# Privilege Management for Unix and Linux 21.1 Release Notes

**June 15, 2021**

**New Features and Enhancements:**

- **Licensing:**
  - Added **freelicenseofautoretiredhosts** setting to **pb.settings**. When set to **yes**, permanently retires the hosts that are automatically retired, which means the number of clients in the license database will be decreased, but it also means that when the same host is reused, it will be only able to run PMUL after recycle period and if there are enough clients left in the license count. Default is **Yes**.
  - Changed the default value of **licensestatswqnum** to **999** and max value to **9999**.
- **Advanced Control and Audit:**
  - HP-UX PA-RISC binaries are no longer supported by ACA on HP-UX Itanium. If PA-RISC binaries are encountered by ACA, the following warning is displayed: *HP-UX PA-RISC executables are no longer supported by ACA.*
  - We now display a warning when ACA is enabled and OS capabilities are enabled that override ACA. The warning is: *WARNING executing binary with capabilities set*. The OS disables ACA.
  - **Role-Based Policy:**
    - In a role-based policy, we can now add both a user and a group to the policy when they have the same name.
  - **REST Services/API:**
    - The default REST call to get the list of events was changed to merge **Accept** event with corresponding **Finish** event into one record.
- **Miscellaneous:**
  - Improved the performance of processing of eventlog records in the SQLite database and the message router.
  - Improved the performance of **pblog -o** when processing eventlog databases over 33K.
  - Added an additional check to verify that the directory where the diagnostics logs are created is secure and is not accessible by non-privileged users.
  - Added an additional check to verify that the directory where the eventlogs are created is secure and is not accessible by non-privileged users.
  - **pb.settings** now shows the default value for all settings that have a default, when the value is not changed by the user.

**Important Information for This Release:**

- Changed the default for eventlog destination back to flat file.
- Privilege Management for Unix and Linux Basic Edition (PBSUDO) is no longer supported. The tar files are no longer included in the PMUL ISO file.
- The name of the tar file for AIX was changed from **pmul_aix61** to **pmul_aix** and **pmul_solaris9-10** to **pmul_solaris10**.
- Added support for RHEL8 on IBM zSeries s390x.
- Added support for SLES 15.
- HP Itanium 11.23 is no longer supported.
- RHEL 6 on IBM zSeries is no longer supported.

**Issues Resolved:**

- **Licensing:**
  - When retiring a host, the number of clients gets decremented by one. There was an issue in which the number was getting incremented when a permanently retired host's **recycle** date/time was reached, even though the host was retired.
  - Resolved issue in which the command **pbdbutil --lic -l '{"retired":true}'** did not return the list of retired hosts as soon as a host was auto-retired.
  - Resolved issue in which even existing licensed clients were not able to run **pbrun/pbsh/pbksh/pbssh** when the number of clients + 50% overage was reached.
- **Registry Name Service:**
  - Resolved issue that occurred when installing a secondary host in RNS environment using Client Registration, if a host was not designated as the primary logserver before **Change Management** feature was enabled.
  - Resolved issue in which assigning a host as secondary failed with a *4001.30 Invalid parameter - must supply reason message* error even when a reason message was supplied, when **Change Management** was enabled in RNS environment.
  - Resolved issue in which promotion failed with a *4053.09 Failed to lookup Servers in Service Group 'registry_name_service' - records or database not found* error if a host was promoted to the primary registry server before the **dbsyncrefresh** time was reached and before the service-related databases on the secondary were synced.
  - Resolved issue in which database synchronization of **/etc/pb.db** was relaunched for all hosts when one host was out of sync and causing **pb.db** on hosts that were synchronized to grow needlessly. We now only relaunch the database synchronization on hosts that are out of sync.
  - Resolved issue in which a database sync of a large **pbrbppolicy.db** file to a secondary failed with error message *4033.03 .. Operation timed out*.
- **Advanced Control and Audit:**
  - We now display a *WARNING executing a setuid/setgid binary on AIX or HPUX* warning on AIX and HP operating systems on which ACA is disabled for setuid binaries. The OS disables ACA.
  - Resolved an issue in which **pbrun** produced a segmentation fault when the ACA default rule was added to a policy and splunk binary was invoked.
  - Resolved issue in which no error was logged at the destination when the ACA default rule was added to the policy, the **enablesessionhistory** argument **noexitonerror** was set to **true: enablesessionhistory(true,true)**, and **errlog=<destination>** was set in **eventdestination** in **pb.settings**.
  - Resolved issue on Ubuntu and Debian systems in which ACA libraries were copied to the incorrect directory. They are now copied to **/lib/x86_64-linux-gnu**.
  - Resolved issue on AIX in which invoking **crontab** failed with the error message: *crontab: 0481-124 Cannot create the cron file in the /usr/spool/cron/crontabs directory* when the ACA default rule was added to the policy.
  - Resolved issue on RHEL 7 and 8 in which invoking **mailx** failed with the error message *temporary mail message file: permission denied* when the ACA default rule was added to the policy.
  - Resolved issue in which the symlinks to a directory or file were not blocked when access to the directory or file was blocked using an ACA rule in the policy.
  - Resolved issue On AIX in which the command **userdel** did not return any error, but the user was not deleted when the ACA default rule was added to the policy.
- **Role-Based Policy:**
  - Resolved issue in which **pbrun -e** (entitlement report) did not failover to next policy server if the first one was unavailable when role-based policy was enabled.
  - Resolved issue in which **pbrun** did not require **-u** as it should have and defaulted to the first user in the list when role-based policy was enabled and the runuser list contained more than one user. We now require **-u <user>** to specify which user in the list should be used.

  - Resolved issue in which the errors were not correctly reported when initializing the role-based policy database.
  - Resolved issue in which the role-based policy connection was not safely closed.
  - Resolved issue in which the **pbrestcall** to get the user/group info for an AD user/group did not return the info when **enumerate** was set to **False**.
  - Resolved issue in which **pbrun -e** failed with error message *3106.07... host not found* when submitmasters was set to an SRV record.
  - Resolved issue in which displaying the role-based policy entitlement report for a single system user did not work when using wildcards in the username.
  - Resolved several entitlement reporting issues that involved role-based policy with multiple roles.
  - Resolved issue in which adding a single user with wildcard character in the role-based policy reported an error, but the user was added to WHO list.
  - Resolved issue in which the exported role-based policy format was different between REST call and the command line interface.
  - Resolved issue in which requests from allowed sssd user failed because the policy server was not aware of secondary sssd groups when **enumerate=False**.
- **REST Services/API:**
  - Resolved issue in which PMUL installation installed init scripts to start/run PMUL daemons but REST services were not properly configured on Linux hosts that had no xinetd/system installed.
  - Resolved issue in which the arguments of the processes **pblighttpd** and **pbconfigd** were missing in the output of **ps** on On RHEL 7 systems.
  - Resolved issue in which the exit code was non-zero and the proper HTTP error was displayed when REST call (in **pbdbutil**, or **pbrestcall**) data was larger than the max 512MB.
  - Resolved issue in which the **pblighttpd-svc** process, responsible for processing the eventlog, was consuming more and more memory when continuously running and processing a large number of PMUL requests. Additionally, when a large flat file **pb.eventlog** was processed by **pblog**, it quickly consumed swap space and memory, and the Linux OOM killer terminated **pblog**.
- **Miscellaneous:**
  - Resolved issue in which **pblog** showed an undefined status for the event when a Finish event was logged before the corresponding Accept event.
  - Resolved issue on RHEL8 systems in which **pbssh** failed with error message *error while loading shared libraries: libtinfo.so.5* when an AKA policy was enabled for **pbssh**.
  - Resolved issue in which **pbrun** failed with error message *5121 readMuxHeader* if PAM was enabled and **pam_session** emitted a text.
  - Resolved issue in which **pbrun -h <runhost> <command>** (or **pbrun --di**) failed with error message *3386 Maximum log server failures (25) exceeded* when **iologack** was enabled on the runhost.
  - Resolved issue in which client could not connect to the policy server when the encryption used on the client was the second on the list of policy servers when Kerberos was enabled and network encryption was set to multiple encryptions.
  - Resolved issue in which **pbrun** hung if both Kerberos and ssl were enabled and **ssloptions** was set to **sslfirst**.
  - Resolved issue in which **pbinstall** added an additional encryption algorithm and file (**aes-256:keyfile=/etc/pbfipskey.key**) to the list when upgrading PMUL.
  - Resolved issue in which the package installer did not fully support PMUL services on Linux systems where xinetd/systemd was not installed.
  - Resolved issue in which the **addressfamily** setting was removed during upgrades, if it was set.
  - Resolved issue in which **pb.key** and its container directory were not created if they did not exist during install.

- Resolved issue in which the install failed if **changemanagement** was set to **yes** on the first server during the installation if client registration was used.
- Resolved issue in which **pbinstall** did not create **pbssl.pem** if **enforcehighsecurity** was set to **no** but **ssl** was set to **yes**.
- Resolved issue in which **pbinstall** reverted the value of some settings to their default values during an upgrade.
- Resolved issue in which **pbinstall** did not correctly exit, but instead asked for the platform type when it was launched in batch mode on an unsupported platform.