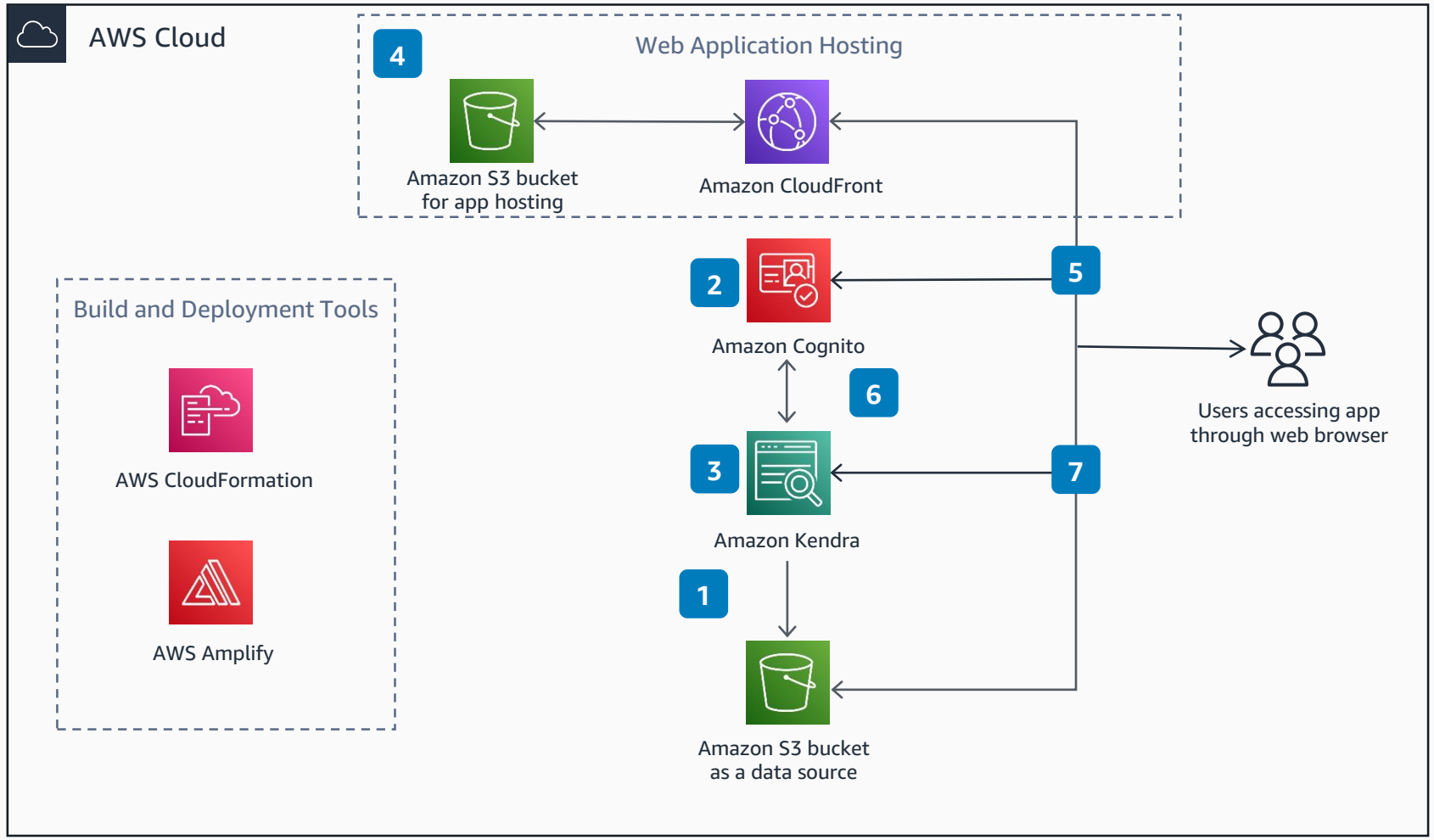
Guidance for Building a Secure & Intelligent Search Application on AWS

With Amazon Kendra, users can control access to documents using user access tokens and document access control lists (ACLs).



1. **Amazon Kendra** crawls and indexes documents from an **Amazon Simple Storage Service (Amazon S3)** bucket and collects the ACLs and document attributes from the metadata files.

2. The **Amazon Cognito** user pool authenticates registered users. The **Amazon Cognito** identity pool authorizes the application to use **Amazon Kendra** and **Amazon S3**.

3. Configure user access control of the **Amazon Kendra** index to use the **Amazon Cognito** user pool as an Open ID provider.

4. **AWS Amplify** builds and deploys the application code that will be used for web application hosting.

5. Your user authenticates and logs in to the application to perform a query.

6. The application sends the user's access token (provided by the **Amazon Cognito** user pool) to the **Amazon Kendra** index. The **Amazon Kendra** index decrypts the access token using the **Amazon Cognito** user pool signing URL and gets parameters such as cognito:username and cognito:groups associated with the user.

7. The **Amazon Kendra** index filters the search results based on the stored ACLs and the information received in the user access token. These filtered results are returned in response to the query API call that the application makes.

Reviewed for technical accuracy January 18, 2023

AWS Reference Architecture