BeyondInsight for Unix and Linux 22.2 Release Notes

June 30, 2022

New Features and Enhancements:

- **SIEM Integration: BIUL System Logs, Console Audit logs and Task Data**

    - Added REST APIs to search BIUL events.

    - Added REST API to configure sending events to SIEM.

    - Send BIUL events to SIEM.

- **Elastic Common Schema and Session Replay**

    - Created common data grid for ADBridge, PMUL, and BIUL events.

    - Support ECS formatted PMUL events.

    - Support ECS formatted AD Bridge events.

    - A conversion tool is available to convert v22.1.0 indexes to the 22.2.0 ECS indexes. Please contact BeyondTrust Support if you have used Elasticsearch with Privilege Management for Unix & Linux or AD Bridge v22.1.0.

    - Added support to search from multiple selected products.

    - Support searching ECS formatted PMUL IOlogs.

    - Updated PMUL SIEM assignment action to configure **elkdatatypes** setting.

    - Add Session Replay component to Unifed Search.

- **Updated Firstrun Wizard**

    - Created new version of First Run REST APIs, deprecated existing First Run APIs.

    - Replaced existing First Run wizard with new wizard.

- **Sudo Manager Integration**

    - Added REST APIs to install/upgrade/uninstall Sudo Manager.

    - Added Sudo Manager section to Software Actions wizard.

    - Added Sudo Manager to profile action.

    - Detect Sudo Manager alias when profiling.

    - Added Sudo Manager to Host Details.

    - Added REST APIs to manage Sudo Manager aliases.

    - Added Sudo Manager support to RNS details.

    - Added REST APIs to manage Sudo Manager policy files.

    - Added Sudo Manager policy file editor.

    - Added Sudo Manager alias management front end.

- **SSH Key Exchange Algorithm Configuration**

    - Added support for specifying custom ciphers and key exchange algorithms.

    - Added support for Diffie-Hellman group exchange SHA-256 and SHA-1 key exchange algorithms.

- **Miscellaneous**
  - Updated SQlite database file permissions.
  - Removed **.hostinfo** file when profiling.
  - Updated labels for switch components.
  - We now use **#!** to specify bash as the shell in remote scripts.
  - Added filter to grid column selector.

Issues Resolved:

- Resolved issue in which roles editor did not display all users.
- Resolved issue in which a SIEM search for the asterisk (*) character could crash Chrome.
- Resolved issue in which downloading key files did not succeed on Windows servers.
- Resolved error in which installing AD Bridge causes user's home directory to be owned by root.