance defines how an AWS customer can import their customer profile information from the Adobe Experience Platform (AEP) into their AWS account and prepare it for consumption in AWS Clean Rooms.



1. The AEP admin schedules a "daily" export job in the AEP to push the profile data to the customer's **Amazon Simple Storage Service** (Amazon S3) bucket within a pre-defined prefix.
2. Create a rule in **Amazon EventBridge** to schedule the data processing in **AWS Step Function** once a day.
3. The **AWS Lambda** function decrypts the files from the source **Amazon S3** bucket using **AWS Key Management Service** (AWS KMS) and places them in a different prefix for **AWS Glue DataBrew** to pick up and process.
4. **AWS Glue DataBrew** recipe will be executed to ingest the data from the decrypted source **Amazon S3** bucket:prefix location. The data will be normalized, and Personal Identifiable Information (PII) data will be hashed (SHA256).
5. The output of the **AWS Glue DataBrew** recipe will be written to the target **Amazon S3** bucket:prefix location in parquet format. The output file setting will be an "overwrite" as the profile data is a full refresh. An **AWS Glue Crawler** job is triggered to "refresh" the table definition and its associated meta-data.
7. The **AWS Lambda** function starts after the **AWS Glue Crawler** completes its run. The **AWS Lambda** will move the source data files to an "archive" prefix location as part of clean-up activity.
8. An event will be published to **Amazon Simple Notification Service** (Amazon SNS) to inform the user that the new data files are now available for consumption within **AWS Clean Rooms**.
9. The user utilizes the latest data within **AWS Clean Rooms** to collaborate with other data producers

Security, Logging and Audit

The solution uses the below AWS services to promote security and access control:

AWS Identity and Access Management (IAM) – least privilege access to specific resources and operations

AWS KMS – provide encryption for data at rest and data in transit (using PGP encryption of data files)

AWS Secrets Manager – provide hashing keys for PII data

Amazon CloudWatch – monitor logs and metrics across all services used in this solution

Reviewed for technical accuracy January 3, 2023

AWS Reference Architecture