Managed Services
Cribl Cloud

Date: 3/8/24

Definitions

- **SOI Solutions (SOI):** The company providing Managed Cribl Services.
- **Managed Cribl Services (The Services):** A comprehensive solution provided by SOI that allows clients to process, route, and control their machine data.
- **Machine Data:** Data in approved formats of Metrics, Events, Logs, or Trace (MELT) and produced from a computer system.
- **Cribl Cloud (The Product):** A product that requires a license and is managed by SOI. Includes configurations related to Routes, Pipelines, Sources, and Destinations in Cribl.Cloud environment.
- **SOI Managed Appliance (The Appliance):** Appliance machine capable of running workloads related to the Services.
- **Service Innovation Center (The Portal):** The Customer's communication channel for the Services. Includes a service catalog, ticketing system, health and monitoring alarm tracking, email notification of service updates, communications, project reporting, and Customer feedback system.
- **Production:** The environment fully managed and operated by SOI Solutions to include The Appliance and Cribl Leader configurations. Al
- **Development:** Environment(s) separate from Productions, which are out of scope of the Health and Monitoring and Subscription Service.
- **Maintenance Windows:** Scheduled periods of patching and maintenance to be performed on the Cribl Appliance nodes that might lead to down-time.
- **Alarms:** Configurations deployed within the Product by SOI that monitor disruptions.

Service Description

SOI Solutions (”SOI”) provides Managed Cribl Services (”The Services”), a comprehensive solution that allows clients to harness the full potential of their machine data. It is designed to provide clients with the ability to process, route, and control their data. The service includes Cribl Deployment, a subscription service, and 24x7 health and monitoring. The Cribl Cloud offering (”The Product”) requires a purchase of the Cribl Cloud license and manages:

- The Product configurations as it relates to Routes, Pipelines, Sources, and Destinations in the Cribl Cloud environment.
- SOI Cribl Worker Appliance (”The Appliance”) deployed by SOI Solutions in the Customer’s environment.

Service Components

Service Innovation Center

The Service Innovation Center ("The Portal") functions as the preeminent conduit for Customer communication pertaining to the Services. All activities are documented within a ticketing system to ascertain adherence to established standards. Access is provisioned to Customers, furnishing them with the ensuing functionalities:

- A service catalog of Service Requests to facilitate the Subscription.
- A ticketing system dedicated to the tracking of Service Level Objectives (SLOs).
- A mechanism for Health and Monitoring Alarm tracking.
- Provision for email notification of Service updates.
- Communication channels incorporating ticket-based communication through the portal or via electronic mail, in addition to telephonic support.

Deployment

SOI Deployments constitute a project-oriented engagement orchestrated with the express purpose of deploying and configuring the Product, pursuant to the guidelines established in an Architecture workshop. The workshop is conducted under the expert guidance of SOI Cribl Engineers, who take responsibility for documenting the Customer’s environment and developing a detailed Project Plan for deployment. After completing the Project Plan and defining all use cases, the engineering team begins developing the Customer's environment for deployment. The Deployment process includes:

- Conduction of Workshops - The Architecture and Use Case workshops are undertaken to document the Project Plan and delineate tasks for the initial deployment.
- Execution of Appliance Deployment - SOI collects required information to configure the Appliance script for deployment and configuration.
- Accomplishment of Use Case Configuration - SOI configures a Customer Git repository with defined use cases and configurations, with the aim of deploying to Cribl Leader.
- Fulfilment of Access Configuration - SOI configures access requirements in compliance with the Access section of this document.
- Completion of Portal Configuration - SOI undertakes the configuration of the Portal, provisioning Customer access, and a comprehensive walkthrough.

Access

During the deployment phase, SOI requires both User and Programmatic access to the Product.

- User access requires the configuration of SOI's SSO solution within the Product. Federated

access can be provided to the Customer for read-only access to the Cribl Leader. It is important to note that the Product only supports a single SSO configuration, which SOI will be responsible for maintaining.

  - The read-only access is limited to read-only as it relates to Sources, Destinations, Routes, Pipelines, and Knowledge Objects. Additional features such as teleport or Cribl Search will be enabled based on the product's capacity.

- Programmatic access is facilitated through approved access requirements as it relates to Cribl.Cloud's API. SOI uses best practices in managing credentials within a secure and temporal environment.

Subscription Service

The SOI Cribl Subscription Service provides Customer access to The Portal to submit Service Requests. The number of Service Requests per month is limited to the contractual agreed up on purchased amount. Service Requests are subject to SOI Subscription Service Level Objectives (SLO's) found here: <insert link>.

Service Requests are bespoke capabilities that can be configured in the Product to produce a Customer's desired outcome. When submitted, each request is assigned to an SOI Engineer for review and implementation. Some requests might require additional communications which are then coordinated with the Customer by the Engineer.

Health and Monitoring

SOI Health and Monitoring provides Customers with 24x7 monitoring of the Product which includes the infrastructure and the software in which SOI has direct and continual access. Once connectivity and deployment are established, the Product becomes the responsibility of SOI Solutions and deemed as a production environment ("Production") rendering the leader read-only.

The Appliance will be managed by SOI Solutions management plane and administered over a reverse HTTPS tunnel. This allows SOI to preform:

- Operating System patching
- Security monitoring of the appliance
- Remediation of Product faults
- Remote monitoring of infrastructure.

Development environments

SOI will provide integrations into a Customer's development environment ("Development"). Development is deployed and managed separately to Production. Development is out of scope of the Health and Monitoring and Subscription Service. If something developed in Development is desired to be promoted to Production, all configurations can be provided via a Service Request and incorporated into Production.

Maintenance Windows

Maintenance Windows are scheduled periods for network or IT system maintenance. SOI will conduct essential activities like updates or patches during these times, with scheduling aimed at minimizing Customer impact. Customers will receive advanced notice of scheduled maintenance via a Portal ticket and email notification. In emergencies, SOI may conduct maintenance outside these windows, providing

notice when possible. SOI is not liable for service disruptions or data loss if Customers fail to follow instructions related to Maintenance Windows.

Alarms

SOI will implement configurations to trigger alerts when the Product's performance is compromised. The outcomes of this alert system are referred to as Alarms. These Alarms can be reviewed by the Customer via the Portal. Alarms alert SOI when the following operations are disrupted:

- Infrastructure of the appliance (CPU, RAM, Disk, etc.)
- Availability of the Cribl Leader
- Availability of source and destination
- Degradation in the quality of data feeds

Appendix

RACI

R- Responsible, A- Accountable, C- Consulted, I-Informed.

Task	Customer	SOI
Create Source	C,I	R,A
Create Destination	C,I	R,A
Create Route	C,I	R,A
Create Pack	C,I	R,A
Create Pipeline and Functions	C,I	R,A
Monitor and report Node performance	C,I	R,A
Monitor and report Cribl Worker performance	C,I	R,A
Scale Cribl Workers up and down based on thruput	C,I	R,A
Deploy Appliance in Customer environment.	C,I	R,A

Review and respond to Alarms	C,I	R,A
Configure Source to send to Cribl	R,A	C,I
Configure Destination to receive from Cribl	R,A	C,I
Maintain GitOps connectivity	C,I	R,A
Manage software updates and patches	C,I	R,A
Manage backups and disaster recovery	C,I	R,A
Implement and manage change control process	C,I	R,A
Provide 24/7 technical support	C,I	R,A
Perform regular configuration audits	C,I	R,A
Plan and implement system improvements	C,I	R,A
Provide training to Customer's team as needed	C,I	R,A
Maintain system documentation	C,I	R,A
Monitor security notifications on Appliance	C,I	R,A
Recover from loss of Cribl Leader	C,I	R,A
Recover from Loss of Cribl Worker	C,I	R,A
Configure load balancing across Nodes	R,A	C,I

Remediate source generated derogation (outside of Cribl)	R,A	C,I
Remediate destination generated derogation (outside of Cribl)	R,A	C,I
Provision service accounts	R,A	C,I
Ensure service accounts has required permissions	R,A	C,I
Recover from loss of Node	R,A	C,I
Scale Nodes up and down based on performance	R,A	C,I
Conduct regular system health checks	R,A	C,I
Review and Update MPSA permissions as needed	R,A	C,I