

DevOps Secrets Safe 20.2 Release Notes

April 14, 2020

Requirements:

- DevOps Secrets Safe deployment is currently supported using Helm 2 or Helm 3.
- DevOps Secrets Safe is currently supported on Kubernetes version 1.13, 1.14, 1.15, 1.16, 1.17.
- 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: 2d567cde18e4cf5a5e37f06f0a571f65
- The SHA-1 signature is: a08f6195037ecc90543540811f164788616e8164

New Features and Enhancements:

- Secrets generation has been added, allowing Secrets Safe to generate cryptographic strings and numbers which can be made persistent for later retrieval.
- Secrets Safe can now be deployed using Helm 3 in addition to Helm 2.
- Secrets Safe can now be integrated with Azure DevOps build processes, using a Secrets Safe extension, available in the Visual Studio Marketplace.
- Auto-complete support has been added to the ssrun command-line interface.
- Secrets Safe now supports using Microsoft SQL Server as a persistent datastore.
- Secret Safe now supports deployment into a Kubernetes namespace.
- Secrets Safe is now supported on Kubernetes up to and including version 1.17.
- The ssrun command-line interface has been updated to add the ability to configure multiple contexts, allowing for easy switching between multiple deployed instances of Secrets Safe.
- Audit event logging has been refactored to reduce event volume while providing better traceability of system activities.
- Support for using Oracle database as a persistent datastore has temporarily been removed from Secrets Safe.
- The API endpoint for GET authorization entries has been refactored. The resource and operation query arguments have been replaced by the new pagination query arguments that are consistent across GET endpoints that use pagination.