Splunk Migration- Advance

SPLUNK-MIG-ADVANCE

Date: 4/4/2024

Service Description

SOI Solutions (”SOI”) provides Professional Services as a project to meet customer’s outcomes as it relates to Splunk Cloud (Collectively known as the “Application Suite”).

The Splunk Migration Standard (“The Service”) migrates all streaming data feeds and approved content from on-prem Splunk environments to the Splunk Cloud environment. This includes migration of Splunk knowledge objects, review of Splunk onboarding practices, and App Vetting through the Splunk App Verification process for all approved applications.

Scope

- Splunk Cloud Configuration – Configure Splunk Cloud for use by the customer. This includes:
    - Creation of indexes based on license storage requirements.
    - Configuration of SAML integrations.
    - Configuration of Roles Based Access Controls.
    - Configuration of security settings such as IP restrictions and required tokens.
- Streaming Data Migration – SOI will perform the following tasks:
    - Configure the Splunk Deployment Server to properly configure Splunk Universal Forwarders (UF) to forward data to Splunk Cloud over secure connections.
    - Install and configure Splunkbase Technology Add-on's (TA) in the Splunk Cloud environment.
    - Validate all index-time parsing is accurate.
    - Configure syslog components to collect syslog data. Syslog components can be syslog-ng, rsyslog, or Cribl based solutions only.
    - Configure Splunk HTTP Event Collection where required.
    - Configure API data collection on the Splunk Cloud provided platform (Input Data Manager or Victoria stack implementation) or from Splunkbase applications.
    - Review data sources for Splunk Common Information Model (CIM) and make changes to Splunkbase TA’s where applicable.
    - There is a maximum limit of 25 data sources for this service.

Content Migration – SOI will migrate approved Splunk knowledge objects and process through the Splunk Application Verification process. This includes;

- Installation and configuration of Splunkbase applications in the Splunk Cloud environment.
- Installation and configuration of customer generated Splunk knowledge objects where no third-party programming language is used.

- Migration of user knowledge objects.

Out of Scope

- Custom programmatic data source collection – Any data source where a third-party programming language such as Python, Perl, or Java is used to collect data.
- Custom TA creation for Splunk CIM modeling.
- Creation of new Splunk applications.
- Installation or configuration of any Splunk Premium Apps such as Enterprise Security or ITSI.
- Deployment of the Splunk Cloud stack.
- Installation or upgrading of the Splunk UF.
- Any Splunk UF not reporting to the Deployment Server. If customers are leveraging other deployment technologies such as Puppet or Chef, SOI will provide recommendations to changes. Any changes to the deployment technologies are out of scope.
- Migration of archived data from original Splunk environment to new Splunk Cloud environment.
  - Splunk can provide this service directly.
  - SOI Solutions recommends a hydration process by cloning data for 30 days to ensure the new environment is properly configured. Historical data can be held outside of Splunk Cloud for compliance purposes.

Deliverables

The following outlines the expected deliverables the customer will receive. All document-based deliverables are provided in PPT, PDF, and MS Word formats. All Splunk configuration-based deliverables are provided as .conf files to be uploaded into the system.

- Splunk Cloud Project Plan – Provided in PDF format to demonstrate the weekly status of the migration.
- Splunk Cloud architecture documentation – Documentation of the Splunk Cloud architecture to include:
  - Components with hostname and IP address.
  - Data flows with ports.
  - Locations of configurations.

Assumption

- Services are initiated through SOI's deployment process. Implementation will begin according to the agreed upon Activation Date.
- All activity will be tracked within the SOI Portal and communicated back to the Customer. SOI will provision access to the SOI Portal for the Customer.

- Customers responsible for installation and configuration of any software or services in the Client's environment, such as agents, sensors, log collectors, workers, and virtual machines.
- Customers will provide remote access to the environment if needed.
- All software licenses are Customer's responsibility.
- Compliance regulatory control reviews are not in scope of this service.
- Customer will make available environment Subject Matter Experts during the engagement term.
- Services will be performed from 8am – 5pm Monday through Friday based on the Customer's time zone(s).
- Service Termination - The Customer has ninety (90) days starting on the Activation Date to schedule and utilize the Services. Unless approved by SOI, the Service will terminate automatically at the conclusion of the ninety-day period. Any unused portion of the Service is nonrefundable and non-creditable.