Privilege Management for Unix and Linux 22.1 Release Notes

January 31, 2022

New Features and Enhancements:

- Added the capability to route eventlog records to Elasticsearch or Logstash instances located either on the customer premises or in the cloud, providing the ability to search all the eventlog records from multiple logservers in a centralized location.
- Added a sudo wrapper script. This script is designed to mimic sudo, using **pbrun** to execute the command.
- Upgraded third-party libraries.
- The third-party libraries used in Privilege Management for Unix and Linux 22.1 (PMUL), as well as lighttpd, have been upgraded to the following releases:
  - OpenSSL 1.1.1k
  - Kerberos 1.19.1
  - OpenLDAP 2.5.5
  - Curl 7.78.0
  - SQLite 3.36.0
  - UnixODBC 2.3.9
  - Jansson 2.13.1
  - libedit 20210714-3.1
  - libevent 2.1.12
  - libxml2 2.9.12
  - lighttpd 1.4.59
- Added support for TLS 1.3.
- With added support for OpenSSL v1.1, PMUL now also supports TLS 1.3. Valid options for the keyword **ssloptions** in **pb.settings** now includes **TLSMinV1.3** and **TLSMaxV1.3**. Valid options for the keyword **restssloptions** in **pb.settings** now includes **TLSMinV1.3**, **TLSMaxV1**, **TLSMaxV1.0**, **TLSMaxV1.1**, **TLSMaxV1.2** and **TLSMaxV1.3**. When using TLSv1.3, the configuration for pblighttpd is also updated to deprecate older SSL and TLS keywords.

  The keywords **sslservercipherlist** and **sslpbruncipherlist** now accept comma-delimited **cipherlist=<value>** and **tlsv1.3=<value>** key-value pairs. The key group **cipherlist=** lists the colon separated TLSv1.2 and below versions supported cipher list. The key group **tlsv1.3=** lists the colon separated TLSv1.3 supported cipher suites.

  A new install of PMUL 22.1 now uses a new default value for **sslpbruncipherlist** and **sslservercipherlist**, and the cipher group cipherlist of the keyword **sslservercipherlist** or **sslpbruncipherlist**.
- When upgrading to PMUL v22.1, we now continue to support older pbsudo clients.
- Before PMUL version 22.1, there was a limit of 512K for the eventlog record size. Version 22.1 now supports eventlog records of any size. Additionally, we have made improvements to the PMUL message router mechanism to efficiently allocate the memory needed to handle the eventlog records.
- The following new fields have been added to eventlog records to store additional timestamps on different hosts in the PMUL environment:
  - Runhost start and finish time
  - Logserver accept and reject time

  - Logserver finish time
  - Logserver keystroke time

  These fields contain the timestamp in UTC.

- Added **basedir** keyword in **pb.settings** to easily change default PMUL base directory during installation.
- Added the ability to search for leftover pblighttpd processes before restarting and when stopping.

Issues Resolved:

- Resolved role-based policy issue in which commands with a single-quote failed with the error *Failed to open/parse Role Based Policy - near "…": syntax error*.
- Resolved a licensing issue in which the comparison of the **auto-retire** value with **pblicenseretireafter** was done incorrectly.
- The binaries using libncurses.so (pbreplay, pbvi/pbnvi) no longer fail with *symbol lookup error: pb2110pbvi: undefined symbol: stdscr* on some Linux platforms.
- Resolved ACA issue with readlinkat() on AIX 7.1.
- Resolved issue in which a warning was not issued when the policy language statements explicitly disabled ACA, or denied the execution.
- Resolved curl errors when pblighttpd was on IPv4 and addressfamily was set to **any** in **pb.settings**.
- Resolved issue in which only the last chunk was wrriten to a file when using **pbrestcall -o** to save output to a file. We now correctly write the entire output.
- Resolved pbinstall issue in which messagerouterqueuesize was overwritten during an upgrade.
- Resolved issue in which pbinstall created pbrestdir base directory with wrong permissions.
- Resolved issue in which the output of **pbdbutil –info –msgs** displayed **maxq_sz** as a negative value if messagerouterqueuesize was set to a value larger than 4095.
- Resolved issue in which PMUL servers could no longer communicate with clients v10.3.2 or older, caused by a fix in v21.1.0 with Kerberos and SSL enabled.
- Resolved issue in which **pbrun --di <cmd>** produced a segmentation fault if the logserver failed due to a fatal error before it communicated back to pblocald.

Supported Platforms:

- ARM64/Graviton2 on Amazon Web Services: Can run PMUL on Amazon Linux 2 and Red Hat 8 ARM Graviton 2 instances within AWS.
- The existing **linux.x86_64** TAR file is now certified to run on RHEL 7 or 8 Workstation.
- Starting with PMUL 22.1, AIX supported releases are AIX 7.1 TL5 and AIX 7.2.

Known Issues:

- Various RHEL 8.x releases and updates have Kerberos/NIS changes that affect PMUL v22.1.0. PMUL diagnostic messages encountered include:
  - 3105.05 Unknown user
  - 3106.03 Unknown user ID
  - Various *connection closed* or *broken pipe* issues (with different numbered identifiers)

The workaround is to use the PMUL-supplied Kerberos library, even though PMUL is not configured for Kerberos. Change the following in **pb.settings**, then restart PMUL daemons (pbmasterd, pblocald, pblogd):

```
loadkrb5libs    yes
```