Cribl Deployment- Basic

PS-CRIBL-DEP-BASIC

Date: 4/11/2024

Service Description

SOI Solutions (”SOI”) provides Professional Services projects packaged to meet customer’s outcomes as it relates to the Cribl Stream, Cribl Edge, and Cribl Search (Collectively known as the “Application Suite”).

The Cribl Deployment - Basic (“The Service”) provides the services required to deploy Cribl in the customer’s environment and configure for at maximum 2 Use Case as described below. The Service includes a preliminary workshop, project coordination, and configuration of the Application Suite to meet the needs of the customer within the scope of section 2. Customers select the Use Cases during the preliminary workshop and agree to the project plan.

Scope

The Service Scope comprises tasks and meetings required to properly implement the Application Suite.

- Preliminary Workshop - SOI will conduct a workshop with the following agenda:
    - Planning.
    - Use Case Planning.
    - Source and Destination identification.
    - Project Coordination documentation.
- Deployment – Once the workshop is complete the following tasks are completed.
    - Deploy Cribl Leader (In the case of Cribl Cloud, this is done by Cribl Cloud Ops).
    - Deploy Cribl Workers as defined in Architecture Planning.
    - Configure Source and Destinations
    - Implement and configure Use Case #1
    - Implement and configure Use Case #2
    - Documentation
    - Cloud Meeting

Use Cases

Use Case	Description	Outcomes
Data Archiving	Configure Cribl to route data to an archive destination such as S3 or Blob storage and ensure data can be retrieved via the Replay configurations.	- Improved financial performance - Compliance - Risk reductions
Data Onboarding	Configure Cribl to collect data via either pull or receive methods and route the data to a destination. During data	- Reduced administrative burden

Use Case	Description	Outcomes
	onboarding, little work is done to the data as we are applying the foundation to access and transform data on the wire.	
Advance Data Onboarding	Some data sources require advanced configurations for interaction with REST APIs. This includes managing pagination to ensure data is properly collected. This is typically found in custom applications or newer SaaS products.	- Reduced administrative burden - better visibility in harder to collect sources
Data Transformation	Cribl is configured to transform data based on desired use cases. This can be formatting for sending to an end destination or reducing the event size. Examples include: • Log to metrics conversion. • Removal of Windows Descriptions. • AWS (Amazon Web Services) VPC flows from events to metrics. • Removal of null values in JSON data.	- Improved financial performance - Reduced administrative burden
Data Filtering	Configure Cribl to only collect what is needed. This can be done by sending only specific events to a specific system or sampling data to reduce spikes. Not only does this allow lean to cost savings, but also release network bandwidth for better performance.	- Improved financial performance - Improved networking and analytics performance - Reduced administrative burden
Data Enrichment	Configure Cribl to enrich events with additional metadata. Examples of this have been Geo-Tagging based on IP addresses, DNS threat intelligence tags, and asset tagging.	- Reduced administrative burden - Reduced risk through better visibility - Increased decision-making capabilities.
Edge Deployment	Cribl Edge provides a fast and easy collection mechanism for all hosts. Edge is a great complement to the Kubernetes monitoring capabilities and allows for advanced collection of data sources.	- Reduced administrative burden - Reduced risk through better visibility - Increased decision-making capabilities.

Out of Scope

- Implementation of any custom-built scripts or collection mechanisms.
- Installation or configurations of any operating systems, containers, 3rd-party agents, firewalls, load balancers, or networking components.
- Configuration of Workflows such as GitOps, CI/CD, Backup/Recovery.

Training on the Application Suite.

- Health and monitoring configurations unless specifically selected as a Use Case to be implemented.

Deliverables

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

- Cribl Architecture Diagram which will include:
  - Hosts
  - Ports
  - IP address
  - Source and Destinations
  - Environment locations

Assumption

- Services are initiated through SOI’s deployment process. Services will commence according to the agreed upon Activation Date.

Activation Date: The date on which the Preliminary Workshop begins.

- 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.
- The Customer will provide remote access to the environment if required.
- The Customer will provide sample data or access to raw data for configuration and implementation.
- All software licenses are the Customer’s responsibility.
- Compliance regulatory control reviews are not in scope of this service.
- The 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).

The Service expires 90 days from the Activation Date. The Service is non-refundable, non-creditable, and non-transferable without written consent from SOI Solutions.