Sumo Logic Professional Services

sumo logic

Log Analytics for Flex Quickstart

Effective Date: December 1, 2024

Overview

Sumo Logic's Professional Services Log Analytics for Flex Quickstart ("Log Analytics for Flex Quickstart") is designed to configure the Sumo Logic platform for the deployment of log analytics capabilities in support of operational monitoring and/or security use cases, as set forth below. The Log Analytics for Flex Quickstart is to be delivered in partnership with Customer via working sessions, during which configuration and enablement activities are performed.

Activities

Sumo Logic shall assist Customer with the following configuration and deployment activities, using an iterative approach that leverages Sumo Logic's best practices and techniques:

Topic	Sumo Logic Activities	Customer Activities
Technical Onboarding	• Conduct project kickoff. • Provide design and configuration guidance for Role Based Access Control ("RBAC") and Single Sign On ("SSO"). • Provide design and configuration guidance for the collection of up to eight (8) log sources. • Provide guidance on scan alerting and budgets. • Provide recommended design for metadata. • Configure metadata according to Customer-validated design.	• Participate in project kickoff. • Configure RBAC and SSO. • Provide input on scan strategy at role and/or user level • Configure and deploy collectors for the ingestion of logs within Customer environment. • Provide input and validate metadata design.
Configuration	• Provide recommended design of partitions. • Configure partitions according to Customer-validated design. • Create up to three (3) log data processing rules (as applicable). • Deploy out-of-the-box dashboards and monitors for log sources, if available, identified during Technical Onboarding. • Deploy Flex administrative content.	• Provide input and validate partition design. • Validate configuration of processing rules.

Topic	Sumo Logic Activities	Customer Activities
Content Development	• Design and create up to three (3) custom Field Extraction Rules (“FERs”). • Design and develop up to ten (10) log searches. *Using the above developed searches, create up to two (2) dashboards and five (5) monitors.*	• Provide use cases for the design of searches. • Validate configuration of FERs, searches, along with the monitor and dashboard.
Knowledge Transfer & Project Closeout	• Conduct knowledge transfer session and project closeout session. • Provide project documentation, including: list of dashboards and searches deployed, and recording of the knowledge transfer session.	• Attend and participate in the knowledge transfer & project closeout session.

Timeline

The Log Analytics and Monitoring Quickstart is expected to be executed in a continuous motion and completed within eight (8) to twelve (12) weeks of project kickoff. If the project extends beyond that timeline, and the delays are due to a lack of Customer participation, Sumo Logic may require a paid project change modification.

Assumptions

- Deployment shall be for one Sumo Logic Organization (“Sumo Org”).
- Customer shall provide timely access to Customer personnel required for Sumo Logic to perform its obligations hereunder (including subject matter experts familiar with security, compliance, and operational requirements of Customer).
- Customer personnel shall timely complete all recommended Sumo Logic self-paced training, prior to participating in any design and/or configuration activities.
- Assistance by Sumo Logic for collection of logs sources is limited solely to sources documented within the Sumo Logic Application Catalog.
- Sumo Logic shall not access and/or perform configuration work within Customer’s non-Sumo Logic environments and/or systems. For clarity, Customer is responsible for the installation and configuration of collectors.
- SSO functionality requires a Sumo Logic Enterprise Package subscription. For the avoidance of doubt, if Customer does not have an Enterprise Package subscription SSO shall not be enabled.
- SSO functionality shall require the Customer to use an identity provider supported by Sumo Logic.
- Professional Services shall be performed exclusively on a remote basis.
- SSO functionality shall require the Customer to use an identity provider supported by Sumo Logic.
- Professional Services shall be performed exclusively on a remote basis.