DevOps Secrets Safe 20.1 Release Notes

December 10, 2019

Requirements:

- DevOps Secrets Safe deployment is currently only supported using Helm 2.
- DevOps Secrets Safe is currently supported on Kubernetes version 1.13, 1.14, 1.15.
- DevOps Secrets Safe CLI (ssrun) is supported on any standard Unix / Linux environment that has Python 3.5 or higher and pip3 installed.
- The MD5 signature is: 177043a577e1a3ddecf684652b2c20a3
- The SHA-1 signature is: 85cb363c364baf3ae4e25e1ed1176c5734c0488a

New Features and Enhancements:

- **Command-Line Interface:** The ssrun command-line interface is a cross platform user friendly tool for managing Secrets Safe deployments.
- **Kubernetes Deployment:** Secrets Safe is a cloud native application designed to be cloud platform agnostic and deployable on Kubernetes.
- **Initialize, Seal, and Unseal:** Secrets Safe supports a RSA private key initialization and sealing workflow.
- **Health Monitoring and Recovery:** Maximize uptime with internal health monitoring and integration with Kubernetes Liveness and Readiness Probes.
- **Key Value Store Secrets and Scopes:** Store arbitrary secrets organized individually or grouped in scopes.
- **Metadata Storage on Secrets and Scopes:** User created key value metadata on any secret or scope allow.
- **User and Group Access Control:** Granular access control allows grant or deny for API endpoints and entities.
- **IP Based Safelist Access Restrictions:** Safelists allow users to explicitly grant or deny access to specific IP addresses for API endpoints.
- **Internal Authentication:** Internal user and group management for simplified initial deployment and configuration.
- **API Key Application Authentication:** Key base authentication for machine to machine application access.
- **Oracle Identity Cloud Services Authentication:** Authentication and group synchronization for users and groups stored in IDCS.
- **Lightweight Directory Access Protocol Authentication:** Authentication and group synchronization for users and groups stored in LDAP.
- **Syslog Event Sink for Auditing and Logging:** Send audit and log events to one or more syslog servers.
- **Elasticsearch Event Sink for Auditing and Logging:** Send audit and log events to one or more Elasticsearch servers.
- **Console Event Sink for Auditing and Logging:** Send audit and log events to one or more Elasticsearch servers.
- **Oracle Database Support:** Supports Oracle database as a persistent data store.
- **Postgresql Database Support:** Supports Postgresql database as a persistent data store.
- **Subscription Based Licensing:** Simple subscription-based licensing.
- **Integration for Ansible:** Native support for Ansible via an Ansible lookup plugin.