RELEASE NOTES

Scribbler Log Manager (Windows) – Enterprise:
Version 1.9.23

Contents

Release 1.9.23

Release Information

Version	1.9.23
Date	September 01, 2022
Work Items	1064
Release Type	Hotfix

Bug Fixes

- 1064 - Scribbler Windows: Stopped collecting logs after upgrading to 1.9.22 followed by system restart

Known Issues

- Nil

Release 1.9

Release Information

Version	1.9.22
Date	August 19, 2022
Work Items	1026, 1014, 975, 974, 897

New Features

- 897: Option to change the default admin username
- 975: Security Compliance: Upgrade all dependency components to their latest versions

Bug Fixes

- 974: Scribbler: Large log storage units failed to back up on some cases.
- 1014: Scribbler Windows: Stopped collecting logs after a random period.
- 1026: Scribbler: Idle session timeout logs out the user bit early than expected.

Known Issues

- Nil

Release 1.8

Release Information

Version	**1.8.39**
Date	April 07, 2022
Work Items	190, 441, 753, 831, 862 743, 739, 742, 721, 637, 856

New Features
- 190: Basic Alerts support added.
  - A new alert page, Where the alerts generated by the system are shown
  - Alerts are also integrated with audit logs.
  - Generates alerts when disk space is low (configurable).
  - Generates alerts if the TLS certificate going to expire.
- 441: Added support to restore backups taken from another scribbler instance
- 718: HCI Support & Validation – VmWare Esxi
  - Scribbler windows version is validated on VmWare vSAN based ESXi cluster
  - Scribbler windows version is working as expected in the VmWare based HCI environment
  - Scribbler requires all the compute nodes tagged with it's VM should have same CPU model.
  - Scribbler does not support running on different model CPU in a cluster
- 753: Scribbler SNMP Agent v3 - Added support for SnmpEngineId & EngineBoot
- 831: Configuration Export & Import
  - System supports exports and import of the entire system configuration (Including encryption keys, licenses & all settings)
  - The exported configuration is encrypted by AES 256 algorithm
- 862: Upgraded to latest dotnet core (6.0.3)

Bug Fixes
- 743: Upper case non-standard month names in RFC 3164 are not handled.
- 739: Scribbler backend service randomly not starting when system resources are low or systems with high disk latency (HCI Environments, HDD on HyperV)
- 742: UTC dates are shown in search and live stream instead of local for some corner cases.
- 721: The system idle timeout is now configurable between 1 and 60 minutes.
- 637: The system shows expired certificates as valid in TLS configuration.
- 856: Installer fails to install on Windows Server 2012 R2 on some corner cases.

Known Issues
- Nil

Release 1.7

Release Information

Version	1.7.7
Date	January 13, 2022
Work Items	BFX – 713, BFX - 727

New Features
- Nil

Bug Fixes
- BFX-713: Scribbler fails to work as expected with McAfee application control (solidifier)
  - Affected Version: 1.6
  - Due to incorrect temp folder configuration of log collector, Scribbler fails to start if McAfee application control also installed on the same computer.
- BFX-727: Scribbler Windows: A typo in the installer screen.

Known Issues
- Nil

Release 1.6

Release Information

Version	1.6.36
Date	December 29, 2021
Work Items	USR – 670, 464, 672, 497, 711, 669, 688, 686 BFX – 709, 706

New Features
- USR-670: SNMP Agent Improvements
  - SNMP V3 support added
  - Health monitoring parameters of log collector, data store, web app and licensing are exposed through SNMP Protocol.

- USR-464: Installation Improvements
  - Added support to remember installation parameters.
  - Added option for lab environments which uses less RAM

- BFX-709: Search & Live Stream UI Improvements
  - Search and live stream user interface improved to efficiently utilize the space to display longer messages better.
  - Added an option to copy message content and expand all messages.

- USR-672: Backup encryption now defaults to AES 256 (Previously it was AES 128)

- USR-497: TLS 1.3 Support
  - The log collection and forwarding now supports TLS 1.3
  - TLS 1.2 and 1.3 are the only supported versions.
  - Other versions are disabled by default.

- USR-711: Release numbering changes
  - Currently, Scribbler uses <Major>.<Minor>.<Build> format for production releases.
- Going forward, it will be still the same. But minor version will be bumped for every new release.
- Nil

Dependency Updates
- USR-669: Updated to Microsoft dotnet 6.0.1 LTS (Long term support) release with latest security patches.

- USR-688: Log collector module (Logstash) updated to latest upstream version with security updates and patches.

- USR-688: Datastore (elastic search) updated to latest upstream version with security updates and patches.

Security Fixes
- Log4J Vulnerability (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105).
  - Scribbler Backend Service: Not using log4j for its internal logging. Vulnerability not applicable
  - Scribbler Log Collector (logstash): For log processing, filtering, and forwarding log4j is not at all used. Log4j is used by the log collector to write its own logs. Based on the vendor statement, it is vulnerable. But the vulnerability only applicable if any received data / user data is sent to log4j. Scribbler log collector does not send any user data to log4j hence the vulnerability is not applicable.
  - Scribbler Data Store (elasticsearch): Log4j is used to write its own log. But the vulnerability is not applicable because a security manager component already mitigated the issue.
  - However, the upstream modules (logstash, elastic search) patched the above vulnerability with the latest patch release. The fixes and patches are incorporated into scribbler.

Bug Fixes
- USR-686: Rare random start delay issue in scribbler fixed.
- BFX-713: Scribbler fails to work as expected with McAfee application control (solidifier)
  - Affected Version 1.6
  - Incorrect temp folder configuration of log collector
  - Scribbler takes long time to start in resource constrained environments and times out.

- o That is fixed by moving the time-consuming work into a background thread which runs after startup initialization is completed.
- BFX-706: A corner case authentication failure issue with Nested Active Directory Groups is fixed.
  - o A user who is part of two similarly named nested groups had issues during login where the system throws access denied.
  - o The problem is now correctly handled.

Known Issues
- Nil

Release 1.5.52

Release Information

Version	1.5.52
Date	June 28, 2021
Work Items	USR-503

New Features
- USR-503: Option to forward messages with IP address instead of hostname.
  - o Forwarding with hostname (old behavior) is the default.
  - o To enable forward with IP Address, the option must be explicitly turned on from the syslog forward settings.

Bug Fixes
- Nil

Known Issues
- Nil