Privilege Management for Unix and Linux Version History

What's new in

PowerBroker for Unix & Linux

PowerBroker for Virtualization

PowerBroker for Network

Version 10.1.0

Document Revision 1, December 17, 2018

Thank you for selecting BeyondTrust PowerBroker. This file contains important
information regarding the current version of this product including new
features and changes. Further details can be found in the PowerBroker for Unix & Linux manuals.
This document is current as of the date of publication. The most
current version is available from www.beyondtrust.com.
BeyondTrust welcomes your comments and suggestions. Please use the
information provided at the end of this file to contact us.

WHAT'S IN THIS FILE

- New Features
- Significant Bug Fixes
- Known Issues
- Additional Information
- Documentation

Note: BeyondTrust recommends that before any clients are upgraded to the latest
release of PowerBroker for Unix & Linux, the Policy Server (Master) and the Log servers
should be upgraded to the latest release.
For the list of new features and bug fixes in PowerBroker for Sudo,
refer to the release notes of PowerBroker for Sudo.

NEW FEATURES IN RELEASE 10.1.0:

1. A Fast Message Router mechanism is now used to better cope with high volumes of event

and log information. The Log Server will communicate all of its updates to the Message Router, which will then log the audit and log information to the appropriate places, including the Event Log, Log Caching, The BeyondInsight Event queues, and the SOLR/lologcloseaction queues.
The pblighttpd service, which previously started the REST and Scheduler services, will now also start the Message Router services. If the Message Router is down, the Log Server will store all of its data in a temporary queue until the Message Router service is available again.
The new Message Router service will streamline the processing of Events and other important messages throughout the system. It allows a single Log Server to quickly accept, process and store tens of thousands of events every second.
The new Message Router mechanism also solves the concurrent writing of eventlog records to pb.eventlog and the resulting locking and performance issues.
2. With the introduction of message router to forward events to BeyondInsight, and the use of event queues to store the events, the store and forward mechanism no longer uses a file and the binary pbfwdevents is obsolete.
3. To mitigate locking of pb.db database, the scheduling related tables were moved from /etc/pb.db to /opt/pbul/dbs/pbsched.db.
4. To mitigate locking of pbiologaction.db database, the iologaction pid tables were moved from to /opt/pbul/dbs/pbiologaction.db.pid.
5. A safety mechanism was added to pbconfigd to gracefully exit and re-start if the memory footprint increases past a specified amount - initially 128mb. The pbconfigd will exit with the following message in pbrest.log: " <date> [pid] pbrest process exiting for refresh..."
6. The setting 'databaselocktimeout' was enhanced to accept delay and retry number for the full list of services: license, rns, dbsync, akapolicy, iologidx, restkey, fim, event, logcache, rbp, sudo, sched, polpvar, logarchive, intprod, clientreg and pbpolicy.
There is also a default service that will be applied when a more specific setting has not been configured.
Values take the format of "service=<delay>,<retries>", where delay is in microseconds.
Example
databaselocktimeouts default=1000,30 fim=2000,60 rbp=500,10
7. masterprotocoltimeout and logserverprotocoltimeout were limited to 1200000 microseconds (1.2 seconds) which was too short for busy system. The maximum was increased to 30000000 microseconds (30 seconds).
8. getuserpasswd/getuserpasswdpam and submitconfirmuser/submitconfiruserpam were enhanced to allow the specification of a persistent variable, which will allow the automatic reauthentication to work as planned across multiple policy servers.
9. ACA function was enhanced to add the ability to block *<command>. If the 'filespecs' argument begin

with “*” it will allow wildcards to match any slash in the path. This allows for example, "*/reboot" to match /usr/bin/reboot, /usr/sbin/reboot, /bin/reboot, /sbin/reboot, and /usr/local/bin/reboot.

10. pblog now reports finish events that appeared before the corresponding accept event.

11. pblogarchive no longer archives the eventlog in a "unknown_logserver" folder, when the first eventlog record in pb.eventlog was a finish event,

12. Two new fields, description and comment, were added to AKA policy structure.

13. The command 'pbdbutil --evt -l' now lists the available 'taxonomy' values.

14. Role-based Policy enhancements:

- Added support for variables for IOLOG location and name
- Added the ability to show Policy Server Name and Role Name on Accept/Reject output
- Added Custom Accept Message & Custom Reject Message
- Added an option -e to pbrun to show user privileges (role-based policy only).
- Added an option --rbp -E to pbdbutil to show privileges and filter by host or filter by user.
- Added a re-authentication options from submithost, runhost or Policy Server Password or call PAM.
- Added an option to allow re-write of ranges of parameters
- Added a REST Endpoint to test roles
- Added the ability to set runuser=submituser
- Added the ability to evaluate the client mode (shell command, run, shell start)

15. New supported platforms:

- SLES 12 on PowerPC (Big and Little Endian)
- Mac OSX 10.13 High Sierra

SIGNIFICANT BUG FIXES IN RELEASE 10.1.0:

1. Syslog messages are no longer truncated to 1024 bytes. There is no longer a maximum size and the entire syslog message is processed.

2. When re-runing pbinstall to upgrade or re-install, the following keywords were not retained in pb.settings:

advkeystrokeactionevents, advkeystrokeactionlog, fileintegritydblocktimeout, indexcommandtimestamps, iologack, iologactioninterval, solrindextimeout, tcpkeepalive, pbresttimeout, licensestatswqnum, logarchivedb_delay, logcachedb_delay, pblicensedblocktimeout, pblicensequeuetimeouts, pblicenserefresh, pblicenseretireafter, messagerouterclosewait, messagerouterqueuesize, messageroutersocketpath, writequeuenum, writequeuepath, writequeuetimeouts

3. solrinstall was failing if JAVA_HOME was not in the list of environment variables and was only

specified through the menu option.

4. solrinstall did not exit with non-zero value if the installation succeeded but solr couldn't be started.

5. The new v10 licensing did not check Solr license if the Log Server was on a different host than the Policy Server.

6. The new v10 licensing was not generating a valid unique hostid for a Mac OSX client.

7. If a "journal" file (/etc/pb.db-journal) is left over after pblighttpd service was not properly shut down, restarting pblighttpd no longer fails with error:
"Exiting settings file /etc/pb.settings does not exist, or is empty".

8. Starting with v10.0, an issue was introduced where pbmasterd failed with error "5622.1 Policy Server error getting peer name - Invalid IP protocol" when configured to unix domain sockets.

9. pbdbutil --sudo -U (unlock locked policy file in sudoersdb) is now working properly, unlocking the sudo database.

10. Starting with v10.0.1, an issue was introduced where running "pbrun -h <host> bash" with iologging on, was causing either the prompt to be lost, or the session exited.

11. When iolog was greater than indexlogsizelimit, pbreplay failed to mark iolog as finished in pbiologaction.db.

12. Starting in v10.0, handling of UTF8 characters failed when a PBUL component with v10.0 communicated with another with version lower than v10.0.

13. When REST services were not installed on a host where only run/submit host was installed, pblocald service was missing.

14. A "reject" eventlog record did not have the "uniqueid" field when it was created due to a license constraint (e.g. no valid license, or not enough clients)

15. Starting with v10.0, submitconfirmuserpam did not process the value of the argument 'pampasswordservice' and was using local authentication instead of pam authentication.

16. pbrun’s optimized run mode no longer creates a pty when there is no tty (e.g. stdin, stdout, stderr are all redirected) or when -p pipe mode is used.

17. ACA’s trap of dup2() resulted in memory corruption when passed the same fd for both oldfd and newfd. This often resulted in pbreplay reporting an error similar to: error unable to decode byte 0xe0 near "" loading json data.

18. Several memory leaks were fixed in pbconfigd, pblighttpd-svc, pblogd and pbmasterd.

NEW FEATURES IN RELEASE 10.0.1:

1. Splunk Integration:

- PowerBroker Unix/Linux now has a Splunk App available from the Splunk

web site called "BeyondTrust App for Splunk". You can find it on
https://splunkbase.splunk.com/app/4017/ or from within
the Splunk GUI “Apps -> Find More Apps”.
- In the default policy installed, a new SplunkRole procedure is added
to pbul_functions.conf, which will be enabled if 'EnableSplunkRole'
variable in pbul_policy.conf is set to 'true' (default is 'false').
This procedure enables iologging, aca history, and sets iologcloseaction
to a script sending records to Splunk.
- The script 'closeactionsplunk.pl' is installed by default in
/opt/pbul/scripts and can be used to send ACA data to Splunk, using the
'iologclosaction()' Policy procedure. Perl modules such as perl-JSON and
perl-Sys-Syslog may need to be installed to use this perl script.

For more information refer to the 'Splunk Integration' chapter in the Admin Guide.
2. Added ability to run a script on the logserver, when an iolog file is closed.
For PBUL iolog, add 'iologcloseaction(<script>)' to the policy.
For PBSUDO, use 'pbsudo_iologcloseaction' in pb.settings.
3. The new 'syslogsession_finished_format_logserver' was added that sends exit
status data to syslog, operating from the logserver, as opposed to the
syslogsession_finished_format keyword that operates from each runhost.
4. A new eventlog variable 'runhostip' was added.
5. When installing PBUL for the first time using pbinstall, two separate keyfiles
will be installed by default: pb.key for networkencryption and pb.rest.key
for restkeyencryption.
6. The REST API can now selectively be installed on the PBUL clients.
7. When installing the license server only, the pbkey binary will now be installed.
8. The iolog queuing mechanism introduced in v10.0.0 was changed. When upgrading
from 10.0.0 to 10.0.1, the data is automatically migrated in pbiologaction.db.

SIGNIFICANT BUG FIXES IN RELEASE 10.0.1:
1. In v10.0.0, the value of "uuid" in the Licensing database was changed when
pbrun was executed in local mode with a non-root user.
2. In v10.0.0, the value of "uuid" was set to the same value when command was
run as a non-root user, and the hosts (VMs within the same ESX server) had

the same /var/lib/dbus/machine-id.

3. In v10.0.0, the command pbadmin --lic -l '{"retired":true}' and '{"retired":false}' displayed the output, but terminated with a "signal 6 (Abort)".

4. In v10.0.0, pbssh intermittently had terminal issues such as lost echo, ^D hanging, and failed with "3201.08 Exec of pbssh failed: Success"

5. pbssh, with AKA enabled, had interactive mode issues with commands that need paging (more, less, ...).

6. pbksh and pbsh did not log a session finish eventlog record when iologging was not enabled.

7. When 'pbrunreconnection' was set to 'true' in the policy, intermittently, pbmasterd terminated with a segmentation violation, resulting in pbrun failing with "8523 Client failure in SSL_connect() error:1408F10B:SSL".

8. The password was captured in the iolog file when the username and password were the same.

9. When an iolog file was created with multiple "parts" (due to logserver failover), and Solr indexing was enabled, only the last iolog file was indexed.

10. When iologging was enabled, pblocald leaked the logserver file descriptor to the secured task.

11. In the ACA session audit, all the exec* mechanisms ended up logging an "owner" "allowed" record when the "owner" perm is not used.

12. When the submituser and runuser have different ulimits for max files, ACA failed to audit ACA command due to bad file descriptors.

13. PBSUDO failed to process the files in "includedir" directive of sudoers. The files were imported into the database, and retrieved into the cache, but were not processed by pbsudoers.so.

14. PBSUDO failed if sudoers contain "#includedir <dir>" and <dir> is empty.

15. If syslog_xxx_format keywords in pb.settings used double-quotes, the keywords lost their values after an upgrade.

NEW FEATURES IN RELEASE 10.0.0:

****

****

PowerBroker for Unix & Linux [PBUL] v10.0

CRITICAL LICENSE CHANGES

If you are upgrading from a prior version of PowerBroker you
MUST OBTAIN A NEW LICENSE.
To obtain a new license follow the instructions below.
On your designated Primary License Server (10.0 and above):
1. Extract the platform specific tarball for that system
2. Navigate to the 'bin' folder where the tarball was extracted
3. Run pbdbutil --info --uuid
4. Contact your BeyondTrust License provider with your HostId
If you need more details about the new ‘License Server’ role please
reference page 152 of the Admin Guide, reference the release notes,
or contact support.
In PBUL Version 10.0 and above, all server components can act as a
redundant license server, however only one license is required on
the PBUL primary license server.
****
****
1. Centralized licensing database with component based licensing options:
A new licensing scheme has been introduced in v10.0.0, where the license string
consists of a JSON (JavaScript Object Notation) string that details services,
facilities and expiry.
The license string is now stored the license server (not the Policy Server),
and will be centralized and synchronized automatically to secondary license servers.
It is based on the "uuid" of the license server host (pbdbutil --info --uuid) and
contains a number of clients for each component (services), except for ACA and Solr
that are either enabled or disabled. For more information on the license services,
and attributes, please refer to the Admin Guide.
pbinstall has been changed to install the license server, setting the new
licensing keywords. The new 'licenseservers' setting is a list of servers that
will manage/maintain the product license and client counts.
A temporary license is installed automatically if a standard license is not provided
when the Primary License Server is installed. It will enable 20 client seats for all
services and enable all facilities. The license will be valid for 60 days.
2. Integration with PowerBroker Management Console (PBSMC) V6:
PBSMC V6 now allows the installation of the primary and secondary licenser servers,

as well as the Solr host.

PBSMC provides interfaces to view and search the eventlog records, search the iolog files indexed by Solr, and replay iologs.

3. Solr install changes:

This release of solrinstall allows SSL keys and certificates, in PEM format, as opposed to acquiring the keys and certificates from BeyondInsight.

OpenSSL is a new requirement for this capability and will be used to convert the PEM files to pkcs12 format for installation into the Solr's Java keystore.

This allow Solr to be installed to work with PBSMC.

Solr install now locate JAVA_HOME automatically if not provided on the command line.

4. IOlog indexing: A new mechanism will be used (on all OS, except for OSX), that will queue the iolog filename, rather than process it immediately. The pbconfigd scheduler will process the queued iolog filenames, launching a configurable maximum number of pbreplay processes.

The default database containing the iolog filename queue is specified with the "iologactiondb" keyword in pb.settings. If not specified, the default is "pbiologaction.db" located in the directory specified by databasedir.

The new "solrmaxindexprocs" specifies the maximum number of pbreplay processes, controlled by pbconfigd, that should be indexing iologs at any given time.

The new pbreplay option -Q will inform pbreplay to de-queue the filename, pbreplay will index the iolog, and loop up to 50 times to de-queue and index additional iolog files.

5. A new keyword was "indexlogsizelimit" was added to pb.settings specifying a size limit for IOlogs to be indexed, and a keyword "logskipindexfile" was added to specify whether IOlogs over that size will be reported to syslog and/or pbreplaylog.

There will not be a default for the 'indexlogsizelimit' keyword, and if not set, all IOlogs will be indexed.

pbreplay will read the indexlogsizelimit keyword, and if present, if the size of the IOlog file is greater than the keyword specifies, a message will be written to syslog and/or replaylog indicating the iolog filename that was skipped.

6. A new keyword "solrindextimeout" was added to pb.settings specifying a time limit in seconds, during iolog indexing, for both the connection phase and the sending of each chunk to Solr. When a timeout occurs, the existing diagnostic message

"2036 file:%s curl_easy_perform error: %d %s http response:%ld"
is written to pbreplay.log.
If solrindextimeout is not set, or is set to -1, there is no timeout.
7. A new keyword "pbresttimeout" was added to pb.settings allowing to set the maximum amount of time a REST service will wait until it times out.
8. pbinstall now creates a pb.settings with all available keywords, with unused settings appearing as commented-out lines.
9. The AIX tar file is now renamed from pbul_aix52+ to pbul_aix53+, reflecting the fact that AIX 5.2 is no longer a supported platform.

SIGNIFICANT BUG FIXES IN RELEASE 10.0.0:

1. When RNS is enabled, the sudo policy database was not synchronized to the secondary sudo policy servers after the initial synchronization.
2. When ACA was enabled, the command "tar cvf" was failing with error:
"tar: <file>: Cannot open: Permission denied".
3. When change management was enabled, deleting a record from the AKA database was failing, asking for a reason message, despite the reason being provided.
4. An extra prompt was displayed at the finish using the "interactive" AKA policy method.
5. FIM reports failed with exit value 22, when JSON data exceeded 20MB.
6. When Solr was enabled and an iolog was indexed, pblogd terminated with Signal 15 on RHEL 7.1 using systemd.
7. When Solr was enabled and an iolog was indexed, pbreplay intermittently terminated with a segmentation violation.
8. solrinstall was ignoring the value specified by -a option for rcsuser.
9. When upgrading from a installation without RNS, and enabling RNS, older clients were failing with the error "3003.03 Could not connect to a log server daemon".
10. When RNS was enabled during the installation of a secondary server, database creation warnings were displayed at the end of the install process.
11. Issues with running daemons with -f options were fixed in the script 'pbul-rc' which is used by pbinstall to create the /etc/init.d pbul daemon scripts when installing on linux machines that do not have systemd/xinetd installed.
12. Settings that allow quotes in value are losing quotes when settings file is re-written with a pbrestcall PUT for a setting update.
13. On RHEL 7, when upgrading from v9.4.3 or older to v9.4.5 or newer, the pblighttpd

daemon was not stopped during the upgrade, and therefore the older release
of pbconfigd and pblighttpd continued to run despite the upgrade.

NEW FEATURES IN RELEASE 9.4.5-10

1. File Integrity Monitoring:

- The option "--noreport" was added to "pbdbutil --fim -U" to not send a report.
- The commands pbdbutil --fim "-A <host>" or "-X <host>" now allow both fully
qualified hostnames as well as short hostnames.
- Reduction of memory footprint and increase in speed for "pbdbutil --fim" search
and filtering commands.

2. REST API:

- Addition of Policy check to allow checking of PBUL script-based policies.
- Addition of Policy check to allow checking of Sudoers policies.
- Addition of methods to check if successfull REST calls can be made to the
specificed hostname.
- Errors in pbrest.log now display the host and user information if applicable.

3. Client-based REST Services:

REST Services are now enabled by default on PBUL runhost/submithost. The processes
pblighttpd/pbconfigd do not run at all time (as they do on Servers), but "wake up"
when necessary.

3. New "Persistent Variables" functions and procedures to the PBUL policy language:

Persistent Variables are a method of setting variables that persist for a specified
time, and are synchronized across all of the Policy Master Servers in the enterprise.
Procedures are provided to list, get, set and delete Persistent Variables.
An example of use can be to define a prompt-free time period after the first
successful password verification in the policy.

4. Addition of include files to Advanced Keystroke Actions to allow the specification
of additional policy.

5. On a fresh install, new default will be used for SSL:

In pb.settings:

sslpbruncipherlist HIGH:!SSLv2:!3DES:!MD5:@STRENGTH

sslservercipherlist HIGH:!SSLv2:!3DES:!MD5:@STRENGTH

In pblighttpd.conf:

ssl.cipher-list = "HIGH:!SSLv2:!3DES:!MD5:@STRENGTH"

ssl.use-sslv2 = "disable"

ssl.use-sslv3 = "disable"

server.use-ipv6 = "enable"

server.set-v6only = "disable"

7. New supported platforms:

- Mac OSX 10.11 and 10.12

- Oracle Linux on Sparc 64

Please refer to the README file for the specific flavor names.

_____

SIGNIFICANT BUG FIXES IN RELEASE 9.4.5-10

1. ACA Issues:

- AIX breaks "find" command

ACA did not trap the opendir64() function, causing the find command to fail.

Added a trap for opendir64.

- AIX csh fcntl F_CLOSEM error closing fd

fcntl with the F_CLOSEM command, resulted in the closing of the ACA policy and audit FDs.

Protected the ACA FDs against closing.

- All numbers in audit logs on AIX are zero. results in pbreplay -A not replaying.

- HPUX tcsh output mangled

Csh closed stdout and stderr. An internal ACA socketpair thus received FDs 2 and 3.

Shifted the socketpair FDs past 3.

- Issues with symlinked directories (memory issues on Solaris)

Malloc returned an area of memory used by the chdir path argument.

Used mmap to create memory for ACA use, thus bypassing malloc.

- Performance issue when ACA is enabled on AIX when 'locale' affects dlerror()

Normal conditions caused dllerror() internals to open

message catalogs many times, causing significant delay (30..45 seconds).

Added code to check and set the locale to "C" if necessary.

- mkdirat AIX returns EINVAL

ACA had the incorrect value for AT_FDCWD for AIX.

Corrected the AT_FDCWD value for AIX

- partial iologs generated after delegated tasks complete

Timing conditions resulted in the daemon detection code to open a new iolog.

Added additional code to close the ACA FDs if applicable.

- Solaris 11.1 segv in dlsym when symbol is unknown

Solaris dlsym was calling fcntl, for which ACA had not yet determined the address.

Moved several unknown-to-Solaris symbols below the fcntl symbol in the internal table.

2. File Integrity Monitoring Issues:

- When a FIM database issue was occuring on the FIM server, the FIM client was not reporting the issue.
- Because the "file" keyword was not in the FIM policy predefs, the changes to filenames were not detected. The keywords "file" and "ftype" have now been added to default policy predefs.
- The "rundate" in FIM reports was not correctly converted to a Unix epoch.
- perm and pmask were always "000" in FIM reports.
- Improvement in error handling of FIM errors, displaying the valid error codes.
- Added correct handling of characters that are not valid UTF-8.
- FIM reports did not always use the --format specified on the command line.

3. REST Services Issues:

- pblighttpd did not use systemd by default on systems that support it.

It was still installing the service as a traditional SysV service.

- The REST API "PUT" only accepted old pb.key format keys generated using "pbkey -f". It now accepts new pb.key generated by "pbkey -F".
- pblighttpd-launch produced a "segmentation fault" on Red Hat Itanium.
- After a "pbrestcall -X PUT" on /etc/pb.settings, the keyword "replaytimeformat" no longer had the double-quotes around the values, making it invalid.
- After a "pbrestcall -X PUT" on /etc/pb.settings, the commented out variables were removed from the re-formatted pb.settings.
- After a "pbrestcall -X PUT" on /etc/pb.settings, the keywords "pbrestkeyfile", "pbsshshell" and "rootshelldefaultiolog" were missing from the re-formatted pb.settings.

4. The registration profiles 'default' was not created when running pbinstall with RNS enabled.

5. The keyword 'eventlog' was missing in pb.settings on a logserver-only host.

6. The keyword 'logserver' was not set on a runhost/submithost installation.

This keyword is now used on runhost/submithost installs for FIM, ACA logs and needs to be enabled.

7. The keyword 'pbadminpath' was not set on on a runhost/submithost installation.
'pbadminpath' is now needed by ACA, and need to be enabled on clients.
8. When in a PBUL policy, if rungroups contained unknown group numbers, pbrun and
pblocald terminated with 'signal 11 (Segmentation fault)'.

9. The options -Q, -Z, -S <yes/no>, -T, and -X were not honored when running
pbinstall -b (batch mode).
10. The following 'pbdbutil CSV output' columns would change order at every use:
List cfg
List rest keys
List FIM cfg
List creds
pbsudo list alias
pbsudo list policies
List svc cache
RNS list service groups
RNS list hosts
dbsync list outstanding
11. PBUL superserver-managed daemon ports are not enabled/not listening after package
installation on solaris9-x86.

NEW FEATURES IN RELEASE 9.4.4-10
1. Advanced Keystroke Action:
A new feature called Advanced Keystroke Action has been introduced to allow control and audit of
command line based network appliances. The new technology has been implemented as an enhancement
to the "pbssh" feature. PBUL policy specifies who can administer designated networking equipment,
integrating with PowerBroker Password Safe to seamlessly provide authentication credentials and new
Advanced Keystroke Action policy defines access, down to the individual command.
Full session logging provides a complete command audit trail through the existing session logging
technology.
Advanced Keystroke Action differs from previous features in that instead of trying to apply command
control as the user types, it emulates an interactive command line, and only then authorizes the
command once the user has pressed "enter" to execute the command. This means the policy can try to
match the command it has received in context to the task the user is performing, and it can choose to

re-write the command, accept it or reject it. It also allows the policy to change the user environment as they carry out their tasks, changing prompts or tab completion.

2. Add functionality to 'eventdestinations' settings to allow REST based events to be piped into a script/binary.

3. Role-based policy improvements:

- In the eventlog, the variable 'lineinfile' will contain 'norole' for an implicit reject.
- An 'ingroup' functionality was added to Role-based policy to allow rules to use a user of an already defined group (local or AD).

4. Improvement to Kerberos error messages:

When Kerberos was enabled, and an error occured, unhelpful diagnostics containing the Kerberos error numbers was displayed. The error messages have been improved to resolve the error codes into a more meaningful diagnostic.

SIGNIFICANT BUG FIXES IN RELEASE 9.4.4-10

1. PBUL was generating user's Kerberos ticket with wrong ownership (owned by root). The ownership of the Kerberos ticket is now set correctly and will be owned by the user that generated the ticket.

2. On a fresh install of v9.4.3, when Registry Name Services is enabled, pbrun failed when executed by a non-root user, due to the permissions of /opt/pbul and /opt/pbul/dbs being set to 600.

3. In v9.4.0 and above, installation on Mac OSX did not install pblighttpd service and the error: "pblighttpd.plist: No such file or directory" was displayed during the install.

4. When the primary NIC is down, some pbdbutil commands failed with the rest error: "4507.02 Failed to call REST service - Failed to connect to host or proxy"
pblighttpd now connects to the loopback device also when the primary interface is down.

5. "pbdbutil --sudo -e" failed with "Failed to call REST service - Failed to write file" and did not export the sudoers file.

6. Role-based Policy Issues:

- The 'command' variable in the eventlog occasionally contained incorrect data.
- pbksh/pbsh failed when Role-based Policy was enabled.
- Setting iolog to a string without trailing XXXXXX produced an error.
- submituser was set to first user from runuser list.

7. "dos2unix" (and some other commands) failed when ACA is enabled in the policy. This was due to lack of support for system call mkstemp in ACA.

8. The atrributes "newer" and "older" in pbdbutil --fim reports were not working and when used, the error: "8301.83 Invalid attribute - hours" was displayed.

9. When any file was retrieved by REST service, if it was versioned, it was truncated at the length of the newest version.

10. When there is no existing eventlog files, and log caching is enabled ('logcachedb' is set), the error: "6105.4 Error adding record to event logfile location cache database - 787 FOREIGN KEY constraint failed" was displayed in pblogd.log at the first invokation of pbrun. This is now fixed.

11. Package Installers Issues:

- If the configuration package was built on a xinetd-only host, when installing on a systemd-capable host, it configured xinetd instead of systemd.
- When upgrading PBUL linux packages from an older version not supporting systemd, the property list of systemd was updated but xinetd was still being used.
- After upgrading the loghost package, programs that rely on the REST service no longer worked.
- Description of pbrest package was wrong.

NEW FEATURES IN RELEASE 9.4.3-18

1. PowerBroker for Unix & Linux GUI is now in maintenance mode only. From 9.4.3 onwards, the GUI will also only provide restricted functionality. PowerBroker for Unix & Linux GUI is now limited to only allow the viewing of the eventlog and iologs.

2. The default policy directory is changed from /etc to /opt/pbul/policies. When installing the Policy Server on a new host, policydir and policyfile will default to this new location. Of course, during an upgrade, the current values are kept.

3. pbguid is now able to replay an iolog file, if the file is archived using PBUL archiving feature.

4. The native package installers now support Registry Name Services.

5. If 'rcseventstorefile' is not specified in the pb.settings, it now uses the default value /var/log/pb.rcs_eventstore (/usr/adm on AIX and /var/adm on HP and Solaris). Also, the parent directory is now created if the path specified does not exist.

6. Role-based policy now logs the role name used in the "lineinfile" eventlog attribute.

7. Advanced Control & Audit (ACA) enhancements:

- ACA diagnostic messages are now sent to a central Policy/Log Server.
- ACA diagnostic messages now have a common "tag": PBULACA

8. File Integrity Monitoring (FIM) enhancements:

- Added pbdbutil capability to remotely manage FIM.
- Added filetype to reports to differentiate files/directories.
- FIM Policy configuration can now be replicated to other FIM Servers.
- Added risk rating fields to report for deleted items.

9. FIM behavioral changes from 9.4.1:
- Symbolic links, when the link is not broken, now save and report the link target's final canonicalized name as well as the link target's device and inode. These are reported as fields 'linktarget', 'linkdev', and 'linkino'. This data is stored, and checked within the hash field.
- Files are new scanned in order of entries in the 'include' section, according to the first pattern that matches the file. Any subsequent file matching patterns will be ignored. This is a reversal of earlier behavior to make file processing more consistent with directory processing.

SIGNIFICANT BUG FIXES IN RELEASE 9.4.3

1. Fixed licensing issue when installing Policy Server from Solaris package installer.
2. Fixed Role-based policy issue where authorization of specific users (non-wildcard) in Role Based Policy was failing.
3. Fixed licensing issues when clients have multiple NICS.
4. Fixed partial IO log file names retaining old part numbers.
5. Fixed PBSUDO partial IO log file when pblogd terminates.
6. Fixed remotesystem policy function assigning to readonly variables.
7. Uninstall of packages did not remove several files.
8. Upgrading rpm packages no longer removes xinetd services.
9. Uninstalling rpm packages now removes all systemd slice unit-files
10. ACA issues:
- Fixed issue when secured task is a shell script without shell directive.
- Several issues with ksh and csh were addresssed.
- The execvpe() was not properly trapped.
- Fixed intermittent segmentation fault with system and popen when log>=3.
- Fixed intermittent policy corruption.
- pbmasterd can now record ACA data without a logserver.
- Fixed issue when pbrun's secured task is different 32/64 bits than the default shell.

- Fixed issue with ACA auditing daemons after pbrun exits.
- Protected internal auditing file descriptors from fcntl.
- Addressed functions susceptible to EINTR.
- When cwd cannot be determined via stat, it is retrieved from the environment.

11. FIM Issues:

- Several link processing issues were addressed.
- Fixed fields appearing out of order in CSV reports.
- Fixed FIM report showing true/false instead of number of files deleted.
- Increased in internal report buffer from 134MB to 1GB.

NEW FEATURES IN RELEASE 9.4.1-03 (replacing 9.4.0-18)

1. When ACA is used only for session history, and no files or operations are blocked, an optional parameter has been added to enablesessionhistory, that when set to true, will cause ACA to continue when non-fatal errors are encountered. This results in the task being allowed to continue, however the session history recorded will be incomplete.

The relevant portion of the policy should be similar to:

aca("file", "default", "all");

enablesessionhistory(true, true);

iolog=<file>;

2. ACA errors are now also logged to syslog.

SIGNIFICANT BUG FIXES IN RELEASE 9.4.1-03 (replacing 9.4.0-18)

1- When running pbsudoinstall, typing return to the question:

Would you like to create a new alias (c), or add the host separately (s) [s]:

will now correctly use the default "s" (add the host separately).

2- pbsudouninstall did not restore the sudoers file when the primary sudo policy server was RNS enabled.

3- When logcachedb is enabled (uncommented) in pb.settings, and numerous simultaneous pbrun requests are issued logcaching was failing with an error:

"6100.4 Error opening database '/opt/pbul/dbs/pblogcache.db' - database is locked".

4- On a fresh install, on CentOS 7.2, systemd services did not setup and started for PBUL daemons.

The problem was due to the fact that pbinstall was setting up and enabling the service before the binary were installed.

5- When using the option -e with pbinstall, Registry Name services option was always set to yes.

6- pbdbutil --sudo -X was requiring the alias to be specified along with the host. It is now working properly

when only the host is specified.

7- "pbdbutil --sudo -e" (without a file name or wildcard) was failing and not exporting all files as expected.

NEW FEATURES IN RELEASE 9.4.0-18

1. The naming convention for the platforms used in the tar files as well as in the ISO file is now changed to a more meaningful naming:

pbia64_hpuxA-<release-build#> pbul_hpux.ia64_<release-build#>

pbhppa_hpuxD-<release-build#> pbul_hpux.hppa64_<release-build#>

pbs390x_linuxB-<release-build#> pbul_linux.s390x_<release-build#>

pbx86_linuxB-<release-build#> pbul_linux.x86-32_<release-build#>

pbx86_64_linuxA-<release-build#> pbul_linux.x86-64_<release-build#>

pbia64_linuxA-<release-build#> pbul_linux.rhel.ia64_<release-build#>

pbrs6000_aixC-<release-build#> pbul_aix52+_<release-build#>

pbi386_appleA-<release-build#> pbul_macosx_<release-build#>

pbx86_solarisB-<release-build#> pbul_solaris9-10.x86_<release-build#>

pbsparc_solarisC-<release-build#> pbul_solaris9-10.sparc_<release-build#>

pbx86_solarisD-<release-build#> pbul_solaris11+.x86_<release-build#>

pbsparc_solarisD-<release-build#> pbul_solaris11+.sparc_<release-build#>

pbpowerpc64be_linuxA-<release-build#> pbul_ linux.rhel.ppc64be_<release-build#>

pbpowerpc64le_linuxA-<release-build#> pbul_linux.rhel.ppc64le_<release-build#>

2. File Integrity Monitoring (FIM) is a new feature that will enhance PBUL system security and audit. FIM policies can be configured to schedule regular checks of the integrity of Operating Systems, software applications and customer data - verifying file permissions, ownership and even cryptographic checksums and produce details report for security alerts, vulnerability assessments and audit.

FIM policies are configured and maintained in a centralized repository.

FIM clients will be assigned to specific policy, and will automatically retrieve and use these policies to compare the local filesystem against a system baseline.

Any policy violations or inappropriate changes to the filesystem will be detailed in a report which is compiled and sent back to the central repository for future reference, and events generated to alert administrators of the security transgression.

3. Registry Name Service is a service, that when enabled, facilitates the location of other services within the PowerBroker Unix/Linux enterprise,

and provides centralized host based data repository.
The Registry Name Service will provide the product with a method of addressing and locating other parts of the PBUL product. Each type of service, currently including "PBUL Policy Authorization", "Sudo Policy Authorization", "Logging Service", "Log Archiving Service", "File Integrity Monitoring Service" and the "Registry Name Service" itself, will have distinct groups which will comprise of one Primary service host, and zero or more Secondary service hosts. The Primary host will accept all the configurational changes within the Service group and will synchronize these changes out to the Secondary service hosts. Other functions, such as Authorization or data retrieval will be available from any of the Secondary hosts within the Service Group. Each host that makes up the Service Group is defined in the database table, including Primary, Secondary's and Clients. This allows every host within the PBUL enterprise to identify every machine that will make up its Service Group.
This will also allow a more fine-grained control of licenses within the product.
3. Database Synchronization: With the introduction of SQLITE in v9.0 as an embedded relational database for storage of configuration information, there was an increasing requirement for synchronization of databases across servers and services. In this release, we can now log changes and synchronize these changes out to groups of servers defined within the new Registry Name Service. Each database will be configured, as a Service Group, and will receive timely regular updates from the Primary Server within that Service Group. The Registry Name Service will maintain a list of Primary Servers within Service Groups. These Primary Servers will handle all the configurational changes for the group, and will then synchronize these changes out to the rest of the Service Group that require it. From the admins point of view these changes are largely transparent, and administration will be driven by the Registry Name Service.
5. When Registry Name Service is enabled, the license data is now synchronized across all Policy Servers within a Service Group. This allows to more effectively provide licenses that cover failover of each Service Group within the enterprise.
6. With the addition of Registry Name Service and the introduction of a Scheduling Service, you can now automatically retire "old" clients from

the PBUL Policy License data, freeing up licenses for newer clients.
The Scheduler service runs constantly within the REST service, and
reads the License Data on any given PBUL Server and decide which Licenses
require retirement based on the values of the keywords "pblicenseretireinterval"
and "pblicenseretireafter" that dictate how often the licenses are processed,
and how old the entry has to be before it is retired.
Note that with the use of the License data synchronization this process only has
to run on the Primary as changes will be replicated back down to the
Secondary Servers on a regular basis.
7. Ability to produce a human readable report from the Change Management Database
8. The binary pbdbutil is now symbolically linked to pbadmin.
9. When any of the PBUL files (pb.settings, pb.conf, pb.cfg) is stored in
the configuration database, the physical file is now renamed (<file>.<timestamp>)
and a comment is added to the top of the file to indicate that the file
was imported.
10. If the directory specified in 'iolog' variable in the policy, or in 'eventlog'
in the settings does not exit, PBUL now creates the directory at runtime.
11. pbreplay is now able to replay an iolog file, if the file is archived
using PBUL archiving feature.
Note: pbguid still does not yet have this functionality in this release and will be
enhanced in a future release to have the ability to replay an archived iolog.
12. Two new session timeout meachnism is added to the policy language in the form
of procedures: runtimewarn() can be used to warn the user on stderr that the
session has exceeded the time limit, and runtimewarnlog() records to logserver's
syslog that a user's session has exceeded the time limit.
13. pbdbutil now has a new --info --fqdn, which takes a required argument <hostname>.
pbdutil --info --fqdn <hostname>, then prints the fully qualified host name.
14. A new keyword daemonfork is added to pb.settings. The keyword defaults to no
indicating that PBUL daemons will not make a second fork when run in daemon mode.
This means that the daemons will be process group leaders and session
leaders (pid == processgroup == session).
When the daemonfork keyword is set to yes, PBUL daemons (in daemon mode) will
fork after the setsid() call, meaning that they are no longer process group
leaders or session leaders.

15. The new optional keyword pidfilepath, when specified, is the path for PBUL daemon pid files, named <pidfilepath>/<prefix><daemonname><suffix>.pid. When run in daemon mode and not foreground mode, the pbmasterd, pblocald, pblogd, pbsyncd daemons write the pid of the daemon after any forks.

16. The new PBUL Policy procedure iologcloseactionrunhost() is used to specify a /path/filename to be executed on the runhost when the iolog is closed. The specified /path/filename can be a shell script or binary. The user to run the program as, environment, arguments, and working directory are specified in the function call. Stdin, stdout, stderr are redirected to /dev/null. The timeout (specified in seconds) is mandatory. A timeout value of zero indicates no timeout. Note that a timeout value greater than zero will cause the end user's invocation of pbrun to pause while the close action takes place or until the timeout expires. Any runtime errors such as invalid user, cwd, or command are logged via syslog, and to the appropriate PBUL log (e.g. pbrunlog, pblocaldlog) if specified in pb.settings.

17. A new PBUL Policy procedure enablesessionhistory() is now available to set a new internal readonly variable pbulacasessionhistory. This is used for iologged, ACA controlled shell sessions (e.g. bash). The enablesessionhistory() procedure takes a Boolean argument. Values of 1 or true will enable session history. Values of 0 or false will disable session history. When enabled, the ACA preload library will audit additional information for the secured task (presumably a shell), giving pbreplay the ability to interpret the shell "history" (pbreplay --history), within certain limitations.
For this feature to work iolog must be set, and ACA must be enabled with at least one aca() statement.

18. The replay of ACA logs is "clogged up" by duplicate entries (for example read of /etc/group three consecutive times). These consecutive entries, when happening within the same second, will now by default be dropped from the output so that only the first entry is displayed. All entries are logged, and the complete log can be viewed with pbreplay's new --showall (-s) option.

19. The PBUL Policy language "aca()" procedure now takes an optional "tag" argument. This specifies a text string that will be logged any time this ACA rule results in an audit log message.

Note: when a 9.4 policy server detects that the client is pre 9.4,
it will silently ignore the tag (without errors or warnings).
20. PBUL 9.4 log levels now affect the verbosity level of the audit
records (for certain functions), and the log level can be specified for
each permission:
Example: aca(control_type, filespec, 'read|write:log=4|exec:log=2');
21. A new replaytimeformat keyword in pb.settings can be used to permanently
specify a time format. The commandline option overrides the keyword.
If the keyword is not specified, behavior is the same as pre 9.4.
pbinstall creates the replaytimeformat with the default
value: "%a %b %d %Y %r", resulting in date/time displayed in weekday
month day year 12 hour AM/PM format.
22. When eventlogs are forwarded to BeyondInsight from the store & forward file
if a record is "rejected" permanetly by BeyondInsight, the record is now
written to the the <store_and_forward>.rejected file and we will not try
to re-send this record again. The file can be manually processed using
'pbfwdevents' binary.
23. If an error occurs while forwarding the records from the store & forward file
to BeyondInsight, the errors are logged to a separate logfile as specified in
the new settings keyword "pbfwdeventlog".
24. If an error occured when sending an event to BeyondInsight, pblogd no longer
tries to forward the events in the "store & forward" file.
25. When installing on Linux, pbinstall will now configure the PBUL daemons to
be managed by systemd if systemd exists and is functional.

26. If the systemd (or inetd/xinetd if systemd is not present) is installed but
not running, pbinstall will now display a warning message.
27. A new wrapper to pbinstall, called run_pbinstall, is now created to simplify
the installation of all PBUL components:
run_pbinstall -a|b|c
-a Install all components of PowerBroker for Unix & Linux
-b Install server (back-end) components of PowerBroker for Unix & Linux
-c Install client components of PowerBroker for Unix & Linux
-L host [-L host]...

-M host [-M host]...

-p prefix

-s suffix

28. An 'admin' appid and appkey is now created during pbinstall of a Policy Server.
This appid/appkey can be used for sub-sequent client installations using
client registration.

29. The use of "vi/Editor" is now removed in pbinstall. pbinstall now display a menu
prompt during the settings check phase, if submitmasters, acceptmasters,
and logservers need values. The user can enter a space-delimited list of
hosts/connections which will be written for that setting.

30. All keywords are now added to pb.settings even when the setting is not enabled,
in which case the keyword will be commented out.

31. pbinstall menu items were reorganized to display the installation of components,
PBSUDO, BeyondInsight, PBIS and REST API, to the first page of the menu options.

32. The Sudo database on the Sudo Policy Server now includes information regarding
on which host, when and last time sudoers was changed. This information is
displayed when 'pbdbutil --sudo -L' is invoked.

33. Two PBSUDO APPIDs is now created during pbinstall of a Policy Server.
One APPID "PBSUDOADMIN" will have full admin rights, and one "PBSUDOREAD" will
have read only rights. The APPIDs and associated keys will be displayed at
the end of installation, so that the administrator can make note of them.

34. A new keyword pbsudorefresh can be used to change the refresh interval.
Values less than 30 seconds are silently changed to 30 seconds.
Values greater than 86400 seconds (1 day) are silently changed to 86400
seconds. The keyword and default value of 30 seconds are written to
a new policy server pbsudo.settings.default file upon a new installation.

35. A new Bourne shell script "pbsudopreinstall.sh" is now available to run
pre-install checks. When run with the -f option, this will output TOML
formatted name value pair data. When run without the -f option, this
will output user friendly text. This utility will check that the host is
supported by pbsudo, determine if an incompatible version of PBUL is
installed verify that sudo is installed and determine if the version of
sudo installed is 1.8 or higher, and attempt to verify that the sudo supports
shared libraries.

36. Solr installation has now several improvements:
- The addition of pbsolr.cfg now allows pbsolrinstall to remember previous
menu selections, preventing users from answering the same menu questions
multiple times with the same answers.
- The installation now checks if the certificates already exist and this
Solr host is already registered in BeyondInsight, and if so the registration
is skipped and the following message will be displayed:
Solr certificates exist. Skipping registration with BeyondInsight CA.
- The solr installation now asks if the 'solr' configuration option should be
added to the local /etc/pb.settings. The solr certificats are copied to /etc
and 'solrhost', 'solrport', 'solrcafile', 'solrclientkeyfile' and
'solrclientcertfile' are added to the local /etc/pb.settings if it exists.
and the following keywords are added to the /etc/pb.settings file:
Note that only the local file /etc/pb.settings is updated. If pb.settings is
stored in the Configuration database, the user need to export the file prior
to running solrinstall and import it back after.
- Added the ability to create tarball with the solr keywords and certificates.
The tarball will be named solr.<shorthostname>.pbsettings.tar and placed in
the PowerBroker Solr installation directory.
- The error returned by BeyondInsight is now parsed and reported. The full
BI response will be logged.
- Addition of command line arguments for each menu option allowing
non-interactive install
37. Support for failover ability on PBSUDO client for submitmaster and logserver
if Registry Name Service is enabled (or if pbsudo.db is manually copied to
all Sudo Policy Servers).
38. Ability to view or manage sudoers files from the PBSUDO client:
a new option '--client' is now added to 'pbdbutil' that allows
the sudoers to be managed also on the PBSUDO client.
To authenticate remote management, the user is required to provide
REST appid/appkey credentials.
39. Ability to cache REST appid/appkey credentials in a secure manner
using 'pbdbutil --auth' option.
40. PBSUDO installation has now several improvements:

- All pbsudo installation menu items now have command line arguments
- pbsudoinstall can now be invoked in non-interactive mode
- The questions to create/join a host alias are now reworked for
an easier understanding
- pbsudoinstall now checks if the host already exist in the Sudo
database on the Sudo Policy Server, either as part of an alias or
individually and takes the appropriate action accordingly
- pbsudoinstall now displays the list of existing Alias groups when
prompted for the Alias group name.

41. New options -J and -C was added to pbdbutil --sudo:
-J <host_alias>: configures PBUL to join a host alias for this sudo client
-C <host_alias>: configures PBUL to create the specified alias for this sudo client
42. pbsudouninstall, when invoked with an admin APPID and APPKEY, will now extract
the sudoers and include files from the cache and be written to disk.
A new pbsudouninstall -P option can be used to skip this step, thus preserving
any local files (or lack thereof). If -P is used, and the sudoers file does not
exist locally (perhaps due to the rename during install feature) a warning will
be issued indicating that sudo will not function properly without a sudoers file.
43. pbsudouninstall will now remove the sudoers file and the sudo client host
from the Sudo database if the host is not part of an alias.
44. New supported platforms:
Ubuntu 16.4 (x86 64-bit)
45. De-supported platforms:
HP-UX 11i (PA-RISC)
SUSE Linux Ent Server 10 (Power5 64-bit)

KNOWN ISSUES IN 9.4.0-18

1- When running pbsudoinstall, the following question is asked:
Would you like to create a new alias (c), or skip creating an alias (s) [s]:
If you just type return (to accept the default), the sudoers is not uploaded. You have to type 's' to actually do the action:
Would you like to create a new alias (c), or skip creating an alias (s) [s]: s
Uploading sudoers file /etc/sudoers
{"sudo":[{"fname":"<host>@/etc/sudoers","version":1}]}
Removing plugin definitions (if any) from /etc/sudo.conf

Adding PBUL plugin definitions to /etc/sudo.conf.

2- pbsudouninstall does not restore the sudoers file when the primary sudo policy server is RNS enabled.

SIGNIFICANT BUG FIXES IN RELEASE 9.4.0-18

- On the non-linux platforms where all the pb logs get created under /var/adm/, pbrest.log goes under /var/log/
- When reinstalling using pbinstall -b, autofwdtime and solrhost keywords were not preserved in "/etc/pb.settings".
- pbinstall was ignoring the answer to the question "Install PowerBroker for Unix & Linux now?" when set to 'no' and continued with the installation.
- pblogd and pbfwdevents did not release the lock on pb.rcs_eventstore file. Because of the lock, many pblogds queued up trying to acquire the lock on the pb.rcs_evenstore file.
- A segmentation fault was produced by pbrun, when the command was longer than 8k. This was due to a buffer overrun issue.
- PBUL daemons did not dissociate from the tty, when started in standalonedaemon mode. This was due to the fact that the pgrp_id and session_id of these processes were not set to the same PID.
- If eventlogencryption was not set in pb.settings, pblogarchive failed with the following error:
8150.3 Failed to archive logfile due to error: 8112.1 Failed to read file /tmp/.pbrest_XwIWvS, No such file or directory
- When aca is enabled, the error 'permission denied' was displayed when changing directories in a 'pbrun ksh93' session.
- On s390 platform, when aca is enabled, the error
<command>: symbol lookup error: /path/to/libaca: undefined symbol: dlsym
was displayed when invoking 'pbrun <command>'
- When the policy set 'runenablerlimits = true', set 'runrlimit_nofile = <value>' and aca('file','default','all') invoking "pbrun bash -c 'ulimit -S -n; ulimit -H -n; exit;'" failed with "Failed to read ACA policy: lock failed ..."
- If a file was blocked by aca in the policy, symbolic links to the file were not blocked.
- When aca is enabled, "lsblk" did not return any output.
- When aca is enabled and ksh was used, piped commands failed with "cannot create pipe [Permission denied]"

NEW FEATURES IN RELEASE 9.3.0-07

1. A new keyword (randomizelogservers) was added that, when set, will randomize the log server used from the list of logserverss. Previously, always the first logserver on the list was used, unless the server was down. When this keyword is set to 'yes', a log server will randomly be picked from the list. The default value for this keyword is 'no'.
Please note that setting this keyword to 'yes' might result in an 'accept' event to be logged to one eventlog, and the 'finish' event to another.

2. For added security, when issuing "pbdbutil --sudo -U --force", the options "-a <appid> -k <appkey>" are now required.

SIGNIFICANT BUG FIXES IN RELEASE 9.3.0-07

- When submitconfirmuser() was used in the policy, and a wrong password was provided, pbrun as well as pbksh and pbssh terminated with a signal 11. This is now fixed.
- The command 'pbdbutil --sudo -l <file>' did not work when the full path and filename was specified. This is now fixed.
- An issue was introduced in v9.0, where the 'sharedldapdependencies' was not set properly on AIX platforms. This has been corrected.
- A dependency to the REST package was incorrectly required, when only run/submit Host packages were installed, creating the user pblight and the directory /usr/lib/beyondtrust/pb/rest, which were not required on a runhost or submithost. This dependency has been removed.
- When installing rpm packages on an x86 64 bit only host, the installation failed on a glibc.i686 dependency. This is now fixed.
- An issue was introduced in v9.2.0, where the pblighttpd service (and pbconfigd) were not stopped after the packages were uninstalled. This is now fixed.
- On hosts with chkconfig, pblighttpd service did not start automatically at system boot. The service is now correctly added to /etc/rc.d and starts at system boot.
- pblogarchive failed if the first record in the eventlog was a Finish event or the eventlog contained only one accept event. These issues are now fixed.
- If pblogarchive fails to archive the eventlog, but the eventlog was rotated, it now displays a message stating that the eventlog was rotated.
- The location of log archiving database (logarchivedb) is now consistent with other database location (Config database, sudo database), and inconsistent checks on its location has been removed.
- pbreplay -O did not display the whitespace recorded in PowerBroker for Sudo iolog files as whitespace but as tabulations. This is now fixed.
- pbreplay -O did not process xterm DCS control commands issued by vi. The Esc P+q<hex>Esc\ command is issued by vi, and not trapped with pbreplay -O. This caused the xterm control command to be passed to the tty, which results in odd terminal behavior. This is now fixed.
- Indexing iolog files with Solr, when iologs contained 0x03, 0x16 and extra NULLs, resulted in a failure to index the files. These charcaters are not supported by Solr and are now being filtered.

- A memory leak was detected in pbreplay and is now fixed.
- Due to a mishandling of socket options, PowerBroker for Unix & Linux daemons failed to reuse the port because it was in "time_wait" state, and the restart failed with: "5454 Could not bind server socket for pbmasterd port <port> family IPV4 Address already in use" The socket option is now correctly set, allowing ports to be reused immediately.
- When aca("file", "default", "all") was used in the policy, certain commands such as 'man <command>' or pipes (echo a | cat) failed with "Failed to read ACA policy: length 4 failed 0 - 0. Exiting...". This is now fixed.
- When ACA was used in the policy to intercept files under a path, for example:

aca("file", "default", "all");
aca("file", "/bin/*", "!all");
aca("file", "*/bin/*", "!all");
aca("file", "/bin/*", "!all");

it failed to intercept some relative paths such as "../. /../bin/hostname" or "../../../../../../bin/hostname".

SIGNIFICANT BUG FIXES IN RELEASE 9.2.2-01

- Issue introduced in 9.2.1-01: Intermittent segmentation fault when iolog was set in the policy

---

SIGNIFICANT BUG FIXES IN RELEASE 9.2.1-01

1. A memory leak in the iologging mechanism was introduced in v8.0 and above, affecting the binaries pbmasterd, pblocald, pbrun, pbksh, pbsh, pbssh and pbsudoers.so.

NEW FEATURES IN RELEASE 9.2.0-08

1. PowerBroker for Unix & Linux now supports DNS names longer than 63 characters.
2. pblicense -r can now retire a client using its UUID. You can now provide either an IP address or UUID when retiring a client.
3. pblicense -r now has a --batch option that can be used to retire clients non-interactively.

SIGNIFICANT BUG FIXES IN RELEASE 9.2.0-08

1. When upgrading from an installation where pb.settings (or pb.cfg) was stored in the registration database, pbinstall was not reading the files from the database and therefore was not using the

existing settings. pbinstall now checks if pb.settings and pb.cfg are in the configuration database, and if so, reads the values from the database instead of the physical files on the host.

2. When installing a client on AIX platforms, using the client registration, pbregister failed to load the shared libraries and the client registration was therefore failing. pbregister now loads the shared libraries properly during the install on AIX.

3. When pb.settings was stored in the configuration database, and later deleted from the database, "pbconfigd --cfg -l" was failing with an error:
3430 Insecure operation - please consult your administrator
This was due to pbconfigd, when reading the settings file, was finding the one in the database, which was marked as deleted, and was incorrectly retreiving it (as an empty file), instead of backing off to use the filesystem copy. This is now fixed.

4. If the keystore file (rest.keystore) was removed, pbconfigd was producing a segmentation violation after displaying an error. This is now fixed.

5. Occasionally, specifically on Red Hat 7 and CentOS 7, pblighttpd and pbconfigd services where not stopped after an uninstall. This is now fixed.

6. If the locale "C" file was not found on the host, pbconfigd failed to start up and displayed the following error:
"Unable to find library '/usr/lib/nls/loc/hpux32/locales.3/C'.". This is now fixed.

NEW FEATURES IN RELEASE 9.1.0-08

1. PowerBroker for Unix & Linux Sudo Integration:

PowerBroker for Unix & Linux can now be integrated with sudo. This integration requires the PowerBroker for Unix & Linux Sudo Client to be installed on hosts where sudo is installed.

Integrating sudo with PowerBroker for Unix & Linux has the following benefits:

- Centralization of sudoers policies, stored in a secure database on PowerBroker for Unix & Linux Policy Server host
- Change management for sudoers policies: Once sudo policies are stored on PowerBroker for Unix & Linux policy server, they can be checked out, modified and checked back in centrally, without the need to go to each sudo host.
- Integration with PowerBroker for Unix & Linux eventlogs: After sudoers policy processing, an accept or reject event is logged in the PowerBroker for Unix & Linux event log.
- Integration with PowerBroker for Unix & Linux iolog: Sudo commands can be iologged in the PowerBroker for Unix & Linux iologs, and read with pbreplay.

Important Note:

PowerBroker for Unix & Linux Sudo plugins are based on Sudo v1.8.11p2.

This limits the support of Sudo Client to Sudo v1.8 and higher. And whilst we've made every effort to minimize any differences in the end use of the sudo product, it is inevitable that newer versions of the product may differ slightly, and features in new versions of Sudo may not be supported.

SIGNIFICANT BUG FIXES IN RELEASE 9.1.0-08

1. An issue was introduced in v9.0 in pbguid when pam was enabled that was breaking the authentication preventing the PBGUI to work. This is now fixed.
2. An issue was introduced in v9.0 in pbguid, when clicking on either "View eventlog" or "View iolog", PBGUI was producing a segmantation fault. This is now fixed.
3. Several issues in ACA functionality has been corrected, specifically on Solaris and HPUX platforms.

NEW FEATURES IN RELEASE 9.0.0-18

1. Role Based Policy

Role Based Policy has been implemented to simplify the definition of policy for administrators. Policies are kept within structured records in a database, simplifying maintenance, decreasing system load, increasing throughput, and providing a comprehensive REST API to integrate policy management with existing customer systems and procedures, including simplified bulk import/export of data. Once the data is held within the Role Based Policy database it is much easier to provide management information, such as user entitlement reports. The policy data is grouped into users, hosts, commands, time/dates and roles detailed in the Admin and Language Guides.

2. Change Management Events:

The new "Change Management Events" are configured on the client by enabling the "changemanagementevents" in the pb.settings, and on the Primary logserver by specifying the "eventdb" setting, and will log all changes made to the Configuration and Settings, and the Role Based Policy databases. When the setting is enabled all changes will require a message, which is logged alongside the username, date/time and the details of the actual change. The events are sent to the logserver defined in the pb.settings and can be retrieved via REST or locally on the logserver with the "pbdbutil --evt" option.

3. Configuration and Settings database:

New facilities in the area of configuration and settings change management have been added. To provide these facilities the existing PowerBroker for Unix & Linux configuration files, including the pb.settings, pb.conf and encryption keys can now be stored within a database. The database will allow the storage of versioning information, and will allow the rollback of individual configuration files, or indeed complete sets of files from the command line.

To use the new change management facilities, simply import files into the database by using the new 'pbdbutil' binary, for example:

pbdbutil --cfg -I /etc/pb.settings /etc/pb.conf /etc/pb.key {"fname":"/etc/pb.settings","version":1}

As soon as the files are imported they are versioned and every PowerBroker for Unix & Linux binary will use the current database copy in preference to the existing files.

4. Advanced Control & Audit:

The new ACA or Advanced Control and Audit, will trap file system related library calls and allow, disallow, and audit the calls.

The new ACA language will specify actions (e.g. open/read/write/exec) that can, or cannot be performed on a file (using shell style file patterns to match files), and will also specify an auditing level. Each specified library function call will be intercepted by a PowerBroker for Unix & Linux library. Once intercepted, the ACA statements will be processed to determine if the action is allowed, or if auditing is required. If auditing is specified, the relevant data will be sent back to the originating client to be written to an IOlog or an ACA log.

When ACA is enabled, the iolog will contain both iologging and auditing information. The new pbreplay -A (--audit) command line option is used to display the audit records from an IOlog.

5. Client Registration

The Client Registration feature has been added to PowerBroker for Unix & Linux to facilitate the installation and configuration of new PowerBroker for Unix & Linux clients into the enterprise.

It consists of a centralized Registration Profile service, normally found on the Primary Policy Server. This service is configured with customized profiles that match the settings required for the installation of hosts that provide differing roles in the organization.

When new PowerBroker for Unix & Linux clients are installed these profiles are retrieved, providing the configuration required to complete the installation.

6. Enhanced Encryption

To enable compliance with US government regulations, and specifically FIPS 140-2, the encryption within PowerBroker for Unix & Linux has been updated. Many of the older less secure encryption algorithms have been deprecated, and when high security is enforced, they are disabled completely.

When new PowerBroker for Unix & Linux servers and clients are installed, the pb.setting "enforcehighsecurity" and "ssl" are both enabled. This switches PowerBroker for Unix & Linux into FIPS 140-2 mode.

All encryption algorithms are FIPS 140-2 compliant, and it will not communicate, encrypt or decrypt any data that isn't encrypted in AES-128, AES-192, AES-256 or TripleDes.

For existing customers who are upgrading their enterprise to version 9, the upgrade script will automatically add the AES-256 encryption algorithm onto the iolog and event log encryption configutation, leaving the existing encryption algorithms at the end of the configuration. This will ensure that new iologs and event logs are encrypted using modern secure algorithms, but allowing existing iologs and event logs that are encrypted in less secure algorithms to be decrypted and retrieved.

Although existing network encryption can continue to use deprecated encryption algorithms, because the data is transient, more permanent data such as iologs and event logs can only be encrypted in FIPS 140-2 compatible algorithms.

Customers who have an existing infrastructure, and would like to be FIPS 140-2 compliant will have to upgrade all PowerBroker for Unix & Linux Servers and Clients to the latest version.

If there are existing iologs and event logs that are encrypted using less secure algorithms you will require a specially configured host that will be dedicated to reading these older logs.

7. Event and IO log archiving

PowerBroker for Unix & Linux now provides a logfile tracking and archiving mechanism for I/O logs and eventlogs. Each logfile created can have its location recorded in a centralized database for future searches. PowerBroker Servers log files can be archived off from the original Logserver hosts, for the purpose of freeing up space on the Logservers or for consolidating logs on designated archive hosts.

The log archiving process is performed by hosts that have been installed and configured with the server components of PowerBroker. Those components mandatorily install the PowerBroker REST service which is essential in logfile movement and tracking.

8. Change "Master" to "Policy Server"

The term "Master" is now changed to "Policy Server" in all the messages in the source code, the installer, the documentation, the man pages, as well as the GUI.

9. The new ISO file

The iso file now contains 3 directories: PBUL, PBIS and SOLR.

Under PBUL directory, you will find all the PowerBroker for Unix & Linux tar files untar'ed as well as the Manuals.

Under PBIS directory, you will find the content of the latest PowerBroker Identity Services iso file.

Under SOLR, you will find the content of Solr tar file untar'ed.

10. PBIS installation

When running pbinstall, when you say "yes" to "PowerBroker Identity Services Integration?", a new menu item, "Install PowerBroker Identity services?", will allow you to install PowerBroker Identity

Services by providing the directory where the install files are located.

When installing from PowerBroker for Unix & Linux iso file, the install directory will be set by default to the directory in the iso file.

11. Support Snapshot

A new shell script, pbsnapshot.sh, is now installed and allow you to create a tar file containing information that could be useful for the support team to reproduce an issue.

12. Allow space in the value of rcsworkgroup

It is now allowed to have space in the value provided for 'rcsworkgroup' passed to BeyondInsight.

13. New SSL, LDAP, Kerberos and Curl shared libraries:

PowerBroker for Unix & Linux is now packaged with the following version of these libraries:

- OpenSSL v1.0.2a
- Kerberos v1.13
- OpenLDAP v2.4.40
- CURL v7.40.0

14. Kerberos keyword 'keytabencryption' introduced in 8.0.1 is no longer required.

PowerBroker for Unix & Linux Kerberos interface should derive the proper encryption from /etc/krb5.conf.

15. New supported platforms:

Oracle Solaris 11.2 (Sparc and x86)

SUSE Linux Ent Server 12 (x86 64-bit)

TeraData Express 13 (SLES 10)

TeraData Express 14 (SLES 11)

Red Hat 6.x, 7.x 64-bit on PowerPC Big Endian

Red Hat 7.x 64-bit on PowerPC Little Endian

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 9.0.0-18

1. Problems with group names starting with a number:

When the secondary group of a user started with a number, 'pbrun id' displayed incorrect group information in the output of 'id'. This was due to the product considering the group name as a group number, and failing the lookup of the group. This is now fixed.

2. Hanging pblogd due to lost communication between pbrun/pblocald and pblogd:

Intermittently pblogd was hanging due to pblogd not exiting and therefore holding a lock on the eventlog which prevented other pblogd to obtain a log, and subsequentally hanging as well.

The issue happens when pblogd is done with logAccept/logReject but waiting for a message to terminate. The error "5101.02 Communication error" was received, however pblogd ignored the return value indicating the error and continued to wait. This is now fixed.

3. When "passwordlogging" was not present in pb.settings (or commented out), the default value was "allow". It is now correctly set to "never".

4. pbbench now recongizes the shell wrappers around pbguid/pbsguid and pbsyncd used on some platforms

5. When using pbsync to merge encrypted iologs, pbsync was failing with invalid checksum and missing header section. This is now fixed.

6. When pbsync was exiting due to an error, the exit status was 0. It is now a non-zero value.

7. When submitconfirmuser was used with a long prompt, the message displayed in the 'reject' had extra characters. This is now fixed.

8. The procedure 'remotesystem' always used /tmp as the cwd and ignored the value in the 5th argument 'cwd'. It is now correctly using the value specified in 'cwd'.

9. When a host with the same UUID used in the new license file (since 8.5.0) had a different ip address, the old ip address was not updated. The Policy Server now updates the ip address of the host when the same UUID is used.

10. When installing package installers on Solaris, any symlink on the directories /usr, /usr/local, /usr/local/bin, /usr/local/man, /usr/lib/secure, /usr/lib/secure/64, /usr/sbin etc.. was broken.
This is now fixed.

11. When 'pbadminpath' was not in pb.settings, events and iologs were not forwarded to BeyondInsight and Solr and there was no error in any logfile. An error is now displayed indicating the missing 'pbadminpath' and the records are stored in the 'store and forward' file until they can be forwarded at a later time.

12. Occasionally, with some iologs 'pbreplay -o -am' produced a bus error on HPUX.
This is now fixed.

13. After the retiring period of a host was elapsed, when running pbrun from the retired host, the first pbrun failed with an error indicating the host is retired, instead of re-activating the host. The subsequent pbrun worked. This is now fixed and no error is displayed the first time.

14. On Linux Itanium only and with v8.5.1, pbbench -V was exiting with 'signal 11'.
This is now fixed.

NEW FEATURES IN RELEASE 8.5.1-01

1. X11 iolog capture and replay: The new X11 capture feature provides two areas of

functionality. It firstly encrypts X windows communications to enhance security, and will provide a full session capture of every graphical session so that the session can be logged and audited.

pbrun has a new command line option -X (--x11forwarding) that will request X11 forwarding. X11 forwarding is allowed by default when pbrun -X is used. The policy variable 'xwinforward' can be used to override this.
When running pbrun with the "-X" option, the DISPLAY environment variables needs to be set, and a valid XAuthority token needs to exist in the user's Xauthority file specified by the XAUTHORITY environment variable or ~/.Xauthority by default.

pbreplay has a new "X" option, using in conjunction with the "-a" option, for example:
pbreplay -o -aX <path/to/iolog>
Will dump relevant X11 captured events from the iolog. Major events such as the creation and destroying of windows, textual window updates, text input and mouse clicks will be displayed as a summary alongside any output from the parent process.
2. A new "noexec" policy variable was added that will enable/disable the capability to prevent secured tasks from using exec() to create subtasks (e.g. prevent a user from obtaining a root shell from an elevated 'vi' process).
The new read/write "noexec" policy variable will default to 0 thus disabling the feature by default. Within the policy, when policy administrators want to disable a secured task's ability to exec a program, they can set the "noexec" variable to 1.
3. Both pbmasterd and pblogd have now the ability to rotate the event log.
The new 'eventlogrotate' keyword specifies a rotate size and an optional path for the resulting rotated file.
Additionally, the new --rotate option (-R) for both pbmasterd and pblogd, allows manual rotation, or rotation via cron, for the event log /path/filename specified in pb.settings.
4. Licensing Improvements: PBUL now uses UUIDs (universally unique identifier) instead of IP addresses to identify and track connected clients.
The option -u of pblicense allows a user to list the UUID of the licensed clients

and the new binary pbclienthost_uuid will display the UUID of the client on the client host.

5. A new -F option has been added to pbkey binary that will creates pb.key with the addition of obfuscation of the key using accredited encryption techniques.

6. Four new encryption standards have been added, namely "ssl3des", "sslaes-128", "sslaes-192" and "sslaes-256", which can be used in all encryption settings. These are implemented using openssl function calls and adhere to FIPS 140-2 encryption standards. They require sharedlibsssldependencies to be set.

7. A new setting, enforcehighsecurity, has been introduced that when set to yes will turn higher security options and will:

- Require enabling of the "ssl" keyword.
- Require the setting of the sslservercertfile and sslserverkeyfile so that ssl communications can be enabled.
- Deprecate the use of all but the FIPS 140-2 accredited encryption algorithms (i.e. AES-128, AES-192, AES-256, ssl3des, sslaes-128, sslaes-192 and sslaes-256).
- Enforce enabling of FIPS in the OpenSSL libraries if available.
- Will enforce the use of the new version of pb.key format (pb.key generated with the new -F option of pbkey binary)

8. REST API: REST API for PowerBroker for Unix & Linux is a new add-on API previously bundled separately. This is now part of the standard tar files and Package installers.

This web-based API allows other software to configure, customize and retrieve data from PBUL. When installed on the PBUL Master, Logserver or run/submit hosts, alongside a suitable HTTP service (one which supports FastCGI), will provide the communications between the client and the REST services. The REST API provide a RESTful interface for product settings, policy configuration and IO log retrieval and replay.

9. A PAM module (pam_radius_auth) is now included to support authentication against a configured RADIUS server. The module allows PBUL to act as a RADIUS client for authentication and accounting requests. A RADIUS server is required before using this module. The RADIUS server must also have the PBUL host requesting authentication already defined as a RADIUS client.

10. In order to allow the user to selectively use PAM authentication in the policy,

two new policy functions and 3 new policy variable have been added to 8.5.0:
- The new getuserpasswdpam() function is similar to the existing getuserpasswd()
but requires a new "pampasswordservice" argument.
- The new submitconfirmuserpam() function is similar to the existing
submitconfirmuser() but requires a new "pampasswordservice" argument.
- The new runconfirmpasswdservice variable works in concert with runconfirmuser
variable. It indicates which PAM password service on the runhost will be used
to perform password authentication and account management.
- The new runpamsessionservice variable indicates which PAM session service will
be used to perform account management and session start and end services to manage
task requests on a run host.
- The new runpamsetcred variable works similarly to the server settings keyword
pamsetcred. The runpamsetcred variable enables the pam_setcred() function,
which is used to establish possible additional credentials of a user.
11. A new 'taskpid' variable has been added which contains the pid of the secured task
launched by pbrun, or the Session associated with pbksh/pbsh if iologging is on.
This variable is populated when the secured task is executed, and has no value
until a session starts and therefore cannot be used in the policy. This variable
is shown in the Finish event of the eventlog only when a logserver is used. It
can also be used in the new 7.0 syslog formatting settings,
syslogsession_start_format and syslogsession_finish_format.
12. De-supported platforms:
The following are no longer supported:
HP-UX 11i v1 (B.11.0) (PA-RISC 32-bit)
IBM AIX 5L v5.1 (POWER 32-bit)
IBM AIX 5L v5.2 (POWER 32-bit)
Red Hat Ent Linux v3 (x86 32-bit and 64-bit)
SUSE Linux Ent Server 9 (x86 32-bit and 64-bit)
IBM zSeries Red Hat Ent Linux v4 (s390 31-bit)
IBM zSeries Red Hat Ent Linux v4 (s390x 64-bit)
IBM zSeries SuSE Linux Ent Serv 9 (s390 31-bit)

13. New supported platforms:
Red Hat Ent Linux v7.1 (x86 32-bit & 64-bit)

Oracle Enterprise Linux 7.1 (x86 32-bit & 64-bit)

Mac OSX 10.9 (i386)

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 8.5.1-01

1. pbrun and pblocald hung intermittently when processing a large file, when no logserver was used and when submittimeout was set.
This is now fixed.

2. The default syslog formatting for Finish event was changed to use exit date and time instead of date/hour/minute. Also all %hour%:%minute% in other syslog formatting were changed to use %time%

3. When installing Package Installers on AIX, the ownership of /usr/sbin, /usr/lib, /usr/share and /usr/local was changed to 600:400. This is now changed to set the ownership to bin:bin.

4. After installing the default policies when using Packages, the default /etc/pb/pbul_policy.conf was missing the "include '/etc/pb/pbul_functions.conf';".
This is now fixed in 8.5.0.

5. When "pbreplay -o -am" was executed on AIX5.3, Solaris10 and HP-UX11.11, it occasionally hung. This was due to an unintialized buffer and is now fixed.

6. When uninstalling Packages on AIX, if /usr/local, /usr/sbin or /usr/share/man were symlinks, the symlinks were removed.

---

o New Feature in 8.0.2-04:

- A new policy procedure, policytimeout(timeout_value), has been added:
This procedure adds an overall policy timeout mechanism so that pbmasterd can abort the request when the policy processing takes an inordinate amount of time.
For example, when submitconfirmuser() is used, but the submitting user (or process) does not enter a password.
This will prevent pbmasterd processes that appear to be hung when the policy is waiting for user input which may never arrive.
pbmasterd informs PBUL 8.0.2 clients (pbrun, pbksh, pbsh, pbssh) of the timeout, and those clients will also timeout.

---

o ISSUES FIXED in 8.0.2-04:

- An issue was introduce in 7.0 and above, with the introduction of "passwordloggingprompts", where when logomit('*') was called in the policy, the variable "passwordloggingprompts" was omitted, unsetting the password prompts and causing passwords entered during secured task execution to be logged in the iolog file. "passwordloggingprompts" is now added to the system variables and will not be omitted by logomit.
- Occasionally, when iologging was on, and a password prompt was encountered, an extra message "5136.02 writeIOLog prior stdin is still pending." was logged. This message was harmless and is now removed.
- Issue in 8.0.1 patch only: In certain circumstances the password is logged in the iolog file. This can occur if password prompt comes in across two reads of standard output data and the byte AFTER the buffer is either 0x0A or 0x0D. This is now fixed.

- Intermittently, when no logserver was used and pbrun invoked a secured task on a remote host (pbrun -h) involving large data transfer between pbrun and pblocald, the data was truncated. This is now fixed.
- Intermittently, when noreconnect was set to true, no logserver was used and pbrun invoked a secured task on a remote host (pbrun -h) involving large data transfer between pbrun and pblocald, pblocald hung. This is now fixed.
- Intermittently, when noreconnect was set to false, no logserver was used and pbrun invoked a secured task on a remote host (pbrun -h) involving large data transfer between pbrun and pblocald, pblocald failed with an error: "Unidentified timeout reached". This is now fixed.
- Intermittently, pbrun failed with the following errors:
"5104.02 Expected CMD_CHARS got CMD_STDIN_CLOSE"
or
"Expected CMD_WINCH got CMD_STDIN_CLOSE"
This is now fixed.
- pbksh and pbsh did not fall back to native root mode when logservers were not reachable. Now, if logged in as root, and there is no logserver available, pbksh and pbsh will switch to native root mode even if a master is available.
- When in native root mode, pbksh and pbsh erroneously set submithostip to "local shell builtin" or "local shell command" in the local eventlog. This is now fixed and submithostip is set to the ip of the submit host.

- An issue was introduced in v7.5.1 only, where pbrun seg faulted when iologging was on, and passwordloggingprompts was set to {":"}, and the output of the secured command contained ":". This is now fixed.
- Due to hard coded encryption type 'des' in the Kerberos support of PBUL, when enabling Kerberos in pb.settings, the Kerberos file kdc.conf had to contain the standard version of des in the variable supported_enctypes: supported_enctypes = des3-hmac-sha1:normal des-cbc-crc:normal des-cbc-crc:v4 for PBUL to function properly. This is now fixed. A new keyword 'keytabencryption' is added to pb.settings and needs to be set to the encryption type used by Kerberos.
- pbpatchinstall failed with no space left on device on Solaris VM When a VMWare guest OS is installed, and the optional configuration called 'hgfs' is present. This is now fixed.

- When running pbcheck -e on the default policy delivered with 8.0.0, it failed with error "2431 Terminating to protect system resources". This was due to the use of input function in a loop, and the fact that during entitlement reporting there was no input to process the loop with. This is now fixed and the loop is only processed once.

- pbcheck -e seg faulted with policy using split function with runhost as the argument. This was due to manipulation of a null pointer and is now fixed.
- An issue was introduced in v8.0.0 where pbbench -V, -l and -m occasionally seg faulted on Linux Itanium and Linux 64 bit when submitmasters/acceptmasters/logservers were using an external program to defined the hosts.

NEW FEATURES IN RELEASE 8.0.0-10

1. The behavior of the existing pb.settings keywords submitmasters, altsubmitmasters, acceptmasters, logservers, masterport, and logport; and pblocald's --accept_masters commandline argument was modified to allow the lookup of such values via DNS SRV records. DNS SRV records specify a service name with one or more host entries that include hostname, port, priority, and weight. This PBUL implementation supports the hostname, port and priority values, and ignores the weight value.
2. The submitmasters, altsubmitmasters, acceptmasters, and logservers keywords now

supports a mechanism to execute an external program to return a single value.
The external program path and filename should be contained within backticks
without whitespace. Command line arguments to the external program are not supported.
Redirection and backgrounding the external program are not supported.
3. Linux, AIX and Mac OSX only: The pbmasterd, pblocald, and pblogd daemons are
modified to optionally update their command line arguments (viewable via ps) to
include information about the originating pbrun request. The customers will then
be able to use the 'ps' command to view pbmasterd, pblocald, and pblogd processes
and determine the associated submituser, submithost, runcommand, and the pbrun pid.
This feature will work only on operating systems that allow a process to overwrite
its argv data (Linux, AIX, Mac OS X). This is known to not work on Solaris and HP-UX.
4. PBUL now provides a new setting, "addressfamily", to actively prevent AAAA DNS
records requests when IPv6 networking is disabled. This is a workaround for an
unacknowledged OS bug in the implementation of getaddrinfo() on
Red Hat (and possibly other platforms). The addressfamily setting specifies which
address family PBUL will use when making remote connections (ipv4, ipv6 or any).
5. A new option, "--testmaster [hostname|IP_address]", was added to pbrun that will
test master processing for a particular master host, but prevents the master from
connecting to the run host and also prevents execution of the command. This option is
only allowed when the submit user is root.
6. A new option was added to pbrun, pblocald, pbmasterd, pblogd to turn on debugging.
Debugging can be on-demand from pbrun when pbrun is called with "--debug=<level>" option.
All PBUL daemons that process the pbrun command will turn on debugging for the duration of that session.
Debugging can be persistent for the PBUL daemons if the superdaemon invokes the PBUL
daemon program with the "--debug=<level>" option. This can be done if the daemon configuration
file is modified and the "--debug" option is inserted. It can also be done for stand-alone
daemons if you manually invoke with "--debug".
7. A default role-based policy will now be installed by default if an existing policy
does not exist. This default role-based policy contains several roles
(Help desk, PBTest, Controlled Shells, Admin and Demo roles) that can be enabled
or disabled in the policy.
8. Installation of Solr for PBUL iolog indexing has been greatly simplified by eliminating
most of the previous steps to generate, and copy BeyondInsight (formerly Retina CS)
certificates.

9. For improved categorization of events in the BeyondInsight (formerly Retina CS) display, a new policy variable, "pbrisklevel" was added to provide a way to give risk rating to accept and reject events. Valid values are whole integers ranging from 0 (no risk) to 9 (highest risk). If the variable is not specified in the policy, the risk level will be defaulted to 0.
10. A new keyword, "rcsworkgroup", was added to pb.settings. The workgroup name is a label which helps BeyondInsight (formerly Retina CS) to identify and group related events sent from PBUL. You can then sort PBUL events based on the workgroup label.
11. A new policy variable, "logcksum", was added and when present in the policy, will log the checksum that was generated for a command/executable/binary in the event log regardless if the policy variable runcksum/runcksumlist/runmd5/ runmd5list is set. If logcksum variable does not appear in the polify file, the checksum value will not be logged.
Valid values for "logcksum" are: "cksum", "md5sum" or "all"
12. Added the eventlog variable "chksum" (for "Finish" events only) to store the checksum value generated for the command/executable/binary. This variable will always be automatically populated. However, it will only be added to the eventlog only if the variable logcksum is set to "cksum" or "all"
13. Added the eventlog variable "md5sum" (for "Finish" events only) to store the md5 checksum value generated for the command/executable/binary. This variable will always be automatically populated. However, it will only be added to the "Finish" events in eventlog only if the variable logcksum is set to "md5" or "all"

14. A new script called pbulpreinstall.sh is now in the 'install' directory of our tar files and can be run prior to install PBUL. This script runs some pre-install checks such as hostname resolution, DNS and name services resolution, verifying if the default ports are not in use, checking on the disk space, etc. This script is installed in the '$inst_admin' directory (/usr/sbin by default) after the install.
15. The 'pbversion' script, previously delivered to the PBUL install directory only, is now installed along with the PBUL binaries to the '$inst_admin' directory (/usr/sbin by default). You can run this script to display the versions of PBUL binaries.
16. For a fresh, new install of PBUL, the shared library directory previously /usr/lib/symark/pb is now renamed to /usr/lib/beyondtrust/pb.
For Solaris installations, the location of the SMF files /var/svc/manifest/symark

was also changed to /var/svc/manifest/beyondtrust.

17. Starting with 8.0.0, the following defaults will be used by PBUL, if the keywords were not set previously in pb.settings. This is relevant with a fresh install or for an upgrade when installing PBUL using the pbinstall script or the delivered package installers. The following defaults are:

* allownonreservedconnections changed from "no" to "yes"
* networkencryption changed from "des" to "aes-256"
* "cps=25000 1" added to xinetd.d/pb<daemon>

These defaults will be used for a fresh install or for an upgrade if the keywords were not set previously.

18. Starting with 8.0.0, the following defaults will be proposed during the install process only. If these values are not set in pb.settings, the defaults will remain the same as before 8.0.0.

* minoutgoingport changed from "600" to "1025"
* maxoutgoingport changed from "1023" to "65535"
* randomizesubmitmasters changed from "no" to "yes"

19. New options were added to pbinstall script:

-d: Installs the static pbdemo.key for a fresh install.
This keyfile is static and shipped as part of the tar file.
Therefore it should only be used for demo purposes and should not be used in the production environment.

-L host: This option with a following word argument specifies the hostname to be used for the "logservers" in pb.settings.
A list of host can be specified by repeating the -L argument followed by the host name: -L host1 -L host2

-M host: This option with a following word argument specifies the hostame to be used for the "acceptmasters" and "submitmasters" in pb.settings. A list of host can be specified by repeating the -M argument followed by the host name: -M host1 -M host2

SIGNIFICANT BUG FIXES IN RELEASE 8.0.0-10

1. If runsecurecommand was set and the binary was secure, but the parent directory had group and write permissions, with 'sticky bit' set, pbrun failed to execute the command for root. This is now fixed and pbrun

correctly allows the execution of the command by root if the binary is secure
and in a directory with 'sticky bit' set.
2. If the extended port specification was used for submitmasters, acceptmasters
and logservers (for example: submitmasters myhost:port=32101:interface=myhost),
the port number specified was ignored and the port specified on the masterport
(or logport) was used. This is now fixed.
3. "pblicense -l" produced a segfault if pb.settings on the master host was missing
the 'validation' keyword.
4. The option "pblocald -m <list of masters>" was not working and the list of masters
was ignored. This is now working.
5. An issue was introduced in v6.2.2, where pbksh and pbsh were creating iologs on
the host specified by the logservers keyword of the submit host's pb.settings.
This is now fixed and the host specified in logservers keyword on the master host
is where the iologs are created
6. When leaving the "Record PTY Session" to default "no" in the install, the
"recordunixptysessions" was commented out to "no" in pb.settings therefore
using the default value of the keyword which was "yes". This is now fixed
and pbinstall sets the keyword to the proper value without commenting it.
7. If during the installation using pbinstall, the option to install third party
libraries was deselected, pbinstall hanged and consumed high CPU. This is now fixed.
8. An issue was introduced in 7.5.0 with the set of LDAP libraries delivered for
hppa_hpuxB tar files, where if ldap was enabled in the policy, pbrun failed to
load the LDAP libraries. This is now fixed.

SIGNIFICANT BUG FIXES IN RELEASE 7.5.1-01

1. An issue was introduced in 7.5.0-12, where, on some platforms, the current time
was set to time in UTC. This affected the "time" variable in the eventlog,
as well as the time displayed by policy functions such as "strftime".
2. An issue was introduced in 7.0.0 and above, where, occasionally, one some
environments, When the passwordloggingprompts list contained the string ":"
as part of the list of strings, the iologging did not log the input.
3. An issue was introduced in 7.0.0 and above, where the password was getting
logged on second or more tries, when the password was entered incorrectly

the first time.

4. The default values for the variable "passwordloggingprompts" was changed to:

{"Password", "password", "Passwd", "passwd"}

where the : at the end of each string was removed. This is to accommodate the

default prompt for "submitconfirmuser".

NEW FEATURES IN RELEASE 7.5.0-12

1. Retina CS Integration - Event log central collection:

PowerBroker for Unix & Linux now incorporates the collection of PowerBroker for Unix & Linux events

(accept events, reject events, finish events, and keystroke action events)

by RCS Web Services. PowerBroker Log Servers will be sending eventlog records to

RetinaCS through Web services. One eventlog record for each Accept, Reject, Finish

and Keystrokeaction event will be sent to RCS.

Using Retina CS, you can then sort and filter this data into useful reports.

Retina CS will also use these events to show the list of PBUL servers in the list

of RCS Assets.

2. Retina CS Integration - IO log Indexing for improved search capabilities:

This integration will allow RCS to search for PBUL IOLogs via an indexed search.

PowerBroker for Unix & Linux will use Solr to index IOLog output data and RCS will perform

queries and interpret/display the results, allowing the user to replay the resulting

IOLogs via pbguid.

Each PowerBroker logserver and master host will be able to communicate with a Solr Server,

submitting PBUL IO log output data for indexing.

A Solr server needs to be installed as a PowerBroker component on a Unix/Linux machine.

A separate tar file for Solr installation is provided. Refer to "Solr Installation"

chapter in PowerBroker Installation Guide for more information on how to install Solr.

3. Added a -e option to pbreplay -O to display the standard error captured during

I/O Logging.

SIGNIFICANT BUG FIXES IN RELEASE 7.5.0-12

1. pbssh failed with error "3511 Problem writing client license file"

on AIX 5.1 and HPUX 11.0

2. pbreplay -O was missing output of a "cat" of a large file. This was due to the

incorrect processing of CRLF.

3. An issue was introduced in 7.1.1, where pbrun will produce a segmentation fault when the submithost hostname was unknown to DNS.
4. An issue was introduced in 7.1.1, where the status of system policy function was set to 0 regardless of the exit status of the command.
5. pbinstall did not correctly calculate free disk space when there was an error listing the files on / directory.
6. There was duplicate Finish events logged in the eventlog with pbrun in Optimized Run Mode when pbrun executes a bad/non-existent command.

7. iolog_list eventlog variable was not populated in eventlog when there is no dedicated logserver and pbmasterd does the logging.
8. An issue was fixed with pbreplay -O producing a segmentation violation when the size of the screen was changed while the session was captured and there was inserted characters or deleted lines.
9. An hang issue was fixed with pbreplay -O with some I/O Logs.
11.pbreplay -O displayed garbage output with utf-8 data in the I/O Logfile. This was due to splitting of UTF-8 multi-byte characters.

SIGNIFICANT BUG FIXES IN RELEASE 7.1.1-05 (7.1.1-05 replaced 7.1.0-15):
1. An issue was introduce in 7.1.0, where the eventlog field 'unixtimestamp' was corrupt. This field is ONLY used when Accept and Reject eventlog records are sent to PBIS to set the PBIS event date/time. This made the date/time of the PBIS event set to a wrong date, which was sometimes in the past and therefore the events did not show in PBIS dashboard since they were considered too old.
2. Intermittently, on Solaris platforms, the output from policy functions and procedures remotesystem, system, egrep, fgrep and grep got truncated, if the output was larger than 1K. This was due to pbmasterd not getting the last buffer send by the child process launched to execute the command, after the child was terminated.
3. pbmasterd did not properly closed all file descriptors opened during the parent-child communication when using the functions and procedures system, remotesystem, egrep, fgrep and grep in the policy.

4. Issue introduced in 7.1.0: the timeout in the policy function/procedure RemoteSystem() did not always work.
5. Issue introduced in 7.1.0: When RemoteSystem was used as function and targethost was the submithost, standard error was displayed to screen rather than to policy variable.
6. Issue introduced in 7.1.0: Several hangs were fixed in the policy function/procedure RemoteSystem()
7. Issue introduced in 7.1.0: pbmasterd hung because the IPV6 license file lock was not released.
8. Issue introduced in 7.1.0: pbreplay failed with an iolog from a policy using setkeystrokeaction

---

NEW FEATURES IN RELEASE 7.1.0-15 and 7.1.1-05 (7.1.1-05 replaced 7.1.0-15)

1. PowerBroker for Unix & Linux is now officially integrated with ArcSight and RSA enVision.
2. Added full support for IPv6 on all platforms supporting IPv6 (all except HP-UX 11.00 and 11.11 PA-RISC)
3. pblicense binary can now show the Nodename (uname -n) as well as the last access date of clients.Two new keywords were added to pb.settings:
The "licensedata" indicates which access data fields are to be saved.
Valid values are "none", "accessdate", and "datenodename".
The licensedatafile keyword indicates the /path/filename of the datafile for storing this additional license data.
pblicense new command line options, --current-access and --obsolete-access, allow to list client machines with and without recent access.
4. pbreplay has been enhanced with new options to allow enhanced search capabilities in IO Log files:
-O option by itself produces searchable output by processing the terminal control codes in a virtual screen, then producing output based on that virtual screen. The following options can be used along with -O:
--regex <regular expression>, enables built-in searching via the standard regcomp mechanism.
--files <glob pattern>, used with --regex option, allows multiple files to be searched.

-c <constraint expression> allows the search to be limited to iologs who's
policy variables meet the criteria specified in the constraint expression.
-p <format expression> allows the output to be customized.
5. A new Policy function, remotesystem(), was added. It is used to run commands
on any runhost as part of the policy.
This can be called as a procedure (command output is shown on pbrun's terminal)
or as a function (command output is captured into a policy variable).
This is similar to the system() function/procedure, however the command
in run on a different host.
6. A new keyword in pb.settings and variable in the policy, execute_via_su,
has been added providing the ability to use the 'su -' command to create
a login shell for the secured task, thus allowing the login mechanism to
setup the run environment.
7. Support for LOG_AUTHPRIV facility on Linux
8. Separated the "allowremotejobs" keyword: The new keyword in pb.settings,
"submitremotejobs", on the submit host, when set to yes/no it enables/disables
the use of the -h command line switch of pbrun. If the submitremotejobs
keyword is not present, the allowremotejobs keyword is used to enable/disable
this feature.
9. Two new policy variables, runcksumlist and runmd5list runmd5sumlist,
allow multiple values when performing cksum checksum verification on a file.
10. PowerBroker for Unix & Linux binaries (except pbbench) no longer fail for unrecongized
keywords in pb.settings. This allows the same pb.settings file to be used on
all PowerBroker components, regardless of the version of the product,
starting with v7.1.0 and above.
11. New supported platforms:
Red Hat Ent Linux v6.2 (x86 32-bit & 64-bit)
Ubuntu 8, 9 and 10.04 (x86 32-bit & 64-bit)
Mac OSX 10.6, 10.7 and 10.8 (i386)
Solaris 11 Sparc
Solaris 11 x86
Oracle Enterprise Linux 6.3 (x86 32-bit & 64-bit)*
Oracle Enterprise Linux 6.4 (x86 32-bit & 64-bit)*
Please refer to the README file for the specific flavor names.

*) This includes support for Oracle Unbreakable Enterprise Linux Kernel 2

ADDITIONAL SIGNIFICANT BUG FIXES IN RELEASE 7.1.0-15 and 7.1.1-05 (7.1.1-05 replaced 7.1.0-15):

1. Occasionally, for encrypted iologs, pbreplay matched the checksum with the wrong encryption key/algorithm pair and failed to display the iolog. The fix for this issue now pre-validates the decrypted data to match a policy variable name specification and post validate the parsing of the data to check the required policy variables. If these validation fails, the next key/algorithm pair on iologencryption list is then tried.
2. On AIX 7.1 only, pblicense -l displayed "licensed until Jan 6, 2036" for a permanent license. This was due to a wrong interpretation of the date 0/0/0 on AIX 7.1 and is now fixed.
3. pbrun produced a segmentation fault when the group of the runuser did not exist. This was due to a memory corruption in the code and is now fixed.
4. Randomly, on some platforms, with PowerBroker for Unix & Linux v7.0.0+, when logged in as an AD user, "pbrun --di <shell>" did not display the prompt. This was due to a memory corruption in the code and is now fixed.
5. In the eventlog Finish events, "exitdate" and "exittime" as well as "i18n_exitdate" and "i18n_exittime" were not defined. These are now correctly added to the finish events.
6. pbinstall did not recognize SLES 11 with Patch 2.
7. pbinstall batch component options did not work for pblogd, pbguid, pbsguid and pbsyncd. This is now fixed.
8. Updated documentation:
- Added clarification on how the localmode works, as well as its interaction with IO logging.
- Examples of "in" operator when using wild characters.
- Clarified that pbsync -l and -i option only merges iologs of the same session.
- Corrected the description of the policy function getgrouppasswd which retrieves the user password (and not the group).
- In the Diagnostic Manual, added a note on how to search for sub-messages (i.e. 3003.01, 3003.02, 3003.03 etc).

NEW FEATURES IN RELEASE 7.0.1-02

1. In the finish event in the eventlog, a new keyword "taskttyname" was added that contains the ttyname of the secured task. This ttyname can be used in association with the new syslog formatting settings to record the ttyname in the syslog of the client and associate that with 'last' command (i.e. the wtmp entry). This will be recorded by pbrun (normal and optimized run mode) and by pbksh, pbsh when iologging is on in the policy (when wtmp is updated).

2. Prior to 7.0.1, Solaris Project implementation was as follows:
A Solaris Project can be specified on the pbrun command line, or specified in the policy (overrides the command line), or when not specified, secured tasks and shells inherit the project from the initiating process, if submituser belongs to a project, and runuser is member of this project.
If the Project is not specified and cannot be inherited, the Solaris default project for the runuser is assigned. In 7.0.1, this behavior was changed for pbrun. Now, the runuser inherits the runuser default project by default unless otherwise specified.

3. A new keyword, loadssllibs, was added to pb.settings. The loadssllibs setting determines whether the libraries that are listed in the sharedlibssldependencies setting are loaded at runtime even if the value of the ssl setting is no. This setting is useful in certain cases where the operating system is configured to use SSL and we need to force PowerBroker Servers to load the SSL libraries.

4. A new keyword, loadldaplibs, was added to pb.settings. The loadldaplibs setting determines whether the libraries that are listed in the sharedlibldapdependencies setting are loaded at runtime even if Policy LDAP functions are not used. This setting is useful in certain cases where the operating system is configured to use LDAP and we need to force PowerBroker Servers to load the LDAP libraries.

5. If the environment variable LANG, or one of the environment variable LC_xxxx is set to an invalid value, PowerBroker Server components no longer error and set LANG to C.

6. New supported platforms:
Oracle Enterprise Linux 6.3 (x86 32-bit & 64-bit)*

Oracle Enterprise Linux 6.4 (x86 32-bit & 64-bit)*

Please refer to the README file for the specific flavor names.

*) This includes support for Oracle Unbreakable Enterprise Linux Kernel 2

SIGNIFICANT BUG FIXES IN RELEASE 7.0.1-02:

1. On AIX the policy functions getgroups and useringroup failed to show all the secondary groups returned by groups for LDAP users. This was due to a shortcoming of the standard OS function on AIX, that did not have support for LDAP users as did other Unix/Linux Operating Systems.

2. A new issue was introduced in 6.1.0, preventing pbsh and pbksh to run commands on a remote runhost. This issue is now fixed.

NEW FEATURES IN RELEASE 7.0.0-08

1. Event log central collection: PowerBroker for Unix & Linux events (Accept, Reject, Finish, and keystroke Action events) can now be centrally collected by PowerBroker Identity Services (PBIS) collectors. This allows viewing of these events on PBIS Operations Dashboard as well as the ability to query against this information through the standard PBIS Report plug-in.

2. PowerBroker for Unix & Linux, can also send "health" events to PBIS Collectors based on the responsiveness of PBUL master servers, log servers and pblocald on run hosts. PBUL clients, pbrun, pbsh, pbksh, and pbssh, will optionally report a new event every time a PBUL master or log server fails to respond in a timely manner.

3. A new binary, pbping, was added to PowerBroker for Unix & Linux, to check on the health of PBUL clients. pbping, run from master daemon, checks connectivity to licensed clients' pblocald daemon.

4. Two new options, -m and -l, were added to pbbench to selectively test connection from the client to the master and to the log server.
The -m option will bypass all other tests, and perform only the master connection test. The -l option will bypass all other tests, and perform only the log server connection test. The -l and -m options can be combined to perform both the master connection test and log server connection test.

5. Accept, Reject and Session Syslog messages can now be customized using keywords

in pb.settings which allow you to specify the format and select the specific fields to be written to syslog.
The new keywords are: syslog_accept_format, syslog_reject_format, syslogsession_start_format, syslogsession_start_fail_format, syslogsession_finished_format.
6. A new policy keyword, passwordloggingprompts, was added to specify the list of password prompts for the lognopassword feature. When passwords should not be logged, all I/O will be logged until a password prompt is recognized on standard output. Password prompts to recognize must be listed in the passwordloggingprompts variable. Once a password prompt is recognized, non-echo'd stdin is not logged until a newline is received, or input exceeds 80 characters.
7. pbinstall now allows "--disable_optimized_runmode" to be added as a pbmasterd argument.
8. SELinux is now supported with RedHat 5.4+ (not including RedHat 6.x).

SIGNIFICANT BUG FIXES IN RELEASE 7.0.0-08:
- On some platforms (Solaris, AIX), the policy function system( ) echo'ing a string larger than 1024 characters was truncated to the first 1024.
This was due to a buffer length limitation on some platforms.
The length is now increased to 8K.
- IO logs generated in optimized run mode were missing the exit status.
- pbrun optimized run mode did not log the finished event in syslog.
- When pbrun was run with an invalid command, pblocald logged a finish event in the syslog with an incorrect program name.
- pblocald did not write an accept/reject message in syslog.
This was due to the missing -a option (--syslog_accepts) for the pblocald daemon.
- pblocald did not log start events in syslog.
- pblocald set the runutmpuser to runuser instead of (submit) user.
- pblocald with PAM and pam_setcred enabled, reported the BSM audit-uid as the runuser. The BSM audit record for the secured task now has the correct audit-uid - the submitting user.
- Exit Status was set to "Unable to get termination status for pid:" instead of the actual exit status when using setkeystrokeaction

or runtimeout in policy.
- pbinstall now updates inittab using rmitab on AIX.
- The HP Configuration Package did not contain shell wrappers for pbguid and pbsyncd
- The Solaris, Linux, and HP-UX guihost packages were missing the html and example (policy) files
- Due to missing "printmenuitem", the uninstall script could not Unintsall an installation installed with pbmakeremotetar.
- pbinstall did not install the binary pbguid when only the Secure PBGUI (pbsguid) was selected to be installed.
- Installation of pbsyncd was inconsistent based on the option to "use log host". pbinstall now allows pbsyncd to be installed on the master regardless of the "use log host" choice.
- pbinstall Outbound Port range was checked prior to entering MaxOutgoingPort. It is now correctly checked after.
- The following settings are now obsolete and no longer supported: logfilepermissions, sendeventlogtopsmc, sendiologtopsmc, psmcinstallationid

SIGNIFICANT BUG FIXES AND ENHANCEMENTS IN PATCH 6.2.8-03:

- Intermittently, on Solaris platforms, the output from policy functions and procedures system, egrep, fgrep and grep got truncated, if the output was larger than 1K. This was due to pbmasterd not getting the last buffer send by the child process launched to execute the command, after the child was terminated.
- pbmasterd did not properly closed all file descriptors opened during the parent-child communication when using the functions and procedures system, egrep, fgrep and grep in the policy.

- The policy functions/procedures system/egrep/grep/fgrep occasionaly emitted extra characters at the end of the output

SIGNIFICANT BUG FIXES AND ENHANCEMENTS IN PATCH 6.2.7-01:

- Intermittently, pbmasterd hung after receiving a SIGHUP and the message

"terminated: signal 1 (Hangup) kernel - command in process, status unknown"
was written to pbmasterd.log. SIGHUP is now ignored in pbmasterd.
NEW FEATURES IN RELEASE 6.2.6-02

_____

Refer to list of new features in 7.0.1-02.
SIGNIFICANT BUG FIXES AND ENHANCEMENTS IN PATCH 6.2.6-02:

_____

Refer to list of bug fixes in 7.0.1-02.

_____

SIGNIFICANT BUG FIXES AND ENHANCEMENTS IN PATCH 6.2.5-04:

- In an internal PowerBroker function, when the read() system call returned that
no data was immediately available for reading, the read() was performed in an
infinite loop and caused pblocald to consume high CPU.
- After the child task was sent a SIGTERM and SIGKILL, pblocald (and pbrun)
had an infinite loop waiting for the system to return that the child task had
completed.
- With pbmasterd version 6.2.0, the secured task launched by pbrun -b
(ignore hangups) did not detach from the parent process and was killed if
the parent process was killed.
- Several issues with ulimit on AIX 6.1 when fsize_hard, core_hard, data_hard,
stack_hard, rss_hard were set to values >= 4194304 && <=2147483646 and when
'default' values were different than submituser values in /etc/security/limits.
- PBUL Password Logging mechanism did not support curses-based application.
Therefore even when passwordlogging was explicitly set to 'never', passwords
entered from ncurses-based applications were captured to I/O logs.

_____

SIGNIFICANT BUG FIXES AND ENHANCEMENTS IN PATCH 6.2.4-09:
- An issue was introduced in PBUL 6.0.1, where hostnames starting with a
number were not recognized anymore, causing a connection failure from pbrun
to pbmasterd and pblocald. This is now fixed.
* ENTITLEMENT REPORTING (pbcheck -e) AND pbcheck ISSUES FIXED in 6.2.4-09:

- Reordering IF clauses was changing the report output

- Policy function syslog(), logged to syslog during entitlement reporting.
- The report failed to produce output case statements that fall through to another case
- CSV lists could not be imported into MS Excel
- Certain IF constructs were preventing later IFs from processing an accept
- Certain IF/list patterns were resulting in incomplete output
- ELSE clauses did not properly keep track of conditions
- pbcheck and pbcheck -e did not process variables and functions when a variable was used to identify the include file in the include statement.
For example:
include policy_dir+"/file.conf"
- Entitlement report did not show entries for all qualified users when nested IF's were used
- High detail Entitlement report (pbcheck -e -D high) did not show constraints after a || (or) defined in the policy
- Entitlement report field runargv was displayed as "" when argv and argc were used to construct runargv in the policy
- runargv was displayed as "" when one of the elements of the list was a variable where the value was only known at runtime
- Fixed several memory leaks
- Entitlement output did not iterate through values of split function when used within an IF statement
- Entitlement reports always emitted the runcommand string as runargv[0] even when runargv[0] was overwritten in the policy
- Entitlement report hung and created infinite children when using FOR loop using argc
- Within an IF statement, mixing || and && resulted in incomplete output
- Expression in IF statement was FALSE but was processed as TRUE causing the wrong policy line to be reported
- Entitlement reporting showed the result of the Accept/Reject in the IF clause but not the result of the Accept/Reject in the ELSE clause when the expression was using non-PowerBroker variables
- For an IF / ELSE statement with 3 conditions, the output for the Accept/Rejects statements in the ELSE clause did not print all constraints

when -D high was set
- Signal 11 (Seg Fault) when "split (system (...))" was used in the policy
- Reusing the same list name with different content did not show the correct output when 'if's with multiple conditions were used
- Fixed several Memory allocation problems
- Signal 11 (Seg Fault) when an empty list was used in an IF statement
- When using a string function in a condition, pbcheck -e did not evaluate the function to get the proper list of values
- Missing output with pbcheck -e -l -AR when the elements of the lists were used in an IF or SWITCH condition
- The -l option expanded the lists in an if condition with an "or" when it should have used the list name
- When lists were used within other lists, the report was missing data
- With -l, the SWITCH's default case was reported even though all list elements have been addressed
- Entitlement reporting failed when datecmp(date, ...) function was used in the policy
- FOR loop did not iterate through the elements, and accessed elements past the list and was producing the error "1534 List is too short for subscript"
- Entitlement reporting no longer produces an error "1591 List or element missing" when a list could not be initialized during entitlement
- Entitlement report output was affected by the pb.settings keyword: 'allowremotejobs' and by the master host name which affected policies that test the masterhost variable
- For entitlement reporting strftime should not have returned the current date/time
- Entitlement reporting showed "" in the runHost column when runhost=submithost
- Entitlement reporting did not evaluate correctly datecmp(date1, date2) function when date1 = date2
- Entitlement reporting did not correctly resolve "IF clause" with multiple conditions mixing && and ||
- Signal 11 (Seg fault) when a function call with argv[1] as an argument used a split(system(...)) call

- The NOT operator did not work properly
- Entitlement report hung in a DO-WHILE loop called in a function when a "soft" variable (variable not defined at entitlement reporting time) was passed to the function as the argument
- Entitlement reporting did not list the values when a function was used in the IF statement
- Entitlement reporting of "Accept" did not happen due to a prior "Accept" when a host (or runhost) variable was used
- Entitlement reporting displayed "<requestuser>" in the runuser field instead of the names of users in the list when runuser was set to requestuser
- pbcheck did not process !func() properly (work-around was to use func() == false instead)
- pbcheck -x option for csv format was not listed in the man page
- Remove the message displayed by pbcheck (since 6.1.0) when -f is used (File <file>.conf will be used instead of previously defined file /etc/pb.conf)
- When pbcheck -e -l is used, display the contents of "runargv" (as when -l is not used) instead of the name "runargv"
- Show the constraint related to the main columns user/host/command/runuser/runhost/runcommand in those columns instead of in the constraint field
- Remove redundant auxiliary constraint from constraint column of "pbcheck -e --detail=high"
- Remove unnecessary \\" from the output

* ENTITLEMENT REPORTING AND pbcheck ENHANCEMENTS IMPLEMENTED in 6.2.4-09:

- Improved performance of Entitlement reporting
- Add an option to pbcheck to output the duplicate members in the lists used in a policy (pbcheck -s)
- Add an argument to -l option of pbcheck -e -l to use lists in certain fields
- Add an option to pbcheck to show the members of groups used in the policy (pbcheck -l)

SIGNIFICANT BUG FIXES IN RELEASE PATCH 6.2.3-04

- When the client environment contained environment variables with non-ascii

characters, older releases of PB clients failed to connect to 6.2.0 PB Master,
displaying an error "5102.04 Invalid communication startup".
The same issue would occur when 6.2.0 PB clients connecting to older releases
of PB Master.
- When multiple network encryption algorithms are used, the client machine
re-write pb.settings re-ording the encryptions algorithms for efficency.
During this re-writing process the keyword "altsubmitmasters" was not re-written
to the new pb.settings.
- pbmasterd occasionally failed with the error:
"5430 header problem in readMuxHeader fd 4. Expected 5 bytes: Connection timed out"

- When runcksum was used in the policy for a non-root runuser,
the secured task ran with root privileges (6.2.1-01 service pack).
- Due to a problem in AT&T Ksh, occasionally when executing "pbrun ksh"
from a ksh session, the shell prompt was lost.
- PowerBroker Shells, pbksh and pbsh, did not fall back to native root mode
when logservers were not reachable.
- On Solaris 11, pbrun --solarisprojects in --di mode was producing the error
"Solaris project specified for non-Solaris Projects platform".
- When the Project (Solaris Project) for a user was changed in the policy or
on the command line, and the library specified in 'sharedlibsolarisprojects'
was not accessible or could not be loaded, pbrun did not error and defaulted
to the default Project of the user.
- 'runcwd' was not enforced when pbrun command was executed from a directory
with execute permissions for "others".
- If the directory specified by 'runcwd' did not exist, no error messages were
displayed and the command was executed in current directory instead of /tmp.
- When enforceruncwd was set to NO, a relative path was used for command, and
runuser did not have permissions for runcwd, an unauthorized program
/tmp/<relative_path>/<command> could run instead.
- alternatesubmitmasters did not work in some cases with metacharacter asterisk.
- pblog and pbreply hung when used with certain options and when logs
contained non-english (Japanese) data (i.e. dates).
- pbrun crashed or set the ulimit value to the wrong value, when value was

larger than 4194303.
- Command Line Arguments were not passed from pbrun to shell scripts that
did not specify the interpreter in the first line.

_____

NEW FEATURES IN RELEASE 6.2.0-09

Note: BeyondTrust recommends that before any clients are upgraded to the latest release of PowerBroker, the Master and the Log servers should be upgraded to the latest release.

1. A new feature was added to allow using an alternate master based on the submituser or command. The keyword 'altsubmitmasters' in pb.settings, on the client side, allows the specification for a different master to be used with a defined list of users and commands.
2. A new keyword (randomizesubmitmasters) was added that, when set, will randomize the master used from the list of submitmasters. Previously, always the first master on the list was used, unless the master was down. When this keyword is set to 'yes', a master will randomly be picked from the list.
3. A new keyword (pktimeout) was added for pbssh to set the timeout period for the PowerBroker Password Safe.
4. A new command line option (-D) was added to pbssh, to specify a domain for PowerBroker Password Safe to use when obtaining a domain account password, or defines a PowerBroker Password Safe managed system alias to use instead of the actual host name.
5. Support for native AIX Package Installers for PowerBroker. This includes support for AIX WPAR.
6. Web-based Task Manager is a PowerBroker browser interface feature, introduced in 6.1.0, that enabled a user to execute commands through pbrun on a Unix or Linux host from the Web browser. Web-based Task Manager now supports pbssh as well as pbrun. When using "pbssh", all commands issued will be executed as "pbssh -h <host> -u <user> -C <command>" and verified against the PowerBroker policy.
7. A separate package is now offered for pbssh (PowerBroker Express)
8. A new setting, "shortnamepk", is introduced to support short names when using PowerBroker Password Safe in pbssh.
9. When pbssh is invoked, "pbclientmode" is now set to 'pbssh' rather than 'run'.

10. An option (-r or --pk_reset_password) was added to pbssh, to optionally
request PowerBroker Password Safe to reset the password.
11. Entitlement report performance has been improved.
12. Two new options were added to 'pbcheck -e' to limit the number of active
processes and as safety mechanisms to prevent crippling a system with too
many processes.
--maxchildren: This option limits the total number of live pbcheck descendant
processes. After this limit is reached, the entire pbcheck
process tree is terminated. The default value is 200.
--maxloopchildren: This option limits the number of child processes that
evaluate the same policy line (for example, an endless loop).
After this limit is reached, the process that encounters the
same line for the specified number exits allowing other
processes to continue. The default value is 4.
13. New supported platforms:
Oracle Unbreakable Enterprise Kernel (x86 64-bit)
VMware ESX 4.1 (x86 64-bit)
Please refer to the README file for the specific flavor names.
14. PowerBroker is now certified on VMware vSphere Management Assistant (vMA) 4.1.
To install and run PowerBroker on a vMA host you need to:
- Use sudo to run pbinstall. You cannot login as root on a vMA host.
- Make sure xinetd is started on the vMA host.
- By default vMA is setup with a firewall closing all incoming connections
except port 22 for ssh.
Make sure the port used for pblocald is open.
- PBGUI was not fully certified on vMA since some features of the GUI need
to open random ports.
- You might run into problems executing some of the vMA commands through pbrun
(vifp, vilogger, vifptarget). This is due to a known issue in v6.2.0-09,
where the command line arguments were not getting passed to the shell scripts
executed through pbrun, in scripts where the interpreter is not specified
on the first line. Some vMA commands are shell scripts in /usr/bin that are
calling binaries in /opt/vmware/vma/bin/, and these scripts do not have the
shell interpreter specified on their first line. To work around this issue,

you can either add the shell interpreter to the first line of these shell scripts, or add the following lines to your PowerBroker policy:

```
if ( basename(command) in {"vifp", "vilogger", "vifptarget"} )
{
runcommand = "/opt/vmware/vma/bin/" + basename(command);
setenv("LD_LIBRARY_PATH", "/opt/vmware/vma/lib64");
accept;
}
```

15. New supported platforms:

Red Hat Ent Linux v6.0 (x86 32-bit)

Red Hat Ent Linux v6.0 (x86 64-bit)

IBM zSeries Red Hat Ent Linux v6.0 (s390x 64-bit)

Please refer to the README file for the specific flavor names.

16. Support for native HP-UX Package Installers for PowerBroker.

17. New supported platforms:

IBM AIX v7.1 (POWER 64-bit)

Red Hat Ent Linux v5.6 (x86 32-bit)

Red Hat Ent Linux v5.6 (x86 64-bit)

Red Hat Ent Linux v5.6 (Itanium 64-bit)

Oracle Solaris 11 Express (SPARC)

Oracle Solaris 11 Express (x86 64-bit)

Red Hat Ent Linux v5.7 (x86 32-bit)

Red Hat Ent Linux v5.7 (x86 64-bit)

Red Hat Ent Linux v6.1 (x86 32-bit)

Red Hat Ent Linux v6.1 (x86 64-bit)

SIGNIFICANT BUG FIXES IN RELEASE 6.2.0-09

Issue 1: In PB 6.1.0, Entitlement report was displaying runhost with the same value as submithost if runhost was not explicitely set in the policy.

Resolution: Entitlement report now correctly shows runhost as "" (ALL) if runhost is not explicitely set in the policy, since the value of runhost can be set to host specified by "-h <host>".

Issue 2: Entitlement report does not show the "fall through" accept in the report when the "if" statement is empty.

Resolution: This is now fixed and the "fall through" accept is correctly shown in the report.

Issue 3: Incorrect entitlement reporting when user variables are used in a decision.

Resolution: User variables are now taken into consideration when they are set to entitlement report fields (submithost, submituser, user, host, command, etc...).

Issue 4: During entitlement reporting, include files are not closed each time they are opened, resulting in too many open files

Resolution: The include files opened are now correctly closed.

Issue 5: Entitlement report shows false accepts when the conditions reported would NOT result in an accept

Resolution: This is now fixed.

Issue 6: Entitlement report is missing data when 'if' statement has three 'or' (||) elements

Resolution: This is now fixed.

Issue 7: Entitlement report in the GUI shows bad data (data from "command" field") when the command field was set to a long value with a list

Resolution: This is now fixed.

Issue 8: In Entitlement report the list of runusers is incorrectly used as list of users

Resolution: This is now fixed.

Issue 9: In Entitlement report the list of runusers is SOMETIMES applied to runuser in later IF statements

Resolution: This is now fixed.

Issue 10: In Entitlement report the use of "runuser=requestuser" was not reported accurately

Resolution: If runuser is set to requestuser, the report now shows <requestuser> in the runuser field.

Issue 11: In Entitlement report, When testing the "host" variable instead of the "runhost" variable, the runhost is not filled out in the report

Resolution: The runhost is now correctly filled in the report.

Issue 12: In Entitlement report, accepts within a switch's default case are not reported.

Resolution: This is now fixed.

Issue 13: Entitlement processing of case statements (and others) builds the statements up with the same incorrect line number

Resolution: The line number is now correct for all cases.

Issue 14: "pbcheck -e --nolist" option fails when number of elements is zero or when the first element is a list

Resolution: This is now fixed.

KNOWN ISSUES IN ENTITLEMENT REPORT IN RELEASE 6.2.0 AND PRIOR:

1. Reordering IF clauses can change the report output.
2. Entitlement report fails to report case statements that fall through to another case.
3. Entitlement report CSV lists cannot be imported into MS Excel.
4. PB Entitlement: certain IF constructs can prevent later IFs from processing an accept.
5. Certain If/list patterns result in incomplete output.
6. Else clauses do not properly keep track of conditions.
7. pbcheck -e -D high option always prints "" for dependencies.
8. pbcheck and pbcheck -e do not process variables and functions when the include statement uses a variable to identify the include file (for example include policy_dir+"/file.conf";)
9. Conditions set by nested IFs are not known to statements past the upper level for the nested IFs.
10. Entitlement report doesn't show entries for all qualified users when nested IF are used.
11. High detail Entitlement report doesn't show constraints after an || (or) defined in the policy.
12. Entitlement report does not populate the argv field when and argv element (e.g. argv[1]) is tested in the policy.
13. Entitlement report might show redundant entries in the report.

NEW FEATURES IN RELEASE 6.1.0-17

1. A new feature was introduced that allows you, using PowerBroker policy and the pbssh program, to control access to, and activities on, SSH-managed

devices. The pbssh program uses the SSH protocol (or, optionally, the telnet protocol) to connect to devices that do not have PowerBroker installed on them; such devices can include Windows computers and certain network devices.

2. Web-based Task Manager is a PowerBroker browser interface feature that enables you to execute commands on a Unix or Linux host from your Web browser. In the background, a pbrun process submits the command to the master host, which processes the command against the PowerBroker policy, and the command is sent to the run host for execution. Results are displayed in the Task Manager interface.

You can customize the Task Manager interface using HTML form tags. In this way, you can limit the set of commands that a user can execute or specify command line options for specific commands.

3. Solaris Package Installers now support Solaris Zones.

4. Solaris 9 introduces the concept of a "project", which associates a running process with a project. PowerBroker Secured tasks can now be associated with a Solaris project.

5. PowerBroker now has support for Unicode (UTF-8) character set in PowerBroker policies. The logging system will also be able to log input/output which contains multi-byte characters. In this first phase of support for Unicode character set, the following PowerBroker components will be supporting Unicode:

- pbrun/pblocald/pbmasterd/pbcheck/pbcall/policy function Unicode(UTF-8) support.
- Logging functionalities: I/O event log, pblogd, pbreplay/pblog, pbsync/pbsyncd.
- Running install related scripts.

In this first phase, we will not provide support for Unicode character set for the Shells (pbksh, pbsh), PowerBroker utilities (pbvi, pbnvi, pbless, pbmg, pbmerge, pbumacs) and the PowerBroker GUI.

6. An option (-b or --nobasename) was added to "pbcheck -e" to explicitly list the command field even when "basename(command)" is used.

7. An option (-l or --nolists) was added to "pbcheck -e" to emit the policy list names, rather than the list elements, for lists of users, hosts, or commands,

resulting in a more concise output.

8. New supported platforms:

IBM zSeries Red Hat Linux Ent Serv 5.2 (s390x 64-bit)

IBM zSeries Red Hat Linux Ent Serv 5.3 (s390x 64-bit)

IBM zSeries Red Hat Linux Ent Serv 5.5 (s390x 64-bit)

IBM zSeries SuSE Linux Ent Serv 10.3 (s390x 64-bit)

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 6.1.0-17

Issue 1: Entitlement reporting (pbcheck -e) failed with a seg fault when the policy contained the function sub() calling the function system()

Resolution: This was due to a bad memory initialization and is now fixed.

Issue 2: pbrun gives no output on SELinux when telnet is used to access the host.

Resolution: This was due to a lack of SELinux permissions on pbrun to write to a telnet session.The PowerBroker SELinux policies have now been updated with this permission.

Issue 3: A 'pbrun vgs' or 'pbrun lvcreate' on Linux produced the error: "File descriptor leaked on vgs invocation"

Resolution: This was due to file descriptors left open before forking for the new process. All extra file descriptors are now closed properly.

Issue 4: pblocald fails to prevent execution of non-secure task when runsecurecommand is set.

Resolution: pblocald now correctly prevents the execution of a non-secure task when runsecurecommand is set.

Issue 5: When a stock PB install was not making use of a logserver, the runconfirmuser displays the clear-text password (6.0.1 release only).

Resolution: This issue is now fixed.

Issue 6: The policy function gsub failed for some regular expressions (6.0.1 release only).

Resolution: This issue is now fixed.

Issue 7: When enforcruncwd was set to yes, and a command was executed from a directory without proper permissions and iologging is on, pbksh was hanging (6.0.1 release only).

Resolution: This issue is now fixed.

Issue 8: When the policy variable "shellcheckbuiltins" was set to true at shell start, a print() statement changed the tty behavior after a "built-in command" was issued (6.0.1 release only).
Resolution: The tty setting is now correctly restored.
Issue 9: When submitconfirmuser was preceded by a command (such as grep), after the password was entered, the output of the secured task run by pbrun was displayed on the same line (6.0.1 release only).
Resolution: This was due to the tty settings not being restored correctly after the password was entered and is now fixed.

Issue 10: The PowerBroker shells (pbksh and pbsh) were echo'ing back the commands when in native root mode (6.0.1 release only).
Resolution: The commands are no longer echo'ed back and the shells behave properly in native root mode.
Issue 11: "pbrun -di" request failed when networkencryption was enabled and runconfirmuser was set (6.0.1 release only).
Resolution: This was due to the communication structure not being properly updated between pblocald and pbrun and is now fixed.
Issue 12: pbreport errors with "FATAL ERR - instruction: mvc.. bb0($rc200),aa0 ($rc2" when the report was filtered by date and the output was too large (6.0.1 release only)
Resolution: This is now fixed.
Issue 13: When running a report from the GUI, as a non-root user, the report failed with a "permission denied" error on the pb.eventlog (6.0.1 release only).
Resolution: This was due to pblog not acquiring the correct privileges and is now fixed.
Issue 14: "pbcheck -e" did not emit the correct value of runargv[0] in the entitlement output. The value reported was always set to the runcommand string.
Resolution: pbcheck Entitlement reporting now shows the correct value of runargv[0].
Issue 15: The single Sign-On mechanism did not work in PBGUI when launched through PowerBroker Management Console when https (SSL) is used

with WebLogic.

Resolution: This is now fixed.

Issue 16: Publishing policies through PowerBroker Management Console caused a hang when a policy larger than 16K and https was used.

Resolution: This was due to the packet size limit with SSL and is now fixed.

SIGNIFICANT BUG FIXES IN RELEASE 6.0.1-11

Issue 1: A new issue was introduced in 6.0.1-10, preventing all PowerBroker components to function correctly when masterport, localport, logport, and/or syncport were changed from their numeric values to their named values in /etc/services.

Resolution: This issue is now fixed in 6.0.1-11 which will fully replace 6.0.1-10.

NEW FEATURES IN RELEASE 6.0.1-11

1. On AIX platforms, PowerBroker pbrun now sets the ulimit of the runuser based on the values in /etc/security/limits of the runhost.
2. The option -d (-d, --display_headers) has been added to "pbcheck -e" to display the header showing the name of the displayed fields.
3. In PowerBroker 6.0.0, pbsyncd had a hard-coded value of 50 milliseconds to waiting time between packets send to PSMC . This value is now configurable (on PSMC side) and has been added to psmc.settings file.
4. "pbsyncd -M" was enhanced to check both incoming and outgoing connections to the PSMC.
5. On Solaris and Linux, PowerBroker patches are also delivered in the form of Packages, and can now be installed using the native platform package installer.
6. pbbench now supports /dev/null for logs
7. Diagnostic messages for submittimeout and runtimeout are now different.
8. Added support for 'shellforbiddencommands' and 'setkeystrokeactions' in the report files.
9. New supported platforms:

IBM zSeries SuSE Linux Ent Serv 10 (s390 64-bit)

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 6.0.1-10

Issue 1: When using the PSMC generated usernames, one could access PBGUI with full privileges if the same username was created as a NIS, LDAP, or local user.

Resolution: PBGUI now authenticates back with PSMC for usernames with a "+PSMC" prefix, even if the same username exists in NIS, LDAP or as a local user.

Issue 2: In a "for" loop in the policy, the counter could not be manipulated within the loop.

Resolution: The "for" loop is now behaving as a standard "for" loop of any language, and if the value of the counter is changed, the value is kept and is not reset to the next iteration.

Issue 3: In PowerBroker 6.0.0, a change of behavior was introduced in the output of "pbreplay -t". The timestamp was not displayed in every line anymore.

Resolution: We now display the timestamp at the beginning of every line of the output.

Issue 4: When the notation "<port>:interface=<ip_address>" was used for the "masterport", "localport" or "logport", PowerBroker client could not resolve the hostname and failed with the error "3411 master <hostname> is not listed in run host <host>'s acceptmaster rules".

Resolution: The <ip_address> is now correctly resolved and the hostnames compared correctly.

Issue 5: When a user-defined variable used in the policy, was unset( ) at the end of the policy, the entitlement report was reporting an "unknown variable" error.

Resolution: Entitlement report is now ignoring the unset( ) action when composing the report.

Issue 6: When the "iolog" variable was set to a statement that contained a variable, the "iolog" field in the entitlement report was always set to "no".

Resolution: The issue is now fixed, and the "iolog" field is now set to "yes" for soft value iolog file names.

Issue 7: If a list within a list was used in the policy, the entitlement report

was not considering the fields within the {} as a separate field
(i.e "a, b, {x, y, z}, c" was interpreted as "a, b, x, y, z, c".
Resolution: The entitlement report now shows the fields within {} as one field.
Issue 8: When runuser, runcommand, runhost and runargv were not explicitly set in a policy and therefore default to the submituser, command, submithost, and argv variables, the entitlement report shows them as empty strings.
Resolution: The entitlement report is now correctly using submituser, command, submithost, and argv for runuser, runcommand, runhost and runargv when they are not explicitly set in the policy.
Issue 9: Due to a bug in the glibc library on Z/Linux S390 31 bit, the binaries compiled on this type of operating system and run on a Z/Linux S390 64 bit were corrupting the wtmp file and causing the "last" command not to work properly.
Resolution: PowerBroker now provides two separate tar files for Z/Linux S390 31 bit and Z/Linux S390 64-bit to work around this glibc bug.
Issue 10: pblog was not displaying the records after the "record with the field not set".
Resolution: This is now fixed and pblog now shows all the records correctly.
Issue 11: Intermittently, when the keystrokes were typed too fast or copied/pasted, keystroke logging failed to log the input in the I/O logfiles.
Resolution: This was due to the incorrect comparison of the input and output buffers and is now fixed.
Issue 12: pbksh ignores the interrupt signal (i.e CTRL-C)
Resolution: We now correctly check the return status of the child (the command) before continuing to run the next command.
Issue 13: The policy function split() was ignoring the last delimiter in a list if it was followed by nothing ("a-b-c-")
Resolution: The function split() now takes the last delimiter into consideration when the third argument of the function is "false".
Issue 14: In a chroot'ed environment, the 'pbrun <command>' hangs when the <command> does not exist in the chroot'ed directory, if pb.settings is not copied to the etc directory of the chroot'ed directory
Resolution: Since pb.settings was missing, pbrun was trying to log an error but

the required information to log the error needed to be obtained
from pb.settings, therefore resulting in an infinite loop.
pbrun is now printing the error to the standard error if pb.settings
is missing.
Issue 15: On Mac OS (both i386 and PowerPC), when "masterprotocoltimeout" is set
to 1000, pbrun --di fails with error "5408.01".
Resolution: This was due to an incompatibility of the time functions used on
Mac OS and is now fixed.
Issue 16: On Mac OS 10.5 i386, when pamsessionservice is set to a service that
uses "pam_securityserver.so", pbrun seg faults.
Resolution: This is now fixed.
Issue 17: pbcall -getgroup(s) produced a segmentation fault when the incorrect
syntax was used.
Resolution: This is now fixed.
Issue 18: pbksh session is stuck and does not continue to write keystroke data
when the primary PowerBroker master becomes unavailable in the middle
of the session.
Resolution: A new keyword, "iologack" was introduced to acknowledge packets sent
and to prevent a hang.
Issue 19: If pb.key was located in a directory with no execute permissions for
non-root users; the error "3033 key file unreachable" was displayed
by PowerBroker.
Resolution: We are now acquiring the correct privileges before checking on the
existence of the file.
Issue 20: PowerBroker truncates values greater than 65535 when used as a port
number.
Resolution: PowerBroker is now correctly reading the values greater than 65535.
Issue 21: Running "pbrun <file>" as a non-root user, where <file> does not have
execute permissions for non-root users, does not fail.
Resolution: PowerBroker is now executing the shell scripts using "sh -c" option.
Issue 22: On Solaris, when a non-root user executes pbrun of a non-existing file,
it fails with "5457 Could not reacquire root".
Resolution: This was due to a non-standard behavior of OS functions used to
acquire the correct privileges on Solaris, and a work-around was

added to correct the behavior.

Issue 23: pbksh was killed if a CTRL-C (interrupt) was issued with "shellcheckbuiltins=true" in the policy.

Resolution: The signal handler is now correctly set when "shellcheckbuiltins" is set to true in the policy.

Issue 24: If the policy contains functions such as getuserpasswd, runconfirmuser, etc and the command run has its pty closed when the password is requested, it is displayed on the standard output.

Resolution: This is now fixed.

Issue 25: For non-root users, the policy 'runcksum' verification failed.

Resolution: This was happening when the file running the check sum did not have access privileges for the non-root users. PowerBroker is now acquiring the correct privileges before checking the existence of the file and running check sum.

Issue 26: Power Broker does not capture input and only captures standard output and standard error streams when a job is run in "pipe mode" and lognopassword is set to true.

Resolution: Since the input was coming from a pipe, it was mistakenly considered to be a password and therefore was not logged. This is now fixed.

Issue 27: pbcheck -e was not processing "include" file inside of an "if" statement.

Resolution: pbcheck is now correctly processing "include" files anywhere in the policy.

Issue 28: When a script was executed by PowerBroker, if the interpreter specified in the first line of the script did not exist, pbrun crashed.

Resolution: pbrun now checks for the existence of the interpreter on the first line of a script before using it.

Issue 29: Rejected keystrokes (set by setkeystrokeaction) resulted in extra or missing finish events in the event logfiles.

Resolution: This was due to missing calls to keystroke logging in some cases or to additional calls in other cases, and is now fixed.

Issue 30: pbrun produced a segmentation fault when submitmaster is an invalid host and pbrunlog is a non existing path.

Resolution: This is now fixed.

Issue 31: Kerberos password is not requested a second time by pbksh after the first failure.

Resolution: The Kerberos ticket cache, used by pblogd and pblocald, was used by pbksh and therefore it was not requesting the password anymore.
This is now fixed.

Issue 32: runchroot policy variable was not working with PBGUI.

Resolution: PBGUI now supports runchroot. This requires both pbguid and pbmasterd to be at version 6.0.1 and above.

Issue 33: On some operating systems, pbnvi showed the following message "Error: /var/preserve/vi.recover: No such file or directory" before opening the file.

Resolution: pbnvi was not checking the existence of the "preserve" path at run time. This is now fixed.

Issue 34: PBGUI did not save GUI configuration variables, such as: "Netgroup Lookup" and "Select List Limit" for Policy Editor.

Resolution: This is now fixed.

Issue 35: On some platforms, when the "runcksum" policy variable contained extra characters at the beginning but the trailing value was the correct check sum, it was considered correct.

Resolution: This was due to the way the content of this variable was read on some platforms, and it is now fixed.

Issue 36: When an event had "\n" in it, the report generated from the event log was not displaying the entire event log.

Resolution: The report generator used by PowerBroker, expects all data to be on the same line. When the report is generated, the \n is now replaced by the character "\n" and the entire event log is displayed.

Issue 37: When pbmasterd rejects a request due to slave protocol error, it does not record the reject in the event log.

Resolution: The reject is now correctly logged in the event log.

Issue 38: Using the asterisk (*) in a regular expression for gsub() function causes pbcheck to hang.

Resolution: The processing of some of the special characters in the regular expressions resulted in an infinite loop. This is now fixed.

Issue 39: pbinstall comments recordunixptysessions in pb.settings backwards

("no" was commented out instead of "yes").
Resolution: pbinstall now comments out recordunixptysessions when it's set to "yes" only, since the default is "yes".
Issue 40: pbpatchinstall was continuing to install when there was not enough disk space.
Resolution: pbpatchinstall now exits if there is not enough disk space.
Issue 41: pbpatchinstall was not checking if a PowerBroker binary, such as pbksh, is in use before trying to replace it.
Resolution: pbpatchinstall now renames the binary, and then tries to replace it. If there is a problem, it will issue a warning message.

KNOWN ISSUES in RELEASE 6.0.1:
1. A problem was introduced in PowerBroker shells (pbksh and pbsh) when running in native root mode. The shells will echo back the command types on the standard input. The eventlog and I/O logs do not contain this extra output.

BUG FIXES IN PATCH 6.0.0-16-SP1
- On some platforms, pbguid produced a seg fault when clicking on "GUI configuration".
- Corrections have been made to two of the sample policies, pbguid.conf and pblib.conf.

NEW FEATURES IN RELEASE 6.0.0-16
1. Event and I/O Log Integration with PowerSeries Management Console (PSMC)
PowerBroker is now integrated with PowerSeries Management Console. If configured to do so, while writing the event logs and I/O logs to disk, PowerBroker logservers will also send the logs to PSMC using a Message Queue server (ActiveMQ).
2. PBGUI new interface
PowerBroker GUI has now a new look that matches the PowerSeries Management Console interface. PBGUI can now be launched either stand-alone, or from PSMC.
3. SELinux compatibility support: PowerBroker is now integrated with SELinux targeted policy on Red Hat Enterprise Linux 5 to confine PowerBroker.

The pbrun, pbmasterd, and pblogd, and optionally the pblocald PowerBroker components will run in their own confined domains.

4. Support for native Linux and Solaris Package Installers for PowerBroker.

5. pbsync now collects and merges I/O logs.

6. pbsync has an added functionality to synchronize old and new event and IO logs to the PSMC.

7. pbsync now reads the local pb.settings for each remote log servers to get the path where the event log is located. Previously, pbsync was using the path of the event log where pbsync was launched from, for the remote log servers.

8. Two new keywords are introduced to disable optimized run mode in the pb.settings file, for the pbrun client and for pbmasterd, and a new policy variable is introduced to disable optimized run mode via the Policy.

9. System node and host names on HP-UX have default length limits of 8 and 64 bytes, respectively. On HP-UX 11i v2 (B.11.23.01) and HP-UX 11i v3 (B.11.31.01) and later versions, the system administrator can configure the system to expand both these limits to 255 bytes. PowerBroker now supports system node and host names up to 255 bytes. On HP-UX PA-RISC systems, the new flavor pbhppa_hpuxD needs to be used in order to support long node and host names.

10. A new setting "syncprotocoltimeout" was added to control the protocol timeout between pbsync and pbsyncd.

11. A new feature "Environment File Processing" allows PowerBroker to alter the run environment using environment configuration files such as /etc/environment. The policy variable "runenvironmentfile" and the settings keyword "environmentfile" can be set to the full /path/filename of the environment file to use.

12. Due to the encryption changes in 5.2.0, when network encryption was used along with Kerberos, a 5.2.0 client was not able to communicate with an older master. In this release, 6.0.0 clients can now communicate with masters and logservers older than 5.2.0.

13. New example policies have been added to PowerBroker. The directory structure where these examples now resides has also changed to better organize the example policies.

SIGNIFICANT BUG FIXES IN RELEASE 6.0.0-16

Issue 1: When I/O logging was enabled in the policy, and iologencryption and networkencryption used different encryption keys, or when I/O logs were encrypted and Kerberos was used, pbksh was failing with "3061 encrypt mangler initMangle failure" for a non-root user.
Resolution: This is now fixed.
Issue 2: In certain circumstances, pbguid was corrupting the policy file.
Resolution: This was due to a memory corruption in the code and is now fixed.
Issue 3: pbsync failed when algorithms specified in eventlogencryption are in a different order on the master and the client.
Resolution: pbsync is now able to merge event logs with different encryption. It will use the oldest encryption algorithm to encrypt the merged event log.
Issue 4: PowerBroker did not honor PAM ulimit
Resolution: PowerBroker was calling PAM session from the parent process, thus the child executing the secure taks did not get the ulimits. It is now correctly calling PAM session from the child and therefore honoring the PAM ulimit.
Issue 5: pbsync and pbsyncd failed when Kerberos and/or SSL was enabled.
Resolution: This was due to a mis-construction of the buffers used to communicate with the master and other coding issues. This is now fixed.
Issue 6: When the Kerberos keytab was empty (0 bytes) on the client machine, pbmasterd was hanging and consuming CPU as a run-away process and pblocald was crashing.
Resolution: This was due to a Kerberos bug. PowerBroker now checks for this condition before calling the faulty Kerberos function.
Issue 7: On AIX 5.2/5.3, when LAM is configured to use KRB5A in the file /usr/lib/security/methods.cfg and the user is configured to use STD_AUTH, submitconfirmuser does not work when Kerberos password is entered at the password prompt.
Resolution: This issue was due to the fact that Kerberos shared libraries were not loaded, since "Kerberos" keyword was set to "no" in pb.settings. A new keyword "LoadKrb5Libs" has now been added to force Kerberos libraries to load even if "Kerberos" keyword is set to "no".

Issue 8: When "networkencryption" is set to none and there is a problem connecting to the local server, pbbench seg faults on the logserver

Resolution: This is now fixed.

Issue 9: pbrun in Optimized Run Mode did not capture the exit status of the delegated job

Resolution: This issue was introduced in 5.1.2 and above. pbrun (in optimized run mode) shows the exit status of pbrun instead of the exit status of the delegated job. This is now fixed.

Issue 10: On MacOS, 'pbrun csh' failed with error "csh: Permission denied", when it was run from a non-root user, with a policy setting runuser and rungroup.

Resolution: This was due to a problem on MacOS only, with changing the group id to the effective group id. The problem is now fixed.

Issue 11: On HP-UX, superdaemons (pbguid and pbsyncd specifically), when launched from inittab, did not inherit the PATH.

Resolution: The installer now has a shell wrapper for pbsyncd and pbguid, setting the PATH before launching the binary.

Issue 12: Syslog messages displayed junk characters instead of %s when %s was used in the first argument passed to the syslog function in the policy, and the command passed to syslog also contained a %.

Resolution: The %s contained within the policy variable was being interpreted by a *printf-like function as a print format character. Corrected the code so that policy or environment variables are not interpreted as printf format specifiers.

Issue 13: When runconfirmuser is used in the policy, and a wrong password is entered for a local user, the event log reports an exit status of "undefined".

Resolution: pbrun is now correctly sending the result of password checking to the log.

Issue 14: Environment variable TERM was not correctly read when another environment variable starting with "TERM" was present

(for example TERMINAL_EMULATOR).
Resolution: This was due to a problem in the code where only the first
4 characters of the environment variables were scanned to find
the variable TERM. This is now fixed.
Issue 15: pbreplay -t -o <file> displays the commands incorrectly.
Resolution: The commands listed were not shown correctly, and had duplicate
characters. This is now fixed.
Issue 16: The timestamp displayed by "pbreplay -t" does not display the timestamp
and the command on the same line.
Resolution: This was a design issue. The timestamp and the command were displayed
on two lines, which prevented the use of "grep" to search for the list
of command of a specific date. The timestamp and the command are now
displayed on the same line.

Issue 17: "pbcall -getgroups <user>" returns a string with a trailing comma.
Resolution: The behavior was changed in 5.1.x releases, and is now changed back
to pre-5.1.0. The string returned no longer has a trailing comma.
Issue 18: The functions gsub and pad did not correctly substitute by %.
Resolution: The % was not substituted correctly, if the string to substitute also
contained %. This is now fixed.
Issue 19: The policy function "system" causes memory corruption on Linux
x86 64 bit when response is exactly 760 characters.
Resolution: This was due to a bad memory initialization in the code and is
now fixed.
Issue 20: PBGUID is not working in https mode on HP 11.0 PA-RISC and AIX 5.1
Resolution: This was due to missing calls to get an RNG (Random Number Generator)
before the SSL functions and is now fixed.

Issue 21: A seg-fault caused within a non-child signal handler results in a hang
on PowerBroker daemons consuming CPU.
Resolution: This was observed on AIX and HPUX: when for any reason a seg fault
caused the program to enter the signal handler then within the signal
handler, a coding error results in a segmentation fault.
This was resulting in a hang, with the process consuming CPU.

This is now fixed.

Issue 22: When a non-root user session is recorded (iolog is used in the policy) and the "iologencryption" and "networkencryption" used different encryption keys, pbksh was failing with "3061 encrypt mangler initMangle failure".

Resolution: The root privileges were not acquired before reading a file owned by root. This is now fixed.

Issue 23: If the "iolog" is set to a secured directory, pbksh fails with "5473 Could not stat file system for <directory>: Permission denied" when executed from a non-root user.

Resolution: The root privileges were not acquired before writing to the secured directory. This is now fixed.

Issue 24: The option "pbguid --https" was not functional even though it was documented.

Resolution: The option name was changed to "--secure" and is now functional.

BUG FIXES IN PATCH 5.2.0-11-SP1

- When a command is executed through pbksh or pbsh, and a directory with the same name as the command exists in PATH, pbksh/pbsh tries to execute the directory.

NEW FEATURES IN RELEASE 5.2.0-11

Note: BeyondTrust recommends that before any clients are upgraded to the latest release of PowerBroker, the Master and the Log servers should be upgraded to the latest release. For PowerBroker 5.2.0, due to the changes in the encryption code, this is an absolute requirement.

1. PowerBroker now allows different encryption algorithm/key pairs to be used on different hosts. This provides the ability to have two or more algorithms/key pairs to be active simultaneously. This allows the old algorithm/key pairs to continue to function on previous releases of PowerBroker while new algorithm/key pairs are phased in during an upgrade.

2. PowerBroker is now separating the encryption algorithm/key pairs for network traffic, event logs, I/O logs and report files. The keyword 'encrypt' and

'keyfile' are now obsolote and have been replaced by the new keywords.
The install script, pbinstall, will take care of "migrating" the old
keywords to the new ones.

3. PowerBroker GUI now has support for PAM and can authenticate non-local users,
such as LDAP or Active Directory users.
4. A new setting called "libpam" has been added to pb.settings to specify the
path to the PAM library location.
5. PowerBroker's pbrun, pbsh, and pbksh submit host clients are no longer
required to have the "Server Side" SSL key/certificates. Also the existence
of the CA that signed the SSL Server's certificate on PowerBroker "clients"
is now optional. Only PowerBroker for Unix & Linux (pbmasterd, pblocald, pblogd
and pbguid) require the SSL "Server side" certificates.
6. A "Font Size" field has been added to "View I/O log" window on PBGUI to
allow the user to control the size of the font used when displaying I/O logs.
7. Added synonyms aes-128 for aes-16-16, aes-192 for aes-16-24 and aes-256 for
aes-16-32.
8. PowerBroker now provides a new utility, pbversion, to display the version of
all PowerBroker binaries installed on the host.
9. A new option, 'requiressl', has been added to 'ssloptions' keyword allowing
you to override the default 'allownonssl'. You can use this option when you
require SSL communications between PowerBroker components. A non-SSL
PowerBroker client will not be able to communicate with the master.
10. PowerBroker is now integrated with the Safenet HSM using the SafeNet SSL
engine.
11. New supported platforms
SuSE Linux 9 (PowerPC 32-bit), SuSE Linux 9 and 10 (Power5 64-bit)
Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 5.2.0-11

Issue 1: pbsync was not functioning correctly when encryption was enabled.
Resolution: pbsync now recognize and properly function when the network and
event or I/O log encryption is enabled.
Issue 2: pbrun was filling the syslog with the error "Kernel has lost command"

when runtimeout was reached. pbrun was hanging and consuming virtual memory.

Resolution: This error is now only logged once to the syslog.

Issue 3: When quitting from the command 'pbrun cat <file> | more', the message 3107 was displayed erroneously.

Resolution: PowerBroker now displays the correct "broken pipe" message.

Issue 4: pbguid policy editor was producing a segmentation violation when used with some policies.

Resolution: The issue has been fixed and pbguid is no longer producing a segmentation violation.

Issue 5: On some platforms pbguid event log viewer was producing a segmentation violation with a very large event log.

Resolution: The issue has been fixed and pbguid is no longer producing a segmentation violation.

Issue 6: During an idle pbrun session when submituser was not root and runtimeout was reached, the error "interrupted system call" was displayed.

Resolution: The timeout is now properly handled by PowerBroker for a non-root user.

Issue 7: When PowerBroker daemon (pbmasterd, pblocald, pbguid, pblogd and pbsyncd) were run in daemon mode (-d option) when launching a child process, the child processes were also listening to the associated port.

Resolution: The associated port is now closed for the child processes.

Issue 8: Occasionally, PBGUID was not saving the policy on AIX 5.2 due to a memory corruption.

Resolution: The issue has been fixed.

Issue 9: On AIX 5.x platforms, PowerBroker binairies were linked statically with libpam library.

Resolution: The binaries are now dynamically loading the libpam library.

Issue 10: When Optimized run mode was used, and runtimeout and/or idletimeout was reached, the error displayed was "Command caught signal 15" instead of "runtimeout (or idletimeout) reached.

Resolution: The correct message is now displayed.

Issue 11: The function ldap_getvalues was producing a segmentation violation on Linux Itanium platforms.

Resolution: The issue has been fixed.

Issue 12: Intermittently 'runtimelimit' was not correctly honored by pbrun.

Resolution: The issue has been fixed.

KNOWN ISSUES in RELEASE 5.2.0 on QNX:

QNX is not certified for use as a PowerBroker Master or as a PowerBroker Log Server. QNX is only supported for use as a PowerBroker client (pbrun).

1. Authentication does not work with the PowerBroker GUI. As a result, root is not allowed to login.

2. When TERM is set to xterm on QNX, pbless produces a segmantation fault. Setting TERM to vt100 works.

3. pbsync -l or pbsync -L will fail with the error: "BeyondTrust : temp File is not ready Resource temporarily unavailable".

4. pbcheck will produce a segmanation fault if used with option -e.

5. The shells (pbksh, pbsh) are not fully supported.

6. "pbrun --di <command>" hangs when <command> is a non-existing command or is not in the path.

NEW FEATURES IN RELEASE 5.1.2-06

1. Added a new 'abridged' option to pbcheck -e: For large policies with hundreds of if statements, pbcheck -e could take a very long time to generate entitlement reports. The "Abridged" option is able to produce Entitlement Reports in this situation by ignoring interactions caused by "self-contained" IF statements. A self-contained IF statement is one which always accepts or rejects once you enter it, with no other way of terminating the IF clause.

2. Added a new -p (--policydir) option to pbcheck to control the location of the include files in the configuration policy.

3. Added a new setting called "pamsuppresspbpasswprompt" to pb.settings to control the behavior of PAM prompt.

4. Added a new setting called "transparentfailover" to pb.settings to allow the user to suppress failover messages and to silently failover to the next master or logserver.

5. Added a new setting called "showunsecurewarnings" to pb.settings to allow the user to display licensing error messages even if warnuseronerror is

set to no.
6. A new setting 'port' field was added to the GUI in the Policy Editor,
to allow the user to specify the port number to use an inbound connection
from the browser. Previously the port number between 0 to 1023 was
randomly picked by PowerBroker.
7. Added a new setting "nameresolutiontimeout" to pb.settings to allow the
user to specify the timeout for DNS resolution for all PowerBroker binaries.
Previously this was only possible for PowerBroker Shells.
This new setting replaces the previous "shellnameresolutiontimeout".
8. New options +/- were added to pbreplay to slow down or accelerate the
replay of keystroke files.
9. Added a new menu option to the install and a setting "logfilepermissions"
to pb.settings to allow the user to specify the file permissions with which
various PowerBroker logfiles should be created.
10. pbbench now recognize "include" and "includedir" keywords in
/etc/xinetd.conf.
11. New supported platforms
Mac OS 10.4 and 10.5 PowerPC and Mac OS 10.5 i386
Restrictions:
- On Mac OS platforms, user authentication can only be done through
PAM. During the installation,the option 'pam' is set to Yes and options
'pampasswordservice' and 'pamsessionservice' are set to login.
This would allow authentication functions such as 'getuserpasswd'
to work properly on Mac OS platforms.
- In this release of PowerBroker, the GUI is not supported on Mac OS platforms.

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 5.1.2-05
Issue 1: Occasionally, pbrun exit with error 3107 even when the command was
successful.
Resolution: pbrun no longer exit with error 3107 when standard input is
redirected.
Issue 2: Occasionally, pbrun and/or pblocald processes were hanging when iologging

was on.

Resolution: This was due to child processing issues in PowerBroker processes and is now fixed.

Issue 3: pbreplay --timestamp=%Y/%m/%d %H:%M:%S -I displayed everything twice.

Resolution: This command now correctly displays everything.

Issue 4: Successive invocations of the logmktemp() function in the policy reported "file name too long".

Resolution: File name initialization has been corrected and multiple calls to logmktemp is now correctly setting the file name.

Issue 5: On HP Itanium, environment variables set in the policy were not passed to programs called from the policy.

Resolution: The environment variables are now correctly passed.

Issue 6: pbsyncd launched without any argument produced a seg fault on Solaris 10.

Resolution: pbsyncd no longer produces a seg fault and displays "pbsyncd is meant to be run from inetd only!".

Issue 7: pbuninstall removed inetd.conf and xinetd.conf on RedHat 2.1 and AIX.

Resolution: These files are no longer removed during the uninstall.

Issue 8: The output of "who -R" was truncated when executed from a 'pbrun bash' on HP 11 PA-RISC platforms.

Resolution: The information in utmp/wtmp is now correctly updated.

Issue 9: During the install, when the pbbuildidr directory was set to a system directory, permissions of all files in this directory was changed.

Resolution: pbinstall now only changes the permissions of the PowerBroker files when copied in system directories.

Issue 10: pbreplay options -I, <space> and 'g' were not working properly.

Resolution: pbreplay options -I, <space> and 'g' are now working properly.

Issue 11: During the install, the permissions of /dev/null were changed if the logfile names were set to /dev/null.

Resolution: When logfile names are set to /dev/null, pbinstall no longer alters the permissions of /dev/null.

Issue 12: In certain conditions, when multiple PowerBroker masters were accessing the license file, an error "3510 Problem reading license file" was displayed due to a locking issue of .pb.license.

Resolution: The locking process has been corrected.

Issue 13: pbmasterd seg faults when multipe calls to setenv, getenv are made in the policy.

Resolution: This was due to a memory corruption in pbmasterd and is now fixed.

Issue 14: When SSL is enabled, "pbrun -di cat" of large files failed.

Resolution: This is now fixed.

Issue 15: The function ldap_initialize was not returning null if it failed.

Resolution: The function ldap_initialize now correctly returns null upon failure.

Issue 16: PBGUID was only showing the first shared library in the list of all shared libraries.

Resolution: PBGUID now shows the list of all shared libraries.

Issue 17: PBGUID configuration item "timeout" incorrectly displayed the default value instead of displaying the current value of the timeout.

Resolution: PBGUID configuration item now correctly shows the current value of the timeout.

NEW FEATURES IN RELEASE 5.1.1-02

1. On HPUX and AIX platforms, PowerBroker binaries are no longer statically linked with Kerberos, OpenSSL and OpenLDAP libraries. These libraries are now provided as shared libraries and dynamically loaded at run time if needed.

SIGNIFICANT BUG FIXES IN RELEASE 5.1.1-02

Issue 1: On AIX and HPUX, the start date and logoff status was not recorded correctly in wtmp.

Resolution: This has been corrected.

NEW FEATURES IN RELEASE 5.1.0-08

1. On Linux and Solaris platforms, PowerBroker binaries are no longer statically linked with Kerberos, OpenSSL and OpenLDAP libraries. These libraries are now provided as shared libraries and dynamically loaded at run time if needed.

SIGNIFICANT BUG FIXES IN RELEASE 5.1.0-08

Issue 1: pbrun failed with error logging subsystem failure when the file system where the logfile resides had over 2.5TB of free space.

Resolution: This has been corrected.

Issue 2: pbguid: the size of character fields present in the reports was limited to 100 characters.
Resolution: The maximum size of character fields has been increased to 500 characters.

BUG FIXES IN PATCH 5.0.4-06-SP1

- If the amount of free space in the log directory was larger than 2,147,483,647K PowerBroker failed to write to the logfile with the following error:
"3387.01 insufficient file system for log file xxxx".

SIGNIFICANT BUG FIXES IN RELEASE 5.0.4-06

Issue 1: pblocald consume cpu when the window where pbrun was running in disabled optimized run mode is killed.
Resolution: Blocked Signal handling has been corrected.

NEW FEATURES IN RELEASE 5.0.4 (5.0.4-05)

1. Added MD5 checksum verification to pbsum. The runmd5sum variable was added to store an MD5 checksum value.
2. New supported platforms
Debian GNU/Linux 4.0 (32-bit and 64-bit), VMware ESX 3.0 (x86 32-bit), RedHat 4.0 Itanium, RedHat 5.1 (x86 32-bit and 64-bit)
Please refer to the README file for the specific flavor names.
3. From this release of PowerBroker, the tar file pbhppa_hpuxB should be used for all HP-UX PA-RISC (32-bit and 64-bit) platforms.
Please refer to the README file for the specific Unix versions.

SIGNIFICANT BUG FIXES IN RELEASE 5.0.4 (5.0.4-05)

Issue 1: pbvi, pbnvi, pbless failed to open files correctly, failed to display data, or failed with "unknown terminal type" message.
Resolution: These utilities now operate correctly.
Issue 2: pbmasterd seg faults when gsub with empty string as second argument is used in the policy.

Resolution: The gsub policy function has been fixed.

Issue 3: pbrun exits with 3107 error code when stdin is redirected.

Resolution: pbrun handling of redirected stdin has been corrected.

Issue 4: pbrun bash ignores interrupts (^C).

Resolution: Interrupt handling has been corrected.

Issue 5: pbrun pbksh hangs when exiting pbksh.

Resolution: SIGCHLD handling has been corrected.

Issue 6: pbrun or pblocald consume cpu when window is killed.

Resolution: SIGCHLD handling has been corrected.

Issue 7: pbguid fails to display eventlog details.

Resolution: pbguid now displays eventlog details.

Issue 8: pbsync reports the imported log is not complete, but the transaction is complete.

Resolution: The correct log size is now transmitted.

Issue 9: pbinstall default installation changed encryption from des to none.

Resolution: Default installation now sets encryption to des.

Issue 10: PB master failover fails on AIX with round robin DNS.

Resolution: Round robins DNS is now handled correctly.

Issue 11: Intermittently commands using a pipe will error with "broken pipe" under pbksh.

Resolution: This is now fixed.

Issue 12: Option -c of pbreplay was not working correctly.

Resolution: This is now fixed.

Issue 13: A problem was introduced in 5.0.3 where saved iologs were no longer replayed correctly.

Resolution: This is now fixed in 5.0.4, however 5.0.3 iologs will not replay correctly.

Issue 14: pbguid errors with "5406.05 listen: Protocol not supported."

Resolution: This is now fixed.

Issue 15: PowerBroker password prompt was suppressed in password functions.

Resolution: This is now fixed.

Issue 16: pbbench -V was returning IPv4-mapped IPv6 addresses when comparing Forward and Reverse DNS lookup.

Resolution: This is an issue on systems that where IPv6 is supported but IPv4

is enabled. This is now fixed.

Issue 17: When pbguid was in daemon mode, policy editor was showing "illegal attempt to open" when attempting to open the configuration file.

Resolution: This is an issue on systems that where IPv6 is supported but IPv4 is enabled. This is now fixed.

Issue 18: wtmp file was corrupted due to an errorneous pid.

Resolution: This is now fixed.

KNOWN ISSUES in RELEASE 5.0.4 on QNX:

QNX is not certified for use as a PowerBroker Master or as a PowerBroker Log Server.

QNX is only supported for use as a PowerBroker client.

1. Authentication does not work with the PowerBroker GUI. As a result, root is not allowed to login.

2. When TERM is set to xterm on QNX, pbless produces a segmantation fault. Setting TERM to vt100 works.

3. pbsync -l or pbsync -L will fail with the error: "BeyondTrust : temp File is not ready Resource temporarily unavailable".

4. pbcheck will produce a segmanation fault if used with option -e.

NEW FEATURES IN RELEASE 5.0.3-4

1. New supported platforms

HP-UX 11i v3 Itanium(B.11.31), HP-UX 11i v3 PA-RISC and IBM AIX v6.1 (POWER 64-bit) are now supported.

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 5.0.3-4

Issue 1: pblocald consume cpu when window is killed.

Resolution: SIGCHLD handling has been corrected.

Issue 2: In optimized run mode, when pbrun window is killed, other processes were killed as well.

Resolution: SIGCHLD handling has been corrected.

Issue 3: In the previous build of PowerBroker 5.0.3 for sparc-solaris (sparc_solarisC tar files) the binairies were not compatible on Solaris

SparcStation and were only running on UltraSparc.

Resolution: This is now fixed.

NEW FEATURES IN RELEASE 5.0.3

1. New supported platforms

Red Hat Enterprise Linux 5 and SuSE Linux Enterprise Server 10 are now supported on the x86 (32 and 64 bit) architectures.

Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, and SuSE Linux Enterprise Server 10 are now supported on the IBM s/390 31 bit and 64 bit architectures.

Please refer to the README file for the specific flavor names.

SIGNIFICANT BUG FIXES IN RELEASE 5.0.3

Issue 1: In previous versions, PowerBroker secured tasks used to be executed from the "/tmp" directory when the runuser lacked the necessary permissions to be in the runcwd. This occurred whenever the submituser submitted the secured request from a directory where the runuser set by the policy lacked the necessary permissions and the policy failed to set the runcwd.

Resolution: A new keyword has been added to pb.settings; "enforceRunCWD" enforces the runcwd when set to "yes" or when it is not set (default). When set to "yes" and the user does not have permissions for the runcwd, the task is rejected. When set to "no" PowerBroker reverts to the old behavior of running the command in "/tmp".

Syntax:

enforceRunCWD <yes|no>

Valid Values:

yes Enforce the runcwd and do not run in /tmp

no Revert to old behaviour and run in /tmp

Example:

enforceRunCWD yes

Issue 2: Normal pbksh and pbsh startup could be blocked by name resolution mechanisms when the network is down.

Resolution: The new pb.settings keyword "shellNameResolutionTimeout" allows a timeout mechanism for the name resolution, and allows pbksh and pbsh to start in native root mode. The allowed values can range from 0 to 7200 seconds.

Syntax:

shellNameResolutionTimeout <number>

Valid Values:

0 Disable PowerBrokers' name resolution timeout feature

number Defines the timeout value, in seconds

Example:

shellNameResolutionTimeout 45

Issue 3: A buffer boundary overflow vulnerability exists in the PowerBroker clients pbrun, pbksh, and pbsh.

Resolution: Corrected boundary checking.

Issue 4: PowerBroker failed to execute some shell scripts on NCR; execution of some NCR shell scripts could possibly return a root shell.

Resolution: NCR platform shell script execution was corrected.

Issue 5: PowerBroker syslog entries for pass/fail were reversed; successful commands were recorded as failures.

Resolution: Exit status recorded on the syslog messages was corrected.

Issue 6: Erroneous iologsyncpath warning displayed in pbbench.

Resolution: Misleading message was removed.

Issue 7: pbrun can intermittently result in a "3107 exited abnormally" message and return a non-zero exit status, even when the secured task ran successfully.

Resolution: Fixed pbrun to preserve exit status.

Issue 8: Piping the output of pbrun to a non-existing command hangs the shell session.

Resolution: Fixed pbrun to display a write error failure message and exit gracefully.

Issue 9: pbcheck resulted in a segmentation fault while executing an entitlement report when the "getstringpasswd" function is used on

the policy.

Resolution: pbcheck now successfully generates an entitlement report.

Issue 10: pbguid may generate a segmentation fault error message when accessed with some versions of Internet Explorer. Firefox, Opera, and other browsers do not exhibit this behaviour.

Resolution: pbguid was corrected to address incompatibilities with Internet Explorer.

Issue 11: Executing pbsyncd with no options results in a segmentation fault.

Resolution: Changed pbsyncd defaults to run without options

Issue 12: PAM/Kerberos-based submitconfirmuser (pbrun), getuserpasswd (pbmasterd), or runconfirmuser (pblocald) fail.

Resolution: These functions now work with PAM using Kerberos.

Issue 13: Invoking pbsync client when there are no logservers entries in pb.settings results in a segmentation fault.

Resolution: Fixed pbsync to display an error message and exit gracefully.

Issue 14: pbbench failed if SSL was enabled and pbsyncd was installed.

Resolution: Resolved the inconsistancies between pbbench and pbsyncd.

Issue 15: If a PowerBroker policy called the rubstr function without a length argument, a bus error would result.

Resolution: Fixed the interpreter to resolve this issue.

Issue 16: PowerBroker corrupts wtmp on HP-UX.

Resolution: Corrected the data written to wtmp.

Issue 17: If the specified runhost does not have PowerBroker installed, the reported host name in the eventlog contains a trailing "[a]".

Resolution: Trailing characters were removed.

Issue 18: Licensing algorithm could truncate license file, generating a "3514 Bad header in license message" error.

Resolution: Modified algorithm to prevent the corruption of the license file.

Issue 19: Replaying a corrupt keystroke file could result in pbreplay or pbguid encountering a segmentation fault.

Resolution: pbreplay and pbguid no longer terminate with a segmentation fault when replaying a corrupt keystroke log file.

Issue 20: pbsync does not merge local event logs.

Resolution: pbsync modified to merge all event logs.

Issue 21: pbinstall enters an endless loop if it cannot determine the platform.

Resolution: Fixed pbinstall to exit with an error message.

Issue 22: Ambiguous keyword "pbiologsyncpath".

Resolution: The keyword is no longer supported.

Issue 23: Installed GUI example policy does not support Entitlement Reports.

Resolution: A new example policy distributed; it contains support for entitlement reports.

Issue 24: pbreplay fails to display a time stamp, and on the screen when using the space bar.

Resolution: Modified pbreplay to display the time stamp then the --timestamp or -t options are used with the combination of the space bar.

Issue 25: PowerBroker LDAP libraries conflict with native nss LDAP libraries, resulting in a segmentation fault.

Resolution: PowerBroker binaries were modified to resolve this issue.

Issue 26: Executing an entitlement report from the GUI may fail and display the message: "Error: pbcheck process (pid:xxxx) exit status 65280"

Resolution: pbcheck was corrected to fix this issue.

Issue 27: Math overflow problems cause PowerBroker log servers to see a negative amount of disk space, resulting in a rejected command.

Resolution: Disk space calculations were corrected.

Issue 28: pbmasterd and pblicense had licensing problems.

Resolution: Licensing problems have been resolved.

Issue 29: pbrun terminated with signal 58 unknown signal code on AIX

Resolution: DLPAR signal handling was added

SIGNIFICANT BUG FIXES IN RELEASE 5.0.2

Issue 1: pbksh does not startup in a timely fashion when network issues are occurring.

Resolution: pbksh now responds quickly in native root mode during network problems.

NEW FEATURES IN RELEASE 5.0.1

1: The new policy language mastertimelimit variable specifies a time limit, between pbmasterd and pblocald, for a task request. If the job does not finish within the specified number of seconds, it is terminated. This is similar to mastertimeout, but is based on total time rather than idle time. This is similar to runtimelimit, from the pbmasterd point of view.

Syntax:

mastertimelimit = number;

Valid Values:

number Enable time limit checking

0 Disable time limit checking. This is the default.

Example:

mastertimelimit = 3600;

2: The new policy language mastertimeout variable specifies the amount of idle time in seconds, between pbmasterd and pblocald. If the job is idle for the specified number of seconds, it is terminated. This is similar to runtimeout, from the pbmasterd point of view.

Syntax:

mastertimeout = number;

Valid Values:

number Enable idle checking

0 Disable idle checking. This is the default.

Example:

runtimeout = 3600;

SIGNIFICANT BUG FIXES IN RELEASE 5.0.1

Issue 1: suffixed install followed by non-prefix/suffix install erases suffixed entries from inetd.conf.

Resolution: pbinstall has been fixed.

Issue 2: pbbench reports errors querying for ports, though pbrun works fine.

Resolution: The pbbench port checks have been changed to warnings.

Issue 3: `pbguid -d` results in segfault.

Resolution: `pbguid -d` now displays the help information and indicates that -p is required with -d.

Issue 4: GUI doesn't display error message when invalid statements are set in policy editor.

Resolution: the GUI now displays an error message when invalid statements are encountered in the policy editor.

Issue 5: pbksh, in native root mode, changes tty characteristics.

Resolution: tty handling has been updated.

Issue 6: `pbrun cat file | less` changes tty characteristics.

Resolution: tty handling has been updated.

Issue 7: pbksh `cat file | wc -l` intermittently returns incorrect results.

Resolution: Timing issues have been addressed so that the complete output is transmitted or piped appropriately.

Issue 8: pb 5.0.0 ssl implementation fails.

Resolution: ssl implementation has been addressed.

Issue 9: `pbrun cat` truncates data intermittently.

Resolution: Timing issues have been addressed so that the complete output is transmitted appropriately.

Issue 10: scp fails when runuser's shell=pbksh & policy system call is used.

Resolution: The policy system() function has been fixed so it does not interfere with scp protocol.

Issue 11: pb shells do not iolog when master and log server are not available.

Resolution: pb shells now iolog when master and log server are not available.

Issue 12: Expression Editor window look-and-feel does not match GUI.

Resolution: Expression Editor window look-and-feel has been updated to match current GUI.

Issue 13: PB syslog entries for pass/fail are reversed.

Resolution: PB syslog entries for pass/fail are now fixed.

Issue 14: PB connections fail when the remote host name is (properly) empty.

Resolution: PB connections now work when the remote host name is empty.

Issue 15: pbcheck segfaults when processing includes in an entitlement report.

Resolution: pbcheck now correctly processes includes in entitlement reports.

Issue 16: Extra quotes are added to day names by pbguid.

Resolution: Extra quotes are no longer added to day names by pbguid.

Issue 17: pbreplay space (go to next input) not working properly in V5.0.

Resolution: pbreplay space now functions correctly.

Issue 18: `pbreplay --timestamp` results in "invalid pointer" message.

Resolution: pbreplay --timestamp option has been fixed.

Issue 19: pbbench command fails when SSL and pbsyncd settings are set.

Resolution: pbbench no longer fails when SSL and pbsyncd settings are set.

Issue 20: Authentication fails using PAM and Kerberos.

Resolution: Authentication now functions properly when using PAM and Kerberos.

Issue 21: insert policy function does not work.

Resolution: The insert() policy function has been fixed.

Issue 22: pbguid policy editor has no support for ACL.

Resolution: pbguid policy editor now supports ACLs.

Issue 23: when setkeystrokeaction ends the execution, ends via
3091 Terminated on protocol failure

Resolution: Execution is now terminated without the protocol failure message.

Issue 24: encountering keystroke set by setkeystrokeaction results in
multiple finished events.

Resolution: multiple finished events are no longer logged.

Issue 25: printvars intermittently prints without returning to
the beginning of the next line.

Resolution: printvars output now displays correctly.

Issue 26: setkeystrokeaction results in pblog reporting:
unknown variable keystrokestatus.

Resolution: keystrokestatus is now logged when setkeystrokeaction terminates
execution.

Issue 27: clients maintain a connection in CLOSE_WAIT status.

Resolution: clients no longer maintain a connection in CLOSE_WAIT status.

Issue 28: pbsync fails with des encryption.

Resolution: pbsync now works with des encryption.

Issue 29: Tru64 5.1B needs additional calls to set_auth_parameters().

Resolution: Authentication now functions on Tru64 5.1B.

Issue 30: pbrun in the background gets sigttou and hangs.

Resolution: pbrun in the background no longer hangs due to sigttou.

Issue 31: pbbench tries connection to pbsyncd when no pbsyncd is configured.

Resolution: pbbench no longer attempts to connect to pbsyncd when pbsyncd
is not configured.

Issue 32: runtimeout and runtimelimit result in finish event and exittime logged twice.

Resolution: finish event and exittime values are now logged once.

Issue 33: pbguid: open help window from show all variables link does not work.

Resolution: help link now works.

Issue 34: pbcheck -e seg faults on getuserpasswd() and submitconfirmuser().

Resolution: pbcheck -e no longer seg faults.

Issue 35: unsetenv() doesn't unset the environment variable.

Resolution: unsetenv now properly unsets the environment variable.

Issue 36: PB 5.0 pbmakeremotetar broken.

Resolution: pbmakeremotetar has been fixed.

Issue 37: pbrun segfaults when executed in a directory where the user has no read permissions.

Resolution: pbrun no longer terminates with Signal 11 when executed in a directory where the user has no read permissions.

Issue 38: `pbsync -d` when syncing eventlog improperly creates temp file that contains the string iolog

Resolution: Temporary file now has a more appropriate name.

Issue 39: pbuninstall: removes but does not unconfigure pbsyncd.

Resolution: pbuninstall now unconfigures pbsyncd.

Issue 40: using "localhost", pbrun request hangs/times out.

Resolution: pbrun request now completes without hanging or timeout.

Issue 41: log server connection dropped while browsing a corrupt iolog file.

Resolution: corrupt iolog file no longer causes log server connection to drop.

Issue 42: pbless help displays incorrect options.

Resolution: pbless help is now correct.

Issue 43: pbguid event reporting: date field in header and footer shows time, not date.

Resolution: pbguid date field now contains the date.

Issue 44: pbguid rewrites encrypted settings file as cleartext.

Resolution: pbguid now rewrites encrypted settings file as encrypted.

NEW FEATURES IN RELEASE 5.0.0

1. New policy language statements

The policy language has been extended with new functions and
new formats for the accept and reject statements.
New function grep - a native policy language interface to the
Unix grep command.
New function fgrep - a native policy language interface to the
Unix fgrep command.
New function egrep - a native policy language interface to the
Unix egrep command
New function tolower - convert a string to all lowercase.
New function toupper - convert a string to all uppercase.
New function getstringsetting - return a string value
from the settings file.
New function getnumericsetting - return a numeric value
from the settings file.
New function getlistsetting - return a list value
from the settings file.
New function getyesnosetting - return a boolean value
from the settings file.
2. Entitlement reporting
pbcheck has been extended to provide entitlement reports based on
the security policy. This will return a report detailing who
can run commands and under what conditions.
3. New GUI interface
The GUI has been made more user friendly.
4. Log synchronization
Two new programs, pbsync and pbsyncd, have been added to synchronize
I/O and event logs from one machine to another.
5. New settings
All of the new settings are to support the log synchconization system.
These are:
syncport: the TCP/IP port to be used by pbsync and pbsyncd
pbsynclog: Absolute path to the pbsync diagnostic log
pbsyncdlog: Absolute path to the pbsyncd diagnostic log
logresynctimermin: How often pbsync should resynchronize

files, when in daemon mode

pbiologsyncpath: List of paths for pbsync to synchronize

when in daemon mode

6. PowerBroker Shell extensions

The shell builtins and shell I/O redirections now honor the runuser,

rungroup and runumask variables.

7. Large File System Support

PowerBroker client and daemon programs are now large-filesystem aware.

8. Optimized Program Structure

When a log server is used and the submit host and run host are the

same machine, pblocald is no longer needed. This reduces startup

overhead, network traffic, eliminates spoofing and increases

security.

9. pbreplay displays time stamps.

pbreplay can now display user-defined timestamps on each line of

output.

SIGNIFICANT BUG FIXES IN RELEASE 5.0.0

KNOWN ISSUES

1.The installation suite requires the superdaemon configuration

files (the files which control inetd and xinetd) to be

non-executable. pbinstall currently reports this as:

Looking for SuperDaemons to configure...

cannot find a superdaemon (inetd or xinetd)

configuration file!

The work-around is to remove the execution bits from the

superdaemon configuration file(s) and retry the installation.

2. The policy language setting warnuseronerror may not be

changed by pbinstall. The work-around is to either use

the web-based settings GUI via pbguid or pbsguid or to

directly edit the setting in the settings file.

3. When a master daemon is installed with a log daemon it is

possible, but not desirable, to successfully install

PowerBroker without specifiying one or more log hosts. If this occurs, the settings file on the master hosts must have the logservers setting added either through the web-based settings GUI or via a text editor.

4. Daemon error log files may be created by pbinstall for daemons not installed on the system. The extraneous files may be removed.

5. Although pbbuilder is no longer distributed, the pbbuilder directory is created and populated with html files when pbguid or pbsguid is installed.

6. No free space checks are done on /tmp (or $TMPDIR) by the installation suite when it is on its own filesystem.

The work-around is to ensure there is adequate free disk space on /tmp for the installation or remote installation function.

---

* FOR QUESTIONS, ORDERS, PROBLEMS, OR COMMENTS *

* FOR ON-SITE TRAINING INFORMATION *

* FOR PRODUCT UPGRADES *

Contact BeyondTrust Software

BeyondTrust Software, Inc.
5090 North 40th Street, Suite 400
Phoenix, AZ 85018
Phone: +1 (800) 234-9072 (General Questions)
+1 (818) 575-4040 (Technical Support)
Fax: +1 (818) 889-1894
E-mail: pb-support@beyondtrust.com
Web: http://www.beyondtrust.com